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

2022 Q3

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

The State Service for Special Communications and Information Protection of Ukraine (SSSCIP) constantly fixates an increase in the number of cyber incidents and cyber attacks targeted on state information resources and critical information infrastructure objects. Since the beginning of the war, the trend towards an increase in the number of cyber attacks has been continuing.

During the 3rd quarter of 2022, 24 billion events were processed with the Vulnerability Detection and Cyber Incidents/Cyber Attacks System. The number of registered and processed cyber incidents increased from 64 to 115.

The main goal of hackers remains cyberespionage, disruption of the availability of state information services and even destruction of information systems with the help of wipers. In the 3rd quarter of 2022, we saw a significant increase in the activity of hacker groups in the distribution of malware, which includes both data stealing and data destruction programs.
Comparing to the statistics for the 2nd quarter of 2022, the number of critical IS events increased by 3,8 times and the number of critical registered cyber incidents increased by 128%.

Comparing to the 1st and 2nd quarters of 2022, the number of critical IS events originating from russian IP addresses increased by 35 times. Also, comparing to the 2nd quarter of 2022, the number of IS events related to active scanning and originating from russian IP addresses increased approximately by 2 times.
These IPs were actively used for carrying out cyber attacks on Ukrainian information resources and propagating fake information, related to discrediting the state bodies during the russian-Ukrainian war.

Currently, the largest number of critical IS events is associated with source IP addresses from the USA. However, automatically determined geolocation of source IP addresses does not necessarily mean their attribution to the identified location.

By attribution, the absolute majority of registered cyber incidents is related to hacker groups funded by the russian federation government. In particular, these are UAC-0010 (Gamaredon) and others, mentioned in the report.

In the 3rd quarter of 2022, the main targets of hackers from the russian federation were the Ukrainian financial and commercial, as well as the government and local authorities sectors. Most information security events can be associated with APT groups and hacktivists activities.

MONITORING STATISTICS

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

9 k
FPS

22.1 k
hosts

7 Tb
input data received

6 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

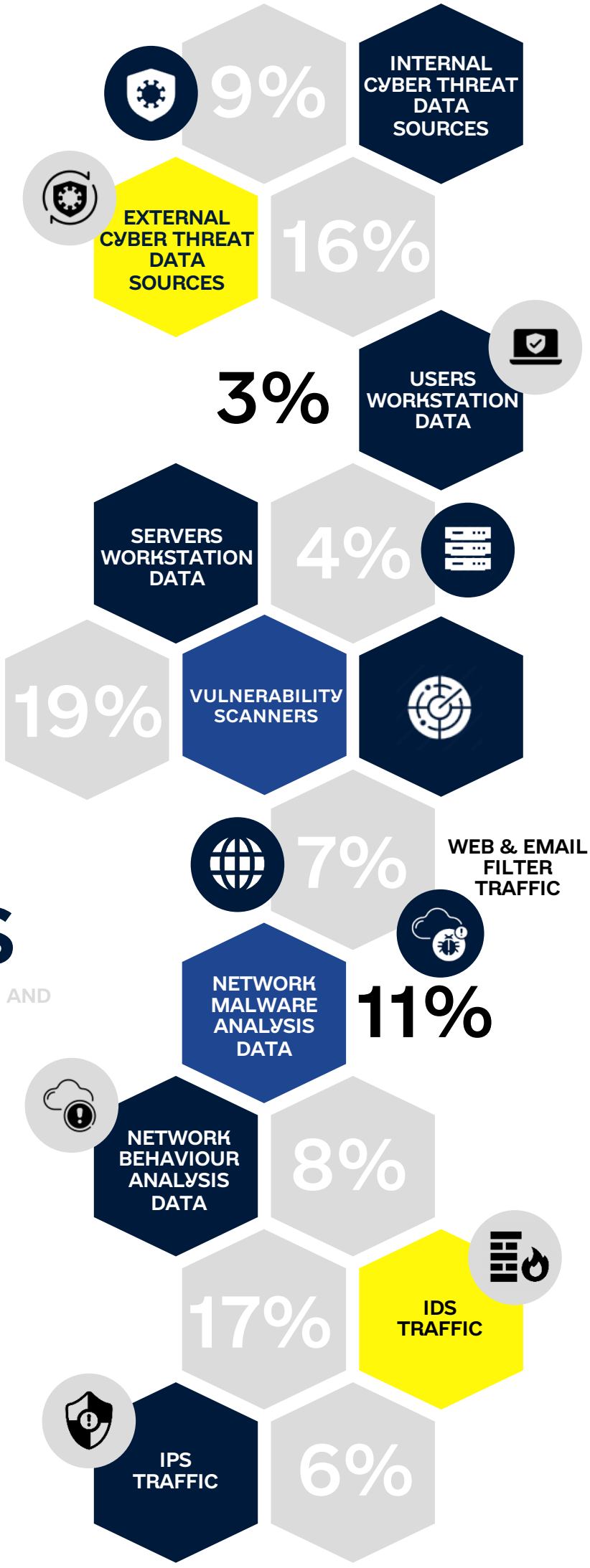
detected suspicious IS events
during primary analysis

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

DATA SOURCES

MAIN SOURCES OF DATA COLLECTION AND CONTEXTUALIZATION



2022(Q3)

