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

Q2

2023

REPORT

ON VULNERABILITY DETECTION AND CYBER INCIDENTS/ CYBER ATTACKS RESPONSE SYSTEM

TLP:WHITE

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

- centralised management of all subsystems of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System;
- centralised collection and accumulation of information about network information 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, which is received from network devices (active sensors, firewalls, vulnerability scanners), workstations and servers, authorisation systems, internal and external cyber threats data sources.

EXECUTIVE SUMMARY

During the reporting period, the Vulnerability Detection and Cyber Incidents/ Cyber Attacks Response System allowed to detect:

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

Compared to the 1st quarter of 2023, the number of IS events :

- related to malware infection and distribution has increased by 95.8%;
- related to information gathering (through scanning methods) has increased by 35.8%;

The total number of critical IS events has increased by 38.1%.

Among the types of malware families detected in the category "02 Malicious software code" Agent Tesla, Snake Keylogger, SmokeLoader, Formbook and Remcos prevail during the reporting period.

During the 2nd 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. "National CyberArmy", "WE ARE BLOODNET", "Solntsepyok", "Xaknet" and "NoName057(16)" are the most active pro-russian hacktivist groups with the number of attacks organised during the second quarter of 2023 accounting for 89% of the total number of recorded attacks organised by similar groups during the reporting period.
The largest number of such attacks targeted the financial, government, media, energy and telecommunications sectors.

April, May and June digests, prepared by the National Cybersecurity Coordination Centre within the National Security and Defense Council of Ukraine, describe the main events in the cybersecurity field during the corresponding periods.

