CYBER INCIDENT RESPONSE OPERATIONS CENTRE OF THE STATE CYBER PROTECTION CENTRE OF THE STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE

2024

ANNUAL REPORT

VULNERABILITY DETECTION AND CYBER INCIDENT/CYBER ATTACK RESPONSE SYSTEM

TLP: CLEAR

VULNERABILITY DETECTION AND CYBER INCIDENT/CYBER ATTACK RESPONSE SYSTEM

Refers to a set of software and 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 entities and may have negative impact on their sustainable functioning.

SUBSYSTEM OF CYBER INCIDENT RESPONSE OPERATIONS CENTRE

Refers to the central component of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System that provides:

- Centralised management of all subsystems within the Vulnerability Detection and Cyber Incident/Cyber Attack 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 Incident Response Operations Centre detects malicious activity as well as system and network anomalies in cyber protection entities 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.

CONTENTS

INTRODUCTION

The 2024 report provides a detailed description of the results of the operation of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System in accordance with the Cabinet of Ministers of Ukraine's Resolution No. 1295 of December 23, 2020, which outlines the necessity of creating and operating such a system as part of the country's defense against cyber threats.

The Vulnerability Detection and Cyber Incident/Cyber Attack Response System is an essential tool for ensuring the security and stability of Ukraine's information space. Throughout 2024, the system carried out continuous monitoring of the cyberspace. As a result, a number of cyber incidents and cyber attacks were detected, and corresponding measures were taken by specialists at the Cyber Incident Response Operations Centre (CIROC) to respond to the detected incidents and attacks.

This report presents statistical data and key events that occurred during 2024, as well as describes the clusters of cyber threats and the actions taken to counter cyber incidents and cyber attacks.

💡 NOTE

This report is based on the statistical data of the Cyber Incident Response Operations Centre of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System from January 1, 2024, to December 31, 2024, inclusive.

KEY FINDINGS

KEY FINDINGS

In 2024, with the help of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System, hundreds of billions of telemetry events were processed, and nearly 3 millions of information security events were recorded. This was achieved through constant monitoring of activity in the ICS using network threat detection tools, analysis of endpoint protection data, and integration of threat intelligence data to identify potential cyber incidents and cyber attacks on cyber protection entities.

Particular attention was given to 28 thousands of critical information security events that required immediate intervention by analysts of the Cyber Incident Response Operations Centre.

During the analysis of these events, 1,042 cyber incidents were identified and processed. The majority of these incidents involved the spread of malware. The primary goal of such attacks was to gain remote access to information systems for cyber espionage or financial theft.

1 Attackers are using increasingly sophisticated attack methods, leveraging legitimate services and tools, which makes detection and response more challenging at the network and endpoint levels.

2 The use of compromised accounts and the distribution of malware via email are among the most common methods attackers use to gain initial access.

3 The most active cyber threat clusters in 2024 were UAC-0010, UAC-0006 and UAC-0050 according to the classification of Ukraine's Computer Emergency Response Team CERT-UA.

MONITORING OVERVIEW

MONITORING STATISTICS

DESCRIPTION OF ORGANIZATIONAL STRUCTURE, TEAMS, TECHNOLOGIES AND TOOLS

During 2024, 9 new organizations were added to the Telemetry Collection Subsystem (NDR), which received 10 sets of network monitoring sensors. 35 organizations were added to the Endpoint Protection Subsystem (EDR), thus more than 28,000 workstations and servers are monitored by the Vulnerability Detection System. 38 organizations were added to the Attack Surface Management (ASM) service, which is 10 organizations more than the previous year.

In total, 13 new organizations were added to the Vulnerability Detection and Cyber Incident/Cyber Attack Response System in 2024, 9 being from the government sector and 4 from the defense sector.

Technologies and tools

Cybersecurity tools

Telemetry Collection Subsystem	Endpoint Protection Subsystem	Attack Surface Management
NDR	**EDR**	**ASM**
Organizations added: **67 +9**	Organizations added: **58 +35**	Organizations added: **38 +10**
Sensors installed: **69 +10**	Hosts protected: **28,000+**	Assets scanned: **1,200+**

Sectors and organizations

Cyber protection entities

81 +9	**2**	**7 +4**
Government	Energy	Defense

MONITORING STATISTICS

QUANTITATIVE METRICS OF COLLECTED AND PROCESSED DATA

The Vulnerability Detection and Cyber Incident/Cyber Attack Response System has processed hundreds of billions of telemetry events and recorded almost 3 million information security events.

