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

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

- **18 billion events**, received by the means of monitoring, analysis and transferring of telemetric information about cyber incidents and cyber attacks;
- **133 million suspicious IS events** (during the initial analysis);
- **148 thousand critical IS events** (potential cyber incidents identified after suspicious IS events filtering and secondary analysis completion);
- **1105 cyber incidents** that were processed directly by security analysts. Compared to 2022, **the number of registered cyber incidents has increased by 62.5%.**

Also **24 new cyber protection objects** of the government (22), energy (1), and military (1) sectors **have been connected** to the Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System during the reporting period.

Among autonomous systems (**AS), the infrastructure of which was identified as an active scanning source most frequently** over the reporting period, we can highlight "**Google", "Hurricane", "Google-Cloud-Platform", "Cloudflarenet" and "DigitalOcean-ASN" .**

1 516 861 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 "Formbook" prevail** during the reporting period.

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 +24	27 +24	33
Sensors installed:	Protected hosts:	Scanned assets:
65 +24	4200+	820+

Sectors and organisations

Cyber protection objects

62 +22	1 +1	2 +1
Government	Energy	Military

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

registered cyber incidents

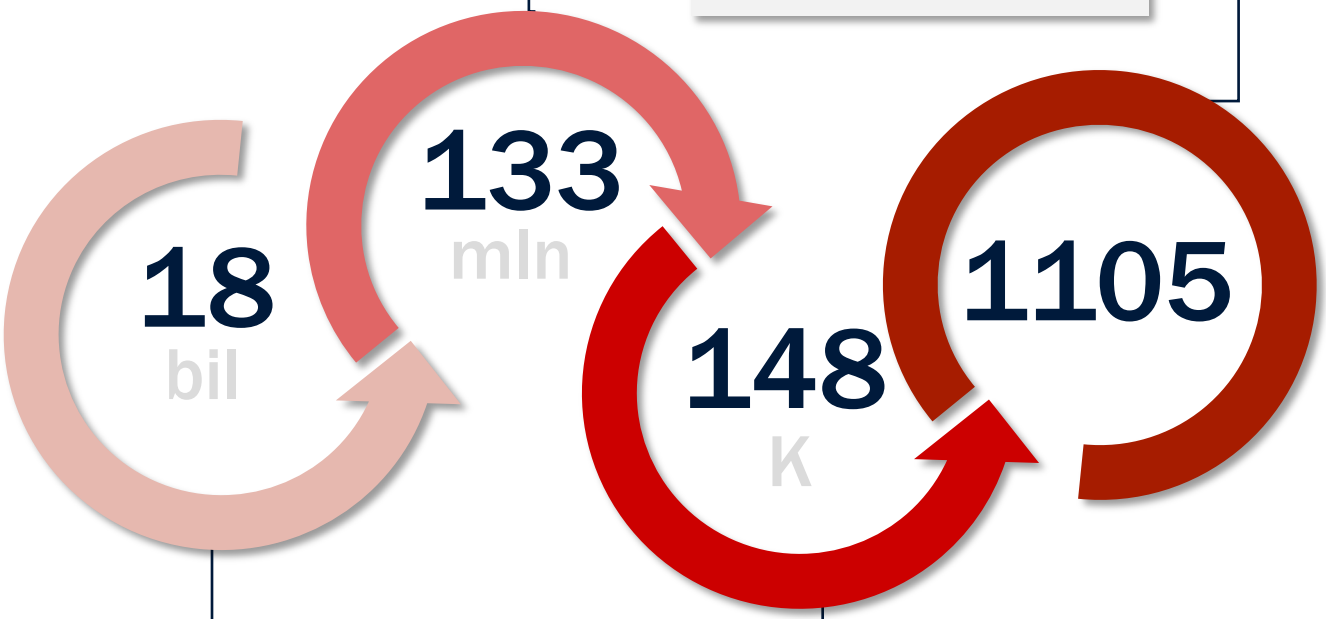
critical IS events identified and processed directly by security analysts

