NuSummit Cybersecurity

cybersecurity.nusummit.com

THREAT ADVISORY REPORT

Mitigating an APT28 Microsoft Office Zero-Day Threat

Threat Actor
APT28 (aka Fancy Bear)

Campaign Name
Operation Neusploit

Severity
Critical

Primary Targets
Central & Eastern Europe (Ukraine, Slovakia, Romania)

Executive Summary

APT28, a Russia-linked advanced persistent threat group, has launched a highly sophisticated cyber-espionage campaign dubbed Operation Neusploit, targeting organizations in Central and Eastern Europe. The campaign exploits a zero-day vulnerability in Microsoft Office's Rich Text Format (RTF) handler (CVE-2026-21509) to achieve silent remote code execution.

The attack leverages socially engineered emails containing weaponized RTF documents and deploys multiple backdoors via a multi-stage infection chain. Zscaler analysts observed active exploitation in the wild on January 29, 2026, shortly after Microsoft released an emergency patch on January 26, 2026, indicating rapid operationalization by the threat actors.

Threat Actor Overview

APT28 is a well-documented Russian state-sponsored threat group known for:

- Cyber espionage and intelligence collection.
- Targeting government, military, diplomatic, and strategic organizations.
- Advanced malware development and rapid exploitation of zero-day vulnerabilities.

Operation Neusploit represents a notable escalation in APT28's tooling and delivery sophistication, particularly in the use of selective payload delivery and application-level persistence mechanisms.

Attack Vector and Initial Access

Delivery Method

- Spear-phishing emails containing malicious RTF attachments.
- Messages crafted in English, Romanian, Slovak, and Ukrainian.
- Content tailored to increase credibility and victim engagement.

Exploitation

- Opening the RTF document triggers CVE-2026-21509.
- No user interaction beyond opening the file is required.
- Arbitrary code execution occurs silently, without visible warnings.

Vulnerability Details

Attribute	Details
CVE ID	CVE-2026-21509
Type	Remote Code Execution
Affected Component	Microsoft Office RTF Handler
Severity	Critical
Patch Release Date	January 26, 2026

Infection Chain and Payloads

The campaign uses two distinct dropper variants, each deploying different payloads depending on the attacker's objectives.

Variant 1: Mini Door Deployment

Mini Door is a lightweight email-stealing backdoor implemented using Microsoft Outlook VBA.

Capabilities

- Monitors Outlook login events.
- Harvests emails from compromised mailboxes.
- Exfiltrates stolen communications to attacker-controlled email addresses.

Persistence Mechanism

- Modifies Windows Registry keys.
- Disables Outlook security controls.
- Forces automatic loading of the malicious VBA macro on Outlook startup.

Variant 2: PixyNetLoader → Covenant Grunt

The second dropper deploys PixyNetLoader, which acts as a staging mechanism.

Capabilities

- Establishes initial foothold.
- Deploys Covenant Grunt implant.
- Enables full command-and-control (C2) functionality.

This variant is used for deeper system compromise and long-term access.

Evasion and Anti-Analysis Techniques

Both dropper variants employ advanced evasion strategies:

- Geographic filtering: Payloads delivered only to victims in targeted countries.
- HTTP header validation: Malicious content served only when specific request headers are present.
- Server-side logic: Prevents payload delivery to sandboxes, researchers, and nontarget regions.

These techniques significantly reduce visibility and complicate detection and reverse engineering.

Attribution

Zscaler analysts attributed Operation Neusploit to APT28 based on:

Overlapping malware design patterns.

Consistent TTPs with previous APT28 campaigns.

Infrastructure and operational behaviour alignment.

Impact Assessment

Compromise of sensitive email communications.

Potential intelligence collection and espionage.

Long-term persistence within victim environments.

Elevated risk to government, defence, and strategic sectors.

Detection and Mitigation Recommendations

Immediate Actions

- Apply Microsoft patch for CVE-2026-21509 immediately.
- Block RTF attachments at email gateways where feasible.
- Enforce macro security policies in Microsoft Office and Outlook.

Defensive Measures

- Monitor registry changes related to Outlook startup and macro execution.
- Inspect outbound email traffic for anomalous forwarding behaviour.
- Deploy EDR rules for suspicious Office child-process execution.

Strategic Controls

- User awareness training focused on RTF-based phishing.
- Geo-aware traffic analysis for selective payload delivery patterns.
- Threat hunting for Covenant Grunt and VBA-based backdoors.

Conclusion

Operation Neusploit highlights APT28's continued investment in zero-day exploitation and stealthy, application-specific persistence mechanisms. The rapid exploitation following Microsoft's patch release underscores the group's operational maturity and ongoing focus on high-value targets in Central and Eastern Europe.

Organizations in the affected regions should treat this threat as active and critical, with immediate remediation and enhanced monitoring required.

References

https://cybersecuritynews.com/apt28-hackers-exploiting-microsoft-office-0-day/

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

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore

Follow us at: