Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

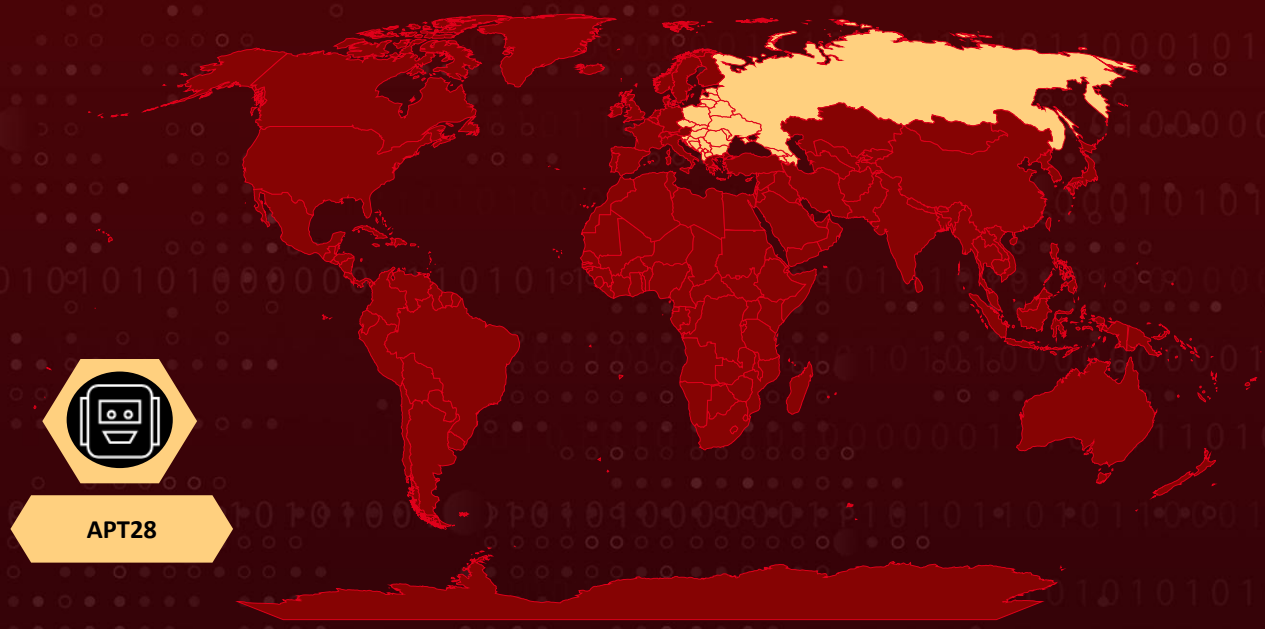
Operation Neusploit: APT28 Weaponizes CVE-2026-21509

Date of Publication	Admiralty Code	TA Number
February 04, 2026	A1	TA2026035

Summary

First Seen: January 2026
Targeted Regions: Central and Eastern Europe
Targeted Platform: Windows
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: MiniDoor, PixyNetLoader
Campaign: Operation Neusploit
Attack: APT28's Operation Neusploit marks a renewed cyber-espionage push across Central and Eastern Europe, where carefully crafted phishing documents exploit a Microsoft Office vulnerability to quietly infiltrate targeted systems. Once inside, the attackers deploy stealthy loaders, hidden shellcode, and memory-resident implants that evade detection while maintaining persistent access. By abusing legitimate cloud services for command-and-control and silently siphoning emails through Outlook manipulation, the campaign blends espionage tradecraft with technical sophistication, enabling long-term surveillance of victims while leaving minimal traces behind.

Attack Regions



CVE

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

Attack Details

#1

In January 2026, the Russia-linked APT28 group launched a new campaign dubbed Operation Neusploit, targeting users across Central and Eastern Europe, with a particular focus on Ukraine, Slovakia, and Romania. The attackers distributed malicious Microsoft RTF documents that exploited CVE-2026-21509, a Microsoft Office flaw allowing local security protections to be bypassed through the abuse of untrusted input. To increase success rates, the attackers crafted phishing lures in English as well as local languages, while also using server-side filtering to ensure that the malicious payload was delivered only to victims connecting from targeted countries and using expected browser identifiers.

