

Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastructure Entities

 trendmicro.com/en_us/research/26/c/pawn-storm-targets-govt-infra.html

March 26, 2026

id	index	OLE Object
0	0027C856h	Not a well-formed OLE object
1	0027DF02h	format_id: 2 (Embedded) class name: b'file\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' data size: 2560 MD5 = '0ea6fc8d476591fd80e6cec26f353d25' CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B unknown CLSID (please report at https://github.com/decalage2/oletools/issues)
2	0027F503h	format_id: 2 (Embedded) class name: b'file\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' data size: 2560 MD5 = '6ce6b82d33d3d7305a321af207e37124' CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B unknown CLSID (please report at https://github.com/decalage2/oletools/issues)
3	00280AB9h	format_id: 2 (Embedded) class name: b'Word.Document.12' data size: 25088 MD5 = 'cad4f8ce48d31d6c10253ddb00a993' CLSID: F4754C9B-64F5-4B40-8AF4-679732AC0607 Microsoft Word Document (Word.Document.12)

Key takeaways:

- Prolific Russia-aligned Advanced Persistent Threat (APT) group Pawn Storm has been using PRISMEX, a collection of interconnected malware components to target the defense supply chain of Ukraine and its allies including Czech Republic, Poland, Romania, Slovakia, Slovenia, and Turkey.
- PRISMEX combines advanced steganography, component object model (COM) hijacking, and legitimate cloud service abuse for command and control.

- Pawn Storm actively exploited multiple vulnerabilities, including a confirmed Windows zero-day (CVE-2026-21513). The .lnk files retrieved via CVE-2026-21509 (a security feature bypass vulnerability in the Microsoft Office Object Linking and Embedding (OLE) mechanism) may chain with CVE-2026-21513 (a Protection mechanism failure in MSHTML Framework) based on shared command-and-control infrastructure identified by [Akamai](#), though TrendAI™ Research has not independently confirmed this linkage.
- Infrastructure preparations was observed to have begun two weeks before the CVE-2026-21509 disclosure, indicating advance knowledge.
- Both espionage and potential sabotage functionality were observed, including wiper commands.
- This blog provides risk management guidelines that organizations can follow to protect against the cyber threat discussed in this blog. TrendAI Vision One™ detects and blocks the IoCs provided at the end of this blog. TrendAI customers can also access tailored hunting queries, threat insights, and intelligence reports to better understand and proactively defend against this campaign.

Prolific Russian-aligned cyber espionage group Pawn Storm has deployed a new malware suite that TrendAI™ Research identifies as PRISMEX. The APT group also known as APT28, Fancy Bear, UAC-0001 and Forest Blizzard in its latest observed campaigns target the operational backbone of Ukrainian defense and Western humanitarian and military aid infrastructure. The campaigns, which have been active since at least September 2025, significantly escalated in January 2026, and continue the long-lasting brazen attacks that Pawn Storm deploys against Ukraine since 2014.

This operation demonstrates that Pawn Storm remains one of the most aggressive Russia-aligned intrusion sets. It also emphasizes the group's notoriety in leveraging newly disclosed vulnerabilities and rapidly weaponizing N-day exploits: Pawn Storm's campaign in late January 2026 exploited the Microsoft Office vulnerability [CVE-2026-21509](#) to target government, military, and critical infrastructure entities across Central and Eastern Europe. The campaign's infrastructure preparation was observed to have begun two weeks prior, hinting of the group's advanced knowledge of the vulnerability.

Looking into these latest Pawn Storm campaigns, TrendAI™ Research identified a series of interconnected malware components collectively referred to as "PRISMEX," named for its steganographic characteristic of distributing the payload across the entire image. It is comprised of a dropper (PrismexDrop), a steganography loader (PrismexLoader), and a Covenant Grunt implant (PrismexStager).

Covenant is an open-source .NET command and control (C&C) framework, and Grunts are its implant agents that feature dynamic compilation and encrypted command-and-control communications. These components are designed to evade modern Endpoint Detection and Response (EDR) systems through "fileless" execution, advanced steganography, and abuse of legitimate cloud services. TrendAI™ Research assesses that the campaigns that use

PrismexStager likely represent a strategic expansion of the "NotDoor" ecosystem, extending its multiple infection chains to now include rapid exploitation of newly disclosed vulnerabilities. TrendAI™ Research also investigated the NotDoor ecosystem in early 2025 and continues to monitor its evolution.

The use of the Covenant framework for final payloads has previously been documented by [CERT-UA](#) and [Sekoia.io](#) since mid-2025, but this current wave of attacks is distinguished by the rapid integration of CVE-2026-21509.

Analysis confirms technical links between the PRISMEX components and previous Pawn Storm activities that TrendAI™ Research has been tracking. Strategically, this latest operation focuses heavily on targeting the Ukrainian defense supply chain. This includes military allies, meteorological data providers, transport hubs, and international aid corridors that are essential to Ukrainian defense and humanitarian operations.

