APT28’s Campaign Leveraging CVE-2026-21509 and Cloud C2 Infrastructure

Archived: 2026-04-05 14:27:19 UTC

This blog is written in collaboration with Trellix

Updated February 9, 2026: This analysis has been updated to clarify malware naming conventions.

Introduction

Russian state-sponsored threat group **APT28** (aka Fancy Bear or UAC-0001) has launched a sophisticated espionage campaign targeting European military and government entities, specifically targeting maritime and transport organizations across Poland, Slovenia, Turkey, Greece, the UAE, and Ukraine. The attackers weaponized a newly disclosed Microsoft Office 1-day (CVE-2026-21509) within 24 hours of its public revelation, using spear-phishing documents to compromise Ukrainian government agencies and EU institutions [1]. This campaign features a multi-stage infection chain and novel payloads, including a simple initial loader, an Outlook VBA backdoor (NotDoor), and a modified Covenant implant ("CovenantGrunt" [7]). The threat actors abuse legitimate cloud storage (filen.io) as command-and-control (C2) infrastructure, blending malicious traffic with normal user activity.

Infection chain overview

APT28's attack begins with spear-phishing emails containing weaponized documents that exploit CVE-2026-21509, a Microsoft Office security feature bypass vulnerability. This vulnerability was addressed by an urgent, out-of-band security update. When victims open these malicious documents, the exploit triggers automatically without requiring macros or user interaction. The vulnerability allows embedded OLE objects to execute by leveraging the WebDAV protocol to fetch external payloads from attacker-controlled infrastructure.

The initial exploitation downloads a malicious LNK shortcut and first-stage loader DLL, which establishes the foundation for a sophisticated multi-stage infection chain. The loader either extracts an encrypted PNG image file containing shellcode, which it decrypts and executes CovenantGrunt in memory, or drops VbaProject.OTM for NotDoor payload. This shellcode loads a .NET-based payload that performs key exchange operations with cloud storage infrastructure.

The entire chain is designed for resilience and evasion, utilizing encrypted payloads, legitimate cloud services for C2, in-memory execution, and process injection to minimize forensic artifacts. This multi-layered approach demonstrates APT28's evolved tradecraft in maintaining persistent access while evading detection across enterprise environments.

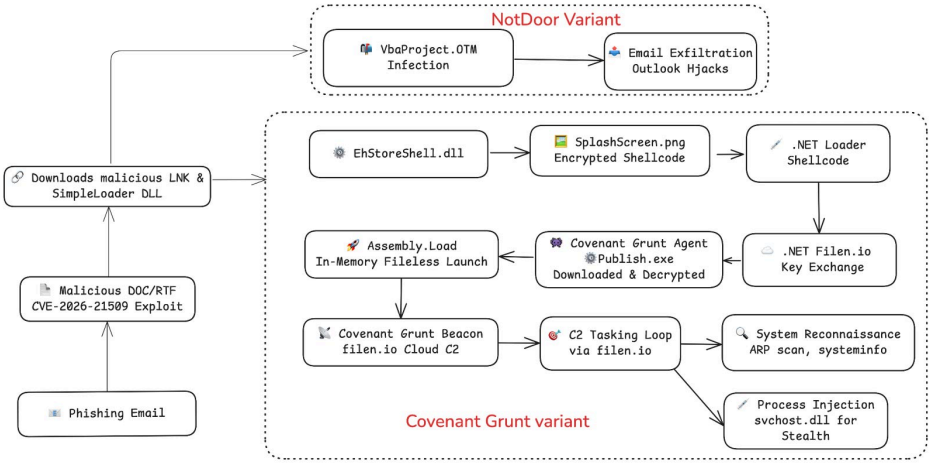

Figure 1: Multi-stage infection chain employed by APT28. The exploit in the document leads to a staged malware execution flow, culminating in an in-memory Covenant backdoor beaconing to cloud storage.

Phishing lures and social engineering

The adversary orchestrated a concentrated 72-hour spear-phishing campaign (January 28-30, 2026), delivering at least 29 distinct emails across nine Eastern European nations, primarily targeting defense ministries (40%), transportation/logistics operators (35%), and diplomatic entities (25%). These emails originated from compromised government accounts of multiple countries, including Romania, Bolivia, and Ukraine.