IS EVENTS MONITORING

QUANTITATIVE INDICATORS OF COLLECTED AND PROCESSED DATA

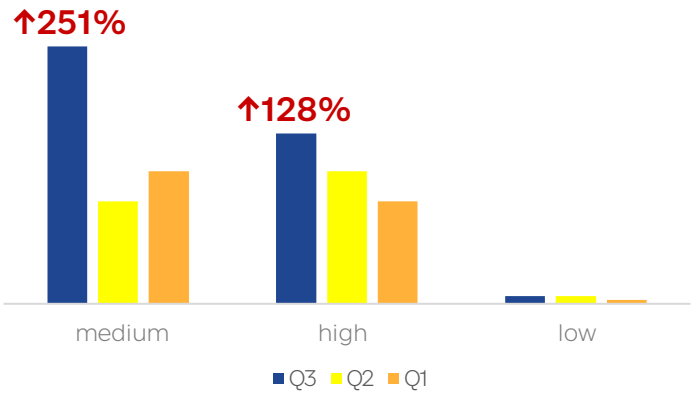
displayed according to **Incident Classification Taxonomy**

approved by the National Coordination Center for Cybersecurity under the National Security and Defense Council of Ukraine

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

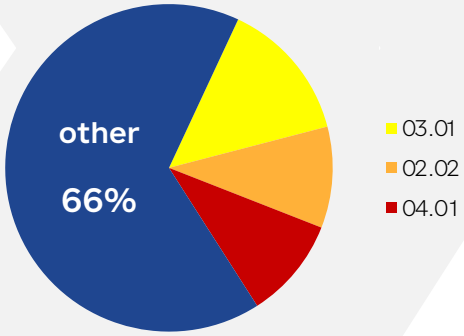
cyber incidents by criticality

presented chart displays statistical information for the reporting period, obtained by analyzing registered cyber security incidents according to the internal criticality rating scale, according to which incidents can be classified by this parameter



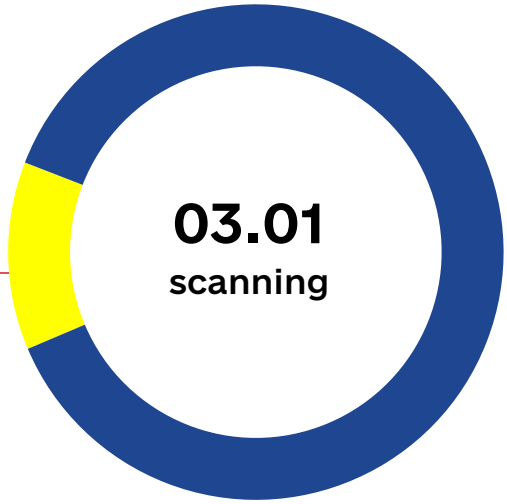
statistics of cyber incidents types

which dominate over other types of cyber incidents in percentage terms during the 3rd quarter of 2022



14%

percentage ratio of IS events of this type to the total number of the other types of incident activity detections, described in Incident Classification Taxonomy, for the reporting period



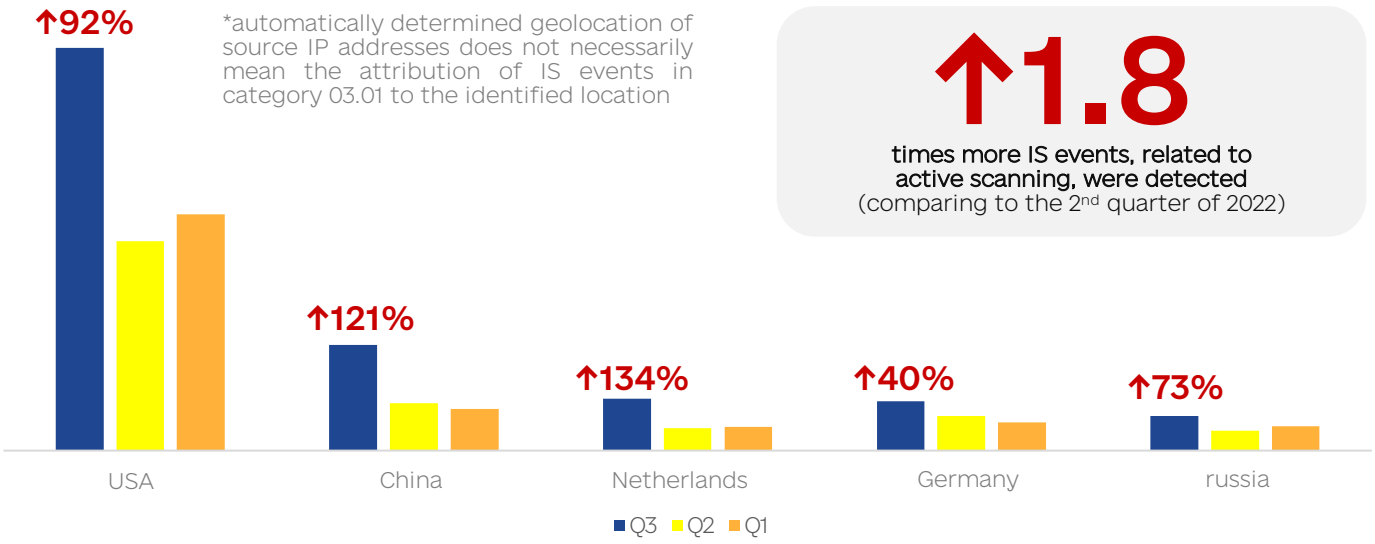
gathering of information about systems or networks

by source IP addresses geolocation*

*automatically determined geolocation of source IP addresses does not necessarily mean the attribution of IS events in category 03.01 to the identified location