The main sources of data are the ICS protection tools of cyber protection entities, namely: tools for network threat detection (NDR) – sensors of the telemetry collection subsystem; tools for analyzing data from workstations and servers (EDR) – sensors of the endpoint protection subsystem; as well as threat intelligence data on compromised accounts and other indicators of compromise (TI).

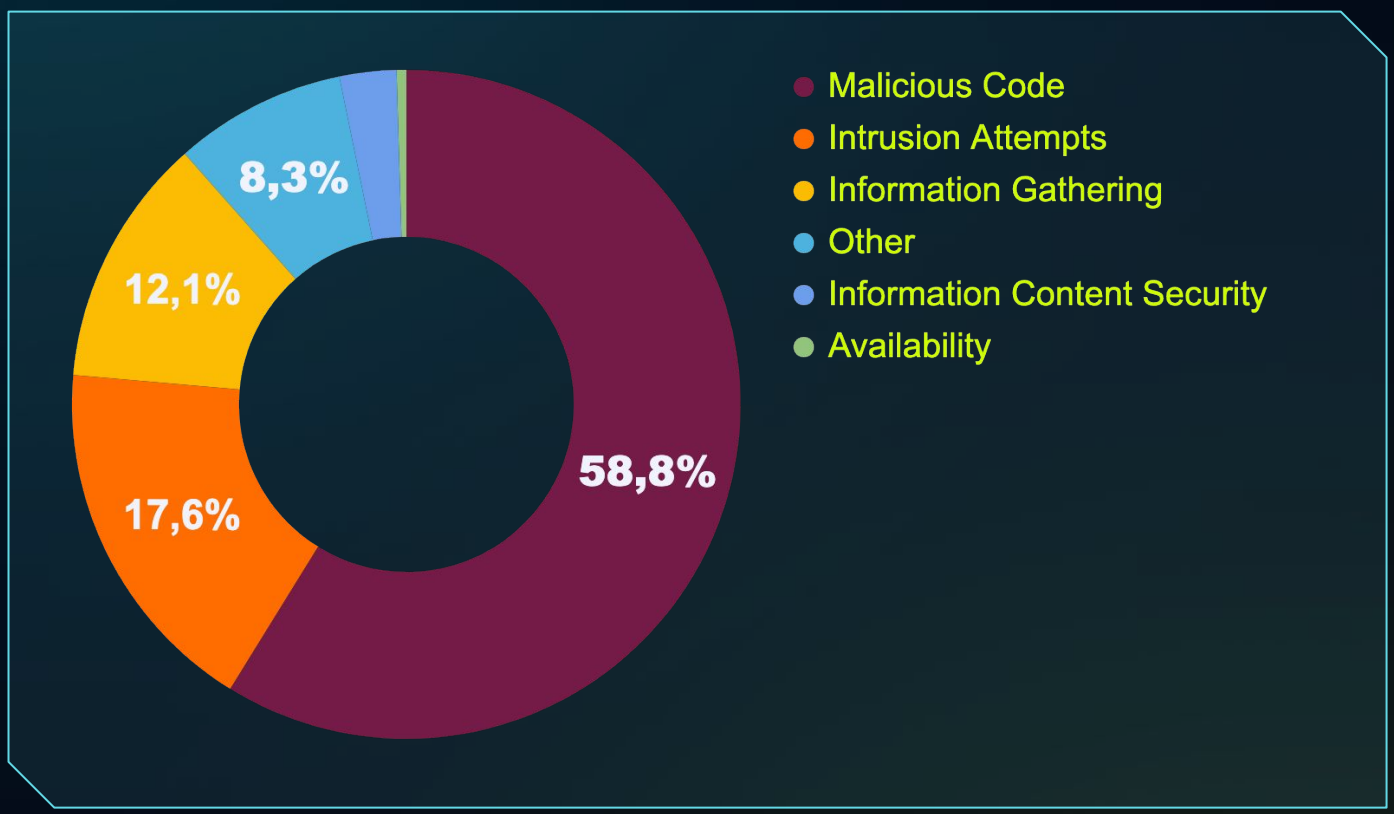
NOTE

It is worth noting that the values of the monitoring metrics are significantly different compared to last year because we have modernised network telemetry collection tools, implemented a SOAR, and applied generative artificial intelligence to automate the detection and processing of potential cyber incidents and cyber attacks. This has reduced the load on the SIEM system and CIROC analysts; however, the number of detected cyber incidents and cyber attacks remains almost at the same level as last year.