#2

Once a victim opened the weaponized document, the exploit triggered the download of a malicious DLL dropper from attacker-controlled infrastructure, including domains such as freefoodaid[.]com. Two dropper variants were observed. One delivered MiniDoor, a lightweight DLL that plants a malicious Outlook VBA project on the system. MiniDoor weakens Outlook's security settings through registry modifications so that macros run automatically, allowing the malicious project to execute each time Outlook is launched. The second variant deployed PixyNetLoader, which installs several components and achieves persistence through COM object hijacking.

#3

The PixyNetLoader infection chain incorporates multiple evasion measures to avoid security analysis. Its loader activates only when executed under explorer.exe and performs timing checks to detect sandbox environments. If the environment appears legitimate, it extracts hidden shellcode from a PNG image using steganography, where data is concealed within image pixels. The recovered shellcode then leverages CLR hosting techniques to load a .NET payload directly into memory, allowing the malware to operate without leaving obvious artifacts on disk.

#4 The final stage delivers a Covenant Grunt implant, an open-source .NET command-and-control agent. To conceal communications, the malware routes traffic through the legitimate Filen cloud service, blending malicious activity with normal network traffic. Meanwhile, MiniDoor acts as an email stealer, quietly monitoring Outlook activity and forwarding emails from folders such as Inbox, Junk, Drafts, and RSS feeds to attacker-controlled addresses. To remain unnoticed, it prevents forwarded messages from appearing in the Sent folder and tags processed emails to avoid repeated exfiltration, enabling long-term surveillance of victim communications.

#5 Separately, Ukraine's Computer Emergency Response Team (CERT-UA) reported related activity in which APT28 exploited the same CVE-2026-21509 flaw to target more than 60 email accounts associated with central executive authorities in Ukraine. Analysis revealed that one malicious Word document used in the campaign was created on January 27, 2026. When opened, the file initiates a WebDAV connection to an external server, triggering the download of a shortcut file containing embedded code that subsequently retrieves and executes an additional payload, allowing attackers to discreetly stage malware delivery before full system compromise.

Recommendations

- **Apply Microsoft Security Update for CVE-2026-21509:** Install the latest update released by Microsoft to patch CVE-2026-21509 across all systems running Microsoft Office.
- **Block Known Malicious Indicators:** Block the identified malicious domains freefoodaid[.]com and wellnesscaremed[.]com at the firewall, proxy, and DNS levels to prevent communication with threat actor infrastructure.
- **Enable Outlook Macro Security Controls:** Ensure Microsoft Outlook macro security is set to disable all macros without notification or require digitally signed macros only, preventing unauthorized VBA project execution.
- **Monitor Registry Key Modifications:** Implement detection rules to alert on modifications to Outlook security-related registry keys.

Restrict RTF File Execution: Consider implementing policies to block or quarantine RTF files received via email attachments, particularly those from external senders or unknown sources.

Hunt for Steganography-Based Payloads: Conduct threat hunting for unusual PNG files in non-standard locations such as that may contain steganographically encoded payloads.

Enable Enhanced Email Security: Deploy email security solutions capable of analyzing RTF documents for embedded exploits and malicious content before delivery to end users.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1203: Exploitation for Client Execution	
	T1106: Native API	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	
Persistence	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
	T1137: Office Application Startup	T1137.006: Add-ins
	T1574: Hijack Execution Flow	T1574.001: DLL