This campaign has also been reported by [CERT-UA](#), [Zscaler ThreatLabz](#), and [Synaptic Systems](#), with each organization providing complementary perspectives on the threat.

Campaign evolution and timeline

TrendAI™ Research has tracked Pawn Storm's activities across three distinct but interconnected campaigns, each building upon its previous infrastructure and tooling. This evolution demonstrates the threat actor's continuous adaptation and capability development.

Vulnerability exploitation

Infrastructure preparation timeline

The timeline of this campaign indicates advanced knowledge of multiple vulnerabilities:

- CVE-2026-21509: Domain registration for WebDAV servers began on January 12, 2026, exactly two weeks prior to the public disclosure on January 26.
- CVE-2026-21513: The LNK exploit sample appeared on VirusTotal on January 30, 2026, while Microsoft's patch was not released until February 10, 2026. This 11-day gap confirms zero-day exploitation in the wild.

This pattern suggests Pawn Storm had access to vulnerability details ahead of public disclosure.

CVE-2026-21509

The PRISMEX campaign's initial access vector relies on the weaponization of CVE-2026-21509, a security feature bypass vulnerability in the Microsoft Office Object Linking and Embedding (OLE) mechanism. Unlike typical memory corruption exploits, this vulnerability exploits a logical gap in

the Microsoft Office OLE allowlist mechanism. Specifically, Office failed to strictly block the instantiation of the *Shell.Explorer.1* COM object (CLSID: *EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B*).

id	index	OLE Object
0	0027C856h	Not a well-formed OLE object
1	0027DF02h	format_id: 2 (Embedded) class name: b'file\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' data size: 2560 MD5 = '0ea6fc8d476591fd80e6cec26f353d25' CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B unknown CLSID (please report at https://github.com/decalage2/oletools/issues)
2	0027F503h	format_id: 2 (Embedded) class name: b'file\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' data size: 2560 MD5 = '6ce6b82d33d3d7305a321af207e37124' CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B unknown CLSID (please report at https://github.com/decalage2/oletools/issues)
3	00280AB9h	format_id: 2 (Embedded) class name: b'Word.Document.12' data size: 25088 MD5 = 'cad4f8ce48d31d6c10253ddb00a993' CLSID: F4754C9B-64F5-4B40-8AF4-679732AC0607 Microsoft Word Document (Word.Document.12)

Figure 2. Dumped object information from a CVE-2026-21509 exploit sample using rtfobj, showing the *Shell.Explorer.1* CLSID

By embedding a specifically crafted OLE object referencing this CLSID within a Rich Text Format (RTF) document, the attacker forces the host application to automatically initiate an outbound connection. This connection targets an attacker-controlled WebDAV server to retrieve and execute a remote *.lnk* (shortcut) file. Crucially, this execution occurs without requiring user interaction beyond opening the document, effectively bypassing Protected View and standard OLE security prompts.

CVE-2026-21509 technical details:

- Vulnerability Class: Security Feature Bypass (CWE-807)
- Affected Component: *Shell.Explorer.1* COM object

- Target CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B
- Attack Vector: Specially crafted RTF documents with embedded OLE objects
- User Interaction: None required beyond opening the document

CVE-2026-21513

[CVE-2026-21513](#) resides in the logic responsible for handling hyperlink navigation within `ieframe.dll` (Internet Explorer frame). Insufficient validation of the target URL allows attacker-controlled input to reach code paths that invoke `ShellExecuteExW`, enabling execution of local or remote resources outside the intended browser security context.

The LNK file embeds an HTML payload immediately after the standard LNK structure. This payload leverages nested *iframes* and multiple DOM contexts to manipulate trust boundaries. The exploit creates an *htmlfile* ActiveX object to expose the DOM interface, then uses nested *about:blank iframes* to establish multiple execution contexts with manipulable trust relationships. The core exploit invokes `document.Script.open()` with a `_parent` target parameter, reaching the vulnerable `_AttemptShellExecuteForHlinkNavigat` function and achieving code execution outside the browser sandbox.

CVE-2026-21513 was exploited as a zero-day vulnerability. The exploit sample (SHA256: `aefd15e3c395edd16ede7685c6e97ca0350a702ee7c8585274b457166e86b1fa`) was first submitted to VirusTotal on January 30, 2026. This was 11 days before Microsoft released the patch on February 10, 2026. Akamai researchers correlated this sample with the vulnerable code path and attributed it to APT28 infrastructure.

While the observed campaign leverages malicious *.LNK* files, the vulnerable code path can be triggered through any component embedding MSHTML. Therefore, additional delivery mechanisms beyond LNK-based phishing should be expected.

The possible two-stage exploitation

Akamai researchers [reported](#) an in-the-wild exploit sample for [CVE-2026-21513](#), a critical security feature bypass vulnerability within Microsoft's MSHTML framework. This sample communicates with the same C&C domain (`wellnesscaredmed[.]com`) used in the campaign exploiting CVE-2026-21509, suggesting a potential connection between the two exploits.

