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

2025

H1

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 24/7 monitoring, analysis, and transmission of telemetry data on cyber incidents and cyber attacks that have occurred or are currently occurring at the protected entities and may have negative impact on their stable operation.

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 at the protected entities by analysing the data obtained from network devices (active sensors, firewalls, vulnerability scanners), workstations, servers, authorisation systems, and internal/external sources of cyber threat intelligence.

INTRODUCTION

The report for the first half of 2025 provides a detailed overview of the performance of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System created in accordance with Resolution No. 1295 of the Cabinet of Ministers of Ukraine dated December 23, 2020, which established the necessity for creating and operating of such a system as part of the country's defence 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 the first half of 2025, the System continuously monitored the cyberspace. As a result, a number of cyber incidents and cyber attacks were detected, and corresponding measures were taken by the Cyber Incident Response Operations Centre (CIROC) team to respond to them.

This report presents statistical data and key events that occurred during the first half of 2025, as well as an overview of cyber threat clusters and 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, 2025 to June 30, 2025, inclusive.

KEY FINDINGS

In the first half of 2025, the Vulnerability Detection and Cyber Incident/Cyber Attack Response System processed billions of telemetry events and detected millions of information security events.

These results were achieved through continuous monitoring of activity in information and communication systems, utilizing network threat detection tools, analysing data from endpoint protection systems, and leveraging cyber threat intelligence.

As a result of analysing the detected events, 535 cyber incidents were identified and processed. Most of these were associated with malware infection. The primary goal of such attacks was typically to gain unauthorized remote access to information systems for the purpose of cyber espionage or financial theft.

1 Adversaries are increasingly employing combined attack vectors, integrating social engineering, physical access (via flash drives), and infection of systems with unlicensed software. This combination significantly complicates early-stage detection.

2 Email remains the most common channel for malware distribution, which confirms its role as the primary initial access vector in attacks perpetrated by the majority of active threat clusters.

3 In the first half of 2025, the most active cyber threat clusters, according to CERT-UA classification, were UAC-0010, UAC-0050, and UAC-0202.

MONITORING STATISTICS

OVERVIEW OF SUBSYSTEMS, TECHNOLOGIES, AND TOOLS

During the first half of 2025, 11 new organizations were added to the Telemetry Collection Subsystem (NDR), receiving 11 sets of network monitoring sensors. Also, 11 organizations were added to the Endpoint Protection Subsystem (EDR), thus more than 40,000 workstations and servers are now monitored by the Vulnerability Detection and Cyber Incident/Cyber Attack Response System. 12 organizations were added to the Attack Surface Management (ASM) service.

Technologies and tools

Cybersecurity tools

Telemetry Collection Subsystem	Endpoint Protection Subsystem	Attack Surface Management
NDR	**EDR**	**ASM**
Organizations added: **78 +11**	Organizations added: **69 +11**	Organizations added: **50 +12**
Sensors installed: **80 +11**	Hosts protected: **40K**	Assets scanned: **4K**

Sectors and organizations

Protected entities

47 Government Organizations	**39** Local Authorities	**9** Strategic Enterprises
8 Security and Defence Sector	**5** Energy Sector	**3** Financial Sector
4 IT Sector	**3** Healthcare Sector	**2** Education and Science

CYBER INCIDENTS AND CYBER ATTACKS

QUANTITATIVE METRICS OF PROCESSED CYBER INCIDENTS

General Information

535 Cyber incidents and cyber attacks registered and processed by CIROC analysts during the first half of 2025

In the first half of 2025, the Cyber Incident Response Operations Centre (CIROC) identified and processed 535 cyber incidents and cyber attacks.

The majority of these cases involved malware infections. The primary objective of such attacks was typically to gain unauthorized remote access to information systems for the purpose of cyber espionage or financial theft.

