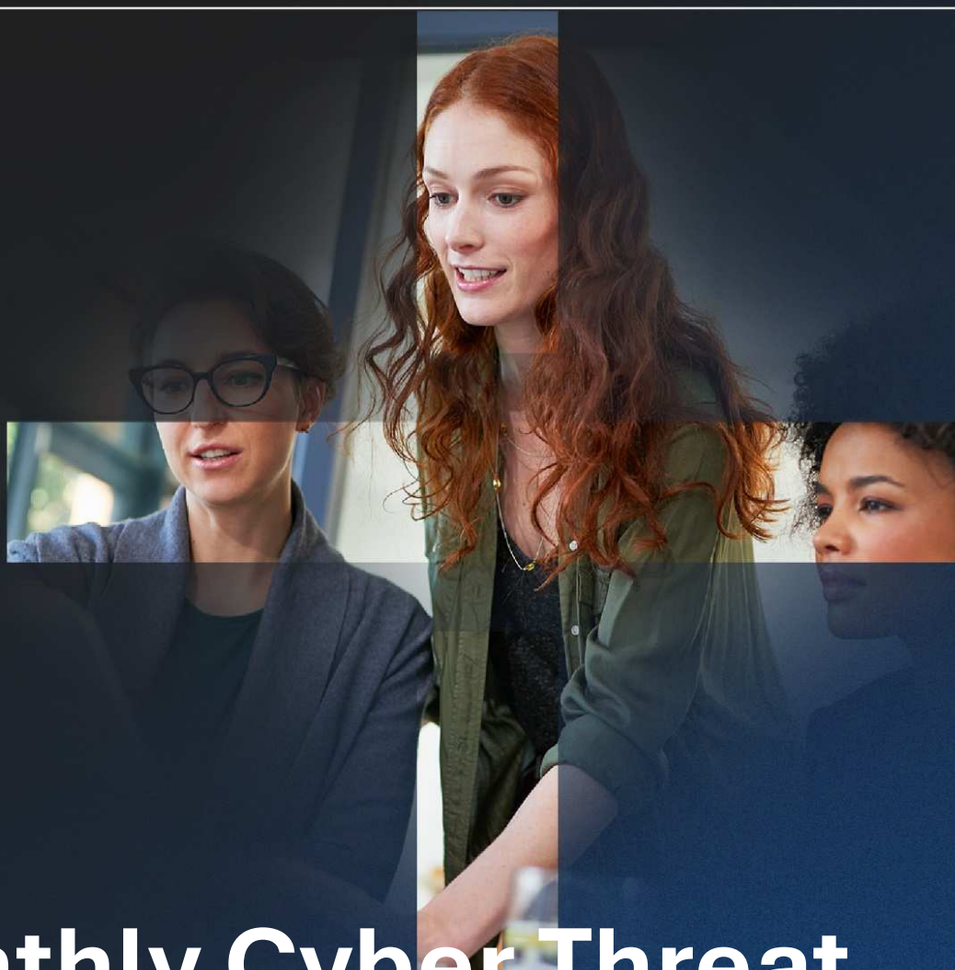
aDvens

For cyber, people & planet



Monthly Cyber Threat Intelligence report

October 2025

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, CERT aDvens offers an overview of emerging threats and current vulnerabilities to watch out for:

- Three new vulnerabilities, including one with a PoC, in addition to those already identified.
- A presentation of the APT group GHOSTWRITTER linked to the Belarusian intelligence services, with an analysis of the attack chain of its PicassoLoader malware, and its TTPs through two of its espionage campaigns.

These topics aim to anticipate risks and strengthen your cybersecurity posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights three vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (proofs of concept available, exploitation...). Applying their patches or workarounds is highly recommended.

2.1. Redis - CVE-2025-49844

On 3 October 2025, Redis published a security advisory regarding the critical vulnerability CVE-2025-49844, also known as RediShell. Discovered by researchers at Wiz, it is believed to have been present in the source code for 13 years.

A memory-release flaw in Redis allows an authenticated attacker, by manipulating the *garbage collection* mechanism via a specially crafted Lua script, to execute arbitrary code.

2.1.1. Type of vulnerability

→ **CWE-416**: Use After Free

2.1.2. Risk

→ Remote Code Execution

2.1.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Impacted Products

→ Redis OSS/CE/Stack:
- Versions prior to 6.2.20
- Versions prior to 7.2.11
- Versions prior to 7.4.6
- Versions prior to 8.0.4
- Versions prior to 8.2.2

→ Redis Software (Enterprise):
- Versions prior to 6.4.2-131
- Versions prior to 7.2.4-138
- Versions prior to 7.4.6-272
- Versions prior to 7.8.6-207

- Versions prior to 7.22.2-12

2.1.5. Recommendations

- Update Redis OSS/CE/Stack to version 6.2.20, 7.2.11, 7.4.6, 8.0.4, 8.2.2 or later.
- Update Redis Software (Enterprise) to version 6.4.2-131, 7.2.4-138, 7.4.6-272, 7.8.6-207, 7.22.2-12 or later.
- When it is not possible to upgrade immediately, it is recommended to temporarily restrict the use of the EVAL and EVALSHA command families through Access Control Lists (ACLs).

Additional information is available in Redis' ttps://redis.io/blog/security-advisory-cve-2025-49844/[advisory].

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. Veeam Backup & Replication - CVE-2025-48983

On 14 October 2025, Veeam published a security advisory regarding the critical vulnerability CVE-2025-48983.

This flaw in the Mount service of Veeam Backup & Replication allows an authenticated attacker to execute arbitrary code on the Backup infrastructure hosts.

2.2.1. Type of vulnerability

None identified

2.2.2. Risk

- Remote Code Execution

2.2.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Impacted Products

- Veaam Backup & Replication versions between 12.x and 12.3.2.3617

2.2.5. Recommendations

Update Veeam Backup & Replication to version 12.3.2.4165 Patch or later.

Additional information is available in Veeam's advisory.

2.2.6. Proof of concept

To date, no proof of concept is available in open source.

2.3. Apache Tomcat - CVE-2025-55754

Researchers from MOBIA Technology Innovations have discovered a critical vulnerability in Apache Tomcat.

An improper handling of ANSI escape sequences exists within log messages. An attacker could, through a specially crafted URL, inject ANSI sequences capable of manipulating the console display and the clipboard, with the aim of tricking an administrator into executing a command controlled by the attacker.

