State Service of Special Communications and Information Protection of Ukraine

TLP:CLEAR

Cyber Threats: Ukraine

Analytics for the H2 2025

Content

Foreword

CERT-UA

National Cyber Incident Response Team

Cyberspace is an integral component of modern warfare. Alongside traditional warfare, adversaries actively employ cyber operations to achieve reconnaissance, informational, and operational objectives. In this environment, a state's ability to swiftly detect, analyze, and respond to cyber threats is vital to national security.

The activity of hacking groups in cyberspace is constantly changing and evolving. Adversaries experiment with new approaches, adapt their tools and tactics, and combine technical means with social engineering methods to achieve their goals. Systematically analyzing these shifts enables us to promptly develop effective countermeasures and enhance the resilience of our information systems.

This report summarizes observations of cyber incidents from the second half of 2025. It highlights key trends in cyber threats, analyzes the activity of specific threat clusters, and describes the new tactics, techniques, and procedures employed by hacking groups.

We would like to express our deepest gratitude to all the professionals who work tirelessly every day to protect Ukraine's cyberspace, including the cybersecurity units of state bodies, the security and defense sector, local specialists, and our international partners. Thanks to these collaborative efforts, we can quickly identify threats, counter adversarial cyber operations, and bolster the resilience of Ukrainian cyberspace.

Conclusions & Insights

Insights

For the first time since the onset of the full-scale invasion, the number of cyber incidents has declined in the second half of the year compared to the first. This slight decrease may indicate that Ukrainian organizations are adapting to the current threat landscape and that countermeasures are becoming more effective. However, the overall intensity of cyberattacks remains steady, though we are tracking shifts in the adversary's approach.

We continue to observe the emergence of new cyber threat clusters, which indicates that adversaries are relentlessly searching for more effective operational methods. Attackers test various tactics, evaluate their success rates, and may revert to previous attack scenarios if they are more effective. However, they never entirely abandon previously tested methods.

We have also observed a trend in which attackers attempt to reenter previously compromised systems. Unfortunately, these attempts sometimes succeed if the root cause of the initial incident has not been completely eliminated.

These observations confirm that the situation in cyberspace remains complex and dynamic overall.

Focus on Persistence

In the previous half-year, a significant portion of cyber incidents involved the "Steal & Go" tactic, which relied on deploying stealers without establishing persistence within the system. This approach allowed attackers to quickly steal necessary information, minimizing their stay within the victim's infrastructure and the risk of detection.

During the reporting period, we observed a gradual shift in focus from one-time data theft to securing unauthorized access to information systems.

Attackers are increasingly prioritizing the ability to reenter compromised infrastructure by abusing legitimate remote access services and building upon their initial compromise.

This strategy indicates an intention to maximize the long-term value of attacks by using acquired access to prepare for subsequent phases of an attack. In this context, a compromise is increasingly viewed not as an isolated event but rather as a foothold for further operations within the victim's network.

Comeback

It is worth noting that, in certain incidents, we observed attackers resuming activity in previously compromised systems after the initial attack. These actions may be an attempt to verify if access is still available, if the exploited vulnerabilities have been patched, or if the previously obtained credentials are still valid.

This practice underscores the critical importance of a comprehensive incident response strategy that eradicates the root cause. Limiting the response to only restoring system functionality or selectively blocking identified activity without analyzing the incident's origins and resolving all vulnerabilities substantially increases the risk of recompromise. Without drawing the right conclusions and implementing corrective measures, an organization risks falling victim to the same or a similar attack again.

Conclusions

Throughout the second half of the year, cyberspace remained a critical domain in Ukraine's ongoing confrontation with its adversary. Hostile actors consistently launched cyberattacks to gather intelligence, disrupt critical systems, and undermine state institutions' operations.

