NCSCC
NATIONAL CYBERSECURITY COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

ICWR
INSTITUTE OF CYBER WARFARE RESEARCH

CYBERSECURITY THREAT LANDSCAPE of UKRAINE in 2023

The study "Cybersecurity Threat Landscape of Ukraine in 2023" was made possible through support provided by the U.S. Agency for International Development within the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENTS

BRIEF OVERVIEW OF THE REPORT

The report "Cybersecurity Threat Landscape of Ukraine in 2023" provides information on the period from January 1, 2023, to December 31, 2023. This report is prepared for the first time and that is why it cannot be compared to reports made in previous years.

The main objectives of the study of the Cybersecurity Threat Landscape of Ukraine in 2023 are to manage cybersecurity, to support decision-making at a strategic level, to determine priorities in development of cybersecurity policies and procedures, to distribute information regarding cyberthreats and ways to counter them. The results of the study are oriented on the audience of strategic and tactical levels: cybersecurity strategy developers, heads of organizations, cybersecurity managers from state and private sectors and representatives of international partners.

The report was prepared using an adapted version of the ENISA[1] methodology "ENISA Cybersecurity Threat Landscape Methodology, July 2022" (ENISA Cybersecurity Threat Landscape Methodology, July 2022). Information on an adapted version of the ENISA methodology is provided in the Appendix.

To prepare the report, we used information from open resources, including publications with cyberthreat analysis from leading cybersecurity companies, data on cyber incidents and cyber-attacks from our own sources, information from the MISP compromising indicator exchange system and the OpenCTI cyberthreats analysis, as well as interviews with Ukrainian cybersecurity experts and questioning representatives of the state agencies, critical infrastructure facilities, private sectors and communities. With an assistance of the National Coordination Center for Cybersecurity (NCCC), 398 respondents filled out questionaries.

A language of the report "Cybersecurity Threat Landscape of Ukraine in 2023" is Ukrainian, and it will be translated into English for distribution and feedback from ENISA and Ukraine's partner countries.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology?v2=1

INTRODUCTION

On a background of Russia's full-scale invasion of Ukraine, the main threat to Ukrainian organizations in 2023 was an activity of hacker groups affiliated with Russia's special services.

According to results of the reporting period, the main subjects of cybersecurity of Ukraine report an increase in number of recorded cyber incidents and cyber-attacks compared to 2022. According to the SBU (the Security Service of Ukraine), 4500 cyberthreats[2] were recorded in 2023; according to the State Service of Special Communications and Information Protection of Ukraine, the CERT-UA Government Response Team handled 2543 cyber incidents[3], the State Cyber Protection Center record 1105 cyber incidents[4]; according to Microsoft Ukraine is the most attacked country in Europe[5]. The increase in number of incident reports from both state and private sector organizations, improved cyberthreat intelligence exchange (cyberthreat intelligence, CTI) sharing both withing the state and with international partners, and better situation awareness due to the implementation of cybersecurity systems and sensors in organizations[6] also contributed to this growth. Therefore, despite the growth in the total number of incidents, the number of cyber incidents with critical consequences is insignificant, considering challenges of cyber warfare faced by Ukraine.

The largest number of cyber-attacks by Russian APT groups targeted the state agencies, the Ukrainian Defense Forces, defense industry organizations and enterprises, telecommunications, energy, and IT sectors. The media is also among the most targeted, with attacks on it being part of broader information operations by Russian special services.

An activity of other countries that support Russia or do not support Ukraine was aimed preliminary at a presence in the information systems of the state agencies and defense sector enterprises for the purpose of espionage[7]. At the beginning of 2023 attempts were recorded, including destructive attacks by Iranian groups after publication of information about weapons supplied to Russia from that country.

[2] The number of cyber-attacks on Ukraine's critical infrastructure per year has increased from 800 to 4500: SBU names organizers, https://minfin.com.ua/ua/2024/05/07/126427603/

[3] CERT-UA government team handled 2543 cyber incidents in 2023, https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

[4, 6] In 2023, the number of registered cyber incidents increased by 62.5%: report of the DTSKZ (the State Cyber Protection Center) Cyber Incident Response Center, https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz

[5] Espionage fuels global cyberattacks, https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

[7] Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

Private citizens, especially internally displaced persons, are most at risk from phishing websites and online fraud that exploit subjects of financial assistance and compensation for damaged property from the Ukrainian Government and international organizations. Financially motivated cyber criminals use social engineering methods, rapidly react to events in the country and continuously improve fraudulent schemes[8].

The key cyberthreats identified and analyzed while preparing the report "Cybersecurity Threat Landscape of Ukraine in 2023":

- social engineering;
- malicious software;
- DDoS-attacks;
- online fraud;
- using cyber-attacks to support information and hybrid operations;
- account compromising and information leaks;
- disruption of availability due to equipment or network failures or damage;
- destructive attacks.

It is to point out that other cyberthreats were also considered while preparing the report: supply chain attacks, exploitation of the zero-day vulnerabilities, ransomware attacks, etc. However, an insufficient amount of available information, a small number of cyber incidents described, and an overall low assessment of the likelihood of their realization by the interviewed experts did not allow us to include such cyberthreats in the cyberthreat landscape report.

[8] https://csirt.bank.gov.ua/cyber-fraud

KEY FEATURES AND CONCLUSIONS

More sophisticated and targeted attacks on organizations of interest using social engineering.

Information leaks, the OSINT data and data stolen as a result of previous attacks are carefully analyzed and used for subsequent targeted attacks. Mobile devices are actively used to distribute phishing messages. In many cases, stolen user accounts are used to gain initial access to organizations' networks.

Attacks on user accounts.

The main target of attackers is user accounts and authentication data for online services. The number of attacks of following types has increased significantly: password mining, password spraying, and Adversary-in-the-Middle (Adversary-in-the-Middle). Malware that collects passwords from browsers, authorization tokens from compromised hosts, and phishing recourses are used to steal accounts.

Using legal services and tools during cyber-attacks.

Both state-sponsored and financially motivated hacker groups are increasingly using trusted legal services and tools to conceal their activity while gaining access to organizations' networks. For example, the Telegram platform is actively used to distribute malware, as a phishing channel, and as command-and-control services.

Better coordination between cyber-attacks and military & information operations.

Starting from autumn 2022, Russia made efforts to align cyber operations with military objectives, and this trend intensified in 2023. The intensity of cyber-attacks, the choice of priority targets at the level of entities, regions, and sectors correlates with a conduct of military operations and targets of kinetic attacks on Ukrainian infrastructure. Compromising information systems of organizations, in particular, security devices (surveillance cameras), in areas of shelling is used, among other things, to analyze consequences of the attacks. Data stole during cyber-attacks, defacement in state agencies and media are used in influence operations.

Control over activities of pseudo-hacktivist groups by special services.

Starting in late 2022 and early 2023, Russian special services took full control of all pro-Russian hacktivist groups, directing their activities to achieve Russia's military and political goals. At the same time, Russia has developed the "technology" of forming, legitimizing and supporting such groups of pseudo-hacktivists on a turnkey basis, depending on geopolitical objectives, and uses it to conduct cyber-attacks and influence operations. For example, at the beginning of Israeli conflict after October 7, 2023, terrorist attack, dozens of new pseudo-hacktivist groups were created to attack Israeli infrastructure, while at the same time, several incidents in Ukraine were at the lowest point in the last few years. At the end of 2023, there was a tendency to "monetize services" of several pseudo-hacktivist groups controlled by Russian special services.

OVERVIEW OF THE LANDSCAPE OF CYBERTHREATS

Russia's ongoing war against Ukraine was the main factor in 2023 that influenced the cyberthreat landscape. The main danger for Ukrainian organizations was an activity of hacker groups affiliated with Russian special services.

This directly influenced on a choice of cyber-attacks targets. The most attacked sectors in 2023 were the following: public administration, security and defense, telecommunications and energy, financial and banking, logistics, IT, and defense enterprises. Also among the most targeted sectors was media sector, which was a part of broader information operations by Russian special services. The figure shows data of the CERT-UA[9] Government Response Team on a number of cyber incidents by sectors, comparing the first and the second half of 2023.

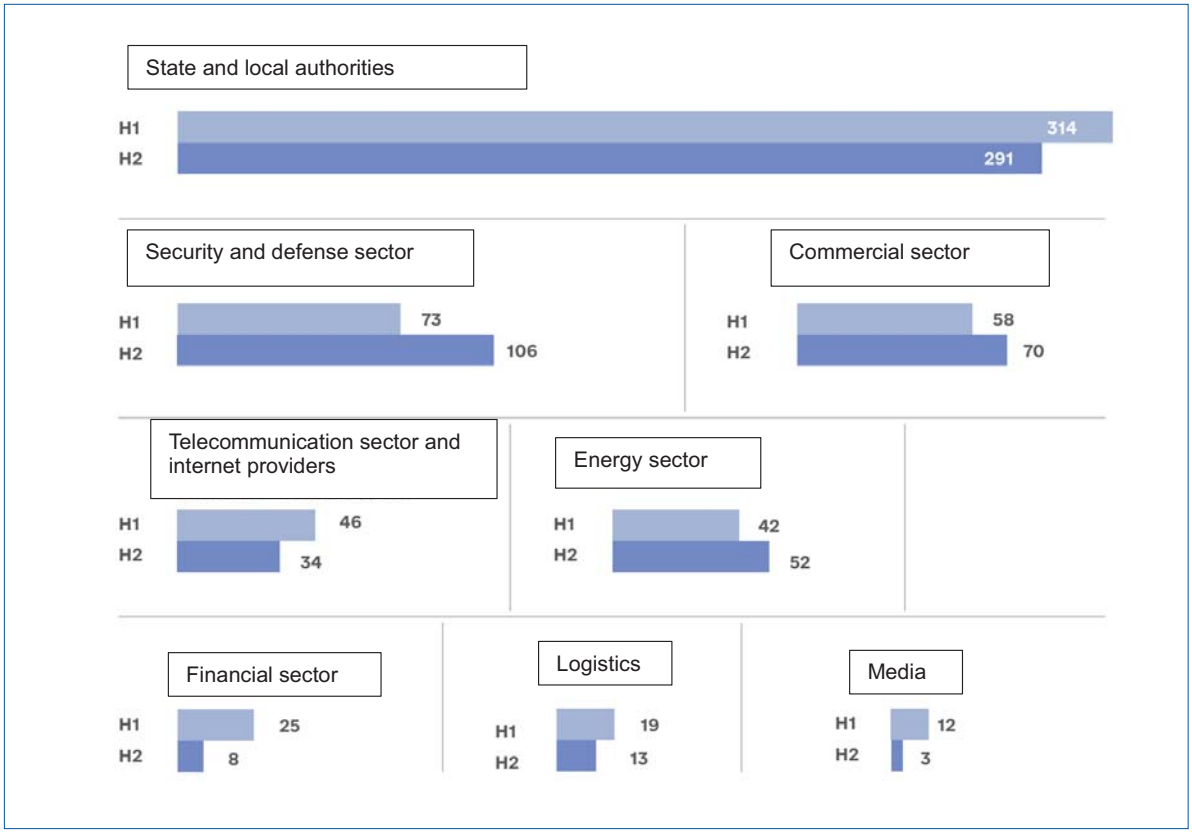


Figure No.1. *Number of incidents by sectors, comparing the first and the second half of 2023.*

[9] Russian cyber operations. Analytics for the second half of 2023, https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi

Starting from autumn 2022, Russia made efforts to align cyber operations with military objectives, and this trend intensified in 2023. An intensity of cyber-attacks, a choice of priority targets at the level of facilities, regions, and sectors correlates with a conduct of military operations and targets of kinetic attacks on Ukrainian infrastructure, as well as with operations of the Ukrainian Defense Forces. In response to July 17, 2023, explosion of the Crimean Bridge the following weeks saw a marked increase in the activity of all major Russian and Belarus hacker APT groups against Ukrainian organizations, including attempts to conduct destructive operations. Russian cyber-attacks on energy sector enterprises, including destructive ones, which increased in the second half of the year, became a preparation for further kinetic strikes on energy facilities.

