REPORT ON CYBER LESSONS LEARNED DURING THE WAR IN UKRAINE

MINISTRY OF NATIONAL DEFENCE OF THE REPUBLIC OF LITHUANIA

NATIONAL CYBER SECURITY CENTRE

REGIONAL CYBER DEFENCE CENTRE

REPORT ON CYBER LESSONS LEARNED DURING THE WAR IN UKRAINE

MINISTRY OF NATIONAL DEFENCE OF THE REPUBLIC OF LITHUANIA

NATIONAL CYBER SECURITY CENTRE

REGIONAL CYBER DEFENCE CENTRE

Table of Contents

01. Preface

The world's attention is focused entirely on the events in Ukraine but it is important to remember that cyber warfare also plays a massive role on the real-life battlefield. The Regional Cyber Defence Centre (RCDC), a subsidiary of the National Cyber Security Centre under the Ministry of National Defence of Lithuania, has developed a Report on Cyber Lessons Learned during the War in Ukraine.
The study was developed by the RCDC Cyber Threat Analysis Cell (CTAC) team and rotating personnel from Poland, Georgia, the United States of America, and Ukraine. Information was gathered mainly by means of Open Source Intelligence and as made available and declassified by Ukraine.

02. List of Acronyms

TERM/ ABBREVIATION	MEANING/ EXPLANATION
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CMS	Content Management System
CTAC	Cyber Threat Analysis Cell
DDoS	Distributed Denial of Service
Disinformation	Disinformation refers to false information intended to manipulate, cause damage or guide people, organisations, and countries in the wrong direction.
DNS	Domain Name System
FSS (FSB)	Federal Security Service (Russian: Федеральная служба безопасности Российской Федерации)
GDP	Gross Domestic Product
MDGS (GUGS/GRU)	The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Russian: Главное разведывательное управление Генерального штаба Вооружённых Сил Российской Федерации)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICS	Industrial Control System
IOC	Indicators of Compromise
IoT	Internet of Things
ISP	Internet Service Provider
Malinformation	Malinformation refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.
MBR	Master Boot Record
Misinformation	Misinformation refers to false information that is not intended to cause harm.

TERM/ ABBREVIATION	MEANING/ EXPLANATION
NCSC	National Cyber Security Centre
NSA	National Security Agency
RAT	Remote Access Trojan
RCDC	Regional Cyber Defence Centre
SOC	Security Operation Center
SSSCIP	State Service of Special Communications and Information Protection of Ukraine, SSSCIP (Ukrainian: Державна служба спеціального зв'язку та захисту інформації України)
FIS (SVR)	Foreign Intelligence Service of the Russian Federation (Russian: Служба внешней разведки Российской Федерации)
TCP	Transmission Control Protocol
TOR	The Onion Router
TTP	Tactics, Techniques, and Procedures
UDP	User Datagram Protocol
UTF	Unicode Transformation Format
WAF	Web Application Firewall

03. Introduction

03.1. Context and Objectives of the Project

Established as a joint initiative of Lithuania and the United States, the Regional cyber defence centre (RCDC) aims to fill the niche of practical cooperation in the field of cyber defence and to strengthen the capacity of both Lithuania and the regional partners to ensure cyber security of states. One of the main aims of the RCDC is to become a regional platform for practical cooperation in helping protect critical infrastructure from cyber attacks. Therefore, to achieve this objective, RCDC activities focus on strengthening resilience and cyber defence capacity of critical public service providers.

The overall objective of this project is to develop a Report on Cyber Lessons Learned during the War in Ukraine starting 2022 until time of publishing this report. More specifically, the Report provides a follow-up on the previous study, Report on Russia's Use of Offensive Cyber Capabilities during the Military Aggression in Ukraine. This intervention is expected to result in several critical outcomes for the RCDC and partner countries:

01. An in-depth analysis of cyber incidents in infrastructure of various sectors.

02. Hardening/proactive and defensive measures taken against the emerged threats.

03. Lessons Learned or identification of the weak links and the best way to mitigate the risk.

04. Synchronization of kinetic and cyber operations.

05. Development of methods and techniques used for detection of cyber incidents and events.

03.2. Approach and Methodology

To achieve the Project objectives, the Report on Cyber Lessons Learned during the War in Ukraine is based on:

01. Secondary research – and an in-depth review and analysis of international open-source information and studies.

02. Analysis carried out by RCDC experts with assistance from the rotating personnel from Poland, Georgia, the United States of America, and Ukraine.

The research is aimed to conclude in the Report on Cyber Lessons Learned during the War in Ukraine providing a systemic analysis of cyberwar over the course of the aggression against Ukraine: how certain attacks affected different sectors, the main attacker's objectives, how the attacks were handled, and the lessons learned from the attacks.

03.3. Proposed Structure of the Report

The Report is proposed to be divided into several separate parts:

- Chapter 4 is the Executive Summary;
- Chapter 5 provides analysis of the public administration sector;
- Chapter 6 focuses on the private sector;
- Chapter 7 offers an analysis of the military sector;
- Chapter 8 looks into the critical infrastructure sector;
- Chapter 9 reviews the combination of different attacks on multiple targets;
- Chapter 10 analyses and discusses the following Distributed Denial of Service, or DDoS, attacks that play a big role in this war;
- Chapter 11 reviews the strategic communication during the cyber crisis;
- Chapter 12 introduces conclusions;
- Chapter 13 proposes a way forward.

04. Executive Summary

Key Observations and Conclusions

- Russia deployed and exhausted its cyber capabilities just before and at the start of the invasion on February 24 2022. Many attacks targeted Ukraine's critical infrastructure to disrupt its operation.
- Since Russia focuses on crippling critical infrastructure, it is safe to say that cyber operations are and will be used as joint operations in support of kinetic war operations in the future.
- The Russian cyber operations have aimed to undermine Ukraine's military operations, economic, and governmental sectors, gain access to critical infrastructure, and restrict the public's access to information.

What

- Research conducted by experts from Lithuania, the United States of America, Georgia, Ukraine, and Poland. It looks deeper into the events occurring before Russia invaded Ukraine on February 24 2022 and onward.
- Open-source information, expertise of members of the Armed Forces of Ukraine.
- An in-depth analysis of cyber incidents in infrastructure of various sectors.
- Hardening of proactive and defensive measures taken against the developed threats.
- Lessons Learned or identification of the weak links and the best way to mitigate the risk.
- Synchronization of kinetic and cyber operations.

So What

- The Russian cyber offences failed to cripple Ukraine's infrastructure for a prolonged period of time.
- Ukraine managed to reduce the damage to its infrastructure by migrating its infrastructure to a cloud solution.
- After every cyber attack, Ukraine's infrastructure systems became less vulnerable.
- Cooperation between institutions and nations is a crucial part in keeping infrastructure protected.
- At first, defence was the main priority in infrastructure protection; as of now, however, they are also focused on an offensive strategy.

What's Next

- Continued strengthening of cooperation and information sharing between nations as it drastically improves security.
- Focus on Russia's cyber capabilities, intelligence, patterns, tactics and tools.
- Using lessons learned in the cyberwarfare in Ukraine, hardening infrastructure to minimise potential damage.
- The Russians mostly concentrate on DDoS assaults, propaganda and defamation operations, and phishing. As a reult, Ukraine is paying more attention to the specifics of such attacks.
- Russia is struggling in reaching its goals, it is going to turn to China which is trying to get a foothold and status in the geopolitical situation in Europe.

- Russia is trying to find new allies and help with their cyber/military operations, which will potentially create more damage.
- It is almost certain that state-sponsored cyber threat actors from Russia will continue their operations to further the strategic and tactical goals of the Russian military in Ukraine.
- Even though the Russian cyber activity mainly focuses on targets in Ukraine, there is a high probability of spillover attacks occurring in Europe and the countries supporting Ukraine.
- Cyber security is no longer an epert-specific matter. In every country, people are the frontline defence against cyber attacks.

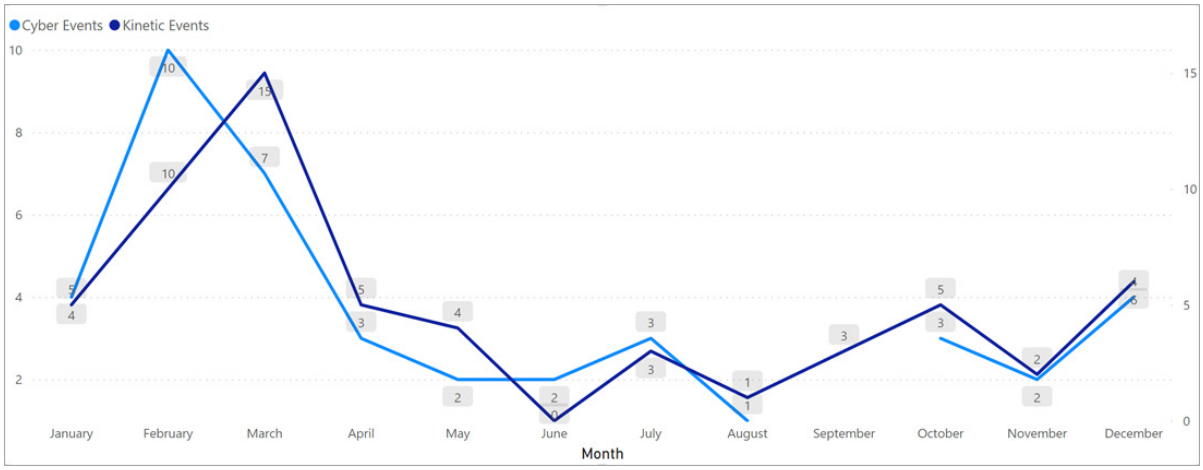


Figure 1. **Kinetic and Cyber Event Timeline**

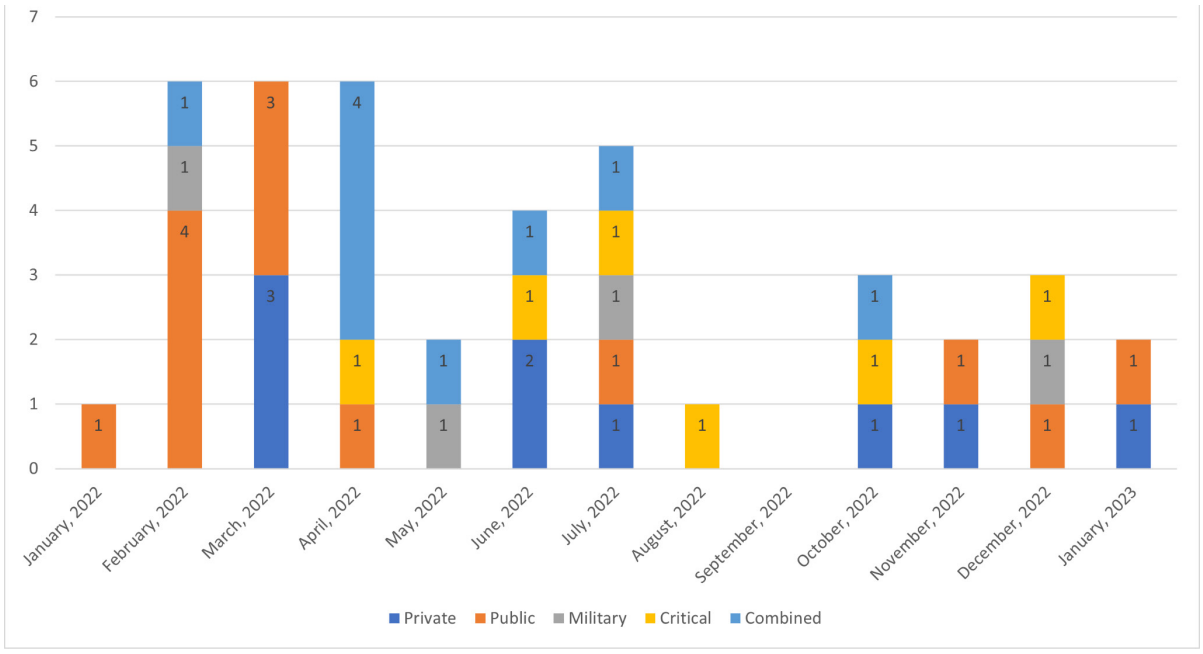


Figure 2. **Timeline of cyber events by sectors**

05. Public Administration Sector Analysis and Lessons Learned

The public administration sector, also called the government sector, is part of the economy composed of both public services and public enterprises. Public administration sectors include public goods and governmental services, such as the military, law enforcement, infrastructure, public transit, and public education, along with healthcare and those working for the government itself, such as elected officials. The effectiveness of a nation's public administration and governance has a significant impact on both the prosperity of its people and its economy. Public administrations that are effective meet the needs of both citizens and businesses. Public authorities must be capable of adapting to shifting conditions. That is why information resources and systems in Ukraine's public administration sector became the main target for the Russian APTs. Ukraine's public administration sector is very heterogeneous regarding the existing equipment and infrastructure, digital services available and data confidentiality, areas of responsibility, and expert involvement. Although providing cyber security is a collective duty of national importance, there are different ways ensuring it in Ukraine depending on the criticality, rules of regulation, experts budget available.

The Government of Ukraine had a global strategy for cyber defence of the public administration sector assets prior to 24 Feb 2022. However, that plan was based on entirely different deadlines, challenges, and budgets. Ukraine had to change it on the fly, in a fast-changing environment, facing new threats and attacks. It has resulted in a revisited and significantly improved role of cyber defence by means of strengthening interdepartmental communications and common usage of unified platforms (the National Cybersecurity Coordination Center and CERT-UA), establishment of new cyber security divisions (in particular, in the Armed Forces of Ukraine), and reorganising law regulations.

Historically, it has been difficult to evaluate the health of the entire Ukrainian public administration sector, but one possible way of evaluating this is by observing the public administration sector spending reported to the World Bank. As shown in the the graph below, we can see a slowdown in the spending during 2015 and 2016, but it has steadily increased since 2017 indicating a steady investment in the national infrastructure. The sector started to invest in modern technologies, including in cyber defence capabilities. Cyber attacks against the public administration sector threaten e-government operations, security of confidential and sensitive government information, and availability of services.

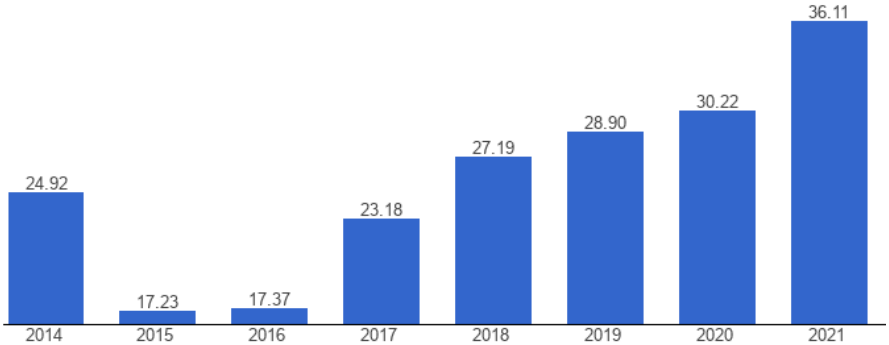


Figure 3. **Public Administration Sector Spending Graph**

Cyber attacks on the public administration sector threaten e-government operations, security of confidential and sensitive government information, and access to services.

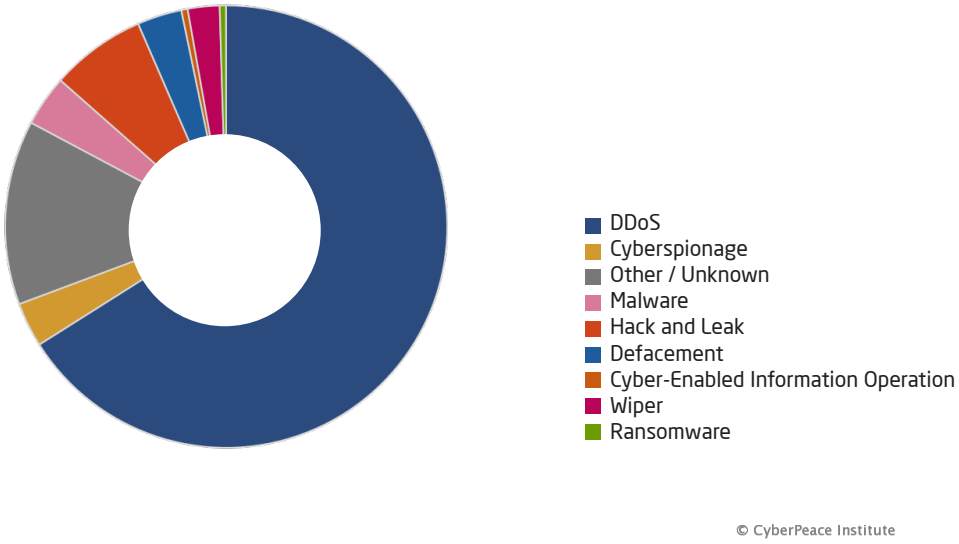


Figure 4. **Documented Types of Attacks against the Public Administration Sector**

The general goal of the cyber attacks conducted before and after the large-scale invasion against the Ukrainian public administration sector was to block citizens' access to state information resources and spread disinformation thus destabilising the socio-political situation in Ukraine.

Destructive wiper attacks were launched by government-supported APT's associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) against hundreds of systems of the Ukrainian Government, as well as the country's energy, IT, media, and financial sectors. The following malware variants were used at once: WhisperGate, HermeticWiper, HermeticRansom, CaddyWiper, DesertBlade, Industroyer2, IsaacWiper, DoubleZero, etc. The listed malware variants are designed to perform a range of malicious operations, such as stealing and deleting data or destroying target computer systems.