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

29.7k

FPS

24.7k

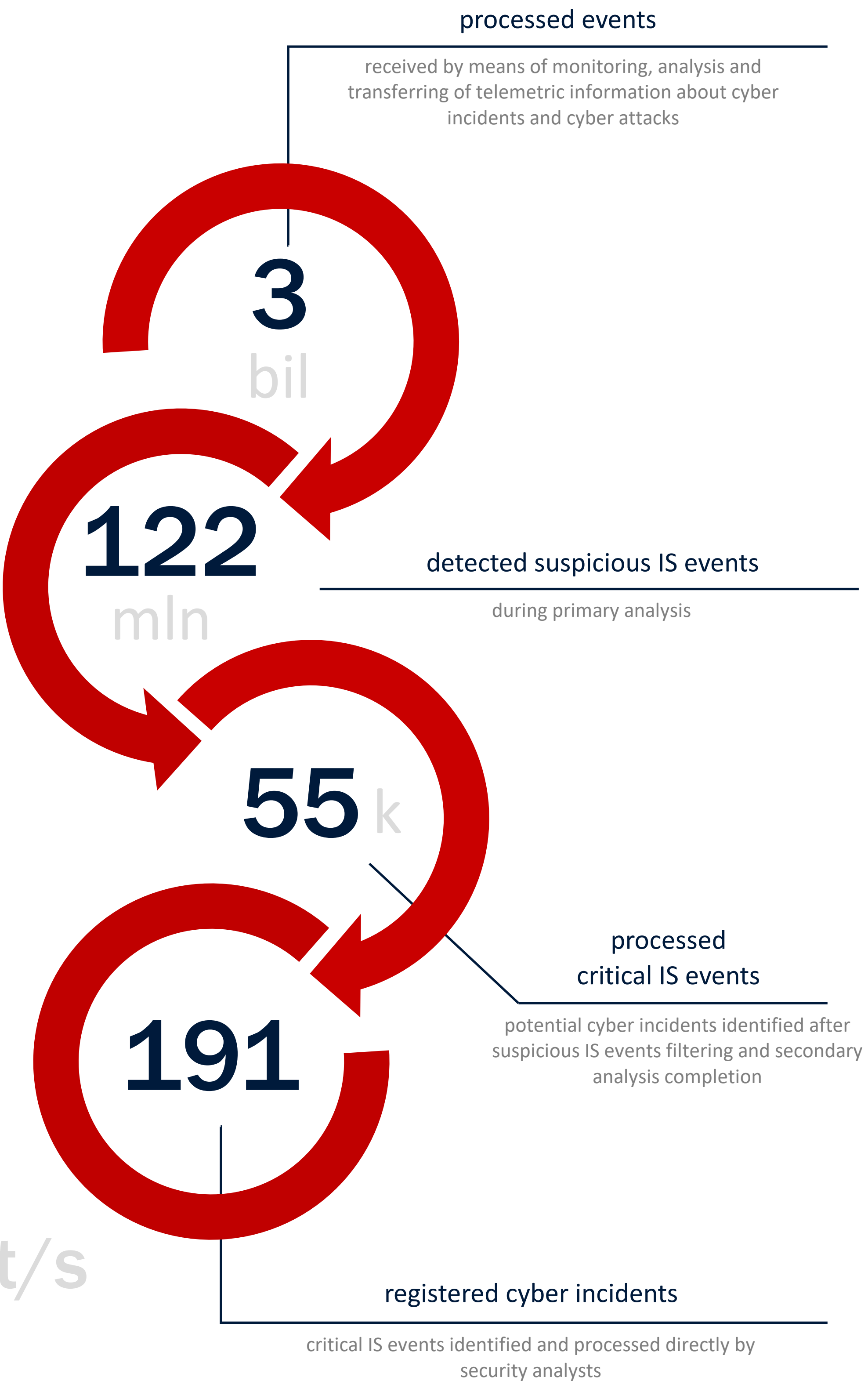
hosts

3.9 Tb

input data received

17.2 Gbit/s

incoming traffic speed
of sensor network



processed events

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

3 bil

122 mln

detected suspicious IS events

during primary analysis

55 k

processed
critical IS events

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

191

registered cyber incidents

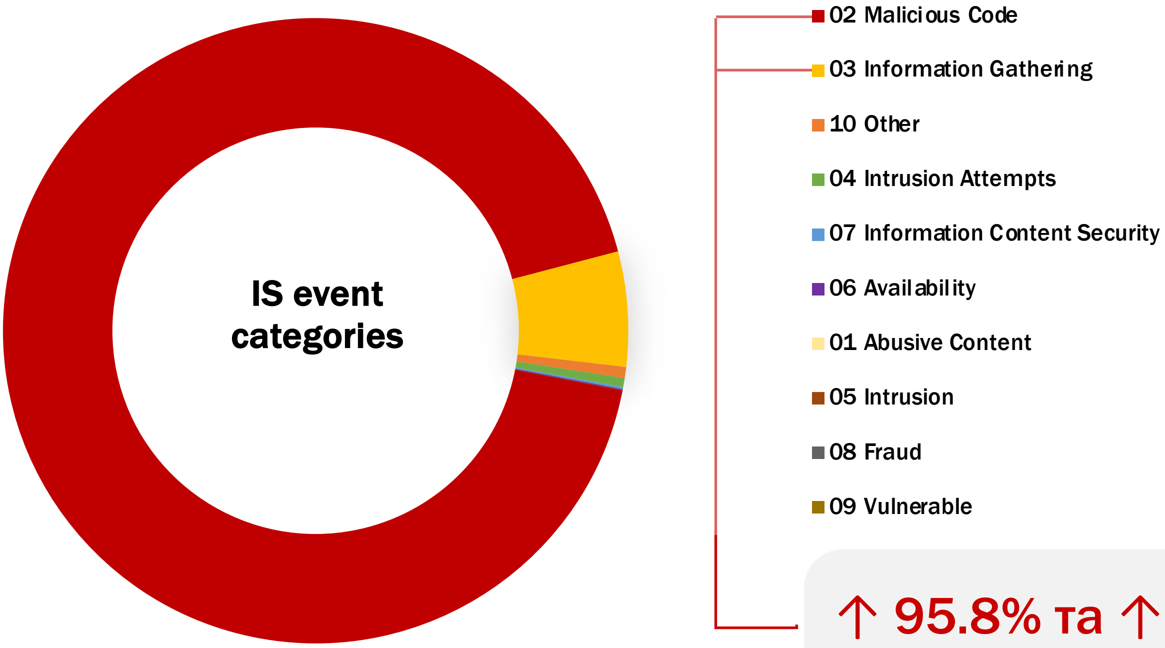
critical IS events identified and processed directly by security analysts

2023 (Q2)

IS EVENTS MONITORING

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

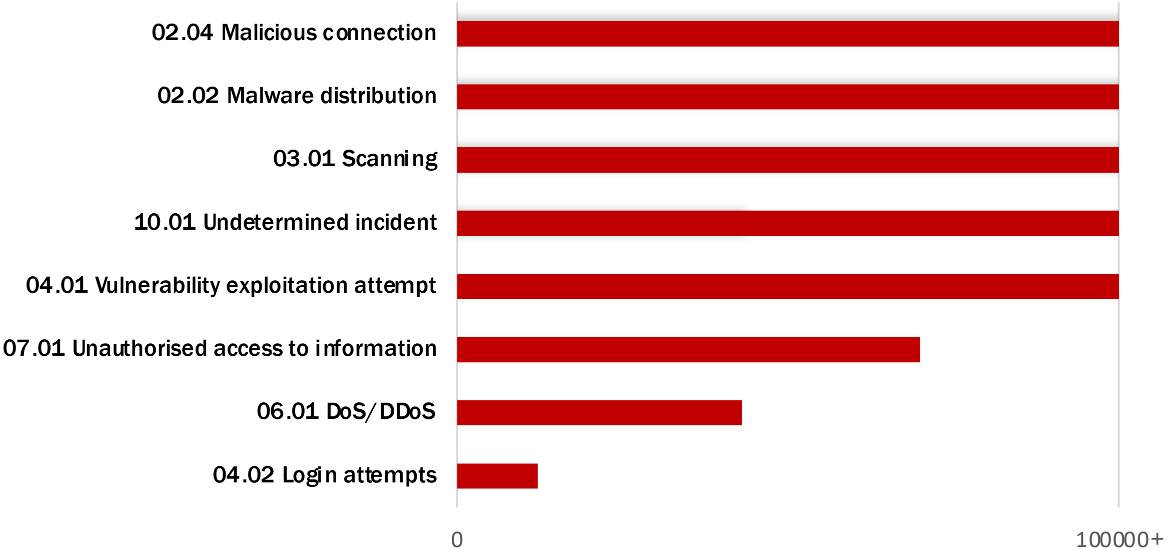
displayed according to [Incident Classification Taxonomy] approved by the National Cybersecurity Coordination Centre within the National Security and Defense Council of Ukraine



↑ 95.8% та ↑ 35.8%

by such amount of % accordingly the number of IS events in categories "02 Malicious Code", "03 Information Gathering" increased (compared to the 1st quarter of 2023).