The most common types of cyber incidents included:

- Malware infections
- Detection of malicious or anomalous network connections
- Compromise of user accounts

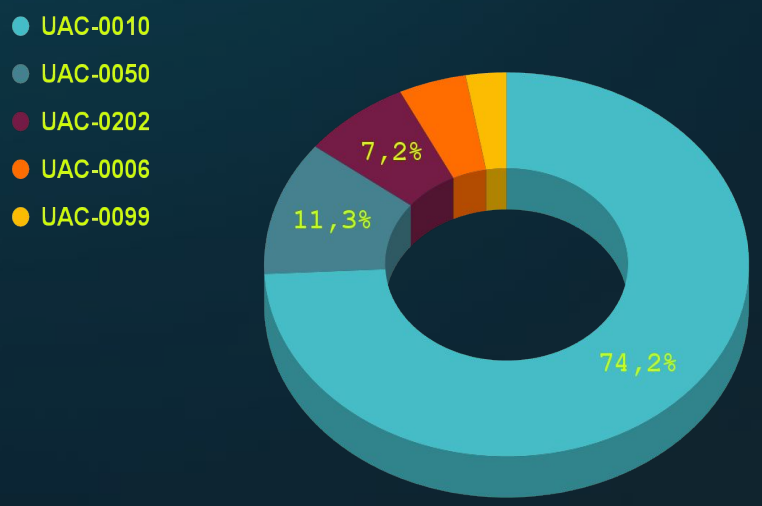
Breakdown by cyber incident type

02.01 – malware infection, 02.04 – malicious connection, 05.01 – account compromise, 03.03 – phishing, 05.02 – system compromise, 04.01 – attempted vulnerability exploitation, 09.01 – vulnerability.

CYBER THREATS

QUANTITATIVE METRICS OF CYBER THREATS

Breakdown of cyber threats



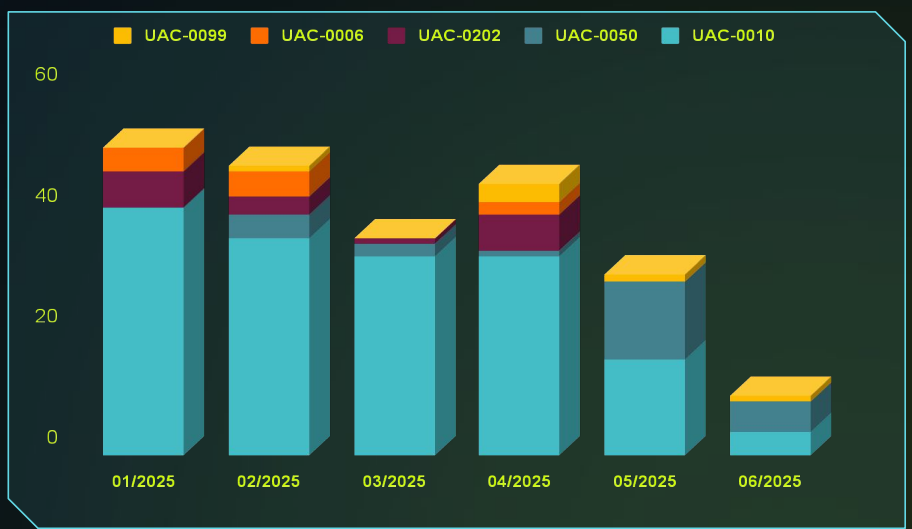
Among the cyber incidents/attacks recorded by the CIROC, **221** were linked to known cyber threat clusters. Thus, in the first half of 2025, the most active ones were UAC-0010, UAC-0050, and UAC-0202.

The primary initial attack vector was the distribution of malware via email — T1566.001 Phishing: Spearphishing Attachment (according to the MITRE ATT&CK classification).

! It is worth noting that the vast majority of tactics and techniques used by attackers as an initial attack vector lose their effectiveness when non-privileged user accounts are employed and basic security configurations are implemented on workstations.

The chart shows the trends of the cyber incidents detected during the first half of 2025 as recorded by the Cyber Incident Response Operations Centre.