The main objective of the attacks was to weaken Ukraine's political governance in the eyes of its citizens and thus diminish their will to resist an occupation. Another objective was to gather the information that would later be used for gaining tactical, operational and strategic advantage on the battlefront. Numerous cyber attacks were presumably carried out by Russian threat actors affiliated with the GRU, Foreign Intelligence Service (SVR), and the Federal Security Service (FSB) to reach that objective.

Public administration sector entities in Ukraine were targeted by threat actors in the interest of the Russian Government even before the start of the full-scale invasion. All available evidence indicates that Russia conducted a coordinated broad cyber campaign intended to provide its forces with an early advantage at the course of the war in Ukraine. The graph below shows quantitative indicators of informational messages about cyber attacks against the Government of Ukraine; the highest figures seen in February and March 2022 speak of Russia's intentions to disorganize the state administration system and increase the psychological pressure on Ukrainian citizens using the cyber component .

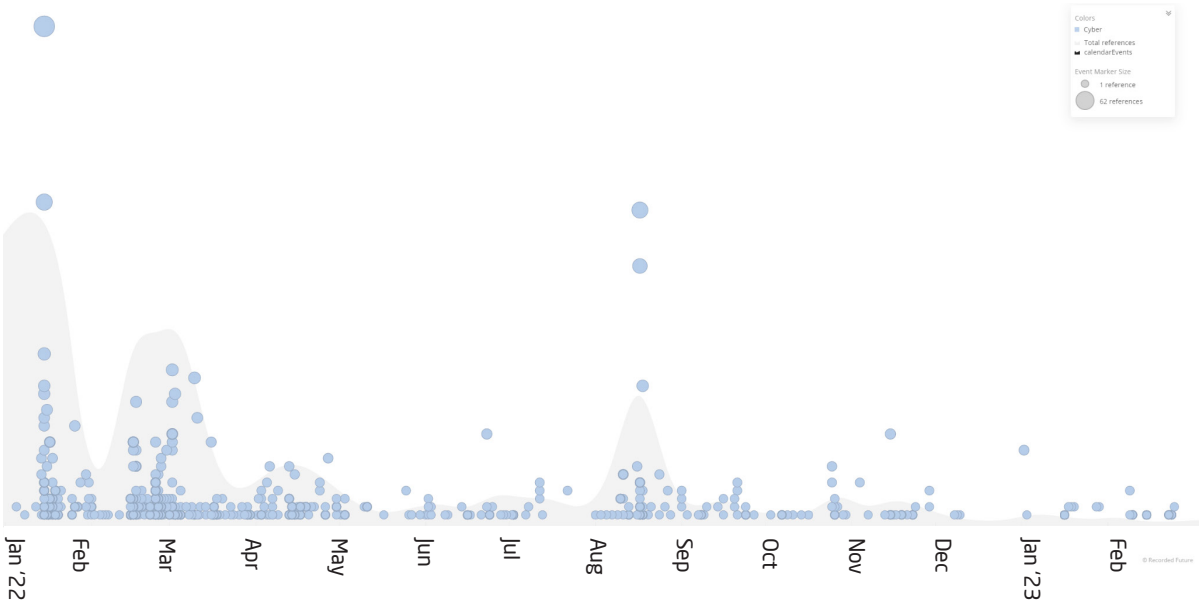


Figure 5. **Cyber attacks (malicious cyber activity) against Ukrainian governmental organizations 2022-2023**

05.1. The Most Significant Cyber Incidents in the Public Administration Sector of Ukraine

ATTACK AGAINST GOVERNMENTAL ASSETS

DATE: January 13 - 14, 2022.
TARGETS: Multiple governmental websites.
TTP's: T1195, T1078, T1072, T1491, T1486, T1485.

DESCRIPTION AND OBSERVED IMPACT:

On January 13 and 14, weeks before the military invasion of Ukraine, over 70 of Ukraine's government institutions were targeted and defaced by UNC1151 to destabilise the day-to-day life in the country. Websites of public institutions were defaced with political imagery and a statement in Russian, Ukrainian, and Polish. Among the affected, there were sites of the Cabinet of Ministers, and the Ministries of Energy, Sports, Agriculture, Veterans' Affairs, and Ecology. According to a report of the Chairman of the State Service of Special Communications and Information Protection of Ukraine: 22 websites of state authorities were hit, information systems were significantly damaged in six of them; a result of the incident, 70 websites were disabled by decree of the SSSCIP and the Security Service of Ukraine (SSU); within three days, the infrastructure was restored without any sensitive information loss having occured.

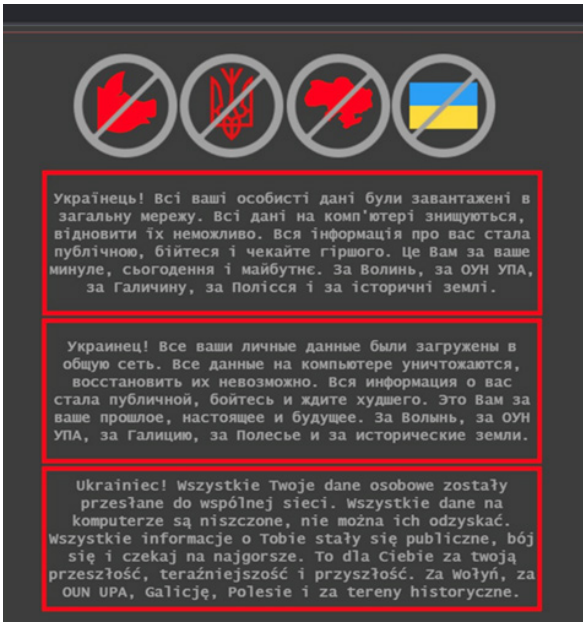


Figure 6. **Ukrainian website defacement screen**

The most likely vector of implementation of a cyber attack is a supply chain compromise, which makes it possible to use the existing trust relationships to disable related information, telecommunication, and automated systems. At the same time, two more possible attack vectors are not ruled out, namely, exploitation of October CMS and Log4j vulnerabilities.

To modify the content of web pages, on the morning of January 14, 2022, attackers from the TOR network gained access to control panels of websites of numerous organisations. At the same time, there is no indication of authentication data collection. The investigation of the compromised systems found suspicious activity carried out from legitimate accounts.

In some cases, to disrupt the regular mode of operation of information and communication (automated) systems, the attackers encrypted or deleted data in the final stage of the cyber attack. For this, at least two types of malicious programs of destructive nature were used: BootPatch (recording the malicious code in the MBR of the hard disk for its irreversible modification) and WhisperKill (overwriting files according to a specified list of extensions with a sequence of 0xCC bytes with the length of 1MB), or data deletion was carried out by manual deletion of virtual machines.

The goal of a cyber attack is psychological pressure and intimidation – in the least, that is evidenced by the published statements "Be afraid..." and "Wait for the worst...". Contrary to the hackers' claims, personal data of the Ukrainian people was not affected.

Weaknesses identified during and after the incident:

An unpatched October CMS vulnerability[01]:

The hack of the hosting service provider enabled the subsequent defacement attacks.

Recovery after the incident:

- Online access to the web server was disabled;
- Web server access log files and images and/or copies of the web server's file system were collected and analysed;
- The web server was restored from a backup;
- Web servers were vetted for web shells (illegitimate files and scripts);
- Third-party CMS and web server OS user accounts were checked and the illegitimate ones removed, passwords on all other accounts were changed;
- Online access to the CMS admin panel was blocked;
- October CMS was updated to the latest version.

Cyber security hardening and proactive defensive measures:

- Keep track of your software and hardware suppliers and their possible vulnerabilities;
- Have redundant front-facing websites on different types of CMS systems;
- Be aware of Zero Day vulnerabilities and take immediate action to mitigate them;
- Update security software with new IOCs regularly;
- Establish or review cyber security processes and policies to be aware of such techniques, and defence options.

---

01 https://www.cvedetails.com/cve/CVE-2021-32648/

ATTACKER MOTIVATION:
UNC1151 is allegedly a Belarussian APT that is closely aligned with the Russian special services-supported APTs and shares a very similar agenda. Their primary motivation was to cause reputational damage to the Ukrainian government sector and spread panic among the general population by means of disinformation.

IDENTIFICATION: UNC1151.
GOVERNMENTAL WEBSITES DOWN
DATE: February 15 - 16, 2022.
TARGETS: Online governmental services, online web and mobile banking applications, and ATMs.
TTP'S: T1566, T1499, T1565.

DESCRIPTION, AND OBSERVED IMPACT:

On February 15-16, 2022, several cyber attacks aimed at further destabilising the domestic political situation in Ukraine were detected. The cyber attacks were primarily aimed at disrupting the work of the national financial system and creating a notion among the citizens of Ukraine of an inability of the authorities to control and respond promptly to threats in cyberspace.

Among the main techniques of putting the malicious plan to work, the following can be noted:

- Sending fake SMS messages to citizens about, as it were, a failure in regular operation of ATMs of certain financial state institutions.
- Sending notifications via e-mail to financial institutions about demining due in their premises and buildings. It was established that the specified activity may be carried out by a resident of the Donetsk region.
- Conducting Distributed Denial of Service (DDoS) attacks against web resources of Ukrainian banks and state institutions and the Diia portal. In the course of the research, it was determined that the Mirai and Meris botnets were involved in the attacks, among others (the malicious information flow is directed through thousands of hacked Mikrotik routers and many other IoT devices with source filtering by using ACL, which allows you to hide the mentioned devices from search engines like Shodan). The above, with a high level of confidence, allows assuming that the available capabilities of the attackers provided as a service (DDoS as a Service) were used to carry out the attacks.
- Denial of web access in the gov.ua domain by conducting DDoS attacks against the DNS servers. The outage of several domain name servers led to a temporary disruption of access to a significant number of government web resources due to the prevented A-record (IP address) determination for the respective domain names.
- Suspicious manipulation of autonomous systems settings at BGP protocol level. According to Cisco Crosswork, for more than two hours, starting at 15:30 on 02/15/2022, the 217.117.7.0/24 prefix which belongs to Inq-Digital-Nigeria-AS (AS16284), was announced on behalf of the autonomous system of PrivatBank (AS15742) through the autonomous system of the Nigerian telecommunications operator (AS37148).

It should be said that the separate cyber attacks on the banking sector were not limited to DDoS, BGP hijacking, information, and psychological actions aimed at bank employees, but also included a significant number of attacks against the users of banking services. During 2022, the following malware was most often used to attack the banking sector: Formbook, Emotet, Agent Tesla, BitRAT, Racoon, Snake Keylogger, LokiBot, AsyncRAT, and BumbleBee, all aiming for the same goals of stealing personal data, collecting information about the infected systems, stealing crypto wallet data, saved passwords, etc. In most cases, email was the primary means of the initial infection. The US and UK Governments subsequently attributed these operations to the GRU.

Weaknesses identified during and after the incident:

Lack of DDoS mitigation instruments and rapid implementation anti-DDoS measures.

Recovery after the incident:

All affected information resources in the government and banking sectors became operational again after several hours of disruption.

Cyber security hardening and proactive defensive measures:

- Anti-DDoS tools and measures must be implemented to protect critical information infrastructure.
- Data that has been encrypted is shielded against interception and illegal access by rendering it unintelligible to anybody without the proper decryption key.
- Measures must be taken to establish redundant DNS servers, apply security protocols like DNSSEC, and require rigorous DNS logging.
- BGP protection should be improved with the use of IP prefix filtering, BGP hijacking detection, and BGPsec protocol.
- To limit access to their networks and systems, banks may employ security methods, such as passwords, two-factor authentication, and biometric verification.
- An incident response plan: it is a set of procedures and guidelines that a bank follows in the event of a security incident or breach. Develop a plan to respond to and recover from cyber incidents, including procedures for reporting incidents, conducting investigations, and communicating with stakeholders.

ATTACKER MOTIVATION:

Disrupting the work of the national financial system and creating a notion among the citizens of Ukraine of an inability of the authorities to control and respond promptly to threats in cyberspace.
IDENTIFICATION: GRU-affiliated APT's.
Wiper attacks on government, financial, energy, and other entities
DATE: February 23 - 25, 2022.
TARGETS: Multiple governmental websites, information, and communication systems.
TTP's: T1499, T1195, T1072, T1486, T1485.

DESCRIPTION AND OBSERVED IMPACT:

February 23-24, 2022 – another massive DDoS attack on the websites of the public administration sector, banking sector, and defence sector. As a result, the websites of the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Foreign Affairs of Ukraine, and the Security Service of Ukraine temporarily stopped working. Another cyber attack was also carried out against more sites damaging the Master Boot Record (MBR) loader and leading to an information and communication systems disruption. In the cyber attack on January 14, 2022, hacker groups associated with the GRU used the WhisperGate malware.

At the same time, the Sandworm APT deployed the FoxBlade (aka HermeticWiper) malware, which destroyed approximately 300 systems in more than 10 government, IT, energy, agricultural and financial organisations in Ukraine, Lithuania, and Latvia. Unlike the NotPetya malware, the FoxBlade deployment was tailored to specific environments. Technical analysis indicates the mechanism of the attack was built at least six weeks before the attack, hinting that the attack had been coordinated with the military invasion and full-scale war

on Ukraine. The peculiarity of the campaign lies with the fact that after the deployment of malware, it quickly affected all devices connected to the domain in the target organisation, and also had common features with the CaddyWiper malware, which will later be used in an attempt to attack an energy facility in Ukraine on 12 April 2022. Destructive malware was unleashed and a large number of Government and private sector companies' websites were defaced[02].

The same morning as the beginning of the Russian invasion of Ukraine, ESET identified a new wiper. The malware was dubbed IsaacWiper and it was found to had affected the remaning organisations not attacked by HermeticWiper. No shared code was found between these two wipers. On February 25, the attackers dropped a new version of IsaacWiper with debug logs, indicating that the attackers were unable to wipe some of the compromised devices. IsaacWiper enumerates logical drives and wipes the content of each disk using randomly generated bytes. The malware recursively wipes the files in a single thread, though the process could be time-consuming for large disks[03].

Weaknesses identified during and after the incident:

- Abuse of legitimate drivers from the EaseUS Partition Master software to corrupt data. EaseUS security key used to sign malicious payload and bypass security measures.

Recovery after the incident:

- There are limited options available to recover from a data wiper. Basically, either a fresh system rebuild or a recovery from the last healthy backup. Ukrainian cyber teams were struggling to recover due to the ongoing conventional military actions.

Cyber security hardening and proactive defensive measures:

- Use XDR systems with the Preventative Approach.
- Have a robust and tested backup and recovery solution. Only healthy backups can help recover after a data wiper attack.
- Isolate potential threats by using a Virtual Desktop Infrastructure (VDI). VDI systems are isolated from the underlying hardware and cannot be escaped by malware in standard scenarios.
- Implement and use a business continuity and disaster recovery playbook. It can help mitigate the damage and recover quickly after a data wiper attack.

Attacker motivation: Cause as much damage to the underlying victim infrastructure as possible.

Identification: GRU-affiliated APT's.

---

02 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

03 https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

5.2. Other Events in the Public Administration Sector

On February 25, 2022: cyber attack on Border Control Station. The Ukrainian border control station located at the Ukraine/Romania border reported they had been struck by a data wiper cyber attack. The attack slowed the process of allowing war refugees to cross into Romania. It is quite likely that computer systems of the Ukrainian border checkpoints became the target of the Wiper campaign too on that day seeking to disrupt the work of state institutions and to deepen the panic among the population. It is now impossible to tell exactly the extent of the damage the wiper malware caused, nor what actions were taken by the Ukrainian side to restore the affected systems to proper operation, but it is known that some people waited in line for more than 28 hours to cross the Ukrainian-Romanian border. It is not known for certain which system was the target of the intruders and what exactly was affected in it, but it is quite likely that it could have been the communication system of the State Border Service of Ukraine and the "Path" system used by the border guards to check the people who cross the state border of Ukraine. The cyber attack on this system in the second half of 2022 and its attribution to the Gamaredon hacker group recently became known from a report of the SSSCIP[04].

On February 28, 2022: Facebook, Google, and Twitter remove disinformation targeting Ukraine. It seems that the two campaigns were small in scale, and Facebook managed to detect them in the early stages. The first campaign involved about 40 Facebook and Instagram accounts, groups, and pages from Russia and Ukraine. The accounts, groups, and pages were disguised as independent news sources and posted fake claims about Ukraine. Meta also detected an increase in attempted hacks against the Ukrainians. Some hacking attempts were attributed to a group that has links in Belarus, Ghostwriter. This group has been making the effort to hack the accounts of high-profile Ukrainians, like military officials, public figures, and journalists. Google also prevented some Russian companies, including the state-run news company RT, from making money from the videos they post on YouTube. It said it would also restrict access to RT and several other channels in Ukraine. In addition, Google cut some Google Maps features in Ukraine to protect its citizens, according to Reuters, which said the company removed live traffic from the app and disabled the feature that shows store congestion. Meanwhile, during the first days of the war, Twitter actively monitored the risks and worked to remove disinformation. It also suspended advertisements in Ukraine and Russia. The platform would start labeling tweets that share links to Russian state-affiliated media websites[05].

On March 1, 2022: On the same day as the Russian military announced the intention to destroy "disinformation" targets in Ukraine and directed a missile strike against the TV tower in Kyiv, Russian threat actors also launched the DesertBlade malware against a major broadcasting company. The DesertBlade actions and the missile strike were meant to showcase its cyber and kinetic impact on a key source of information to the Ukrainian public. This malware was again deployed against Ukrainian organisations around the 17th of March, 2022[06].

