State Service of Special Communications and
Information Protection of Ukraine

RUSSIAN CYBER OPERATIONS

Analytics for the H2 2024

CONTENT

FOREWORD

Yevheniia Nakonechna
Head of the State Cyber
Protection Center

The cybersecurity landscape in Ukraine faced fresh challenges throughout 2024. Every day brings new and evolving threats: on one side, we confront familiar adversaries such as russian hacker groups with ties to the GRU or FSB; on the other, emerging players whose attacks are increasingly aggressive and automated. While the number of critical incidents has slightly decreased, their complexity, and consequently the resources required for mitigation, have significantly increased.

The threat of hostile attacks targeting Ukraine's energy infrastructure and other critical infrastructure remains a pressing concern. These attacks are often observed in advance of missile strikes, suggesting a coordinated hybrid warfare strategy.

Our focus remains on proactive defense to prevent destructive attacks. However, our adversaries are constantly probing for new vulnerabilities. Their objective extends beyond mere technical damage; they aim to paralyze critical sectors of national functioning and to influence civil society through intimidation, disinformation, and information-psychological operations (IPSO). The December 2024 attack on state registries proved to be just as impactful as the December 2023 attack on Ukraine's largest telecommunications provider. This underscores a vital point: a nation possesses a wide range of "pressure points" that require careful assessment to ensure effective cybersecurity and resilience against modern threats.

Our primary goal is not simply reacting to threats but preventing them altogether. We consistently dedicate extensive effort to identifying adversary activity within the networks of government institutions and critical infrastructure, thereby strengthening their defenses. Effective cyber defense, however, is inherently a collective endeavor. International support, experience exchange, and technology sharing remain crucial to bolstering our resilience. By working together, we not only protect Ukraine but also contribute to a safer cyberspace for all of Europe.

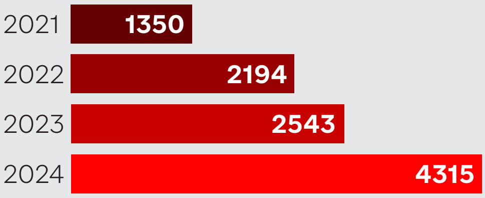
CERT-UA STATISTICS

CERT-UA STATISTICS

In the second half of 2024, specialists from CERT-UA observed a significant surgein the number of cyber incidents. Activity peaked in October and November, marked by a series of mass malware distribution campaigns. Overall, the number of cyber incidents in the second half of 2024 increased by more than 48% compared to the previous semester. Looking at the full-year figures, the increase is even more pronounced, reaching nearly 70%.

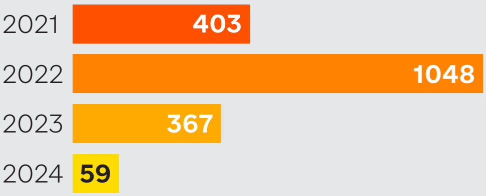
NUMBER OF HANDLED INCIDENTS

Total number of registered cyber incidents



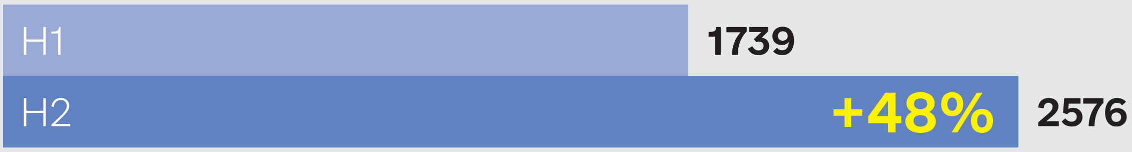
The increasing number of cyber incidents indicates that Russian intelligence services are willing to amplify their use of cyber components as a means of waging war.

Critical and high-severity cyber incidents

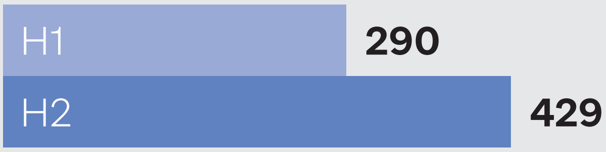


Due to cooperation with the partners and their support, we were able to lower the destructive influence of the cyber attacks targeting Ukrainian organizations.

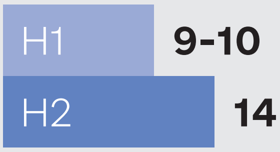
GROWTH IN THE REGISTERED INCIDENTS RATE IN H2 2024



AVERAGE PER MONTH



AVERAGE PER DAY



As illustrated by the charts, the total number of cyber incidents continues to rise. Concurrently, the number of high and critical severity incidents is gradually decreasing.

Severity of registered incidents	H1 2024	H2 2024	Change for the period
Critical	3	1	-67%
High	45	10	-78%
Medium	1670	2457	+47%
Low	21	108	+414%
Total	1739	2576	+48%

There was a 77% decrease in the number of high and critical severity incidents.