At the same time, compared to the previous stages of cyber warfare, in 2023, the number of destructive operations involving elimination of data and/or damage to the functioning of information systems decreased. The activity of Russian APT groups has become more focused on espionage and information operations. Under these circumstances, Russia has expanded its cyber and information operations to Western countries that support Ukraine.

This section does not contain a comprehensive list of all trends identified in 2023, but rather provides a view of important trends and cyberthreats observed at the strategic level.

Social engineering

Social engineering covers a wide range of activities aimed at exploiting human behavior or mistakes to gain access to data or services. It uses various forms of manipulation to trick victims into making a mistake or giving away confidential information. Users may be encouraged to open documents, files, or emails, click on links, fill out an online form, or provide access to systems or services. Social engineering is a convenient attack method because of its simplicity, low cost and an ease of use.

> Phishing, which means distribution of emails aimed at stealing important information such as passwords or credit card numbers, is the main method of initial compromise. During 2023 it was used by almost all hacker groups[10].

Depending on an audience and motivation of a hacker group, different topics and lures were used. These include password or account expiry, fake documents from state angencies, law enforcement agencies, payment documents, etc.

A particular topic of phishing messages is an offer of cooperation from the Russian special services. As a rule, such messages are sent via messengers and contain a link to a channel in the Telegram messenger for communication and further instructions.

To bypass security measures, they use password-protected archives with a password in an email body, ISO files, LNK files, scripts and documents with macros as well as links of legal cloud

[10] Microsoft Digital Defense Report. Building and improving cyber resilience. October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

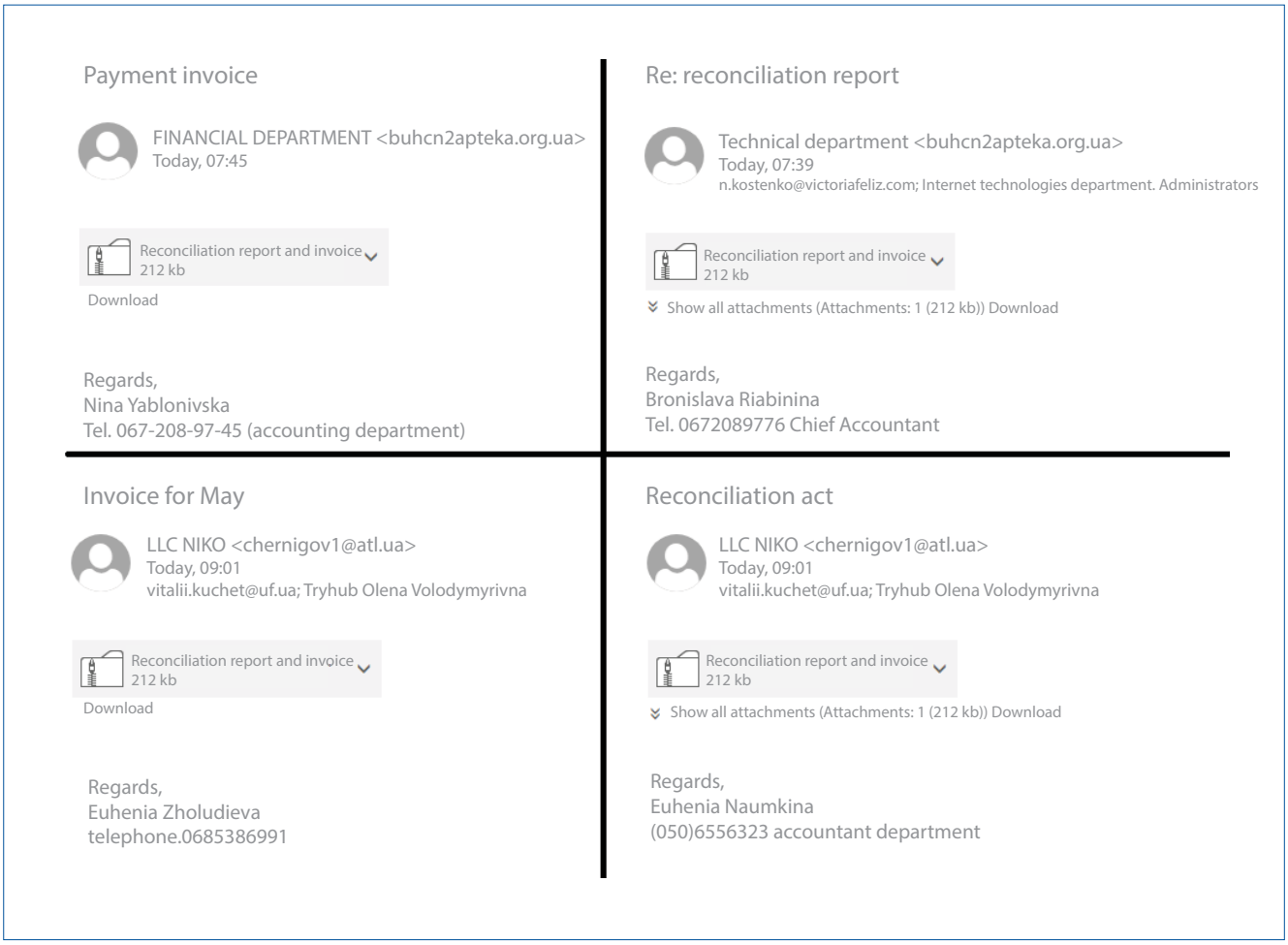


Figure No.2. *Sample phishing email from group UAC-0006 with the SmokeLoader malicious attachment*

services. Despite Microsoft disabling macros by default in 2022, many organizations use non-updated version of operating systems and MS Office, which supports the use of built-in macros by attackers.

To increase a level of trust in phishing emails, they are sent from compromised email accounts of state agencies or well-known enterprises. Sector-specific mailings are recorded. In such targeted phishing, emails within a sector are sent from compromised email addresses of organizations in that sector. For state agencies, compromised accounts of state agencies are used, for energy sector enterprises, a compromised email address of an energy sector enterprise is used, etc.

There has been a significant increase in the use of phishing emails via mobile communications, such as SMS and popular messengers. During the preparation of the report, it was identified that a relevance of this treat is even higher than that of traditional email phishing. Financially motivated agents are actively using a topic of receiving a parcel or a letter through delivery services, with messages containing links to phishing websites of delivery services. The main goal of hacker groups affiliated with Russian special services is to gain access to accounts registered on mobile phones, including messaging platforms, to access command chats and situational awareness system of the Ukrainian Defense Forces.

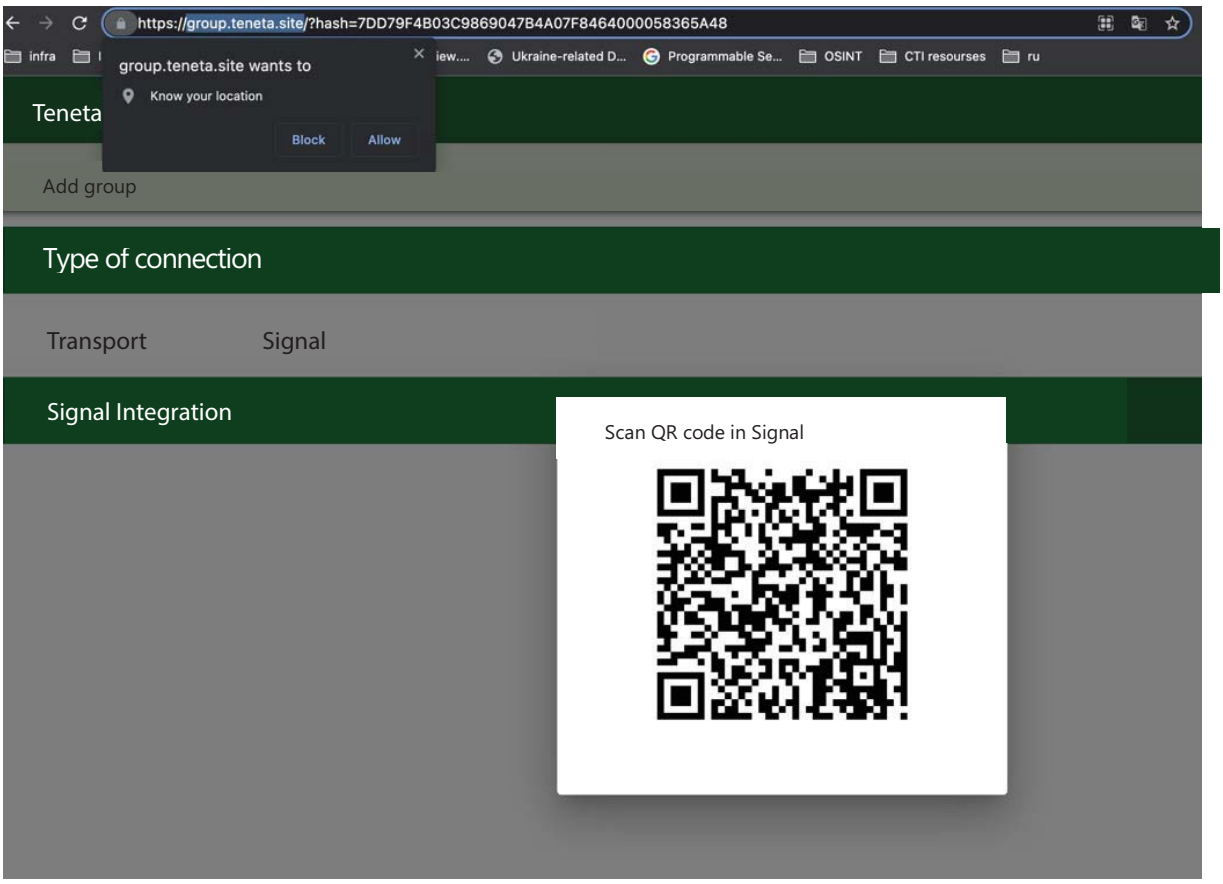


Figure No.3. *Sending phishing links via SMS and Signal to steal military personnel's Signal sessions*

Malicious software

Malicious software (malware) – is a general term that describes any software product or firmware that is designed to perform unauthorized processes in a system, which will result in a breach of an integrity, confidentiality or availability of information. One of the options for spreading malware is the Malware-as-a-Service (Malware-as-a-Service) model, which allows attackers not to develop code but to focus on executing attacks, gaining unauthorized access to systems and achieving attack targets after compromise.