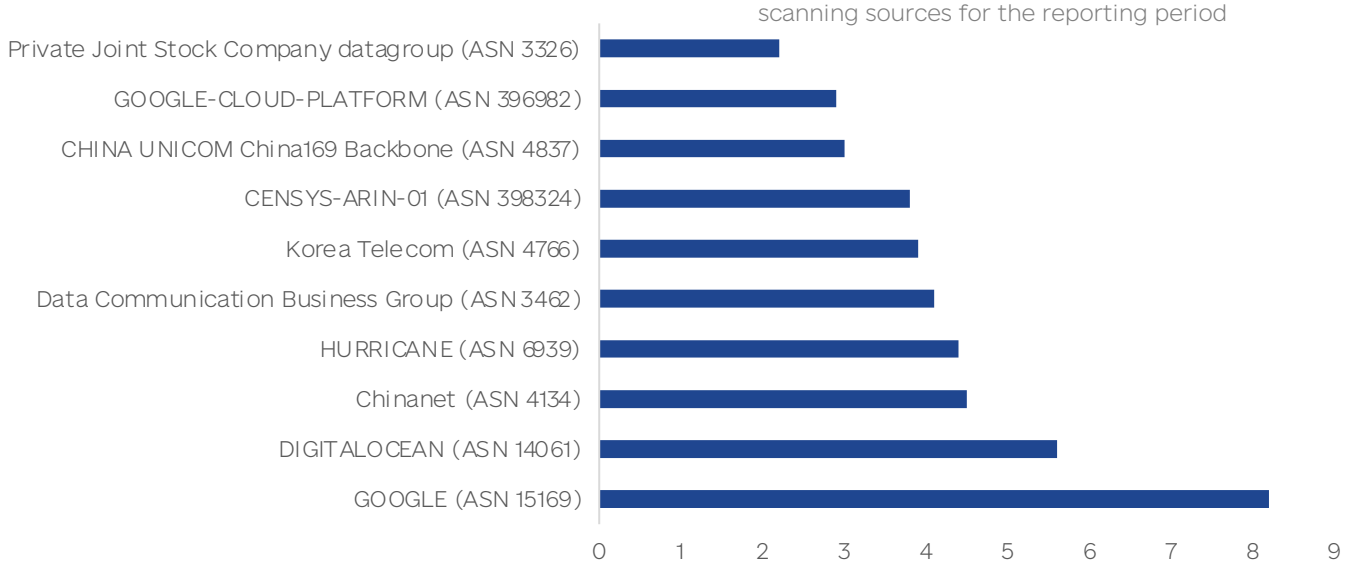
↑1.8

times more IS events, related to active scanning, were detected (comparing to the 2nd quarter of 2022)



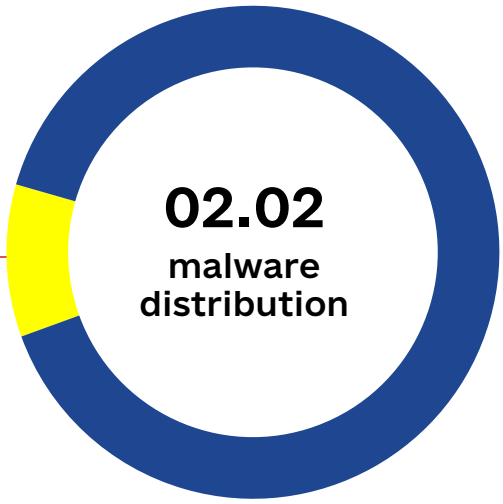
top 10 ASN by source IP-addresses

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



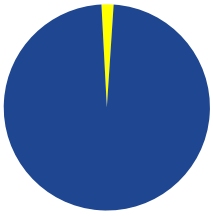
10%

percentage ratio of IS events of this type to the total number of the other types of incident activity detections, described in Incident Classification Taxonomy, for the reporting period



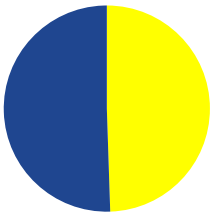
62 314

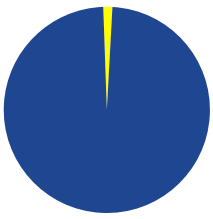
unique suspicious files were automatically detected
by The Subsystems of the
Vulnerability Detection and Cyber Incidents/Cyber Attacks Response System



network events
from the Telemetry Collection Subsystem,
that identify malware distribution
by HTTP, SMTP, POP3, IMAP protocols

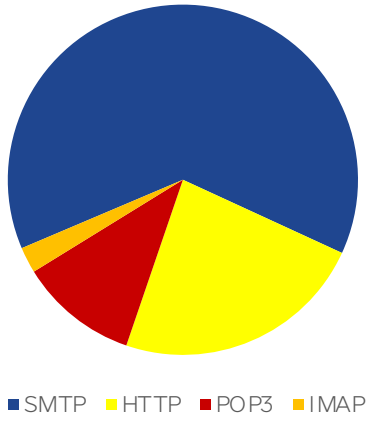
alerts
from the Endpoint Detection and Response Subsystem
on the level of user and server workstations
about detecting malicious activity on them



