Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

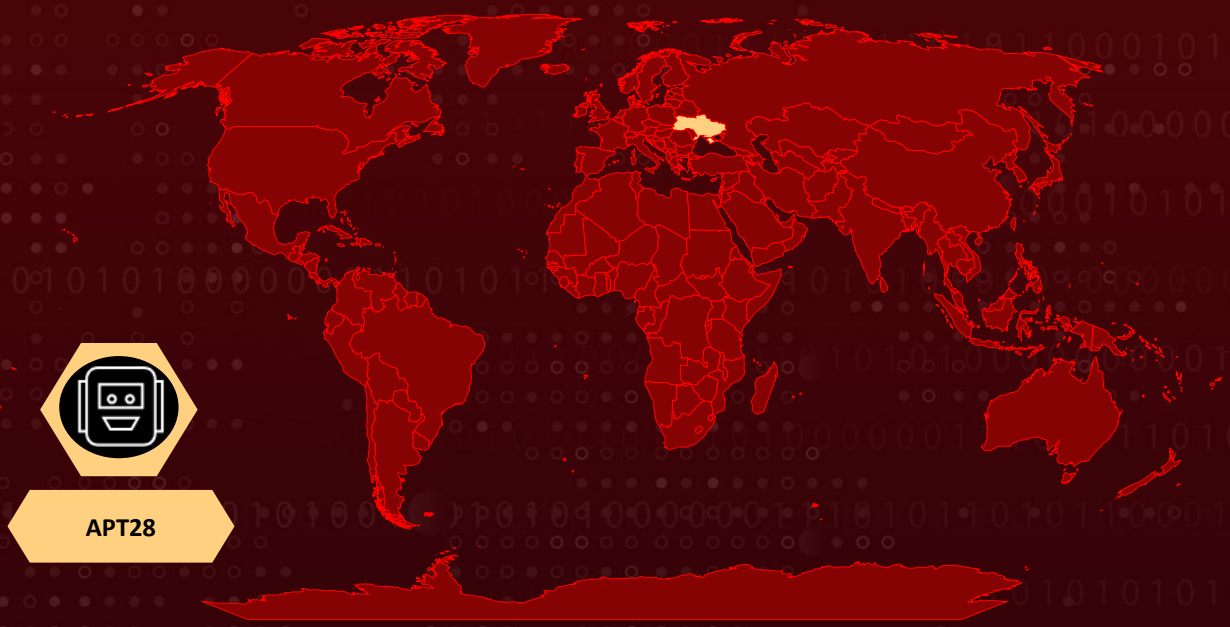
APT28 Deploys Modified Covenant to Spy on Ukrainian Government

Date of Publication	Admiralty Code	TA Number
March 12, 2026	A1	TA2026068

Summary

First Seen: April 2024
Targeted Region: Ukraine
Targeted Platform: Windows
Targeted Industries: Government, Military
Threat Actor: APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)
Malware: SlimAgent, BeardShell, Covenant
Attack: The Russian-linked threat group APT28 has launched a stealthy espionage campaign targeting Ukrainian government entities by exploiting the Microsoft Office vulnerability CVE-2026-21509 through weaponized documents delivered via spear-phishing and messaging platforms like Signal. Once opened, the malicious files deploy a modified version of the Covenant framework to establish covert access, alongside custom implants such as BeardShell and SlimAgent to steal keystrokes, screenshots, and sensitive data. By routing command-and-control traffic through legitimate cloud storage services like Filen and Icedrive, the attackers conceal their activity within normal cloud traffic, enabling long-term surveillance of compromised systems and allowing them to quietly monitor victims for months while evading traditional detection mechanisms.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-21509	Microsoft Office Security Feature Bypass	Microsoft Office	✓	✓	✓

Attack Details

#1

The Russian state-sponsored threat group APT28 (aka Sednit) has been observed conducting long-term espionage campaigns using a customized version of the open-source Covenant post-exploitation framework. Recent investigations revealed that these operations targeted Ukrainian government entities, particularly central executive bodies, by exploiting the vulnerability CVE-2026-21509 in Microsoft Office. The campaign relied on spear-phishing emails distributing specially crafted Office documents designed to exploit the flaw.

#2

To initiate the attack, operators sent malicious Office files to carefully selected targets and relied heavily on social engineering to persuade recipients to open them. In one instance documented by CERT-UA, the attackers even used the messaging platform Signal to deliver a document named Акт.doc. The file contained embedded macros that triggered the infection chain once opened, allowing the attackers to establish an initial foothold on the victim's system.

#3

After execution, the document deployed a memory-resident Covenant backdoor that downloaded additional components, including a DLL named PlaySndSrv.dll and a shellcode-embedded WAV file. These files were used to install BeardShell, a custom C++ implant. Persistence for both the loader and the main payload was achieved through COM hijacking in the Windows registry. Alongside these tools, the attackers deployed SlimAgent, a surveillance implant derived from the group's older XAgent malware framework. SlimAgent enabled the operators to capture keystrokes, screenshots, and clipboard data, generating espionage logs in HTML format with color-coded entries to help operators quickly analyze stolen information.

#4 Researchers also discovered that the threat actors heavily modified the Covenant framework to better support long-term espionage operations. Instead of generating random implant names, the developers implemented a deterministic naming method derived from system characteristics, allowing them to consistently track infected machines even after reboots. The execution process was also redesigned to evade behavioral detection mechanisms. Additionally, the group integrated cloud-based communication capabilities using the C2Bridge project, enabling the malware to communicate with legitimate cloud storage platforms such as pCloud, Koofr, Filen, and Icedrive.