On March 16, 2022: Hackers breached a national news broadcast on the television channel Ukraine 24 and hacked the program news ticker to display messages looking as though they were issued by President of Ukraine Volodymyr Zelenskyy. The messages urged Ukrainians to stop fighting and give up their weapons while claiming that Zelenskyy "wanted to take Donbas" but failed so he fled to Kyiv[07].

On March 24, 2022: Unknown actors compromised and potentially destroyed data on a portal that connects citizens to government services, and compromised the network of another major media organisation using both HermeticWiper and HermeticRansom[08].

---

04 Ukraine border control hit with wiper cyber attack, slowing refugee crossing | VentureBeat

05 Facebook, Twitter remove disinformation accounts targeting Ukrainians

06 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

07 'Hacked' Ukrainian TV Station Transmits Fake Zelensky Surrender Announcement

08 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

On April 1, 2022: Russian APT Sandworm deployed CaddyWiper against three victims, two of them local authority representatives in Ukraine. A new variant of CaddyWiper that involves a multi-stage loading process was identified. In this case CaddyWiper is loaded by the ArguePatch loader which is typically a modified, legitimate binary used to load shellcode from an external file. A similar scenario was detected on May 16, 2022, where ArguePatch took the form of a modified ESET binary. Similar events repeated on May 16, June 20, and on June 23, 2022[09].

In July-August 2022: Among other high-profile events, a cyber attack by the CyberAzov Turla (FSB) hacker group. Installation file of the application called CyberAzov.apk, not distributed through Google Play, was said to participate in DDoS attacks against the Russian Federation when installed on a victim's device; however, the malicious application contained a Trojan. In 2023 state-sponsored hacking groups, such as Turla, Gamaredon, APT28, Sandworm, APT29, etc., just like in the past, will maximally tie their campaigns to the information field and the mood of the population to achieve their goal .

Figure 7. **CyberAzov contacts in Twitter**

On November 8, 2022: The Gamaredon group mounted a cyber attack using spoofed emails that imitated the State Special Communications Service. A phishing email was detected targeting the Ukrainian government sector. The email included a link to hXXp://tzi.info-cip[.]org/07_11_2022.xhtml, an HTML file that contains JavaScript code which creates a RAR archive on the victim's computer, such as 08.11.2022.rar[10].

On December 16, 2022: Ukrainian government entities were hacked in targeted attacks after having their networks compromised via trojan-infected ISO files posed as legitimate Windows 10 installers. While the malicious Windows 10 installers were not specifically targeting the Ukrainian Government, the threat actors analysed the infected devices and performed further, more precise attacks on those determined to belong to Government entities. The threat group behind this supply chain attack is tracked as UNC4166. Based on the similarity of the victims of the campaign, Mandiant binds UNC4166 with APT28[11].

On January 25, 2023: A new wiper, SwiftSlicer, was deployed against the Ukrainian local authority entities. SwiftSlicer was deployed in its target environment using the Active Directory Group Policy. ESET attributed the attack to Sandworm[12].

On February 1, 2023: CERT-UA discovered a web page imitating the official website of the Ministry of Foreign Affairs of Ukraine that offered to download software for "detecting infected computers".

Opening the link started a file download, the file downloads and runs on the affected computer PowerShell scripts, one of which starts off a recursive search for files in desktop directories, taking screenshots, and further exfiltrating data using HTTP. At the same time, it creates scheduled tasks designed to ensure persistence. The mentioned activity is tracked under the identifier UAC-0114 (also known as Winter Vivern)[13].

09 https://msrc.microsoft.com/blog/2022/02/analysis-resources-cyber-threat-activity-ukraine/
10 https://cert.gov.ua/article/2681855
11 Ukrainian govt networks breached via trojanized Windows 10 installers
12 Sandworm APT Deploys New SwiftSlicer Wiper Using Active Directory Group Policy - Blog | Tenable®
13 https://cert.gov.ua/article/3761023

05.3. Summary and lesson learned

In the initial stage of the so-called special military operation the hacker groups affiliated with Russian special services primarily targeted the public administration sector of Ukraine.

At the same time, such TTPs as supply chain compromise, valid accounts, data encrypted for impact, exploitation of remote services, data destruction, endpoint denial of service, defacement, etc. were widely used. In most cases, Russian cyber actors apply commonplace methods for initial access, such as spear phishing, trojanized applications or removable media, compromise software supply chains, etc. It is an established fact that Russian hackers had access to victim systems long before the full-scale intrusion. Access monitoring and penetration testing are very important aspects of work for entities that provide cyber defence for the national critical information infrastructure. GRU-related cyber threat actors often use group policy objects for lateral movement within the victim system, that is why it is necessary to strengthen control over user actions and least-privilege administrative models should be implemented by cybersecurity divisions.

Several cyber defence weaknesses in the public administration sector were exposed. Existing cyber policies, instructions, and handling plans that required regular review and update were obsolete. The public administration sector lacked a proper concentration of experienced cyber experts to counter the threats effectively. Fragmentation of cyber defence systems and lack of collaboration between different cyber divisions during and after the attack played in disadvantage of the Ukrainian side. No timely action was taken to fix the vulnerabilities.

Lessons learned and recommendations that have been implemented and should be implemented in the reasonable future are listed:

- Review of cyber security processes and policies so as to be aware of new TTPs and defence options.
- Expanded cyber security forces, ensuring quality training of personnel in cyber defence.
- Operational communication and the process of information exchange between state bodies, critical infrastructure facilities, and CERTs have to be improved. The main lesson here is to have an effective communication with the main cyber defence governing body of the country.
- Involvement of the main private companies in the cyber security field (Google, Microsoft, Cisco, etc.) in repelling aggression in cyberspace.
- Updates of security software regularly with new IOCs.
- Anti-DDoS tools, such as CloudFlare and Akamai, should be used across organisations.
- Updates of environments with regular patches constantly.
- Proper management of data backups, disaster recovery, and business continuity strategies needs to be implemented and documented
- The US Cybersecurity and Information Security Agency (CISA) issued an alert warning of foreign operations pairing cyber threat activity with disinformation to undermine security and hinder the functioning of critical infrastructure (Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure). The recommendations should be implemented organisation-wide.
- Organisations with business-critical public-facing web resources should implement situationally specific network access policies which only permit internet traffic via required IP protocols and ports.
- Organic, on-site intelligent DDoS mitigation capabilities should be combined with cloud-based or transit-based upstream DDoS mitigation services to ensure maximal responsiveness and flexibility during an attack.

06. Private Sector Analysis and Lessons Learned

The private sector is part of the economy, sometimes referred to as the citizen sector, which private groups own, usually as a means of establishing profit or non-profit, rather than being owned by the government. The private sector is also a target for cyber attacks due to its close relations with the national interests, such as common shared infrastructure (Internet providers and communications), participation in national services (news, banks, transport, etc.), and co-governmental partners or subcontractors. To undermine the operational capabilities of the Ukrainian organisations and enterprises, just like in the public administration sector of Ukraine, Russian malicious actors widely used wiper malware to target private sector entities. In most cases, they had access to the victim systems long before the destructive attacks were carried out. The private sector is essential to the economy because it fosters job growth, produces goods and services, and creates new jobs. For governments, it is a significant source of tax revenue. Businesses contribute to the funding of public services and allow governments to make investments in infrastructure and other significant projects by paying taxes. Innovation is largely driven by the private sector. Private companies make investments in R&D, which produces new goods and services that advance the society and the economy. Government agencies and the public sector work together with private sector businesses to access resources and create new products. Cyber attacks against this sector can influence both public and military, as well as critical infrastructure fields, as all of entities in the mentioned fields usually rely on private sector services. As pointed out earlier, the public sector gets tax revenue from the private sector. Private companies are usually the main suppliers of military equipment to the armed forces. As for critical infrastructure, the components necessary for its systems are produced mainly by private sector entities. Therefore, the private sector has a huge stake in the majority of aspects of every country and cyber attacks can harshly damage other sectors in parallel. Companies rely on one another for products, services, and components in many industries thanks to interconnected supply chains. A cyber attack on a significant partner or supplier in the private sector can sabotage the supply chain, impacting numerous industries. If a supplier's cyber attack prevents a manufacturing company from accessing crucial parts or raw materials, production may be forced to stop. This may then have an effect on downstream industries that depend on the manufacturer's goods. Economic stability and growth are significantly influenced by the private sector. Broader economic repercussions may result from a cyber attack that disrupts businesses, results in financial losses, or erodes consumer confidence. This effect goes beyond the private sector and has the potential to influence investment choices, employment rates, and overall economic performance.

06.1. The Most Significant Cyber Incidents in the Private Sector of Ukraine

CYBER ATTACK CAUSES UKRTELECOM JSC TELECOMMUNICATION COMPANY AND TRIOLAN ISP OUTAGE

DATE: March 10/28, 2022.
TARGETS: Ukrtelecom, Triolan.
TTPS: T1498.

DESCRIPTION AND OBSERVED IMPACT:

On March 10, 2022, Ukraine's national telecommunication company Ukrtelecom suffered a 40-minute nationwide outage. Internet service provider Triolan, meanwhile, was down for more than 12 hours amid DDoS attack reports, as Russia continues its war in Ukraine. Triolan ISP is a collective of independent business entities that together offer Internet and cable TV services across Ukraine. Later a cyber attack on 28 March

2022 denied access to some Ukrtelecom customers. The incident continued throughout the day and caused a nation-scale network disruption, including communications networks of military and other high-priority users. The responsibility for the cyber attack was claimed by hacktivist groups XakNet and KillNet.

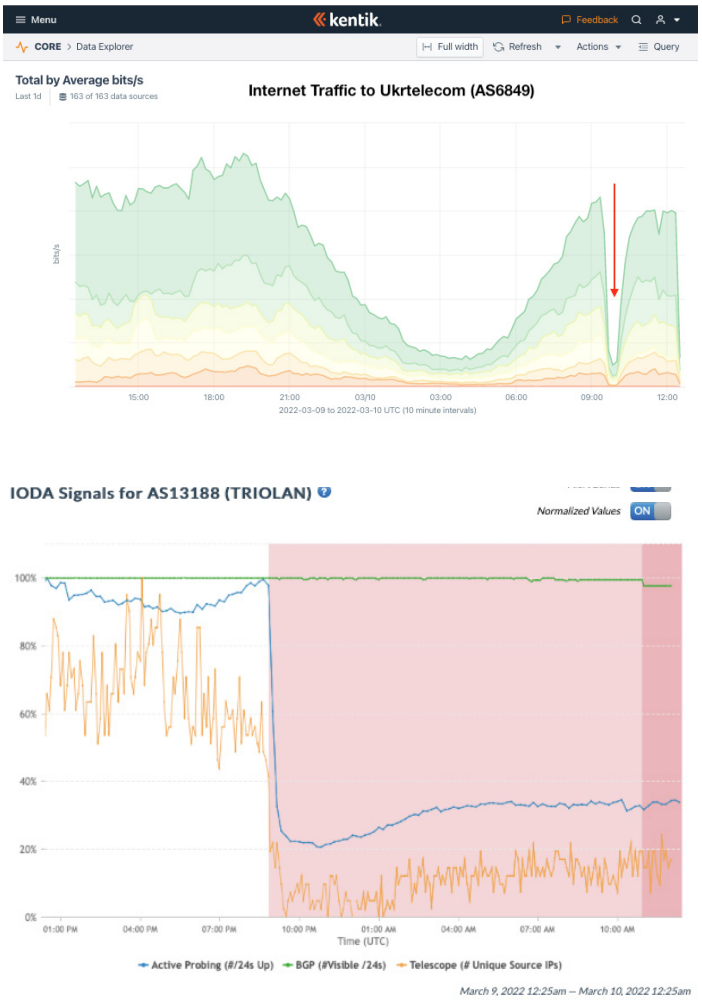


Figure 8. **Loss of network traffic graph**

Weaknesses identified during and after the incident:

ISP infrastructure was designed with standard bandwidth capacity. But it was not considered the possibility of malicious traffic in such a large volume during wartime. Limits of physical hardware were reached and it was identified that a standard overhead capacity of 20-30 % is not sufficient.

Recovery after the incident:

Such a large DDoS is unsustainable for long periods. It was possible to wait it out. But to ensure the high availability of services to all related sectors an overhaul and increase in network hardware and capacity was done. Additionally, anti-DDoS techniques like blackholing, sinkholing, and IP geo-blocking were employed.

Cyber security hardening and proactive defensive measures:

- It is critical to put DDoS mitigation in place via services like Cloudflare, Akamai, or AWS CloudFront. Having just a firewall will not stop the volume of the traffic we observed hittinh the Ukrainian targets in Netflow analysis.
- It is also important to correctly configure the installed CDN, otherwise it will not be as effective.
- Automate the disaster recovery runbooks for on-premise systems and ensure that you can move workloads to the disaster recovery site with a single click, if possible.
- Furthermore, blocking Russian IPs will not stop DDoS attacks. The attackers are using proxies and the attacks are coming from across the world, neutral countries in Latin America, the EU (not Russia or Belarus), and Southeast Asia.

Attacker motivation: the main objective was the disruption of communication in order to leave the Ukrainian citizens in the unknown, thus spreading panic and disorder.

Identification: Xaknet, Killnet, and its affiliated groups.

ATTACK ON UKRAINIAN MEDIA USING CRESCENTIMP

DATE: June 10, 2022.
TARGETS: Ukrainian media.
TTP'S: T1566.

DESCRIPTION AND OBSERVED IMPACT:

It became known on June 10, 2022, that Russian hackers launched another malicious email campaign leveraging Follina vulnerability, targeting more than 500 recipients at various media organisations in Ukraine, including radio stations and newspapers. The sent emails had "LIST of links to interactive maps" written in the subject line and a .DOCX attachment with the same name. When the file is openend, JavaScript code fetches payload named "2.txt" which CERT-UA classified as "malicious CrescentImp." CERT-UA attributes the activity to UAC-0113 associated with the Sandworm group, with medium confidence.

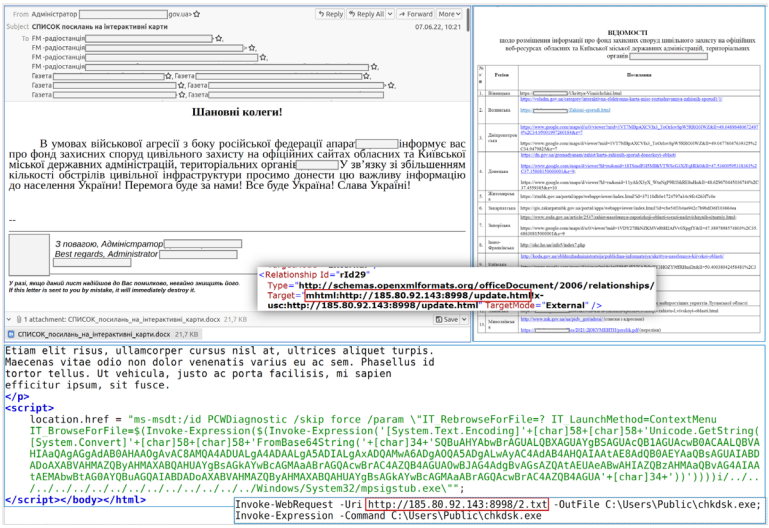


Figure 9. **Phishing email analysis**

Weaknesses identified during and after the incident:

Follina is a high-severity vulnerability discovered in the Microsoft Office suite of products that is easy to exploit for remote code execution (RCE) attacks. Microsoft has released security updates for all products affected by Follina; however, many versions of Microsoft Office products are still unpatched and vulnerable.

Recovery after the incident:

Collection of IOC, adding C2 from documents to the firewall detecting harmful document, as well as Microsoft Office pack and antivirus updates for Follina detection.

(Follina is using Microsoft Support Diagnostic Tool (MSDT) to execute code or reach the URL)

Cyber security hardening and proactive defensive measures:

Ensure that msdt.exe does not have any suspicious child processes in critical situations, MSDT can be listed out from the trust program list.

After a confirmed machine clearance, updates and security patches should be applied.

Install or update antiviruses and endpoint protection software. Most of them detect Follina; however, security products can conflict with each other and render office documents irresponsive.

Attacker motivation: Espionage, information gathering, deployment of Remote Access Trojan (RAT).

Identification: Russian Nexus, possible affiliation with Sandworm APT.

06.2. Other Events in the Private Sector

On March 14, 2022: Sandworm deployed the destructive CaddyWiper malware against a Ukrainian bank. CaddyWiper erases user data and partition information from attached drives. ESET telemetry showed that it was seen on a few dozen of systems. The information from the CaddyWiper PE header suggests it was compiled the same day as deployed against the targeted networks. As in the discussed case, CaddyWiper is delivered via the default group policy object (GPO), it is capable of erasing user data and partition information from attached drives but sidesteps data on domain controllers[14].

On March 17, 2022: Sandworm conducted a destructive attack against the network of a transportation/logistics provider, the type of organisation that could be involved in moving Ukrainian supplies to conflict hotspots. The company is headquartered in Western Ukraine where much of the foreign military and humanitarian assistance is entering the country.

A Wiper DoubleZero attack hit Ukraine's enterprises: CERT-UA discovered several ZIP archives containing the mentioned DoubleZero wiper. The activity is tracked under identifier UAC-0088. The goal of the campaign is believed to be disruption of regular operation of information systems in Ukraine's enterprises[15].

On June 24, 2022: DarkCrystal RAT malware cyber attack against Ukrainian telecommunications operators. CERT-UA was noitified about distribution of e-mails with a RAR archive attachment that was protected by a

14 https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/

15 https://cert.gov.ua/article/38088

password address in the domain gov.ua. The RAR archive contained a document on obtaining legal aid. When the document is opened and macro is activated, a PowerShell command is executed to download and run the NET bootloader MSCommondll.exe. The mentioned executable file, in turn, downloads and runs the DarkCrystal RAT malware. Based on the recipient email addresses, as well as the domain management DarkCrystal RAT, it is assumed that the attack was aimed at Ukraine's operators and telecommunications providers, such as Datagroup, Kyivstar, EuroTransTelecom LLC. On the19th of September, 2022, Recorded Future published a report where an identified infrastructure continues the trend of masquerading as telecommunication providers operating within Ukraine and delivers malicious payloads via a HTML smuggling technique that deploys Colibri Loader and the Warzone RAT malware. CERT-UA tracks this campaign as UAC-0113[16], which, with moderate confidence, is linked with Sandworm[17].

On July 13-14, 2022: Cyber attack by Infor Zarya hacker group against Warnet ISP. As a result, unauthorised access to the company's servers was gained and used to host about 100 web resources, including state-owned[18].

On October 11, 2022: New Prestige ransomware campaign targeted Ukraine and Poland. A coordinated ransomware campaign targeted the Ukrainian and Polish transportation and logistics sectors with a previously unknown payload. Microsoft observed the new ransomware deployed in attacks occurring within an hour of each other across all targets. Investigators attributed the campaign to the Sandworm APT [19].

On November 21, 2022: RansomBoggs attacks linked to Russian hackers held against Ukraine. According to ESET experts, networks of multiple Ukrainian businesses were targeted by a brand-new malware named "RansomBoggs". The PowerShell script used to deploy RansomBoggs payloads on the victims' networks is known as POWERGAP and was also behind the delivery of the CaddyWiper destructive malware in the attacks against Ukrainian organisations earlier this year in March. Based on similarities with the earlier operations carried out by the same group, investigators linked the RansomBoggs attacks with the Sandworm APT [20].

In January 2023: Disruption of several elements of information and communication system of Ukrainian National News Agency Ukrinform. Five samples of malicious programs (scripts) were detected in the system: CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe[21].

06.3. Summary and lessons learned

In general, private sector companies are engaged in cyber defence independently based on internal instructions and available resources but guided by current legislation of state governing institutions. There are a large number of companies that have their cyber defence units, software, and incident response plans, especially companies which are related to the public administration sector or critical infrastructure. Naturally, various types of attacks occur against such companies constantly, but the cyber threats of today demonstrate the need for an increased cyber security for any company that has digital assets because they can either serve as an entry point to the infrastructure of others (via shared access) or become a part of the attacking infrastructure.

- It is recommended that private companies and enterprises to have an established local Security Operation Center (SOC) or at least an Infosec Unit.
- Private companies sometimes avoid sharing information about suffered cyber attacks to avoid

16 https://cert.gov.ua/article/405538
17 https://go.recordedfuture.com/hubfs/reports/cta-2022-0919.pdf
18 https://cybershafarat.com/2022/12/03/zarya-cyberfront-z%D0%B0%D1%80%D1%8F/2/
19 New "Prestige" ransomware impacts organizations in Ukraine and Poland - Microsoft Security Blog
20 https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/
21 https://cert.gov.ua/article/3718487

unnecessary media attention, in most cases, it costs the company decreased reputation and loss of clients (customers), especially in the cae of large enterprises. Not sharing the information, however, causes much more financial and reputational damage. A dialogue between the private and government sectors is recommended on actions to be taken in the case of an incident, as well as refraining from financial penalties, like fines or other disciplinary actions, unless necessary.

- Information transfer about cyber incidents by one company to another, especially if it is critical infrastructure, can save others and prevent major damage. If companies share cyber attack information, other potential targets are ready and able to put out prevention measures in their systems to escape harm.
- National private companies and governmental sectors should increase cooperation and information exchange with international cybersecurity organisations and communities.
- Relevant state bodies should control and check the compliance of cyber security systems in enterprises and private sector organisations. They should provide support and offer cooperation, especially to those that participate in or ensure the functioning of the state management system, or critical infrastructure and national defence facilities.

07. Military Sector Analysis and Lessons Learned

The military sector, or simply the military, also known collectively as the armed forces, is a heavily armed, highly organised force, primarily intended for national defence. It is typically authorised and maintained by a sovereign state, its members are identifiable by their distinct military uniforms. It may consist of one or more military branches, such as the army, navy, air force, etc. Mission of the military is typically defined as defence of the state and national interests against external armed threats.

Cyber attacks against the military sector can lead to exposed force coordinates, leaked military movement and/or planned offensive/defensive action data. Therefore, protection of the military sector is crucial to protect the personnel and equipment and gain/maintain superiority over the enemy. Cyber attacks can disrupt command and control systems, which are critical for coordination and direct military operations. Cyber attackers have the ability to compromise such systems and interfere with the communications, decision-making, and an efficient use of force. For information about potential threats, military organizations rely heavily on intelligence and surveillance systems. Such systems may become a target of cyber attacks resulting in loss or alteration of critical data, and consequently – hampered situational awareness, jeopardized operational planning, and military missions rendered ineffective.

Cyber security forces are located in various units across the Armed Forces of Ukraine, mainly, but not limited to, the Communications and Cyber Security Command. Traditionally, it is an extensive area of responsibility: public and private network assets, military software, and private user data – in general, it is a huge semi-structured hardware, software, and network infrastructure. In March 2022, Ukraine's Ministry of Defence established a dedicated Cyber Security Operational Centre with cyber security and analytical capabilities and scope limitation only to the assets related to the Ministry of Defence. It helped to narrow the scope of work and separate the assets of the Ministry of Defence and the Armed Forces.

Yet another important step was the establishment of new cyber divisions at operational and tactical (for special cases) levels and their enhancement with regular cyber expert squads and divisions (as a result of the increase in military software usage), in opposition to the approach applied by the previous central government. It allowed building more flexible and quick-to-react systems/teams without the necessity of approval of any step on a high level. It, however, also widened the field for cyber attacks.

The ongoing warfare has also highlighted another problem – the necessity to protect not only military-owned assets but also military-affiliated organisations, such as various contractors (both in the public and private sectors) and non-profit organisations: this problem does not have simple solutions but requires propagation of well-designed tools, incident-handling plans and communication channels, as well as perfect collaborative efforts.

In addition, Ukraine has sharply strengthened communication with foreign partners (in the military and commercial sectors) specifically in the military cyber security sector.

07.1. The Most Significant Cyber Incidents in the Military Sector of Ukraine

ATTACK ON VIASAT

DATE: February 24, 2022.
TARGETS: Several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe impacted.
TTP'S: T1133, T1021, T1498, T1485.

DESCRIPTION AND OBSERVED IMPACT:

The satellite service interruptions began on the morning of February 24, just as the Russian forces started going in and firing missiles striking major Ukrainian cities, including Kyiv. Hackers disabled the modems of communication with Viasat Inc's KA-SAT satellite, which supplies internet access to some European customers, including Ukrainian military units. More than two weeks later, some were still offline.

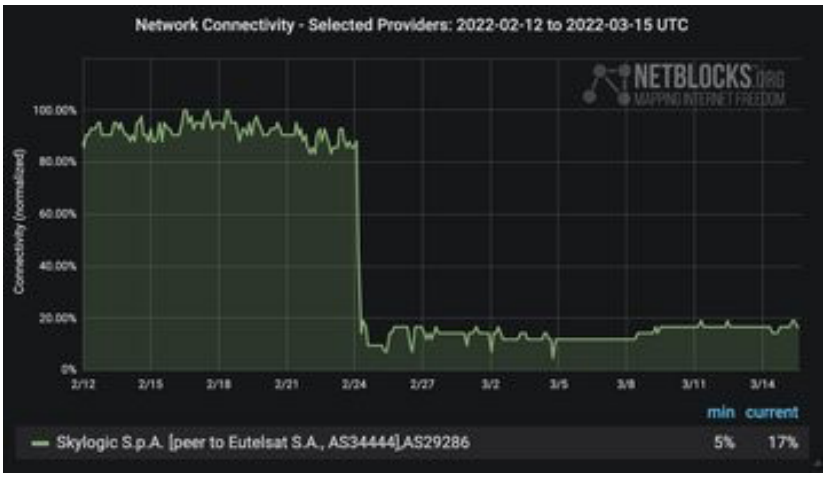


Figure 10. **Loss of satelite network connectivity**

At approximately 0302 UTC on February 24, 2022, high volumes of focused, malicious traffic were detected emanating from several SurfBeam2 and SurfBeam 2+ modems and/or associated customer premise equipment, physically located within Ukraine and serviced by one of the KA-SAT consumer-oriented network partitions. This targeted Denial of Service attack prevented many modems from remaining online.

Ultimately, tens of thousands of previously online and active modems dropped off the network and were not detected attempting to re-enter the network again. The attack impacted the majority of active modems in Ukraine and a substantial number of additional modems in other parts of Europe.

Figure 11. **Hardware in use example**

The attackers likely managed to compromise/spoof a Ground Station (Gateway Earth Station), specifically, the "Element Management" section (which likely is synced across gateways), to issue a command by abusing the legitimate control protocol (probably TR-069) which deployed to terminals a malicious firmware update. Later SentinelLabs researchers discovered a new wiper malware they named "AcidRain" which Viasat confirmed to have been used in the attack against their modems on the 24th of February.

The new wiper iterates over all possible device file identifiers (e.g., mtdblock0 – mtdblock99), opens the device file, and either overwrites it with up to 0x40000 bytes of data or erases it with IOCTL.

The modems were no longer able to access the network and even if not permanently unusable, therefore, could only be restored by a factory reset. Although Viasat did not provide the precise information on the number of affected devices, it stated that "nearly 30,000 fresh modems had already been shipped to distributors to bring customers back online". The EU Agency for Cybersecurity reported at least 27,000 devices impacted. However, the attack did not compromise users on other Viasat networks worldwide, including airlines or other government users of the KA-SAT satellite network. It has not damaged the satellite itself, nor the network infrastructure.

The subsequent investigation and forensic analysis identified the ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance and thus gaining remote access to a trusted management segment of the KA-SAT network[22].

Weaknesses identified during and after the incident:

- Misconfiguration in the VPN appliance of the satellite service provider;
- Slow replacement of the affected equipment by the service supplier;
- The need to have redundant digital communication channels employing another technology;
- Lack of good coordination and collaboration between different handling the incident and further security hardening.

Recovery after the incident: Mitigation and recovery actions began immediately to stabilise the network and restore the service which was largely a success within hours, and the network was fully stabilised within several days. As of May 2022, thousands of customers remained offline. The company's spokesperson confirmed that the priority in the recovery effort was given to "critical infrastructure and humanitarian assistance".

The following actions were taken during and after the incident:

- Switching to other communication channels.
- Incident investigation to close identified vulnerabilities and detect any others.
- As of May 2022, the attack has been investigated by the Mandiant Company and multiple intelligence and security agencies, including the US National Security Agency[23] and the National Cybersecurity Agency of France.

Cyber security hardening, and proactive defensive measures: Viasat initiated Network stabilisation and security mitigation actions immediately after the incident. The specific technical details of the mitigation actions have not been shared publicly at this time. The available open-source information shows that Viasat satellite modems were returned to the vendor for maintenance and reprogrammed with clean firmware.

---

22 https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

23 Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say | Reuters

Attacker motivation: The attack ostensibly aimed at interrupting the service by rendering the modems of the entire parcel of customers inoperable, and the attack could have been intended to hit the military command and control in Ukraine.

Identification: APT28 is suspected to have been involved, based on similarities between the AcidRain[24] malware used in the Viasat attack and the VPNFilter malware used to crash hundreds of thousands of routers in 2018. And more recently, the NSA and CISA tied the attack to Sandworm.

KROPYVA BREAKDOWN ATTEMPT

DATE: May 22, 2022.
TARGETS: Combat control system.
TTP's: T1566, T1499.

DESCRIPTION AND OBSERVED IMPACT:

The tactical unit combat command and control system Kropyva is a battle-tested system designed for automation of individual control tasks at the level of battalion (division), company (squadron), platoon, and separate unit of equipment (gun). Kropyva is a mapping intelligence application run on Android which allows user with a terminal, usually a tablet, to easily mark enemy positions. It can be used by various land force units: artillery, motorised infantry, tank units, all-arms intelligence, land air defence units, field engineering units, etc.

Figure 12. **Kropyva software**

On May 22, the XakNet Team and Killnet hacker groups organised a spam attack on Telegram servers used to collect information about enemy force location to coordinate artillery targeting. Anyone could connect to the Kropyva system and write or call via Telegram to provide the consequential coordinates. XakNet Team and Killnet orchestrated a spam attack on Telegram to bring chaos and disinformation into the battle management system. This had a partial but not critical effect on the coordination process: any coordinates provided go through a pre-moderation process so that users are not affected.

24 https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

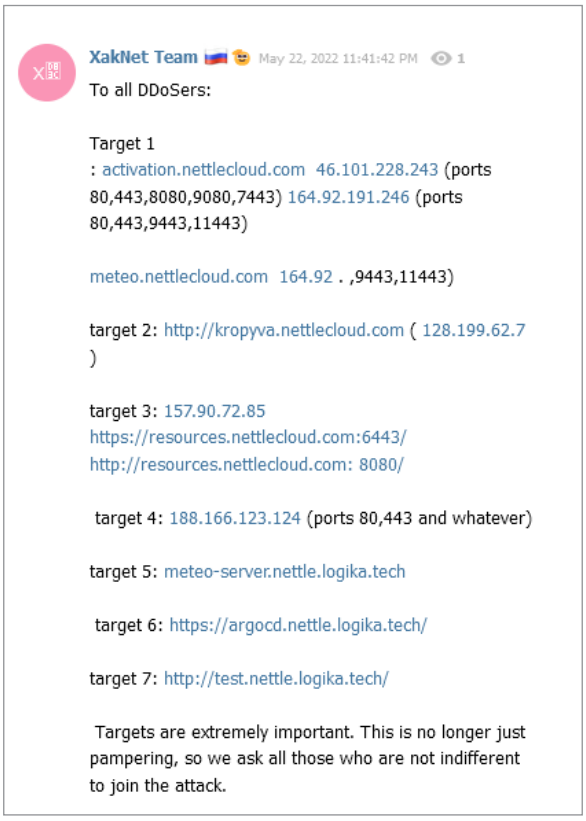


Figure 13. **Systems targeted by XakMet**

At the same time, a DDOS attack was carried out against the servers where the system was located but with no harmful impact.

On November 7, the XakNet Team hacker group announced a DDOS attack against the information resources of Design Bureau Logika (https://logika.ua), developer of Kropyva. The cyber attack disrupted the website of the design bureau for over a day.

Client acknowledgement receipt file information from the Kropyva combat control system was repeatedly published in Russian Telegram channels, probably because of a tablet with installed apps Kropyva taken hold of. However, there is currently no publicly available information on unauthorised access to system management servers.

The Russian military recognized the effectiveness of Kropyva and declared to begin developing an analogue for the needs of artillery units of the Russian Federation. The activity of the Russian cyber actors and special services targeting Design Bureau Logika and its product Kropyva system confirms its effectiveness on the battlefield[25].

Weaknesses identified during and after the incident:

- Although civilian involvement in reconnaissance and information gathering is fairly helpful in support of fast reaction on the battlefield, it requires a more elaborate pre-moderation process and to respond to the necessity to build, support, and protect the public information gathering channels.
- Tools for in-depth verification of data entered into the system, as well as protection against DDoS, were not implemented in time.

Recovery after the incident:

- There is no exact data but judging by the statements of the attackers, insignificant failures in the system operation, specifically, registration of new users, were occurring for a few days. The measures taken restored the system to normal operation.

Cyber security hardening and proactive defensive measures:

- Processing and moderation of information obtained through public channels has been significantly revised and automated to exclude the attack possibility.
- Spam on Telegram groups dedicated to combat systems should be blocked by all possible methods.
- CDN and WAF should be applied.
- The DDoS defence was improved.

Attacker motivation: Disruption of the proper operation of the combat tactical system.

Identification: XakNet, Killnet.

25 https://cybershafarat.com/2022/10/31/xaknet-kremlin-proxy-given-specific-instructions-to-hack-kropyva-ddos-telegram/

COMBINED ATTACK ON DELTA

DATE: July 26 - August 27, 2022; December 13 - 18, 2022.
TARGETS: Military software.
TTP's: T1566, T1498, T1041.

DESCRIPTION AND OBSERVED IMPACT:

Delta (https://delta.mil.gov.ua) is a Ukrainian military software used for situational awareness of military and paramilitary squads and organisations, the system supports Ukrainian defenders with up-to-date verified data about the enemy and coordination of defence forces. It was developed by the Center for Innovation and Development of Defence Technologies of the Ministry of Defence of Ukraine.

Starting February 24, 2022, Delta grew explosively, especially from a user perspective. That was considered and a public service as a web application (introduced in June 2022) was established. Because of Delta's popularity and importance, cybersecurity capabilities of the Ministry of Defence formed a defence line for its assets: components, data, and system services. Starting on 27 July 2022, it already detected reconnaissance and exploitation attempts by the Russian-affiliated groups that, however, proved unsuccessful. Concurently, a threat group launched several fake websites (for example delta[.]milgov[.]site) to serve in an enourmous phishing campaign. A certain amount of accounts were compromised as a result; however, the defence team noticed such accounts and took control of them. On August 15, 2022, a powerful DDoS attack was launched as a cover-up for another malicious activity. The threat actors were concurently trying to get into the system by means of compromised accounts. All their malicious activities were blocked by WAF and network administrators.