↑62.5%

by such amount of % **the number of registered cyber incidents increased** (comparing to the same time period during 2023)

detected suspicious IS events

during primary analysis



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

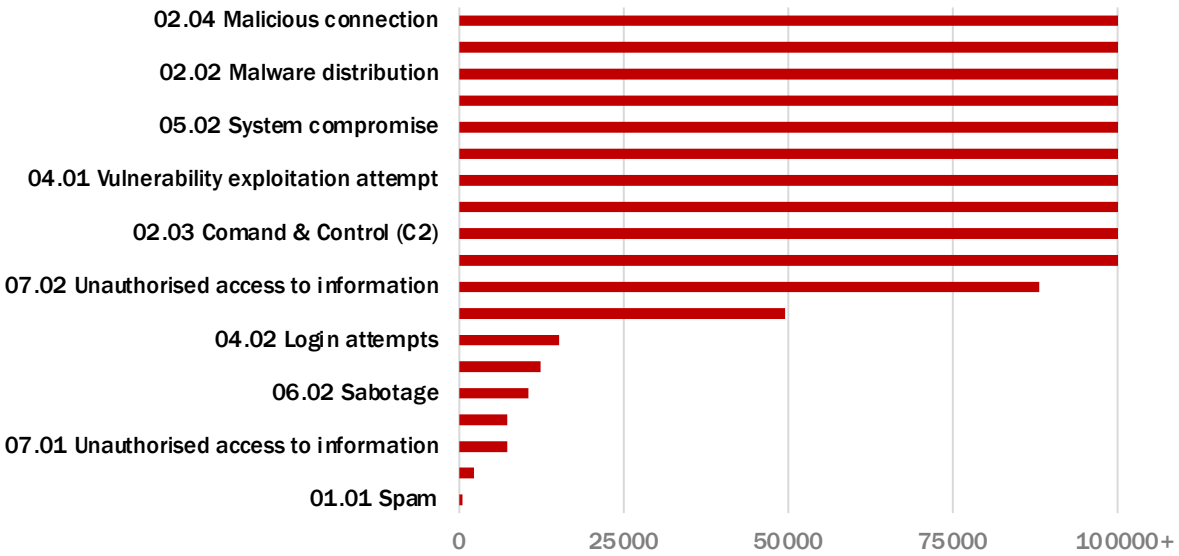
displayed according to Incident Classification Taxonomy approved by the National Cybersecurity Coordination Centre within the National Security and Defense Council of Ukraine

- 02 Malicious Code
- 03 Information Gathering
- 04 Intrusion Attempts
- 06 Availability
- 07 Information Content Security
- 09 Vulnerable
- 08 Fraud
- 05 Intrusion
- 01 Abusive Content

↑ 36.2%, ↑ 43.8%

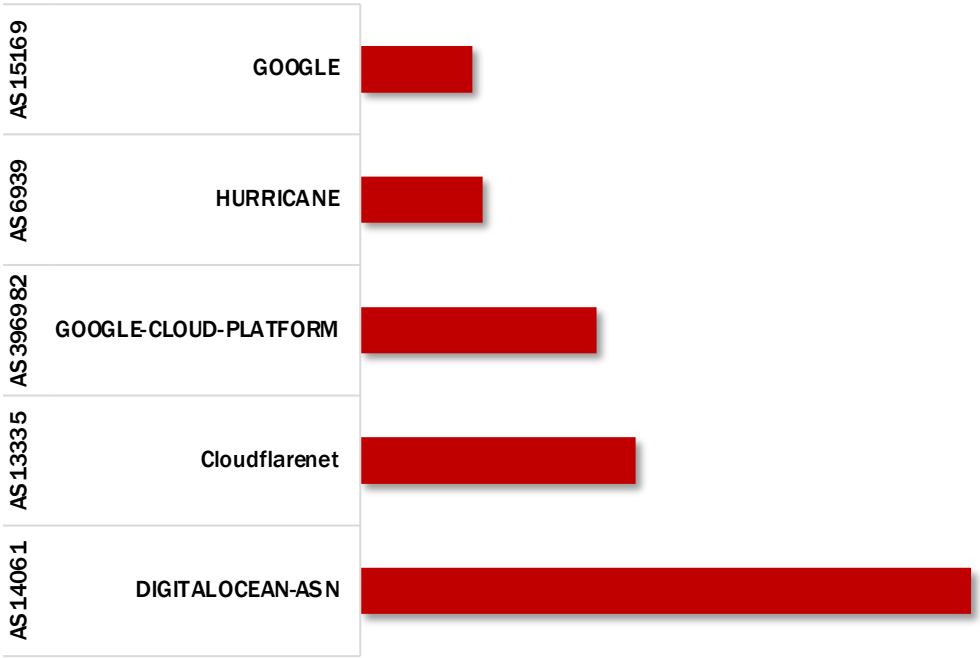
by such amount of % accordingly the number of IS events in categories "02 Malicious Code", "03 Information Gathering" increased (comparing to the same time period during 2023)