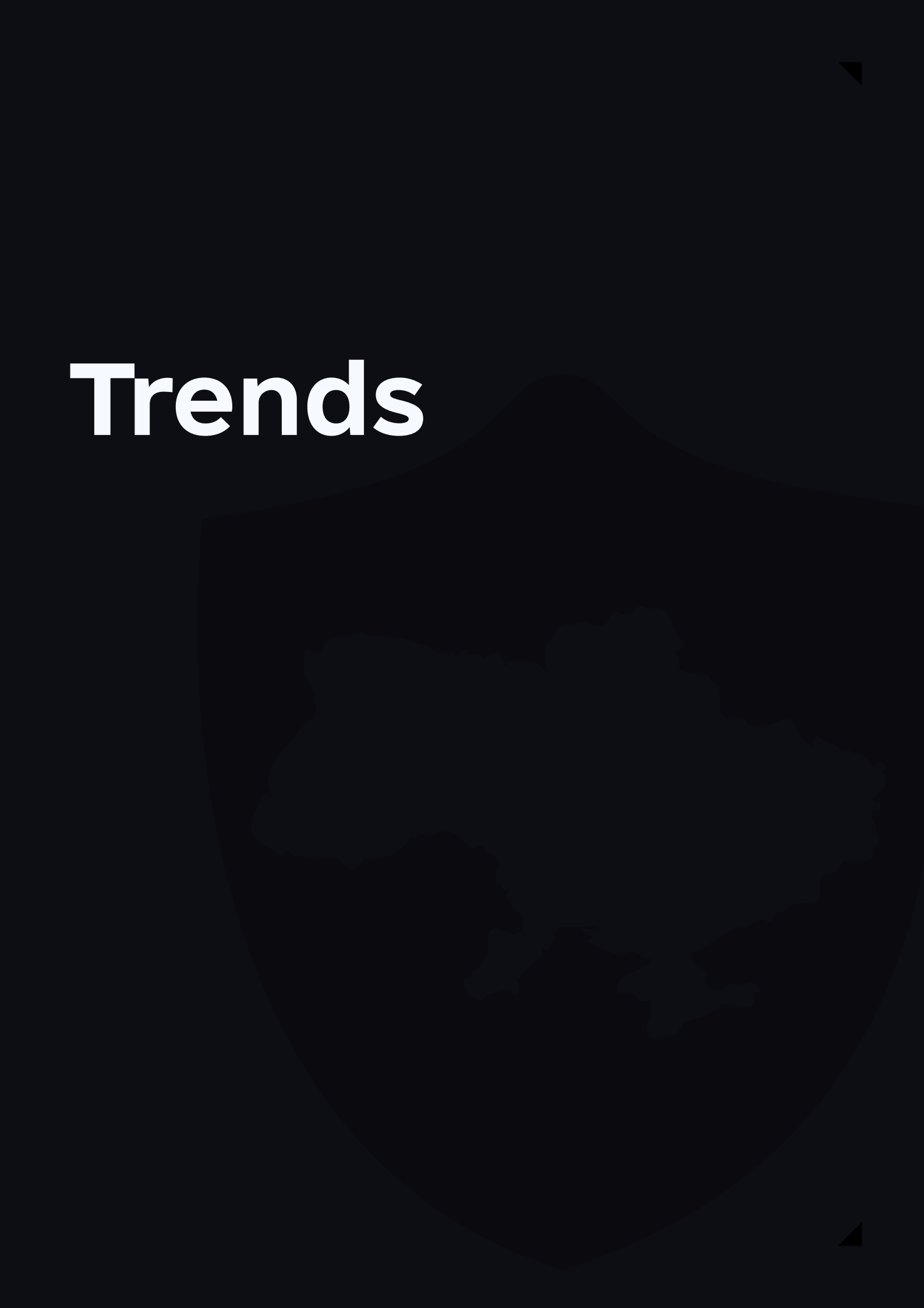
A defining feature of this reporting period was the continuous evolution of threat actor tactics. Security analysts have observed the emergence of new cyber threat clusters, as well as the active testing of novel techniques. Meanwhile, adversaries have frequently recycled proven attack scenarios. The standardization of malicious toolkits demands particular attention because effective exploits and methodologies now spread rapidly across different hacking groups.

At the same time, the focus of initial compromise vectors has shifted. Attackers are increasingly relying on highly sophisticated social engineering. They deliberately build trust with their targets, exploit legitimate communication channels, and use deeply personalized approaches to trap victims.

Alongside these psychological tactics, adversaries maintain a strong focus on technical mechanisms to secure persistent access within compromised systems.

Despite these challenges, findings from the reporting period demonstrate a steady increase in the resilience of national information systems and the effectiveness of countermeasures overall. However, the adversary's sustained activity, high adaptability, and ability to reinfiltrate previously breached networks highlight the urgent need for a comprehensive cybersecurity strategy. This requires completely resolving the aftermath of any incident and rigorously implementing robust preventive security measures.