If the *.lnk* files retrieved via the CVE-2026-21509 exploit chain leverage CVE-2026-21513, this would represent a sophisticated two-stage exploitation: the first vulnerability (CVE-2026-21509) forces the victim's system to retrieve a malicious *.lnk* file, which then exploits the second vulnerability (CVE-2026-21513) to bypass security features and execute payloads without user warnings. While TrendAI™ Research has yet to independently confirm this linkage, the shared infrastructure and timing strongly suggest these exploits are part of the same campaign.

Attack chain

Delivery

Spear-phishing emails are sent to targeted individuals with subject lines related to "Hydro-meteorological Warnings," "Invitation to Military Training Program," or "Weapon Smuggling Alerts."

Exploitation

The attached malicious RTF document triggers CVE-2026-21509 upon opening. This bypasses OLE security restrictions, forcing the *Shell.Explorer.1* object to browse a remote WebDAV share and automatically execute a malicious shortcut (.lnk) file contained therein.

LNK execution (potential CVE-2026-21513 exploitation)

The executed .lnk file likely exploits CVE-2026-21513 (MSHTML Security Feature Bypass) to bypass Mark of the Web and IE Enhanced Security Configuration. Based on Akamai's analysis of a related sample communicating with the same C&C infrastructure, the exploit leverages nested iframes and DOM context manipulation to reach the vulnerable *_AttemptShellExecuteForHlinkNavigate* function in *ieframe.dll*, enabling payload execution without security warnings and downloading the next-stage executables from the C&C server. Note that while the shared infrastructure strongly suggests this linkage, TrendAI™ Research has not independently confirmed that the .lnk files in this campaign exploit CVE-2026-21513.

Payload selection

The C&C server delivers one of two primary payload chains: Path A (PRISMEX) or [Path B](#) (MiniDoor Chainm which is reported by Zscaler ThreatLabz).

An analysis of the PRISMEX components

TrendAI™ Research uses the name "PRISMEX" to collectively refer to the interconnected malware components identified across these campaigns. While our investigation cannot confirm whether the threat actor developed these as a unified framework, TrendAI™ Research has observed that the components work together in coherent infection chains designed to evade modern EDR systems through fileless execution, advanced steganography, and abuse of legitimate cloud services.

PRISMEX includes the following components, which this section analyzes in detail:

- PrismexSheet: A malicious Excel dropper with VBA macros that extracts payloads embedded within the file itself using steganography techniques.
- PrismexDrop: A native dropper that prepares the environment for subsequent stages, establishing persistence via COM hijacking.

- PrismexLoader: A proxy DLL that extracts payloads from steganographic PNG images using a unique "Bit Plane Round Robin" algorithm.
- PrismexStager: A Covenant Grunt Stager that abuses File.io cloud storage for C&C communications.

PrismexSheet: The Excel dropper

PrismexSheet is a highly obfuscated Excel dropper that serves as the initial access vector in the September-December 2025 steganography campaign. The specimen is designed to extract malicious payloads (executable files and configuration information) hidden within the Excel file's binary data area and execute/persist them on the infected terminal. A notable feature is the use of steganography techniques to embed the payload within the file itself.

TrendAI™ Research identified and analyzed several variants of PrismexSheet, all sharing the same core functionality but with variations in configuration and obfuscation. The malware execution flow consists of five distinct stages illustrated in figure 4.

Stage 1: Initialization and evasion

When the macro is enabled, *Workbook_Open* is triggered to perform initial setup and sandbox evasion:

- Worksheet Concealment: Sets `Visible = 2 (xlSheetVeryHidden)` to hide the malicious sheet from the user.
- Sandbox Evasion: Uses the `gethostbyname` API to attempt name resolution of `dropbox[.]com`. This confirms internet connectivity and suppresses operation in automated analysis sandbox environments where the network is isolated.

Stage 2: Configuration and payload extraction

The macro reads the Excel file's own binary data and searches for specific signatures to locate embedded components:

- Self-reading: Uses `ADODB.Stream` to read its own file binary into memory.
- Signature search: Uses custom functions `SearchBytes` and `SearchEB` to locate configuration start signatures (variant-specific), PNG image markers (89 50 4E 47 0D), and PE executable markers (4D 5A 90 00 03).
- Configuration parsing: The Config block is delimited by pipe characters (|) and contains drop destination paths, payload filenames, PNG image filenames, and other operational parameters.

```

003E80 6F 25 E7 A8 9C A3 72 8E-CA 39 2A E7 A8 9C A3 72 0%.r..9*...r
003E90 8E AA 78 2E 79 7A F5 04-1E 9A F2 1E 2C 00 00 00 ..x.yz.....,...
003EA0 00 49 45 4E 44 AE 42 60-82 31 33 38 45 32 34 37 .IEND.B`.138E247
003EB0 33 7C 70 72 6F 67 72 61-6D 64 61 74 61 7C 61 64 3|programdata|ad
003EC0 77 61 70 69 36 34 2E 64-6C 6C 7C 70 72 6F 67 72 wapi64.dll|progr
003ED0 61 6D 64 61 74 61 7C 4D-69 63 72 6F 73 6F 66 74 amdata|Microsoft
003EE0 5C 44 65 76 69 63 65 53-79 6E 63 5C 38 61 63 64 \DeviceSync\8acd
003EF0 36 65 37 31 2D 62 66 31-30 2D 34 38 30 30 2D 61 6e71-bf10-4800-a
003F00 65 65 65 2D 37 64 65 30-30 65 64 63 39 37 38 31 eee-7de00edc9781
003F10 7C 62 61 63 6B 67 72 6F-75 6E 64 2E 70 6E 67 7C |background.png|
003F20 44 45 46 41 55 4C 54 2D-33 51 37 4A 36 31 57 2D DEFAULT-3Q7J61W-
003F30 32 30 32 35 31 31 30 31-2D 31 30 34 35 2E 6C 6F 20251101-1045.lo
003F40 67 7C 53 6F 66 74 77 61-72 65 5C 43 6C 61 73 73 g|Software\Class
003F50 65 73 5C 43 4C 53 49 44-5C 7B 36 38 44 44 42 42 es\CLSID\{68DDBB
003F60 7C 35 36 2D 39 44 31 44-2D 34 46 44 39 2D 38 39 |56-9D1D-4FD9-89
003F70 43 35 2D 43 30 44 41 32-41 36 32 35 33 39 32 7D C5-C0DA2A625392}
003F80 5C 49 6E 50 72 6F 63 53-65 72 76 65 72 33 32 7C \InProcServer32|
003F90 25 70 72 6F 67 72 61 6D-64 61 74 61 25 5C 55 53 %programdata%\US
003FA0 4F 53 68 61 72 65 64 5C-4C 6F 67 73 5C 55 73 65 OShared\Logs\Use
003FB0 72 5C 61 64 77 61 70 69-36 34 2E 64 6C 6C 7C 55 r\adwapi64.dll|U
003FC0 53 4F 53 68 61 72 65 64-5C 4C 6F 67 73 5C 55 73 S0Shared\Logs\Us
003FD0 65 72 7C 74 61 73 6B 6B-69 6C 6C 2E 65 78 65 7C er|taskkill.exe|
003FE0 65 78 70 6C 6F 72 65 72-2E 65 78 65 7C 77 69 6E explorer.exe|win
003FF0 64 69 72 7C 4D 5A 90 00-03 00 00 00 04 00 00 00 dir|MZ.....
004000 FF FF 00 00 B8 00 00 00-00 00 00 00 40 00 00 00 .....@...
004010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
004020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
004030 10 01 00 00 0E 1F BA 0E-00 B4 09 CD 21 B8 01 4C .....!..L
004040 CD 21 54 68 69 73 20 70-72 6F 67 72 61 6D 20 63 ..!This program c
004050 61 6E 6E 6F 74 20 62 65-20 72 75 6E 20 69 6E 20 annot be run in
004060 44 4F 53 20 6D 6F 64 65-2E 0D 0D 0A 24 00 00 00 DOS mode....$.
004070 00 00 00 00 3E B6 24 FE-7A D7 4A AD 7A D7 4A AD ....>$.z.J.z.J.

```

Figure 5. Configuration section embedded within the Excel file, showing pipe-delimited parameters

Stage 3: File dropping

Based on the extracted configuration, the macro generates the following files:

- Payload DLL: Writes the extracted PE binary to *%TEMP%* under an initial filename (e.g., *DEFAULT-786XQ7W-20251022-2145.log*), then copies it to *%ProgramData%\USOShared\Logs\User\adwapi64.dll*.
- Steganographic PNG: Drops an image file with encrypted shellcode embedded to *%ProgramData%\Microsoft\DeviceSync\{GUID}\background.png*.

Stage 4: Persistence via COM hijacking

PrismexSheet establishes persistence by hijacking a COM object that is loaded by explorer.exe:

- 9/19

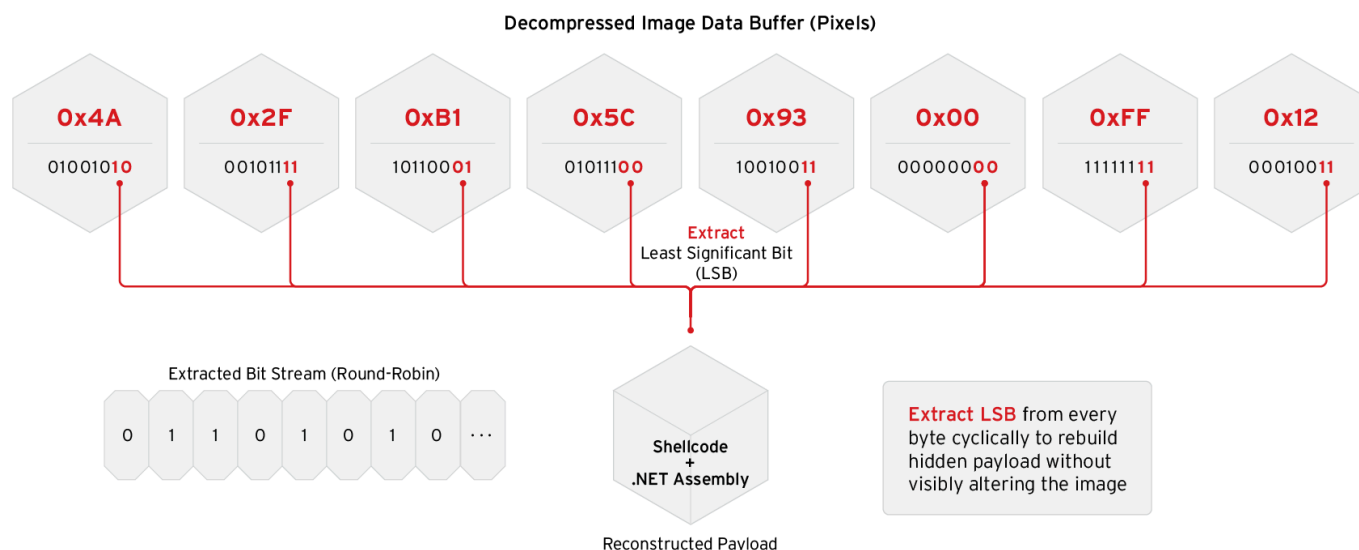
- Drop targets: Places files at `%PROGRAMDATA%\USOPublic\Data\User\EhStoreShell.dll` (malicious proxy DLL), `%PROGRAMDATA%\Microsoft OneDrive\setup\Cache\SplashScreen.png` (steganography carrier), and `%TEMP%\Diagnostics\office.xml` (task definition).
- Registry modification: Registers the dropped *EhStoreShell.dll* as the handler for `CLSID {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}` under `HKCU\Software\Classes\CLSID`.
- Trigger mechanism: A hidden scheduled task ("*OneDriveHealth*") runs once, one minute after infection, executing a command sequence that terminates and restarts `explorer.exe`. This causes the hijacked CLSID to be loaded, executing the malware within a trusted process context.

PrismexLoader: The Proxy DLL

This component masquerades as the legitimate Windows DLL like *EhStoreShell.dll*. It functions as a Proxy DLL, forwarding legitimate function exports to the real system DLL to prevent crashing the host process, while silently executing its malicious payload in a background thread.

The "Bit Plane Round Robin" steganography algorithm

The most distinctive feature of PrismexLoader is its unique method of extracting the next stage from *SplashScreen.png*. Unlike common Least Significant Bit (LSB) techniques which hide data in the last bit of consecutive bytes (often filling the image from top to bottom), this malware uses a custom "Bit Plane Round Robin" distribution that scatters the payload across the entire file structure in multiple passes.



©2026 TREND MICRO

Figure 8. Visualizing the "Bit Plane Round Robin" extraction method used by PrismexLoader. The malware cycles through the entire image buffer extracting the LSB of every byte before moving to the next bit plane.

The algorithm works as follows:

- The extraction treats the image data as a circular buffer, avoiding concentration of changes in one part of the image.
- For a given *GlobalIndex* (the sequential bit number being extracted), the algorithm computes: $ByteIndex = GlobalIndex \% BufferLength$ (which byte to read from) and $BitPosition = GlobalIndex / BufferLength$ (which bit plane to extract).
- During pass 1 (LSB Layer), the loader iterates through the entire image buffer, extracting the 0th bit (Least Significant Bit) of every byte.
- In pass 2 (Next Bit Layer), once the end of the image is reached, the extraction index wraps around to the beginning. It then extracts the 1st bit of every byte.
- Subsequent passes continue (2nd bit, 3rd bit, etc.) until the entire payload size (defined in the first 32 bits extracted) is reconstructed.

This specific algorithmic implementation is identical to code used in a previous Pawn Storm campaign from 2025 that targeted Ukrainian military drone lists. This exact algorithm has not been observed in public repositories, serving as a high-fidelity fingerprint for this developer unit.



Figure 9. The steganographic PNG image as seen when opened normally. The hidden payload is invisible to casual inspection.

Payload extraction and in-memory execution via CLR bootstrapping

After reconstructing the raw byte stream from the steganographic image, PrismexLoader performs several critical steps to prepare and execute the .NET payload entirely in memory:

- Payload sanitization: The loader scans the reconstructed byte array for the MZ header (0x4D 0x5A) to locate the start of the PE file. Data preceding the MZ header is discarded.
- CLR hosting API resolution: The loader dynamically resolves the *CLRCreateInstance* function from *mscorlib.dll*, serving as the entry point for hosting the CLR within a native process.

- Runtime interface acquisition: Using *CLRCreateInstance*, the malware obtains an *ICLRMetaHost* interface, enumerates installed runtimes, and retrieves *ICLRRuntimeInfo* for .NET Framework 4.0 or later.
- Runtime host initialization: The *ICLRRuntimeHost::Start()* method is invoked to initialize the CLR within the current process context (*explorer.exe*).
- In-memory assembly loading: The malware uses *System.Reflection.Assembly.Load(byte[])* to load the .NET assembly directly from the in-memory byte array.
- Entry point invocation: The entry point method (typically a static method in the GruntStager class) is identified and invoked using reflection APIs.