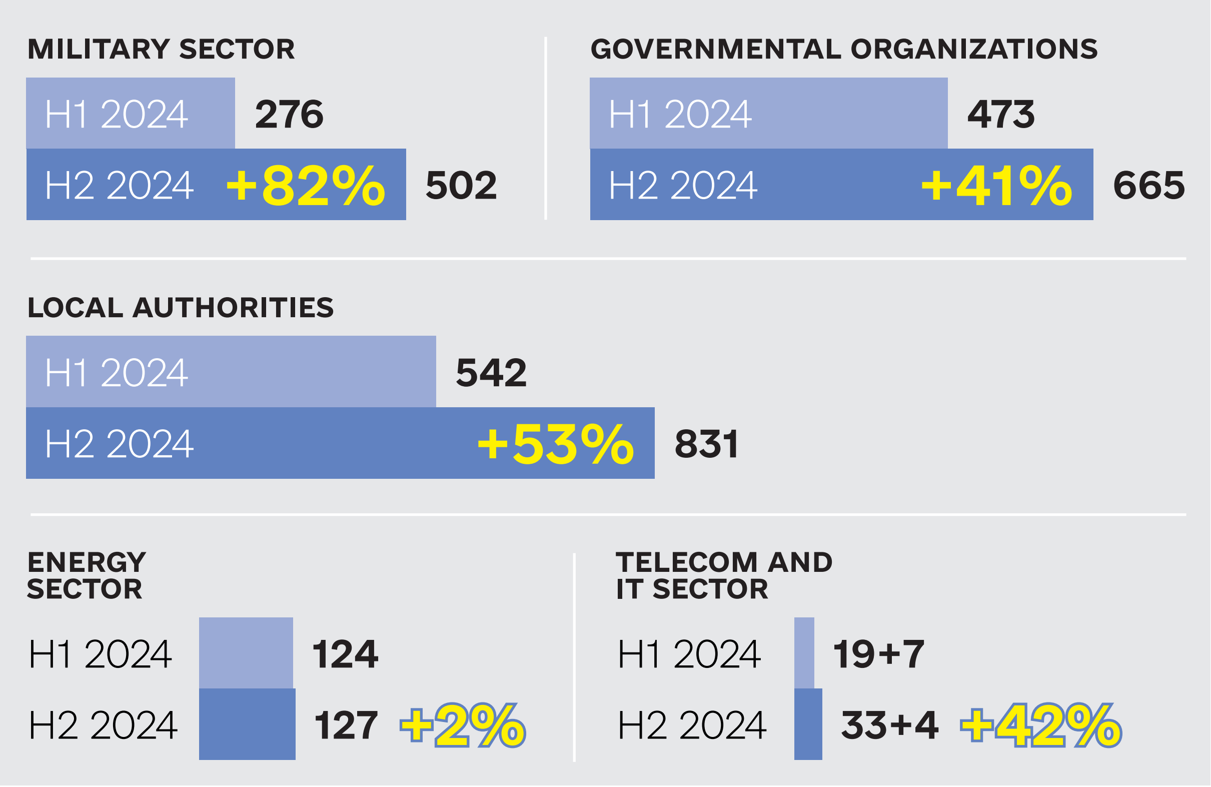
Number of incidents	H1 2024	H2 2024	Change for the period
Critical and high severity	48	11	77%

112% increase in malware distribution-related cyber incidents. Malware infection incidents up by 63%*.

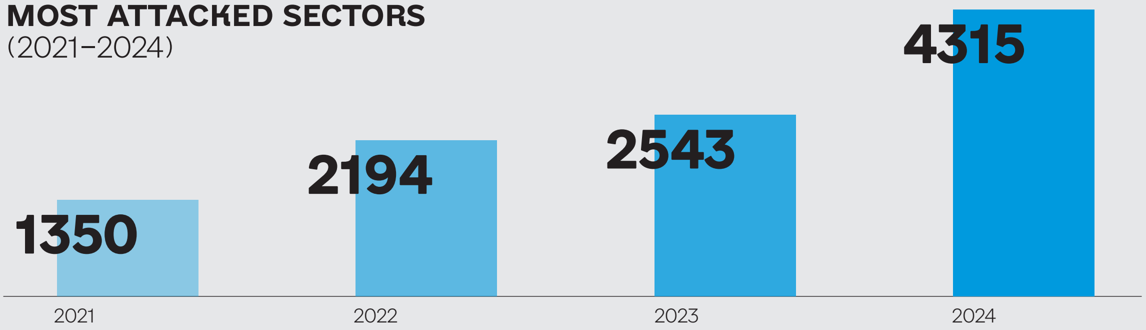
Number of malware incidents	H1 2024	H2 2024	Change for the period
Distribution	531	1123	112%
Infection	196	320	63%

The surge in cyber incidents involving malware infections can be primarily attributed to the increase in malicious email campaigns and enhanced visibility, with changes in TTPs having a lesser impact*.

In the second half of 2024, government institutions, as well as the military sector, were the most frequent targets of cyberattacks.