The lures exploited 4 geopolitically-charged narratives: transnational weapons smuggling alerts (45% of emails) impersonating a Central European border security agency warning of "200 RPG-7 rounds in transit from Syria via Ukraine" with fabricated courier identities; “military training program invitations”(25%) spoofing a regional defense university with professional signature blocks and time-sensitive enrollment deadlines; EU/NATO diplomatic consultations (20%) masquerading as high-level parliamentary requests for policy positions on the Ukraine conflict; and meteorological emergency bulletins abusing compromised national weather service infrastructure to disseminate fabricated flood warnings.

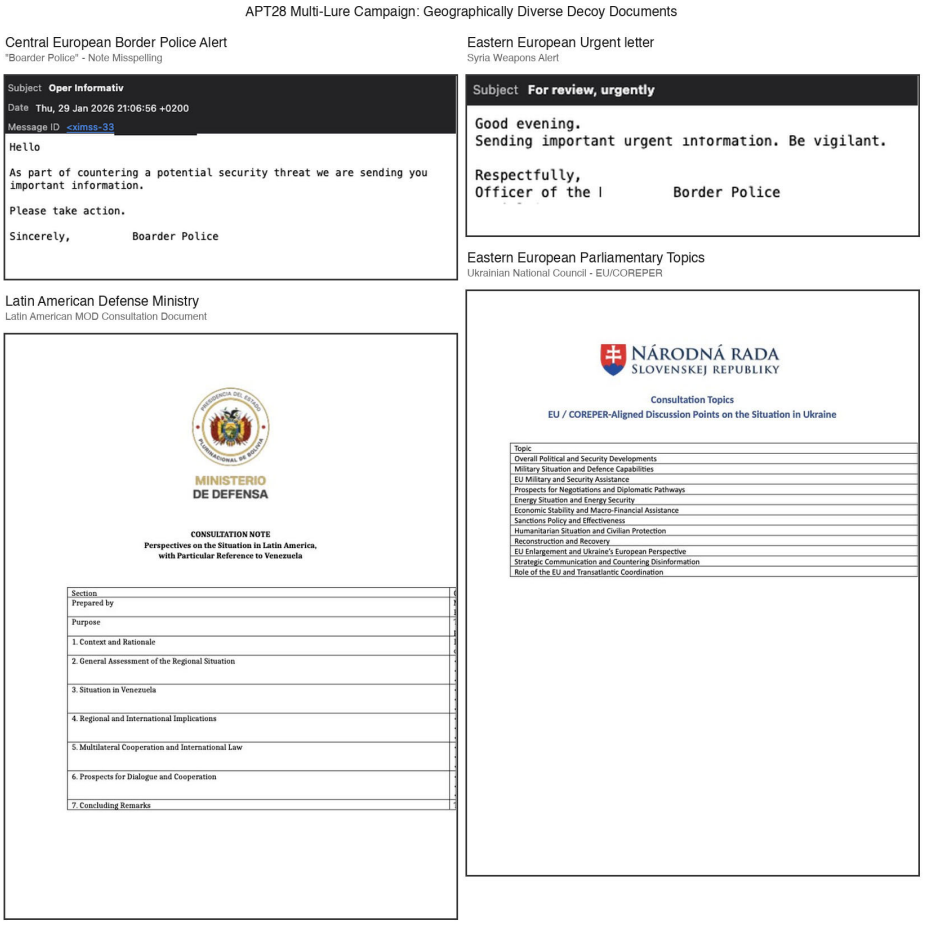

Figure 2: Phishing email and decoys

We identified an orthographic inconsistency - alternating usage of "Boarder Police" versus "Border Police" across temporally-clustered messages, consistent with distributed APT taskings where non-native English speakers independently crafted lure variants. All emails carried weaponized RTF/DOC attachments (e.g., BULLETEN_H.doc, Courses.doc, OperInformativ_163.doc) exploiting CVE-2026-21509, with decoy content meticulously replicating authentic government communication aesthetics, which could potentially be based on real, previously stolen documents, including official letterheads, bilingual formatting (Romanian/English, Ukrainian/English), color-coded hazard maps, and ministerial seals/-visual elements designed to exploit institutional trust mechanisms and circumvent user suspicion during the critical file-open decision point.