Trends

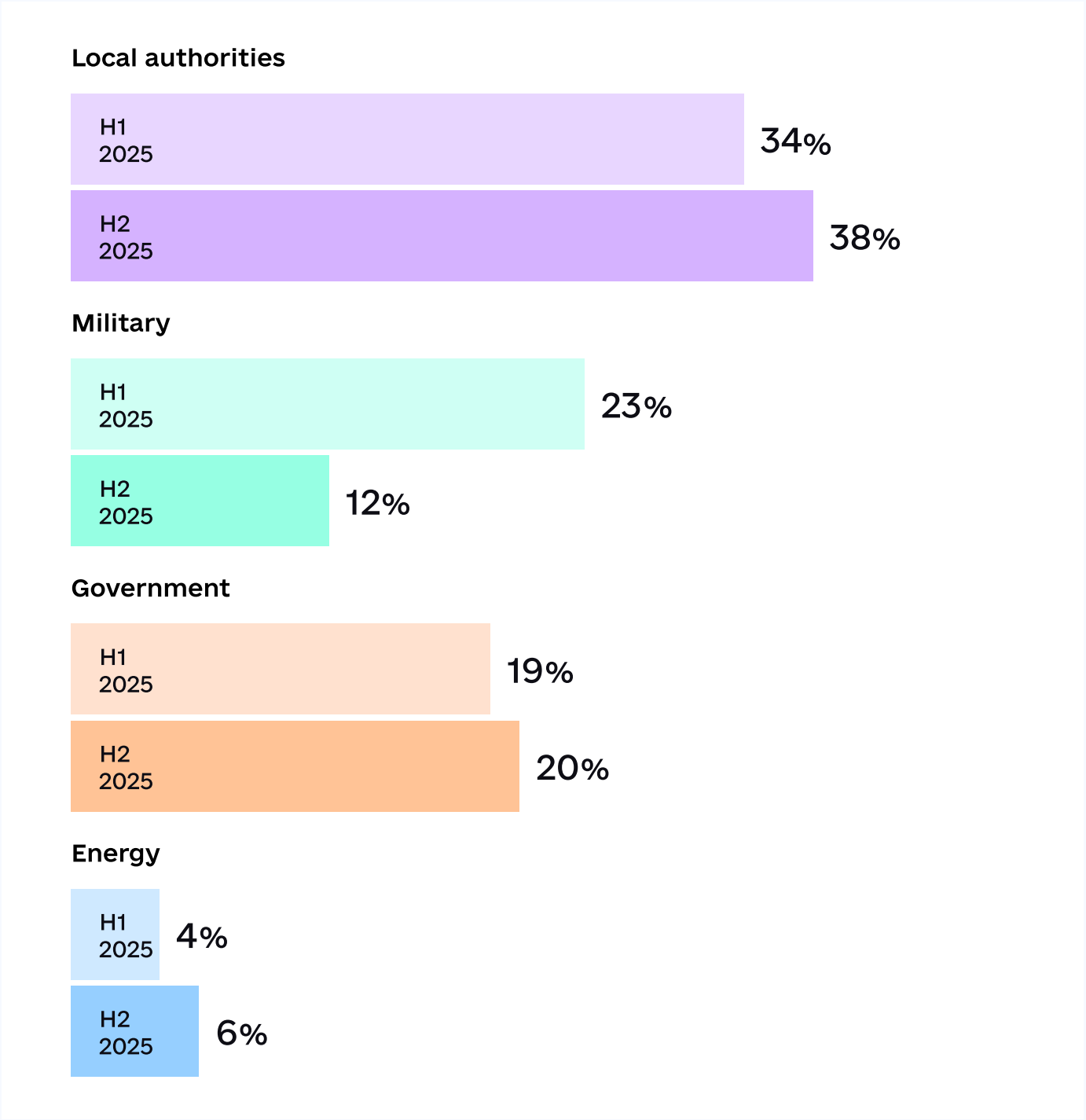


During the reporting period, the overall intensity of cyber incidents remained consistent with the first half of the year, though the total number decreased slightly. At the same time, we did not record any critical incidents, and the number of high-level incidents dropped as well.

Incidents by severity	H1 2025	H2 2025	Difference
Critical	1	0	-100%
High	6	5	-17%
Medium	2 944	2895	-2%
Low	67	9	-87%
Total	**3 018**	**2 909**	**-4%**

The adversary's objectives remain unchanged. Although our statistics show a decrease in cyberattacks against the security and defense sector, this does not accurately reflect the situation.

