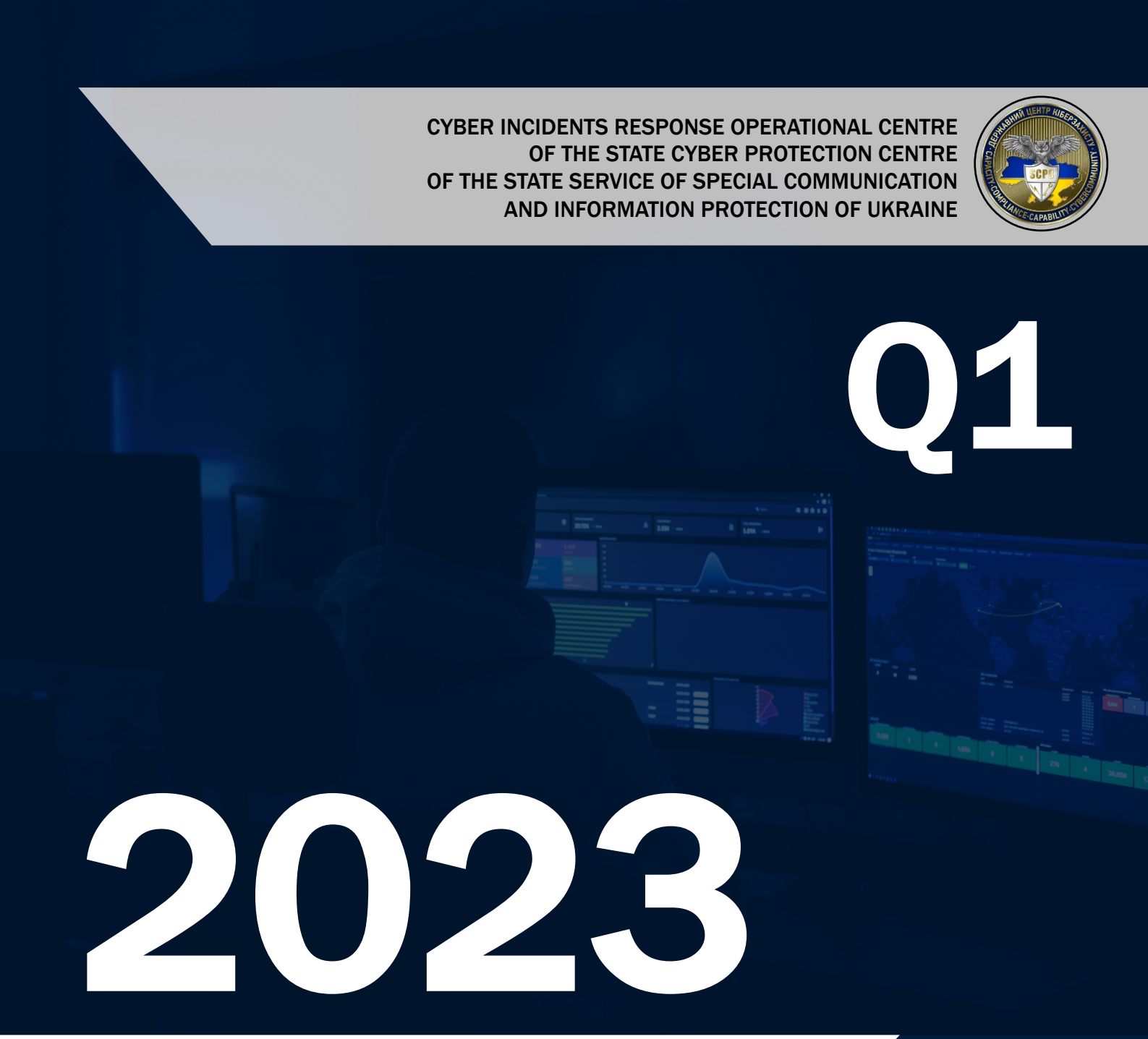
CYBER INCIDENTS RESPONSE OPERATIONAL CENTRE
OF THE STATE CYBER PROTECTION CENTRE
OF THE STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE



Q1

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:

- centralized management of all subsystems of the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System;
- centralized 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, authorization 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:

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

BARAT, Emotet, Cobalt Strike and Meris represent the most frequently used C2 infrastructure determined as the source of potential network intrusion events or organizational security policies violations detected in incoming network traffic by the Telemetry Collection Subsystem.

Among the types of malware families detected in the category "02 Malicious software code", Snake Keylogger, Agent Tesla, LokiBot, PurpleFox, Formbook, Guloader, Remcos, Asyncrat, Azorult and NanoCore prevail during the reporting period.

Since the beginning of 2023, the number of attacks organized by pro-russian hacktivist groups targeting the commercial, financial, government and local authorities as well as the security and defence sectors has significantly decreased (by 1.5-2.9 times for different sectors) compared to the 4th quarter of 2022. At the same time, the intensity of cyberattacks targeting the energy and media sectors remains at the same level.
XakNet, NoName057(16), RussianHackersTeam, RaHDit and Free Civillian are the most active pro-russian hacktivist groups, with the number of attacks organized during the first quarter of 2023 accounting for 90% of the total number of recorded attacks organized by similar groups during the reporting period.

According to the popular Russian-Ukrainian war cyber tracker maintained by @Cyberknow20, Telegram is used by hacktivists as a leading platform for organizing malicious activity. The interest to the platform as a "cybercrime ecosystem" is confirmed by the recent release of the article Telegram - How a messenger turned into a cybercrime ecosystem by 2023 by KELA, the cyber threat intelligence company.

Since the beginning of 2023 (compared to the 4th quarter of 2022), there has been a decrease in the total number of cyberattacks organized by pro-russian hacktivist groups, but their systematicity and intensity continues to be on a high level. However, Kremlin intensificates information operations to justify an unprovoked invasion of Ukraine creating conditions for a protracted war in Ukraine, so there is no fundamental reason to believe that the downward trend in the number of cyberattacks targeting Ukrainian organizations of various forms of ownership and industries will continue.