The usage of malware increased significantly, almost doubling in the second half of 2023. The most active attempts to spread malware were recorded for SmokeLoader, AgentTesla, Snake Keylogger, Remcos, Formbook, RMS Rat.

DDoS attack

DDoS attack is a type of a cyber-attack aimed at disrupting availability, in which an attacker tries to disrupt an operation of a web recourse, a network or an online service by overloading them with a large number of fake or unwanted requests.

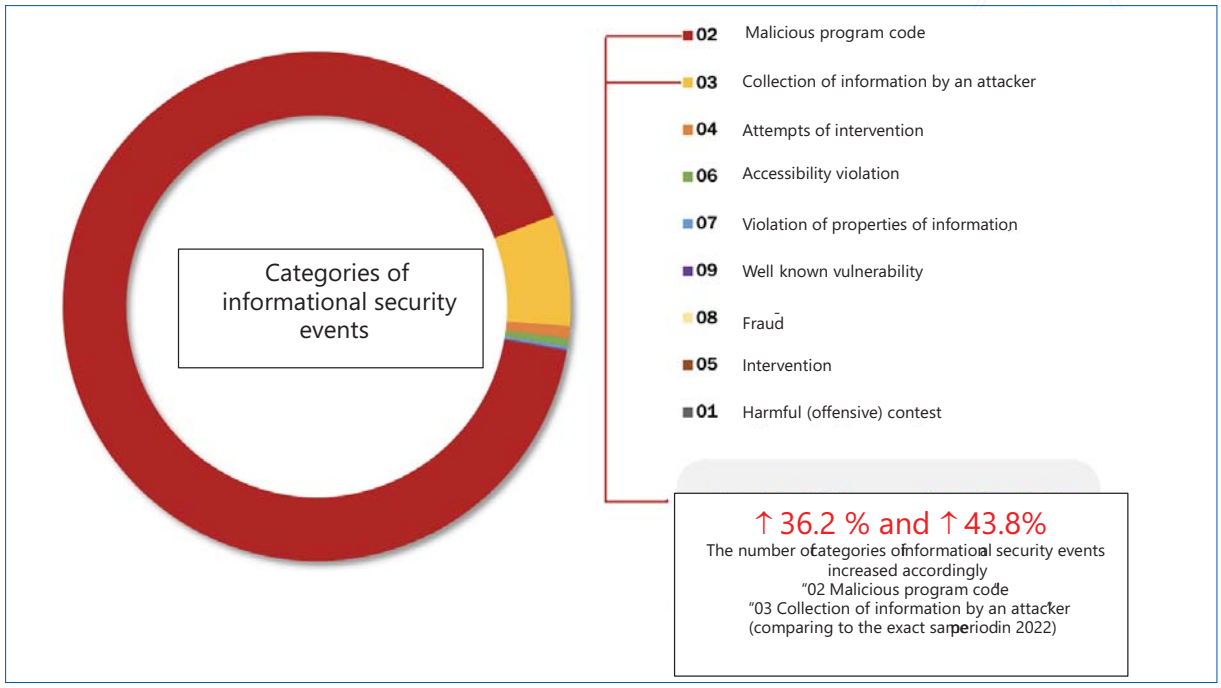


Figure No.4. *The usage of malicious program code* [11]

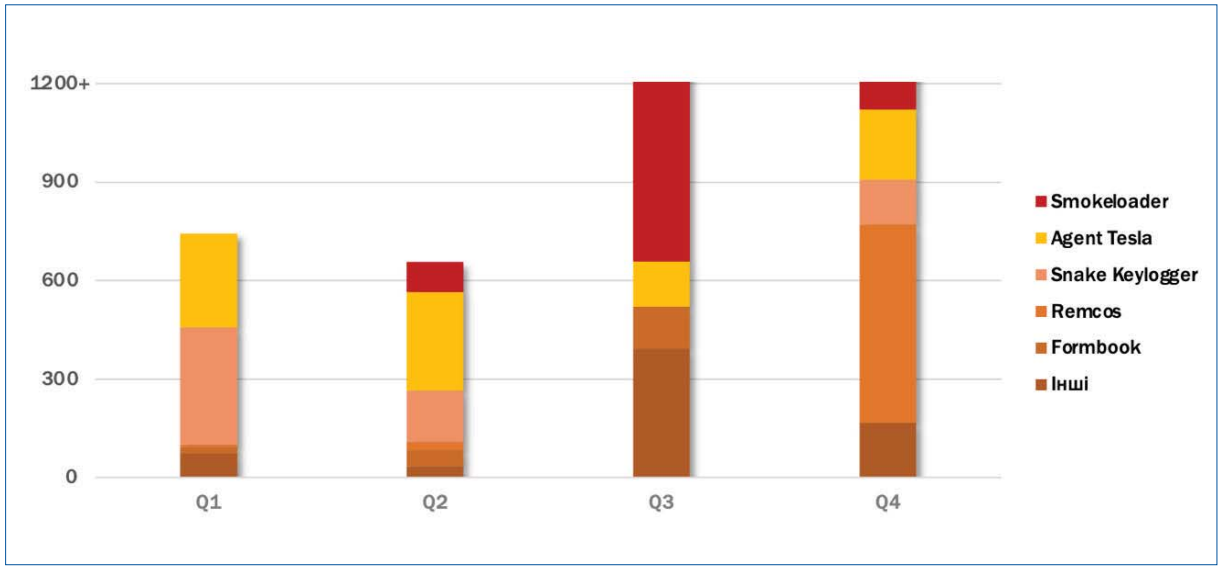


Figure No.5. *The main families of malware*[12]

Thousands of DDoS attacks on Ukrainian organizations[13] were recorded during the year; several such attacks are significantly influenced by activities of pseudo-hacktivist groups affiliated with Russian special services[14].

[11] Report on the operation of the system for detecting vulnerabilities and responding to cyber incidents and cyber-attacks 2023, https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

[12] Report on the operation of the system for detecting vulnerabilities and responding to cyber incidents and cyber-attacks 2023, https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

[13] 2023 in Review: DDoS Attacks Report by StormWall, https://stormwall.network/ddos-attack-report-2023

[14] Radware Global Threat Analysis Report, https://www.radware.com/threat-analysis-report/

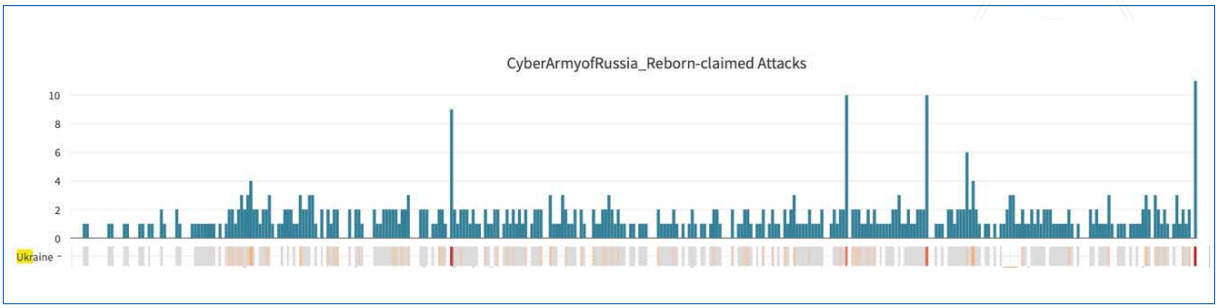


Figure No.6. *In 2023, the pseudo-hacktivist group CyberArmy of Russia Reborn reported 341 DDoS attacks on Ukraine*

In the period from late 2022 to early 2023, Russian special services took full control of all pro-Russian hacktivist groups, directing their activities to achieve Russia's military and political goals. Therefore, a significant number of DDoS attacks in 2023 targeted information recourses and networks of government agencies, mostly institutions that provide public services to citizens or ensure an operation of state registers. The tactics of pro-Russian pseudo-hacktivist groups include a publication of targeted organizations before these attacks and reports on unavailability during DDoS-attacks. The attacks usually last several hours.

DDoS-activity by pseudo-hacktivist groups do not have a significant impact on the operation of state information systems. On one hand, a reason for this is a low level of capabilities of most of these groups, on the other hand, many state agencies, thanks to the support of international partners, have been using DDoS attacks countermeasures from Cloudflare, Akamai and others since the beginning of Russia's full-scale invasion of Ukraine.

At the same time, attempts at sophisticated application-level DDoS attacks have been reordered, mainly in banking and service sectors.

Online fraud

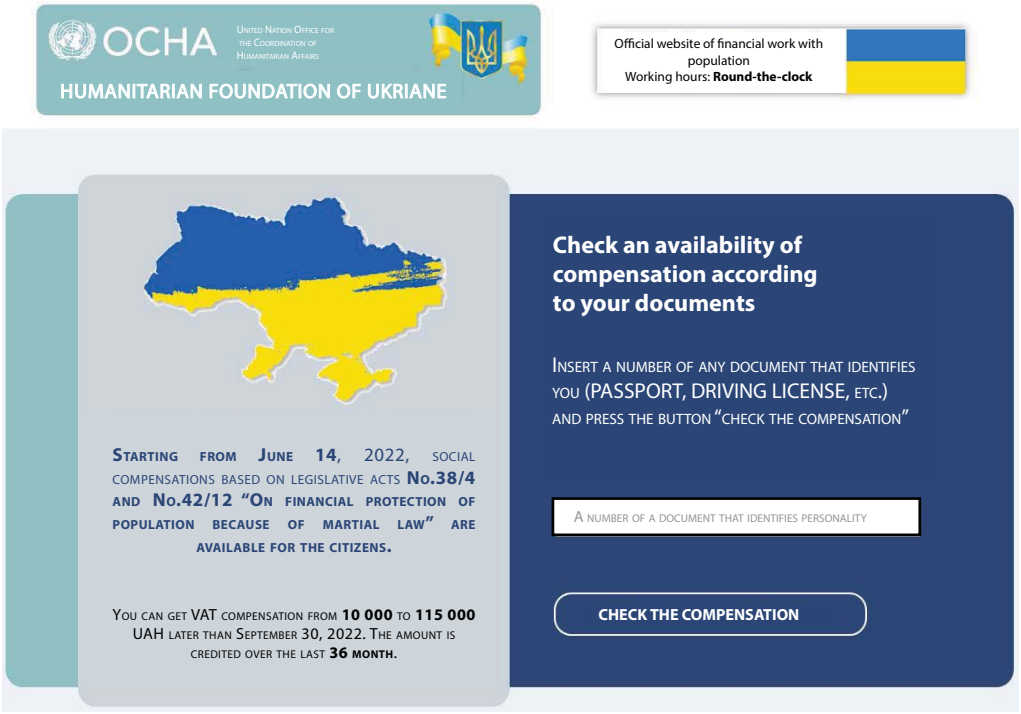
Since mid-2022, there has been a rapid increase in online fraud against Ukrainian citizens, which exploited themes of an assistance from the state and international organizations such as the UN, Red Cross, UNICEF, NATO, etc. A typical scheme involved filling out a form with personal data and a bank card number to likely receive a payment.

Phishing sites imitating official resources of state agencies and volunteer organizations are also actively used to collect donations.

Russian state-supported groups use the similar approach to collect personal data from military personnel and their families. Their phishing sites, which imitate assistance to internally displaced persons, contain detailed forms for collecting personal data, including photos in military uniform, allegedly to confirm service in the Ukrainian Defense Forces.

[13] 2023 in Review: DDoS Attacks Report by StormWall, https://stormwall.network/ddos-attack-report-2023

[14] Radware Global Threat Analysis Report, https://www.radware.com/threat-analysis-report/



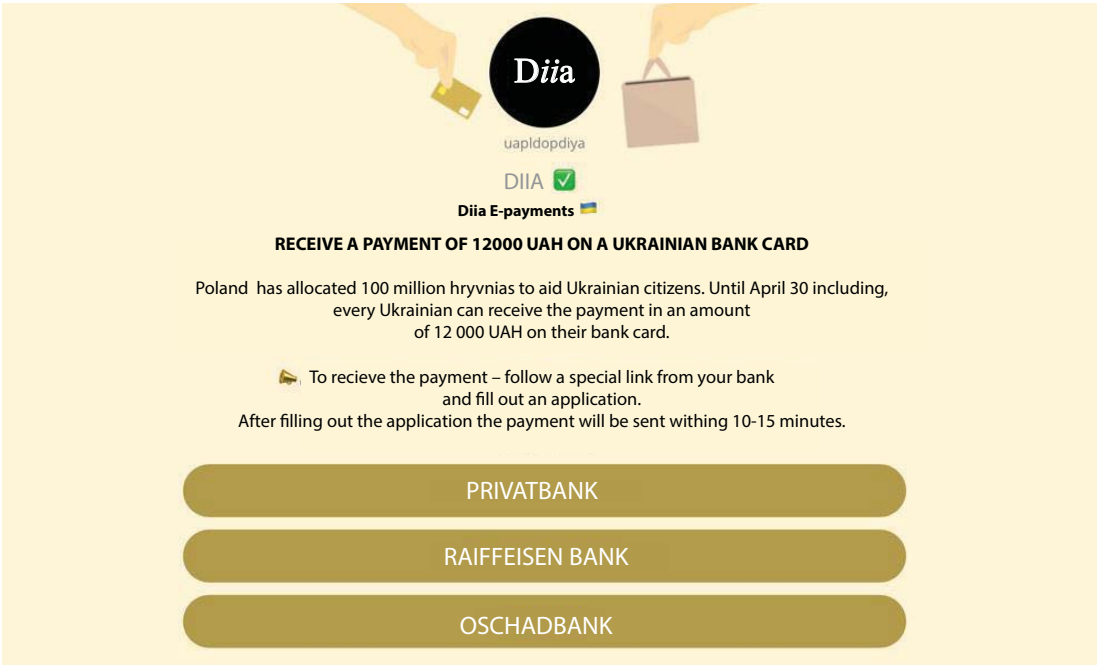


Figure No.7. *Fraudulent schemes that exploit topics of payments and compensation to Ukrainian citizens*[15]

Cybercriminals quickly change topics and create new fraudulent resources. On average, a phishing site is used for several hours to a day, after which its owners move it to a new domain.

The tactics of creating phishing domains in national zones of partner countries, where many

[15] https://csirt.bank.gov.ua/cyber-fraud

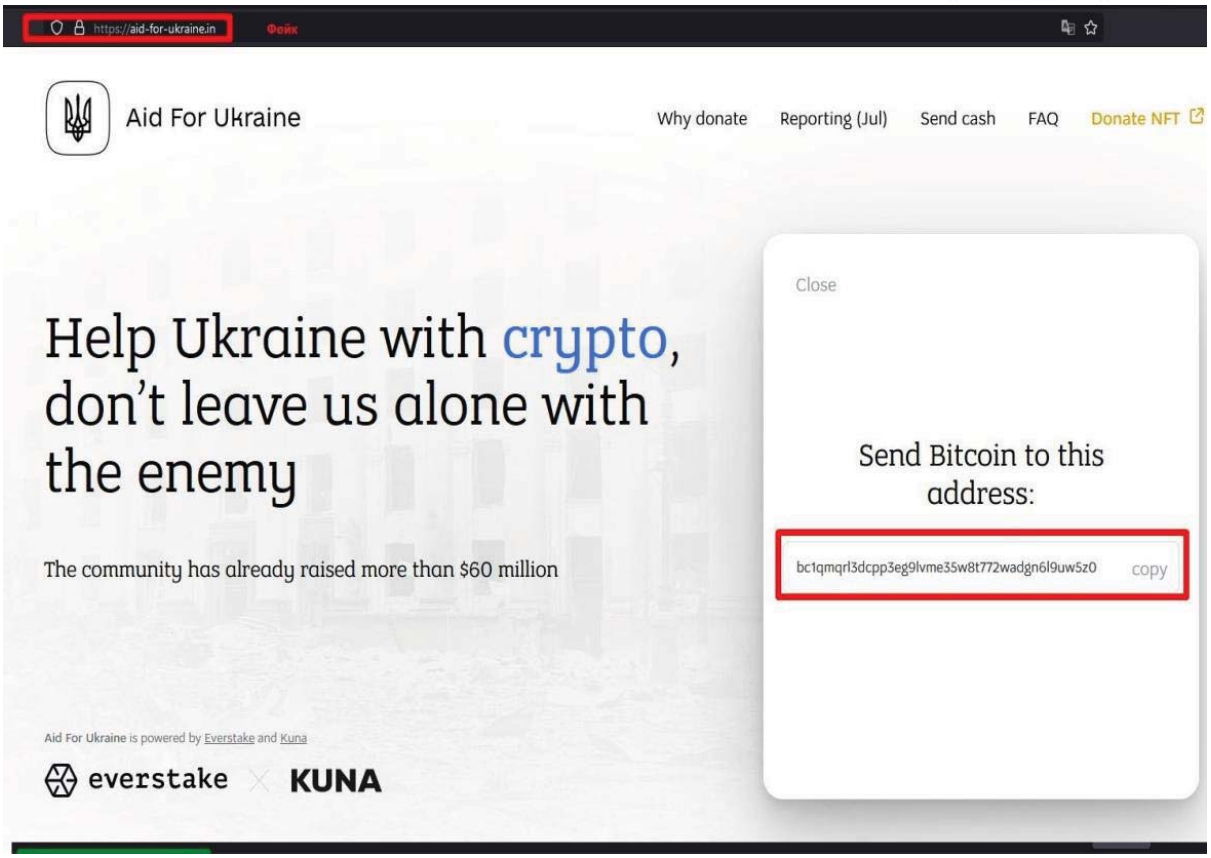


Figure No.8. *Fake donation collection site imitating an official website of the Ministry of Digital Transformation*

Ukrainian citizens live, and limiting (geo-filtering) requests from Ukraine to avoid detection of such domains were recorded.

In the fourth quarter of 2023, the most active fraudulent phishing campaigns were aimed at phishing schemes involving Ukrposhta, Nova Post, DHL, and other delivery services. Such phishing campaigns are often distributed via SMS and popular messengers.

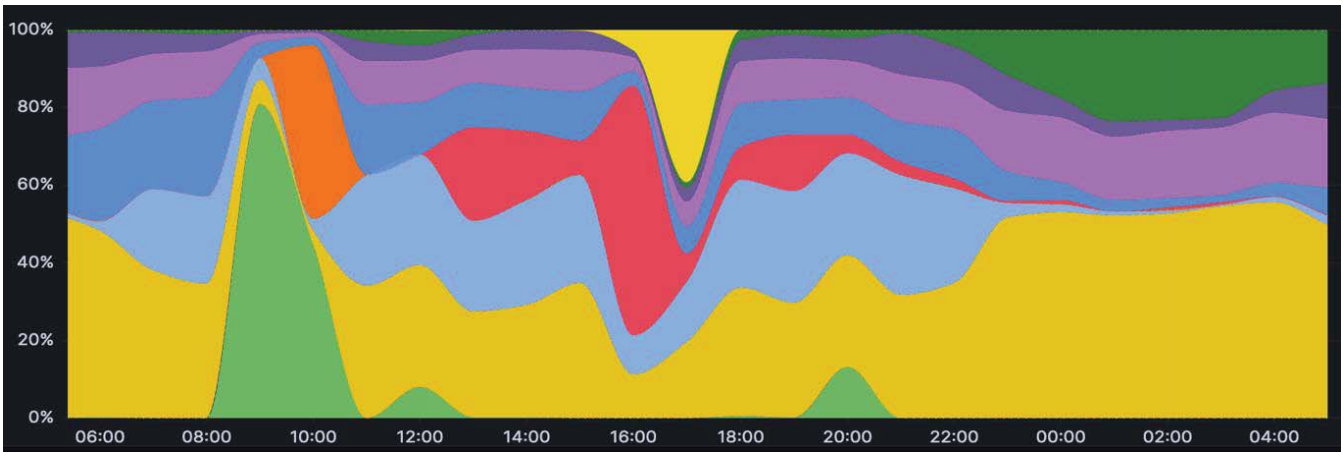


Figure No.9. *The lifespan of phishing domains can be several hours. The NCCC data*

Google, Facebook, Telegram are the main channels of advertising and distribution of phishing links, as well as the usage of Tiktok has also been recorded.

Based on the results of the analysis of registration and hosting data, it was found that in 2023, more than 80-90% of phishing domains use Cloudflare services to hide real IP addresses and counteract automated phishing detection and blocking algorithms.

Usage of cyber-attacks to support information and hybrid operations

Russian state-supported groups use cyber-attacks to facilitate information and hybrid operations.

Defacement of government websites and compromise of media information systems are used to spread disinformation and propaganda.

On February 23, 2023, Russians conducted a large-scale cyber-attack on state agencies, like the BleedingBear operation on January 13, 2022, during which they attempted to destroy information, deface official websites of state agencies, volunteer organizations and media. At the same time, Inter TV channel was compromised, which led to a substitution of the broadcast during an interview with the Secretary of the National Security and Defense Council of Ukraine (the USSR anthem began to play).

A tactic of pro-Russian pseudo-hacktivist groups is to publish messages about their plans to conduct DDoS attacks and results achieved on their own websites and in the Telegram network.

Part of the network of Telegram channels controlled by Russian special services regularly publishes personnel data of military personnel, various databases and accesses obtained because of cyber-attacks on Ukrainian organizations.

Although most of the published data on "successful cyber-attacks" are not confirmed, it takes time to verify such information and creates an impression of high level of capability of such groups.

Account compromising and information leaks

A trend in 2023 is a usage of valid user accounts to gain initial access to organizations' networks. Information leaks, the OSINT data and data stolen from previous cyber-attacks are carefully analyzed and used in subsequent targeted cyber-attacks.

In many cases, attackers target user accounts and authentication data for online services. Several attacks such as password mining, password spraying, and Adversary-in-the-Middle (Adversary-in-the-Middle) attacks have increased significantly. Malware that collects passwords from browsers, authorization tokens from compromised hosts and phishing resources are used to steal accounts.

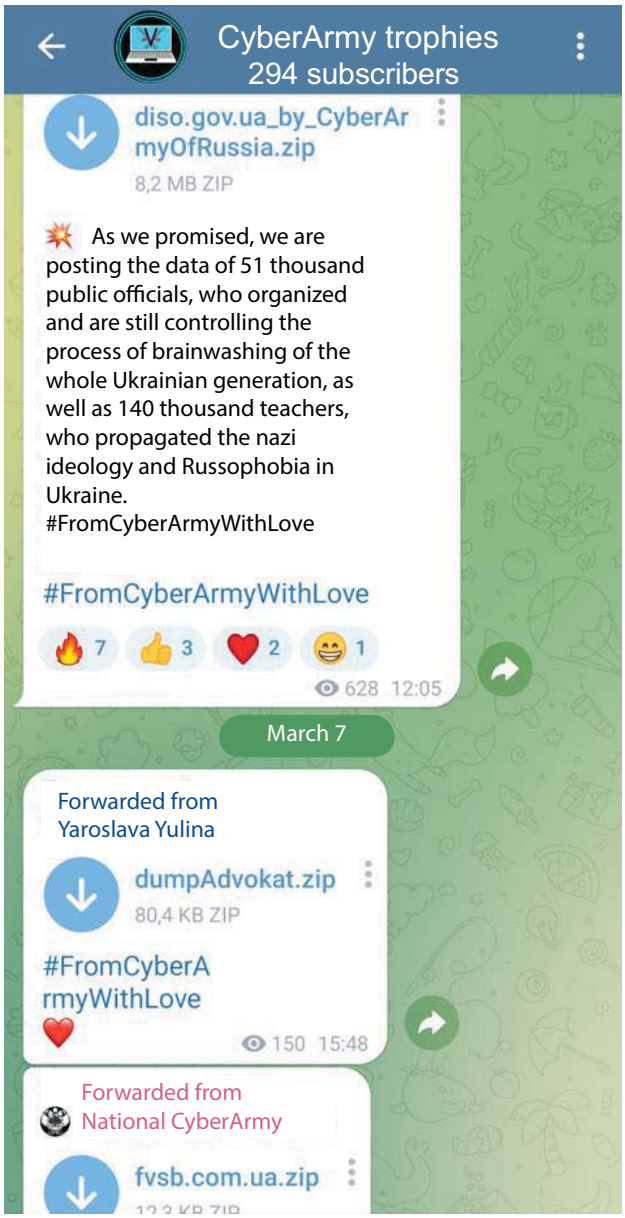


Figure No.10. *Screenshot from the "Cyber Army Trophies" Telegram channel*

Disruption of availability due to equipment or network failures or damage

As a result of Russian aggression on Ukraine, 25% of fixed networks were damaged and 4.3 thousand mobile base stations were destroyed or damaged[16].

Under conditions of war, Ukrainian organizations are threatened not only by hostile actions in cyberspace, but also by disruption in availability due to equipment or network failures or damage. Power outages or damage to communication lines can result in an unavailability of information or services.

[16] "25% of fixed-line networks and 4,000 mobile towers were damaged," Fedorov said, https://mbiz.censor.net/news/3489565/v_ukrayini_poshkodjeno_25_merej_fiksovanogo_zvyazku_ta_4_tysyachi_vyshok

Most organizations with important business processes have ensured backup of data, energy and communication channels, including using cloud technologies, but the experts identify this threat as relevant.

Destructive attacks

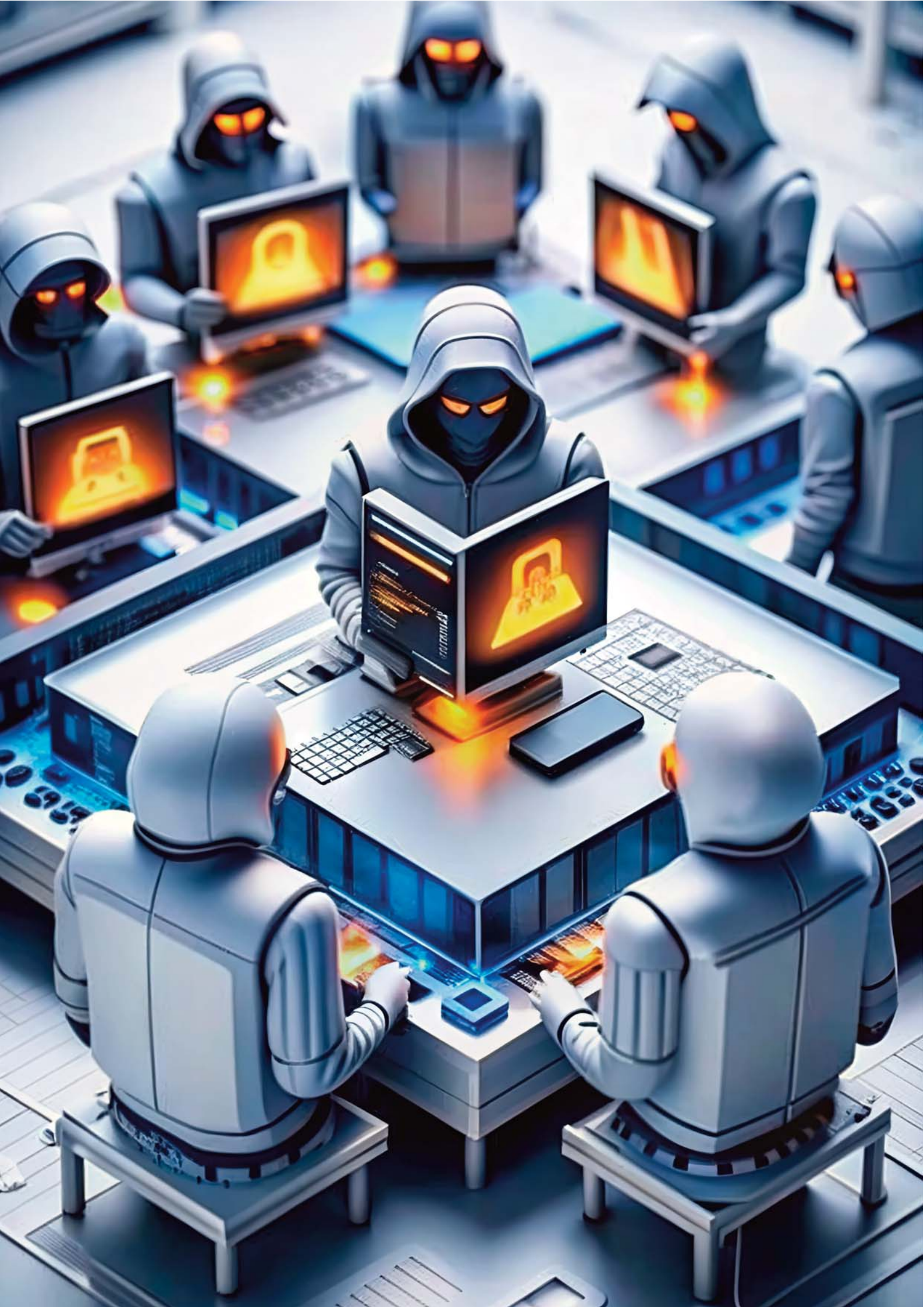
In 2023, several destructive cyber-attacks decreased significantly.

In the reporting period, destructive attacks were aimed at destroying data and damaging network infrastructure.

Modified versions of Sdelete utility were used to destroy data on individual hosts. To distribute it, ActiveDirectory tools were used, if available / compromised, or tools such as Impacket.

Tactics for gaining access to a management console of virtual machine management systems and mass deleting virtual machines and/or virtual disk storages have been detected.

In the electronic communications sector, attackers also use a tactic of damaging or deleting network equipment configurations, which leads to termination of network functioning. On December 12, 2023, such a destructive attack on Kyivstar was recorded, which resulted in the temporary unavailability of communication for millions of Ukrainian citizens.



THE MOST ACTIVE HACKER GROUPS

A table below shows hacker groups that were the most active in Ukraine in 2023.

Group	Belongs to	Main objectives	Capabilities
APT28	Military Unit 26165 Main Intelligence Agency, Russia	Military organizations, energy infrastructure, state agencies, diplomatic agencies	Oceanmap, Masepie, Steelhook, Impacket, Headlace, CVE-2023-23397, CVE-2023-38831
APT29	Foreign Intelligence Service, Russia	Military organizations, diplomatic institutions	Envyscout, Halfrig, Quarterrig, Snowyamber, Cobalt Strike, Brute Ratel, CVE-2023-38831
Sandworm	Military Unit 74455 Main Intelligence Agency, Russia	Telecommunications providers, critical infrastructure	BIASBOAT, QueueSeed, LOADGRIP, AcidRain, AcidPour, Poemgate, Poseidon, Whitecat
Turla	Military Unit 71330 Federal Security Service, Russia	Military Organizations	Kazuar
Callisto	Military Unit 64829 Federal Security Service, Russia	Military organizations, diplomatic institutions	Spear-phishing, Evilginx
Gamaredon	Federal Security Service Office in Crimea	Military organizations, law enforcement agencies, state and diplomatic institutions	LoadShort, GammaLoad, GammaDrop, HockSeat, LakeFlash,
WinterVivern	Activity in the interests of Russia and Belarus	Military organizations, state institutions	CVE-2023-5631, CVE-2022-27926,
Ghostwriter	Military, Belarus	State institutions	CVE-2023-38831, PicassoLoader, Cobalt Strike
DaVinci Group (UAC-0050)	Law Enforcement Agencies, Russia	Enterprises and organizations of private and state sectors	LummaStealer, RemoteUtilities, Remcos, Quasar, Venom
Smokeloader Group (UAC-0006)	Financially motivated criminals, Russia	Enterprises and organizations of private and state sectors	Smokeloader, Taleshot, RDPWrapper, Hangthread
NoName057 (16)	Pseudo-hacktivists, Federal Security Service, Russia	Enterprises and organizations of private and state sectors	DDoSia
CyberArmyof Russia	Pseudo-hacktivists, Federal Security Service, Russia	Enterprises and organizations of private and state sectors	Killweb, CA_DDoS

EVALUATION OF THE IMPACT OF CYBERTHREATS

Most Ukrainian organizations do not evaluate the scale of damage and consequences of cyber-attacks, limiting themselves to post-incident recovery measures or do not make such information publicly available.