2.3.1. Type of vulnerability

- **CWE-150**: Improper Neutralization of Escape, Meta, or Control Sequences

2.3.2. Risk

- Remote code execution

2.3.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	Required	Impact on availability	High

2.3.4. Impacted Products

Apache Tomcat:

- Versions between 9.0.40 and 9.0.108
- Versions between 10.1.0-M1 and 10.1.44
- Versions between 11.0.0-M1 and 11.0.10

2.3.5. Recommendations

- Update Apache Tomcat to version 9.0.109, 10.1.45, 11.0.11 or later.

Additional information is available in Apache's advisory.

2.3.6. Proof of concept

To date, no proof of concept is available in open source.

3. BELARUS : THE GHOSTWRITER APT GROUP

Author : Thibaut MADEC

3.1. Introduction

Belarus presents a unique face in Europe. A republic born from the dismantling of the Soviet Union in 1991, it has been led by Alexander Lukashenko since 1994. While state communism was abandoned in favor of a more liberal economic model, large sectors of the country, such as agriculture and industry, have remained resistant to privatization. Ethnically and culturally very close to its Russian neighbor, the country is heavily dependent on the Russian Federation, while simultaneously trying to minimize the European sanctions imposed on it. While Belarus is aware of its vassalage to Moscow, which uses its territory as a rear base for military operations in Ukraine, it also seeks to position itself as a negotiating space between the stakeholders.

Sometimes nicknamed "the last dictatorship in Europe," it suffers from growing opposition from its civil society and a significant diaspora, which adds to the polarization of this country caught between two worlds: past and present, West and East. Belarus therefore offers an interesting geopolitical landscape: both excluded from other countries on the European continent, and at the same time a space for conciliation between the West and Moscow.

Despite a struggling economy, Minsk allocates significant resources to its defense. This third-tier power appears to possess two to three documented state-sponsored APTs, which is quite rare. The geopolitics and challenges facing Belarus will be presented, along with the cyber capabilities dedicated to them. The APT group GHOSTWRITER is analyzed here, including its strategy, its evolution from an influence network to a credible APT group, its own malware PicassoLoader, and its TTPs in two campaigns conducted against Ukraine and Poland.

3.2. Geopolitics of Belarus

The military parade on Independence Day in Minsk, held every July 3rd, offers a striking spectacle, as if we were back in the middle of the Cold War.

Figure 1. Military parade of 2019 (Source: Ministry of Defence of the Russian Federation, Wikimedia).

Even today, in its politics and economy, the Republic of Belarus remains fundamentally Soviet. From an external perspective, the country can be defined by three main issues and challenges:

- Its very close ties with Russia,
- Its almost non-existent ties with the rest of the European continent, or its poor relations with its Polish, Lithuanian, and Latvian neighbors,
- A segment of its population and diaspora that opposes the regime of the current leader.

3.2.1. Links with Russia

Belarus is very close culturally to Russia. A project for a union between the two countries was even envisioned in 1997. The country's subservience to Russia has accelerated since 2020 and the Kremlin's support in the contested re-election of Alexander Lukashenko that year. As a result, Belarusian territory is being used as a rear base for the Russian army, and the interests of the two countries are directly aligned.

3.2.2. Links with Europe

Belarus is aware of its position as a satellite state of Russia, and its leader is attempting to strike a balance with the rest of Europe. Alexander Lukashenko repeatedly offered to host a peace conference on Russian separatism in eastern Ukraine, leading to the Minsk I and II agreements. Despite increasing diplomatic isolation since 2020, Minsk continues to be used as a venue for meetings and negotiations between parties involved in the war in Ukraine, under the watchful eye of the Belarusian KGB. Similarly, numerous foreign embassies are present in Minsk.

3.2.3. Home surveillance

Growing popular opposition is challenging the regime led by Alexander Lukashenko. His highly contested re-election in 2020 has severely destabilized the country. A segment of the Belarusian diaspora, refugees in neighboring Poland, Lithuania, and Latvia, is working to oppose the Belarusian regime and calling for its replacement. The regime itself is particularly authoritarian, suppressing all protests and actively monitoring its population, both at home and abroad.

3.3. Belarus's cybersecurity policy

Country of 9 million people, a tertiary power and a former Soviet economy, Belarus can nevertheless pursue its interests through 3 APTs:

- **MOUSTACHEDBOUNCER**: This group was documented in 2023 but has likely been active since 2014. It targets almost exclusively foreign embassies in Belarus and their diplomatic staff. It carries out its interception at the level of Internet service providers in Man-in-the-Middle attacks. This group has also developed the modular backdoor NightClub and the malware Disco.
- **WINTER WIVERN** (aka TA473, UAC-0114 or Group G1035): This group has no formal affiliation but serves Russian and Belarusian interests and has been operating since 2020. It is characterized by creative TTPs for limited resources, notably by exploiting CVE-2023-5631 which affects Roundcube webmail portals. It targets European and sometimes Asian public entities, or certain companies, for espionage purposes in the context of the war in Ukraine. **Advens CTI published an article on this APT group in its March 2024 monthly bulletin**.
- **GHOSTWRITER** (alias UNC1151, UAC-0057, Storm-0257, FrostyNeighbor, Blue Dev 4, Moonscape or TA445): Active since 2016, the group was first documented in 2020 and is formally affiliated with the Minsk intelligence services. It targets both pro-NATO Eastern European countries and Belarusian citizens. Initially, GHOSTWRITER specialized in disinformation campaigns involving the writing of fake articles, hence its name. The group evolved its capabilities after 2020 and now conducts espionage campaigns. It has also developed its own malware: PicassoLoader.

> Cyber intelligence currently strongly suspects the Kremlin's involvement in this recent increase in capabilities, although no concrete evidence can formally confirm it. Collaboration between intelligence agencies, particularly the Russian FSB and the Belarusian KGB, is already underway and has been officially endorsed by A. Lukashenko. Belarus had shown serious technical shortcomings in its handling of the internal unrest in 2020, particularly against the Cyber Partisans group, composed of dissidents and former officers. These deficiencies seem inconsistent with the level of sophistication currently displayed by GHOSTWRITER.