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

9.6 k
FPS

17.3 k
hosts

2.5 Tb
input data received

13.2 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

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

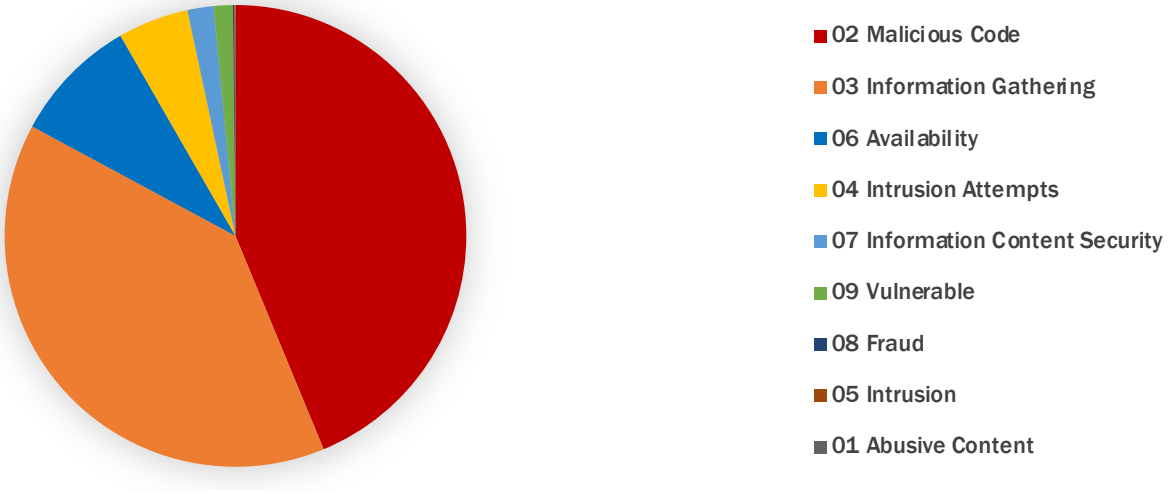
critical IS events identified and processed directly by security analysts

IS EVENTS MONITORING

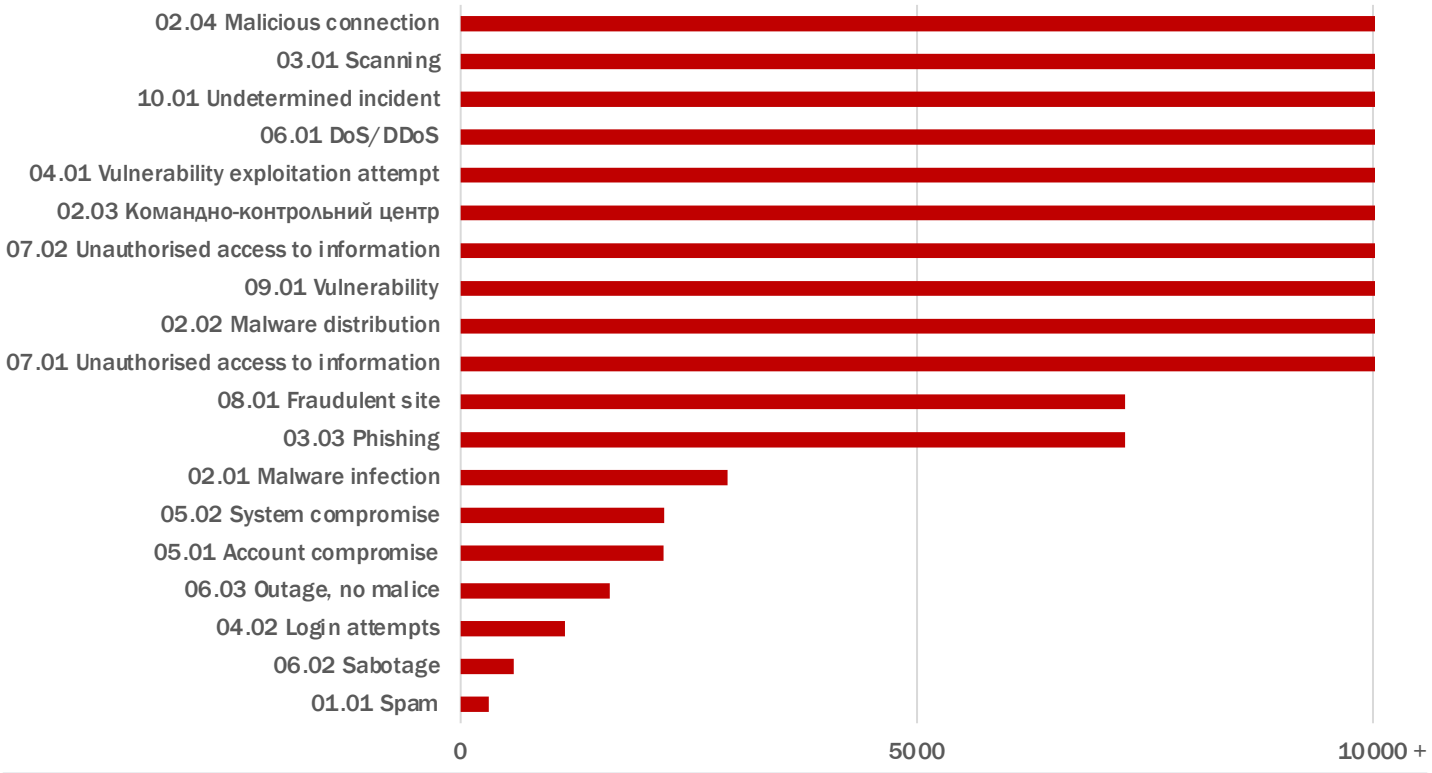
QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

displayed according to Incident Classification Taxonomy approved by the National Coordination Center for Cybersecurity under the National Security and Defense Council of Ukraine