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

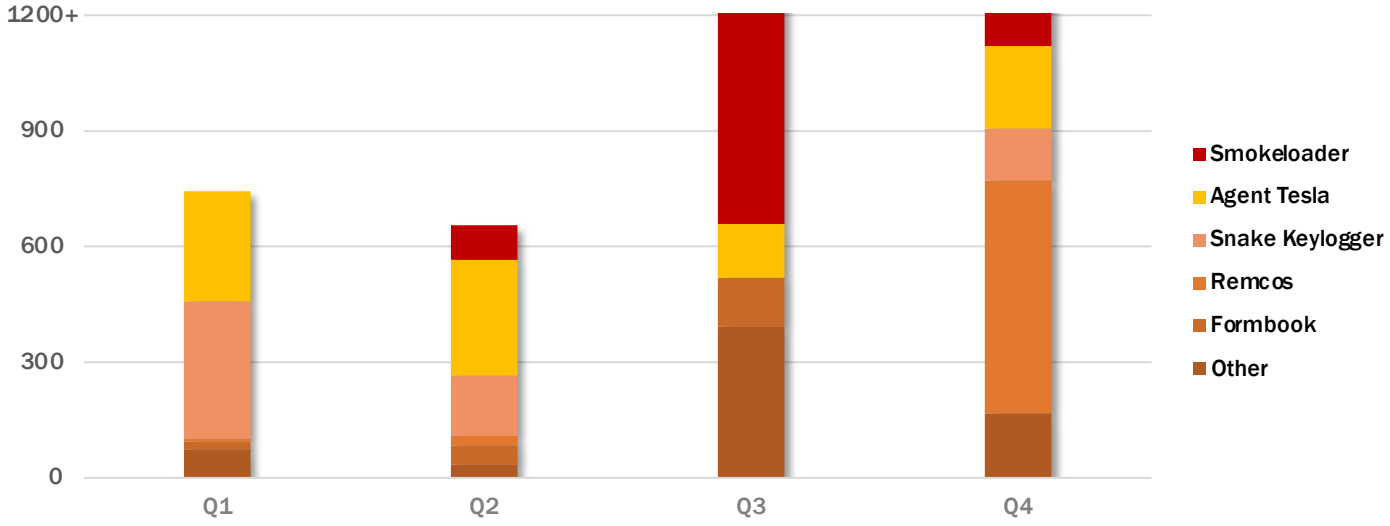
the chart displays top 10 IP addresses (in percent ratio), which were identified as active scanning sources during the reporting period

src	src country	AS NUMBER	AS NAME	%
80.85.141.227	Netherlands	AS204601	Zomro B.V.	3,29%
51.159.196.227	France	AS12876	SCALEWAY S.A.S	3,16%
46.101.146.130	Germany	AS14061	DigitalOcean LLC	2,51%
216.244.66.240	United State	AS23033	Wowrack.com	2,1%
185.174.137.26	Swedish	AS210644	AEZA INTERNATIONAL LTD	1,6%
5.255.231.33	russian federation	AS13238	Yandex LLC	1,38%
62.210.101.204	France	AS12876	SCALEWAY S.A.S	1,14%
212.29.233.209	Israel	AS1680	Cellcom Fixed Line Communication L.P	0,94%
89.208.107.26	Netherlands	AS210644	AEZA INTERNATIONAL LTD	0,59%
61.219.11.155	Republic of China	AS3462	Data Communication Business Group	0,35%