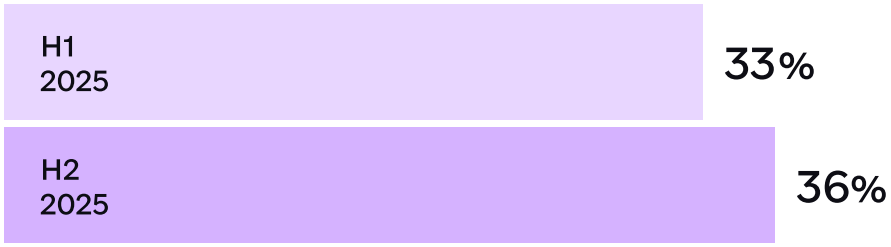
A significant portion of these incidents are handled directly by the cyber defense units of military formations. Nevertheless, the security and defense sector continues to be a primary target for the adversary because any impact on it can directly affect the course of hostilities.



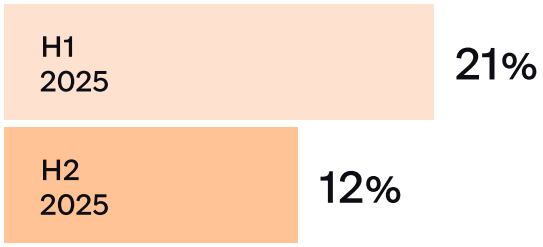
The second half of the year revealed a positive trend. Despite a slight increase in malware distribution, the number of actual infections decreased.

This improvement was driven by increased user awareness of cyber threats and the proactive threat detection and blocking measures implemented by our team.

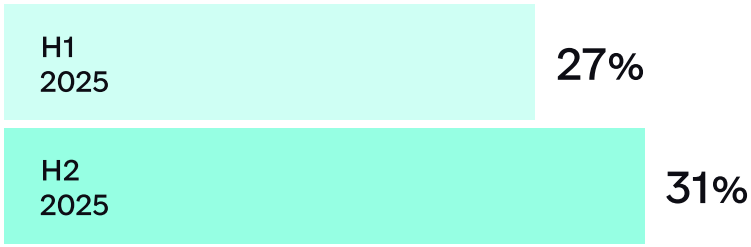
02.02 Malware distribution



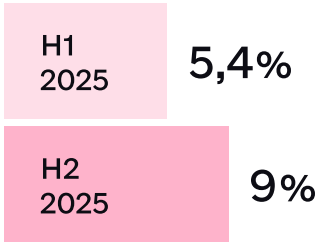
02.01 Malware infection



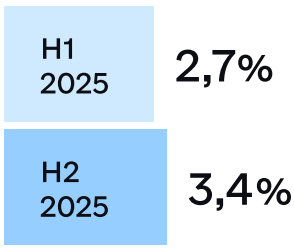
03.03 Phishing



05.01 Account Compromise



05.02 System Compromise



Intensity HeatMap

An intensity heatmap is provided below to visually represent the distribution of cyber incidents across specific threat clusters. The heatmap displays the total number of cyber incidents attributed to each cluster and allows one to evaluate the relative activity of various groups during the reporting period.