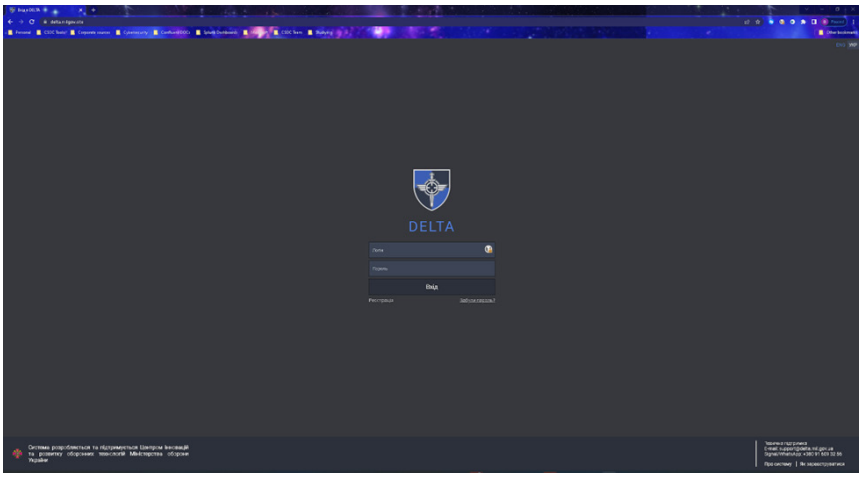


Figure 14. **Delta web portal**

The impact was minimal, the system never went down, and critical data was not compromised, but the public (commonly shared) data, authorization and authentication process were disclosed.

Starting August 20, 2022, the threat group, probably affiliated with the GRU, continued to exploit the same approach: phishing sites (or Messenger messages), account compromise attempts, and DDoS to cover the intrusion into the system.

On November 1, a piece of concerning information surfaced: two cases of unauthorised access to Delta were detected in August. It was a primitive technology, phishing through mailboxes and social networks, which means, links containining a virus program that exposed user passwords were sent. Two users who opened the link and planted the Russian virus on their Delta-enabled gadget. One user is a resident of a subdivision

in the Kryvyi Rih region, the other is from the Kharkiv region. This allowed Russians to enter the program. The Delta breach did not occur because the enemy obtained the passwords. Delta's defences anticipated such a threat, therefore, each user has their own limited level of access and a certain layer of data that they can see. Because of this, the Russians were able to see only a small amount of information realting to the Russian forces. The unauthorised access was quickly detected, the enemy was only able to watch one of the system fragments for 13 minutes. It reflected the location of Russian troops in southern Ukraine, and then the access was broken off. The enemy got an understanding of what Delta is but the data received already lost its relevance. Both users who handed over their passwords were been identified and counterintelligence is working with them.
On December 18th, 2022, CERT-UA reported a cyber attack against Delta with information-stealing malware. The attackers sent messages from a hacked email address belonging to a Ukraine Ministry of Defence employee to users of Delta. The hackers' messages included fake warnings to update digital certificates commonly used for encryption and authentication. The malicious emails contained a PDF document instructing users to upload a ZIP archive with digitally signed executable files protected by VMProtect, a Russian-made security software. Each step simulated the certificate installation process but infected victim computers with two malware strains - FateGrab and StealDeal, which steal documents, emails, and internet browsing data. Ukrainian military officials stated that the incident has been detained in the preparation stage.

The cyber security team took the following actions to strengthen cyber defence:

- Changes in the authorization and authentication processes were introduced to make them more secure: force reset period was shortened, multi-factor authentication (MFA) was made mandatory (as opposed to several exceptions before), and the policy of obtaining and renewing authorization keys was updated.
- The compromised user accounts were reset.
- Honeypot mechanism was employed creating fake user accounts to exaine attacker behavior and techniques.
- Additional cyber security software was added to fortify the defence perimeter.
- Monitoring of the Internet was increased to detect and block phishing sites.

Weaknesses identified during and after the incident:

- Lack of public awarness of the dangers in phishing tactics.

Recovery after the incident: Not required, the system was not broken down and data was not compromised.

Cyber security hardening and proactive defensive measures:

- The authorization and authentication process was changed adding regular reviews of user behaviour.
- Polygraph test introduced for system developers with access to user data.
- Protocols for recognizing patterns of suspicious behaviour were introduced.
- The system is regularly checked for vulnerabilities by Ukraine's international partners.
- Monitoring of the darknet and of information channels used by the Russian threat actors introduced.

Attacker motivation: To get a stable access to the Delta data and obtain critical information.

Identification: APTs affiliated with the GRU.

07.2. Summary and lessons learned

Ukraine's military cyber space is a high-intensity battlefield with non-stop attacks and threats initiated by different actors from different countries, not limited to Russia only. Various attack types and directions are mostly targeted to steal data, conduct cyber espionage, and damage assets seeking to create a direct and indirect impact on Ukraine's ability to fight. Ukraine had to significantly accelerate the development of and to strengthen its capabilities in the field of cyber security in the military sector. New capabilities have upgraded the "traditional" solutions in cyber protection (user training, regular system inventory, and development of the existing cyber protection solutions).
The military in general is one of the primary targets for opponents before and during an armed conflict. It is important to state that different countries have different military doctrines to cover cyber security. Weak links in cybersecurity in the military can lead to a breakdown of communications, impaired operational efficiency, and reduced command and control abilities. Listed below are the main points that any independent state can apply to increase its military cybersecurity:

- A separate unit in the structure of the country's military organisation of (command) responsible for cyber security and capable of conducting intelligence activities, defensive (offensive) operations in cyberspace;
- In the event of a crisis, presence of a mechanism for attracting the necessary quantity of experts to repel the aggression in cyberspace;
- Ability to rapidly establishment of new secure communication channels, software solutions, and workplaces;
- Quick investigation of new threats and delivery of investigation results to cyber security entities;
- Fast-producing, revising, and processing incident response plans;
- Establishment of a stable communication with foreign partners from the military and commercial sectors;
- Adjustment of rapidly developed cyber protection systems to existing legislation and regulatory instructions;
- Although not specifically ca matter of cyber defence, it is recommended to have rapidly deployable GSM/4G communication towers for the case of military conflict or natural disaster. These are vehicle-mounted self-powered (generators) communication towers that extend in locations suffering from blackouts and provide voice and data communication via satellite or line of sight link, and can cover a 3-6 KM range.

08. Critical Infrastructure Sector Analysis and Lessons Learned

The critical infrastructure sector is in effect the body of systems, networks, and assets so essential that the security of a given nation, its economy, and the public health and/or safety depends on their uninterrupted operation. Critical infrastructure usually includes power grids, transport network, information, and communication systems. Traditional energy technologies are becoming progressively more connected to modern, digital technologies and networks. This increasing digitalization makes the energy system smarter and enables consumers to better benefit from innovative energy services. At the same time, digitalization creates significant risks as increased exposure to cyber attacks and cybersecurity incidents potentially jeopardises the security of the energy supply and the privacy of consumer data. Cybersecurity and the challenges related to it are evolving at a rapid pace.

It goes in its name why this sector is so important in the defece from cyber attacks: it is critical. It directly affects the citizens of the country. Cyber attacks may deny to people electricity, heating, or water supply. Those are just a few things essential for survival. Therefore, the defence of critical infrastructure is usually taken very seriously. The society depends on the critical infrastructure sectors, including energy, water, transportation, and healthcare, to deliver these necessities. Cyber attacks targeting the control systems and networks that manage the services may cause the interruption of provision of power, water, transportation services, or healthcare. It may result in severe financial losses, discomfort for the general population, and even endanger lives. Some cyber attacks aim to harm vital infrastructure on a physical level. Cyber attackers can manipulate or take down vital equipment, such as power generators, pipelines, or dam gates, by compromising industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems. Such assaults may result in infrastructure breakdowns, environmental harm, or even actual accidents.

Historically, Russian Federation-supported threat actors have been targeting Ukrainian critical infrastructure for a number of years. The most notable of that are the 2015 Ukrainian power grid attacks. On December 23, 2015, hackers used the BlackEnergy 3 malware to remotely compromise the information systems of three energy distribution companies in Ukraine and temporarily disrupted electricity supply to consumers. Consumers in Prykarpattyaoblenergo (Ukrainian: Прикарпаттяобленерго; servicing Ivano-Frankivsk Oblast): 30 substations (7 110 kW substations and 23 35 kW substations) were hit the worst and switched off, approx. 230,000 people had no electricity power for a period between 1 to 6 hours. At the same time, customers of two other energy distribution companies, Chernivtsioblenergo (Ukrainian: Чернівціобленерго; servicing Chernivtsi Oblast) and Kyivoblenergo (Ukrainian: Київобленерго; servicing Kyiv Oblast), were also affected by a cyber attack, only at a smaller scale. According to representatives of one of the companies, the attacks were conducted from computers with IP addresses allocated to the Russian Federation.

Cyber attacks against critical infrastructure are the most difficult to execute, requiring careful planning and a lot of time. It is known that the attack on the Ukrainian power grid was planned for more than a year. During the 2022 Ruso-Ukraine war, the Russian Federation attempted several attacks on the Ukrainian power grid with very limited success. The failure possible depended of resource and time shortage. We will dig deeper into the most famous cases and see what can be learned from cyber defence strategies Ukraine has implemented.

08.1. The Most Significant Cyber Incidents in the Critical Sector of Ukraine

ATTACK ON ENERGY SYSTEMS

DATE: April 8, 2022.
TARGETS: Energy systems of Ukraine.
TTP's: T1587.001, T1072.

DESCRIPTION AND OBSERVED IMPACT:

CERT-UA disrupted Sandworm's attempt to take down a Ukrainian energy provider. The Russian-backed hacking group attempted to disconnect an unnamed provider's electrical substations using a new version of the infamous Industroyer malware. The Sandworm APT group used Industroyer to cut power in Ukraine in 2016 which left hundreds of thousands of customers without electricity two days until Christmas. Researchers at the ESET cybersecurity company, that collaborated with CERT-UA to analyse and remediate the attack, said they "with high confidence" assess that the industrial control system (ICS) malware was built using the source code of the malware deployed in 2016, which it at the time branded as "the biggest threat to industrial control systems since Stuxnet". Hackers deployed the new variant, dubbed "Industroyer2" by the researchers, in an attempt to cause damage to high-voltage power substations. It was used alongside CaddyWiper which was planted on systems running Windows to erase the traces of the attack.

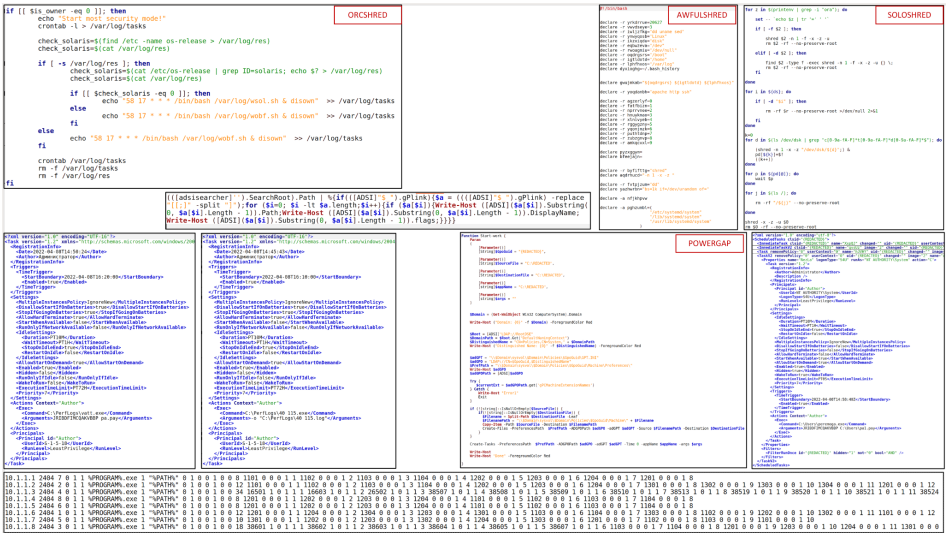


Figure 15. **Code examples of ICS malware**

The attackers also targeted the organisation's Linux servers using other variants of wiper malware dubbed Orcshred, Soloshred, and Awfulshred. The attackers breached the energy provider's network "no later than February 22," according to the security advisory, and had planned to cut power in a Ukrainian region on April 8. However, CERT-UA said that "the implementation of Sandworm's malicious plan has so far been prevented." ESET said that it did not know at that moment how the attackers compromised the target, nor how they moved from the IT network to the ICS network.

Sandworm (also known as VOODOO BEAR, Iridium, Iron Viking, UAC-0082, and HADES) is the notorious division of the Agency's hacker forces responsible for many of the GRU's most aggressive cyberwar and sabotage campaigns. According to WIRED, Sandworm's current commander is an official called Yevgeny Serebryakov

who was indicted, along with six other GRU agents, after getting caught in the midst of a close-range cyber-espionage operation that targeted the Organization for the Prohibition of Chemical Weapons in The Hague in the Netherlands in 2018. However, he was later released under unclear circumstances.
The group has been operational since at least 2014. The unit associated with Sandworm consists of 3 sub-groups, each focused on specific activities: Kamacite serves as an access and enablement group; Electrum conducts actions against objectives, including disrupting ICS; and TeleBots conducts cyber sabotage against a broader range of targets. All 3 sub-groups have an overlap between the TTPs used to conduct their activities[26].

The following actions were taken during and after the incident:

- CERT-UA was notified and involved in further investigation.
- Threat analysis was completed to define malware features, including the ability to go through defence systems.
- Policies of defence and security systems were revisited to better prevent malware.

Weaknesses identified during and after the incident:

- Penetration testing is needed to define potential holes and backdoors.
- Security systems require revisiting their policies and hunting tools regularly due to constantly changing malware and attack methods.

Recovery after the incident:
Most ICS have manual override capability. Manual override can be engaged in case of automatic system compromise or failure. In this case, luckily the attack was prevented and no impact was caused. Recovery was standard, with the disinfection or rebuilding/reinstalling of infected systems.

Cyber security hardening and proactive defensive measures:

- Updating security software regularly with new IOCs.
- Regular penetration testing.
- Establishing or reviewing cyber security processes and policies to be aware of threat techniques, and defence options.
- Training personnel to recognise USBs, emails, malicious attachments, etc.

Attacker motivation: Destroy software and damage infrastructure of an energy provider.

Identification: Sandworm.

26 https://cert.gov.ua/article/39518

"ENERGOATOM " STOPPING ATTEMPT

DATE: August 16, 2022.

TARGETS: Energoatom: Ukraine's state nuclear power company.

TTP's: T1489.

DESCRIPTION AND OBSERVED IMPACT:

Ukraine's state nuclear power company Energoatom said that Russian hackers had launched an "unprecedented" cyber attack on the company's official website. The Russian hacktivist group People's Cyber Army, which claims to include more than 8,200 volunteer members, used 7.25 million bot accounts to flood Energoatom's website with layer 4 and layer 7 DDoS traffic, rendering it unreachable. The attack lasted three hours but had no larger impact on the company's operations. Energoatom said in a statement that it managed to quickly regain control of the website and limit the attack[27].

Cyber security experts took the following actions during the incident:

- CERT-UA was informed about the incident to help with detection and blocking of the attackers' hosts.
- System administrators and the cyber security team were strengthened on the basis of the existing incident handling plans.

Weaknesses identified during and after the incident:

- The existing DDoS protection system was rated as weak and in need of replacement.
- Incident handling plans need to be reviewed regularly.
- Incident handling training should be organised on a regular basis.

Recovery after the incident:
the website was restored, no interruptions in the operational work of energy infrastructure.

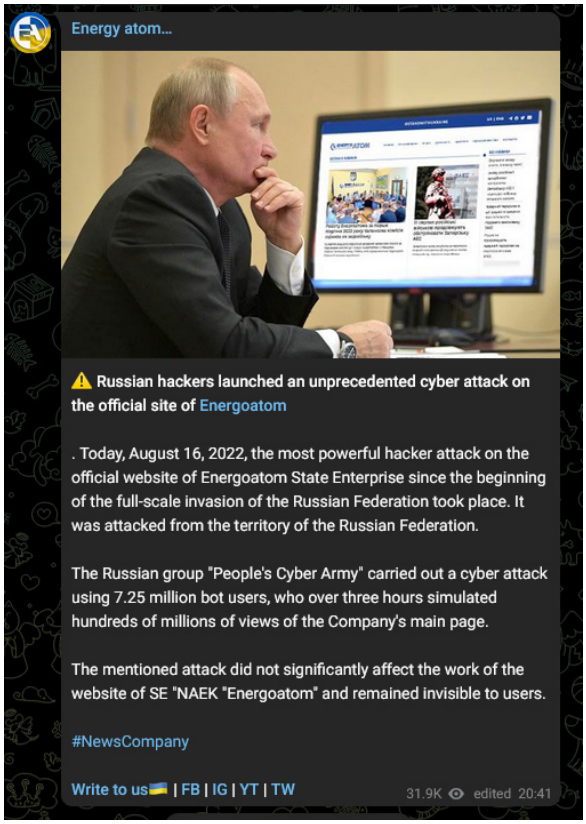


Figure 16. **Cyberattakcs on "Energoatom" in social media**

Cyber security hardening and proactive defensive measures:

- Training staff responsible for cyber security.
- Reviewing cyber security processes and policies to be aware of threat techniques, and defence options.

Attacker motivation: To spread and accumulate panic.
Identification: People's Cyber Army.

27 Ukraine's state-owned nuclear power operator said Russian hackers attacked website

08.2. Other Events in The Critical Infrastructure Sector

On June 20, 2022: A CERT-UA investigation of an attack against one of the critical infrastructure objects found a malicious document named "Imposition of fines.docx", when opened, it leads to download an HTML file and execute JavaScript code (CVE-2022-30190), which downloads and launches the malicious Cobalt Strike Beacon program. In interaction with the subject of coordination it was found that the mentioned DOCX document was contained in a password-protected archive "Imposition of Penalties.zip" which, in turn, was distributed by email, supposedly, on behalf of the "State Tax Service of Ukraine". This activity is attributed to the UAC-0098 (Trickbot) group[28].