MONITORING STATISTICS

QUANTITATIVE METRICS OF COLLECTED AND PROCESSED DATA

Statistics are presented according to the List of Cyber Incident Categories approved by the National Cybersecurity Coordination Centre under the National Security and Defense Council of Ukraine



Among the detected information security events, the main part, namely 58.8%, is related to Malicious Code. Intrusion Attempts account for 17.6%, while Information Gathering accounts for 12.1%. Other events account for 8.3%, Information Content Security and Availability account for 2.7% and 0.5%, respectively.

This data on the types of events processed by the CIROC during the reporting period helps to identify priority areas for strengthening cyber defense measures.

CYBER INCIDENTS OVERVIEW

CYBER INCIDENTS AND CYBER ATTACKS

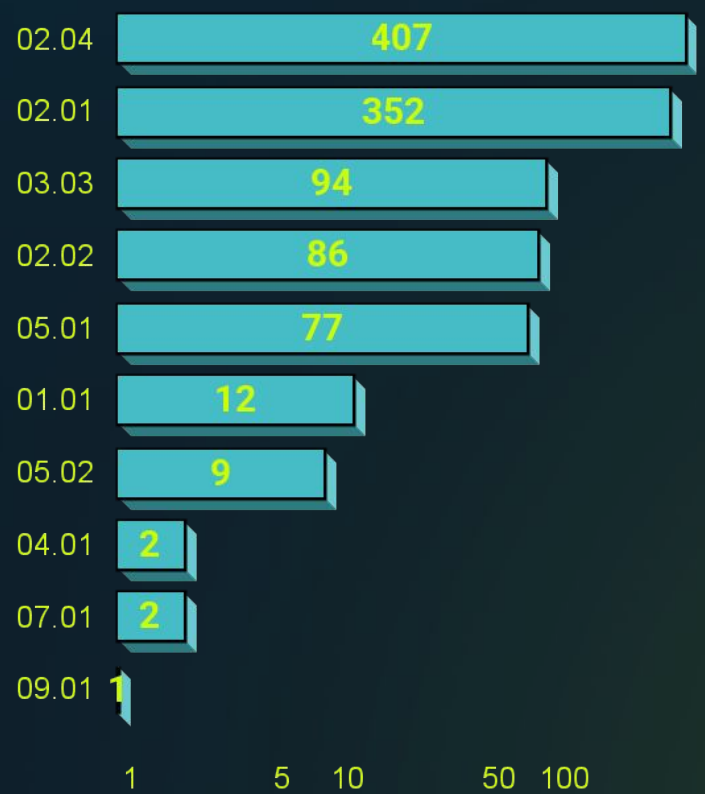
QUANTITATIVE METRICS OF PROCESSED CYBER INCIDENTS

Breakdown by type of source

1,042 Cyber incidents registered and processed by the CIROC analysts in 2024

249	739	54
EDR	NDR	TI

Breakdown by type of cyber incident



More than 90% of the analyzed cyber incidents involved government organizations.

By classification, most cyber incidents are of the type "02.04 Malicious connection", which refers to attempts to connect from/to a URL or IP address associated with a known malware, such as C&C, or a distribution resource for components associated with the activity of a particular botnet.

