

Weekly Intelligence Summary

Report Date: 09.02.2026

Intelligence Cut-off Date: 06.02.2026

Weekly Focus: Targeted supply chain compromise delivers trojanised Notepad++ updates

A highly targeted campaign in 2025 abused a trusted update infrastructure to distribute malware to selected victims via the Notepad++ software update mechanism.

A supply chain compromise affecting the Notepad++ text editor has been attributed to the China-aligned threat actor Lotus Blossom. Instead of exploiting vulnerabilities in Notepad++ itself, attackers compromised a third-party hosting provider used to deliver software updates, allowing them to intercept update requests and selectively distribute trojanised update packages. The activity took place over several months in 2025 and targeted a small number of specific organisations, suggesting espionage-motivated objectives.

The malicious updates deployed a custom backdoor known as Chrysalis, designed to provide persistent, stealthy access to infected systems. The malware used techniques such as DLL sideloading, encrypted configuration data, and API hashing to evade detection. Once installed, it enabled remote execution, reconnaissance, credential access, file exfiltration, and follow-on payload delivery, while maintaining low-frequency command-and-control communications to avoid detection.

Following the discovery of the campaign, the affected hosting infrastructure was secured, and users were advised to update to verified clean versions of Notepad++ and review systems for indicators of compromise, including unexpected outbound connections from Notepad++ processes, mismatched update hashes, and unusual process behaviour following updates.

Why It Matters...

This incident highlights the continued evolution of software supply chain attacks targeting trusted update mechanisms rather than application vulnerabilities. By compromising update delivery infrastructure, Lotus Blossom was able to bypass conventional security controls that rely on trusted software distribution channels, enabling long-term, covert access to high-value targets. The selective delivery of malicious updates reduces the likelihood of detection.

The campaign reinforces the need for organisations to treat software updates as a critical trust boundary, implement update validation and monitoring controls, and inspect network and process activity from trusted applications. As supply chain compromises increasingly target widely used utilities and development tools, trusted software ecosystems themselves are becoming a primary attack surface for advanced persistent threat groups.

Intelligence Overview

Vulnerabilities

In Operation Neusplit, APT28 exploited a recently patched Microsoft vulnerability tracked as CVE-2026-21509 (CVSS: 7.8 | OVSS: 90) to target Central and Eastern European users.

Two actively exploited in the wild vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), tracked as CVE-2026-1281 (OVSS: 77 | CVSS: 9.8) and CVE-2026-1340 (OVSS: 74 | CVSS: 9.8), enable remote arbitrary code execution in affected systems.

CISA added four vulnerabilities in Sangoma FreePBX, GitLab and SolarWinds Web Help Desk (WHD) to its KEV catalogue based on evidence of active exploitation.

Data Breaches

Investment platform Betterment confirmed a data breach affecting 1.4 million customers. The breach reportedly resulted from a targeted social engineering campaign, which provided access to a third-party software platform.

Two novel extortion groups, 0APT and CoinbaseCartel, respectively claimed the breaches of Urban Outfitters and NGC software, two leading enterprises in the retail sector.

Supply Chain

Unidentified threat actors deployed a supply chain campaign targeting developers that was distributed via the compromise of a legitimate Open VSX Registry that pushed malicious OpenVSX extensions with embedded GlassWorm malware.