On July 1, 2022: A cyber attack was launched against Ukraine's largest private energy sector company DTEK in coordination with missile attacks on the Kryvorizka power plant in the eastern part of Ukraine. According to Victor Zhora, the deputy head of the SSSCIP, Ukraine's cyber watchdog, the attack adds to a list of evidence of cyber and kinetic attacks used in unison. "It is a one more piece of evidence of coordination of kinetic and cyber operations by the Russian aggressors. The largest Ukrainian private energy company DTEK was cyber-attacked simultaneously with the shelling of a thermal power plant of the same company in Kryvyi Rih," Zhora wrote in a tweet. The owner of the Kryvorizka power plant, DTEK, confirmed that the company was under a Russian cyber attack to destabilise the technological processes of power generating and distribution companies. "It was at the same time as the terrorist missile attack on the Kryvorizka thermal power plant took place that another attempt was witnessed to attack the company's digital infrastructure," reads DTEK's statement. The enemy's special focus on actively attacking DTEK's facilities can be explained by the firm and proactive position taken by the company's shareholder Rinat Akhmetov concerning Russia's barbaric war against Ukraine and the massive assistance provided to the Ukrainian military and and the Ukrainians. DTEK works with state authorities and international partners to investigate the hostile actions cybercriminals and help strengthen the country's IT security with its findings and experience. Presumably, the culprit behind the attack is the pro-Russian hacker group XakNet, but looking at the past, it is not too sophisticated and has mostly conducted DDoS attacks. It is possible that XakNet conducted the attack in coordination with another group, but since they posted screenshots of DTEK's data on their Telegram channel as proof, the attack was attributed to them.

On October 2022: NikoWiper was used against an energy sector company in Ukraine. The wiper targeted a company in the energy sector in Ukraine in October 2022. NikoWiper is based on SDelete, a command line utility from Microsoft used for securely deleting files. Sandworm launched the wipers in parallel with the Russian Armed Forces' missile strikes on energy infrastructure. While ESET is not able to proove that those events were coordinated, it suggests that Sandworm and the military forces of Russia have related objectives[29].

On December 12, 2022: DolphinCape malware allegedly targeted JSC Ukrainian Railways and other government agencies. CERT-UA disclosed that the state railway and various government agencies in the country were targeted by a wave of phishing attacks. The topic of kamikaze drones, which were widely used by the Russian side at the time, was chosen for phishing emails. Attached to the email was a RAR archive containing a PPSX document, which in turn contained a VBScript code designed to create a scheduled task, as well as decrypt, build on the PC, and run a PowerShell script. The payload file is classified as DolphinCape malware, which is developed using the Delphi programming language, its main function is to collect information about the victim computer[30].

---

28 https://cert.gov.ua/article/339662

29 https://www.welivesecurity.com/wp-content/uploads/2023/01/eset_apt_activity_report_t32022.pdf

30 https://cert.gov.ua/article/3192088

08.3. Summary and lessons learned

Disruption of the operation of critical infrastructure enterprises, including through cyber influence, is a priority task in the Russian hybrid warfare doctrine. The presence of a separate hacker group Sandworm (a special unit of the GRU) of the Russian Federation and a series of successful attacks on the energy sector of Ukraine should be a serious reminder and an example in terms of ensuring cyber protection of critical infrastructure assets for the countries that see the Russian Federation as a threat. The ability of the Ukrainian cyber security capabilities to quickly detect and eliminate the threat of damage/destruction was a factor that pushed the Russian higher political and military command to use long-range missile systems to damage the Ukrainian energy facilities.

There is a substantial list of actions that can be taken to increase cyber defence of critical infrastructure:

- Monitoring and checking anomalous Process Flows, Equipment Performance, and Data Flows in order to detect cybersecurity breaches within 24 hours;
- Identification and recording of all the component pieces and versions in hte control system;
- Review of available patches and updates of OT devices found closer to the industrial process, such as PLC's and other intelligent industrial electronic devices (IIED);
- According to configuration, changing the management and safety procedures test and applying selected patches and updates;
- Responsibility for monitoring control and safety system cybersecurity vulnerabilities;
- Monitoring the current patch levels, malware notifications, and newly discovered vulnerabilities as announced by cybersecurity institutions and by vendors;
- Regular training and education on ICS cybersecurity, including attendance at organised ICS security conferences and training, such as S4, DEFCON, and Black Hat;
- Participation (sending at least one staff member or more per year) to NATO, EU, and other tabletop and live-fire exercises, such as Locked Shields, that train handling cyber attacks against control systems;
- Implementing the recommendations of this Report beyond the means of the current staff capabilities and resources;
- Operation of the network management system, Intrusion Detection, or Security Information and Event Management (SIEM) system;
- Internal operating system health tools that can be used in both an investigative and a forensic capacity to identify the source of a problem;
- Organisation and control of the use of A/V scanning-based solutions according to established policies and procedures;
- Conduct and/or organisation (in line with established industrial safety requirements) with the help of vendors a Certified Ethical Hackers' full offline black box and white box penetration testing against the switches, routers, firewalls, controllers, and instruments that the operator uses;
- Operation of a security test lab. It should be used to validate patches before deployment, to test security exploits on existing equipment and firmware, and to find and diagnose other bugs and test code before downloading it to the field;
- Ensure that users log on to the system and IED configuration changes are documented, updated and made available on-site for operations personnel.

09. Combination of Different Attacks on Multiple Sector Targets and Lessons Learned

This paragraph discusses the attacks not clasiffied in the pervious sections of the Report that occurred across combined sectors. Usually, specific cyber attacks target specific sectors due to the nature of the sector itself. Tendencies show that the attacks targeting the financial sector may not be efficient enough versus critical infrastructure. However, the most common attacks do not discriminate based on sector and target as many entities as possible. Examples os such attacks are mass phishing, spear phishing, whaling, smishing, and other social engineering techniques. Phishing is the most common technique among Russian threat groups to infect victims with malware, steal credentials, install wipers, etc. Below is a graph of the types of incidents that occurred in H2 of 2022, according to Ukraine's services. One of the most frequent types of attacks is phishing which is a popular attack vector to start targeting infrastructure.

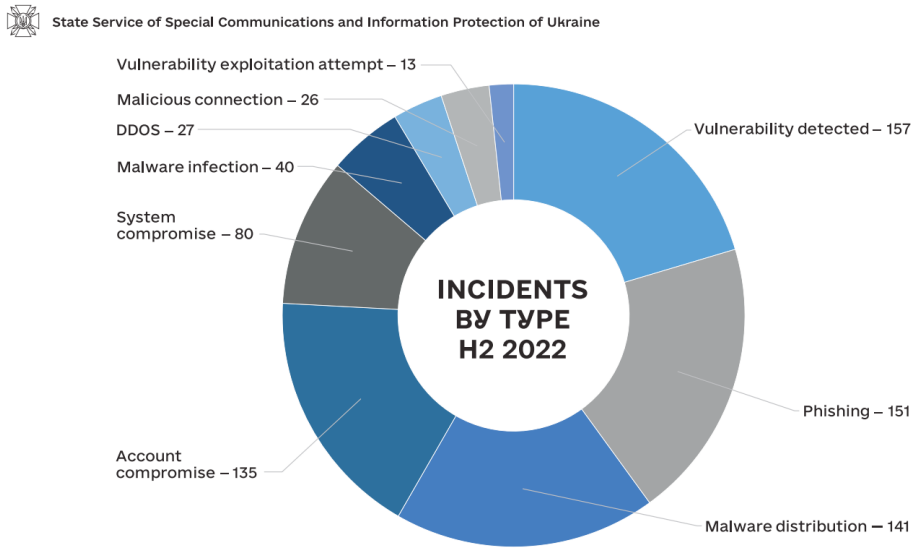


Figure 17. **The most popular threat techniques during H2 of 2022 according to SSSCIP**

09.1. The Most Significant Cyber Incidents in Multiple-Sector Targets in Ukraine

COBALT STRIKE BEACON ATTACK

DATE: April 18, 2022.

TARGETS: User systems in public networks.

TTP's: T1566, T1204, T1041.

DESCRIPTION AND OBSERVED IMPACT:

On April 18, 2022: the Ukrainian cybersecurity agency CERT-UA alerted organisations about the ongoing cyber attacks targeting Ukrainian entities using the Cobalt strike beacon malware. The threat actors behind this campaign distributed phishing emails equipped with malicious macros with the subject line "Urgent!". When the recipients open the document, the macro gets activated. Furthermore, the macro downloads creating a pe.dll file on the disk and executes it allowing the Cobalt strike beacon malware to further damage the system. With high confidence, it has been reported that the file pe.dll is protected by a cryptocurrency related to the TrickBot group. Organisations are suggested to prohibit office programs, such as EXCEL.EXE, WINWORD.EXE, etc., from initiating dangerous processes, like rundll32.exe, wscript.exe, etc[31] [32] [33].

Public military networks fell under attack as well, pieces of evidence was found about the existence of such malware on some computers (infected at the end of April) with established network connections to suspicious C2 hosts. The root cause of the infection was USB flash drives with infected Word files. Further investigation also found that the threat actor used other malicious hosts which led to a much broader threat actor's network infrastructure than expected.

Military cyber security experts took the following actions during the incident:

- CERT-UA was informed about the whole discovered network infrastructure to initiate blocking of the corresponding suspicious hosts.
- Affected user systems were investigated to check the damage impact; finally, systems were rebuilt as a result of the discovered mass infection.
- Threat analysis was carried out to define malware features and its ability to go through defence systems.
- Policies of defence and security systems were revisited to prevent another similar malware infection.
- Malicious hosts were banned so that the network connections were blocked.

Weaknesses identified during and after the incident:

- User non-compliance with security policies when using flash memory devices.
- Late review and amendment of security policies and hunting tools due to constantly changing TTPs and attack vectors.
- Improper monitoring of outbound traffic and detection of illegal connections.

31 https://cert.gov.ua/article/39708

32 https://cert.gov.ua/article/38155

33 https://cert.gov.ua/article/40559

Recovery after the incident:

User systems were rebuilt.

Cyber security hardening and proactive defensive measures:

- Increased user awareness regarding consequences of mishandled use of flash drives, opening of suspicious emails, malicious attachments, etc.
- Establishment of endpoint security systems.
- Regular security software updates with new IOCs.
- Establishment or review of cyber security processes and policies to ensure awareness of threat techniques, and defence options.

Attacker motivation: Establishing persistent C2 connection, cyber espionage.

Identification: TrickBot.

GAMAREDON OPERATIONS

DATE: 2013 - till now.
TARGETS: State body public networks.
TTP's: T1566, T1204, T1047, T1053, T1078, T1210, T1534, T1021, T1119, T1005, T1568, T1219, T1102, T1020.

DESCRIPTION AND OBSERVED IMPACT:

The Gamaredon group (aka Shuckworm, Armageddon, Actinium, Primitive Bear, Trident Ursa, UAC-0010) has been active since 2013, just before Russia annexed the Crimean peninsula. The SSSCIP claims that Gamaredon includes hackers from an FSB unit in the town of Yalta who are former employee of the Security Service of Ukraine defectors to the enemy. The malicious activity of this group has primarily focused on Ukrainian government officials and organisations. Along with the beginning of the military invasion of the Russian Federation, Gamaredon targeted its phishing campaigns against Ukraine's security and defence sector.

According to the SSSICP, the Gamaredon group was the most active APT group during 2022 and carried out the largest number of cyber attacks – 113 registered cases.

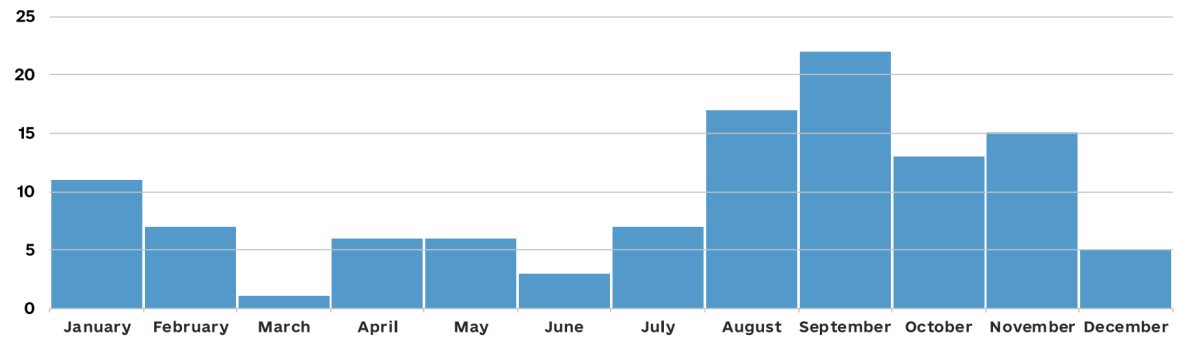


Figure 18. **Gamaredon activity in Ukraine during 2022**

The main aim of their activity is cyber espionage. But CERT-UA investigates cases of lateral movement within the network with TTPs belonging to other Russia-related threat actors after the network was infected by the Gamaredon malware.

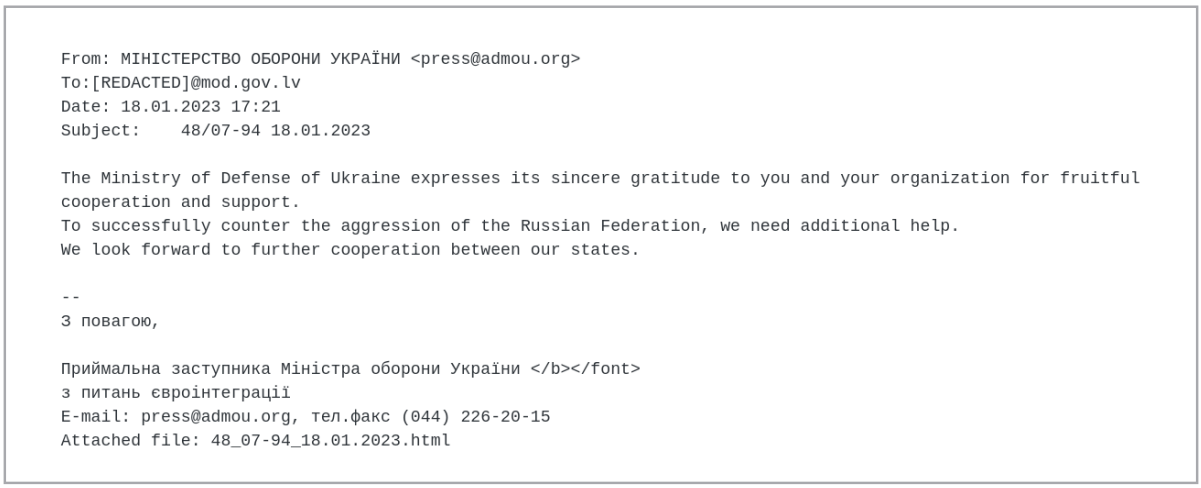
From 2022 to the present, the Security Service of Ukraine, the Ministry of Internal Affairs, the National Police, the Prosecutor's Office, military command bodies, and the judicial authorities of Ukraine are the most frequent targets of Gamaredon.

Compromised email boxes of various state institutions and organisations of Ukraine are used for sending phishing messages, while names of the topics of the letters and attachments are created using information relevant to the victim organisation.

In most cases, Gamaredon is not bothered by stealth because of its performance. They have more than 1000 compromised nodes, and more are added daily. They attacked the Ukrainian Police hunting for their privileged/unlimited access to databases/catalogues/ social registers, as the Police stores and processes information on cars, movement, cameras, road situations, arrests, etc.

Most often, Gamaredon uses phishing emails containing malicious Word documents for GammaLoaddistribute malware, such as Pterodo/Pteranodon, Giddome, GammaSteel.NET, and GammaLoad.PS1, or freely available remote access tools for targets, including Remote Manipulator System (RMS), Ammyy Admin, AnyDesk, and UltraVNC. Typically, the "Template Injection" technique is used to infect documents.

However, phishing emails are not the only ones. In the second half of 2022, Gamaredon hackers targeted the credentials of employees of the Security Service of Ukraine via the Signal messenger to gain access to accountsto steal data.



```
From: МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ <press@admou.org>
To:[REDACTED]@mod.gov.lv
Date: 18.01.2023 17:21
Subject:    48/07-94 18.01.2023

The Ministry of Defense of Ukraine expresses its sincere gratitude to you and your organization for fruitful
cooperation and support.
To successfully counter the aggression of the Russian Federation, we need additional help.
We look forward to further cooperation between our states.

--
З повагою,

Приймальна заступника Міністра оборони України </b></font>
з питань євроінтеграції
E-mail: press@admou.org, тел.факс (044) 226-20-15
Attached file: 48_07-94_18.01.2023.html
```

Figure 19. **Example of sent phishing email**

As usual, the threat actors download and install variants of their backdoor, execute scripts to ensure persistence using their C2 server, and create scheduled tasks to run every few minutes. They also use the flush DNS command to update the DNS records for their C2s.

A recent research shows an evolution in the group's tactics, whereby a hard-coded Telegram channel or cloudflare-dns[.]com service is used to obtain the IP address of the server hosting the malware (C2) to bypass network traffic detection. Another method involves the use of the Windows Management Instrumentation technique of Execution tactic by resolving the malicious IP address of Xor[.]autometrics[.]pro subdomain, that the infected host will further interact with, using the Windows Management Instrumentation.