CYBER INCIDENTS AND CYBER ATTACKS

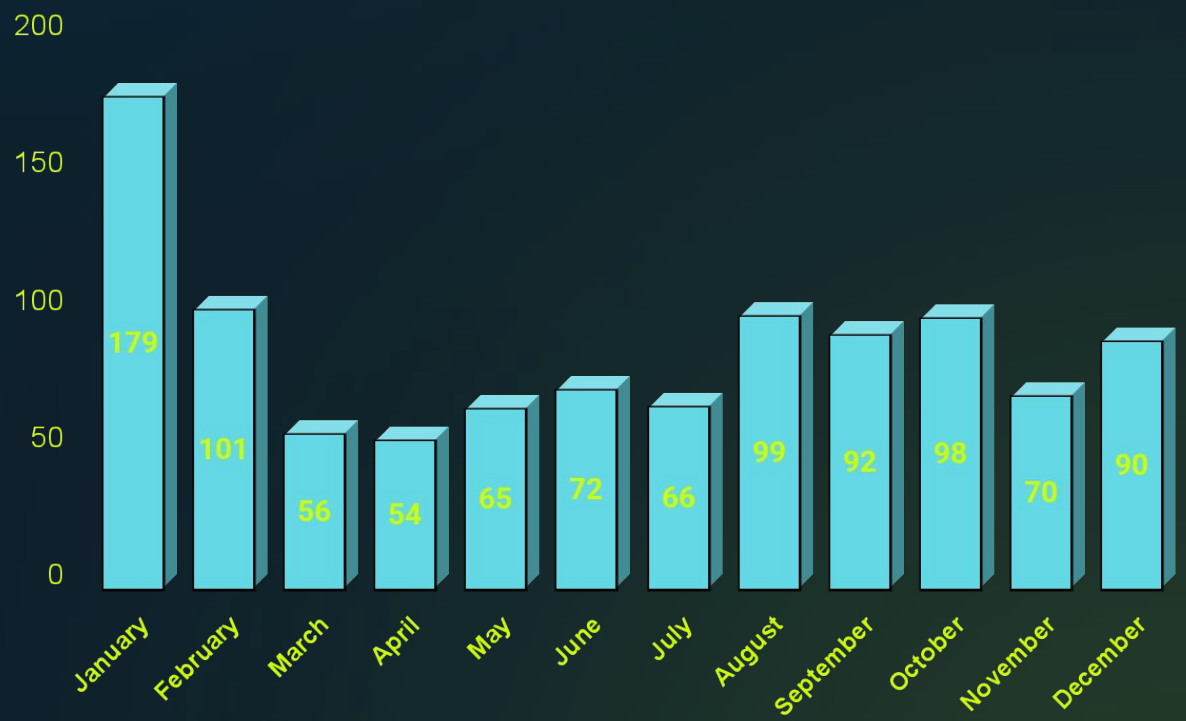
QUANTITATIVE METRICS OF PROCESSED CYBER INCIDENTS

Breakdown of cyber incidents by sector

71 Cyber protection entities suffered cyber attacks and/or cyber incidents during 2024

5	65	1
Military	Government	Energy

Breakdown of cyber incidents by month

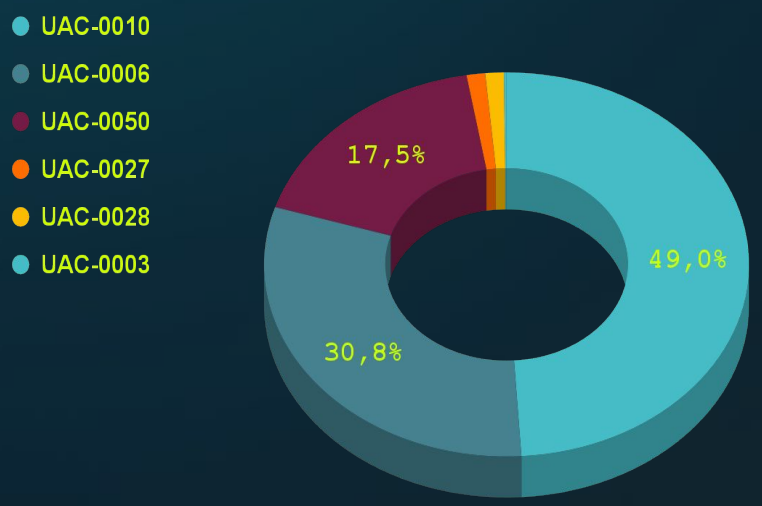


CYBER THREAT OVERVIEW

CYBER THREATS

QUANTITATIVE METRICS OF CYBER THREATS

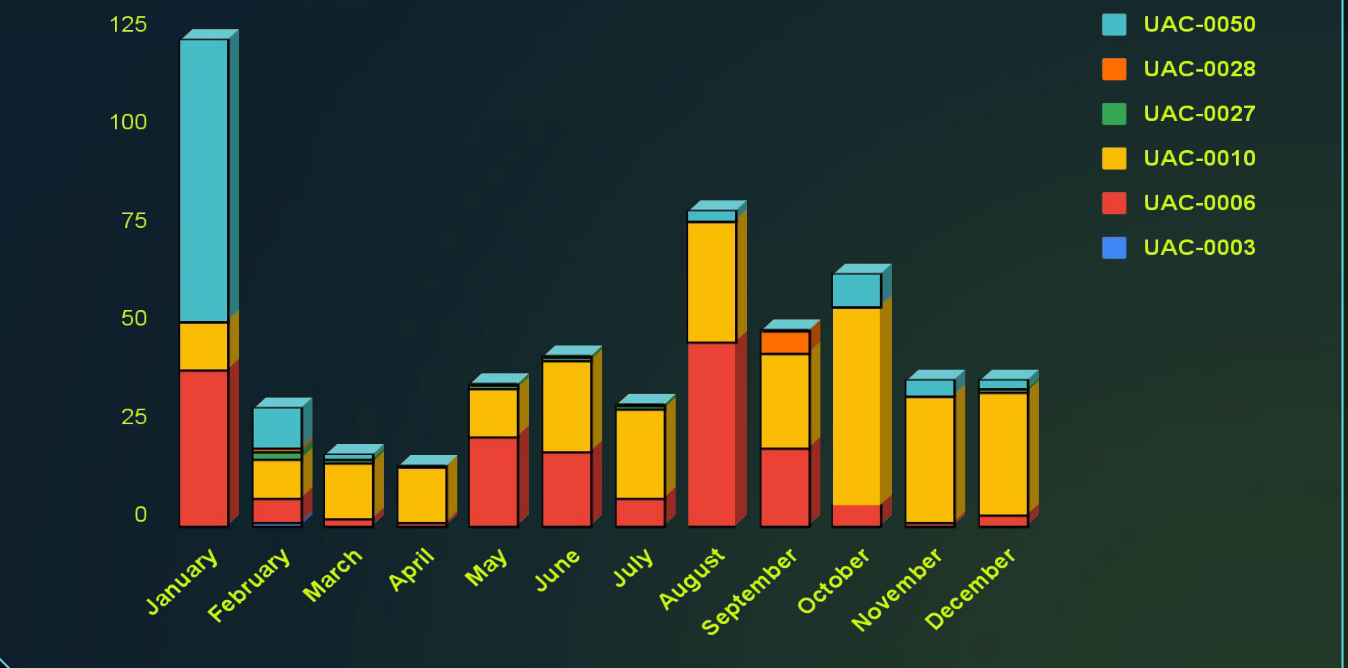
Breakdown of cyber incidents