MOST ATTACKED SECTORS
(2021–2024)



20%	Government sector and local authorities	**26%**	Government sector and local authorities	**25%**	Government sector and local authorities	**58%**	Government sector and local authorities
16%	Security and Defense sector	**14%**	Security and Defense sector	**7%**	Security and Defense sector	**18%**	Security and Defense sector
6%	Commercial	**6%**	Commercial	**5%**	Commercial	**6%**	Energy
6%	Finance	**5%**	Finance	**4%**	Energy	**3%**	Commercial
3%	Energy	**5%**	Energy	**4%**	Telecom and ISP	**2%**	Educational institutions

This dataset is compiled based on incident analytics provided by the Computer Emergency Response Team of Ukraine CERT-UA and the SOC of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine excluding cases registered by other cyber centers.

KEY FINDINGS AND INSIGHTS FROM H2 2024

KEY FINDINGS AND INSIGHTS FROM H2 2024

General Trends

2024 was characterized by variable approaches to cyberattacks, both from new and well-known hacker groups. The 48% increase in incidents compared to the previous semester resulted in a significant rise in the workload of the response team and a longer time required to handle threats.

The complexity of the attacks investigated and the sensitivity of their targets remain high. Adversaries are employing increasingly sophisticated methods, combining various tactics to achieve their goals, which complicates early detection and neutralization.

In many cases, we cannot disclose important details regarding the affected organizations, identified attack vectors, and the specifics of our investigations. Public disclosure could lead to adversaries adapting their methods, making it more difficult to detect and prevent similar attacks in the future.

During the second half of 2024, approximately 70 separate campaigns related to the mass distribution of malware were identified and analyzed. Concurrently, over 750 reports were received from users targeted by phishing attacks. However, the actual number of confirmed malware infection cases was 90% lower. This reflects improvements in cyber hygiene among organizations interacting with the State Service of Special Communications and Information Protection of Ukraine, enhanced threat detection mechanisms, and effective incident response teams.

The second half of 2024 saw a significant increase in cyberattacks targeting the military sector, highlighting the critical role of the cyber component in adversary intelligence operations. The primary attack vector is espionage, aimed at gathering critical information that could directly influence the operational situation in the combat zone.

Tactics Shift

Well-known hacker groups affiliated with the GRU and FSB continue to employ traditional attack methods. In contrast, new military cyber units are demonstrating a higher level of automation, aggressiveness, and operational scale. Russian hackers systematically attempt to disrupt the operations of Ukraine’s energy sector, coordinating cyberattacks with mass missile strikes on the energy system.

Furthermore, a systematic campaign by Russian hackers against Ukraine’s commercial sector continues. The primary objective is financial theft and the spread of ransomware. The scale of these attacks has reached record levels.

Despite the severity of the threat, the business sector is significantly less prepared for cyberattacks than government institutions and is not always willing to openly share information about incidents. An additional challenge is the low level of trust in government agencies responsible for cybersecurity, despite the significant improvements in their effectiveness and the quality of approaches over the past three years.

Incident with State Registries

One of the most significant attacks of the second half of 2024 was the December attack on the state registries of the Ministry of Justice of Ukraine. The incident led to serious disruptions in the operation of key government services, causing problems at border crossings and customs operations. The scale of the consequences highlighted the critical dependence of processes in government agencies on existing digital infrastructure and the need to review backup strategies and enhance resilience for all organizations in the public sector.

Ongoing Challenges for Critical Infrastructure

Direct attacks on critical infrastructure (CI) have become significantly more complex to execute. Cybercriminals are forced to alter their tactics and use supply chain attacks as the primary vector for intrusion. They primarily focus on compromising suppliers of specialized software used in CI, as such companies often lack sufficient cybersecurity measures, and their compromise opens up new opportunities for hackers to extend access to critical systems.

Despite significant improvements in the protection of Ukrainian energy companies and the extensive experience gained over the past 11 years in responding to attacks, Russian APT groups continue to operate, leveraging their knowledge of the internal architecture of Ukraine’s energy systems, which have already been attacked before. Since the complete redesign of OT networks is a complex task, the adversary attempts to regain access to historically compromised segments of the infrastructure, constantly searching for new entry points. These points will always exist due to the dynamic and complex nature of the infrastructure, making the situation particularly dangerous.

Thus, attacks on the energy sector have evolved into more complex and prolonged operations, the execution of which may take 6 to 8 months. These operations require adversaries to adopt new approaches for initial access, maintaining access, and exploiting vulnerabilities in interconnected systems.

However, thanks to strengthened cooperation with international partners, the growth of the monitoring sensor network, and improved early threat detection mechanisms, a significant number of adversarial operations were identified and neutralized before they could be fully executed. At the same time, ensuring more effective attack detection requires further deployment of additional sensors and analytical systems across critical infrastructure facilities. During this period in 2024, we recorded several such attacks that, according to the NIS2 directive, qualify as "near misses," highlighting a high threat level and the continued need to reinforce protection.

Espionage and Information Operations

Both large-scale and targeted attacks continue to be carried out against individuals via Signal, Telegram, and WhatsApp, aiming to steal private correspondence and sensitive information, as well as to infect mobile devices and Windows systems with implants enabling persistent espionage activities.