3.4. GHOSTWRITER

The group takes its name from its initial disinformation campaigns starting in 2016: it stole the real credentials of journalists, columnists, and bloggers to publish articles in their names, promoting an anti-NATO narrative in Central and Eastern Europe. The platforms used were varied: online newspapers, blogs, and social media, all with the goal of influence and disinformation. These articles were then disseminated via email and social media. The name GHOSTWRITER refers indistinctly to both the group and the influence campaign, which has been ongoing since 2016. This campaign revolved around an anti-NATO narrative before 2020. From mid-2020 onwards, this narrative evolved to target specifically Belarus's immediate neighbors.

Since 2016, domain names impersonating legitimate resources have been registered to exfiltrate credentials from media outlets, regional webmail providers, national and local administrations, as well as private companies. The targeted countries include Ukraine, Poland, Lithuania, Latvia, Germany, but also France, Spain, and Ireland (with the notable exception of Estonia). Belarusian media outlets and opposition public figures have also been targeted in Belarus.

The group refined its tactics, techniques, and procedures (TTPs) after 2020: It uses GoPhish for sending phishing emails, leveraging the SMTP2GO service to appear legitimate. CloudFlare is now used for hosting instead of Freenom, which may indicate an increase in its resources.

Two small malware programs were developed in .NET with basic command functionalities:

- HIDDENVALUE: Backdoor distributed via phishing email. It allows for the execution of remote commands and the collection of information on the compromised machine.
- HALFSHELL: A variant that offers new commands and evasion techniques.

Activity continued in 2022 with the Russian offensive in Ukraine and the targeting of Ukrainian users on Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki (Ok.ru, a Russian-language social network), and VK, still with the aim of spreading disinformation. However, the observed modus operandi, tracked as UNC1151/GHOSTWRITER, appears to be increasingly focused on espionage rather than influence operations, and is changing in scope. On March 7, 2022, CERT-UA published an alert regarding the targeting of Ukrainian public entities to distribute MicroBackdoor via phishing emails, attributing the activity to UNC1151. MicroBackdoor is an open-source backdoor used for C2 communication.

Starting in 2022, CERT-UA issued several alerts regarding the distribution of a new malware, PicassoLoader. The Ukrainians officially attribute the development of this malicious software to UNC1151/GHOSTWRITER.

The resources and infrastructure do not indicate any overlap with APT groups from the Russian Federation; however, some of their activities strongly converge with those of GHOSTWRITER during similar periods.

The following diamond model illustrates GHOSTWRITER's activities at a strategic level:

3.5. PicassoLoader

The malware gets its name from its use of JPEG files to conceal the payload within a file overlay.

In its first incident, CERT-UA identified a phishing email campaign on March 16, 2023, with a PPT document attached. This document contained a thumbnail of the Ivan Chernyakhivsky Defense University, the Ukrainian Military Academy, and a macro. Opening this macro generated the file *APPDATA%\Signal_update_6.0.3.4\glkgh90kjykjkl650kj0.dll*, along with a shortcut to run it. glkgh90kjykjkl650kj0.dll was identified as PicassoLoader, which was required to download and decrypt an image to launch Cobalt Strike Beacon.

In a second incident reported on 23 July 2023, CERT-UA identified the targeting of Ukrainian public organizations by phishing emails this time containing XLS documents. PerekazF173_04072023.xls and Rahunok_05072023.xls contain a legitimate macro, and another allowing PicassoLoader to launch and ensure its persistence. The malware includes a new feature: it does not execute if it detects Avast, FireEye, or Fortinet on the victim's computer (by searching for the processes AvastUI.exe, AvastSvc.exe, xagt.exe, fcappdb.exe, and FortiWF.exe). PicassoLoader then downloads, decrypts, and launches the njRAT trojan.

Analysis of an incident reveals how victims are tricked into running the macros:

- An Excel file containing macros (XLSM) sent via email masquerades as a spreadsheet for calculating the salaries of Ukrainian employees.
- The macro is named "sumpropua," short for "Suma Propisom UA," a Latin transliteration of the Ukrainian "сума прописом UA." This term refers to financial documents where the total amount paid must be written out in words.
- This process of converting currency to words is tedious, and macros are commonly used to automatically fill in the cells.