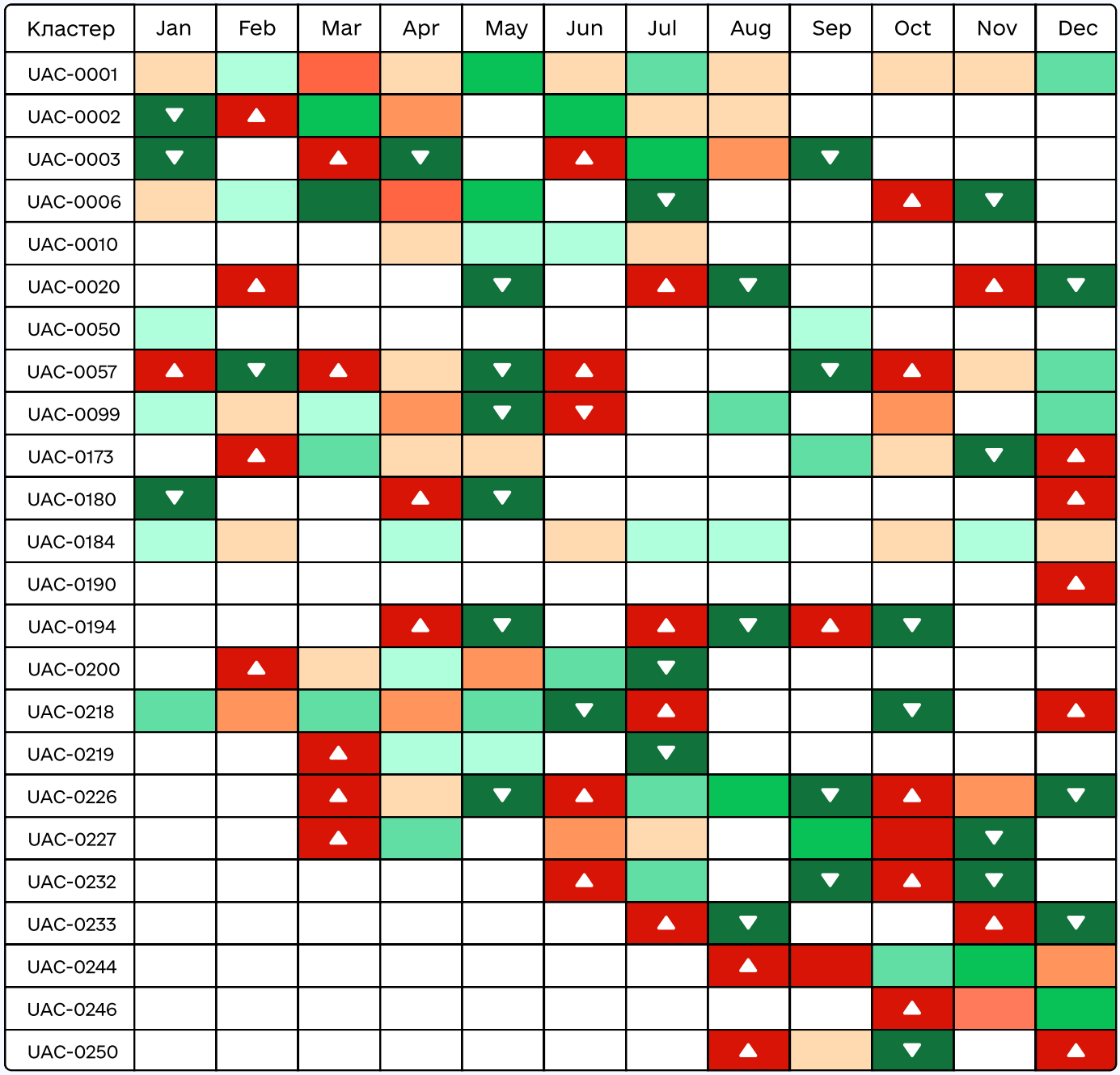
Кластер	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
UAC-0001												
UAC-0002												
UAC-0003												
UAC-0006												
UAC-0010												
UAC-0020												
UAC-0050												
UAC-0057												
UAC-0099												
UAC-0173												
UAC-0180												
UAC-0184												
UAC-0190												
UAC-0194												
UAC-0200												
UAC-0218												
UAC-0219												
UAC-0226												
UAC-0227												
UAC-0232												
UAC-0233												
UAC-0244												
UAC-0246												
UAC-0250												

low high

HeatMap of Dynamics

To illustrate the activity trends of specific cyber threat clusters, the following heatmap demonstrates the monthly dynamics of cyber incidents attributed to these clusters.

The values in each cell reflect either the emergence of new activity or a change in attack intensity compared to the previous month.



Onset/resumption of activity

Activity has stopped

significant decrease

no changes

significant increase

Current Threats

Emerging Activities

During the reporting period, we observed the continued emergence of new cyber threat clusters, which is consistent with the trend noted in the previous report. We identified novel approaches to cyberespionage and cyberattacks involving the deployment of ransomware. Meanwhile, activity involving the exploitation of zero-click vulnerabilities remains highly relevant.

Zero-clickers: UAC-0233, UAC-0250

UAC-0233 activity was first detected in the first half of 2025, and the exploitation of Roundcube vulnerabilities (CVE-2024-37383 and CVE-2025-49113) was described in a previous analytical report. At the time, however, it was considered one incident. The cluster's primary activity peaked in the second half of 2025, prompting the creation of a distinct identifier to track this threat.

Since late September 2025, we have recorded a series of campaigns that exploit zero-click vulnerabilities in the Zimbra mail server.

The threat actor has exploited CVE-2025-48700 and CVE-2025-66376 across various attacks, allowing them to execute arbitrary code without requiring any user interaction.

Upon successful compromise, the attackers gained access to mailbox contents, including correspondence compiled into a TGZ archive, multi-factor authentication backup codes, application passwords, and the global address book. This activity is tracked under identifier UAC-0250.