Exploitation and initial loader (“SimpleLoader”)

The spear-phishing document uses the **CVE-2026-21509** exploit to achieve code execution as soon as it is opened. According to Microsoft, CVE-2026-21509 allows an attacker to bypass Office’s OLE security restrictions, exposing unsafe COM controls to execution [6]. In practical terms, APT28’s malicious documents embedded a specially crafted OLE object (for instance, a Shell.Explorer ActiveX control) that automatically retrieves the next-stage payload over HTTP/WebDAV.

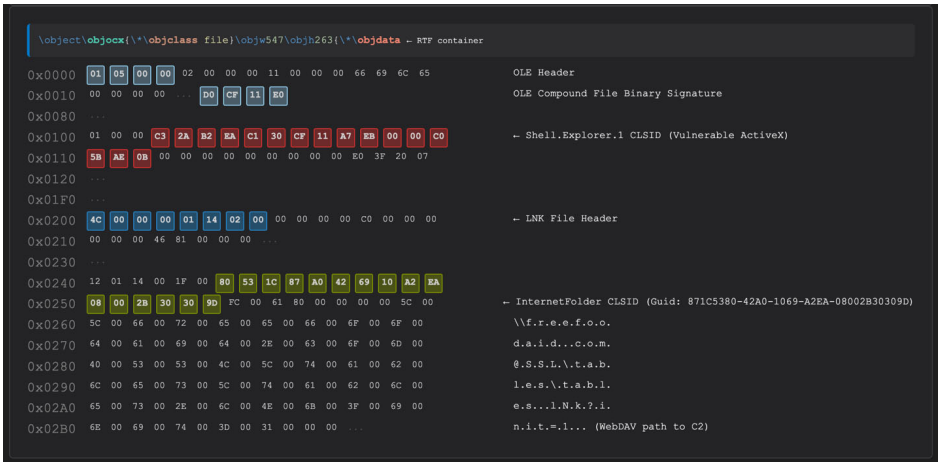

Figure 3: RTF Object Linking and Embedding (OLE) Exploitation via Shell.Explorer.1 in the malicious attachment

The downloaded LNK's execution results in a SimpleLoader DLL loaded.

The infection chain deploys **SimpleLoader** which utilizes three distinct XOR encryption schemes: simple single-byte XOR (0x43) for mutex generation, alternating-byte XOR with null padding for path strings, and a 76-character rotating XOR key for embedded payload decryption. Upon execution in the steganography loader, the loader establishes a single-instance mutex and initiates its dropper routine, which writes three files to disk: the primary payload (EhStoreShell.dll) to *%PROGRAMDATA%\USOPublic\Data\User*, a scheduled task configuration XML to the user's temp directory, and an encrypted-payload PNG file mimicking legitimate OneDrive installation artifacts.

Persistence is achieved through COM object hijacking targeting CLSID {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}. The loader creates a scheduled task named "OneDriveHealth" that triggers 60 seconds post-registration, executing a command sequence that terminates explorer.exe, relaunches it (triggering the hijacked COM object load above), and self-deletes the scheduled task. Once loaded into the new explorer.exe process, EhStoreShell.dll establishes C2 communication with filen.io.

The steganography loader (EhStoreShell.dll) executes anti-analysis routines, including a three-second sleep with timing validation (≥2.9s threshold) to detect sandbox time acceleration and process name verification to ensure execution within explorer.exe. The loader decrypts embedded strings using single-byte XOR (key 0x43) and resolves ten Windows APIs through hash-based lookups. Following successful validation, the loader locates and processes `SplashScreen.png` dropped earlier. The malware implements a complete PNG decoder consisting of ten specialized functions handling IHDR header parsing, PLTE palette extraction, IDAT chunk decompression via zlib inflation, Huffman table construction, and Adam7 interlacing, ultimately extracting a.NET loader shellcode concealed within the image's data chunks.

