Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

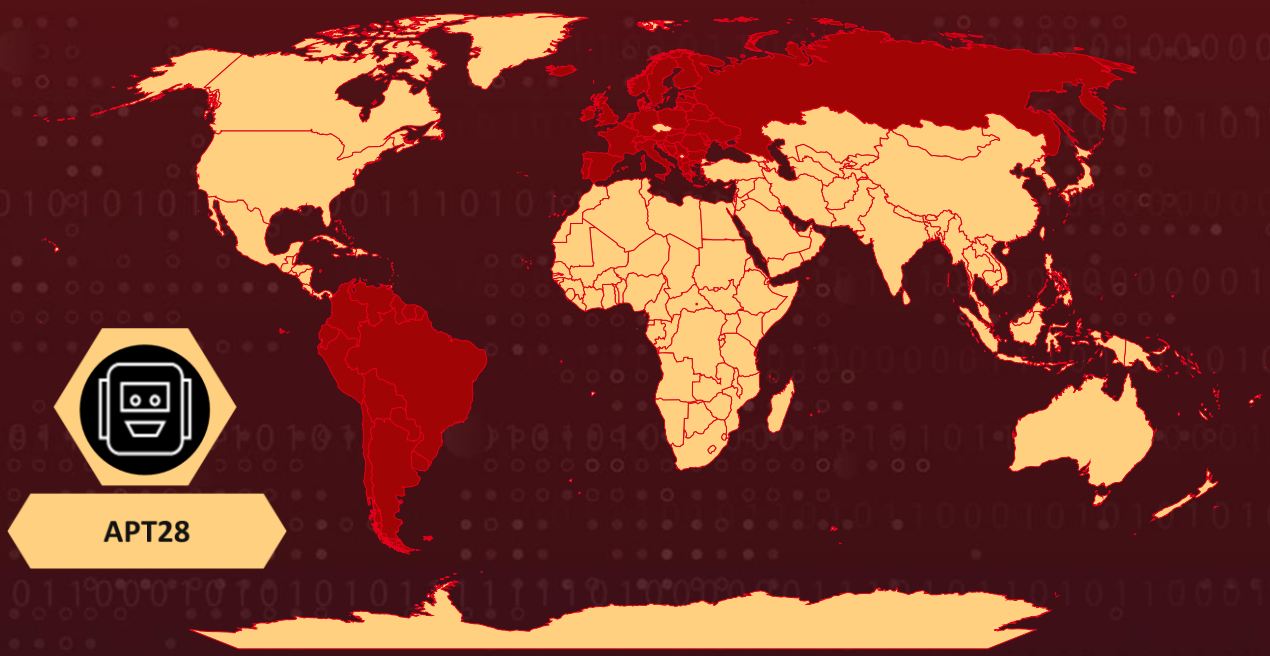
Operation RoundPress: APT28's Webmail Espionage Exposed

Date of Publication	Admiralty Code	TA Number
May 19, 2025	A1	TA2025154

Summary

Attack Discovered: 2023
Targeted Countries: Eastern Europe, Governments in Africa, Europe, and South America
Affected Industries: Governmental Entities, Defense Companies, Telecommunication, Academic, Military, Transport
Malware: SpyPress
Actor: APT28 (aka Sednit group, Sofacy, Fancy Bear, 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)
Campaign: Operation RoundPress
Attack: In Operation RoundPress, Russian state-backed hackers known as APT28 carried out a stealthy webmail espionage campaign by exploiting known vulnerabilities in popular email platforms like Roundcube, Horde, and Zimbra. The attackers sent specially crafted emails containing malicious JavaScript code that executed as soon as the email was opened-no clicks needed. This allowed them to silently steal session tokens, email content, and other sensitive data, which was then exfiltrated to their remote servers. Their targets included high-profile entities. The attackers kept a low profile by using lightweight scripts and frequently rotating domains to evade detection. This operation highlights how dangerous unpatched webmail systems can be even a single overlooked update can open the door to nation-state espionage.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-43770	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	✗	✓	✓
CVE-2020-35730	Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	✗	✓	✓
CVE-2024-11182	MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability	MDaemon Email Server	✓	✗	✓
CVE-2024-27443	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)	✗	✗	✓

Attack Details

#1

In a carefully orchestrated cyberespionage campaign dubbed Operation RoundPress, the notorious **Sednit group** (also known as APT28) has been exploiting vulnerabilities in webmail platforms to infiltrate high-value targets across Eastern Europe and beyond. At the core of this campaign are cross-site scripting (XSS) vulnerabilities in popular webmail software like Roundcube, Zimbra, MDaemon, and Horde, which Sednit weaponizes to deliver JavaScript-based payloads directly into the victim's inbox.