The second half of 2024 was also marked by an increase in cyberattacks targeting the defense industry. The adversary actively employs all available resources to obtain intelligence that could impact the course of military operations. Targeted attacks were observed against individual military personnel whose computers may contain information about the operational situation on the front line, details on the quantity and type of deployed forces and assets, as well as access to situational awareness systems. Attacks were also carried out against defense industry enterprises, aiming to steal data on advanced weaponry and protection technologies — information that could be exploited by the adversary to advance its own weapons development programs.

Software Vulnerabilities

Outdated software and other critical misconfigurations remain among the key threats for organizations across all sectors. Test servers and supporting systems are often overlooked, creating potential entry points for attackers. In practice, threat actors exploit unpatched vulnerabilities with remarkable speed — often within hours of their public disclosure.

Conclusions

The year 2024 marks a shift in russia's approach to cyberwarfare: increased automation of attacks, a focus on the supply chain, and an expansion of espionage campaigns, including targeting the commercial sector. The rise in the number of attacks calls for greater coordination between government agencies, private companies, and international partners to ensure effective response and countermeasures against threats.

CASES

CASES

Hacking of the Ministry of Justice State Registries

On December 19, hackers attacked the registries of the Ministry of Justice of Ukraine, effectively halting the operation of 14 key state registries.

The cyberattack paralyzed a significant portion of the country's economic activities. Financial transactions, counterparty verification, government procurement, and access to important state services were all placed under threat. The cyberattack caused major disruptions in critical sectors:

- **Border crossing.** Registry failures made it impossible to verify information on travel bans, resulting in delays and denials at border checkpoints.
- **Customs clearance.** The disruption of access to data on legal entities and vehicle owners paralyzed customs operations, causing shipment delays.
- **Notary services and property transactions.** The lack of access to real estate registries by notaries and state registrars blocked property sales, inheritance processing, and other legal transactions.
- **Passport services.** Inability to verify personal data in the registries hindered the issuance of passports, ID cards, and other official documents.

This incident highlighted the critical dependence of both governmental and commercial institutions on the functioning of state registries, underscoring the need to revise backup strategies and ensure uninterrupted operations.

Implantation in Telecom Providers

We are observing the continuation of a campaign targeting telecom providers via vulnerable web applications, followed by the deployment of espionage-focused PAM modules such as **POEMGate** to collect credentials of administrators and other potential users.

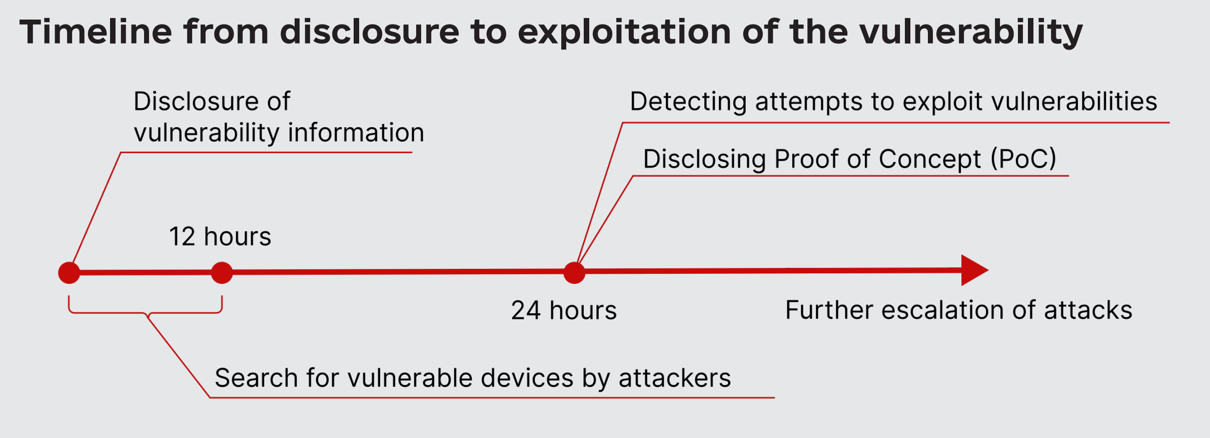
The implantation and collection of credentials and encryption keys enable persistent hidden access to telecom provider networks. This allows attackers to exploit trust relationships between providers while operating under the guise of legitimate users—without triggering any security system alerts.

The infrastructure of telecom companies can be leveraged by adversaries to launch attacks against other targets using legitimate IP addresses within the Ukrainian segment. Such activity typically attracts less scrutiny from SOC analysts and cybersecurity professionals.

Exploitation of Vulnerabilities

One of the critical vulnerabilities in the GeoServer software was exploited by adversaries just 20 days after it was publicly disclosed. They used it to gain access to an organization's network, where they remained undetected for an extended period while preparing for a destructive operation.

Overall, experts are observing a clear trend: the time between vulnerability disclosure and the first exploitation attempts is steadily decreasing.


Timeline from disclosure to exploitation of the vulnerability
Disclosure of vulnerability information
Detecting attempts to exploit vulnerabilities
Disclosing Proof of Concept (PoC)
12 hours
24 hours
Further escalation of attacks
Search for vulnerable devices by attackers

Typically, adversaries need no more than 12 hours after a vulnerability is publicly disclosed to identify at-risk devices. Within 24 hours, they begin the first exploitation attempts. Proof-of-concept (PoC) codes also tend to appear publicly within the same timeframe.