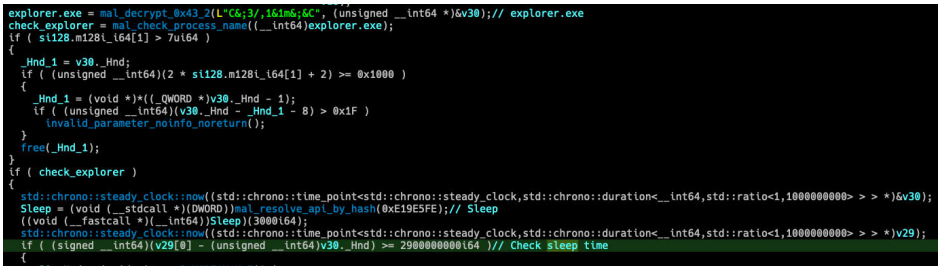

Figure 4: EhStoreShell.dll's anti-analysis routines

The extracted shellcode functions as a fileless .NET assembly bootstrap mechanism that directly invokes the Common Language Runtime without touching disk. Utilizing Process Environment Block (PEB) traversal to resolve APIs dynamically (bypassing the Import Address Table), the shellcode loads `MSCOREE.DLL` and `OLEAUT32.DLL`, then invokes `CLRCreateInstance` to initialize the .NET runtime within the compromised explorer.exe process.

Post-exploitation payloads: CovenantGrunt with cloud-based C2

Following successful shellcode execution, the infection chain progresses to a *staged .NET loader* ("Publish"- modified Covenant backdoor) that implements cryptographic handshake protocol with the adversary's command infrastructure: 2048-bit RSA key pair. The operator's C2-monitoring the base folder UUID on filen.io -detects the new victim registration, generates a cryptographically random 32-byte AES-256 session key, encrypts it with the victim's RSA public key, and uploads the encrypted session key back to the victim's dedicated subfolder. Upon receiving this response, the victim decrypts the session key using its private RSA key, then engages in a challenge-response exchange to prove the handshake. Once the

handshake completes successfully, the loader downloads the encrypted Covenant Grunt assembly, decrypts it using the newly established session key, and executes it via Assembly.Load() with reflection-based method invocation targeting the *[DisplayName("Invite")]* attribute, achieving completely fileless execution.

The Covenant Grunt implant was reengineered to utilize filen.io cloud storage. The .NET assembly implements 4 core components: `FilenApi` (complete REST API client for filen.io's gateway, ingest, and egest endpoints across 24 subdomains), *`FilenMessenger`* (implements the IMessenger interface for polling and uploading encrypted task files), *`FilenEncryptor`* (provides AES-256-GCM encryption with per-file nonces and HMAC-SHA256 integrity verification), and *`GruntExecutor`* (task execution engine supporting .NET assembly loading, PowerShell execution, and output streaming through anonymous pipes). The implant encrypts results with AES-256-CBC plus HMAC-SHA256, and uploads them back to the folder where the threat actor retrieves and processes them.

Analysis of the compromised filen.io infrastructure revealed the operational scale of this campaign: confirmed victims distributed across at least two accounts *(fiscalizacionycontrol@cordoba.gov.ar* and *jannet.stillman@outlook.com)*. Post-exploitation capabilities include system reconnaissance *(arp.exe, systeminfo.exe, tracert.exe)*, process injection into svchost.exe for persistence, and preparation for lateral movement,-all executed through dynamically loaded .NET assemblies that leave no disk-based forensic artifacts beyond memory resident code injection.

“NotDoor” Outlook backdoor variant

Infrastructure: APT28’s campaign stands out for its heavy abuse of legitimate cloud services. In this 2026 wave, **filen.io** – a cloud storage provider – serves as the core C2 channel for the CovenantGrunt implants. All beaconing and tasking occurs via HTTPS requests to filen.io API endpoints, appearing as normal cloud storage traffic. Earlier related operations used Koofr and Icedrive for C2, indicating APT28’s flexibility in swapping out cloud platforms [2].