In November 2022, another Gamaredon phishing campaign was spotted. The threat actor has been distributing phishing emails allegedly on behalf of the SSSCIP. The emails are sent using the @mail[.]gov[.]ua service to deceive users into clicking the attached link. As users click the malicious link, an HTML file with embedded JavaScript is downloaded on the system which further archives the data on the victim's computer in RAR format. The RAR file contains a shortcut file (.lnk) which triggers a sequence of downloads. First, a HTA file is downloaded and launched automatically. It creates a scheduled task to maintain persistence and subsequently launches a VBScript. Lastly, other malicious programs, such as information stealers, get downloaded on the victim's system.

On January 23, 2022 it became known that the Gamaredon phishing campaign had targeted the Lithuanian Ministry of Defence, likely by impersonating a Ukrainian Ministry of Defence email . The level of success of the phishing attack is currently unknown. It can be argued that Gamaredon has expanded the geography of its malicious activities, namely, the victims of cyber espionage can be government institutions of European countries that support Ukraine in the war.

On March 28, 2022: Gamaredon launched an attack targeting state organisations of Ukraine using a "Salary debt" theme. Attached to the letter was a document named "Salary debt.xls" with legitimate statistical data and macros. At the same time, a hexadecimal coded file was added to the collected document as an attachment. Once activated, the macro decodes data, creates an EXE file Base-Update.exe on the computer and executes it.

The file is a downloader program developed using the GoLang programming language. The program downloads and runs another bootloader which in turn allows the GraphSteel and GrimPlant malware to download and run on the victim computer. Upon execution, the GraphSteel variant of the malware runs a set of reconnaissance and credential-harvesting commands.

Additionally, the malware achieves persistence by setting the current user's registry CurrentVersion\Run value to execute the Go downloader at logon.

On April 4, 2022: Gamaredon launched an attack targeting state organisations of Ukraine using an "Information about war criminals of the Russian Federation" theme. The phishing email contained a HTML file "Військові злочинці РФ.htm" ("War criminals RF.html"), the opening of which leads to the creation of a RAR archive named "Viyskovi_zlochinci_RU.rar" on the target computer. The mentioned archive contains a shortcut file with a .lnk extension, opening which will lead to downloading a HTA file containin a VBScript code, which, in its queue, will ensure download and launch of a PowerShell script get.php (GammaLoad.PS1). The task of the latter is to determine the unique identifier of the computer (based on the computer name and the serial number of the system disk), transfer the information to be used as an XOR key to the management server by means of a HTTP POST request, and download, XOR-decode, and payload launch[34].

On July 26, 2022: Gamaredon cyber attacks using the GammaLoad.PS1_v2 malicious program. CERT-UA became aware of a mass distribution of emails with subjects saying "Information bulletin" and "Combat order", ostensibly from the National Academy of the Security Service of Ukraine. Emails were also at the same time sent to private email addresses of the targets of the attack.

During the first half of 2022, the main observed way of malicious activity implementation was distribution of HTM-droppers (including UTF-16 encoding) via e-mail (from compromised accounts and to private email addresses) that initiate the chain of delivery of GammaLoad.PS1 to victim computers.

The attackers' purpose, among other things, was to steal files with a specified list of extensions and authentication data of Internet browsers, for which GammaSteel.PS1 and GammaSteel.NET are used, respectively. GammaSteel.PS1 is likely a PowerShell implementation of the previously used HarvesterX.

---

34 https://cert.gov.ua/article/39138

In addition, one of the tactics used by the attackers was to damage the template file C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Templates\Normal.dotm using a macro the code of which generates a URL and its addition to the created document in the form link (so-called "Remote template injection"). That leads to infection of all documents created on the computer and their further unintentional distribution by the user.

Typically, scheduled tasks, the Run registry branch, and environment variables are used to execute persistence and launch payloads. PowerShell (powershell.exe), wscript.exe, and mshta.exe[35 36 37 38 39 40].

It is difficult to define actions taken to strengthen cyber defence as these are regular day-to-day attacks, however:

- CERT-UA was informed about the whole discovered network infrastructure to initiate blocking of the suspicious hosts.
- Affected user systems were investigated to examine the damage impact: to cure or rebuild.
- Threat analysis was completed by cyber experts to define malware features, including the ability to go through defence systems. This process is repeated with each new version or script of malware, as Gamaredon constantly evolves.
- Policies of defence and security systems were revisited to prevent another similar malware infection.
- Malicious hosts were banned so that the network connections were blocked.

Weaknesses identified during and after an incident:

- Increased user awareness regarding the risk of phishing tactics is necessary.
- Policies and hunting tools in security systems are revised irregularly and do not reflect the constantly changing malware and attack methods.
- No proper email protection solutions in the security systems of individual victim organisations.

Recovery after the incident:

The infected systems were cleansed using commercial high-quality anti-virus and anti-malware software. Where cleansing not possible, systems were freshly reinstalled or recovered from healthy backups.

Cyber security hardening and proactive defensive measures:

- Update security software regularly with new IOCs.
- Establish or review cyber security processes and policies to be aware of threat techniques, and defence options.
- Train people on safe use of USBs, emails, malicious attachments, etc.
- Monitoring of outbound traffic and detection of illegal connections must be a part of common cyber security policies.

Attacker motivation: Establishment of a persistent C2 connection, cyber espionage.

Identification: the Gamaredon group.

---

35 https://cert.gov.ua/article/971405

36 https://cert.gov.ua/article/1229152

37 Russia's Cyber Tactics: Lessons Learned 2022 – аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни росії проти України

38 https://cert.gov.ua/article/2681855

39 https://cert.gov.ua/article/971405

40 ANOTHER UAC-0010 STORY

09.2. Other Events in Multiple-Sector Targets

On April 13, 2022: The TrickBot group launched an email campaign attack targeting Ukraine with IcedID and Cobalt Strike. At least three Excel files were sent to Ukrainian organisations in email attachments.

The investigation found that if the document is opened and the macro is activated, the latter will ensure that the executable file is loaded and launched. The downloaded EXE file decrypts and launches the GzipLoader malware on the victim computer, which in turn downloads, decrypts, and launches the IcedID malware[41].

On April 18, 2022: The TrickBot group launched another attack targeting state organisations of Ukraine using the "Azovstal" theme and the Cobalt Strike Beacon malware. The phishing email contained an XLS document attachment bearing a macro. When the document is opened and the macro is activated, it downloads, creates on disk, and runs a pe.dll file, thus infecting the victim computer with the Cobalt Strike Beacon malware[42].

On May 19, 2022: The TrickBot group used "support@starlinkua[.]info" to send phishing emails impersonating representatives of Elon Musk and StarLink to deliver software required to connect to the internet via StarLink satellites. The email included a link to https://box[.]starlinkua[.]info/cloud/index[.]php/s/{GENERATED_ID}, an MSI installer dropping IcedID downloaded from the attacker-controlled domain, starlinkua[.]info. On May 23, 2022, a similar attack was performed against a wider range of Ukrainian organisations operating in the technology, retail, and government sectors. The delivered payload was the same IcedID binary under a filename KB2533623.msi to resemble a Microsoft update and was hosted on https://box[.]microsoftua[.]com/cloud/index[.]php/s/{GENERATED_ID}.

On June 20, 2022: Cyber attack by APT28 using CredoMap malware. Ukraine's CERT-UA intercepted a malicious document named "Nuclear Terrorism A Very Real Threat.rtf". The hackers selected the filename to ta pinto the fear of a potential nuclear attack among the Ukrainian people. Opening the document downloads a HTML file and executes JavaScript code: CVE-2022-30190 which ensures download and launch of the CredoMap malware. Meta-data indicates that the document was modified on June 9, 2022, so its distribution could have taken place on June 10, 2022. According to the set of characteristic features, CERT-UA considers it plausible to associate the detected activity with the activities of the APT28 group[43].

On October 21, 2022: A cyber attack against state organisations of Ukraine using RomCom malware. CERT-UA tracked down an email dissemination campaign pretending to come from the Press Service of the General Staff of the Armed Forces of Ukraine and delivering a link to an unofficial web page to download an alleged "order". Running the mentioned file decodes and runs the rmtpak.dll file. The latter is classified as RomCom malware. This activity is attributed to the Tropical Scorpius (UNC2596) group[44].

09.3. Summary and lessons learned

Only a handful of attacks were efficient in their nature against multiple sectors or entities. Phishing and DDoS is an example of such an attack. Email phishing, spear phishing, whaling, smishing, and other social engineering techniques are the most popular method to get the initial access to a target system and are usually the main vector of infection/compromise. There are numerous mitigation techniques regarding phishing campaigns but most of them concentrate on user education. There are some common practices to mitigate phishing attacks:

---

41 https://cert.gov.ua/article/39609

42 https://cert.gov.ua/article/39708

43 https://cert.gov.ua/article/341128

44 https://cert.gov.ua/article/2394117

- Have a policy established for users who tend to constantly get compromised in phishing simulations, have a mandatory course about the dangers of phishing;
- Constantly improve user awareness about cyber security threats on national, state, and local levels;
- Extend and strengthen cyber security teams and systems to build more effective security perimeters;
- It is also advisable for larger organisations to deploy Secure Email Gateways. For example, the Symantec™ Messaging Gateway is an on-premise email security solution that provides inbound and outbound protection against the latest messaging threats, including ransomware, spear phishing, and business email compromise (BEC). This tool intercepts user emails and attachments, analyses the attachments in a sandbox for malicious activity employing heuristics algorithms, and either releases them or removes them from emails. Additionally, the message gateway replaces all email hyperlinks with a proxy link, which prevents the accidental downloading of malicious payloads;
- Have redundant additional communication channels for organisation employees about ongoing cyber threats;
- Conduct regular training and information campaigns for top-level executives, managers, or commanders who might be a target for whaling attacks.

10. Distributed Denial of Service Attacks and Destructive Noise

In general, DDoS attacks are a very popular Russian-affiliated hacktivist technique. According to various open sources and media reports, the following websites and online resources were targeted by DDoS attacks on multiple different occasions. Here are several examples:

- Ukrainian Ministry of Foreign Affairs – mfa.gov.ua;
- Ukrainian Ministry of Defence – mil.gov.ua;
- Ukrainian Ministry of Internal Affairs – mvs.gov.ua;
- Security Service of Ukraine – ssu.gov.ua;
- Ukrainian Cabinet of Ministers – kmu.gov.ua;
- Oschadbank – oschadbank.ua;
- Privatbank – privatbank.ua.

The IP addresses of the listed domains were resolved and a Netflow analysis was conducted for the period corresponding with the DDoS attacks. The available Netflow results revealed more than 3,000 unique IP addresses spanning multiple countries and continents that were the source of the DDoS attacks. It is important to note that the majority of the IP addresses involved in any of the observed DDoS attacks were not located in Russia or Belarus. Further analysis was conducted on the 50 most active IP addresses retrieved from each attack using proprietary data enrichment techniques and open and closed intelligence sources.

10.1. Notable DDoS Attacks in Ukraine

FEBRUARY 15 DDOS ATTACK

On February 15, 2022: Minister of Digital Transformation of Ukraine Mykhailo Fedorov announced that a cyber attack against the websites of Ukraine's Defence Ministry and Armed Forces, as well as the interfaces of the country's two largest banks, was the largest assault on its kind in the country's history and "bore traces of foreign intelligence services." Ilya Vityuk, the Head of the Ukrainian Intelligence Agency's Cyber Security Department, blamed Russia for the attack, citing as evidence that execution of the attack likely cost "millions of dollars", far beyond the capabilities of individual hackers or groups. He asserted that Russia was the only country interested in such strikes againts Ukraine.

More than 200 unique IP addresses were identified in the February 15 DDoS attack. The attack consisted of HTTPS flooding on port 443. This type of attack is designed to overwhelm a targeted server with HTTP requests. Once the target has been saturated with requests and is unable to respond to normal traffic, a denial-of-service will occur for additional requests from actual users. Analysis of the 50 most active IP addresses revealed that approximately half of them appeared to be MikroTik routers, or other devices running SquidProxy.

Analysis data also revealed that the majority of the IP addresses have prie viously been associated with the activity from the following implants:

- Xorddos;
- Cobaltstrike;
- Amadey;

- Trickbot;
- Qakbot;
- Lokibot;
- Jedobot;
- Bluebot;
- Betabot;
- Gumblar;
- Kasidet;
- PonyLoader;
- Smokeloader.

Unfortunately, it is not possible to determine from the available data if the malicious HTTP requests were sent by the routers, compromised hosts behind them, or a combination of both. It makes attribution of this particular attack to any one threat actor extremely difficult.

Fortunately, the attack appeared to have only a minimal impact on its targets. According to a statement from Victor Zhora of the Ukrainian Center for Strategic Communications and Information Security, Ukrainian cyber-security officials managed to significantly reduce the amount of harmful traffic to the websites. Furthermore, while the targeted banks confirmed the attack, they indicated that users had only been temporarily unable to withdraw money from their accounts. Banking services were quickly restored and customers' balances were not affected.

FEBRUARY 23 AND 28 DDOS ATTACKS

On February 23, 2022: Mykhailo Fedorov reported yet another DDoS attack against Ukrainian websites.

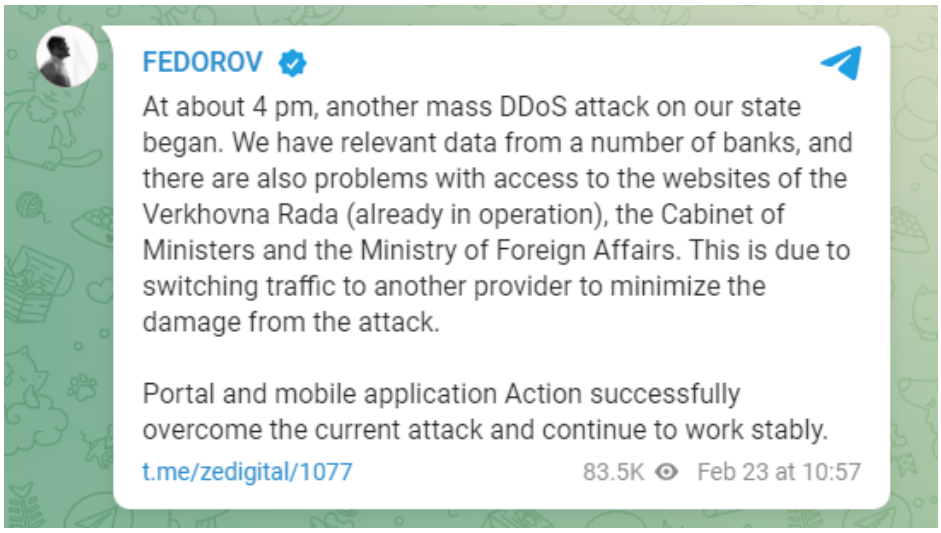


Figure 20. **Report on DDoS attack**

Another DDoS attack that took place between February 27 and 28 was largely unreported in the media, likely because such attacks were becoming a commonplace at that point.

More than 3,000 unique IP addresses were identified in the DDoS attacks of February 23 and 27-28. The analysis of the identified IP addresses revealed that the vast majority of them were running MikroTik Bandwidth-test server on port 2000 with a connection signature of \x01\x00\x00\x00, recursion enabled on UDP/TCP port 53, and multiple versions of MikroTik RouterOS services on various ports. Analysis of the 50 most active IPs retrieved in the second and third attacks revealed that 76% and 92%, respectively, can be identified as MikroTik devices .

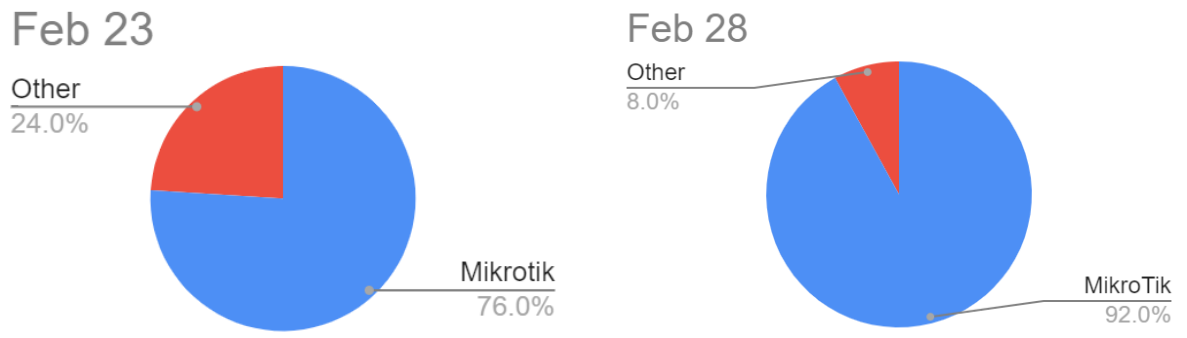


Figure 21. **Increase in MikroTik botnet use**

100% of the identified IPs had DNS recursion enabled on port 53. It means that the threat actor sent spoofed DNS requests to the MikroTik devices, which allowed DNS recursion. The requests were then processed as valid and returned to the spoofed recipients, in this case, the targeted Ukrainian websites. It is known as an amplifier attack because this method takes advantage of misconfigured DNS servers to reflect the attack onto a target while amplifying the volume of packets. SecurityScorecard (SSC) has named the botnet used to conduct the second and third DDoS attacks "Zhadnost" - Russian for "Greed."