IS event categories



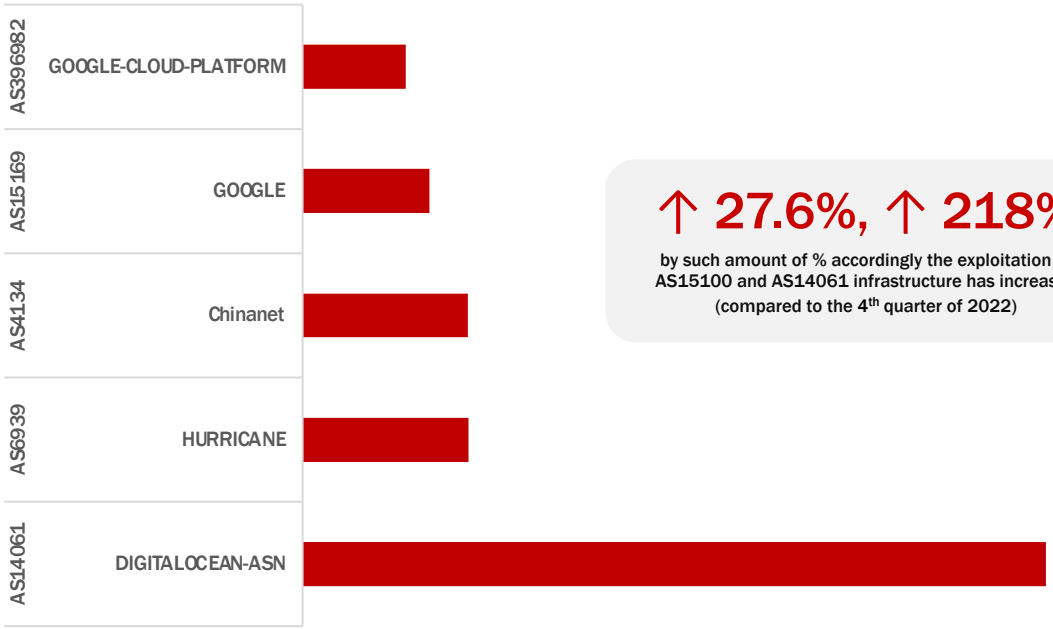
IS event types



2023 (Q1)

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



↑ 27.6%, ↑ 218%

by such amount of % accordingly the exploitation of AS15100 and AS14061 infrastructure has increased (compared to the 4th quarter of 2022)

top 10 source IPs

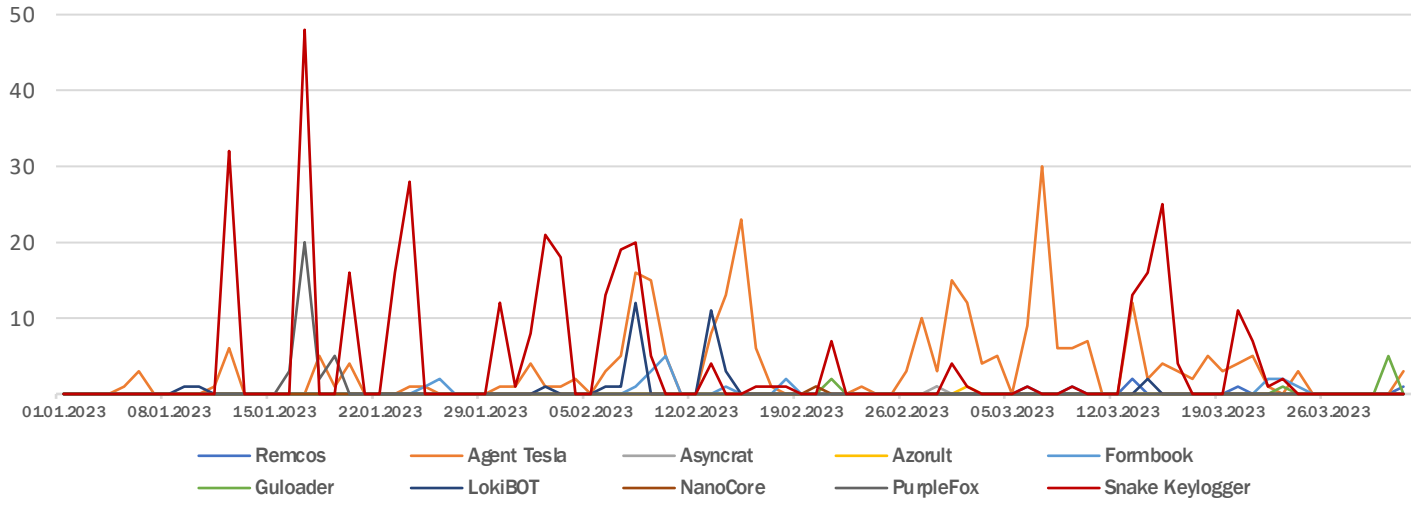
the chart displays top 10 IP addresses (in percent ratio) that were identified as active scanning sources during the reporting period

src	src country	AS NUMBER	AS NAME	%
91.191.209.218	Bulgaria	AS57509	L&L Investment Ltd.	0.95
103.14.224.123	Vietnam	AS135918	Viet Digital Technology Liability Company	0.61
79.124.59.74	Bulgaria	AS50360	Tamatiya EOOD	0.58
185.224.128.17	Netherlands	AS49870	Alsycon B.V.	0.30
51.158.46.120	France	AS12876	ONLINE S.A.S.	0.29
170.39.218.4	France	AS49434	Harmony Hosting SARL	0.25
89.248.163.200	Netherlands	AS202425	IP Volume inc	0.19
89.248.165.14	Netherlands	AS202425	IP Volume inc	0.16
146.88.240.4	The United States of America	AS20052	Arbor Networks, Inc.	0.15
89.248.165.209	Netherlands	AS202425	IP Volume inc	0.14