The VBA macro itself implements email surveillance through dual automatic triggers: `Application_MAPILogonComplete` executes upon Outlook login, while `Application_NewMailEx` activates instantly upon new message arrival for real-time forwarding. The exfiltration logic systematically enumerates 4 folder types (Inbox, Drafts, Junk Mail, RSS Feeds), processing up to 10 messages per folder per execution. For each unprocessed email, the macro invokes the native Outlook object model to save the complete message (headers, body, attachments, metadata) as a `.msg` file to `%TEMP%\temp_email.msg`, creates a new forwarding message with the original attached, and transmits it to two adversary-controlled addresses via standard SMTP. Furthermore, it marks processed emails with a custom "AlreadyForwarded" property to prevent duplicate transmissions, sets `DeleteAfterSubmit = True` to automatically purge forwarded messages from the Sent Items folder. This technique proves particularly effective against organizations with diplomatic or government email systems, where high-privilege accounts receive sensitive policy documents, classified cables, and strategic communications-precisely the intelligence targets consistent with APT28's collection priorities.

Infrastructure and TTPs

Infrastructure: APT28’s campaign stands out for its heavy abuse of legitimate cloud services. In this 2026 wave, **filen.io** – a cloud storage provider – serves as the core C2 channel for the Covenant/BeardShell implants. All beaconing and tasking occurs via HTTPS requests to filen.io API endpoints, appearing as normal cloud storage traffic. Earlier related operations used Koofr and Icedrive for C2, indicating APT28’s flexibility in swapping out cloud platforms [2].

In terms of delivery, the initial stage relied on compromised or attacker-registered web servers hosting the malicious documents and LNKs. For example, domains like `wellnessmedcare[.]org, wellnesscaremed[.]com, freefoodaid[.]com,` and `longsauce[.]com` were used to host and deliver the Office exploits (possibly as part of the WebDAV fetch and as decoy content) – see IoC table below. The threat actors moved quickly, even registering new domains the same day they were used in attacks, reflecting a highly agile operation.

Attribution to APT28

This campaign is **attributed to APT28 with high confidence** based on technical indicators and victimology. CERT-UA officially attributed the January 2026 attacks to threat actor UAC-0001 [1], which corresponds to APT28 (Fancy Bear), a unit of Russia’s GRU military intelligence. In the past, APT28 swiftly weaponized Office vulnerabilities and was among the first to use them in the wild, demonstrating a capability for 0-day or n-day exploitation that few groups possess at this level.

APT28 has a long history of cyber espionage and influence operations. The tradecraft in this campaign – *multi-stage malware, extensive obfuscation, abuse of cloud services, and targeting of email systems for persistence* – reflects a well-resourced, advanced adversary consistent with APT28’s profile. The toolset and techniques also align with APT28’s fingerprint. The use of COM hijacking for persistence and macro-enabled Outlook backdoors (NotDoor) are TTPs recently tied to APT28 operations targeting European organizations. The BeardShell malware has been explicitly attributed to APT28 by Ukrainian authorities and security researchers. These implants, along with the Covenant framework, were all found in incidents responded by CERT-UA and partners, linking them to the same adversary. Furthermore, the focus on Ukrainian government and military bodies, as well as NATO-aligned targets, strongly correlates with APT28’s strategic interests over the past decade (especially post-2022 invasion of Ukraine).

Code analysis indicates that this steganography loader exhibits 47 unknown, 10 malicious, and 542 benign components, according to analysis from Threatray. Furthermore, 10 malicious functions align with the reference Beadshell malware loader 88e28107fbf171fdbcf4abbc0c731295549923e82ce19d5b6f6fefa3c9f497c9 previously reported by Sekoia [3].

Address	Function Name	Matching Address
0x180008600	mal_png_master_decoder	0x18000b310
0x180007f60	mal_png_itxt_parser	0x18000ad20
0x1800052b0	mal_png_adam7_interlace	0x180008230
0x1800047e0	mal_png_plte_parser	0x180007750
0x180004510	mal_png_ihdr_parser	0x180007470
0x180004230	mal_png_chunk_parser	0x180007190
0x180004000	mal_png_text_storage	0x180006f90
0x180003240	mal_crc32_calculate	0x180006120
0x180002440	mal_zlib_inflate_decompress	0x1800054c0
0x180001f30	mal_huffman_table_builder	0x180004fc0

While attribution in cyberspace can be challenging, in this case the convergence of indicators (including code overlaps, infrastructure reuse, and timing) makes a compelling case that the **Russian GRU-linked APT28 is behind the campaign**.