This approach provides several advantages from an evasion perspective: the .NET payload never touches the filesystem (evading file-based detection), the malicious code executes within *explorer.exe* (a highly trusted system process), and the payload exists only in memory until the host process terminates (leaving minimal forensic evidence).

PrismexStager: Covenant Grunt stager

The payload extracted from the image is the Covenant Grunt Stager, which we have internally tracked as PrismexStager. This is a .NET assembly responsible for C&C and executing further tasks from the Covenant framework. It is heavily obfuscated with randomized function names to hinder static analysis.

The malware abuses the legitimate end-to-end encrypted cloud storage service *Filen.io* for C&C communications. By leveraging this trusted service, the malicious traffic blends in with normal encrypted web traffic, effectively bypassing reputation-based filtering and firewall rules.

The C&C infrastructure utilizes multiple *Filen.io* subdomains:

- Gateway domains: *gateway.filen.io*, *gateway.filen.net*, *gateway.filen-1.net* through *gateway.filen-6.net*
- Egress domains: *egest.filen.io* (for payload download)
- Ingress domains: *ingest.filen.io* (for data exfiltration)

MITRE ATT&CK mapping

Tactic	Technique
Initial Access	T1566.001 - Spearphishing Attachment
Execution	T1059.001 - PowerShell
	T1059.005 - Visual Basic
	T1204.001 - User Execution: Malicious Link

Persistence	T1546.015 - Component Object Model Hijackin
	T1053.005 - Scheduled Task
Defense Evasion	T1574.002 - DLL Side-Loading
	T1027.003 - Steganography
	T1562.001 - Disable or Modify Tools
	T1055 - Process Injection
	T1553.005 - Mark-of-the-Web Bypass
Collection	T1114.001 - Local Email Collection
Command-and-Control	T1071.001 - Web Protocols
	T1102 - Web Service
Exfiltration	T1048.003 - Exfiltration Over Alternative Protocol

Table 1. A summary of MITRE ATT&CK techniques used in the observed Pawn Storm campaign discussed in this blog

Victimology

The targeting pattern reveals a strategic intent to compromise the supply chain and operational planning capabilities of Ukraine and its NATO partners. This targeting is a continuation of previous campaigns where Pawn Storm used their foothold in related organizations like border police, military, parliament and a meteorological institute. The choice of these sender organizations appears strategic: recipients in target organizations would be more likely to open attachments from such trusted sources, particularly those involved in cross-border cooperation and military training programs.

Targets in Ukraine:

- Sectors: Central Executive Bodies, Hydrometeorology (Strategic planning for ground/drone operations), Defense, Emergency Services.
- Specific lures: Documents related to "Hydro-meteorological Centers" (essential for artillery and drone warfare weather adjustments) and "Military Training Programs."

Targets in NATO Logistics Hubs and military allies of Ukraine:

- Poland: Rail logistics. Poland serves as the primary transit hub for Western military aid entering Ukraine.

- Romania, Slovenia, Turkey: Maritime and transport sectors. Romania is critical for Black Sea grain corridors and alternative supply routes.
- Slovakia and Czech Republic: Political and logistical support partners involved in ammunition initiatives.
- Military and NATO partners

