ultraviolet

THREAT ADVISORY

Notepad++ Hijacked for Six Months

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
February 3, 2026
TLP:GREEN

Executive Snapshot

The compromise of the Notepad++ update feature by Chinese state-sponsored hackers underscores the urgent need for organizations to strengthen their cybersecurity measures, particularly regarding software supply chains. This incident highlights vulnerabilities that can be exploited through legitimate software channels, necessitating proactive strategies to mitigate risks.

- Implement strict verification procedures for software updates, ensuring integrity through signature checks and validation mechanisms.
- Conduct regular security audits of third-party software providers to identify and address potential vulnerabilities in supply chains.
- Foster a culture of vigilance, encouraging employees to report unusual behaviors and anomalies within systems to enhance overall security awareness.

TIDE Team Analysis

The Notepad++ update feature was compromised by suspected Chinese state-sponsored hackers, particularly the group known as Lotus Blossom, exposing vulnerabilities in the widely used text editor from June to December 2025. The attackers exploited a compromised hosting provider, redirecting legitimate update traffic to their servers. By delivering malware disguised as authentic updates, they targeted sensitive sectors, such as government and telecommunications. This incident underscores the escalating threat posed by supply chain attacks, where adversaries manipulate established software mechanisms to infiltrate networks.

An official update from Notepad++ detailed the attack as an infrastructure-level compromise rather than a flaw within the software itself. This ensured that while Notepad++ maintained its integrity, the update mechanism became the unwitting vessel for the attack. Researchers identified a custom backdoor that was utilized by Lotus Blossom. This sophisticated malware enabled attackers to perform reconnaissance, data exfiltration, and other malicious activities within compromised networks.

The timeline of the attack reveals that although the immediate access was interrupted in September when server maintenance took effect, the attackers maintained residual control until December. This is indicative of the agility and preparedness displayed by advanced persistent threat (APT) groups, illustrating their capacity to adapt and evolve after initial setbacks. Researcher analysis noted that the backdoor employed was not previously documented, emphasizing the group's capabilities to create innovative tools for cyber espionage.

In response to the breach, Notepad++ implemented swift remedial measures. The development team migrated their update infrastructure to a more secure hosting provider and enhanced the update verification process. Versions 8.8.8 and older had a weakness in their 'WinGUp' update tool. Starting with version 8.8.9, updates underwent rigorous signature checks, ensuring that any failures in verification would halt the installation of potentially malicious software.

Lotus Blossom's operations are not isolated incidents; they reflect a broader pattern in cyber espionage tactics employed by state-affiliated groups. By focusing on critical infrastructure, the group aims to gather intelligence and potentially disrupt operations in sensitive sectors. Their approach is methodical, leveraging real-time understanding to identify opportunities for exploitation. This is yet another reason the threat actors were attributed to an APT group.

The specific targeting of Notepad++ further illustrates the importance of monitoring and securing supply chains in software development. The attack's implications extend beyond Notepad++ itself, serving as a stark reminder of the vulnerabilities that can exist in software distribution mechanisms. Organizations must remain vigilant and adopt updated security protocols to mitigate risks associated with similar threats.

Notepad++ urged users to remain aware of any unusual behaviors on their systems, prompting individuals to be more proactive in their cybersecurity practices. This cultural shift implies a growing awareness of the risks associated with software and a collective responsibility among users and developers to safeguard their digital environments.

The Notepad++ incident highlights a critical turning point in the ongoing battle against state-sponsored cyber threats. With the increasing sophistication of threat actors, organizations must adapt their defense strategies, ensuring that their software supply chains are fortified against exploitation. This incident serves as a call to action for the software community to prioritize security measures and continuous vigilance to effectively counter the evolving tactics of adversarial groups like Lotus Blossom.

Why It Matters

The compromise of the Notepad++ update feature highlights the concerning reality that widely used applications can become significant attack surfaces. As a tool favored by developers and IT professionals globally, Notepad++ presents a rich target for malicious actors looking to exploit vulnerabilities. The fact that it is installed and updated across various environments, often without rigorous oversight, means administrators may lack visibility into potential security risks associated with its deployment. This opens avenues for attackers to leverage the software as a vector for delivering malware, allowing them to infiltrate networks and extract sensitive data efficiently.

One of the key issues surrounding Notepad++ is the lack of a centralized inventory and management system for its various versions across organizations. Because many users obtain updates individually, inconsistencies can emerge, with some systems running outdated or vulnerable versions. This fragmentation not only complicates patch management efforts but also creates potential weak points that attackers can exploit. Without a cohesive management strategy to monitor which versions are in use, organizations may inadvertently keep insecure instances active, allowing for ongoing vulnerabilities within their operational landscape.

Historically, similar threats have been observed with various applications, illustrating a pattern where reliance on popular software creates opportunities for exploitation. Take, for instance, the SolarWinds attack, where a compromised update mechanism was used to breach multiple high-profile organizations, including government entities. Similarly, incidents such as the CCleaner malware incident where attackers inserted malicious code into a legitimate software update serve as cautionary tales about the risks associated with unmonitored update processes. These parallels illustrate the critical need for heightened security protocols and rigorous oversight to safeguard against the evolving tactics of sophisticated cyber adversaries.

How to Respond

- Perform regular audits of all applications, including Notepad++, to identify and patch vulnerable versions across your network

- Incorporate signature checks and integrity validations within your software management system to ensure only verified updates are applied

- Continuously monitor network traffic and system behavior for signs of unauthorized access or unusual activities

What UltraViolet Cyber is Doing

- Monitoring client environments for suspicious activity, including commonly exploited applications like Notepad++
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | in UltraViolet Cyber | 𝕏 ▶ @uv_cyber