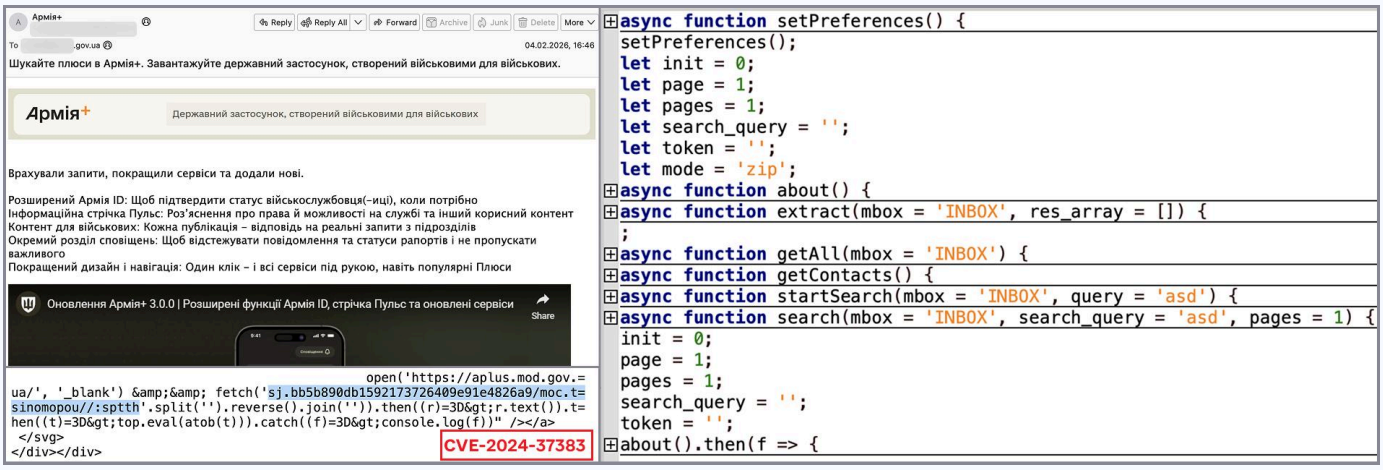


Fig. 1. Example of activity UAC-0233

Ransomware: UAC-0238, UAC-0243

Various groups deployed ransomware in cyberattacks in the second half of 2025.

Since at least July 2025, the UAC-0238 has targeted local government bodies by encrypting data on Windows-based workstations with Proton ransomware. The attackers gained initial access to information and communication systems (ICS) through internet-facing administrative interfaces, primarily Remote Desktop Protocol (RDP). Before encrypting the files, the hackers deleted the operating system's shadow copies, which made it impossible to recover data via this method.

Regarding the UAC-0243 threat, attackers typically gain access to the local network through a vulnerable Microsoft SharePoint server. The attackers deployed X2anylock (Warlock), a LockBit 3.0 variant, to encrypt the data.

Notably, to establish persistence and move laterally across the network during the attack, the threat actors used several legitimate utilities, including the Cloudflare Tunnel traffic tunneling service, as well as the Velociraptor and RClone tools to exfiltrate files.

This activity has been seen before on a global scale. Similar cyberattacks have targeted government bodies, critical infrastructure, and other organizations in Portugal, Croatia, Turkey, and North America. Ukraine experienced its first such attack in October 2025.

Cyber Spies: UAC-0232, UAC-0246

Throughout the reporting period, new cyber threats aimed at cyberespionage emerged. This suggests that the adversary is strategically focused on gathering intelligence by any available means.

Information resources belonging to the military, government bodies, and local authorities are still the primary targets of interest.

The UAC-0232 group is notable for its unique approach. Each of its campaigns targets a specific region of Ukraine.

Emails containing a link to a webpage mimicking the official site of the regional administration were distributed among state institutions within the targeted region. The webpage supposedly hosted a list of bomb shelters. However, instead of the expected document, users downloaded an archive containing an executable file. This file carried the STELLDOCK malware, which combines stealer and backdoor functionalities (specifically, it gathers data and can execute a limited set of commands on the infected computer).