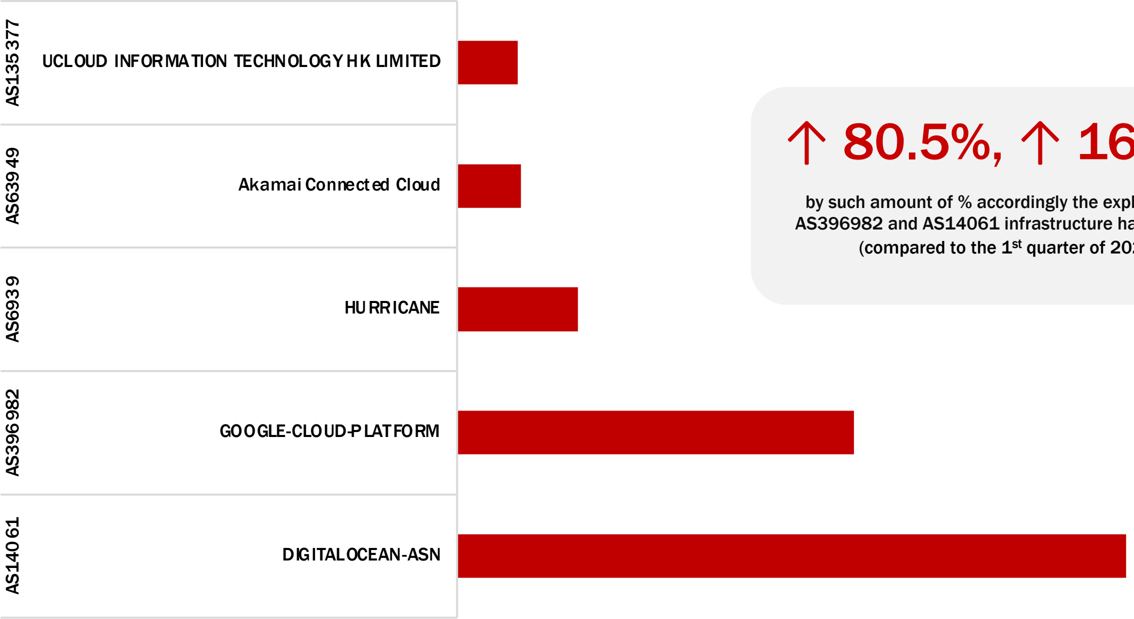
IS event types



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 for the reporting period



↑ 80.5%, ↑ 16.8%

by such amount of % accordingly the exploitation of AS396982 and AS14061 infrastructure has increased (compared to the 1st quarter of 2023).

top 10 source IPs

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

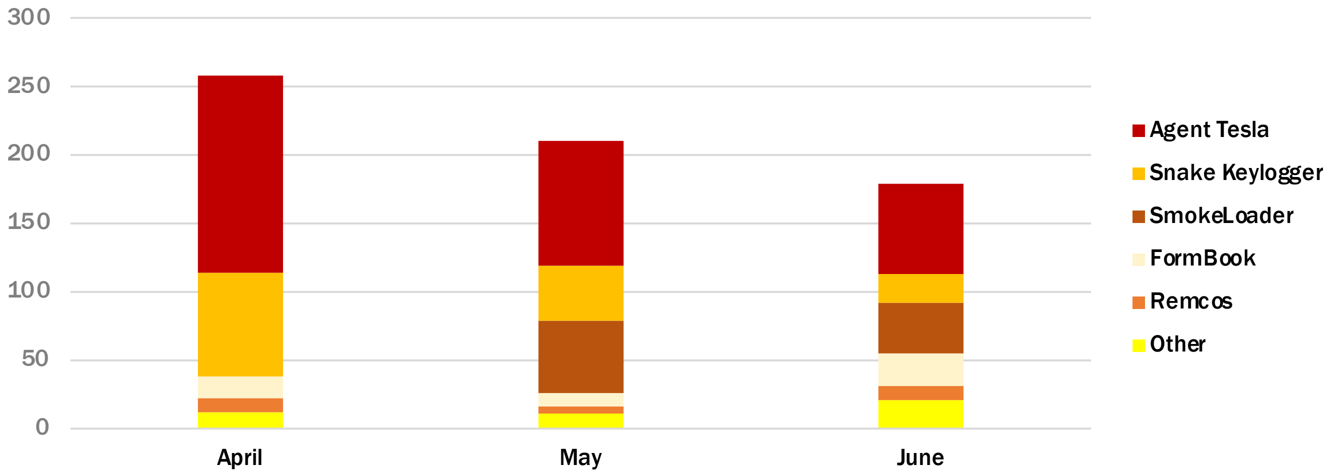
src	src country	AS NUMBER	AS NAME	%
185.174.137.26	Finland	AS210644	AEZA GROUP Ltd	8.36%
185.246.130.106	Sweden	AS42237	W1N Ltd	1.6%
109.205.213.26	United State	AS19318	Interserver INC	1.3%
45.143.200.102	Bulgaria	AS212283	ROZA HOLIDAYS EOOD	0.98%
148.153.34.102	Germany	AS63199	CDS Global Cloud Co., Ltd	0.83%
89.248.163.200	Netherlands	AS202425	IP Volume inc	0.8%
185.224.128.17	Netherlands	AS49870	Alsycon B.V.	0.52%
89.248.165.14	Netherlands	AS202425	IP Volume inc	0.51%
89.248.165.109	Netherlands	AS202425	IP Volume inc	0.47%
78.11.84.52	Netherlands	AS202425	IP Volume inc	0.45%