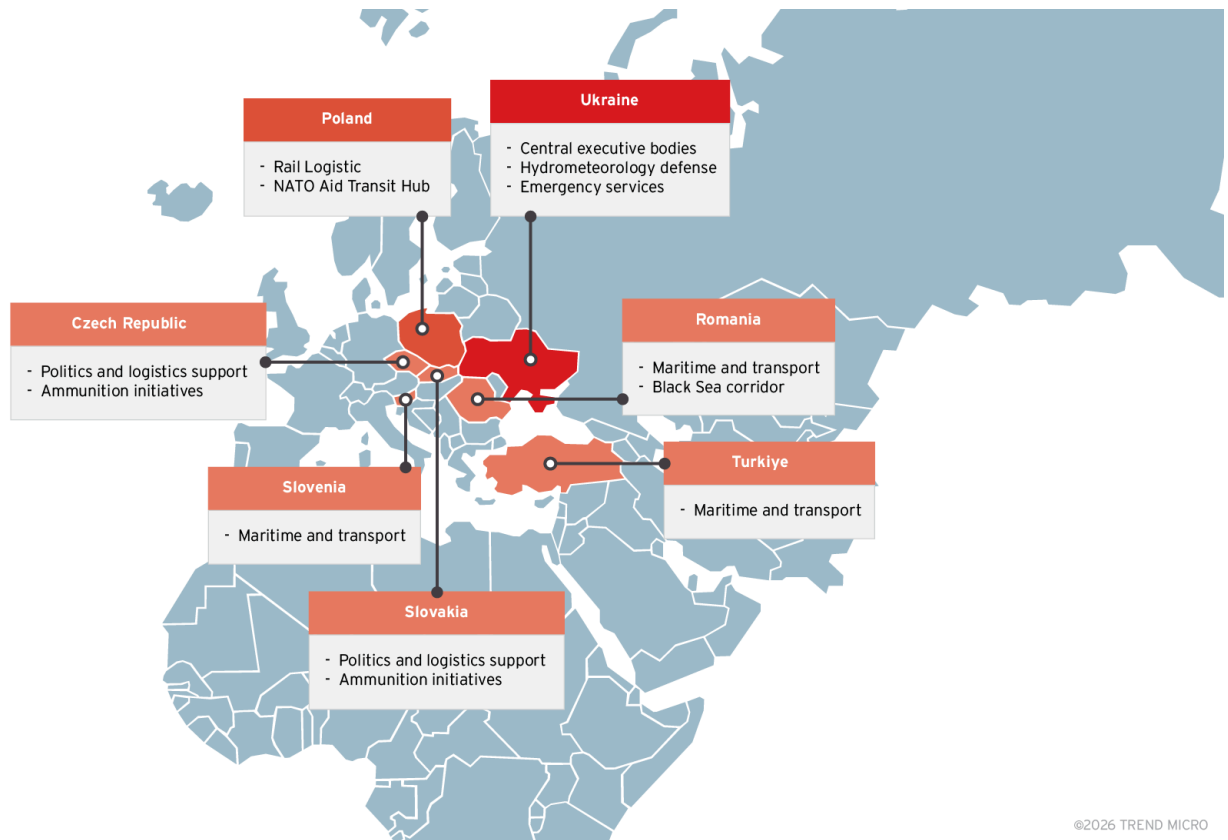


Figure 10. Pawn Storm's strategic targeting of Ukraine and NATO logistics hubs supporting military aid transit

Attribution analysis

Based on technical artifacts, infrastructure overlaps, and victimology, TrendAI™ Research attributes this campaign to Pawn Storm with high confidence. This assessment is significantly bolstered by threat hunting data and internal telemetry that correlates the PRISMEX components with specific previous operations monitored by TrendAI™.

This attribution applies the threat attribution framework of TrendAI™, which uses an adapted version of the Diamond Model to anchor observations across four interdependent nodes (adversary, capability, infrastructure, and victim), an evidence-based scoring system to measure the strength of each piece of information, and Analysis of Competing Hypotheses (ACH) to test conclusions against alternative explanations.

For details on our methodology, see [Threat Attribution Framework: How TrendAI™ Applies Structure Over Speculation](#).

Capability node

Custom tooling requires development effort and often persists across campaigns, making it a strong indicator of actor capability:

- Identical steganography algorithm: The "Bit Plane Round Robin" implementation is functionally identical across the October 2025 and January 2026 campaigns. This unique algorithm has not been observed in any other threat actor's toolkit.
- MiniDoor/NotDoor lineage: According to Zscaler ThreatLabz, the MiniDoor backdoor deployed in this campaign is a variant of NotDoor, demonstrating continuity in malware development. This assessment aligns with our own analysis of the malware lineage.
- Covenant Grunt Deployment: The use of the Covenant C2 framework with identical configuration patterns links these campaigns.
- COM Hijacking persistence: The use of COM DLL hijacking for persistence is a documented Pawn Storm TTP.

Infrastructure node

Infrastructure choices that persist over time carry more weight than disposable indicators:

- Filen.io abuse pattern: The abuse of Filen.io with a specific 24-domain redundancy structure is consistent across campaigns.
- Infrastructure pre-positioning: Domain registration two weeks before vulnerability disclosure indicates advance planning capabilities.
- CVE-2026-21513 infrastructure overlap: The exploit sample uses the same infrastructure as the CVE-2026-21509 campaign, providing corroboration.

Adversary node

Certain behaviors and operational patterns recur across campaigns:

- Working hours: Malware compilation timestamps cluster between 07:00-17:00 UTC, consistent with Moscow time (UTC+3).
- Rapid weaponization: The campaign commenced almost immediately following CVE-2026-21509 patch availability, consistent with Pawn Storm's known operational tempo.
- Multi-language development: The use of Go, .NET, and native code within single campaigns is a characteristic Pawn Storm pattern.
- CVE-2026-21513 zero-day: Exploited at least 11 days before the February 10, 2026 patch release.

Victim node

Repeated victim selection reflects strategic intent:

- Victim profile alignment: Ukrainian government and military, NATO logistics infrastructure, and humanitarian organizations supporting Ukraine align with Pawn Storm's documented targeting history since 2014.
- Regional presence: The use of compromised accounts from law enforcement, parliamentary, and military education institutions in Romania and Slovakia demonstrates the actor's established presence in these regions.

Confidence assessment

Evidence aligns across all four Diamond Model nodes. Alternative hypotheses, including false flag operations and tool sharing scenarios, were tested through ACH and found inconsistent with the totality of evidence. The unique steganography algorithm and MiniDoor/NotDoor malware lineage serve as primary attribution anchors, as these are not tools available on underground markets or shared between groups. This convergence of evidence across capability, infrastructure, adversary behavior, and victimology supports our high-confidence attribution to Pawn Storm.