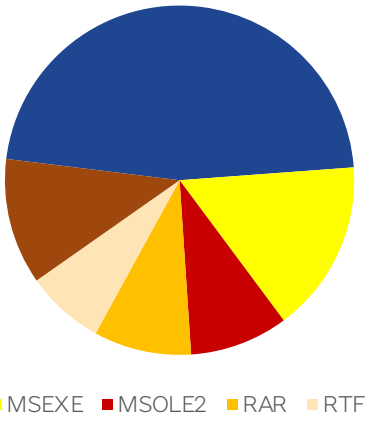


alerts
from email security gateways
about sending malware, identified
during incoming/outcoming traffic filtration

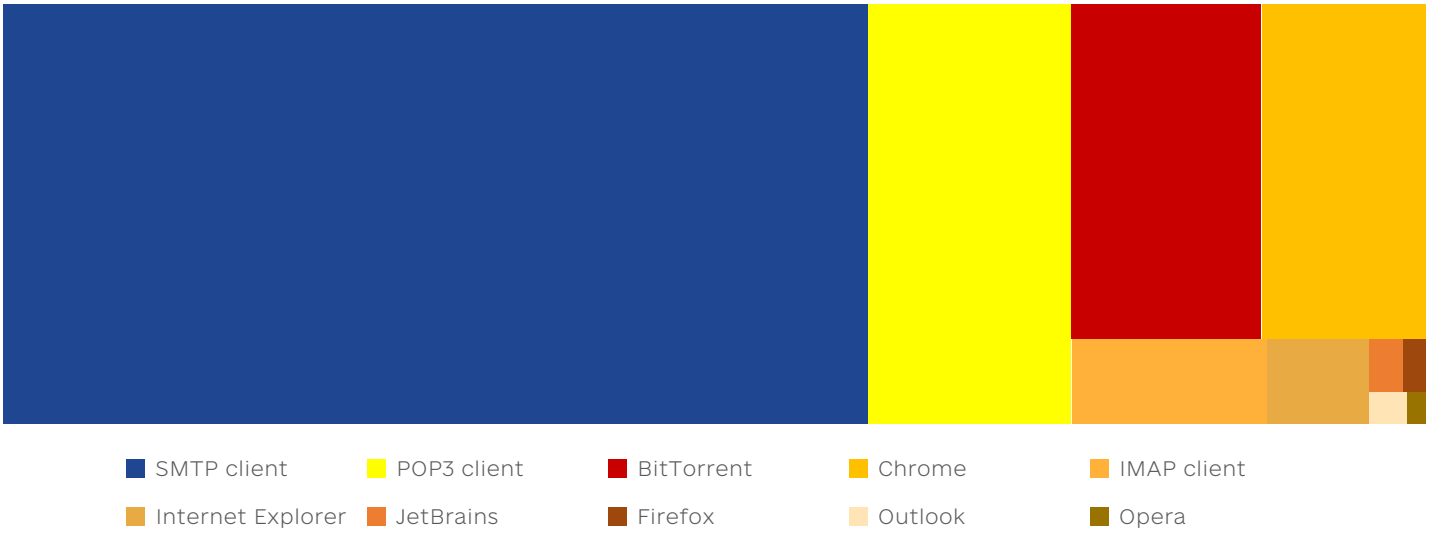
by malware distribution protocol



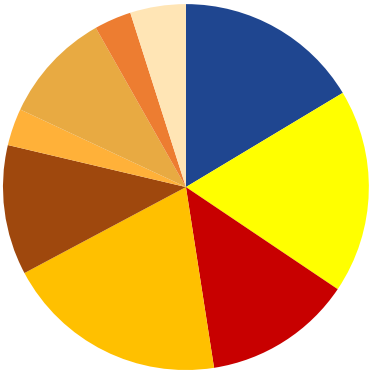
by malware extention



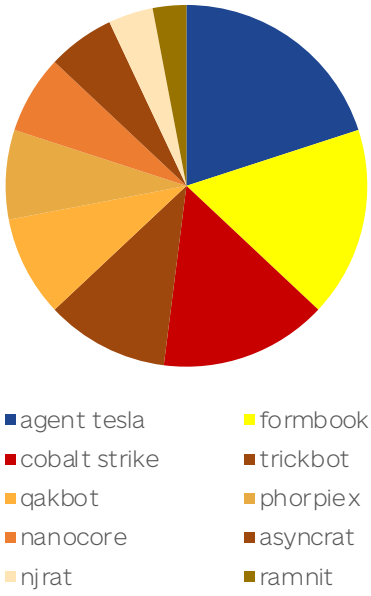
by associated software, used as a malware distribution channel