The result of the survey of public and private sector experts and qualitative analysis, which is somewhat subjective, were used to evaluate an overall impact of cyber-attacks. For the purpose of this report, the following types of consequences of cyber incidents were selected:

- ☑ Digital consequences related to system unavailability, data corruption or information leaks.
- ☑ Economic consequences related to direct and indirect financial losses.
- ☑ Social consequences related to the loss of trust because of disruption of important public services or leaks of personal data.
- ☑ Reputational consequences related to a possible negative public perception of an organization that has been a victim of a cyberthreat.
- ☑ Physical consequences related to an injury or a harm of citizens.

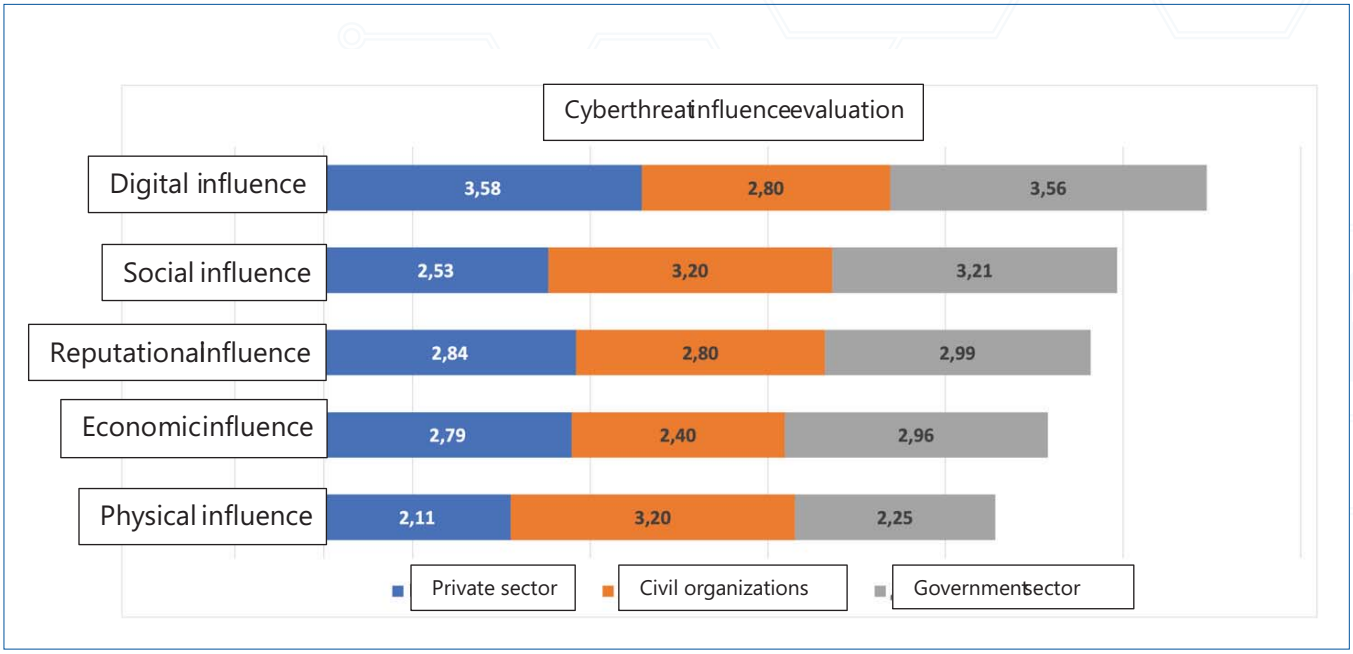


Figure No.11. *Evaluation of consequences of cyberthreats*

The greatest consequences of cyber-attacks in 2023 are digital and social consequences, economic and reputational losses are considered less important, and physical consequences are not considered significant.

VULNERABILITIES

According to the data of the "Report on a work of the system of detecting vulnerabilities and responding to cyber incidents and cyber-attacks in 2023" of the Cyber Incident Response Operations Center of the State Service of Special Communications and Information Protection of Ukraine, the most frequently recorded attempts to exploit vulnerabilities were CVE-2022-20776, CVE-2021-26084, CVE-2021-40438, CVE-2022-31699, CVE-2023-45802, CVE-2022-25762, CVE-2022-20920, CVE-2021-34699, CVE-2021-21974, CVE-2023-34048. At the same time, not all of these vulnerabilities have been identified in products distributed in Ukraine.

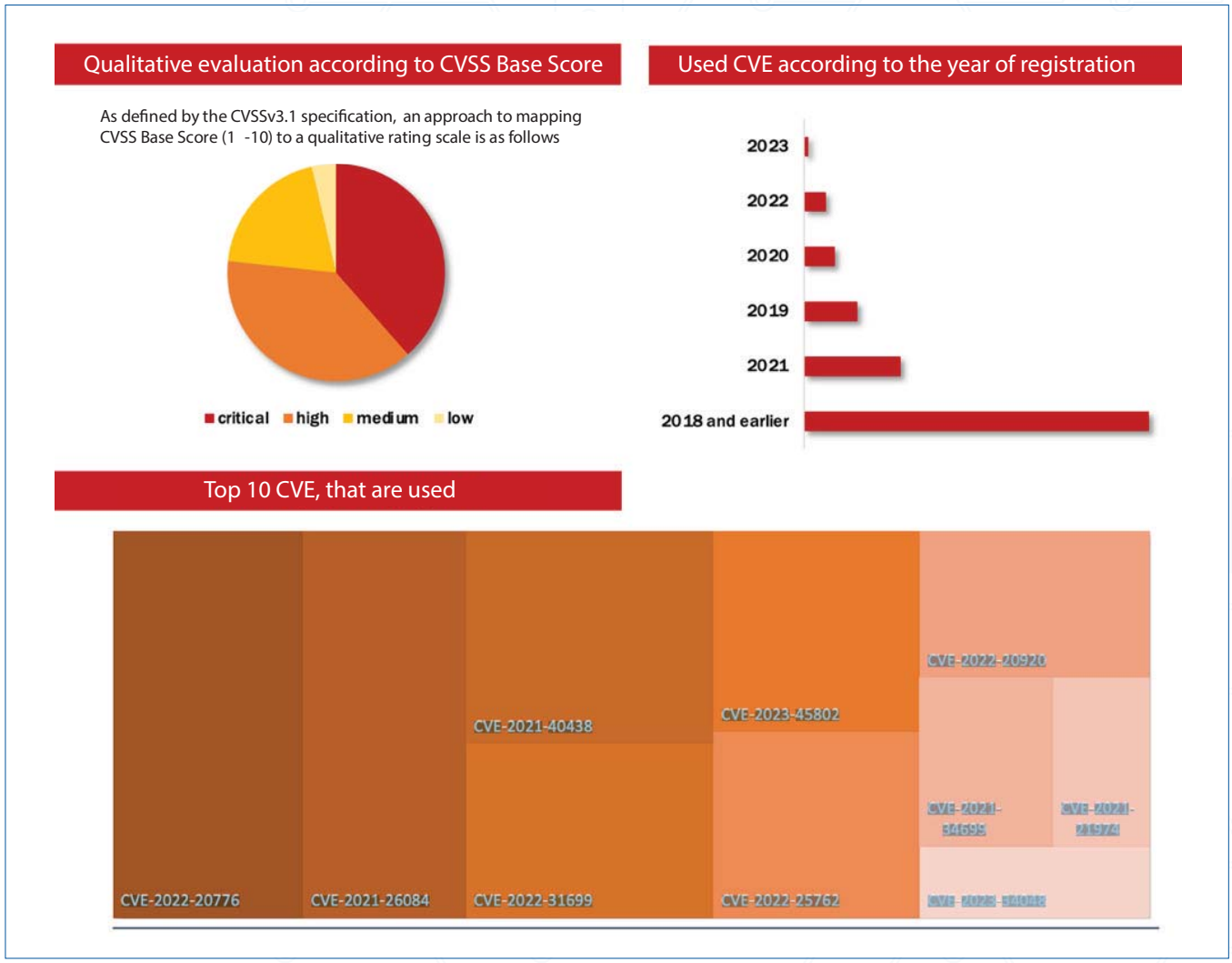


Figure No.12. *Main vulnerabilities*

The Government Response Team CERT-UA has published several reports containing information about vulnerabilities used in attacks on Ukrainian infrastructure, namely vulnerabilities in Zabbix (CVE-2022-23131, CVE-2022-23134), WinRAR (CVE-2023-38831), Roundcube (CVE-2020-35730, CVE-2021-44026, CVE-2020-12641).

According to the survey, experts identified additional vulnerabilities that were exploited in 2023: Zimbra Collaboration Suite (CVE-2018-6882), Fortinet FortiGate SSL-VPN (CVE-2023-27997), Fortinet FortiOS (CVE-2018-13379), Microsoft Outlook (CVE-2023-23397), Apache Log4j (CVE-2021-44228).

APPENDIX. INFORMATION ABOUT AN ADAPTED VERSION OF THE ENISA METHODOLOGY

The ENISA methodology "ENISA Cybersecurity Threat Landscape Methodology, July 2022" (ENISA Cybersecurity Threat Landscape Methodology, July 2022) was used to conduct the study of the cyberthreat landscape in Ukraine and prepare the report. Based on a strategic nature of the NCCC's activities, the methodology was adapted using the following principles.

The overall process of creating the cyberthreat landscape report in accordance with the methodology is shown in Figure below.

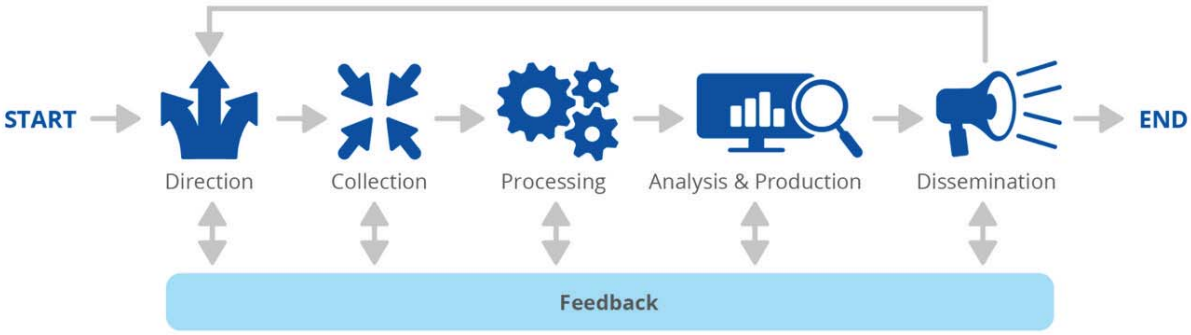


Figure No.13. *Overall process for creating the cyberthreat landscape report*

It consists of five main stages: defining a scope, collecting data, processing data, analyzing data, and preparing and distributing the report.