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

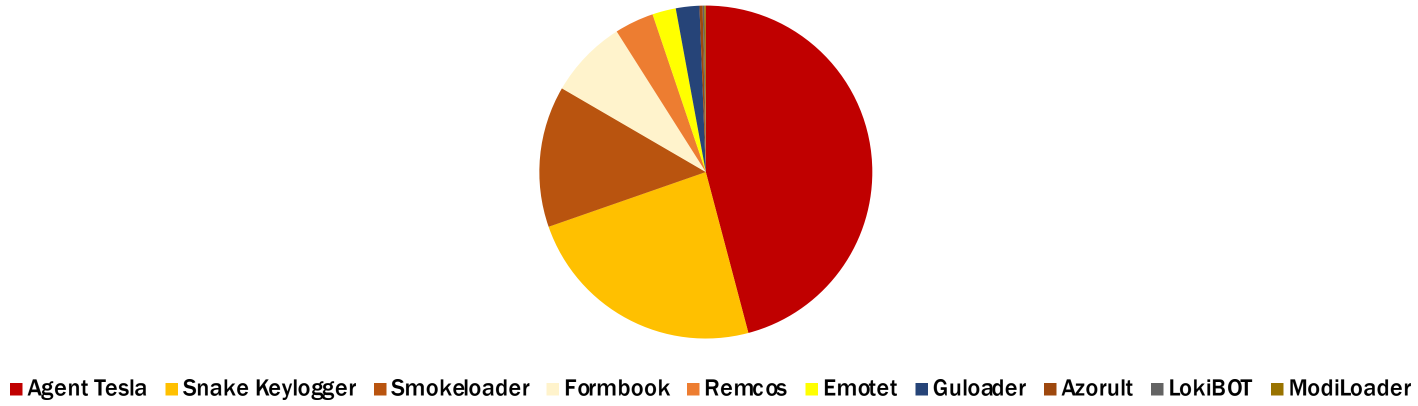
60 075

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

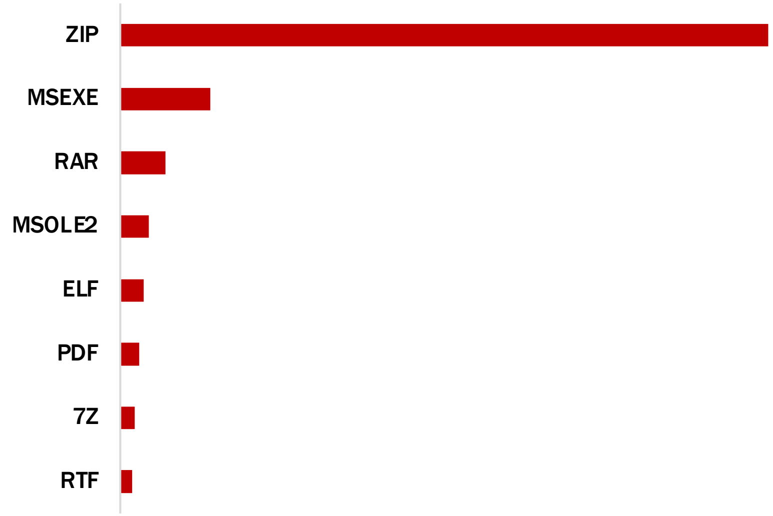
timechart of IS events of category "02 Malicious program code" by malware families



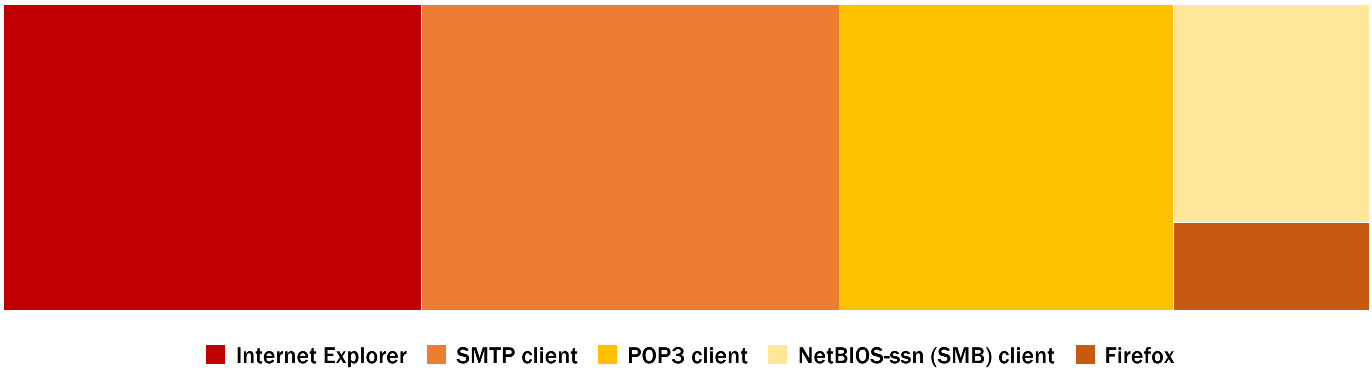
types of malware families detected in IS events of category "02 Malicious program code"