by malware type



by malware family



10%

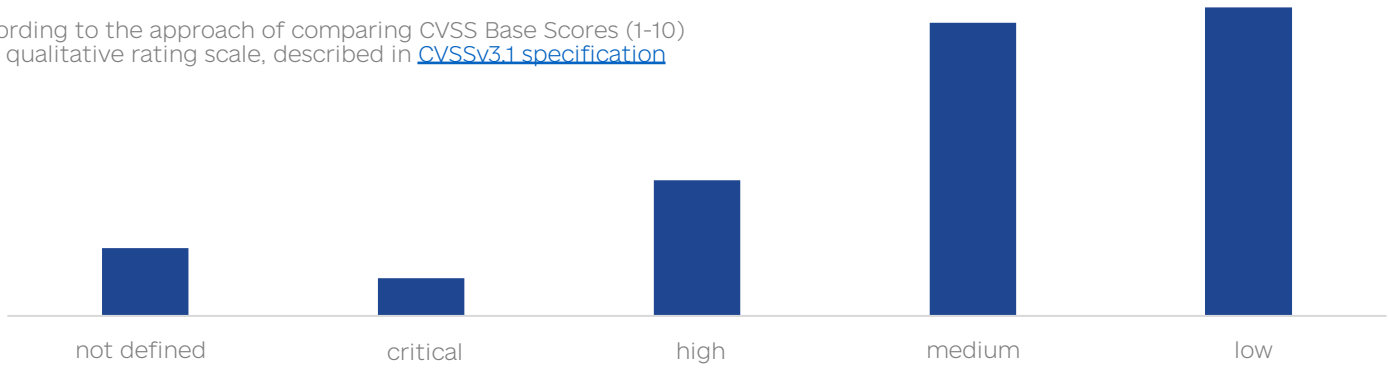
percentage ratio of IS events of this type to the total number of the other types of incident activity detections, described in Incident Classification Taxonomy, for the reporting period

an intrusion attempt using a vulnerability in a system, component, or network

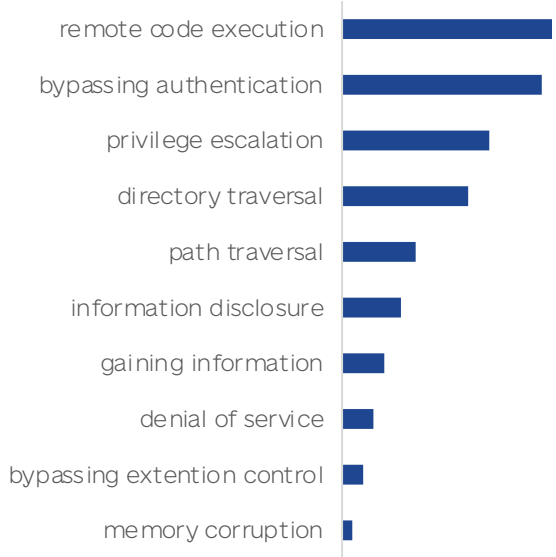
presented charts display statistical information for the reporting period, obtained by analysing IS events, which were triggered by intrusion attempts targeted on the networks of cyber protection objects and the realization of cyber threats with the aim of detecting software vulnerabilities, finding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

qualitative rating by CVSS Base Score

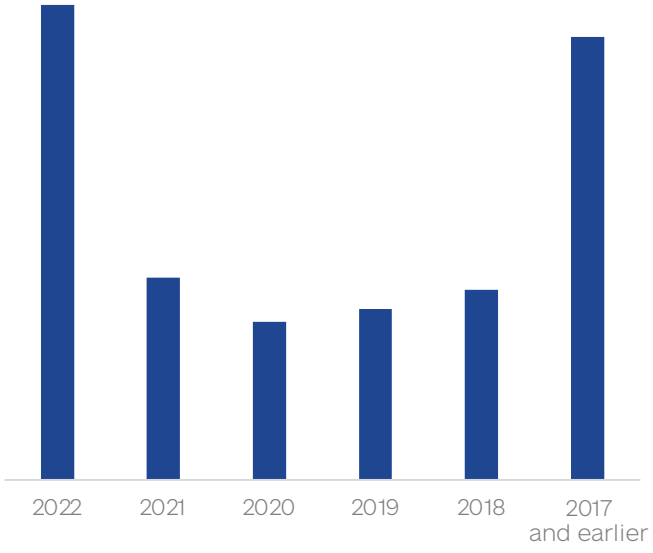
according to the approach of comparing CVSS Base Scores (1-10) to a qualitative rating scale, described in CVSSv3.1 specification



most exploited vulnerabilities by category



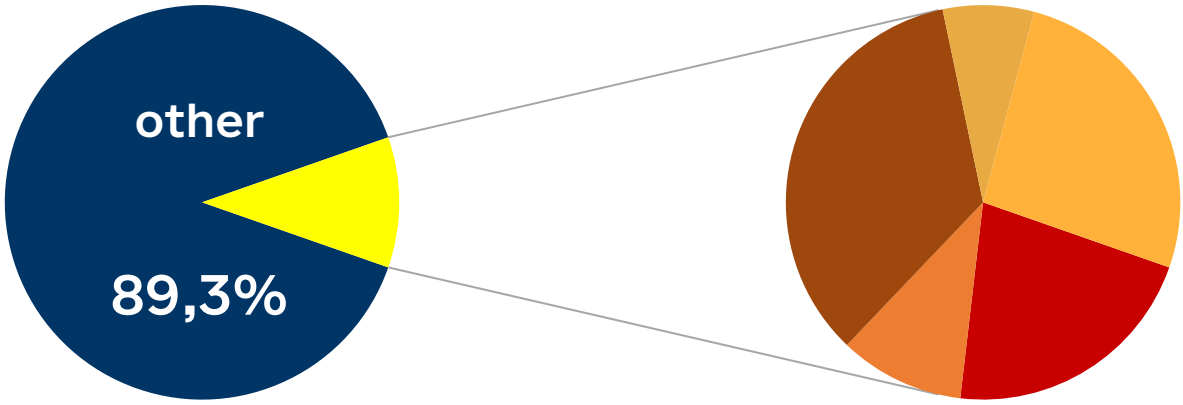
most exploited vulnerabilities by year



relevant vulnerabilities

The following list of current software vulnerabilities is not complete and describes CVEs that have been documented by known cyber threat intelligence expert groups and that continue to be actively exploited in order to gain unauthorized access or privileged control.

The chart shows the % of detected activity in the network traffic of cyber protection objects (potentially related to the exploitation of the list of CVEs described below), to the total number of activity detections, related to all identified vulnerability identifiers, during the reporting period.



CVE-2022-33874

Successful exploitation of the *SSH Login Handler* component in vulnerable versions of Fortinet products, can be initiated remotely. It can result in **unauthenticated remote arbitrary code execution.**
CVSS: 9.8

CVE-2022-33872

Successful exploitation of the *Telnet Login Handler* component in vulnerable versions of Fortinet products, can be initiated remotely. It can result in **unauthenticated remote arbitrary code execution.**
CVSS: 9.8

CVE-2022-41352

Successful exploitation of the *cpio utility of content filter Amavis* that belongs to Zimbra Collaboration products, can result in **web-shell placing.**
CVSS: 9.8

CVE-2021-44228

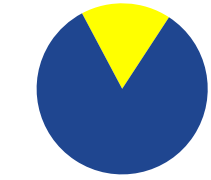
Successful exploitation of Log4Shell vulnerability, that is associated with *Apache Log4j library*, can result in **unauthenticated remote arbitrary code execution**
CVSS: 10

CVE-2022-30190

Successful exploitation of the vulnerability in *Microsoft Windows Support Diagnostic Tool (MSDT)*, which is a part of Microsoft's troubleshooting pack, can result in **remote arbitrary code execution with the privileges of the calling application**. The vulnerability, better known as "Follina", affects most supported Windows OS (also server-side).
CVSS: 7.8

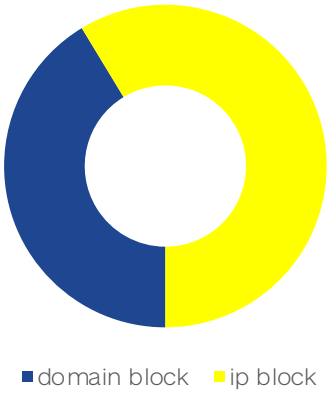
EMAIL SECURITY GATEWAY

83%
blocked in automatic mode



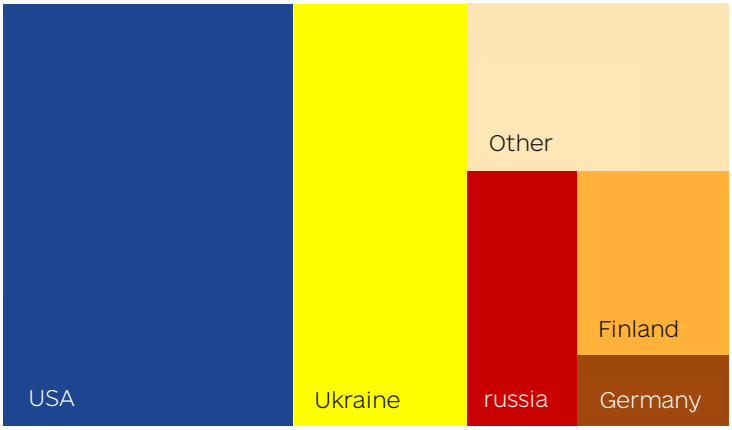
1.7 mln
emails received and analysed during reporting period

Sender Validation failure reason

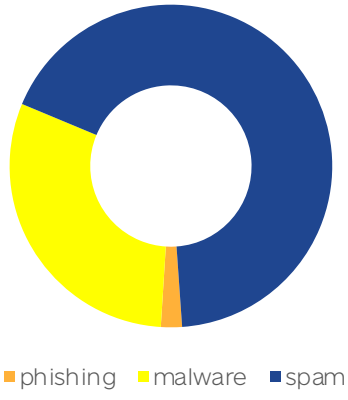


Sender Authentication failure reason

Sender Threat category (by country)



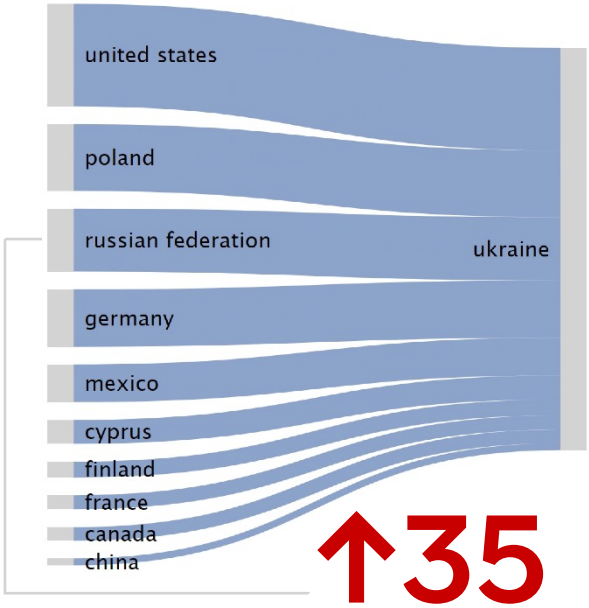
Sender Threat category

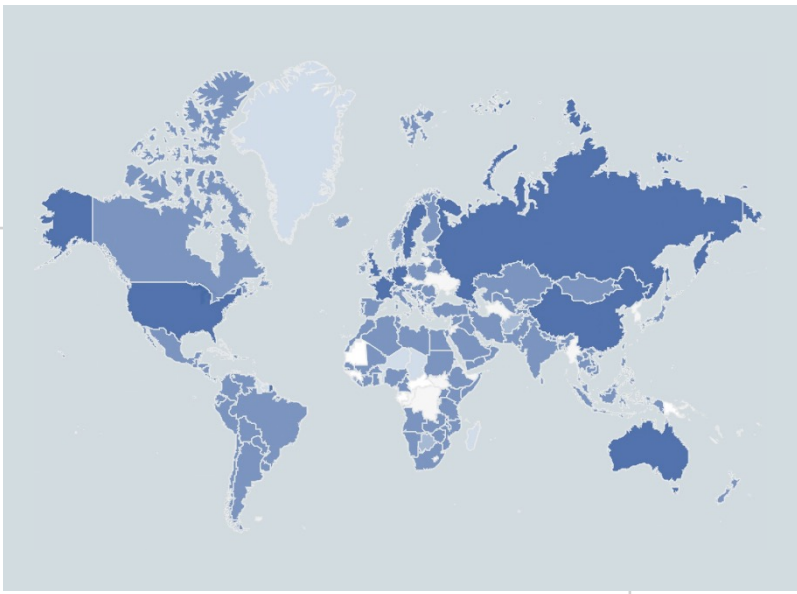


GEOGRAPHY OF DETECTIONS

OF CRITICAL INFORMATION SECURITY EVENTS *

*automatically determined geolocation of source IP addresses of critical IS events does not necessarily mean their attribution to the identified location





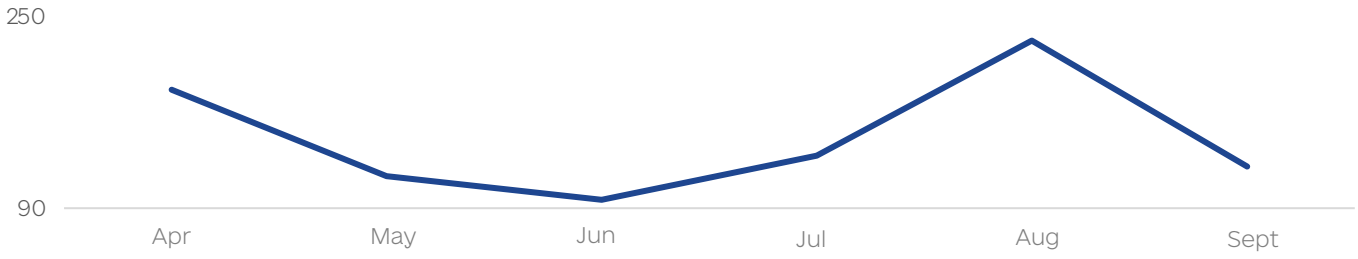
↑35

times more critical IS events were detected, that originate from russian IP addresses
(comparing to the 1st and 2nd quarters of 2022)

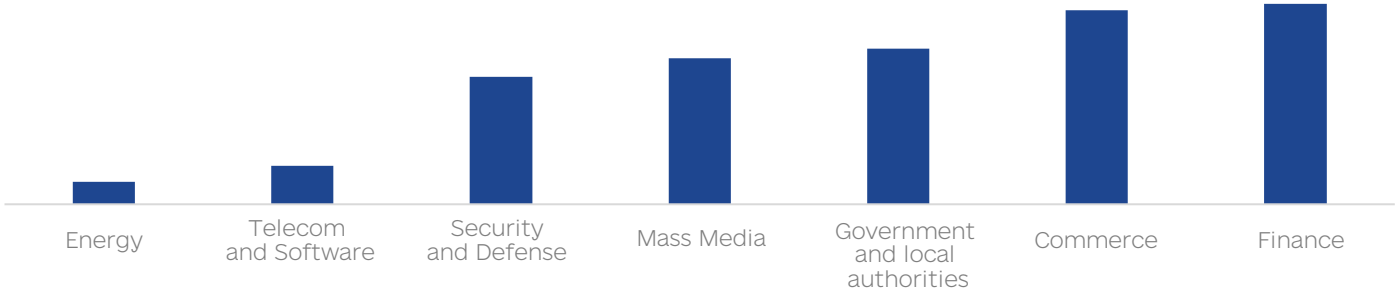
↑3,8

times more critical IS events were detected
(comparing to the 2nd quarter of 2022)

dynamics of russian hacker groups activity during Q2, Q3



dynamics of russian hacker groups activity during Q3 by sectors



THREAT ACTORS ACTIVITY

the following list describes current hacker groups targeting Ukraine information resources, whose activity identifiers were detected in the networks of cyber protection objects during the reporting period

UAC-0010

Related names: Gamaredon, Armageddon, PrimitiveBear
Category: Nation State Sponsored
Location: russia
First Reference: 2013-2014

Read more: Cyber attack of UAC-0010 (CERT-UA#4634,4648)
Cyber attack of UAC-0010 (CERT-UA#4434)

UAC-0100

Related names: -
Potential Category: Financial Crime
Potential Location: -
First Reference: Apr, 2022

Read more: Cyber attack of UAC-0100 (CERT-UA#4964)

UAC-0056

Related names: Lorec53, SaintBear, GraphSteal, GrimPlant
Potential Category: Nation State Sponsored
Potential Location: russia
First Reference: Jul, 2021