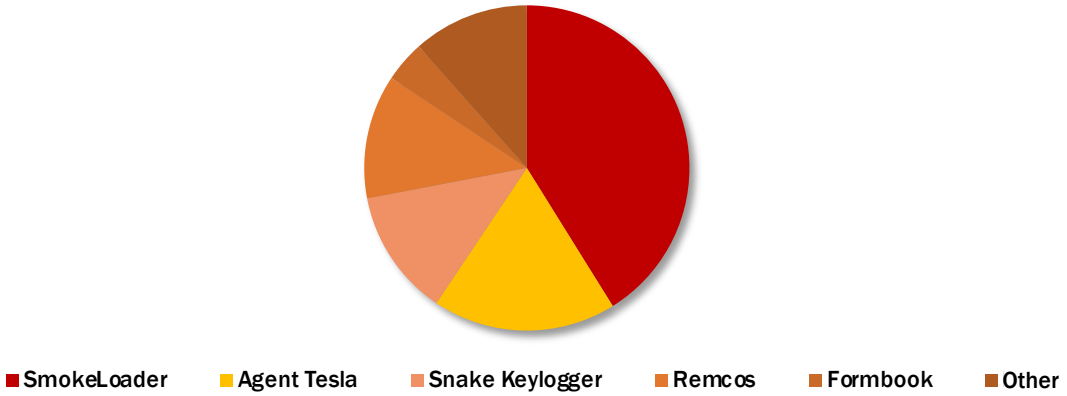
1 516 861

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

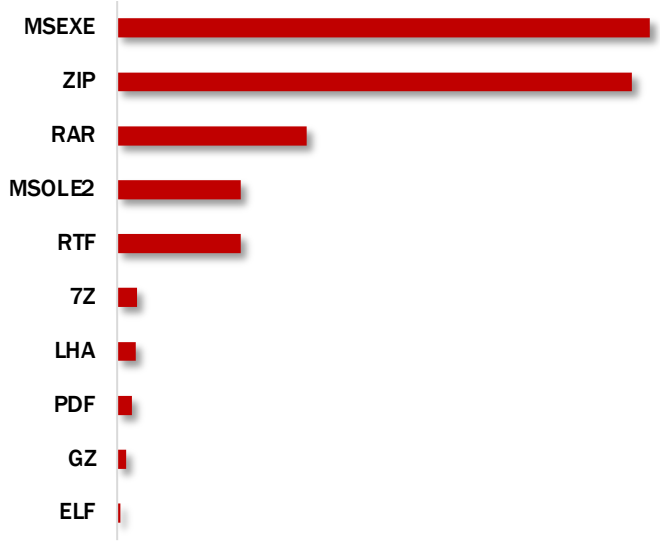
Timechart of IS events of category "02 Malicious code" by malware families