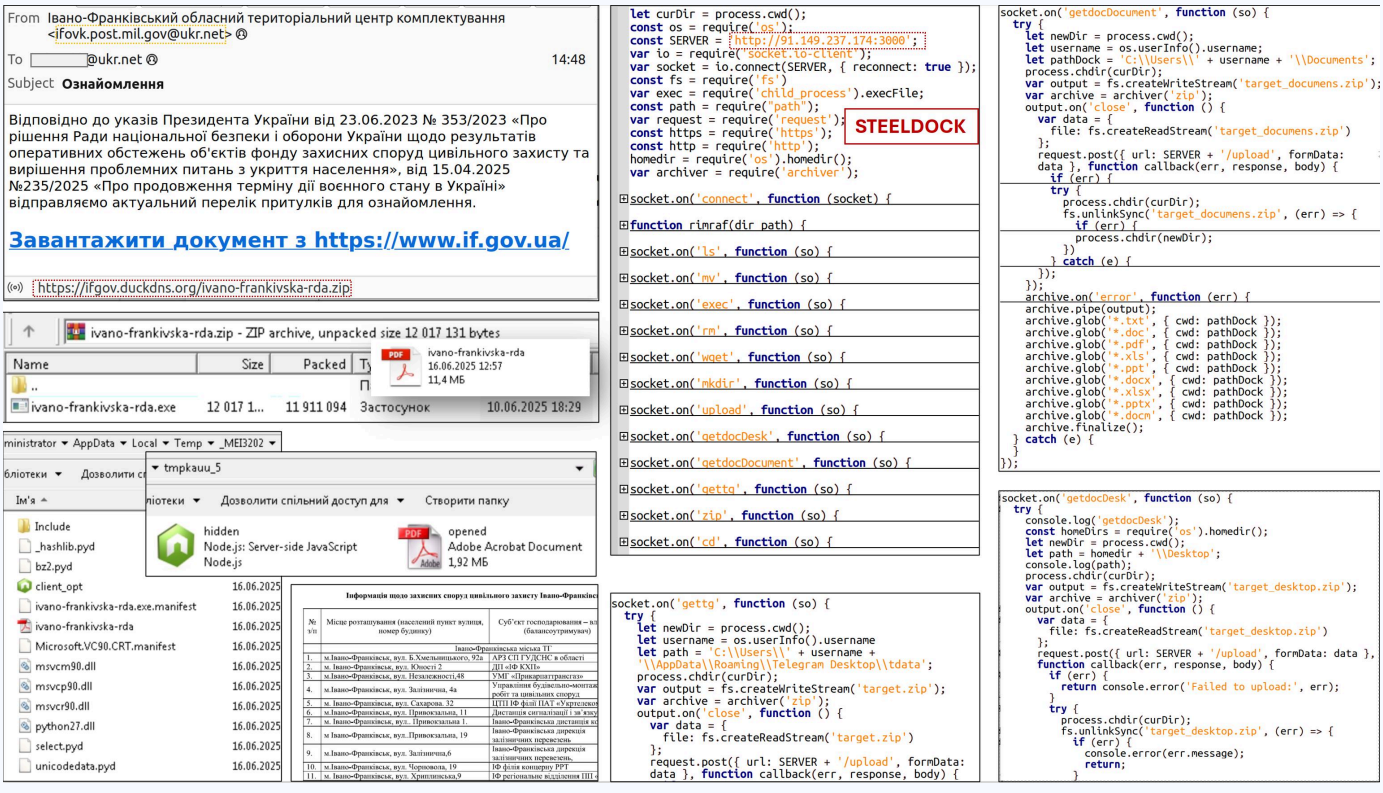


Fig. 2. Example of activity UAC-0232

Corporate mail servers typically have robust cybersecurity measures in place, meaning a significant portion of malicious emails are blocked before reaching the user. However, the UAC-0246 group employs a different strategy: they send malicious emails to the personal email accounts of Ukrainian citizens.

Their primary targets are users of the I.UA email service. Importantly, the malicious file is not directly attached; rather, the victim receives a link to the I.UA file storage hosting the executable. Opening this file infects the system with XenoRAT, a remote access Trojan (RAT).

Current tactics, techniques, and procedures

During the reporting period, we observed specific shifts in the tactics, techniques, and procedures used by hacking groups. Some techniques proved highly effective and were adopted and used simultaneously by multiple groups.

CVE-2025-8088

The WinRAR vulnerability (CVE-2025-8088) became quite prevalent during the reporting period. Information about the vulnerability was published in August, and by September, we began detecting email campaigns with attached archives containing an exploit for it. This vulnerability allows files to be written outside the user-selected directory during archive extraction.

Consequently, vulnerable versions of WinRAR silently create an additional file in a directory specified by the attackers. This exploit is most frequently used to drop malicious files into the Startup directory, ensuring their automatic execution the next time the user logs in.