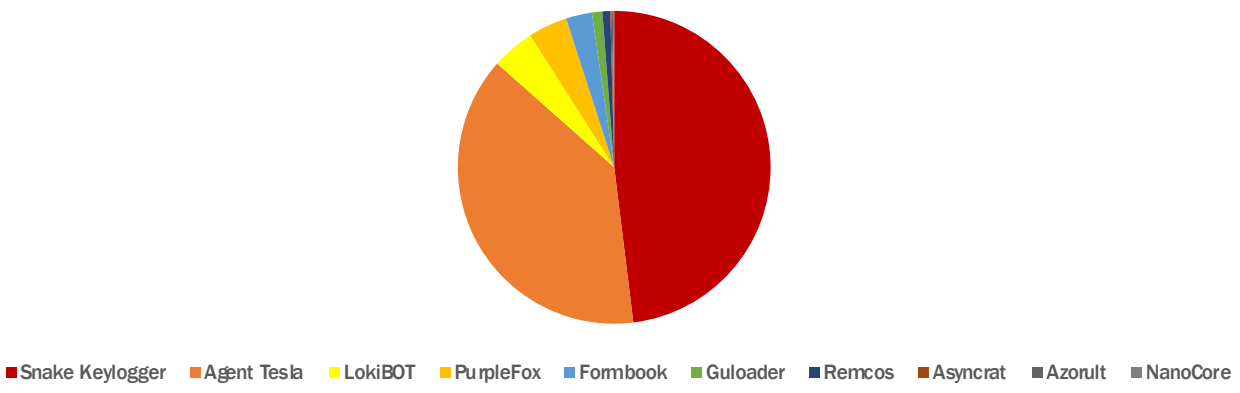
43 946

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

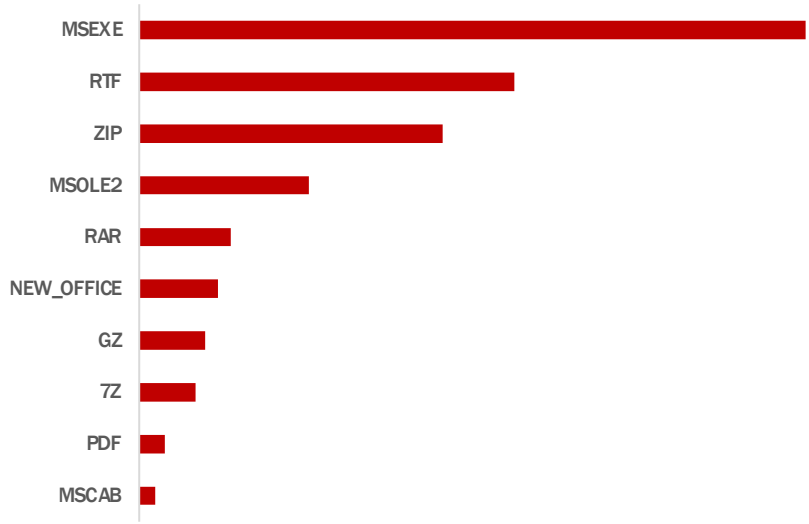
timechart of IS events of "02 Malicious program code" category by malware families



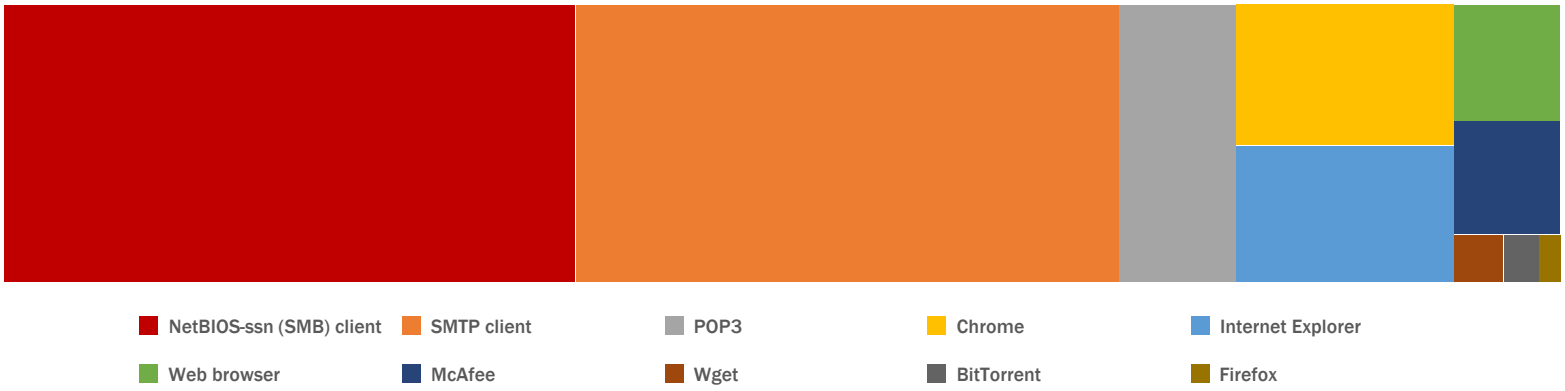
distribution of malware families detected in IS events of "02 Malicious program code" category



by malware files extentions

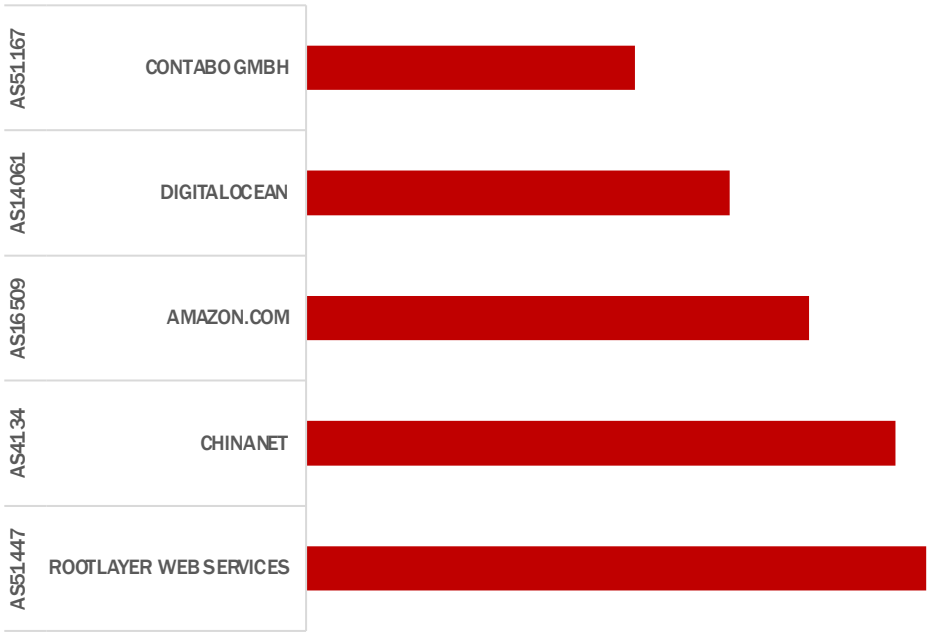


by associated software, used as a malware distribution channel



top 5 source ASN

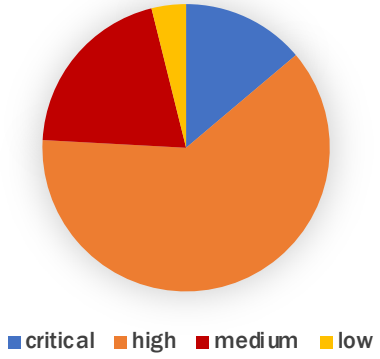
the chart displays top 5 ASN (in percent ratio), the dominant number of IP addresses of which were identified as active malware distribution sources during the reporting period



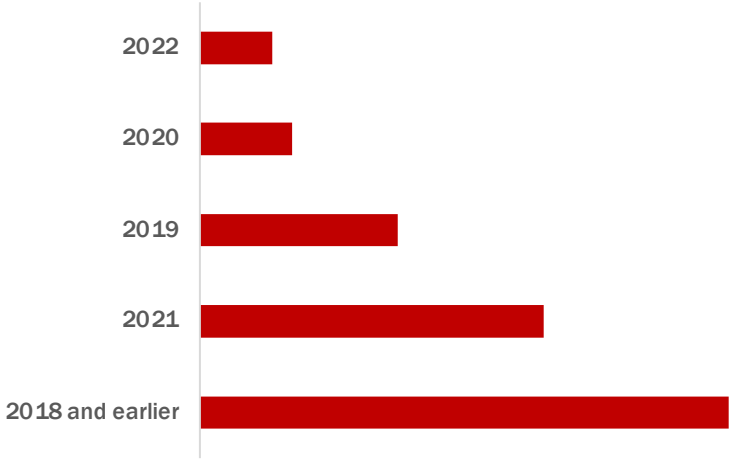
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts of all priorities targeted on the networks of cyber protection objects and the realization of cyber threats with the aim of detecting software vulnerabilities,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

qualitative rating by CVSS Base Score

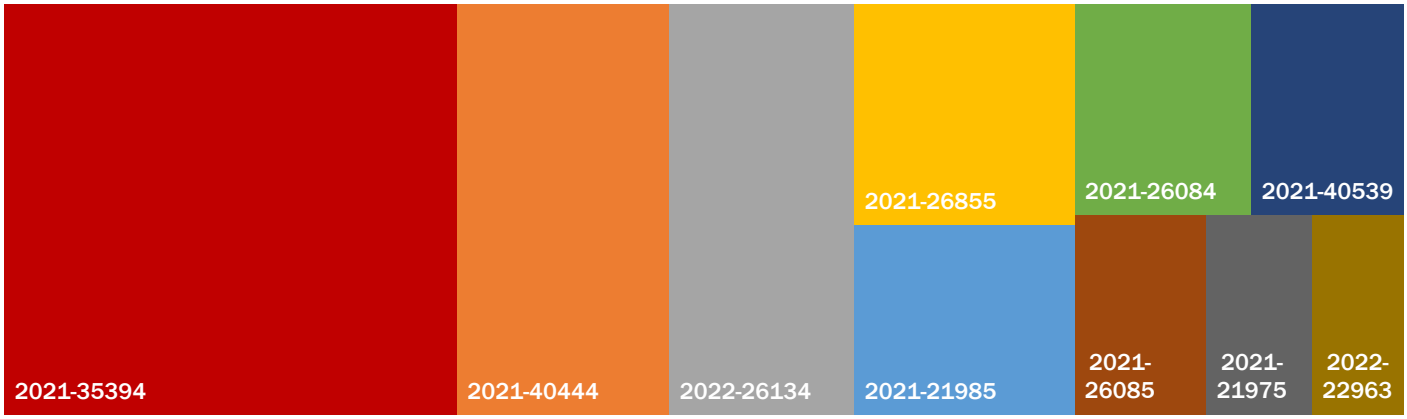
according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in [CVSSv3.1 specification]



top exploited vulnerabilities by year



top 10 exploited vulnerabilities



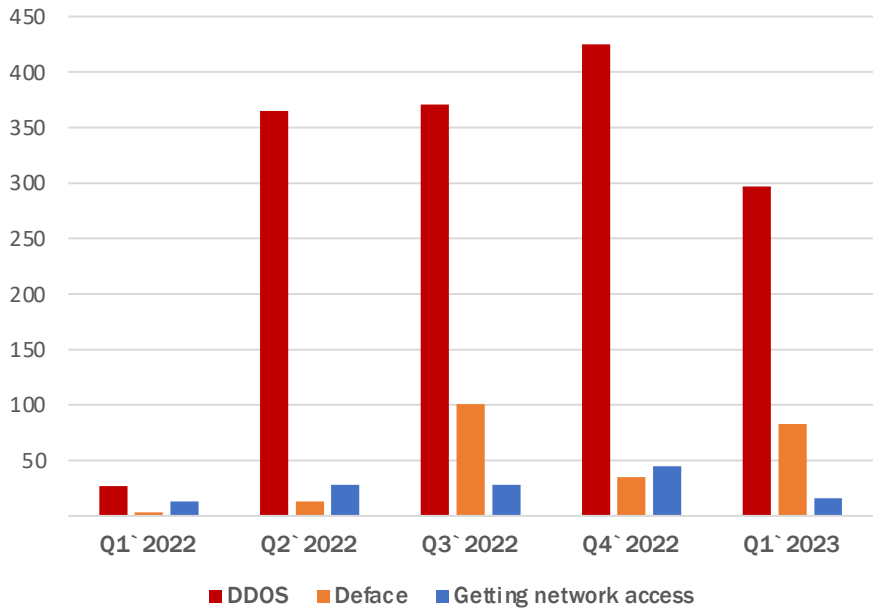
russian-UKRAINIAN CYBERWARFARE

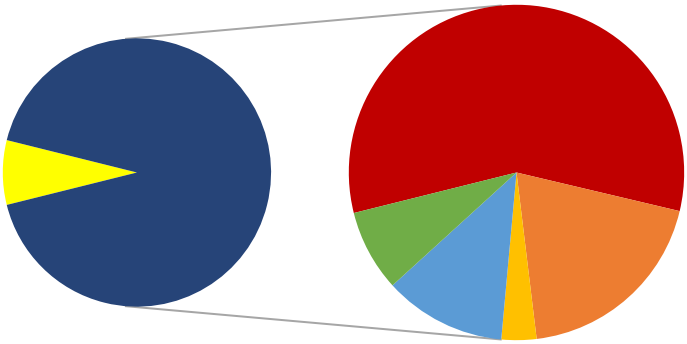
The graphs reflect statistical information for the reporting period, obtained by analyzing data from open communication channels of pro-russian hacktivist groups that publish announcements and results of future or already implemented cyberattacks targeting Ukrainian organizations, as well as conduct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

Since the beginning of 2023 (compared to the 4th quarter of 2022), there has been a decrease in the total number of cyberattacks organized by pro-russian hacktivist groups, but their systematicity and intensity continues to be on a high level.

However, Kremlin intensificates information operations to justify an unprovoked invasion of Ukraine creating conditions for a protracted war in Ukraine, so there is no fundamental reason to believe that the downward trend in the number of cyberattacks targeting Ukrainian organizations of various forms of ownership and industries will continue.

timechart of pro-russian hacktivist groups activity by cyberattack type

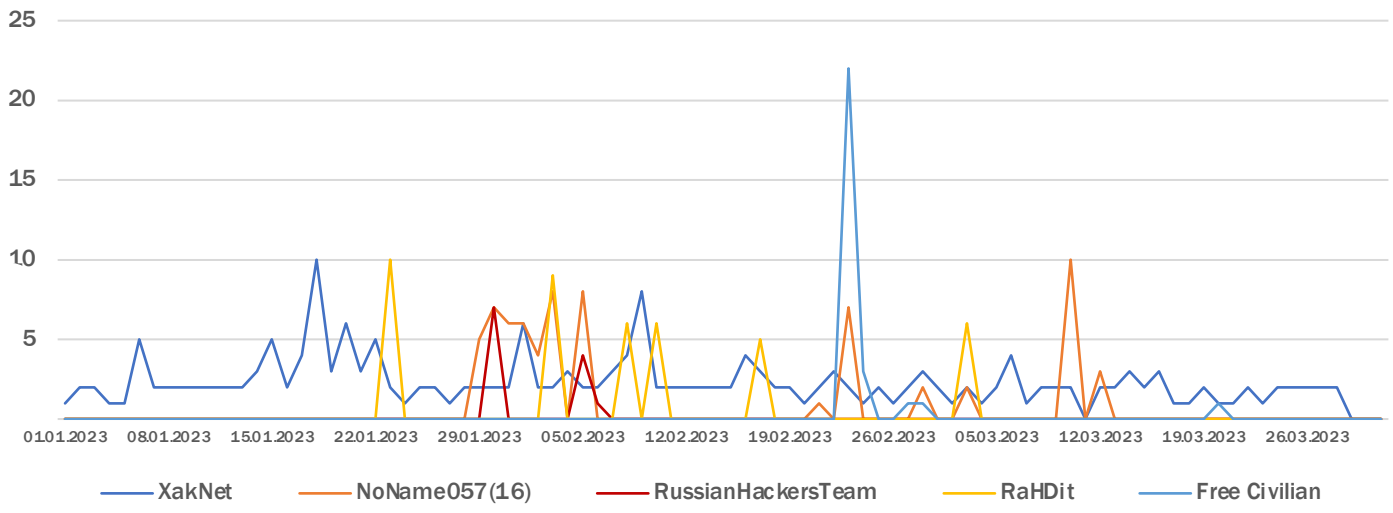




Other
XakNet
NoName057(16)
RussianHackersTeam
RaHDit
Free Civilian

5 most active pro-russian hacktivist groups with the number of attacks organized during the first quarter of 2023 accounting for 90% of the total number of recorded attacks organized by similar groups during the reporting period

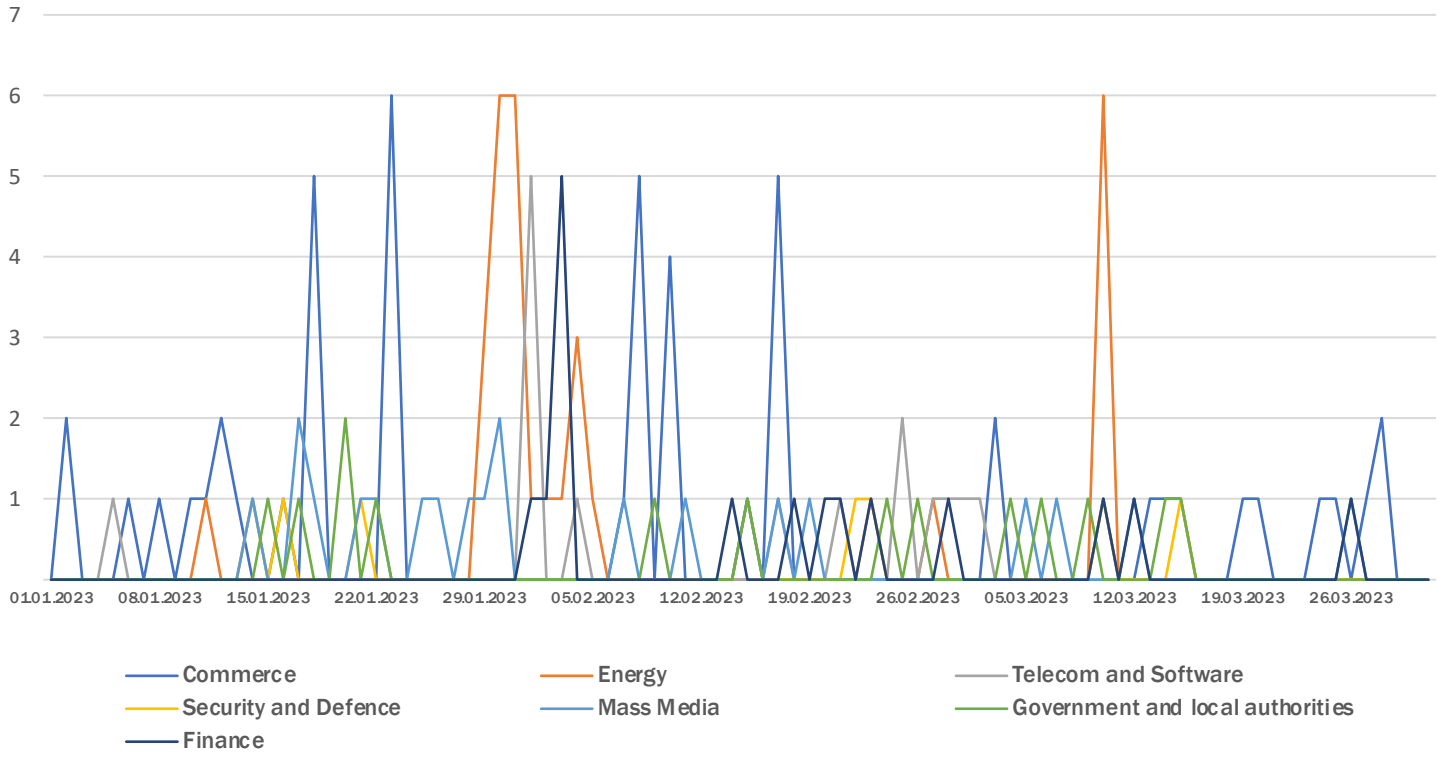
timechart of pro-russian hacktivist groups activity by name



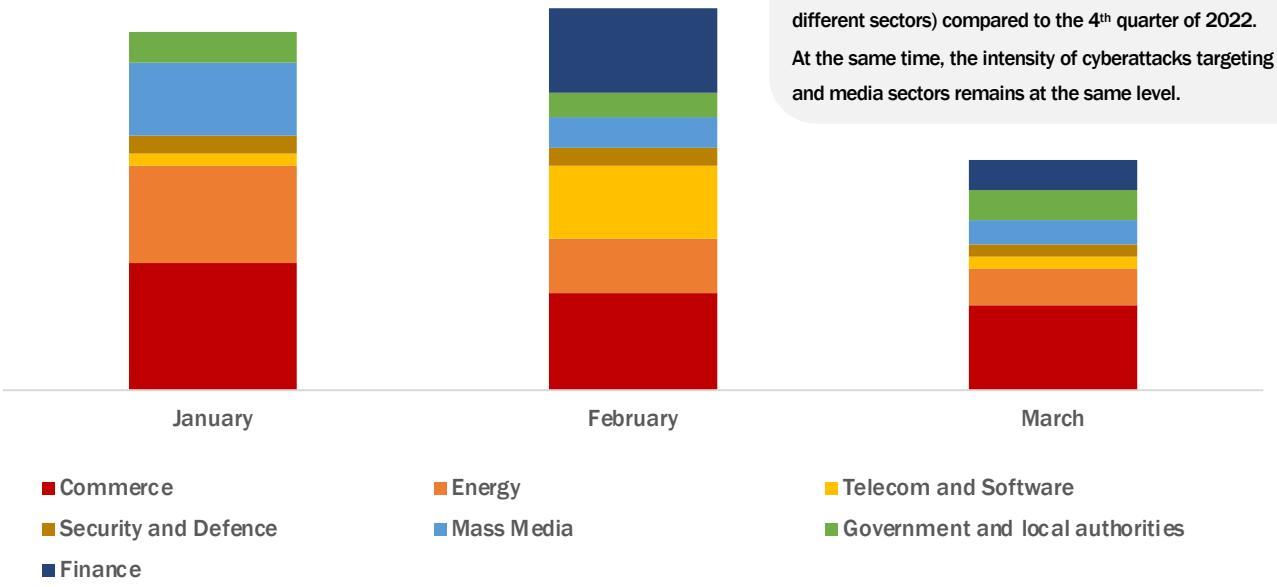
russian-UKRAINIAN CYBERWARFARE

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

timechart of pro-russian hacktivist groups activity by sectors



distribution of pro-russian hacktivist groups activity by sectors



Since the beginning of 2023, the number of attacks organized by pro-russian hacktivist groups targeting the commercial, financial, government and local authorities as well as the security and defence sectors has significantly decreased (by 1.5-2.9 times for different sectors) compared to the 4th quarter of 2022.

At the same time, the intensity of cyberattacks targeting the energy and media sectors remains at the same level.

MALICIOUS C2 INFRASTRUCTURE

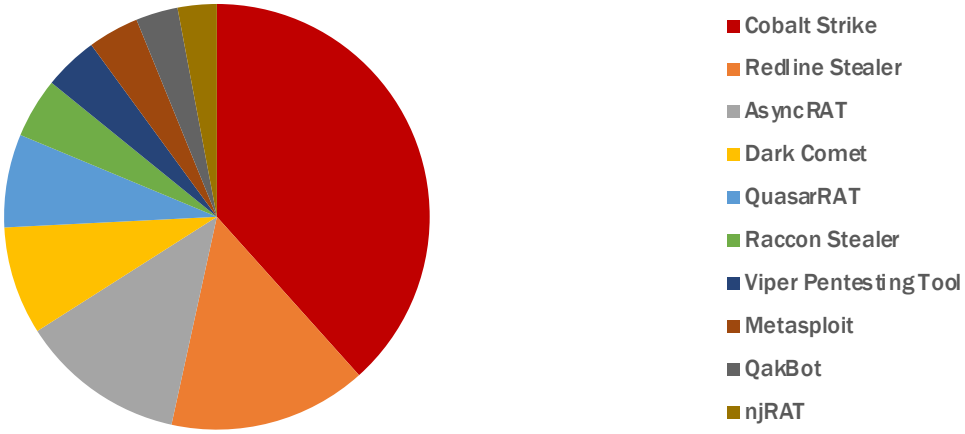
Over 80 000 network intrusion attempts and 600 outbound connections to unique command-and-control (C2) servers (identified to be so according to the data sourced from the Recorded Future Platform) have been observed since the beginning of 2023.

Recorded Future continiously tracks the creation and modification of new malicious infrastructure for a multitude of post-exploitation toolkits, custom malware and open-source remote access trojans using proactive scanning and collection methods.

The collection of such servers, involved in potentially malicious network activity or organizational security policies violations in 2023 Q1, is dominated by Offensive Security Tools (OST) (Cobalt Strike, Metasploit), RATs (BARAT, AsyncRAT, QuasarRAT, njRAT) and botnet families (Emotet, Mirai, Meris).

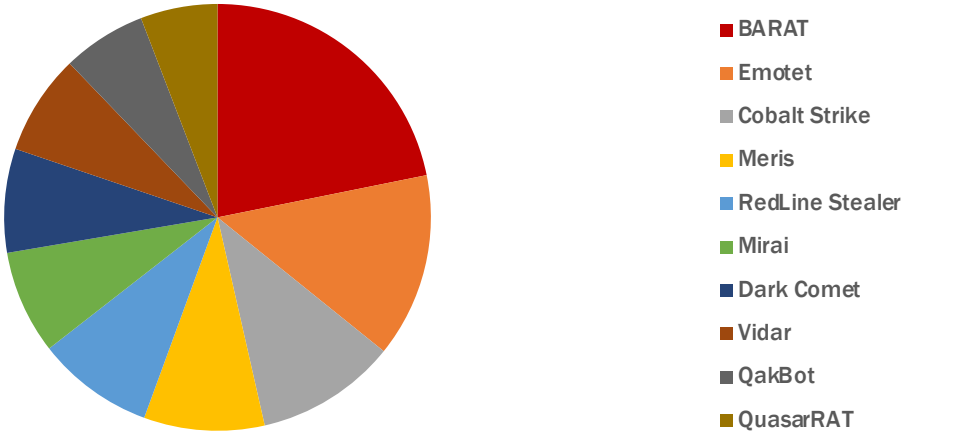
C2 detections of IS events, related to outbound traffic

The diagram shows the command and control infrastructure (C2) involved in potentially malicious network activity or organizational security policies violations detected in outbound network traffic by the Telemetry Collection Subsystem of the Vulnerability Detection and Response System for Cyber Incidents/Cyber Attacks.



C2 detections of IS events, related to inbound traffic

The diagram shows the command and control infrastructure (C2) involved in potentially malicious network activity or organizational security policies violations detected in inbound network traffic by the Telemetry Collection Subsystem of the Vulnerability Detection and Response System for Cyber Incidents/Cyber Attacks.

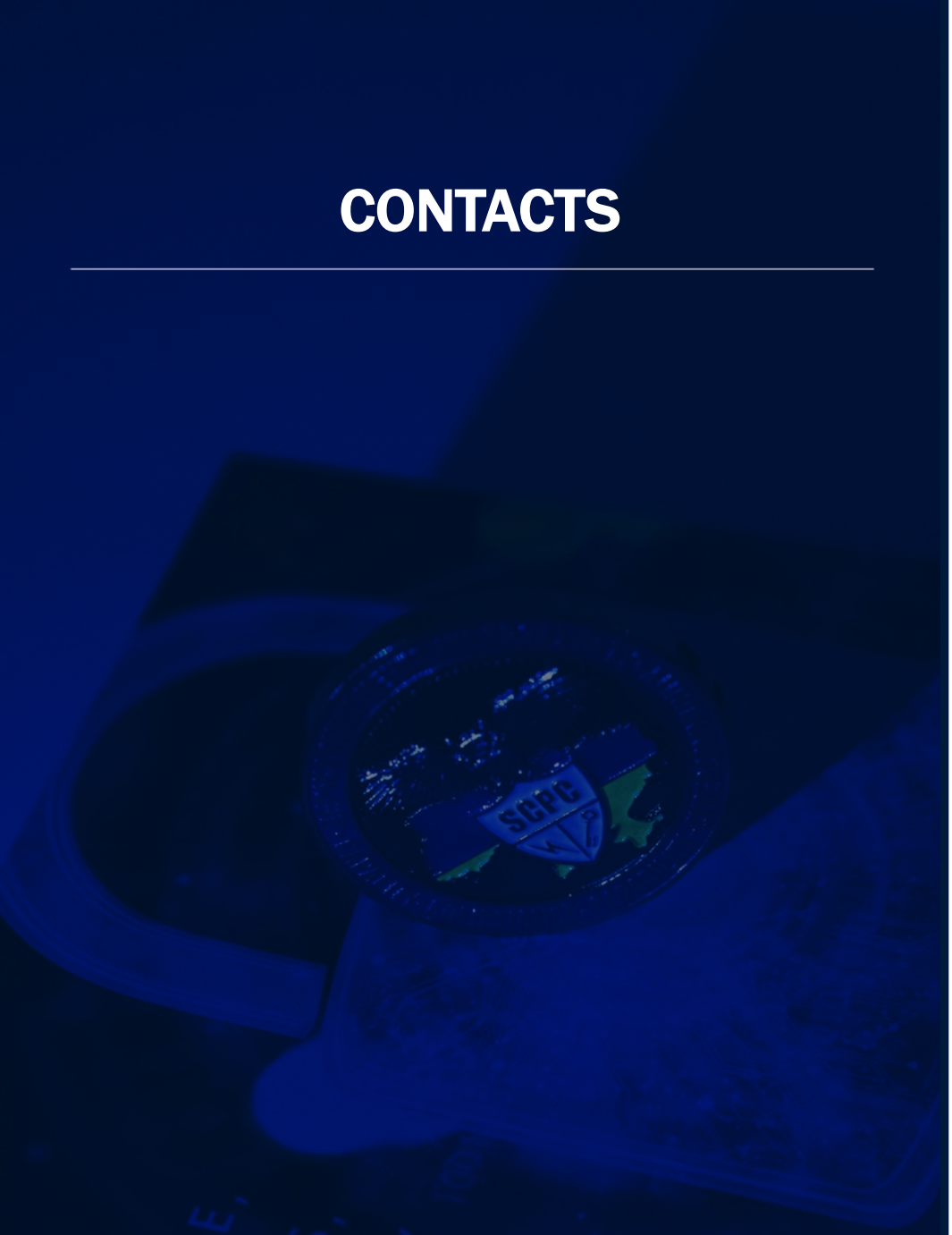


REGULATORY LEGAL BASE

◦ The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine", which defines the legal and organizational 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, organizations, 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