Zhadnost is somewhat similar to the Mēris botnet identified by Russia-based companies Yandex and Qrator Labs in 2021. Yandex/Qrator Labs reported that 90 to 95% of the Mēris bots that had recently targeted Yandex with a DDoS attack had MikroTik Bandwidth Test running on port 2000 with a connection signature of \x01\x00\x00\x00. According to a different report released by NetScout on October 28, 2021, NetScout discovered that at least two distinct MikroTik-based IoT botnets are inhabiting the same population of unpatched, exploitable MikroTik routers; Mēris, which uses HTTP Pipelining as a form of attack, and a botnet called Dvinis (Latvian for "twin"), which does not. Instead, Dvinis uses an apparent typo in the attack generator which appends an extra '/' character to the end of the URIs targeted in HTTP POST and GET floods.

In response to the Yandex/Qrator labs discovery, MikroTik released a report identifying Mēris bots as MikroTik routers that were compromised in 2018 when MikroTik RouterOS had a vulnerability which was then quickly patched. There was no new vulnerability in RouterOS and there was no malware hiding inside the RouterOS filesystem, however, the attacker was reconfiguring RouterOS devices for remote access using commands and features of RouterOS itself. Unfortunately, closing the old vulnerability did not immediately protect these routers.

Although MikroTik provided some mitigation advice in its official statement, it did not say anything about ensuring that DNS recursion was properly configured. But there is evidence that MikroTik is aware of this vulnerability. According to MikroTik's website, every MikroTik that has the Allow-Remote-Requests feature

turned on is a potential attack vector, representing a 1:179 bandwidth amplification factor.

A preliminary analysis using the Mēris identification tool of Qrator Labs has revealed that none of the Zhadnost IP addresses were part of the Mēris botnet. Such an identification tool does not exist to test the Dvinis nodes. However, only the first attack utilised HTTP floods which Dvinis is known for. Zhadnost bots do not require a compromised router, only a router with a misconfigured DNS recursion. Therefore, the SSC assesses that Zhadnost IPs are not like to be part of Dvinis. Thus, we believe they are a new botnet, controlled by a different actor.

Analysis of the 50 most active Zhadnost bots/MikroTik routers used in the second and third attacks has also revealed that several devices behind them had previously been associated with the activity of the following implants:

- Amadey;
- Betabot;
- Gumblar;
- Lokibot;
- Ponyloader.

All threat actor had to do to create Zhadnost was to establish and maintain a list of MikroTik and other devices with misconfigured DNS recursion settings, which would forward spoofed requests to the targeted websites. It can be easily done using tools such as Shodan and Google Dorks. According to our Attack Surface Intelligence Data, there are at least 875,000 MikroTik devices located all over the world. This could potentially represent a near-infinite number of bots, provided DNS recursion is not properly configured on these devices .

Figure 22. **Zhadnost botnet activity**

Attack Date	Feb 15th	Feb 23rd	February 28th
% MikroTik	50%	76%	92%
DDoS Attack Type	HTTP Flood	DNS Amplification	DNS Amplification
# of unique IPs	200	1892	1958
% previously compromised	50%	4%	12%
DNS Recursion Enabled %	20%	100%	100%

Figure 23. **Botnet activity statistics comparison (2022)**

Attribution of Zhadnost and the DDoS attacks to any threat actor is difficult given that anyone could have taken advantage of this misconfiguration with little effort. Furthermore, it is difficult to differentiate between the traffic from the router itself and the legitimate traffic of the devices behind it, making identification of the command and control infrastructure extremely difficult. However, taking into account the current geopolitical factors, and considering which country is likely to profit from such attacks, the SSC assesses with moderate confidence that Russia, or Russian-aligned actors, are likely behind the discussed DDoS campaign.

Despite the involvement of MikroTik devices in all three attacks, a further comparison reveals that the first attack is quite different from the second or third :

Based on the identified differences, the SSC assesses with moderate confidence that the IP addresses used to execute the second and third DDoS attacks against the Ukrainian government and financial websites were solely Zhadnost bots, meaning MikroTik and other routers with misconfigured DNS recursion settings. We assess that the IP addresses used in the first attack were a combination of Zhadnost45 bots and other botnets possibly controlled by criminal actors who partnered with or were hired by the same threat actor.

The SSC also assesses with moderate confidence that the DDoS attacks had a minimal impact on their targets. This is likely a result of Ukraine's adequately preparedness to handle such incidents since similar tactics had been used in the previous attacks. Furthermore, various Ukrainian officials have made public statements regarding Ukraine's success in minimizing the effects of the attacks.

45 SecurityScorecard discovers new botnet, 'Zhadnost,' responsible for Ukraine DDoS attacks

10.2. Ongoing Persistent DDoS Noise

Since Russia began the full-scale invasion of Ukraine in February 2022, several hacktivist groups such, as KillNet, NoName057(16), Legion Spetsnaz RF, Anonymous Russia, QBotDDoS (Mirai), Passion Botnet, Russian Hackers Team, Lira, Furious Russian Hackers, Anonymous Sudan, etc, have sided with Russia and carried out cyber attacks against Ukrainian information resources, as well as assets of countries that support Ukraine. Based on tactics, techniques, and procedures (TTPs) associated with the groups, they appear to be technologically less sophisticated and unable to conduct continuous, destructive DDoS attacks.

The hacktivist activity of pro-Russian DDoS collectives is increasingly aimed at maintaining a constant informational influence on the domestic audience of Russia, and at maintaining the narrative of the omnipotence of the Russian state in all spheres, including cyber. At the same time, cyber attacks of pro-Russian hacktivist groups remain the main tool of information pressure on the population of the target country in return for political decisions that harm the Russian interests.

10.3. Summary and lessons learned

The DDoS attacks conducted against the Ukrainian infrastructure websites disrupt their availability for short periods of time and have close to no long-term impact. Learning this, threat actors have turned towards targeting more critical assets, such as networks used for power generation, communications, military units, and hospitals. DDoS attacks have become very popular since the beginning of the war and were the most often used technique in 2022 all over the world. Even though DDoS is a relatively easy attack to execute, it can cause harm in different scenarios ranging from reputational damage or panic to threatening crucial life services.

The following mitigation techniques can be used to protect from this type of attack:

- The SSSCIP recommends that organisations check the DNS recursion settings in their routers, whether they are MikroTik or of another vendor. It is recommended that DNS recursion is disabled if it is not required in the daily activities. If required, it should be configured to only conduct recursion for trusted domains/hosts.
- It is critical to put DDoS mitigations in place, via a service like Cloudflare, Akamai, or AWS CloudFront. Having a firewall will not stop the volume of traffic shown observed against Ukrainian targets in a Netflow analysis.
- Automate the disaster recovery runbooks for on-premise systems and ensure that you can move workloads to the disaster recovery site with a single click, if possible.
- Furthermore, blocking Russian IPs will not stop DDoS attacks. The attacks are coming from across the world from neutral countries in Latin America, the EU (not Russia or Belarus), and Southeast Asia.
- A RCDC CTAC team published a study named Distributed Denial of Service attack (DDoS) and Methods of Mitigation. The study brings the depth of analysis into its area of research, and a brief list of measures that engineers can take before, during, and after a DDoS attack. The study can be found on the website.

11. Strategic Communication during a Cyber Crisis and Lessons Learned

Modern warfare presented new challenges in establishing communication between the government and foreign partners, the government and the military, and especially, between the government and the population. Traditional channels, such as TV, radio and news, are still important but do not allow fast notifications about dangerous events, like air or artillery strikes, natural disasters, and cyber threats as well. There is also a significant necessity for different kinds of feedback from the population, such as information about enemy squads on occupied territories, damaged critical infrastructure, etc. Mobile internet, various messenger systems, special mobile applications - there are many modern digital services, which can serve better in this role. On the other hand, introduction of digital services increases the risk of cyber threats, both to the services and to their users.

Here are several examples of services established in Ukraine:

01. National roaming: The Ministry of Digital Transformation together with the largest national mobile operators launched a national roaming service. With national roaming, it has become possible to connect to the network of other operators if the connection disappears46.
02. Emergency Population Warning System was developed by the State Emergency Service of Ukraine to warn the population about any kind of dangers, such as air or artillery attacks, chemical or nuclear attacks, natural disasters, etc. The new notification system works based on Cell Broadcast technology, which has significant advantages over SMS notification: faster receipt of notifications, flexibility in choosing locations to be notified, and presence of a sound signal even if the sound on the subscriber's smartphone is turned off. It is not necessary to install something specific on the phone - all Ukrainian users can receive the signals. In September 2022, the State Emergency Service reported that the system was completely tested and ready to use47.
03. Telegram bot of the Security Services of Ukraine @stop_russian_war_bot, created by the SSU in the very beginning of Russia's full-scale invasion to allow people to send in notifications about enemy troops and vehicles, their locations, movements, war crimes, collaborators, etc. On October 18, 2022, it was reported that the bot had received over 100,000 messages from Ukrainians. This helped to destroy hundreds of units of enemy military equipment and even eliminate several Russian generals48.
04. The State Emergency Service of Ukraine developed an interactive map of the territory, potentially polluted with explosive objects. This map sdisplays the sites where explosive objects have already been found or are likely to be found, and the level of threat they pose according to the information available from the State Emergency Service (localization error is up to 30 m). There is also a mobile application (both Android and iOS) with an interactive map, as well as recommendations on how to detect dangerous items, safety instructions, etc. It also contains an alert function with an immediate signal if the person enters the red zone[49].
05. єBopor - the Telegram bot developed by the Ministry of Digital Transformation of Ukraine, fully integrated with Diia (Ukraine digital service) and advanced functionality for detection:

46 https://www.kmu.gov.ua/en/news/mincifri-ukrayinski-operatori-dozvolyat-peremikatisya-mizh-merezhami-shchob-lishatisya-na-zvyazku
47 https://mediacenter.org.ua/emergency-population-warning-system-of-state-emergency-service-covers-67-of-subscribers/
48 https://ssu.gov.ua/en/novyny/zavdiaky-chatbotu-sbu-znyshcheno-sotni-odynyts-vorozhoi-tekhniky-i-navit-dekilkokh-heneraliv-illia-vitiuk
49 https://mine.dsns.gov.ua/

- Enemy equipment and troops
- Collaborator activities
- Explosive or suspicious items
- Photo/video of Russian military in de-occupied settlements50.

06. єППО - an air strike prevention notification system. Ukraine has created an application for mobile phones that will help air defence units supplement radar information about air targets for their subsequent destruction.

How the app works: if you see an air target, for example, a missile or a kamikaze drone, you need to open єППО on your smartphone, select the type of air target, point your smartphone in the direction of the target and press the big red button.

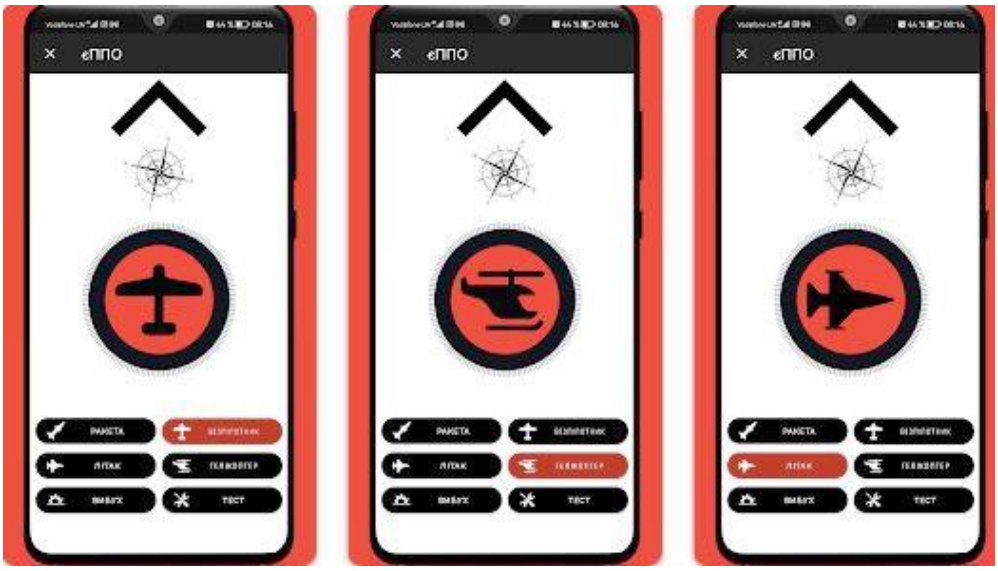


Figure 24. **Interfaces of єППО app**

50 https://en.interfax.com.ua/news/telecom/810765.html

51 Українці через застосунок єППО можуть допомогти зенітникам збивати ворожі дрони та ракети

11.1. Summary and lessons learned

Ukraine has given some good examples of people and resources mobilised for strategic communication in a short period of time. Ukraine has shown expertise with its widespread use of digital technologies in ensuring stable communications between the population and state management bodies, and vice versa, during the crisis period. The communication methods demonstrate the importance of a sustainable population access to communication services and the internet, as well as keeping all citizens updated about any possible threats, thus allowing them to assist the armed forces in tracking down the enemy.

Each country or alliance should consider having a well-developed, tested, and reliable public communication and warning system.

Also, it is worth noting that a stand-alone system is not sufficient in today's complex communication landscape, thus state security bodies and state government bodies should maintain an online presence within such networks as Signal, Telegram, Twitter, and others. The key point is that accounts on such platforms need to be verified and reliable. Trust and confidence in such accounts need to be at a high level to avoid impersonation or misinformation.

12. Conclusions

Looking back at the military history, the cyber domain was used for the first time in parallel with the conventional military domains during the war in Ukraine. Cyber played a massive role even before the kinetic actions started – by crippling the adversary offensive and defensive capabilities, and thus impacting the morale. Cyber actions from the side of Russia were aimed at supporting ground operations.

According to the statistical report of the State Cyber Protection Centre of Ukraine, in 2022 there were 2.8 times more cyber incidents than in 2021. The number of cyber incidents in the Malware and Informational gathering categories increased by 18.3 and 2.2 times accordingly. The number of events detected and related to Russia increased by 26%. In 2022, there were 2194 officially detected and investigated cyber attacks (1655 beginning from Feb 2022).

Russia's offensive cyber operations, along with the electronic warfare, failed to cripple Ukraine's command and control (C2) capabilities and its critical, private, and public infrastructure for a prolonged period of time. Ukraine, with the assistance from private companies and Western governments, was able not only to mitigate the majority of cyber attacks against its infrastructure but also to develop offensive cyber capabilities of its own.

The greatest threat in cyberspace to Ukraine is hacker groups associated with the FSB, GRU, and SVR. To a lesser extent, financially motivated hacking groups and pro-Russian hacktivist groups are also a threat. The most active hacking groups are Sandworm, APT28, EmberBear, Turla, Gamaredon, Calisto, and APT29, while Killnet, NoName057, People's Cyber Army, XakNetTeam, and RaHDit are the most active pro-Russian hacktivist groups.

This Report looks deeper into the cyber aspect of the Russo-Ukrainian war. Multiple incidents and mitigation techniques are analysed and summarised. Unfortunately, the war is still ongoing, and the information adds and changes every day. Additionally, a thick "Fog of War" covers the entire conflict, political landscape to cyber landscape, and makes any predictions, recommendations, and lessons difficult to draw. It is crucial to be aware that this study is a point-in-time overview of the situation and the situation can drastically change at any moment.

13. Way Forward

Since the cooperation of the Russian Federation and China has become closer, and the latter makes efforts to gain a new geopolitical status, an increase in espionage activities of Chinese state cyber actors, such as APT27, APT30, APT31, Ke3chang, Gallium, and Mustang Panda, is expected against the EU and NATO countries, along with the constant threats from the politically motivated Russian APTs and hacktivists. Taking into account the considerable experience and capabilities of the Russian special services, it is also important to physically protect data centres and network equipment from unauthorised bookmarking of third-party devices and software that could allow attackers to remotely access target systems.

The future will see an ever-growing investment in cyber defence and even offence, which is essential to mitigate security risks. Organisations can significantly reduce their vulnerability to cyber attacks by implementing robust cybersecurity measures, such as firewalls, intrusion detection systems, and employee training programs. Moreover, having a comprehensive cyber defence strategy in place can help to minimise the impact of a successful attack. Investing in cyber defence is essential self-defence for businesses and governments against the growing threat of cyber attacks. Costs of a successful attack can be devastating, and the risks are only increasing as our world is becoming more digital.

The technology revolution has reached even the most everyday people around the world, and cyber threats followed. Cyber security is no longer relevant only to professionals. People are the frontline defence against cyber attacks in every country. They are often the first point of contact with potential threats, and their actions can either increase or decrease the likelihood of a successful attack. Educating people about the risks and best practices can help to prevent attacks and minimise the damage in the event of a successful attack. From providing information via state and private media channels, like TV and the radio, to education and training at schools and universities, cyber awareness and defence needs to be taught and trained.

The recent explosion of AI technology has the potential to become a game changer in cyber warfare. AI is already used in cyber defence to detect and respond to threats more quickly and efficiently. However, AI can also be used by aggressors to carry out sophisticated cyber attacks. One way in which AI can be deployed to cyber warfare is through the use of machine learning algorithms for identification of patterns and anomalies in network traffic. It could ensurereal-time detection of and response to threats and improved speed and accuracy of cyber defence. Yet another potential use of AI in cyber warfare is in the development of autonomous malware that can adapt and evolve in response to changing conditions. It could make cyber attacks more difficult to detect and mitigate for the defenders. Overall, while AI has the potential to be a powerful tool in cyber defence, it also poses significant challenges for those working in the field. As such, it will be important that cybersecurity professionals develop new strategies and tools to counter the threats posed by AI in cyber warfare.

Report on Cyber Lessons Learned during the war in Ukraine
Layout by the Visual Information Section of the MOD General Affairs Department,
Totorių str. 25, LT-OI 121 Vilnius. 2023