A slight decrease is observed in the number of cyber incidents associated with the activity of the UAC-0010 threat cluster.



CYBER THREATS

ACTIVITY OF CYBER THREAT CLUSTERS

UAC-0010 cluster overview

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

Tracked since:
2013

Motivation:
cyber espionage

Targets:
government authorities, defence forces

Throughout the first half of 2025, CIROC specialists identified 164 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.

The summary 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-0050 cluster overview

Aliases:
unavailable

Tracked since:
2020

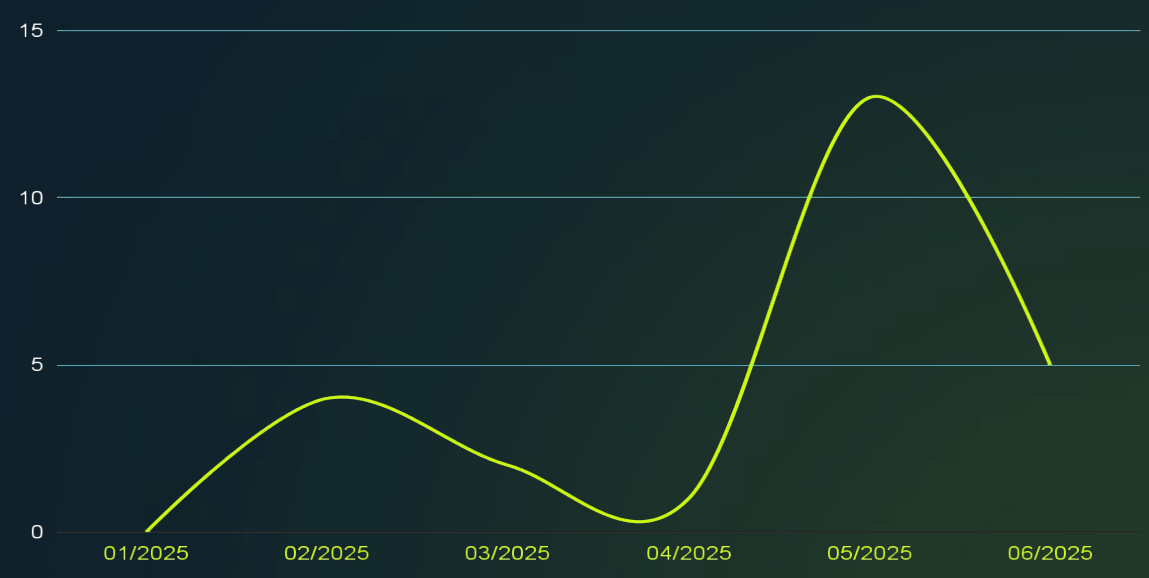
Motivation:
cyber espionage, stealing money, PSYOPS

Targets:
government authorities, defence forces, financial institutions

Throughout the first half of 2025, CIROC specialists identified 25 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.

The summary of the UAC-0050 group activity is available here: **https://cert.gov.ua/article/6281009**.

UAC-0050 cyber attacks timeline



CYBER THREATS

ACTIVITY OF CYBER THREAT CLUSTERS

UAC-0202 cluster overview

Aliases:
unavailable

Tracked since:
2013

Motivation:
cryptomining,
cyber espionage

Targets:
not determined

During the first half of 2025, CIROC specialists identified 16 cyber incidents related to the activity tracked by CERT-UA under the identifier UAC-0202.

In most cases, the initial infection vector was the use of unlicensed software that contained embedded malware. This approach enabled attackers to covertly compromise systems during the installation of pirated software.

UAC-0202 cyber attacks timeline

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 to identify existing vulnerabilities, potential risks, and attack vectors, as well as provide detailed reports with descriptions of vulnerabilities and other related information.

To contact 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

Cyber Incident Response Operations Centre

State Cyber Protection Centre

State Service of Special Communications and Information Protection of Ukraine

Email: soc@cip.gov.ua

Phone: +38 (044) 281 87 37