The most active clusters of cyber threats identified by the Cyber Incident Response Operations Centre in 2024 were **UAC-0010, UAC-0006, and UAC-0050** (according to CERT-UA classification).

The main initial vector of cyberattacks was the distribution of malware via email – **T1566.001** Phishing: Spearphishing Attachment (according to the MITRE ATT&CK classification).

Time distribution of cyber incidents attributed to cyber threats



CYBER THREATS

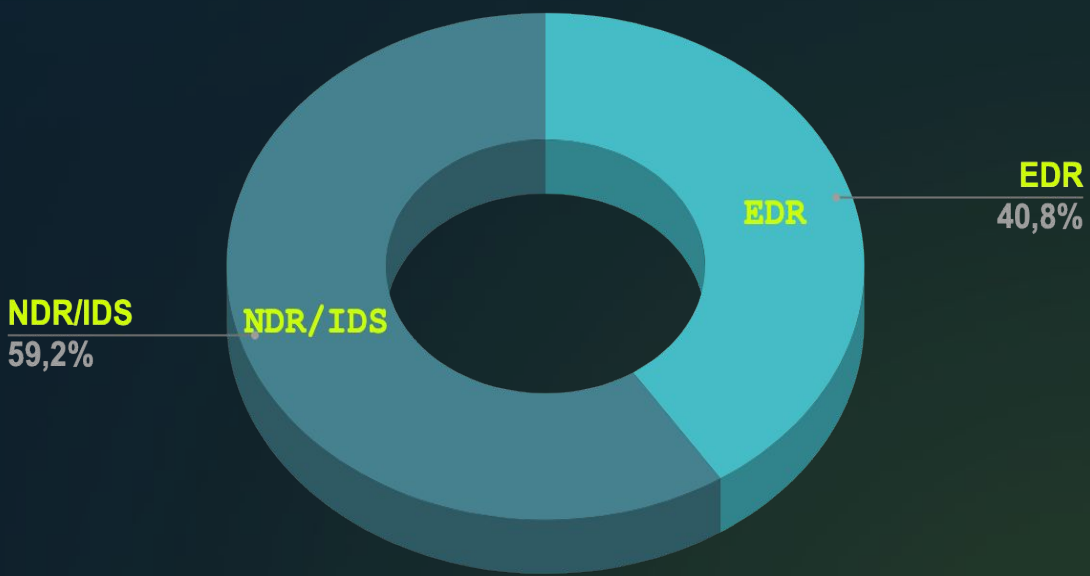
QUANTITATIVE METRICS OF CYBER THREATS

Breakdown of cyber incidents by sector

61 Cyber protection entities experienced cyber attacks or cyber incidents linked to known cyber threat clusters during 2024

