
Weekly Cybersecurity Briefing (21 September – 27 September 2026)

CyberSecBrief Team

CyberSecBrief provides clear, concise cybersecurity briefings that summarise the most relevant developments of the week. The report highlights notable incidents, key themes, and significant activity across the threat landscape, supported by daily updates sourced from trusted feeds and advisories. Its purpose is to offer a practical, time-efficient overview for readers who need a reliable snapshot of current cybersecurity events.

For more briefings, visit [CYBERSECBRIEF.COM](https://cybersecbrief.com).



September 28, 2026

Editorial Analysis

ShinyHunters appeared in several of this week's stories, and the surrounding reporting shows how little the ransomware brand itself tells us about an extortion operation. The group renewed mass exploitation of **Oracle PeopleSoft CVE-2026-35273**, seized **CI0p**'s leak site with an eight-figure demand tied to the gang's Oracle E-Business Suite campaign, and claimed a breach of **FBI Jobs**, which the FBI says it is investigating. Elsewhere, encryption became optional. **PAYLOAD** disrupted a Middle Eastern manufacturer through a malicious Group Policy Object without running a ransomware binary on Windows machines. The new **n0n** group threatens to destroy backups and shadow copies after gaining access with infostealer credentials, and claimed 13 victims in its first week. Microsoft's **Storm-2570** research found one affiliate deploying Qilin, DragonForce, Anubis and BERT while reusing MeshAgent, ntdsutil, s5cmd and Rclone. The tools and branding change between incidents, while access, credential theft and exfiltration remain central to the operations.

Several exploited weaknesses this week had been public for months. The **PeopleSoft** flaw was a zero-day between 27 May and 9 June, Oracle patched it on 10 June, and the September campaign targeted organisations that had added WAF rules but had not applied the patch. ASEC reported attacks on unpatched Korean IIS servers through **CVE-2019-18935**, while the **Mini Shai-Hulud** worm continued spreading through the hijacked [actions-cool/issues-helper](#) GitHub Action, which had gone unaddressed for four months. Six more repositories were infected between 20 and 24 September through routine workflows.

Cryptocurrency theft ran at two very different scales. **Bitget** lost \$351.6 million in a single backend compromise attributed to suspected North Korean actors, with Arkham tracing roughly \$228 million leaving in 18 minutes. The **Contagious Interview** campaign works through individual developers instead, using fake recruiters to reach more than 30,000 devices and more than 7,000 wallets, and now targeting Rust crates.io maintainers. The criminal cases resolved this week moved much more slowly. **Vardanyan** was sentenced for Ryuk-related access work from 2019 and 2020, while **Wagenius** received 70 months for the AT&T and Verizon extortion, in both cases years after the underlying intrusions.

Highlights of the Week

Citrix Patches Eight NetScaler Flaws, Two Exploited in the Wild

Citrix disclosed eight NetScaler ADC and Gateway vulnerabilities on 27 September, confirming exploitation of CVE-2026-88771, an unauthenticated remote code execution flaw affecting default configurations, and CVE-2026-88772, a DTLS memory overflow, both scoring 9.5 on CVSS v4.0. watchTowr had reported the zero-days a day earlier, and some administrators took appliances

offline. Fixes are available in builds 14.1-73.37 and 13.1-64.23.

Sources:

- [Citrix](#)

ShinyHunters Bypasses WAF Rules to Exploit Oracle PeopleSoft Flaw

Mandiant and Google Threat Intelligence Group reported renewed mass exploitation of Oracle PeopleSoft flaw CVE-2026-35273 by ShinyHunters, tracked as UNC6240. The group bypasses web application firewall rules by URL-encoding one character of the PSEMHUB path and has deployed web shells on dozens of systems across education, technology, healthcare and government. Follow-on tools include the SIDEYE backdoor and the Neo-reGeorg tunnelling toolkit.

Sources:

- [Mandiant](#)

North Korean Hackers Steal \$351.6M From Bitget

Bitget confirmed suspected North Korean actors stole \$351.6 million from hot and warm wallets on 24 September. Attackers compromised backend wallet infrastructure, spoofed transaction data and triggered the authorisation process to move funds across Ethereum, XRP Ledger, Arbitrum, Optimism, BSC and Base. The exchange later raised its loss estimate to \$387.5 million after identifying additional stolen assets on Zcash and TRON.

Sources:

- [The Hacker News](#)

WordPress Core Flaws Enable Admin Takeover and Remote Code Execution

WordPress patched CVE-2026-93485, an unauthenticated stored cross-site scripting flaw in core comment handling that can be chained to remote code execution, and CVE-2026-87902, a path traversal flaw allowing inclusion of arbitrary local PHP files. Attacks on CVE-2026-87902 began within hours of the 22 September release. Fixes arrived in versions 7.1.1 and 7.1.2, backported as far as 4.7.

Sources:

- [IDNSEC](#)
- [Kaspersky](#)
- [GitHub Security Advisories](#)

Threats

ShinyHunters Hijacks CI0p Ransomware Gang's Leak Site

ShinyHunters seized CI0p's dark web leak site and defaced it with an eight-figure demand tied to the gang's Oracle E-Business Suite campaign. CI0p later restored a message asking ShinyHunters to make contact through another platform.

Sources:

- [The Record](#)

North Korean Contagious Interview Campaign Targets Rust Developers

The Rust Project warned that Contagious Interview operators are posing as recruiters to target crates.io maintainers with malware. Authorities report over 30,000 infected devices and credentials stolen from more than 7,000 cryptocurrency wallets since December 2025.