Most companies disclose information about product vulnerabilities alongside updates or patches that address them. Therefore, to prevent successful exploitation, it is critical to apply updates and patches in a timely manner—especially for systems and resources that are publicly accessible via the Internet.

In particular, during the second half of 2024, CERT-UA observed the use of exploits for several vulnerabilities across different operations, including:

- GeoServer — CVE-2024-36401.
- HFS HTTP File Server — CVE-2024-23692.
- Adobe Acrobat Reader — CVE-2023-21608.
- Roundcube — CVE-2023-43770.
- WinRAR — CVE-2023-38831.

UAC-0050

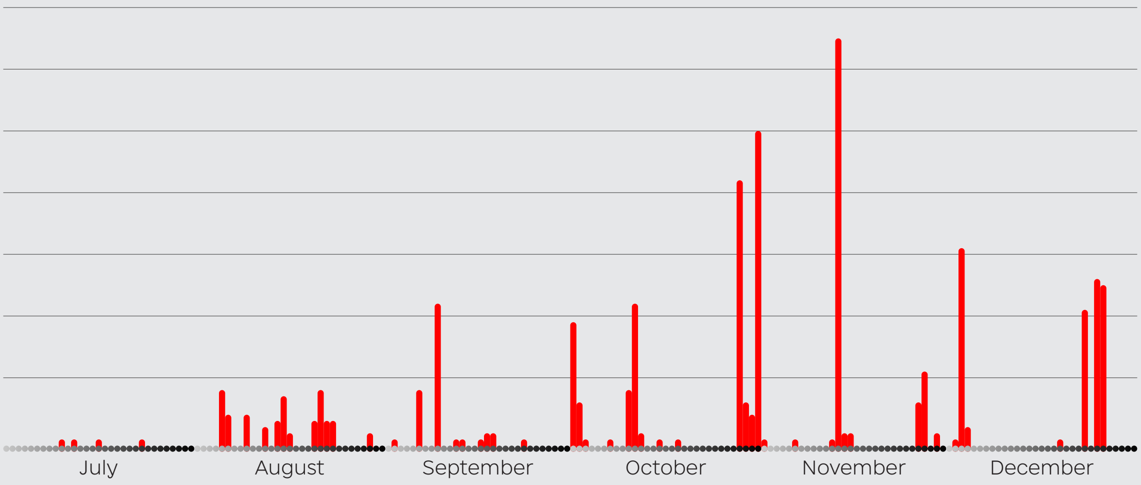
In the second half of 2024, the UAC-0050, known for its focus on information theft (cyber espionage), altered its tactics and techniques. A key difference was the development of additional areas of activity, specifically the theft of financial assets and the conduct of information-psychological operations under the "Fire Cells Group" brand.

One of the new features was the implementation of parallel malware distribution campaigns, including through legitimate services such as Bitbucket, Dropbox, 4Sync, Google Drive, and GitHub.

It can also be assumed that UAC-0050 has expanded its list of potential "victims" by sending phishing emails to an increasing number of organizations. This was likely influenced by a shift in focus — from cyber espionage to financial theft.

It is worth noting that in order to increase credibility, the attackers continue to send emails that appear to come from well-known

Activity of the UAC-0050



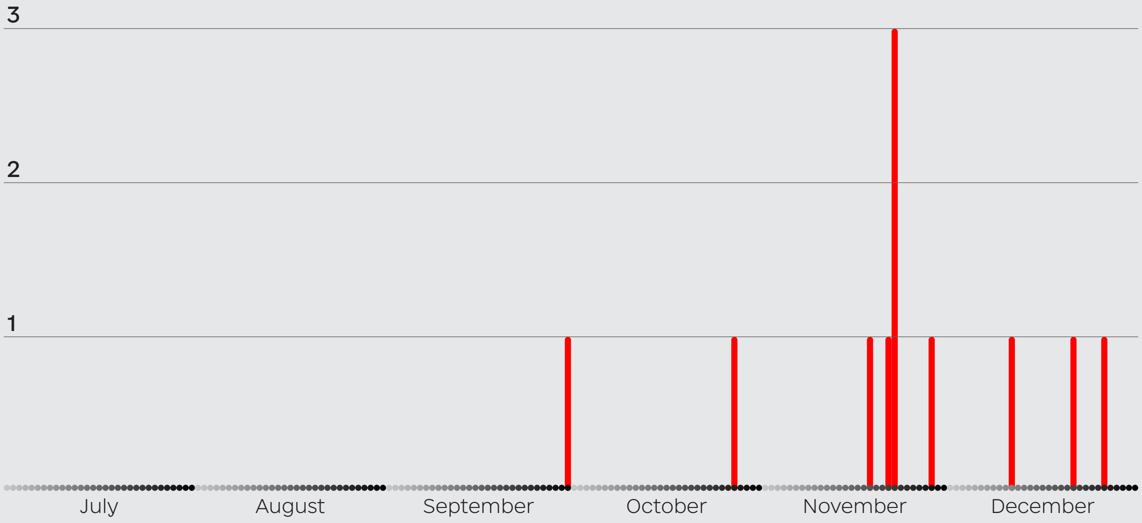
companies, such as Nova Poshta. (https://x.com/NP_official_ua/status/1871897036376748461).