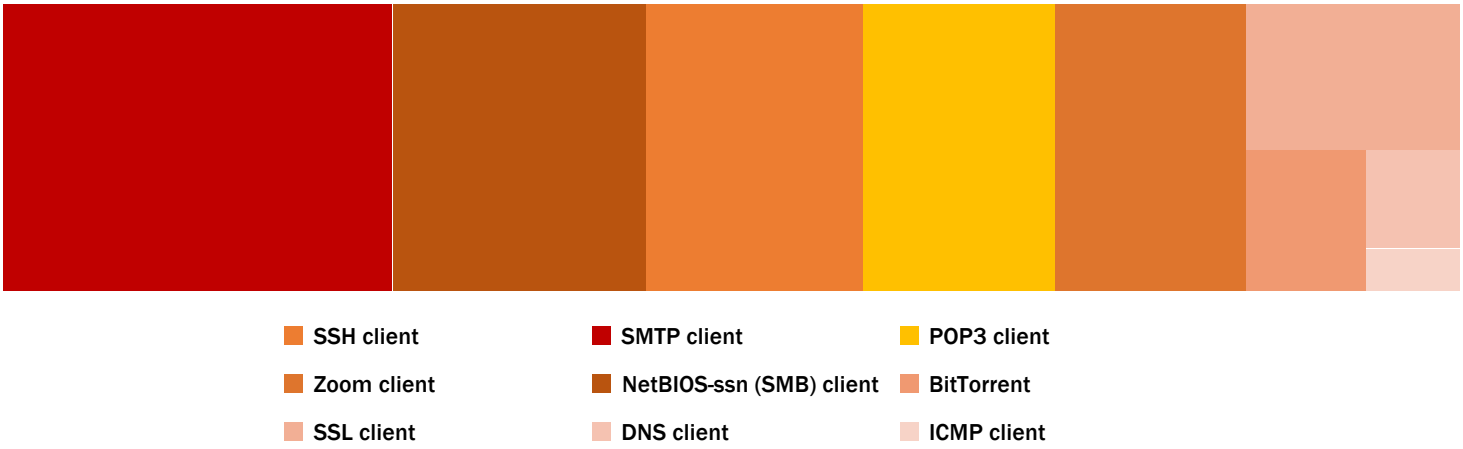
Distribution of malware families detected in IS events of category "02 Malicious code"



By malware files extentions

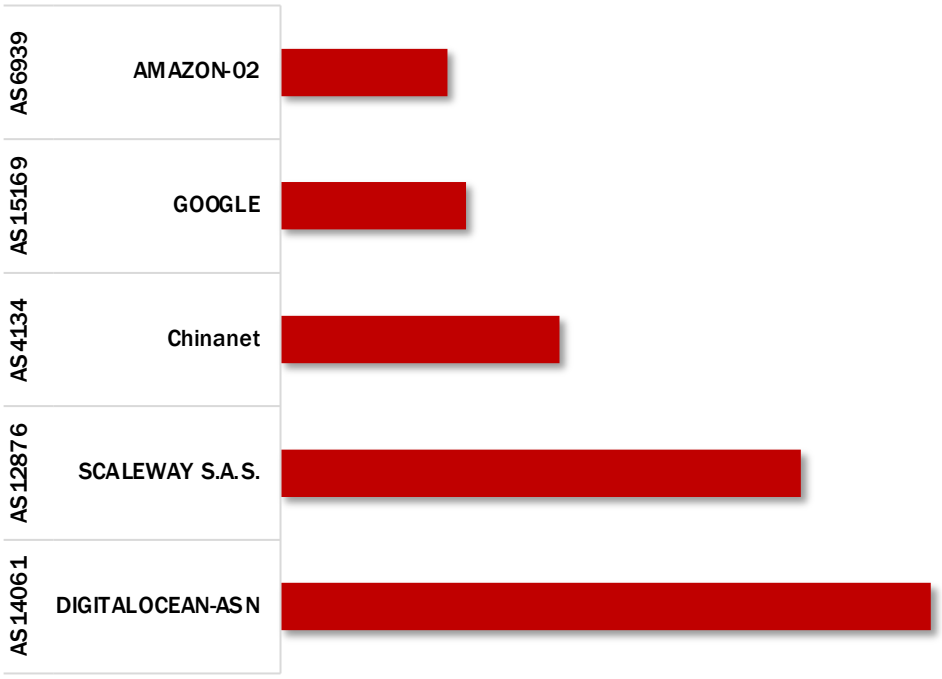


By associated software, used as a malware distribution channel



Top 5 source ASN

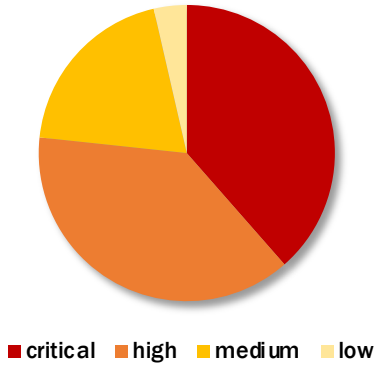
the chart displays top 5 ASN (in percent ratio), the dominant number of IP addresses of which were identified as active malware distribution sources during the reporting period