5	55	1
Military	Government	Energy

Breakdown by detection source



CYBER THREATS

ACTIVITY OF CYBER THREAT CLUSTERS

UAC-0010 cluster description

Aliases:
Gamaredon, Primitive Bear, Trident Ursa, Aqua Blizzard

Tracked since:
2013

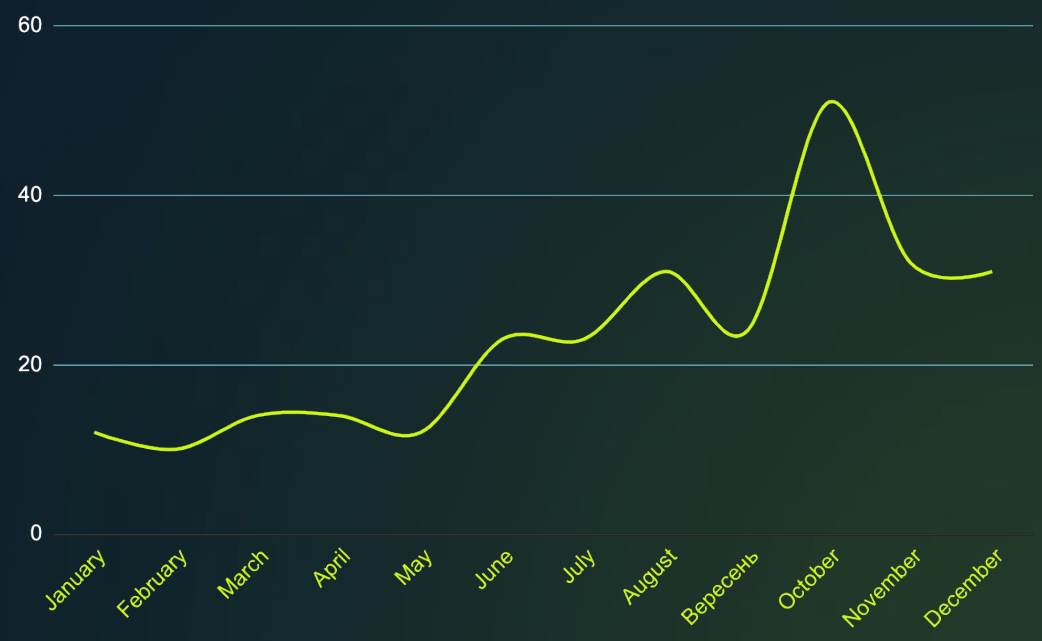
Motivation:
cyber espionage

Targets:
government authorities, defense forces

Throughout the year, CIROC specialists identified 277 cyber incidents attributed to the activity tracked by CERT-UA under identifier UAC-0010. Among the investigated cyber incidents, the primary vector of infection was malware spread via email and USB flash drives.

Summary information of the UAC-0010 group activity is available here: **https://cert.gov.ua/article/5160737**.