Tactic	Technique	Sub-technique
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1480: Execution Guardrails	T1480.002: Mutual Exclusion
	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
		T1027.003: Steganography
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
Collection	T1114: Email Collection	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.002: Bidirectional Communication
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	95e59536455a089ced64f5af2539a449, 2f7b4dca1c79e525aef8da537294a6c4, 4727582023cd8071a6f388ea3ba2feaa, d47261e52335b516a777da368208ee91, 7c396677848776f9824ebe408bbba943, f3b869a8d5ad243e35963ba6d7f89855, f05d0b13c633ad889334781cf4091d3e, 859c4b85ed85e6cc4eadb1a037a61e16, e4a5c4b205e1b80dc20d9a2fb4126d06, 154ff6774294e0e6a46581c8452a77de, ee0b44346db028a621d1dec99f429823, ea6615942f2c23dba7810a6f7d69e2da, d8e880975ab01c745386663409a9d3aa, 744bbe8d7c3d0421fa0deb582481f5ba, 4423b8f3456e54eb48dfbde0b4c7984b, 418dc7365e78f79ef7dfcfbfe1bc8b0e, 331e055e6a519d443233bd740dbfe8ee, 6f528ad405bffa4a8c2f61b1fa2172fd, 95e59536455a089ced64f5af2539a449, b6a86f44d0a3fa5a5ac979d691189f2d
SHA1	4592e6173a643699dc526778aa0a30330d16fe08, c4799d17a4343bd353e0edb0a4de248b99295d4d, d788d85335e20bb1f173d4d0494629d36083dddc, c8c84bf33c05fb3a69bc5e2d6377b73649b93dce, d577c4a264fee27084ddf717441eb89f714972a5, c1b272067491258ea4a2b1d2789d82d157aaf90a, 7bbb530eb77c6416f02813cd2764e49bd084465c, da1c3e92f69e6ca0e4f4823525905cb6969a44ad, e52a9f004f4359ea0f8f9c6eb91731ed78e5c4d3, 22da6a104149cad87d5ec5da4c3153bebf68c411, cea7e9323d79054f92634f4032c26d30c1cedd7e, 23b6f9c00b9d5475212173ec3cbbcff34c4400a7
SHA256	b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546, 1ed863a32372160b3a25549aad25d48d5352d9b4f58d4339408c4eea69807f50, 5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02, fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b,

TYPE	VALUE
SHA256	c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f, a944a09783023a2c6c62d3601cbd5392a03d808a6a51728e07a3270861c2a8ee, bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e, 0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e, a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1, 2822c72a59b58c00fc088aa551cdeeb92ca10fd23e23745610ff207f53118db9, 9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8, 3f446d316efe2514efd70c975d0c87e12357db9fca54a25834d60b28192c6a69, b2e771cbfa0a74d0774db162d28c1eecd3a7cb384dfe97522e9baabd1c04d304, 8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9, 52b6fb40e7efb09c2bebe8550178e7e30009600bdedd1acae085d753761b7598, c4389cc34b672c4f885547f413bf38575e6ee2b23a0ddfdd306a69c1775db6fc, 495cf3fd22d4fc2c6c86b689b68141ac7d0130b0bb5cbc834ef59275132ee5c2, 40c2e559992a7f595c593b419930a3f216516c3042ad86fb985348d53b6e01b9, b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546, 969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae
Domains	freefoodaid[.]com, wellnesscaremed[.]com, wellnessmedcare[.]org
IPv4	159[.]253[.]120[.]2, 193[.]187[.]148[.]169, 23[.]227[.]202[.]14
URLs	(smb)[:]//freefoodaid[.]com/documents/template_2_2[.]doc, (smb)[:]//wellnesscaremed[.]com/davwwwroot/buch/Downloads/blank[.]doc, (smb)[:]//wellnesscaremed[.]com/davwwwroot/venezia/Favorites/blank[.]doc,