#2

These attacks typically begin with well-crafted spearphishing emails, which appear to relay legitimate news or intelligence, but carry hidden malicious code. For example, one phishing email sent to a Ukrainian user in September 2024 referenced a supposed SBU operation arresting a banker in Kharkiv, clearly designed to appear urgent and credible. When the recipient opens the email in a vulnerable webmail interface, the embedded JavaScript executes silently, launching the SpyPress malware. These payloads don't install anything persistently; instead, they live inside the email and activate only when viewed in an unpatched browser-based client.

#3 Each SpyPress variant, tailored to its respective platform (Roundcube, Horde, Zimbra, MDaemon) focuses on stealing email content, credentials, contacts, and even two-factor authentication secrets. The Roundcube and Zimbra variants, for instance, can generate Sieve rules that forward every incoming email to a server controlled by the attackers, enabling continuous access even after a password reset. Some variants also exfiltrate app passwords or session histories, allowing the threat actors to log in undetected.

#4 Despite some missteps like deploying an outdated exploit in Horde webmail Sednit has shown technical sophistication. They even discovered a zero-day flaw in MDaemon (CVE-2024-11182), which they abused before a patch was released. Each variant of the SpyPress payload communicates with a set of hardcoded command-and-control (C2) servers, using obfuscated JavaScript and standard HTTP POST requests to quietly siphon off sensitive data.

#5 Operation RoundPress reflects a broader trend in cyberespionage: a shift toward exploiting web-based email clients that remain vulnerable despite years of public security disclosures. Sednit continues to target outdated systems with low-effort but high-reward attacks. As long as organizations rely on unpatched or legacy webmail software, the door remains open for attackers to silently surveil inboxes and harvest intelligence on a global scale.

Recommendations

- **Keep Your Webmail Software Updated:** Make sure you're using the latest versions of webmail tools like Roundcube, Horde, and Zimbra. Updates often fix bugs that hackers use to break in.
- **Use a Web Application Firewall (WAF):** A WAF acts like a filter between your webmail and the internet. It can block suspicious activity like strange scripts hiding in emails.
- **Clean Up Incoming Emails:** Emails can carry hidden code. Use tools that automatically clean and check emails before they reach inboxes to remove dangerous content.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1583 Acquire Infrastructure	T1583.001 Domains	T1583.004 Server
T1587 Develop Capabilities	T1587.004 Exploits	T1587.001 Malware	T1190 Exploit Public-Facing Application
T1203 Exploitation for Client Execution	T1027 Obfuscated Files or Information	T1187 Forced Authentication	T1556 Modify Authentication Process
T1556.006 Multi-Factor Authentication	T1087 Account Discovery	T1087.003 Email Account	T1056 Input Capture
T1056.003 Web Portal Capture	T1119 Automated Collection	T1114 Email Collection	T1114.002 Remote Email Collection
T1114.003 Email Forwarding Rule	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1071.003 Mail Protocols
T1132 Data Encoding	T1132.001 Standard Encoding	T1020 Automated Exfiltration	T1041 Exfiltration Over C2 Channel
T1566 Phishing	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter
T1059.007 JavaScript			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	41FE2EFB38E0C7DD10E6009A68BD26687D6DBF4C, 60D592765B0F4E08078D42B2F3DE4F5767F88773, 1078C587FE2B246D618AF74D157F941078477579, 8EBBBC9EB54E216EFFB437A28B9F2C7C9DA3A0FA, F95F26F1C097D4CA38304ECC692DBAC7424A5E8D, 2664593E2F5DCFDA9AAA1A2DF7C4CE7EEB1EDBB6, B6C340549700470C651031865C2772D3A4C81310, 65A8D221B9ECED76B9C17A3E1992DF9B085CECD7, 6EF845938F064DE39F4BF6450119A0CDBB61378C, 8E6C07F38EF920B5154FD081BA252B9295E8184D, AD3C590D1C0963D62702445E8108DB025EEBEC70, EBF794E421BE60C9532091EB432C1977517D1BE5, F81DE9584F0BF3E55C6CF1B465F00B2671DAA230, A5948E1E45D50A8DB063D7DFA5B6F6E249F61652
IPv4	185[.]225[.]69[.]223, 193[.]29[.]104[.]152, 45[.]137[.]222[.]24, 91[.]237[.]124[.]164, 185[.]195[.]237[.]106, 91[.]237[.]124[.]153, 146[.]70[.]125[.]79, 89[.]44[.]9[.]74, 111[.]90[.]151[.]167
Domains	sqj[.]fr, tgh24[.]xyz tuo[.]world, lsjb[.]digital, jiaw[.]shop, hfuu[.]de, raxia[.]top, rnl[.]world, hijx[.]xyz, ikses[.]net