UAC-0010 cyber attacks timeline



CYBER THREATS

ACTIVITY OF CYBER THREAT CLUSTERS

UAC-0006 cluster description

Aliases:
unavailable

Tracked since:
2013

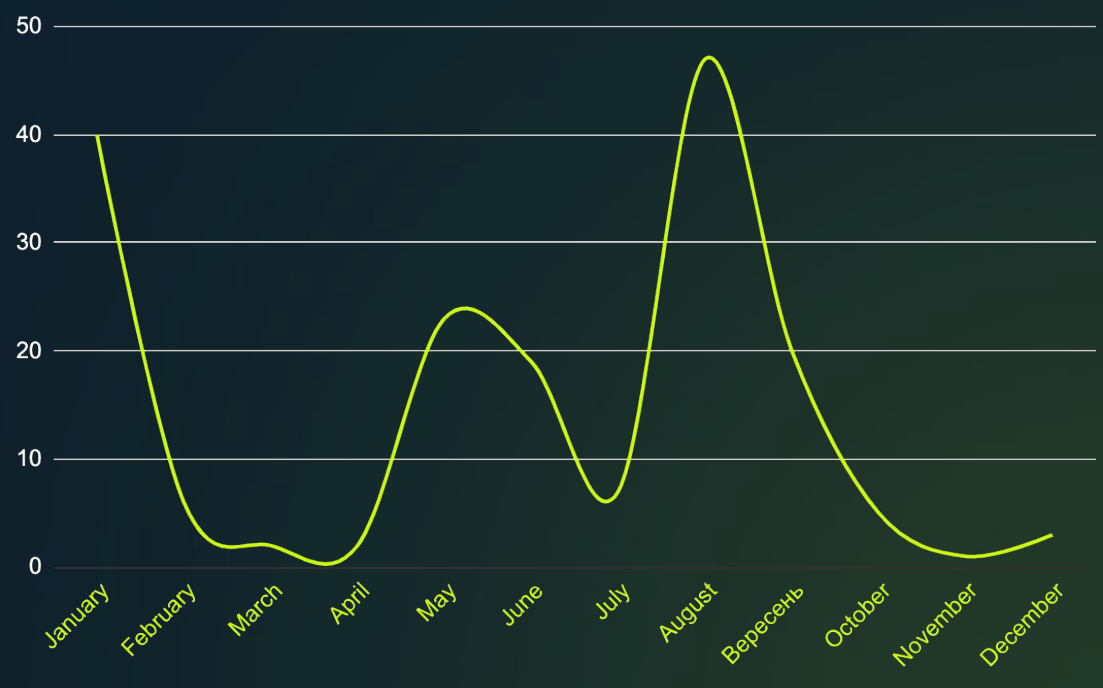
Motivation:
stealing money

Targets:
finance departments

In 2024, CIROC specialists identified 174 cyber incidents attributed to the activity tracked by CERT-UA under identifier UAC-0006. Among the investigated cyber incidents, the most common primary vector of infection was distribution of the SmokeLoader malware via email.

Summary information of the UAC-0006 group activity is available here: **https://cert.gov.ua/article/6276584**.

UAC-0006 cyber attacks timeline



CYBER THREATS

ACTIVITY OF CYBER THREAT CLUSTERS

UAC-0050 cluster description

Aliases:
unavailable

Tracked since:
2020

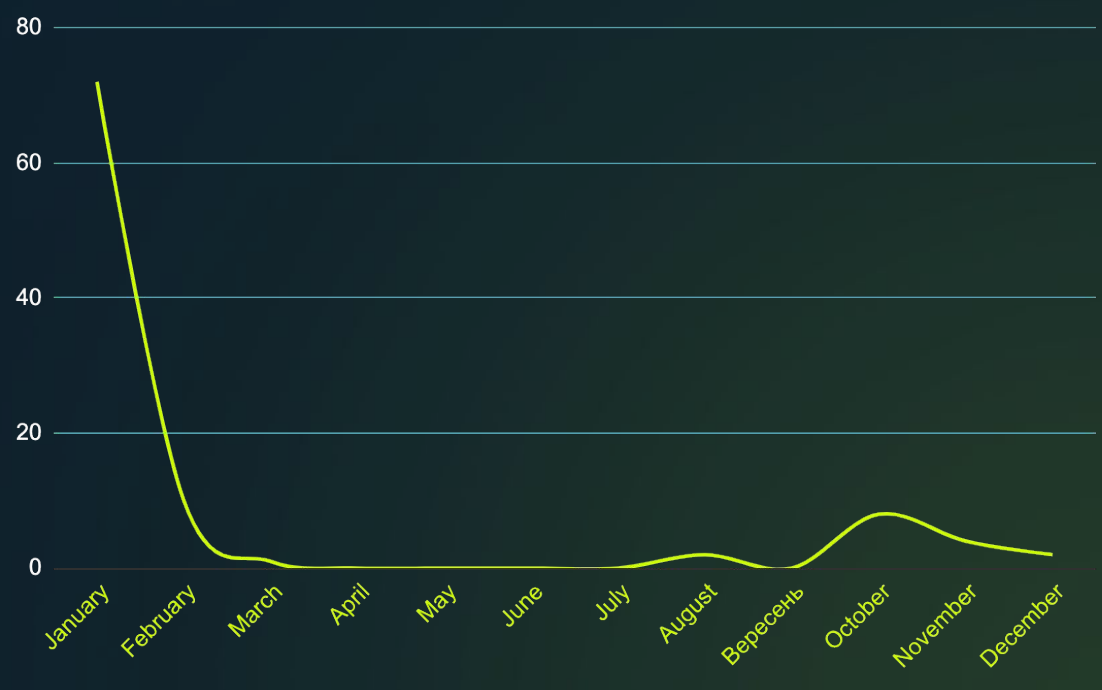
Motivation:
cyber espionage, stealing money, PSYOPS