by malware files extentions

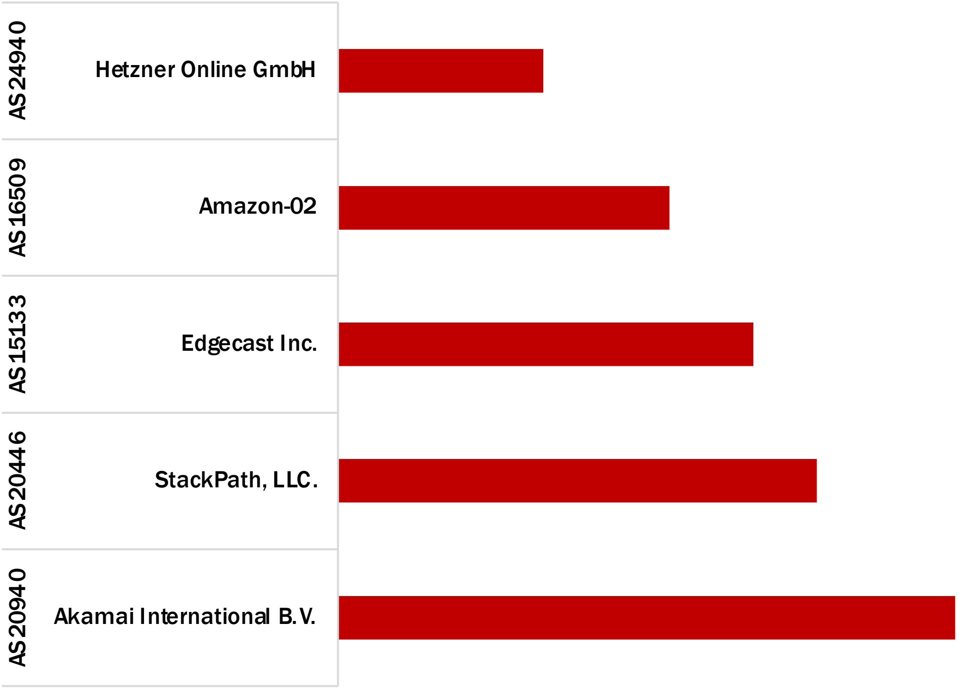


by associated software, used as a malware distribution channel



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 distribution of the malware for the reporting period

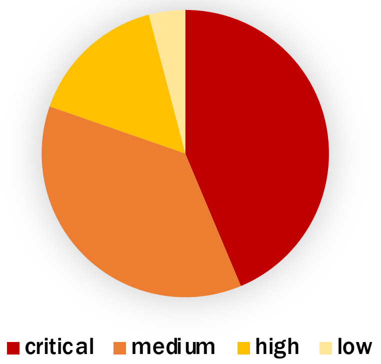


vulnerability exploitation attempt
unauthorized modification of information
malware infection
scanning
account compromise
misconfiguration
spam
malware distribution
malicious connection
fraudulent site
command&control
sabotage
unauthorized access to information
login attempts
undetermined incident
vulnerability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

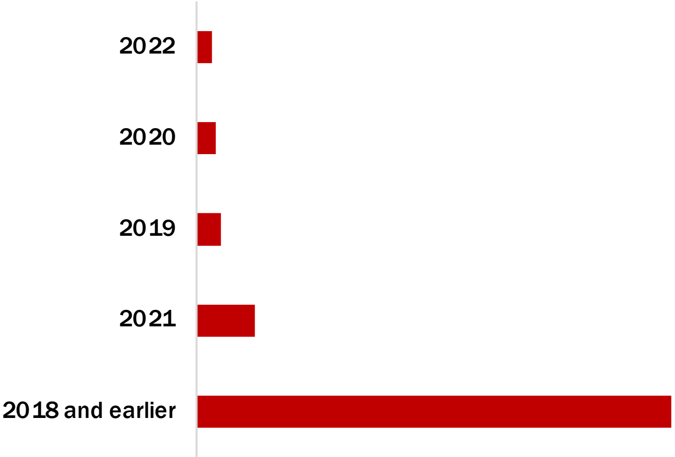
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts of all priorities targeted on the networks of cyber protection objects and the realisation of cyber threats with the aim of detecting software vulnerabilities,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

qualitative rating by CVSS Base Score

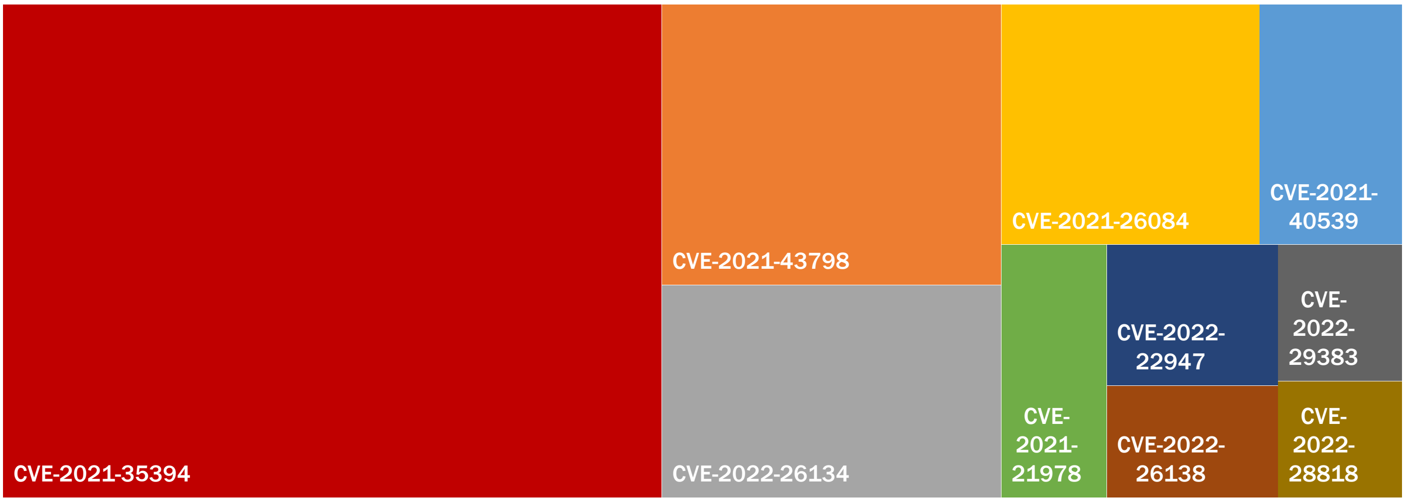
according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in CVSSv3.1 specification