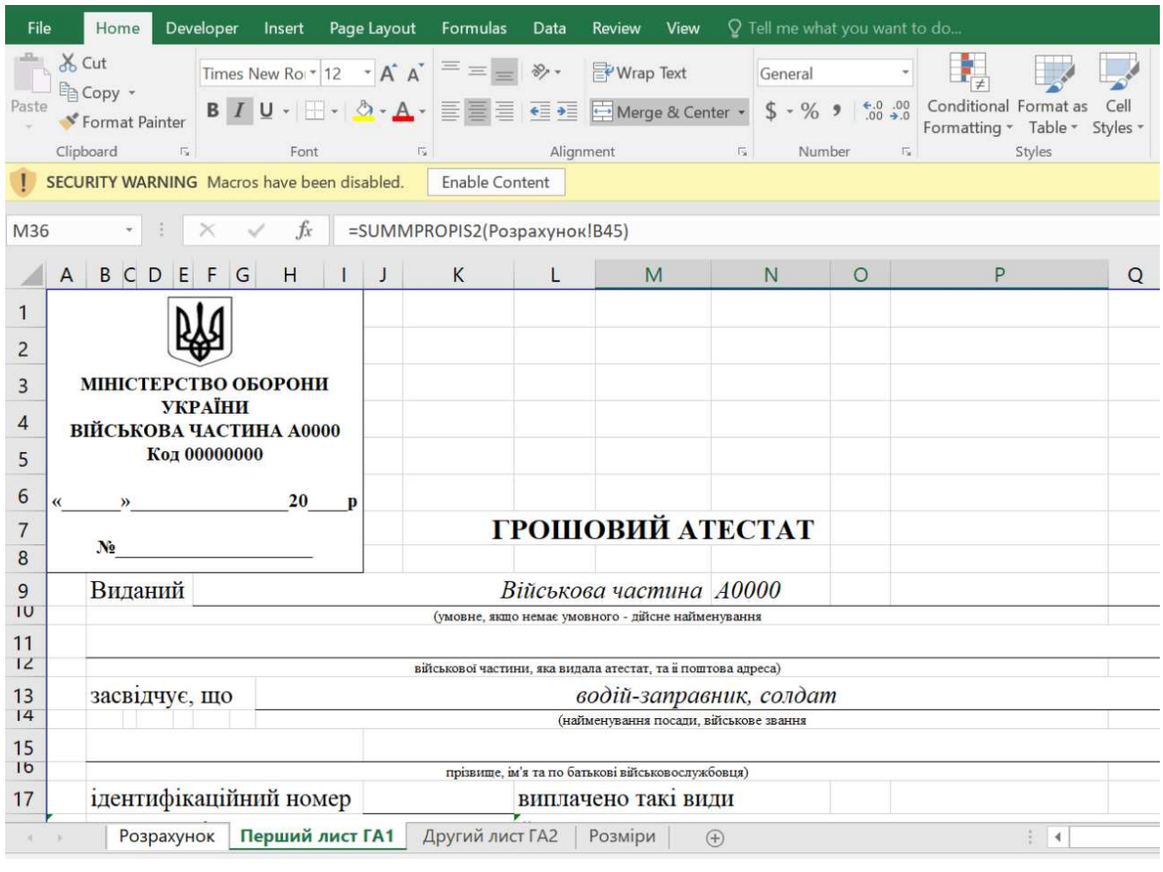


Figure 2. Malicious XLSM document distributed as an attachment (Source: Fortinet).

The malicious function *SUMMPROPIS2* executes as soon as the file is opened via the *Workbook_Open()* function. This malicious function is present in several cells, allowing the malware to execute multiple times after the file is opened. The VBA code uses simple obfuscations to avoid detection; the embedded malicious binary file is encoded as a hexadecimal string.

Meanwhile, the main malicious function *OpenModule* decodes a binary file from this string and saves it to the

%AppData%\Microsoft\fhasbqwn.dll directory.

3.5.1. First step loader

The first stage loader is executed with the following command:

```
C:\Windows\System32\regsvr32.exe /u /s « %AppData%\Microsoft\fhasbqwn.dll
```

The /s option enables silent execution without opening any Windows dialog boxes. The /u option executes the exported function *DllUnregisterServer*. This DLL is protected by ConfuserEx, an open-source .NET application protection tool, to prevent any analysis.

A second exported function, *DllCanUnloadNow*, is executed with the following command:

```
C:\Windows\System32\rundll32.exe %Temp%\kbdlisus.dll,DllCanUnloadNow
```

An apparently harmless JPEG file is downloaded from a domain name registered by the attackers (here hxxps://ellechina[.]online/01_logo_HLW-300x168[.]jpg)

Figure 3. Example of a downloaded image (Source: Fortinet).

Additional binary data within the JPEG contains the second-stage loader, encrypted and compressed within a file overlay. This overlay is decrypted using the AES algorithm with a hard-coded key. Another .NET file, sdafsfdpieowrfb.exe, is then extracted, also protected by ConfuserEx.

Here are other examples of images downloaded by PicassoLoader (Source: Cisco Talos):

3.5.2. Second step loader

This second-level loader searches for specific antivirus scanning processes like Avast, or tools like Process Explorer and Process Hacker. If these processes are detected, the operation is stopped. A third-level DLL is extracted and placed in *%AppData%*, randomly named after a subdirectory, such as *Adobe.dll* or *Microsoft.dll*.

The malware then creates a scheduled task named "Scheduled," described as "NTFS Volume Health Scan." Microsoft Corporation is listed as the task's author to make it appear as a legitimate system task. Instead of using schtasks.exe to create the scheduled task, the malware uses the COM function *ITaskFolder::RegisterTaskDefinition*. This could be a mechanism for concealing itself from EDRs, which are capable of detecting suspicious use of schtasks.exe. This task then executes the previously deposited DLL to ensure persistence when the victim logs into Windows.

This DLL developped in C/C++ is a loader for distributing Cobalt Strike Beacon, in order to infiltrate the victim's computer, along with an identified C2 server URL.

Another activity of PicassoLoader was reported by CERT-UA between 12 and 18 July 2024, targeting Ukrainian local authorities. The use of this malware bears the exclusive signature of the GHOSTWRITER threat. Excel files containing malicious macros are being sent via email regarding local government reform (USAID/DAI and HOVERLA projects). The targeted agents and the theme used indicate precise targeting by the attacker.

3.6. GHOSTWRITER campaigns

It is thus observed that the capabilities, motivations, and scope of GHOSTWRITER evolved significantly starting with the 2022 offensive. It is suspected that these developments began before the offensive, starting in 2020. Current intelligence also suggests that this evolution from an influence network producing fake articles to a credible threat actor focused on espionage and a potential IAB was initiated and facilitated by the Kremlin. These hypotheses are plausible given Belarus's role as a proxy for Moscow and the fact that its territory serves as a rear base for Russian troops in the Ukrainian theater.

3.6.1. November-December 2024 campaign

Belarusian targets

It has been observed that the TTPs deployed against Ukrainian targets are also being used against Belarusian citizens.

Phishing emails are being sent with an attached RAR archive containing an Excel spreadsheet named политзаключенные(по судам минска).xls ("Political Prisoners (Minsk Courts).xls"). The archive was created on January 14, 2025, a date likely corresponding to the presidential election of January 26, 2025. To date, this is the first time that the GHOSTWRITER activity has been directed against Belarusians people rather than foreign personnel.

The XLS document again contains a VBA macro that activates when the document is opened, as soon as macros are enabled by the victim. This macro creates a DLL file in the *%Temp%\Realtek(r)Audio.dll* directory, which is launched by the following command:

```
C:\Windows\System32\regsvr32.exe /u /s "C:\Temp\Realtek(r)Audio.dll"
```

It launches regsvr32.exe, which activates the *DllUnregisterServer* function embedded in the first DLL. This function loads and executes Dwnldr.dll. This DLL is protected by ConfuserEx, following a similar pattern to UNC1151. This DLL hosts a simplified version of PicassoLoader. This variant appears to have been modified to make it a less expensive and more easily replaceable tool.

Dwnldr.dll creates a decoy Excel spreadsheet in *%AppData%\Roaming\Microsoft\temp.xlsx*, while simultaneously downloading other files from the internet. The file temp.xlsx is immediately opened in Excel to make the victim believe that they are viewing the attachment политзаключенные(по судам минска).xls:

	A	B	C	D	E	F	
1	**Имя и фамилия**	**Предъявленые обвинения**	**Решение суда**	**Вид наказания**	**Судья**	**Прокурор**	**Место з**
2	Троцкий Василий	ст. 369 Уголовного кодекса — Оскорбление представителя власти	1 год и 2 месяца	лишение свободы в колонии в условиях общего режима	Андрушенко Андрей	Ярошникова	освобож
3		ст. 391 Уголовного кодекса — Оскорбление судьи					
4							
5	Синяк Евгений	ст. 342 Уголовного кодекса — Организация и подготовка действий, грубо нарушающих общественный порядок, либо активное участие в них	2 года	ограничение свободы с направлением в исправительное учреждение открытого типа ("химия")	Маручек Сергей	Ярошик, Плышевский	
6							
		ст. 342 Уголовного кодекса — Организация и подготовка действий, грубо нарушающих общественный порядок,		ограничение свободы без направления в			

Sheet1

Figure 4. File containing a list of people charged with the names of prosecutors and judges (Source: SentinelOne).