UAC-0099

UAC-0099's activity is conducted for the purpose of espionage, and both the list of targeted entities and the methods used to execute malicious plans continue to evolve.

In November–December 2024, CERT-UA investigated a series of cyberattacks carried out by the UAC-0099 against several government organizations, including forestry departments, forensic medical institutions, as well as factories and other entities.

Activity of the UAC-0099



To deliver cyber threat tools, the group continues to rely on phishing emails containing attachments in the form of double-layered archives with LNK or HTA files.

Upon successful compromise, the LONEPAGE program is executed on the affected machine, enabling remote command execution. It is also important to highlight changes in tactics, techniques, and procedures (TTPs): whereas previously LONEPAGE was delivered as a VBS file placed in one of the system directories, as of December the same functionality is implemented using two components — an encrypted (3DES) file and a .NET program designed to decrypt it and execute the resulting PowerShell code directly in memory.

UAC-0001

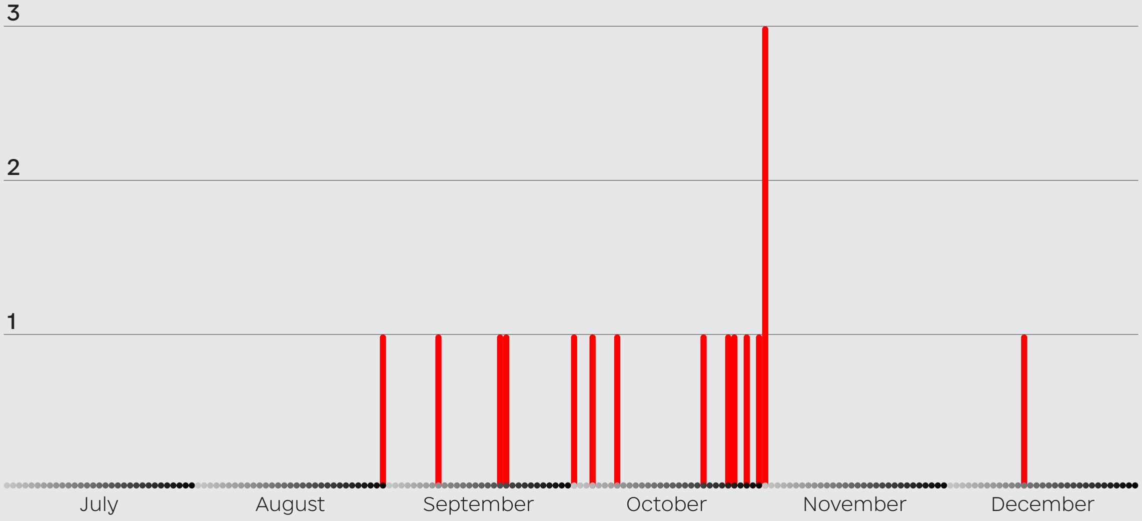
In the second half of the year, the main focus of activity remained gaining access to mailboxes using various techniques.

For example, ongoing phishing campaigns aimed at stealing authentication data from mailboxes continued, using attachments in the form of PDF or HTML files, the content of which mimics the official pages of ukr.net resources and contains links to phishing web pages. However, several campaigns were observed where a QR code was placed in the body of the email, scanning which directs the user to a phishing page. Thus, hackers bypass email protection measures. The placement of phishing pages on the Mocky service remains unchanged.

In September 2024, CERT-UA investigated a cyberattack during which attackers specifically sent out emails containing an exploit for the Roundcube vulnerability (CVE-2023-43770). Its successful exploitation could lead to the theft of authentication data and the creation of a filter to redirect the contents of the victim's mailbox to the attacker's email address.

Considering the exploited vulnerability and cyber threat indicators, the activity is associated with the UAC-0001 (APT28) group with a medium level of confidence.

Activity of the
UAC-0001



Additionally, in the fall, fake CAPTCHA pages began to be actively used worldwide for malware distribution. In October, this scheme was detected during a cyberattack on the Ukrainian network segment.

Among local government bodies, emails were distributed with a link to a page displaying a window that mimics the reCAPTCHA mechanism. Following the instructions described on the page led to the execution of a PowerShell command, which ensured the download and execution of malicious files. The main purposes of these files were to establish an SSH tunnel, launch the METASPLOIT tool, and steal and exfiltrate authentication and other browser data. After analyzing the used network infrastructure, which overlaps with the infrastructure described above, we also associate this activity with the UAC-0001 with a medium level of confidence.

As mentioned earlier, during this half-year, we observe a trend of increasing cyberattacks targeting the military sector. New threat clusters have emerged on the scene, and those that existed previously continue to evolve and change. Therefore, the focus in this section will be on this activity.