The first cyberattack exploiting this vulnerability that we recorded was attributed to UAC-0010. However, we also observed subsequent exploitation of CVE-2025-8088 in activities linked to UAC-0002, UAC-0226, and other groups.

Alternate Data Streams (ADS)

The reporting period also saw the use of alternate data streams (ADS). ADS is a standard feature of the NTFS file system in Windows environments that allows additional data streams to be associated with a file or directory. Attackers exploit this mechanism to hide malicious code.

The UAC-0010 group is known for creating over a hundred malicious files in various directories on an infected computer and for storing malicious code in the Windows registry. However, in 2025, we observed an expansion of their toolkit when they started placing malware components within the alternate data streams of empty (0-byte) files and directories. This made detection and analysis significantly more difficult.

A similar approach can be applied to virtual hard disks (VHD files). Once mounted, they appear in the system as a separate drive with an NTFS file structure and ADS support. The UAC-0099 group used this exact mechanism. The attackers distributed download links for VHD files that contained an LNK file, a VBScript, and text files with seemingly benign content (e.g., "Hello First"). The malicious payload was hidden within the alternate data streams (ADS) of these files and was ready to be read and executed by the aforementioned script.

russian intelligence services

Cyberattacks conducted by groups associated with the Main Intelligence Directorate (GRU) of the russian federation and other intelligence agencies of the aggressor state are among the most dangerous. These groups are constantly identifying new ways to compromise systems for espionage and destructive cyberattacks.

Evolution of Social Engineering

During the reporting period, we observed a transformation in social engineering approaches. Traditional phishing emails and messenger texts with attachments are gradually becoming less effective due to increased user awareness and caution. Instead, initial engagement with targets is increasingly conducted via phone numbers of Ukrainian mobile operators and legitimate accounts. The attackers speak fluent Ukrainian, utilize audio and video calls, and demonstrate relevant knowledge about the individual or organization. This allows them to build trust and increase the success rate of their attacks.

UAC-0001 (APT28) and UAC-0190 (Void Blizzard, Laundry Bear) notably employed this tactic during attacks on representatives of the Ukrainian defence forces and state bodies. Malicious files were only sent to victims via messenger after direct telephone communication had taken place.

For example, UAC-0001 orchestrated a large-scale cyber operation targeting Ukrainian service members and employees of the defence industrial complex. The campaign aimed to conduct reconnaissance by securing unauthorized remote access to infected systems and gathering information of interest to the attackers. Potential victims were sent an XLS file with an embedded malicious macro disguised as official documentation during their interactions. Details of this activity are outlined in a CERT-UA publication.

Compromised Devices as a Source of Sandworm (UAC-0002) Attacks

An investigation into a cyber incident does not usually end with merely identifying and eradicating the root cause. For instance, after investigating a cyber incident at a critical infrastructure facility and resetting credentials, monitoring event logs shifted towards detecting repeated authentication attempts on compromised accounts. This revealed unsuccessful connection attempts from a range of Ukrainian IP addresses. These IP addresses shared a common trait – they belonged to the Ukrainian network segment and hosted publicly accessible network device administration panels.

While investigating the devices in question, we discovered that the native SOCKS functionality and SSH forwarding had been enabled. This allowed the devices to be used as intermediary nodes for routing and tunneling traffic during subsequent attacks.

By monitoring the traffic of these nodes, we can identify other elements of the attackers' infrastructure, such as additional compromised devices and potential victims of their campaigns.

To make it more difficult to attribute the actual source of the attack, the attackers frequently routed traffic through a chain of several such devices. They also used compromised public web resources hosting traffic tunneling tools as intermediary points.

Therefore, during the recovery phase following a cyber incident, it is crucial to thoroughly remediate identified vulnerabilities by restricting administrative access, patching flaws, changing credentials, and reviewing remote management settings. Thoroughly implementing these measures is the only way to minimize the risk of a repeat compromise.

Previous reports

To provide a complete picture and understanding of the transformation in cyber capabilities during the full-scale war, previous analytical reports are available at the following webpage:

Analytical materials of the SSSCIP

Media Contact Center

press@cip.gov.ua

Stay connected:

https://x.com/SSSCIP

https://x.com/_CERT_UA

https://www.linkedin.com/company/dsszzi

https://www.linkedin.com/company/cert-ua

https://www.facebook.com/dsszzi

https://www.facebook.com/UACERT

State Service of Special Communications and Information Protection of Ukraine

Cyber Threats: Ukraine

Analytics for the H2 2025