The source of the data used to deceive the victim demonstrates a pernicious social engineering tactic. While the displayed data may appear to be a government leak, it actually originates from Spring96, a political opposition website banned in Belarus.

Meanwhile, Dwnldr.dll retrieves a JPG file from a domain name belonging to the attackers:

Figure 5. File retrieved from hxxps://everythingandthedog[.]shop/petsblog/2020/2/25/tips-for-taking-difficult-dogs-on-a-walk[.]jpg (Source: SentinelOne).

The HTTP request is issued with a hard-coded User-Agent string:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/555.36 (KHTML, like Gecko) Chrome/97.0.4692.71
```

```
Safari/537.36
```

The JPG file here is benign and comes from an open-source image bank. The same image exists on the legitimate website hxxps://www.everythingandthedog[.]com, which the attackers copied. The file is then renamed and saved in *%APPDATA%\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll*. It is thus registered to be loaded at machine startup.

Analysis reveals that this JPG file is indeed harmless. The payload distribution is managed by the attackers only after verification of several pieces of information: UserAgent, IP addresses, etc. Previous incidents on Ukrainian targets show that the payload is only distributed to machines with a Ukrainian IP address.

Ukrainian targets

The same activity targeted Ukrainian personnel around the same time, with slight variations. The phishing emails were sent under the guise of an anti-corruption initiative within Ukrainian government agencies. The attackers used Macropack, a now-abandoned open-source obfuscation tool, to write macros for other malicious XLS documents.

The pattern is otherwise the same as observed previously. Once the macro is executed, an obfuscated .NET DLL launches a function exported via rundll32.exe. A decoy document is displayed while an image file is downloaded from the domain hxxps://sciencealert.shop. Again, the same image is available from a legitimate domain, hxxps://www.sciencealert.com, copied by the attackers. Once downloaded, the malware extracts the file to the following location: %APPDATA%\Roaming\Microsoft\SystemCertificates\CertificateCenter.dll.

A configuration text file is created in *%APPDATA%\Roaming\Microsoft\SystemCertificates\config*.

This file is used to execute MSBuild.exe, which compiles a new application: _C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe %AppData%\Roaming\Microsoft\SystemCertificates\config

If the command is successful, a file is created in this location, containing the final payload: *%AppData%\Roaming\Microsoft\SystemCertificates\Bin\Certificate.exe*

Other phishing campaigns targeted Ukrainian entities around the same time, using the theme of supplying the armed forces. Attached XLS documents contain malicious macros; the infection chain then follows the same pattern.

3.6.2. April 2025 campaign

In July 2025, a campaign was observed that had been active since April 2025 and was attributed to GHOSTWRITER, targeting Ukraine and Poland. This time, the malicious XLS files were compressed into archives, likely distributed via malicious emails. The XLS files executed VBA macros, which created DLL files loaded by regsvr32.exe. This first DLL was obfuscated with ConfuserEx, collected information, and sent to a C2 server from which it retrieved instructions for the second stage.

Ukrainian targets

The decoy file покрокова інструкція.pdf (“step-by-step instructions”) contained in the archive was created on May 30, 2025. A similar legitimate document was published on April 17, 2025, by the Ministry of Digital Transformation of Ukraine. The archive also contains XLS files whose infection chain leading to the DLL evolved between June and July 2025. Here are three examples:

- A VBA macro registers a DLL in *%TEMP%\DefenderProtectionScope.log* and uses the Shell.ShellExecute method to load it with the command *regsvr32 /u /s %TEMP%\DefenderProtectionScope.log*.
- A VBA macro decrypts the DLL and saves it to *%LOCALAPPDATA%\Serv\0x00bac729fe.log*. It then creates an LNK file (*%APPDATA%\Microsoft\Windows\Protection overview.lnk*) configured to execute the command *C:\Windows\System32\regsvr32.exe /u /s "%LOCALAPPDATA%\Serv\0x00bac729fe.log"*.
- Another example does not directly drop the DLL, but first writes a Microsoft Cabinet (CAB) file to *%TEMP%\sdw9gobh0n*. An LNK file is created that uses expand.exe to extract the DLL from the CAB file to *%LOCALAPPDATA%\Logs\sdw9gobh0n.log*.

This DLL is used to download a second-stage loader to collect information about compromised machines:

- Operating system platform ID and version,
- Hostname,
- Processor name (via a WMI request),
- Current username,
- Operating system installation date (via a WMI request),
- System boot date,
- Name and installation date of the installed antivirus product (via a WMI request),
- Information about the IP address used for internet browsing (obtained via an HTTP GET request to hxxps://ip-info.ff.avast[.]com/v1/info).

This information is then sent to the C2 server via an HTTP POST request, for example hxxps://punandjokes[.]icu/cannabis-jokes.jpg. Information is sent every 10 minutes, and an attempt to download the next sequence is initiated every 30 minutes. Once retrieved, it is saved in *%APPDATA%\Microsoft\System\ProtectedCertSystem.dll*. It is executed with the following command:

```
rundll32 %APPDATA%\Microsoft\System\ProtectedCertSystem.dll,#1
```

Polish targets

The same activity targeted Poland with documents 1_39ZO ZGWRP_zaproszenie.pdf in Polish. This invitation to the general assembly of the Związek Gmin Wiejskich Rzeczypospolitej Polskiej (Union of Rural Municipalities of Poland) further confirms GHOSTWRITER's tendency to target local authorities. Here again, the PDF document is copied from a legitimate PDF created on 21 April 2025, by the Polish authorities. The other malicious XLS documents contain macros developped with MacroPack that follow the same processes as those already observed.

The DLL developped in C++ generates a second DLL registered in the *%APPDATA%\DiagnosticComponents\DiagnosticComponents.dll* location.

It again uses the Windows Task Scheduler's COM interface to register the scheduled task \ExpDiagnosticDataSettings, which executes DiagnosticComponents.dll. This file then serves as a loader for Cobalt Strike Beacon, which communicates with a remote C2 server (here, hxxps://medpagetoday[.]icu).

The identified C2 infrastructures are the same as those used in the activities that targeted Ukraine and Poland. For each of the registered domains, the attackers use Cloudflare proxy servers. The domain names again spoof legitimate websites (for example, medpagetoday[.]icu is a copy of medpagetoday[.]com).

The domain name sweetgeorgiayarns[.]online, used as a C2 address by the attackers, automatically redirects to the legitimate video game website curseforge[.]com. A website curseforge[.]icu, registered in the same way, also redirects to curseforge[.]com. It is not confirmed whether this redirection is intentional. This configuration could allow the attackers to bypass web filtering services.

3.7. MITRE ATT&CK matrix

INITIAL ACCESS

T1566.001 : Phishing: Spearphishing Attachment T1190 : Exploit Public Facing Application

EXECUTION

T1053.005 : Scheduled Tak/Job : Scheduled Task T1059.005 : Command and Scripting Interpreter : Visual Basic T1059.006 : Command and Scripting Interpreter : Python T1203 : Exploitation for Client Execution

PERSISTANCE

T1547.001 : Boot or Logon Autostart Execution : Registry Run Keys / Startup Folder

DEFENSE EVASION

T1218.005 : System Binary Proxy Execution: Mshta T1112 : Modify Registry T11140 : Deobfuscate/decode files or information T1027 : Obfuscated Files or Information T1208.011 : System Binary Proxy Execution: Rundll32 T1218.010 : System Binary Proxy Execution: Regsvr32

PRIVILEGE ESCALATION

T1574.002 : Hijack Execution Flow: DLL Side-Loading

DISCOVERY

T1057 : Process Discovery T1518.001 : Security Software Discovery

IMPACT

T1491 : Defacement T1486 : Data Encrypted for Impact T1498 : Network denial of service

COMMAND AND CONTROL

T1071 : Application Layer Protocol T1105 : Ingress Tool Transfer

3.8. Conclusion

GHOSTWRITER presents a unique and unprecedented profile within the landscape of state-sponsored APT units. Initially an influence network specializing in the creation of fake articles, a kind of enhanced troll farm, the group has capitalized on its credential theft capabilities to completely reinvent itself. This reinvention was not only based on the skills of its members or the Belarusian KGB, and suggests the existence of exchange programs between Russian and Belarusian intelligence services and officers. Regardless, GHOSTWRITER, with its new tactics and tools, is now positioning itself as a credible threat actor.

Beyond its unique history, GHOSTWRITER still maintains a distinctive identity, with domain names mimicking legitimate websites and payloads disguised within images.

That said, with its increased scale, GHOSTWRITER may well assume a more active and less clandestine role in Europe. While the group has so far focused on Ukraine and its immediate neighbors, Belarusian interests could lead it to target other Western European countries. According to Mandiant, the group already registered a domain name mimicking a French military website in 2021. This anticipated expansion could be initiated by Belarus, or to conduct proxy attacks on behalf of Moscow.

3.9. Indicators of compromission

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	SHA-256	5df1e1d67b92e2bba8641561af9967e3a54ec73600283c66b09c8165ddcb7de9	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	699c50014cdbe919855c25eb35b15dfc8e64f73945187da41d985a9d7be31a71	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	26ea842c4259c90349a1f4db92efa89ac4429a5ff380e7f72574426cfd647f1a	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	6e562afa3193c2ca5d2982e04de78cf83faa203534a6098ab5f08df94bbeb944	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	3fff6c8a8ef3f153ebbe6d469a0d970953358a25bb9b4955a2592626f011cbd6	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	730c1a02bb31d548d91ba23fce870b1dc53c4802ea4fcb0d293f96de670d74af	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	57e0280dc5b769186588cc3a27a8a9be6f6e169551bbef39f95127e9326627f2	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	f6fec3722a8c98c29c5de10969b8f70962dbb47ba53dcbcd4a3bbc63996d258d	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	deaa3f807de097c3bfff37a41e97af5091b2df0e3a6d01a11a206732f9c6e49c	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	aac430127c438224ec61a6c02ea59eb3308eb54297daac985a7b26a75485e55f	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	06380c593d122fc4987e9d4559a9573a74803455809e89dd04d476870a427cbe	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	082877e6f8b28f6cf96d3498067b0c404351847444ebc9b886054f96d85d55d4	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	082903a8bec2b0ef7c7df3e75871e70c996edcca70802d100c7f68414811c804	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	69636ddc0b263c93f10b00000c230434febbd49ecdddf5af6448449ea3a85175	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	a2a2f0281eed6ec758130d2f2b2b5d4f578ac90605f7e16a07428316c9f6424e	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	8a057d88a391a89489697634580e43dbb14ef8ab1720cb9971acc418b1a43564	July 2025 campaign against Ukraine