Strategic assessment

The timing and targeting of these campaigns reflect a shift in Russian military intelligence priorities toward operational and tactical disruption of Ukrainian logistics, rather than purely strategic political intelligence.

In the context of 2026

As the geopolitical conflict between involved territories enters its fifth year, the static nature of front lines has elevated the importance of ancillary support systems:

- Weather warfare: Accurate hydrometeorological data is crucial for drone operability, artillery trajectory planning, and assessing ground trafficability during mud season. Compromising the national hydrometeorological service provides insight into Ukraine's ability to conduct offensive maneuvers in specific windows.
- Supply chain intelligence: Targeting Polish rail infrastructure and Romanian/Slovenian transport entities suggests intent to map, track, and potentially sabotage the flow of Western materiel into Ukraine.
- Humanitarian disruption: Targeting aid organizations may serve to gather intelligence on Western support efforts and disrupt the flow of humanitarian assistance.

Potential for destructive operations

The deployment of the post-exploitation framework Covenant Grunt indicates intent to move laterally within compromised networks. Access to a rail logistics network or a national weather service could be used not just for data theft, but as a beachhead for destructive attacks (which could include but is not limited to wiping servers or falsifying data) timed to coincide with kinetic military operations.

TrendAI™ Research analysis of the October 2025 campaign observed not only information-gathering tasks but also a destructive wiper command that deleted all files under %USERPROFILE%. This dual capability confirms that these campaigns may serve both espionage and sabotage objectives.

Conclusion and risk management guidance

The PRISMEX components represent a capable and stealthy addition to Pawn Storm's arsenal. By combining zero-day exploitation (CVE-2026-21513) with rapid weaponization of newly disclosed vulnerabilities (CVE-2026-21509), valid cloud infrastructure, and unique steganography, the actor has demonstrated a continued ability to evolve. The strategic focus on targeting the supply chains, weather services, and humanitarian corridors supporting Ukraine represents a shift toward operational disruption that may presage more destructive activities.

The technical links between the PRISMEX components and previous campaigns demonstrate the threat actor's continuous development cycle and modular approach to capability building. Organizations in the targeted geographic and industry sectors should consider themselves at elevated risk and implement the countermeasures detailed above immediately.

The use of newly disclosed vulnerabilities and legitimate cloud services makes detection challenging. Defenders must adopt an "assume breach" mentality and focus on behavioral anomalies rather than just static indicators.

Immediate mitigations

- Patching: Prioritize the remediation of both CVE-2026-21509 and CVE-2026-21513 across the entire fleet immediately. Ensure Microsoft Office and Windows are updated to the latest builds.
- Network blocking: Review and restrict access to non-business-essential cloud storage services at the perimeter firewall and web proxy. Organizations should maintain an allowlist of approved cloud storage platforms and block unauthorized file-sharing services that lack verified business justification.
- Attack surface reduction: Disable the *Shell.Explorer.1* COM object via registry keys if patching is not immediately feasible.
- Macro restrictions: Enforce policies blocking macro execution for Office files from the Internet (Mark of the Web).

Detection and hunting

- Registry: Audit *HKCU\Software\Classes\CLSID* for user-registered COM objects pointing to %PROGRAMDATA% or %TEMP%.
- CLR monitoring: Monitor for unusual CLR initialization patterns in non-.NET native processes, particularly *explorer.exe* loading *clr.dll* or *mscorlib.dll* unexpectedly.

- ETW logging: Enable Microsoft-Windows-DotNETRuntime ETW provider to detect assembly loads from byte arrays rather than file paths.

Email security

- Implement strict attachment filtering for RTF documents.
- Enable enhanced logging for Outlook VBA macro execution.
- Monitor for unusual patterns in email deletion (rapid move to Deleted Items followed by permanent deletion).
- Audit Outlook VBA projects for unauthorized modifications.

Proactive security with TrendAI Vision One™

[TrendAI Vision One™](#) is the industry-leading AI cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. TrendAI Vision One™ Threat Intelligence Hub

[TrendAI Vision One™ Threat Intelligence Hub](#) provides the latest insights on emerging threats and threat actors, exclusive strategic reports from TrendAI™ Research, and TrendAI Vision One™ Threat Intelligence Feed in the TrendAI Vision One™ platform.

- Threat Actor: [Pawn Storm](#)
- Related Emerging Threat entities: "[Pawn Storm: The Prism of War with CVE-2026-21509](#)"

TrendAI Vision One™ Intelligence Reports (IOC Sweeping)

Intelligence Reports for Pawn Storm can be accessed [here](#).

Hunting Queries

TrendAI Vision One™ Search App

Hunting queries are available for TrendAI Vision One™ with Threat Intelligence Hub entitlement enabled.

Indicators of Compromise (IoCs)

The IoC list can be found in this [link](#).