Targets:
government authorities, defense forces, financial institutions

Throughout the year, CIROC specialists identified 99 cyber incidents attributed to the activity tracked by CERT-UA under identifier UAC-0050. Among the investigated cyber incidents, the primary vector of infection was malware spread via email.

Summary information of the UAC-0050 group activity available here: https://cert.gov.ua/article/6281009.

UAC-0050 cyber attacks timeline



RECOMMENDATIONS

RECOMMENDATIONS

Ensure timely updates of software and hardware	Regularly update your software and apply security patches. Also, ensure that your hardware is not outdated. Monitor the attack surface accessible from the Internet.
Use email protection tools	Be cautious with emails, especially those containing unfamiliar or suspicious attachments or links. Never enter your personal information on suspicious websites.
Use endpoint protection tools	Use antivirus software, update it regularly, and periodically scan your system. Real-time protection can help prevent system compromise. Additionally, avoid installing unwanted programs that could become sources of threats.
Conduct asset inventory and network monitoring	Ensure a complete inventory of all assets, including servers, workstations, mobile devices, and network equipment. Regularly update information about corporate networks, guest Wi-Fi networks, DNS records, and IP addresses. This will enable quick identification and localization of assets in the event of a cyber incident.
Use multi-factor authentication	Use long and complex passwords that consist of a combination of various characters. Enable multi-factor authentication for added protection of your account.
Set up logging	Ensure comprehensive event logging in your infrastructure, including user activity, network connections, changes to configuration files, and access to critical data. A full log volume enables timely detection and response to cyber incidents and cyber attacks.

Also, read the recommendations prepared by the Governmental Computer Emergency Response Team of Ukraine (CERT-UA) available at the following link: https://cert.gov.ua/article/5436463

RECOMMENDATIONS

To enhance the level of cyber protection of your organization's ICS, we recommend utilizing the cybersecurity services available within the Vulnerability Detection and Cyber Incident/Cyber Attack Response System for real-time cyber threat detection and cyber incident management.

NDR	The service involves the installation and configuration of a network sensor to monitor network traffic and detect cyber incidents and cyber attacks. The sensor can be deployed either inside the network or at its perimeter.
EDR	The service provides comprehensive endpoint protection for your organization (personal computers, servers, virtual machines) through the installation and configuration of EDR (Endpoint Detection and Response) technology.
ASM	The service includes scanning public information resources, covering the identification of existing vulnerabilities, potential risks, and attack vectors, as well as providing detailed reports with descriptions of vulnerabilities and other related information.

For contacting the State Cyber Protection Centre about gaining access to the services listed above:

Email: info_scpc@cip.gov.ua

Phone: +38 (044) 281 87 37

RECOMMENDATIONS

The List designed to implement taxonomy as a tool for sharing cyber incident information.

Code xx	Incident category	Code xx	Incident type
01.	Abusive content	01	Spam
02.	Malicious Code	01	Malware infection
		02	Malware distribution
		03	Command & Control (C2)
		04	Malicious connection
03.	Information Gathering	01	Scanning
		02	Sniffing
		03	Phishing
04.	Intrusion Attempts	01	Vulnerability exploitation attempt
		02	Login attempts
05.	Intrusion	01	Account compromise
		02	System compromise
06.	Availability	01	DoS/DDoS
		02	Sabotage
		03	Outage, no malice
07.	Information Content Security	01	Unauthorised access to information
		02	Unauthorised modification of info
08.	Fraud	01	Fraudulent site
09.	Vulnerable	01	Vulnerability
		02	Misconfiguration
10	Other	01	Undetermined incident

Cyber Incident Response Operations Centre

The State Cyber Protection Centre

State Service of Special Communications and Information Protection of Ukraine

e-mail: soc@cip.gov.ua

Phone: +38 (044) 281 87 37