top exploited vulnerabilities by year



top 10 exploited vulnerabilities



russian-UKRAINIAN CYBERWARFARE

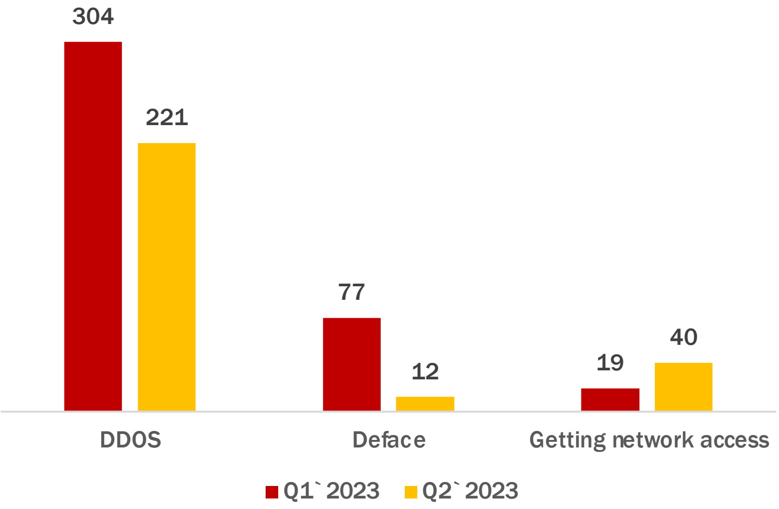
The graphs reflect statistical information for the reporting period, obtained by analysing data from open communication channels of pro-russian hacktivist groups that publish announcements and results of future or already implemented cyberattacks targeting Ukrainian organisations, as well as conduct disinformation campaigns

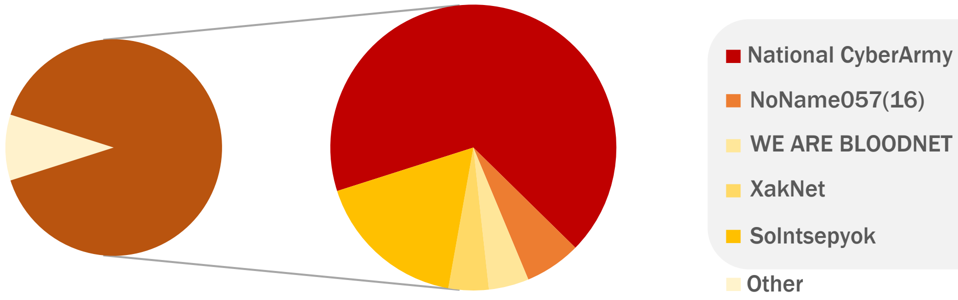
timechart of pro-russian hacktivist groups activity by cyberattack type

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, re-publish 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.

However, despite this, hacktivists activity continues to be tracked in order to monitor trends and changes.

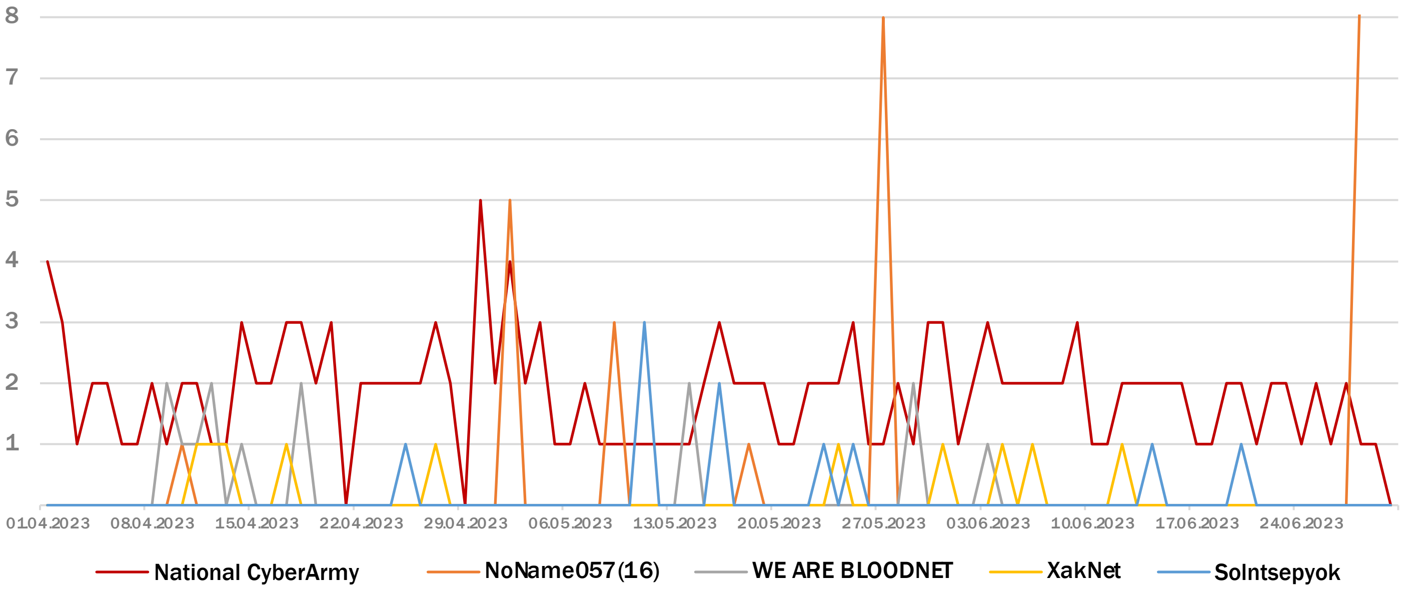
During the 2nd quarter of 2023, the trend towards the decrease in the total number of cyberattacks targeting Ukrainian organisations of various forms of ownership and industries, that has been observed since the beginning of 2023, continued.