UAC-0020 (Vermin)

In the summer of 2024, CERT-UA observed two targeted cyber attacks by the UAC-0020 (Vermin) against military personnel using a new tool, FIRMACHAGENT (CERT-UA#10742), run by officers from temporarily occupied Luhansk.

The first campaign was described in the report for the first half of 2024. In both cases, the well-known toolset from 2019, the SPECTR malware, was used to collect information from the infected computer. For example, here are a few modules of this malware:

https://cert.gov.ua/article/6279600

https://cert.gov.ua/article/6280422

- **Screengrabber** — captures screenshots every 10 seconds if the application window contains the following names: "word", "excel", "office", "signal", "whatsapp", "discord", "пошта", "диск", "disk", "wallet", "anydesk", "browser", "viewer", etc.
- **FileGrabber** — copies files from specified directories and with specified extensions to another folder.
- **Usb** — has functionality similar to FileGrabber but copies files from removable (USB) drives.
- **Social** — steals configuration (authentication) data from messengers.

- **Browsers** — steals data (authentication data, session data, history) from web browsers.

Both attacks, according to the emails’ subject, were targeted at the Defense Forces of Ukraine. In the first case, the email attachments were **supposed to contain** technical specifications of the "Вовчок" turret. In the emails from the second campaign, there was a link purportedly to a list of prisoners of war being transferred from the Kursk region.

For data exfiltration **collected by SPECTR**, the attackers in these campaigns used different methods. In one case, it was the legitimate utility SyncThing, designed for file synchronization between multiple devices. Using it, they synchronized the contents of the %APPDATA%\sync\Slave_Sync\ directory, where the stolen files were copied, and transferred the data to the attackers’ host. In the other case, it was the new malware FIRMACHAGENT, designed to upload this same directory using the HTTP protocol.

UAC-0180: "Polyglots" Attack Defense Industry Enterprises (CERT-UA#10375)

At the beginning of the second half of 2024, CERT-UA detected an attempted cyberattack by the UAC-0180. Although the hackers’ activities have a wide geographical scope, its members persist in their attempts to gain unauthorized access to the computers of employees of defense enterprises and the Ukrainian militaries.

https://cert.gov.ua/article/6280099

It should be noted that they use a wide and constantly updated arsenal of malware in their cyberattacks. This malware is developed using various programming languages, including: C (ACROBAIT), Rust (ROSEBLOOM, ROSETHORN), Go (GLUEEGG), Lua (DROPCLUE).

In July, CERT-UA received information about the distribution of emails among Ukrainian defense enterprises with the subject of purchasing UAVs and an attached ZIP file, which contains a PDF document with a link.

The file named ’adobe_acrobat_fonts_pack.exe’ is downloaded from the link. This file is a malicious program called GLUEEGG, developed using the Go programming language. It is designed to decrypt and execute the DROPCLUE loader, which is developed using the Lua programming language.

The latter ensures the download and opening of the decoy document "UA-2024-07-04-010019-a-open.pdf" as well as the EXE file "font-pack-pdf-windows-64-bit”. It launches a BAT file, which in turn uses the standard utility "curl.exe" to download and install the MSI file of the legitimate remote management software ATERA, providing hackers with access to the computer.

Mobile Implants Mimic "Military" Program

Modern warfare is impossible without the use of advanced technologies for battle management, intelligence, and situational awareness. Mobile devices are used to operate special military systems. Consequently, malicious actors make significant efforts to compromise the smartphones and tablets of military personnel to steal authentication data (used to access information systems) and transmit the GPS coordinates of the devices, which can have direct negative consequences for the lives of the military personnel.

https://cert.gov.ua/article/6280563

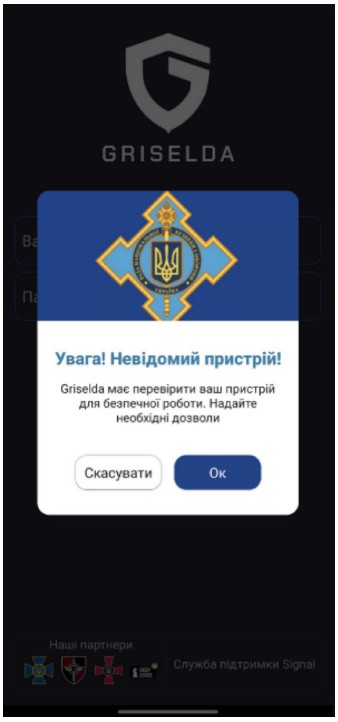
In September 2024, cyberattacks involving the distribution of malicious software for mobile devices that mimic applications of military systems GRISELDA (an automated system for input, processing, and transmission of information using artificial intelligence) and the surveillance system "Очі" were detected.

Using the Signal messenger, hackers distributed links (in the case of GRISELDA, to a copy of the project's official website, and in the case of the "Очі" system, to Google Drive) where APK files were hosted.

It should be noted that there is no "mobile version" of the GRISELDA application, and the fake website hosted the HYDRA malware, which among other things, has the functionality to steal session data (HTTP Cookies), contacts, keylogging, etc.