Read more: Cyber attack of UAC-0056 (CERT-UA#4545)
Cyber attack of UAC-0056 (CERT-UA#4293)

UAC-0097

Related vulnerability: CVE-2018-6882
Threat Category: Cyber espionage
Potential Location: -
First Reference: Apr, 2022

Read more: Cyber attack of UAC-0097 (CERT-UA#4461)

UAC-0120

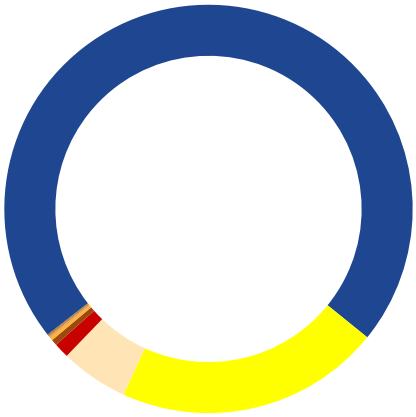
Related Malware: AgentTesla
Threat Category: Cyber espionage
Potential Location: -
First Reference: Aug, 2022

Read more: Cyber attack with AgentTesla usage (CERT-UA#5252)

MITRE ATT&CK MAPPING

attack surface

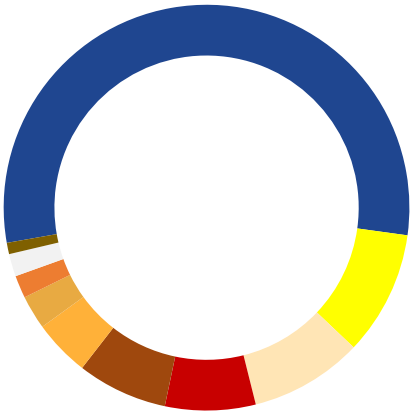
statistics on identified tactics/techniques (according to the MITRE ATT&CK knowledge base) associated with a set of detected and processed IoCs that were used at different stages of the life cycle of cyber attacks which occurred during the reporting period



- T1566 [Phishing]
- T1110 [Brute Force]
- T1090 [Proxy]
- T1498 [Network Denial of Service]
- T1568 [Dynamic Resolution]
- T1071 [Application Layer Protocol]
- T1584 [Compromise Infrastructure]
- T1583 [Acquire Infrastructure]
- T1190 [Exploit Public-Facing Application]
- T1210 [Exploitation of Remote Services]

detect surface

statistics on identified tactics/techniques (according to the MITRE ATT&CK knowledge base) associated with a set of detected and processed IoCs that were used at different stages of the life cycle of cyber attacks which occurred during the reporting period and on the fact of which cyber incidents were registered



- T1071 [Application Layer Protocol]
- T1204 [User Execution]
- E1133 [External Remote Services]
- T1566 [Phishing]
- T1598 [Phishing for information]
- T1498 [Network Denial of Service]
- T1190 [Exploit Public-Facing Application]
- T1078 [Valid Accounts]
- T1565 [Data Manipulation]
- T1110 [Brute Force]

METHODOLOGICAL RECOMMENDATIONS

FOR INCREASING THE LEVEL OF CYBER SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Methodological recommendations for increasing the level of cyber security of critical information infrastructure were developed in accordance with sub-clause 1 of part two and clause 3 of part three of Article 8 of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", paragraph two of part one of Article 3, clauses 85, 86 and 88 of part one of Article 14 of the Law of Ukraine "On the State Service for Special Communications and Information Protection of Ukraine", paragraph two of sub-clause 1 of clause 3 of the Regulation on the Administration of the State Service for Special Communications and Information Protection of Ukraine, approved by the Resolution of the Cabinet of Ministers of Ukraine, September 3, 2014, № 411 and General requirements for cyber security of critical infrastructure objects, approved by the Resolution of the Cabinet of Ministers of Ukraine, June 19, 2019, № 518 in order to increase the level of cyber security of critical information infrastructure.

The Recommendations were developed taking into consideration the Framework for Improving Critical Infrastructure Cybersecurity, issued in 2014 and updated by the National Institute of Standards and Technology of the United States of America in 2018.

The Recommendations do not establish legal norms and are voluntary for use.

The Recommendations describe a general approach to ensuring cyber security that allows to:

- carry out an analysis and provide a description of the current cyber security state of critical information infrastructure objects;
- describe the target cyber security state of critical information infrastructure objects;
- identify and determine priorities, the level of implementation of cyber security measures in the context of continuous and repetitive process of risk management in the field of cyber security of critical information infrastructure objects;
- assess progress in achieving the target cyber security state of critical information infrastructure objects;
- ensure communication between entities that are directly on the critical information infrastructure objects and with entities that can be considered as organization's partners in terms of risk management in cyber security field.

The Recommendations consist of 3 main parts:

➢ systems (taxonomies) of cyber seacurity measures;

➢ levels of implementation of cyber security measures;

➢ cyber security profile.

The approach which is defined in the Recommendations is not the only one for cyber security risk management, as critical information infrastructure objects, belonging to different sectors of such infrastructure, may have either the same or various risks – specific threats, different vulnerabilities, unique acceptable risk levels. The approach for ensuring cyber security state depends on the method of implementation of cyber security measures, which are outlined in the Recommendations.

Decree of the SSSCIP Administration About the adoption of Methodological recommendations for increasing the level of cyber security of critical information infrastructure

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