5 most active pro-russian hacktivist groups with the number of attacks organised during the second quarter of 2023 accounting for 89% of the total number of recorded attacks organised by similar groups during the reporting period

timechart of pro-russian hacktivist groups activity by name



russian-UKRAINIAN CYBERWARFARE

During the 2nd quarter of 2023, some changes in the activity of monitored pro-russian hacktivist groups took place.

In particular, on April 4, the Telegram channel announced the launch of official training from the KillNet team "DARK SCHOOL". The list of 9 courses for "conducting professional cyber warfare and increasing the balance of your own wallet" includes:

1) DDOS (L7/4);
2) Google AdWords Arbitration;
3) Fakes (creation, promotion, profit);
4) Carding (Europe, America);
5) OSINT/DEANON (cyber intelligence);
6) Pegasus (spyware for Android/IOS);
7) Social engineering;
8) Methods of cyber warfare (psychology and influence on the subconscious of any participant of the World Wide Web);
9) Online sabotage (techniques).

The training is available in four languages - Russian, English, Spanish and Hindi. Previously, until April 2023, KillNet hadn`t created or republished any Hindi language content.

On May 24, the news was published about the dissolution of the main KillNet membership due to the fact that 50 groups (1250 people) "are not engaged in hacktivism" and a large number of members are guided by personal motives, promoting their own services, taking advantage of the group's popularity. On the same day, a call for new members was announced.

On April 28, the Tesla DDoS botnet project, which uses MACAN-TLS, HTTP-FLOOD, and SMYKL-FLOOD methods to carry out attacks, is officially launched. On May 23, the development of the TESLA-BOTv3 update was announced, which would include bypassing static and dynamic raid limits, classic UAM, CAPTCHA and DDG, as well as DOOMINATE mode. Despite a previous statement by Radis (leader of Anonymous Russia and the main developer of the Tesla Botnet) on June 4, the release is still scheduled for August 2023.

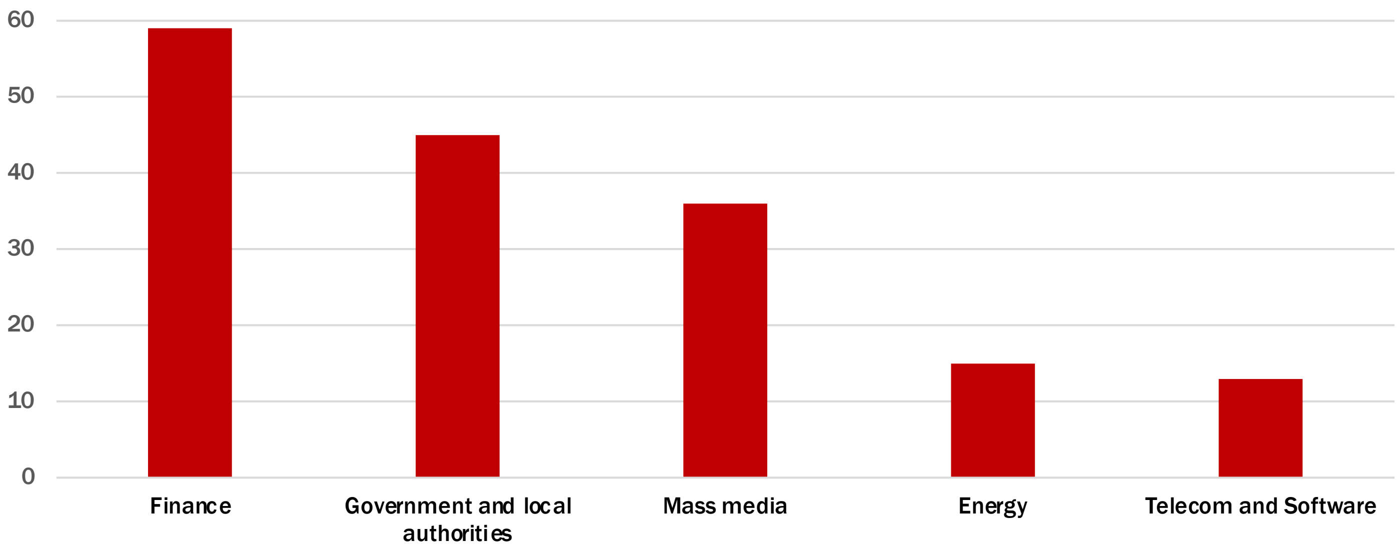
Since May 1, the PHOENIX group has expanded the list of its own TTPs by adding the dissemination of personal data of citizens of "unfriendly countries" - members of NATO and the EU. Also, since March 27 this year, their Telegram channel has been disseminating compromised account data to platforms whose operation is associated with the activities of foreign countries.

On May 11, the " Solntsepyok" Telegram channel (whose administrators are mentioned as followers of the "DNR Joker"), which has been active since at least April 25, 2022, and previously functioned exclusively as a database of personal data of Ukrainians allegedly involved in hostilities, announced the "beginning of the cyberwar against Ukraine." Accordingly, starting from May 11, the channel periodically published news about hacking websites and gaining access to the networks of Ukrainian organisations (including providers and government agencies).