Conclusion

APT28's latest campaign underscores the group's technical prowess and adaptability. By integrating a fresh Office exploit, multi-layered loaders, cloud-based C2 channels, and even an Outlook backdoor, APT28 continues to expand its arsenal for infiltrating high-value targets. The use of CVE-2026-21509 demonstrates how quickly state-aligned actors can weaponize new vulnerabilities, shrinking the window for defenders to patch critical systems. The campaign's modular infection chain – from initial phish to in-memory backdoor to secondary implants was carefully designed to leverage trusted channels (HTTPS to cloud services, legitimate email flows) and fileless techniques to hide in plain sight.

Attribution to APT28 is reinforced by the continuity in their tactics: early observations by CERT-UA and others tie these activities back to the same unit behind prior operations like the **Signal Messenger lures (BeardShell/Covenant)** and the **NotDoor Outlook backdoor** [4][5]. This consistency provides valuable intelligence on APT28's evolving toolkit. Organizations are urged to apply the latest Office patches (including the emergency fix for CVE-2026-21509) and implement Microsoft's recommended registry hardening that blocks this OLE exploit path [6].

Defending against such an advanced threat requires a defense-in-depth approach. **User awareness** is crucial, as highly convincing lures are in play. The MITRE ATT&CK mapping above can guide threat hunting for specific techniques like COM hijacks and macro abuse. Trellix Email Security and **IVX** sandbox proactively stopped this zero-day campaign by employing a generic signature that identified the malicious attachment's behavior.

Trellix detection

Product	Signature
Trellix Network Security Trellix VX Trellix Cloud MVX Trellix File Protect Trellix Malware Analysis Trellix SmartVision Trellix Email Security Trellix Detection As A Service Trellix NX	 Malware.Binary.doc Script.Trojan-Downloader.Agent.BNX

MITRE ATT&CK techniques mapped

The following table maps key techniques observed in this APT28 campaign to the corresponding MITRE ATT&CK tactics and technique IDs:

Tactical Goal	ATT&CK Technique (Technique ID)	Implementation Details
Initial Access	T1566.001 Phishing: Spearphishing Attachment	Weaponized RTF documents with CVE-2026-21509 exploit
Initial Access	T1199 Trusted Relationship	Compromised Slovak and Bolivian government accounts
Initial Access	T1189 Drive-by Compromise	Automatic remote content download via CVE-2026-21509
Execution	T1203 Exploitation for Client Execution	CVE-2026-21509 exploitation
Execution	T1204.002 User Execution: Malicious File	User opens RTF document
Execution	T1218.011 System Binary Proxy: Rundll32	DLL execution via rundll32.exe
Execution	T1059.003 Command and Scripting Interpreter: Windows Command Shell	cmd.exe for orchestration
Persistence	T1546.015 Event Triggered Execution: Component Object Model Hijacking	CLSID {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D} hijacked
Persistence	T1053.005 Scheduled Task/Job	"OneDriveHealth" scheduled task (temporary)
Persistence	T1137.001 Office Application Startup	Outlook VBA macro (NotDoor persistence)
Defense Evasion	T1027 Obfuscated Files or Information	Triple XOR encryption (Simple, Alternating-byte, 34-char rotating)
Collection	T1114 Email Collection	NotDoor: Automated diplomatic email collection from Outlook
Exfiltration	T1048 Exfiltration Over Alternative Protocol	NotDoor: Email forwarding as exfiltration channel
Defense Evasion	T1055 Process Injection	Injects into explorer.exe via COM
Defense Evasion	T1070.004 Indicator Removal: File Deletion	Deletes scheduled task after persistence established
Defense Evasion	T1140 Deobfuscate/Decode Files or Information	Runtime XOR decryption
Defense Evasion	T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion	3-second sleep with timing validation
Credential Access	T1528 Steal Application Access Token	Government account compromise (Slovak, Bolivian)
Discovery	T1082 System Information Discovery	Queries system information
Discovery	T1057 Process Discovery	Checks for explorer.exe
Command and Control	T1102 Web Service	filen[.]io cloud storage for C2
Command and Control	T1071.001 Application Layer Protocol: Web Protocols	HTTPS/TLS for C2
Command and Control	T1573.001 Encrypted Channel: Symmetric Cryptography	AES-256-GCM/CBC encryption
Command and Control	T1090.003 Proxy: Multi-hop Proxy	Multiple filen[.]io gateway domains
Exfiltration	T1567.002 Exfiltration Over Web Service: Cloud Storage	Diplomatic data exfiltration via filen[.]io
Exfiltration	T1020 Automated Exfiltration	Automated via Covenant Grunt