#5 The attackers employed a dual-implant architecture to maintain operational resilience. Covenant acted as the primary access channel, while BeardShell served as a backup in case the main communication infrastructure was disrupted. This setup allowed the operators to maintain long-term visibility into compromised networks. Analysis of Sednit-controlled cloud storage accounts revealed that some systems had been monitored for more than six months. By routing command-and-control traffic through legitimate cloud services, the attackers ensured that malicious communications blended with normal cloud activity, making detection significantly more difficult. Meanwhile, data collected by SlimAgent was encrypted using AES and RSA before being stored locally and later exfiltrated through separate command-and-control channels.

Recommendations

Patch Microsoft Office Against CVE-2026-21509: Apply the emergency security update released by Microsoft across all affected versions, including Office 2016, Office 2019, Office LTSC 2021, Office LTSC 2024, and Microsoft 365 Apps for Enterprise. Customers running Office 2021 and later should restart Office applications to activate service-side protections.

Block Cloud Storage C2 Domains: Monitor and restrict network communications to cloud storage domains abused by APT28 for C2, specifically app.koofr.net, api.icedrive.net, and filen.io endpoints. Implement allowlisting policies that only permit authorized cloud storage services within the organization's network perimeter.

Filter Malicious Office Attachments at the Email Gateway: Quarantine or block Office documents containing embedded OLE objects from external and untrusted sources. Pay particular attention to .doc files with macros, as the threat actor distributed malicious documents via both email and encrypted messaging platforms like Signal.

Enable Protected View and Macro Controls: Ensure Protected View is enabled by default for all documents originating from external sources. Enforce group policies that disable macros in documents received from the internet and require explicit user or administrator approval for macro execution.

Monitor for SlimAgent Keylogger Artifacts: Search for HTML-formatted keylogger output files on endpoints, particularly those with color-coded entries in blue, red, and green. Also look for the known SlimAgent file indicators such as eapphost.dll and tcpiphlpsvc.dll loaded as DLLs via suspicious processes.

Implement Network Segmentation for Sensitive Systems: Isolate military and government-sensitive workstations from general-purpose networks. Given APT28's demonstrated capability for six-month-plus persistent access, segmentation limits the blast radius of any single compromise and restricts lateral movement.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.006: Web Services
	T1587: Develop Capabilities	T1587.001: Malware
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1129: Shared Modules	
Persistence	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
Defense Evasion	T1211: Exploitation for Defense Evasion	
	T1027: Obfuscated Files or Information	

Tactic	Technique	Sub-technique
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1480: Execution Guardrails	
	T1564: Hide Artifacts	
Collection	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1005: Data from Local System	
Discovery	T1082: System Information Discovery	
Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
	T1001: Data Obfuscation	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	5603E99151F8803C13D48D83B8A64D071542F01B, 6D39F49AA11CE0574D581F10DB0F9BAE423CE3D5
Filename	eapphost.dll, tcpiphlpsvc.dll

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

References

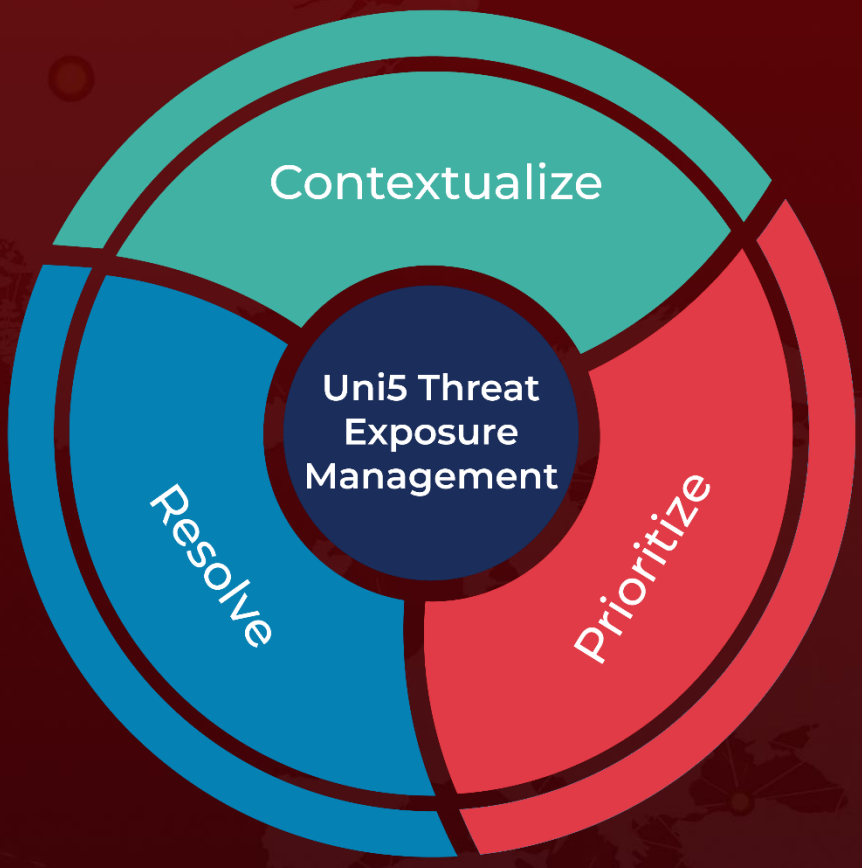
https://www.welivesecurity.com/en/eset-research/sednit-reloaded-back-trenches/

https://hivepro.com/threat-advisory/cve-2026-21509-microsoft-office-zero-day-under-active-exploitation/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 12, 2026 • 08:20 AM

More at www.hivepro.com