Patch Links

https://roundcube.net/news/2023/09/15/security-update-1.6.3-released

https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13

https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html

https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes

References

https://www.welivesecurity.com/en/eset-research/operation-roundpress/

https://www.hivepro.com/threat-advisory/roundcube-webmail-faces-unrelenting-exploitation/

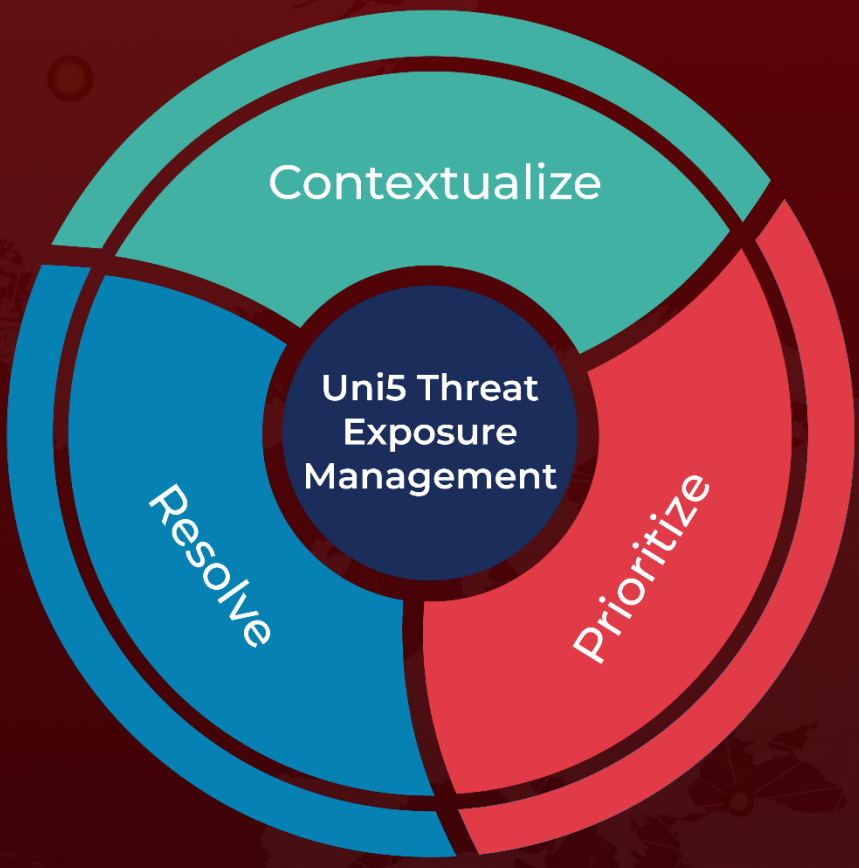
https://hivepro.com/threat-advisory/apt28-leveraged-three-roundcube-exploits-in-espionage-campaign/

https://www.hivepro.com/threat-advisory/apt28s-tactical-exploitation-of-critical-vulnerabilities/

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

May 19, 2025 • 6:00 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com