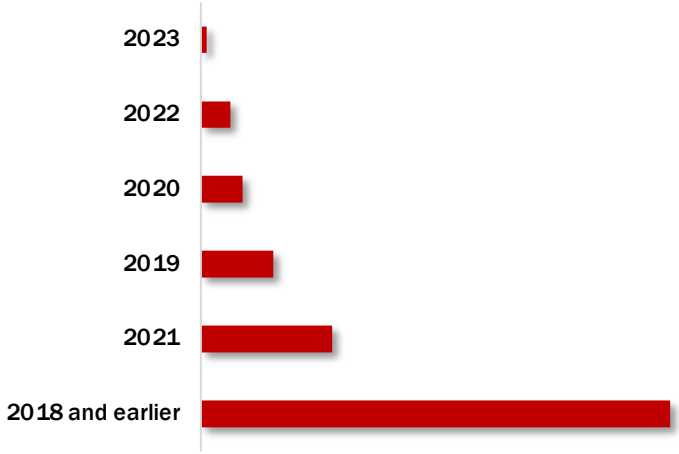
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts of all priorities targeted on the networks of cyber protection objects and the realisation of cyber threats with the aim of detecting software vulnerabilities,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

Qualitative rating by CVSS Base Score

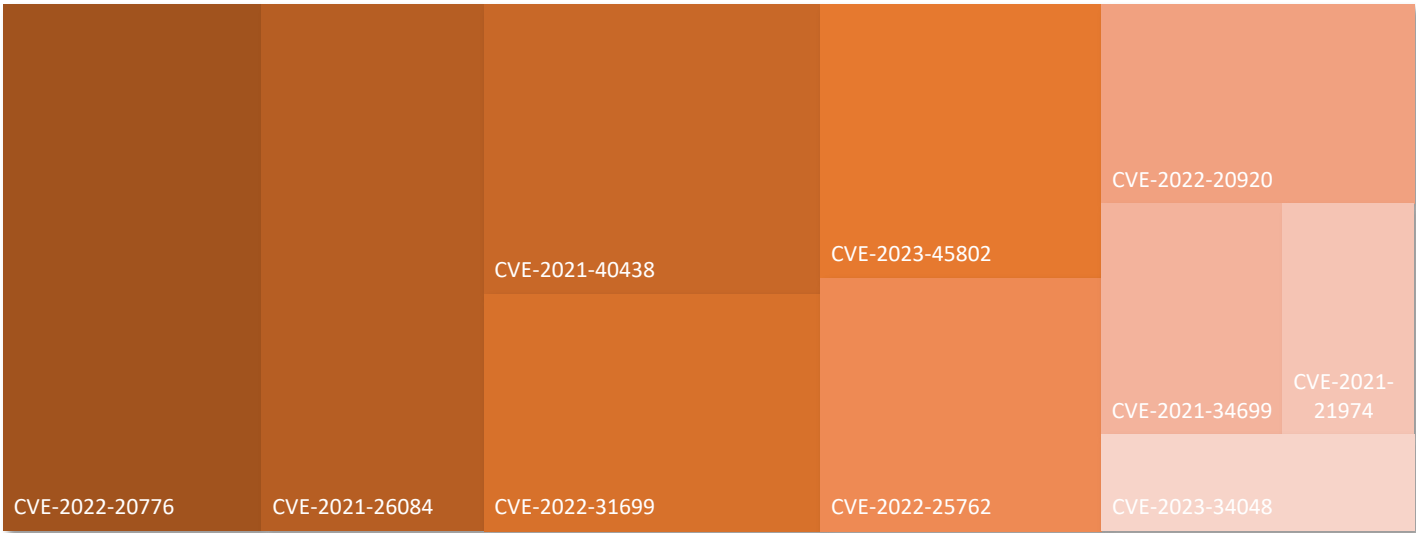
according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in CVSSv3.1 specification



Top exploited vulnerabilities by year



Top 10 exploited vulnerabilities



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