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	SHA-256	707a24070bd99ba545a4b8bab6a056500763a1ce7289305654eaa3132c7cbd36	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	5fa19aa32776b6ab45a99a851746fbe189f7a668daf82f3965225c1a2f8b9d36	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	3b5980c758bd61abaa4422692620104a81eefbf151361a1d8afe8e89bf38579d	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	c7e44bba26c9a57d8d0fa64a140d58f89d42fd95638b8e09bc0d2020424b640e	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	7c77d1ba7046a4b47aec8ec0f2a5f55c73073a026793ca986af22bbf38dc948c	July 2025 campaign against Ukraine
TLP:CLEAR	SHA-256	559ee2fad8d16ecaa7be398022aa7aa1adbd8f8f882a34d934be9f90f6dcb90b	July 2025 campaign against Ukraine
TLP:CLEAR	MD5	e34d6387d3ab063b0d926ac1fca8c4c4	довідка.zip
TLP:CLEAR	MD5	2556a9e1d5e9874171f51620e5c5e09a	dovidka.chm
TLP:CLEAR	MD5	bc6932a0479045b2e60896567a37a36c	file.htm
TLP:CLEAR	MD5	bd65d0d59f6127b28f0af8a7f2619588	ignit.vbs
TLP:CLEAR	MD5	fb418bb5bd3e592651d0a4f9ae668962	Windows Prefetch.lNk
TLP:CLEAR	MD5	a9dcaf1c709f96bc125c8d1262bac4b6	desktop.ini
TLP:CLEAR	MD5	d2a795af12e937eb8a89d470a96f15a5	core.dll (.NET-лоадер)ukr
TLP:CLEAR	MD5	65237e705e842da0a891c222e57fe095	microbackdoor.dll (MicroBackdoor)
TLP:CLEAR	SHA-256	4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b	XLSM Document
TLP:CLEAR	SHA-256	c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8	fhasbqwn.dll - First step loader
TLP:CLEAR	SHA-256	2927794d7c550c07303199752b8226f197d7ef497d04cf038859f95b60edc9ce	JPEG containing compressed payload
TLP:CLEAR	SHA-256	b03c9f7823810e3eeef3c0b1d6c00da4f16fdc2ced92f97f78e5676d0989d9b3	sdafsfdpieowrfb.exe - Second step loader
TLP:CLEAR	SHA-256	de8c789ef2e1da81182a7529e7b42adf2984cd6e70b02e60fd770ebe658086ae	Cobalt Strike loader

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	SHA-256	815c1571356cf328a18e0b1f3779d52e5ba11e5e4aac2d216b79bb387963c2be	Malicious Excel document
TLP:CLEAR	SHA-256	6f4642a203541426d504608eed7927718207f29be2922a4c9aa7e022f22e0deb	Malicious Excel document
TLP:CLEAR	SHA-256	88c97af92688d03601e4687b290d4d7f9f29492612e29f714f26a9278c6eda5b	Malicious Excel document
TLP:CLEAR	SHA-256	9649d58a220ed2b4474a37d6eac5f055e696769f87baf58b1d3d0b5da69cbce5	Malicious Excel document
TLP:CLEAR	SHA-256	af8104e567c6d614547acb36322ad2ed6469537cd1d78ae1be65fbde1d578abc	Malicious Excel document
TLP:CLEAR	SHA-256	de1bceb00c23e468f4f49a79ec69ec8ad3ed622a3ffc08f84c0481ad0f6f592b	Malicious Excel document
TLP:CLEAR	SHA-256	83545b07d74087acd8408d7810cafdb6c2200a72ae7dd990af40b082ad533368	Malicious Excel document
TLP:CLEAR	SHA-256	9ac5fa37f5cf3d0201f0e70a3e6527e58250ddcff77370262b8cb377e8c5995f	Malicious Excel document
TLP:CLEAR	SHA-256	d90f6e12a917ba42f7604362fafc4e74ed3ce3ffca41ed5d3456de28b2d144bf	DLL loader
TLP:CLEAR	SHA-256	08fa6aaf064470dbfac7894469457b2d78541adccba3f1bb278dd4c3f936131a	DLL loader
TLP:CLEAR	SHA-1	18151b3801bd716b5a33cfc85dbdc4ba84a00314	temp.xlsx
TLP:CLEAR	SHA-1	2c06c01f9261fe80b627695a0ed746aa8f1f3744	Донесення 5 реч фонд зборів- зразок.xls
TLP:CLEAR	SHA-1	301ffdf0c7b67e01fd2119c321e7ae09b7835afc	Zrazok.xls
TLP:CLEAR	SHA-1	853da593d2a489c2bd72a284a362d7c68c3a4d4c	Додаток 8 реч новий.xls
TLP:CLEAR	SHA-1	9d110879d101bcaec7accc3001295a53dc33371f	Донесення 5 реч – зразок.xls
TLP:CLEAR	SHA-1	ebb30fd99c2e6cbae392c337df5876759e53730d	политзаключенные (по судам минска).xls
TLP:CLEAR	SHA-1	18bcc91ad3eed529d44926f4ae65acf44480f39d	Téléchargeur
TLP:CLEAR	SHA-1	64fca582cb69d9dc2afb1b432df58fb32ac18ca1	Téléchargeur
TLP:CLEAR	SHA-1	7261ad5d4e760aa88df94b734bc44598a090852a	Téléchargeur
TLP:CLEAR	SHA-1	9fa00a4ee4e95bc50a3919d2d3c0be2a567d8845	Téléchargeur

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	SHA-1	e5ebc7deca1ff1f0a4b1462d37ef813dad8413a6	Téléchargeur
TLP:CLEAR	Domaine	sweetgeorgiayarns[.]online	C2 - July 2025 campaign against Ukraine
TLP:CLEAR	Domaine	kitchengardenseeds[.]icu	C2 - July 2025 campaign against Ukraine
TLP:CLEAR	Domaine	punandjokes[.]icu	C2 - July 2025 campaign against Ukraine
TLP:CLEAR	Domaine	taskandpurpose[.]icu	C2 - May 2025 campaign against Poland
TLP:CLEAR	Domaine	medpagetoday[.]icu	C2 - May 2025 campaign against Poland
TLP:CLEAR	Domaine	pesthacks[.]icu	C2 - April 2025 campaign against Poland
TLP:CLEAR	Domaine	curseforge[.]icu	Potential registered domain
TLP:CLEAR	URL	hooks.slack[.]com/services/T08NWSF1L78/B08P91RQ1EW/ZQzZ7IvlT81VpQijneCR0iYa	Slack C2 - April 2025 campaign against Poland
TLP:CLEAR	URL	files.slack[.]com/files-pri/T08NWSF1L78-F08NQETU5M5/owjomlhoms.jpg	Slack C2 - April 2025 campaign against Poland
TLP:CLEAR	URL	hooks.slack[.]com/services/T08N1F1F64W/B08N1FMAN94/2QGu5K7wE3k6cVQ448Qa9n4W	Slack C2 - April 2025 campaign against Poland
TLP:CLEAR	URL	files.slack[.]com/files-pri/T08N1F1F64W-F08P2HJNU2F/ocnijrarcjvzenxyqhztf.jpg	Slack C2 - April 2025 campaign against Poland
TLP:CLEAR	Domaine	carpetmarker[.]pw	C2
TLP:CLEAR	Domaine	everything-everywhere.at.ply[.]gg	C2
TLP:CLEAR	IP	185[.]175.158.27	C2
TLP:CLEAR	Domaine	backstagemerch[.]shop	C2
TLP:CLEAR	Domaine	empoweringparents[.]shop	C2
TLP:CLEAR	Domaine	lauramcinerney[.]shop	C2
TLP:CLEAR	Domaine	ellechina[.]online	C2
TLP:CLEAR	Domaine	pedaily[.]link	C2
TLP:CLEAR	Domaine	goudieelectric[.]shop	C2
TLP:CLEAR	Domaine	thevegan8[.]shop	C2
TLP:CLEAR	Domaine	americandeliriumsociety[.]shop	C2
TLP:CLEAR	Domaine	cookingwithbooks[.]shop	C2
TLP:CLEAR	Domaine	everythingandthedog[.]shop	C2
TLP:CLEAR	Domaine	pigglywigglystores[.]shop	C2

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	Domaine	sciencealert[.]shop	C2
TLP:CLEAR	Domaine	backstagemerch[.]shop	C2
TLP:CLEAR	Domaine	bryndonovan[.]shop	C2
TLP:CLEAR	Domaine	chaptercheats[.]shop	C2
TLP:CLEAR	Domaine	clairedeco[.]shop	C2
TLP:CLEAR	Domaine	connecticutchildrens[.]shop	C2
TLP:CLEAR	Domaine	disneyfoodblog[.]shop	C2
TLP:CLEAR	Domaine	eartheclipse[.]shop	C2
TLP:CLEAR	Domaine	empoweringparents[.]shop	C2
TLP:CLEAR	Domaine	foampartyhats[.]shop	C2
TLP:CLEAR	Domaine	ikitas[.]shop	C2
TLP:CLEAR	Domaine	jackbenimblekids[.]shop	C2
TLP:CLEAR	Domaine	kingarthurbaking[.]shop	C2
TLP:CLEAR	Domaine	lansdownecentre[.]shop	C2
TLP:CLEAR	Domaine	lauramcinerney[.]shop	C2
TLP:CLEAR	Domaine	medicalnewstoday[.]shop	C2
TLP:CLEAR	Domaine	moonlightmixes[.]shop	C2
TLP:CLEAR	Domaine	penandthepad[.]shop	C2
TLP:CLEAR	Domaine	physio-pedia[.]shop	C2
TLP:CLEAR	Domaine	semanticscholar[.]shop	C2
TLP:CLEAR	Domaine	simonandschuster[.]shop	C2
TLP:CLEAR	Domaine	thevegan8[.]shop	C2
TLP:CLEAR	Domaine	twisterplussize[.]shop	C2
TLP:CLEAR	Domaine	utahsadventurefamily[.]shop	C2

4. SOURCES

CVE-2025-49844

- https://www.cve.org/CVERecord?id=CVE-2025-49844
- https://www.sysdig.com/blog/cve-2025-49844-redishell
- https://redis.io/blog/security-advisory-cve-2025-49844/
- https://www.wiz.io/blog/wiz-research-redis-rce-cve-2025-49844

CVE-2025-48983

- https://www.cve.org/CVERecord?id=CVE-2025-48983
- https://www.veeam.com/kb4771

CVE-2025-55754

- https://www.cve.org/CVERecord?id=CVE-2025-55754
- https://lists.apache.org/thread/j7w54hqbkfcn0xb9xy0wnx8w5nymcbqd

*Bielorussia: the GHOSTWRITER APT group

- WILDE Gavin, SHERMAN Justin, Belarus: Cyber upstart, or Russian staging ground? [Online] CYBERSCOOP 13/01/2022, Available at : https://cyberscoop.com/belarus-cyber-upstart-or-russian-staging-ground/
- TASS, Belarus, Russia will step up security cooperation, Lukashenko pledges [Online] 13/11/2021, Available at : https://tass.com/world/1361041
- Pierre GASTINEAU, Maître-espion | Biélorussie : Ivan Tertel, le maître-espion le plus courtisé d'Europe [Online] INTELLIGENCE ONLINE 29/08/2025, Available at : https://www.intelligenceonline.fr/europe-russie/2025/08/29/ivan-tertel-le-maitre-espion-le-plus-courtise-d-europe,110513791-art
- Lee FOSTER, Sam RIDDELL, David MAINOR, Gabby RONCONE, Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned With Russian Security Interests [Online] MANDIANT 28/07/2020, Available at : https://cloud.google.com/blog/topics/threat-intelligence/ghostwriter-influence-campaign?
- Université de Cardiff, Ghostwriter Campaign as a multi-vector operation: Attempts to control its influence & the limitations of current counter-measures [Online] 2023, Available at : https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf
- CERT-UA, Цільова кібератака UAC-0057 у відношенні державних органів із застосуванням PicassoLoader/njRAT (CERT-UA#6948) [Online] 07.07.2023, Available at : https://cert.gov.ua/article/5098518
- CERT-UA, Кібератака групи UAC-0057 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109) [Online] 07.03.2022, Available at : https://cert.gov.ua/article/37626
- CERT-UA, Точковий сплеск активності UAC-0057 (CERT-UA#10340) [Online] 24.07.2024, Available at : https://cert.gov.ua/article/6280159
- FortiGuard Labs Threat Research, Ukrainian Military-Themed Excel File Delivers Multi-Stage Cobalt Strike Loader [Online] FORTINET 11/10/2022, Available at : https://www.fortinet.com/blog/threat-research/ukrainian-excel-file-delivers-multi-stage-cobalt-strike-loader
- Vanja SVAJCER, Malicious campaigns target government, military and civilian entities in Ukraine, Poland [Online] CISCO TALOS 13/07/2023, Available at : https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/
- Tom HEGEL, Ghostwriter | New Campaign Targets Ukrainian Government and Belarusian Opposition [Online] SENTINELONE 25/02/2025, Available at : https://www.sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/
- HarfangLab Cyber Threat Research Team, UAC-0057 keeps applying pressure on Ukraine and Poland [Online] HARFANGLAB 20/08/2025, Available at : https://harfanglab.io/insidethelab/uac-0057-pressure-ukraine-poland/
- Cyble Research and Intelligence Labs, UNC1151 Strikes Again: Unveiling Their Tactics Against Ukraine's Ministry of Defence [Online] CYBLE 04/06/2024, Available at : https://cyble.com/blog/unc1151-strikes-again-unveiling-their-tactics-against-ukraines-ministry-of-defence/

→ Kerstin ZETTL-SCHABATH, Jakob BUND, Lena ROTTINGER, Camille BORRETT, UNC1151 Fusing Technical and Social Vulnerabilities [Online] European Repository of Cyber Incidents [Online] 13/05/2023, Available at : https://eurepoc.eu/wp-content/uploads/2023/05/EuRepoC-APT-profile-UNC1151.pdf