Sources:

- [Rust Project](#)

Ransomware Affiliate Storm-2570 Reuses Toolset Across Brands

Microsoft tracked ransomware affiliate Storm-2570 deploying Qilin, DragonForce, Anubis and BERT payloads while reusing MeshAgent, ntdsutil, s5cmd and Rclone. The actor has been active since April 2025 and affected healthcare, government and financial organisations.

Sources:

- [Microsoft Threat Intelligence](#)

Infrastructure & Exploits

F5 Patches Actively Exploited BIG-IP APM Zero-Day

F5 disclosed CVE-2026-94127, a heap-based buffer overflow in BIG-IP APM configured as an OAuth Authorisation Server that allows unauthenticated remote code execution. F5 confirmed in-the-wild exploitation and released engineering hotfixes for affected branches.

Sources:

- [F5](#)

Check Point Firewalls and Management Servers Under Active Attack

Check Point confirmed exploitation of CVE-2026-85102, a pre-authentication RCE in Security Gateway VPN certificate handling, since 12 September. It also disclosed zero-day CVE-2026-93616, a Security Management path traversal flaw, with fixes available for both.

Sources:

- [Check Point](#)

CISA Adds Exploited SharePoint and MikroTik RouterOS Flaws to KEV Catalogue

CISA added Microsoft SharePoint flaw CVE-2026-65660 and MikroTik RouterOS flaw CVE-2026-67279 to its Known Exploited Vulnerabilities Catalogue on evidence of active exploitation. Federal agencies had a patching deadline of 28 September for the SharePoint flaw.

Sources:

- [CISA](#)

Tools & Techniques

First Malware Using AI Models as Command and Control

Cisco Talos disclosed CLOSEDQUORUM, a Windows implant in which four commercial large language model providers vote on actions such as credential theft, process injection or persistence. The majority choice executes automatically, and stolen data leaves through an encrypted Discord webhook.

Sources:

- [Cisco Talos](#)

Lunex Stealer Uses Vulnerable AMD Driver to Blind Security Tools

Ontinue analysed a Lunex campaign that uses AMD's PDFWKRN.sys driver to zero the kernel callbacks of 20 listed security drivers before deploying a browser and wallet stealer. It also registers a Chrome Native Messaging Host that survives deletion of the stealer.

Sources:

- [Ontinue](#)

PAYLOAD Ransomware Disrupts Systems Through Group Policy

Kaspersky investigated an April 2026 attack on a Middle East manufacturer in which actors with domain admin access created a malicious Group Policy Object that delivered ransom notes and disabled the local administrator account. No ransomware binary ran on Windows machines.

Sources:

- [Securelist \(Kaspersky\)](#)

Policy & Legal

Ryuk Ransomware Access Broker Sentenced to 24 Months

Karen Serobovich Vardanyan, extradited from Ukraine, was sentenced to 24 months in prison for gaining network access used in Ryuk ransomware attacks between March 2019 and June 2020. Prosecutors said he and co-conspirators received about 1,610 bitcoins in ransom payments.

Sources:

- [BleepingComputer](#)

US Soldier Sentenced to 70 Months for AT&T and Verizon Extortion

Cameron Wagenius, known as "Kiberphant0m", was sentenced to 70 months in prison and ordered to pay \$294,978 in restitution. He stole call and text metadata for over 100 million AT&T customers using exposed Snowflake credentials and extorted the victims.

Sources:

- [Krebs on Security](#)

Weekly Topic Distribution



Copyright and Legal Notice

© CyberSecBrief. All rights reserved.

Reproduction, redistribution, or modification of this document or its contents without explicit written permission is strictly prohibited.

Disclaimer & Terms of Use

CyberSecBrief is a personal, non-commercial project operated from Germany and is not affiliated with any company or organisation. The information provided is intended solely for general informational and educational purposes and does not constitute professional cybersecurity, legal, or financial advice. Security-related information changes rapidly; although accuracy and timeliness are sought, no guarantee is given regarding completeness, correctness, or applicability. Users must verify details with official sources or qualified professionals before making decisions.

The owner disclaims liability for any indirect, incidental, or consequential damages arising from reliance on this material. External links and third-party feeds are offered for convenience; their content, accuracy, availability, and privacy practices are outside our control and are not endorsed. Sponsored or promoted material may appear, yet inclusion does not imply endorsement.

Original content is protected by copyright. Where external material is used, appropriate attribution is provided. Reproduction of original content without prior written consent is prohibited. Content may be updated, modified, or removed at any time without notice.

This disclaimer and the Terms of Use are governed by the laws of Germany and applicable European Union regulations. Should any provision be deemed invalid, the remaining provisions shall continue in full force and effect.

Credits and Sources

CVE entries are sourced from the [CVE® Program](#), operated by [The MITRE Corporation](#), and from the [National Vulnerability Database \(NVD\)](#), maintained by the National Institute of Standards and Technology (NIST). The NVD is provided “as is” without warranty of any kind.

Definitions for APT groups are derived from the [MITRE ATT&CK® knowledge base](#), reproduced and distributed with the permission of The MITRE Corporation. © 2025 The MITRE Corporation.

All feeds and advisories are properly acknowledged and linked to their original sources where referenced, including within briefings.

Logo icon created by Ida Desi Mariana — [Flaticon](#).

Powered by [CyberFeedBites](#).

Source

This briefing is published by *CyberSecBrief* –
<https://www.cybersecbrief.com/>