Indicators of Compromise (IoCs)

File Hashes – Malicious Documents & Malware

File Name	MD5 Hash	SHA-256 Hash
1301.doc	b6a86f44d0a3fa5a5ac979d691189f2d	969d2776df0674a1cca0
5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02.doc	4727582023cd8071a6f388ea3ba2feaa	5a17cfaea0cc3a82242fd
Consultation_Note_Ministry_of_Defense_Bolivia(Final).doc	1550ae7df233bb9a9c9e78bf8b236072	e792adf4dff54faca5b9f3
Consultation_Topics_Ukraine(Final).doc	045d1e0686f8b4b49b2d9cf48ac821f8	d213b5079462e737eb94
Courses.doc	2f7b4dca1c79e525aef8da537294a6c4	1ed863a32372160b3a25
Oper Informativ Possible International Weapons.doc	0df3fde016f3c0974d4aa01b06724a33	968756e62052f9af8093
OperInfConsdin Siria în România 145.doc	4727582023cd8071a6f388ea3ba2feaa	5a17cfaea0cc3a82242fd
OperInformation.doc	6408276cdfd12a1d5d3ed7256bfba639	baad1153e58c86aa1dc9
OperInformativ_163.doc	41c51784f6d601ffd0e09b7d59ff6025	b7342b03d7642c894eba
Запитання для інтерв'ю (1).doc	58f517bdc9ba8de1b69829b0dcf86113	be859b4f4576ec09b69a
BULLETEN_H.doc	7c396677848776f9824ebe408bbba943	c91183175ce77360006f
1291.doc	d47261e52335b516a777da368208ee91	fd3f13db41cd5b442fa26
International Weapons Smuggling from Syria to Europe 51.doc	c306e0a3ec528368f0b0332104148266	8b0ab7f7f48bf847c3af5
BULLETEN_H.doc	7c396677848776f9824ebe408bbba943	c91183175ce77360006f
SimpleLoader	859c4b85ed85e6cc4eadb1a037a61e16	0bb0d54033767f081cae
EhStoreShell.dll	e4a5c4b205e1b80dc20d9a2fb4126d06	a876f648991711e44a8d
VbaProject.OTM	337cecf067ecf0609b943b54fb246ed2	7ccf7e8050c66eed69f35

Network Indicators – Domains and IPs

Domain	IP Address
wellnesscaremed[.]com	23.227.202[.]14
wellnessmedcare[.]org	193.187.148[.]169
freefoodaid[.]com	159.253.120[.]2
longsauce[.]com	72.62.185[.]31

Email-based C2 (NotDoor Exfiltration)

Email Address	Provider
chmilewskii@outlook[.]com	Microsoft Outlook
chmilewskii@proton[.]me	ProtonMail

Filen[.]io Cloud Storage Accounts

Email	API Key
jannet.stillman@outlook[.]com	s_zTx8oEG3MySPkv0EJH8N-TKNU8fzpm9d2BRYzXq_lbEFTruBAs-Of0sdrYd3vU
fiscalizacionycontrol@cordoba.gov[.]ar	nJlCvhtYI4CS4XrB0T5vsrUMF6T83GuZxtH8gFeQQDSf0be4QMDBQ4vblYVWTz7o
nagipeterson@emailasso.net	OgaBSQfSJaNtNlb7_SY9UOCzh-NgJFGgep2yyHyxCtQUUkckr3N5CFBy3ehTgb3K

Malicious URLs (Embedded in RTF Documents)

URL
http://wellnessmedcare[.]org/cz/Downloads/blank.doc
https://wellnessmedcare[.]org/cz/Downloads/document.LnK?init=1
http://wellnesscaremed[.]com/buch/Downloads/blank.doc

https://wellnesscaremed[.]com/buch/Downloads/document.doc.LnK?init=1
https://freefoodaid[.]com/documents/1_1.LnK?init=1
http://freefoodaid[.]com/documents/2_1.lNk?init=1
https://freefoodaid[.]com/tables//template_tables.doc
https://freefoodaid[.]com/tables/tables.lNk?init=1
http://wellnesscaremed[.]com/ankara/Favorites/blank.doc
https://wellnesscaremed[.]com/ankara/Favorites/document.doc.LnK?init=1
https://longsauce[.]com/DAv/DEFault/data.LnK?init=1
https://longsauce[.]com/DAv/DEFault/df.doc
http://wellnesscaremed[.]com/venezia/Favorites/blank.doc
https://wellnesscaremed[.]com/venezia/Favorites/document.doc.LnK?init=1
http://wellnessmedcare[.]org/pol/Downloads/blank.doc
https://wellnessmedcare[.]org/pol/Downloads/document.LnK?init=1
http://wellnesscaremed[.]com/ljub/Downloads/blank.doc
https://wellnesscaremed[.]com/ljub/Downloads/document.doc.LnK?init=1

Host-based Indicators

File Paths (BEARDSHELL Chain)
C:\ProgramData\USOPublic\Data\User\EhStoreShell.dll
C:\ProgramData\Microsoft OneDrive\setup\Cache\SplashScreen.png
C:\Users*\AppData\Local\Temp\Diagnostics\office.xml

File Paths (NotDoor Chain)
%APPDATA%\Microsoft\Outlook\VbaProject.OTM
%TEMP%\temp_email.msg

Registry Keys (BEARDSHELL - COM Hijacking Persistence)
HKCU\Software\Classes\CLSID\{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32

Registry Keys (NotDoor - Outlook Security Bypass)
HKCU\Software\Microsoft\Office\16.0\Outlook\Security\Level = 1
HKCU\Software\Microsoft\Office\16.0\Outlook\LoadMacroProviderOnBoot = 1

Mutex Names
adjgfenkbe (SimpleLoader)
dvyubgbqfusdv32 (BEARDSHELL)

Scheduled Task
OneDriveHealth (temporary, deleted after COM persistence established)

Process Indicators
rundll32.exe tables(1).dll
cmd.exe /c (taskkill /f /IM explorer.exe >nul 2>&1) & (start explorer >nul 2>&1)
schtasks.exe /Create /tn "OneDriveHealth"

References:

[1] "Бюлетень небезпеки": UAC-0001 (APT28) здійснює кібератаки у відношенні України та країн ЄС з використанням експлойту CVE-2026-21509 (CERT-UA#19542).
https://cert.gov.ua/article/6287250

[2] Кібератаки UAC-0001 (APT28) у відношенні державних органів із застосуванням BEARDSHELL та COVENANT.
https://cert.gov.ua/article/6284080

[3] APT28 Operation Phantom Net Voxel - Sekoia.io Blog.
https://blog.sekoia.io/apt28-operation-phantom-net-voxel/

[4] NotDoor Insights: A Closer Look at Outlook Macros and More - Splunk.
https://www.splunk.com/en_us/blog/security/notdoor-insights-a-closer-look-at-outlook-macros-and-more.html

[5] Analyzing NotDoor: Inside APT28's Expanding Arsenal.
https://lab52.io/blog/analyzing-notdoor-inside-apt28s-expanding-arsenal/

[6] Microsoft Office Security Feature Bypass Vulnerability CVE-2026-21509.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

[7] APT28 Leverages CVE-2026-21509 in Operation Neusploit
https://www.zscaler.com/fr/blogs/security-research/apt28-leverages-cve-2026-21509-operation-neusploit

---