TYPE	VALUE
URLs	(smb)[:]//wellnessmedcare[.]org@ssl/cz/Downloads/blank[.]doc, (smb)[:]//wellnessmedcare[.]org@ssl/pol/Downloads/blank[.]doc, hxxp[:]//freefoodaid[.]com/davwwwroot/2_2[.]lNk?init=, hxxp[:]//freefoodaid[.]com/documents/2_2[.]lNk?init=, hxxps[:]//wellnesscaremed[.]com/buch/Downloads/document[.]doc[.]LnK?init=, hxxp[:]//wellnesscaremed[.]com/buch/Downloads/document[.]doc[.]LnK?init=, hxxp[:]//wellnesscaremed[.]com/venezia/Favorites/document[.]doc[.]LnK?init=, hxxp[:]//wellnesscaremed[.]com/venezia/d/sd, hxxps[:]//wellnessmedcare[.]org/davwwwroot/cz/Downloads/document[.]LnK?init=, hxxp[:]//wellnessmedcare[.]org/davwwwroot/cz/Downloads/document[.]LnK?init=, hxxps[:]//wellnessmedcare[.]org/davwwwroot/pol/Downloads/document[.]LnK?init=, hxxp[:]//wellnessmedcare[.]org/davwwwroot/pol/Downloads/document[.]LnK?init= hxxps[:]//freefoodaid[.]com/documents/2_2[.]d, hxxps[:]//freefoodaid[.]com/tables/tables[.]d

Patch Link

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

References

https://www.zscaler.com/blogs/security-research/apt28-leverages-cve-2026-21509-operation-neusploit

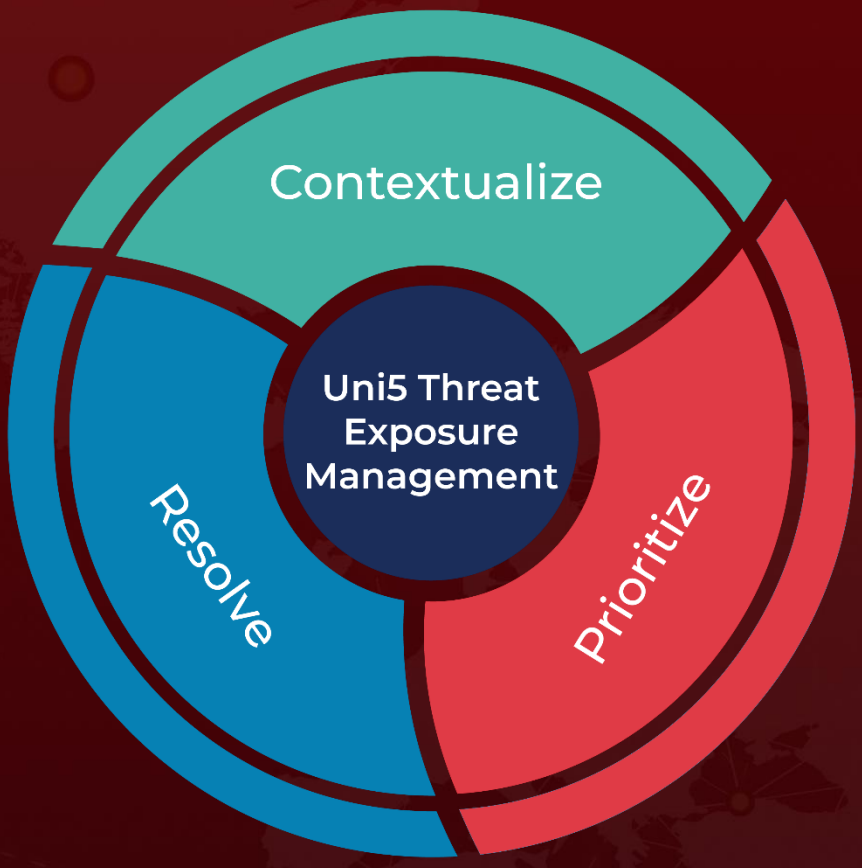
https://hivepro.com/threat-advisory/cve-2026-21509-microsoft-office-zero-day-under-active-exploitation/

https://cert.gov.ua/article/6287250

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

February 04, 2026 • 7:30 AM

More at www.hivepro.com