Regarding the "Очі" system, the APK file, in addition to the standard functionality of the original application, contained third-party code that enabled the theft of the user's login and password, as well as the collection and transmission of the device's GPS coordinates. We assume that the attackers modified the legitimate application by adding a third-party JAVA class and implementing its call in the relevant code blocks.

To track activity related to the modification of the "Очі" application, the identifier UAC-0210 has been created.



Увага! Невідомий пристрій!

Griselda має перевірити ваш пристрій для безпечної роботи. Надайте необхідні дозволи

"CONFERENCE INVITATION" FROM UAC-0185 (UNC4221) (CERT-UA#12414)

The activity of the UAC-0185 (UNC4221) group has been ongoing since at least 2022. Cybercriminals specialize in stealing credentials from messengers such as "Signal," "Telegram," "WhatsApp," and military systems like "DELTA," "ТЕНЕТА," and "Кропива." At the same time, more limited cyberattacks are conducted with the aim of gaining unauthorized remote access to the computers of employees of the defense industry enterprises, as well as the Defense Forces of Ukraine, using remote management software such as MESHAGENT and ULTRAVNC.

https://cert.gov.ua/article/6281632

In December 2024, hackers sent out emails supposedly on behalf of the Ukrainian League of Industrialists and Entrepreneurs with an invitation to a conference dedicated to the topic of changing Ukrainian defense industry products to NATO technical standards. The conference suppose to be held in Kyiv on December 5, 2024, in a hybrid format.

The email contained a hyperlink stating "The attachment contains important information for your participation," from which a shortcut file named "лист_02-1-437.lnk" was downloaded. Opening this file led to the download and execution of the "start.hta" file using the built-in mshta.exe utility. This file contained JavaScript code designed to execute two PowerShell commands: one to download and open a decoy file resembling a letter from the Ukrainian League of Industrialists and Entrepreneurs, and the other to download the "Front.png" file, which was a ZIP archive containing three files: "Main.bat," "Registry.hta," and "update.exe." The contents of the archive were extracted to the "%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update" directory, and the "Main.bat" file was executed.

The final script moves the “Registry.hta” file to the startup folder, executes it, and deletes part of the downloaded files from the computer.

As a final step, “Registry.hta” launches “update.exe,” which has been classified as a remote access tool (RAT) — MESHAGENT.

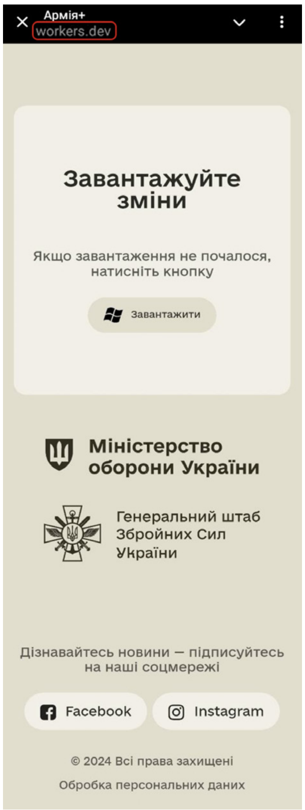
UAC-0125 Cyberattack Leveraging the "Army+" Theme

In August 2024, the “Army+” application was launched to support digital document management within the Armed Forces of Ukraine. It didn’t take long for threat actors to target the initiative. By the end of 2024, CERT-UA received reports of several malicious websites mimicking the official “Army+” app page, hosted using the Cloudflare Workers service.

https://cert.gov.ua/article/6281701

These sites offered a fake version of the “Army+” application for Windows, despite the fact that the legitimate app is only available for Android and iOS mobile devices.

The distributed fake installer ("ArmyPlusInstaller-v.0.10.23722.exe") included not only a decoy .NET application ("ArmyPlus.exe"), but also a bundled Python interpreter, an archive with Tor client files, and a PowerShell script named "init.ps1".



Армія+
workers.dev

Завантажуйте зміни

Якщо завантаження не почалося, натисніть кнопку

Завантажити

Міністерство оборони України

Генеральний штаб Збройних Сил України

Дізнавайтесь новини – підписуйтесь на наші соцмережі

Facebook

Instagram

© 2024 Всі права захищені

Обробка персональних даних

When the file "ArmyPlusInstaller-v.0.10.23722.exe" is executed, it launches the decoy application along with a PowerShell script, which is designed to:

- Install an OpenSSH server on the victim’s machine;
- Generate an RSA key pair;
- Add the public key to the "authorized_keys" file for authentication;
- Exfiltrate the private key to a threat actor-controlled server via curl (hosted on a TOR address);
- Publish a hidden SSH service using the Tor network.

As a result, a technical capability for remote and hidden access to the victim’s computer is established.

The described activity is tracked by CERT-UA under the identifier UAC-0125 and is, with a high degree of confidence, attributed to the UAC-0002 cluster (APT44 aka Sandworm).

PREVIOUS REPORTS

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

Russia’s Cyber Tactics H2’2022-EN

Russia’s Cyber Tactics H1’2023-EN

Russia’s Cyber Tactics H2’2023-EN

Russia’s Cyber Tactics H1’2024-EN

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

RUSSIAN CYBER OPERATIONS

Analytics for the H2 2024