Determining the main direction

A purpose of this stage is to determine objectives, an audience and a scope of study. Based on the results of consultations with the NCCC and considering ENISA recommendations, the following objectives were identified:

- ☑ strategic decision-making;
- ☑ risk management;
- ☑ prioritizing recommendations for cybersecurity policies;
- ☑ identifying areas for training and capabilities development;
- ☑ distribution of information useful for cybersecurity.

The audience of the report are specialists and managers, who operate at strategic and partially tactical levels:

- ☑ representatives of the NCCC member organizations involved in a development of the cybersecurity strategy;
- ☑ cybersecurity managers of the state agencies and critical infrastructure facilities;
- ☑ heads of private enterprises;
- ☑ representatives of international organizations and national cybersecurity agencies and institutions.

Considering the strategic nature of the report, its structure includes a section "Key Trends and Conclusions" that allows the targeted audience to quickly familiarize themselves with the main results of the study.

Since the study was conducted in the interests of the NCCC, and the main stakeholders were the employes of the National Security and Defense Council of Ukraine Secretariat, who provided information on priorities, general guidance and feedback.

The field of the study includes answering the following questions: the most attacked sectors, main trend, types of cyberthreats, vulnerabilities, agents and evaluation of the impact of cyberthreats. The report provides information on the period from January 1, 2023, to December 31, 2023. The report was prepared using an externally focused approach.

Data collection

At the stage of data collection, information from open sources was used, including publications of cyberthreat analysts from leading cybersecurity companies, data on cyber incidents and cyber-attacks from social networks, own resources, information from MISP and OpenCTI compromise indicator exchange and cyberthreat analytics, as well as the NCCC materials, interviews with Ukrainian cybersecurity experts and surveys of representatives of the state agencies, critical infrastructure facilities, public and private sectors by questionaries.

There is no mechanism for mandatory reporting of cyber incidents and cyber-attacks in Ukraine. Mechanisms and procedures for sharing information about cyber incidents are partially regulated in various bylaws and are voluntary for the state agencies (according to practices), critical infrastructure facilities and private sector enterprises. In addition, in many cases the main goal of organizations when responding to incidents is to eliminate their consequences without establishing exact causes and methods of interference with their information systems, as well as a scale of the incident's impact.

A taxonomy of cyber incidents adopted in Ukraine, approved by the National Coordination Center for Cybersecurity in 2021[17], is used mainly by the state agencies. It was developed using the ENISA recommendations of January 2018 (ENISA Reference Incident Classification Taxonomy[18]), as well as a joint document of ENISA and the European Cybercrime Centre Europol (Common

[17] The list of cyber incidents, https://cert.gov.ua/recommendation/16904

[18] Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Taxonomy for Law Enforcement and The National Network of CSIRTs[19]) and is focused primarily on information exchange at the level of CEFT/CSIRT response teams, i.e. technical/tactical information exchange,

In Ukraine, there is no nationally agreed naming system for hacker groups (agents). Most often, the taxonomy of the CERT-UA Government Response Team (UAC-xxxx) is used for attribution of names of hacker groups proposed by Microsoft, Mandiant, ESET, Recorded Future and other companies are used.

These factors make it difficult to compare information from different sources and limit possibilities of quantitative analysis.

For the analysis, information was collected from the website of the CERT-UA Government Team (37 publications in 2023); (semi-)annual reports of the CERT-UA and the State Cyber Protection Center; depersonalized data on cyber incidents provided by a number of Ukrainian Cybersecurity companies (27 reports); publications from the websites of Cisco Talos, Cloudflare, Crowdstrike, Darktrace, ESET, Fortinet, Google TAG, Mandiant, Microsoft, PaloAlto, Radware, Recorded Future, Sophos, StormWall, etc. (143 publications); the OSINT data, materials from news sites and social networks containing information and statements of organizations about the attack on them. The NCCC received data on 241 events from the MISP systems, and 103,701 reports on cyber-attacks and cyber incidents were received from its own STI system. The NCCC also received 50 weekly information reports on a situation in cyberspace.

As the study was conducted for the first time over a relatively short period of time, the data for the report was collected for a limited period. Subsequently, in accordance with the ENISA methodology, the data will be collected on an ongoing basis, according to the following plan.

Source of data	Type of data	Time of data collection
Main entities	Tactical, strategic	Within a year, annual and semiannual reports
Publications by Cybersecurity companies and STI providers	Operational, tactical	Within a year
Social networks	Operational, tactical	Within a year
Cybersecurity news	Operational, tactical, strategic	Within a year
Vulnerability data	Operational, tactical	Within a year
Science materials	Tactical, strategic	Within a year
The OSINT data	Operational, tactical	Within a year
Data from technical exchange systems	Operational, tactical	Within a year
Situational awareness reports from partners	Operational, tactical, strategic	On a periodic basis, within a year

[19] Common Taxonomy for Law Enforcement and CSIRTs, https://www.europol.europa.eu/publications-events/publications/common-taxonomy-for-law-enforcement-and-csirts

In accordance with the methodology, different sources were assigned appropriate levels of confidence: low, medium and high. The high level of confidence is given to information from key entities, the medium level to data from internal technical exchange systems and the internal OSINT and research data and the low level to external sources and survey data.

With assistance of the NCCC, the survey was conducted among representatives of the state agencies, the private sector (cybersecurity companies and critical infrastructure facilities) and the public sector. The total of 398 respondents answered the questionnaire: 373 from the public sector, 19 from the private sector, 5 from the civil society sector and 1 respondent indicated as the "other" (the Armed Forces of Ukraine).

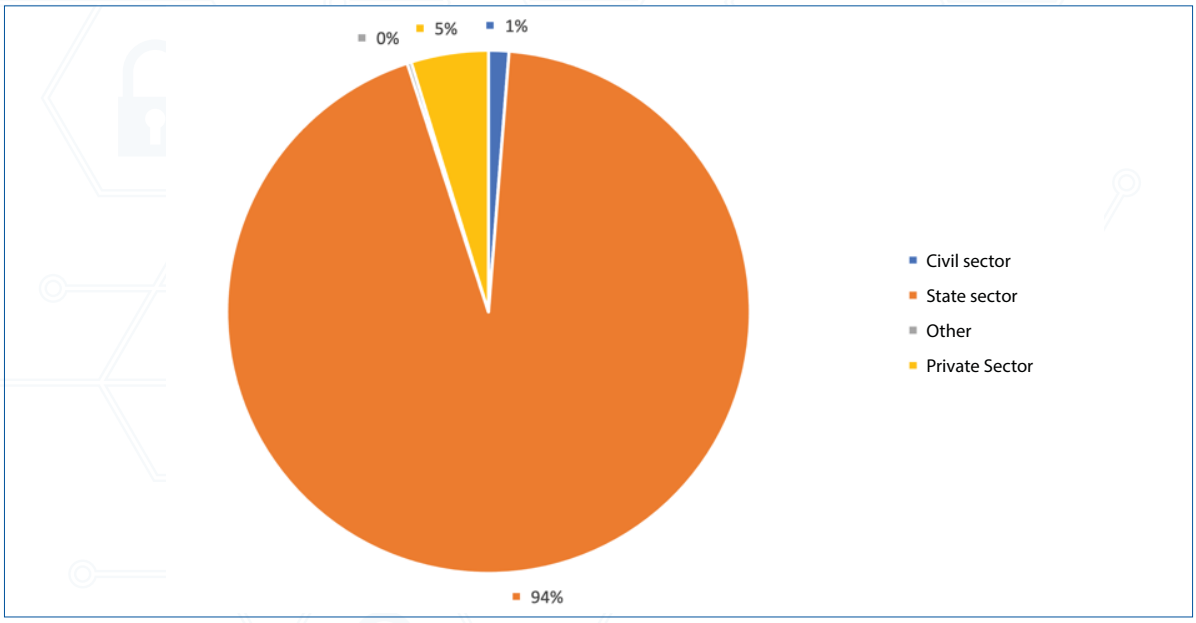


Figure No.14. *Respondents' structure*

The questionnaire contained 13 questions grouped by topic: information about a respondent (1 question); current threats (2 questions); sources, goals and consequences of cyber-attacks (4 questions); tools (3 questions); respondent's evaluation (3 questions).

In order to identify the most relevant threats, the questionnaire contained a question "What threats were the most relevant to Ukrainian organizations and citizens in 2023?" with options to choose from the list of threats identified in the ENISA Threat Landscape 2023 report (ENISA Threat Landscape 2023[20]) and an ability to determine a degree of their relevance on a scale from 1 (less relevant) to 5 (more relevant). It is worth noting that even though phishing on mobile devices is an element of social engineering, this threat was singled out due to a large number of incidents related to this type of threat.

The most common threats identified by respondents were malware, phishing on mobile devices, and DDoS-attacks. Representatives of different sectors have a very similar perception of threats, but there are differences.

[20] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

For the private sector representatives, malware represents less threat (only the 5th place), while for the state sector representatives this threat is tied for the 1st place with phishing on mobile devices. On the other hand, business respondents rate the threat from DDoS-attacks, destructive attacks and information leaks 5-15 percentage points higher than the government, which is likely due to stricter requirements for process continuity and reputational risks. Interestingly, all respondents noted a high level of threat from cyber-attacks aimed at supporting information and hybrid operations, although the private sector perceived this threat to be higher than other sectors.

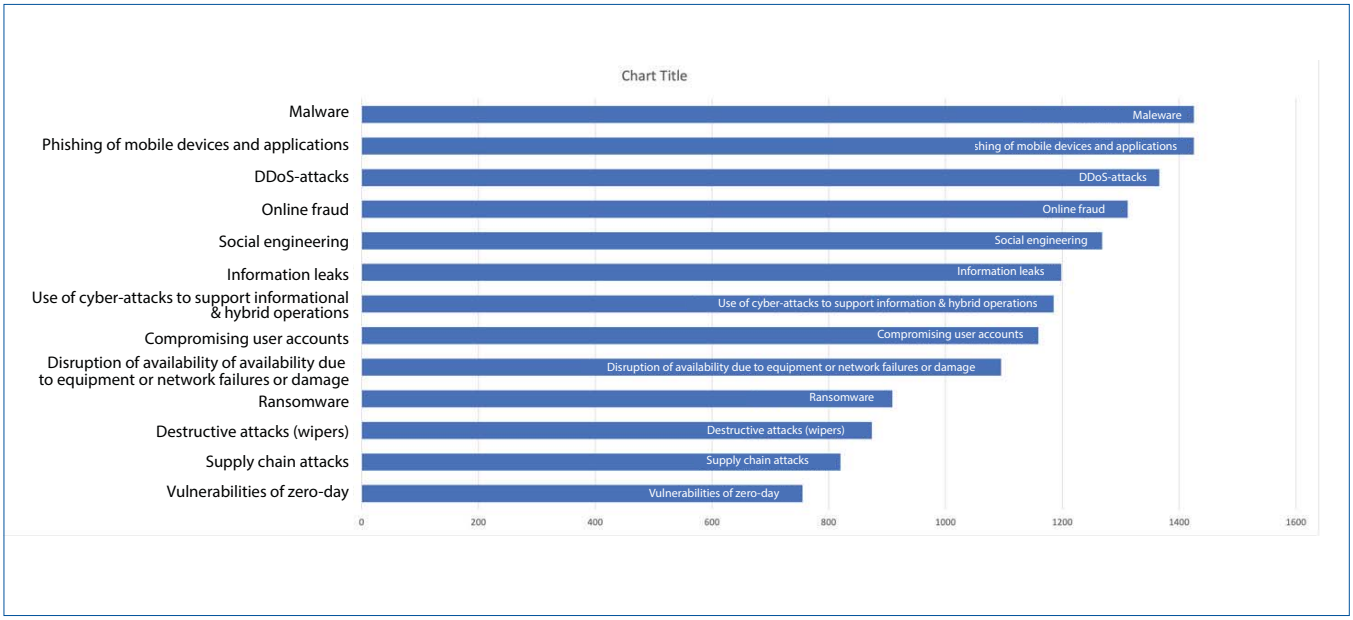


Figure No.15. *Actual threats*

Based on the survey results and collected data on cyber-attacks and cyber incidents, the following major threats were selected for consideration in this report: social engineering, malware, DDoS-attacks, online fraud, use of cyber-attacks to support information and hybrid operations, account compromise and information leaks, disruption of availability due to equipment or network failures or damage and destructive attacks.

The result of the answers to a question "Which sectors and categories of citizens were the most often targeted by cyber-attacks in 2023?" were used to analyze sectors that suffered the most attacks. The data obtained from the survey generally correlates with the information in the CERT-UA Government Team report. Interestingly, both the public and private sectors recognize that the state agencies are the most attacked. However, business believes that the next most attacked sectors are telecommunications, IT and banking, while the state sectors, security and defense energy sectors are considered to be more attacked.

Questions about motivation of attackers and consequences of their influence were used to evaluate the impact of cyber-attacks. Despite a relatively small number of destructive attacks, damage to the functioning of systems was ranked second in the answers to a question "What are the main goals and motivations of cyber-attacks on Ukrainian organization and citizens in 2023?". This indicates a higher level of subjective perception of threats from this type of cyber-attacks due

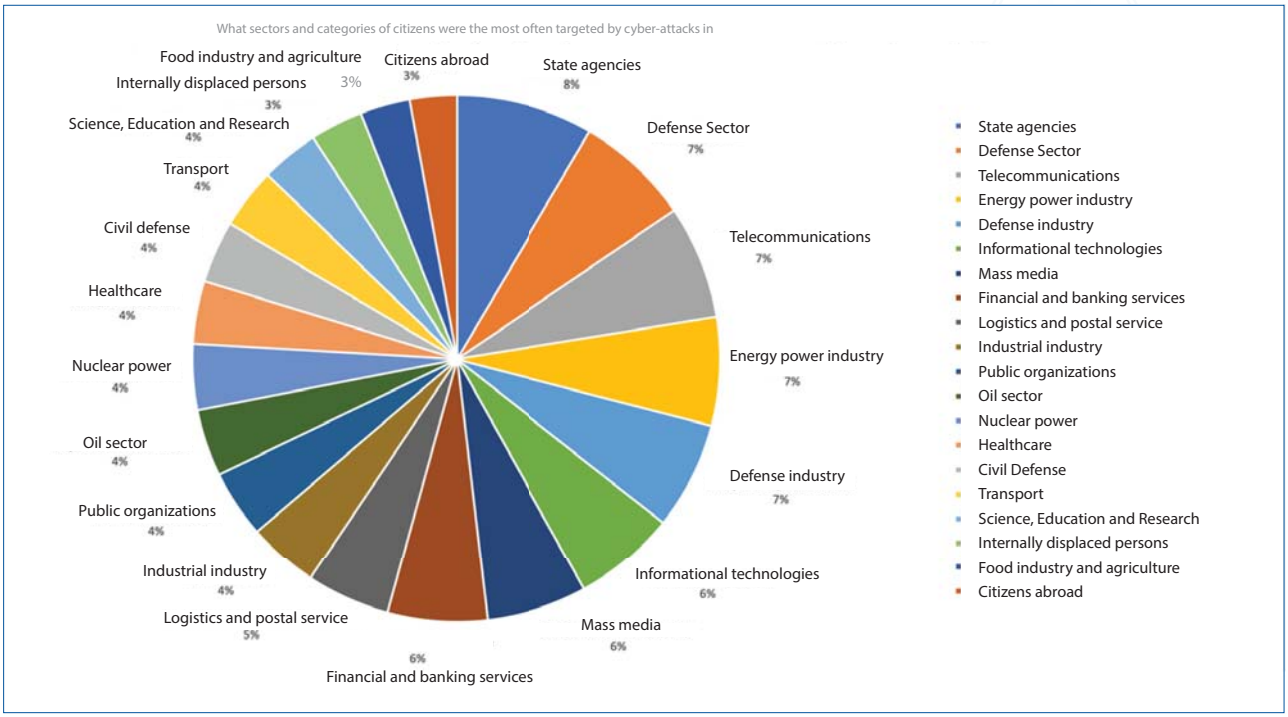


Figure No.16. *Attacked sectors and categories of citizens*

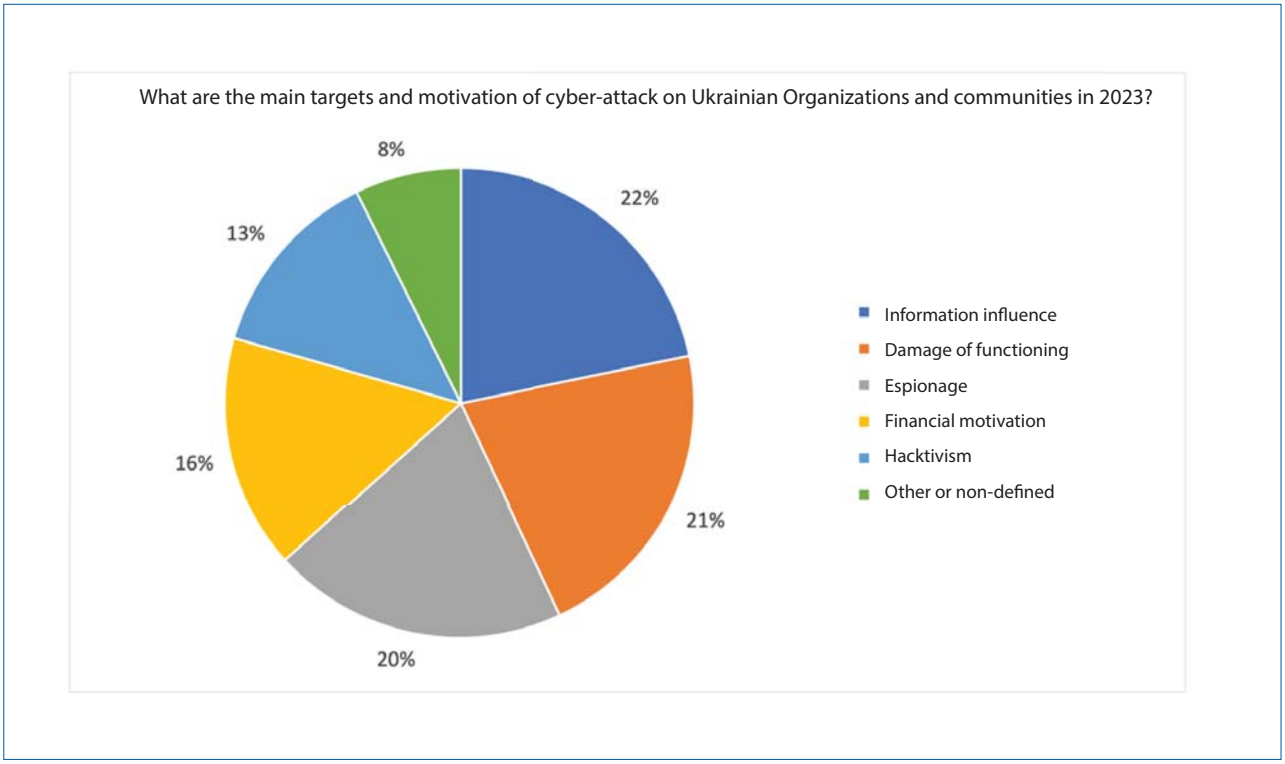


Figure No.17. *Motivation for cyber-attacks*

to a greater damage and their implementation, as well as wider awareness of such attacks due to publications in media.

Data processing and analysis

The data processing stage converts collected data into a format that can be used by cyberthreats analysis at the analysis and report formation stages. Since initial data comes in different formats (structured and unstructured), with different depths of details, levels of trust, etc., the main task of this stage is to eliminate duplicate information, bring data to common formats that can be processed, in the automated CTI systems.

During processing, the data was converted to a format that minimally describes data, a type of an incident, an attacked sector, an attribution, consequences, the level of trust, etc. Materials from international companies were translated into Ukrainian.

The ENISA methodology involves the usage of the following cyberthreat taxonomies: ENISA Threat Taxonomy[21], JRC Taxonomy[22], Cybersecurity Incident Taxonomy[23], ENISA Reference Security Incident Classification Taxonomy[24]. It is also recommended to use the results of prospective studies and the requirements of the EU regulations. When processing data, it is necessary to ensure that ENISA Threat Taxonomy can be compared to the cyber incident taxonomy approved in Ukraine[25].

[21] ENISA Threat Taxonomy 2016, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[22] A Proposal for a European Cybersecurity Taxonomy, https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

[23] Cybersecurity Incident Taxonomy, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

[24] ENISA Reference Security Incident Classification Taxonomy, https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/reference-security-incident-taxonomy-working-group-2013-rsit-wg

[25] List of categories of cyber incidents, https://cert.gov.ua/recommendation/16904

The following frameworks are used as data-dependent CTI frameworks by ENISA methodology: MITRE ATT&CK®, Cyber Kill Chain®, MITRE CVE®, OASIS Cyberthreat Intelligence (CTI) STIX™.

For the main technical format is used the JSON framework.

Depending on types of data, traditional analysis techniques with the usage of expert opinions and structured analytical methods were used.

Interim versions of the report were submitted to the NCCC for review and feedback.

Preparation and distribution of the report

The report was prepared in Ukrainian language, in a pdf format. It is planned to distribute it through publication on the NCCC's online recourses, as well as through presentations to key interested parties. Additionally, a translation of the report into English is being considered for distribution to international partners.