On May 24, the “Anonymous Sudan” group expanded the list of its own TTPs to include ransom payments for preventing and stopping DDoS attacks. The first case of such activity was an attack on the Scandinavian airline system, the initial ransom for stopping a DDoS attack on which was $3,500.

On June 5, the “Devils Sec – 1967” Telegram channel, which has been operating since May 26, announced the coordination of operations with the KillNet group: "We declare our solidarity with Russia in its cyberattacks on Ukraine and will target very critical objects for the Ukrainian side." However, based on the June 14 post, Devils Sec - 1967 is seeking to de-associate itself with the exceptionally pro-russian position.

timechart of pro-russian hacktivist groups activity by sectors

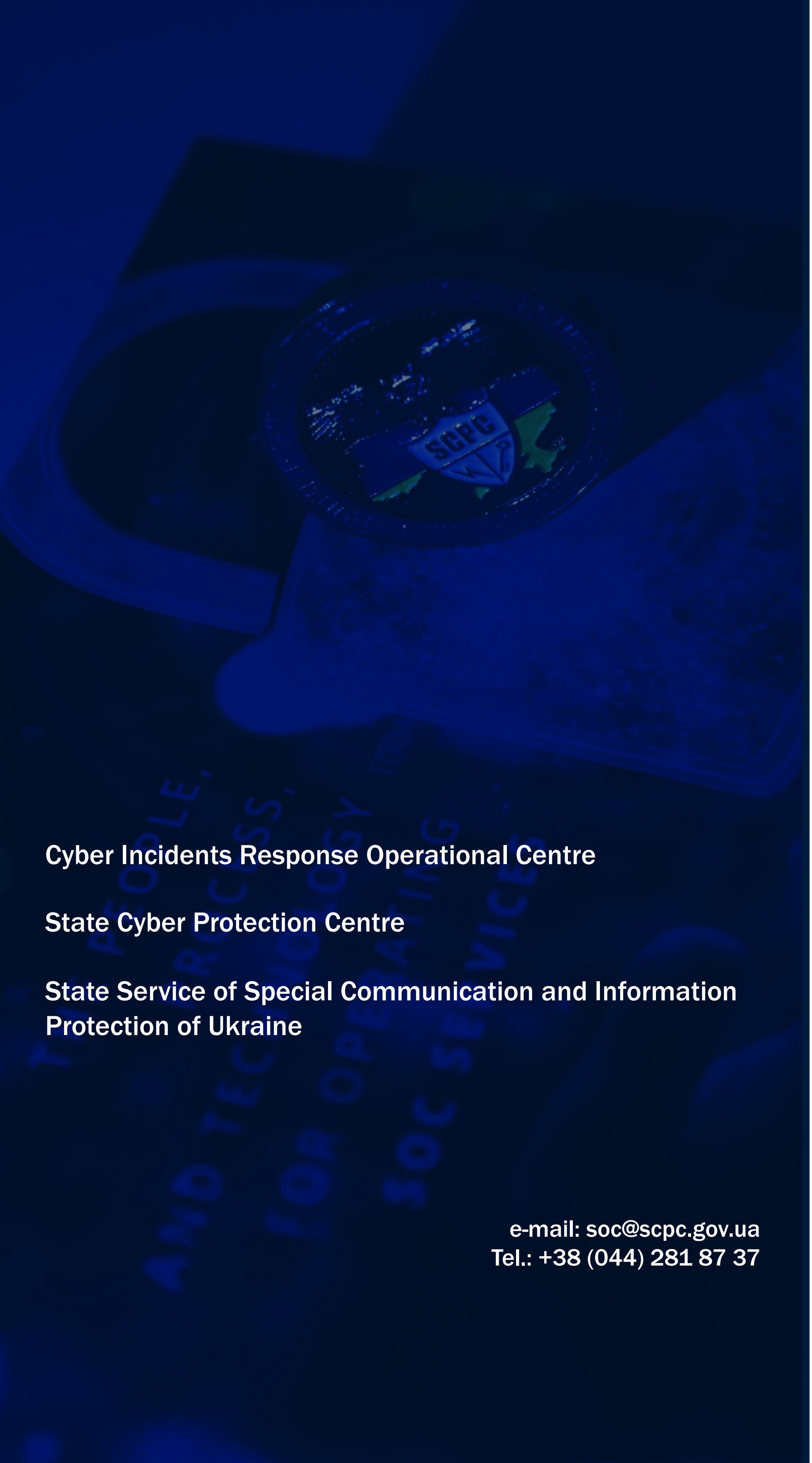


REGULATORY LEGAL BASE

- The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine", which defines the legal and organisational foundations for ensuring the protection of the vital interests of a person and a citizen, society and the state, national interests of Ukraine in cyberspace, the main goals, directions and principles of the state policy in cyber security field, powers of state authorities, enterprises, institutions, organisations, individuals and citizens from this area, the main principles of their activities coordination to ensure cyber security.

- Decree of the Cabinet of Ministers of Ukraine, December 23, 2020, № 1295 "Some issues of ensuring the functioning of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System", that defines the principles of functioning of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System, which are carried out in relation to cyber protection objects, designated in the second part of Article 4 of the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine".

CONTACTS



Cyber Incidents Response Operational Centre

State Cyber Protection Centre

State Service of Special Communication and Information Protection of Ukraine

e-mail: soc@scpc.gov.ua
Tel.: +38 (044) 281 87 37