Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

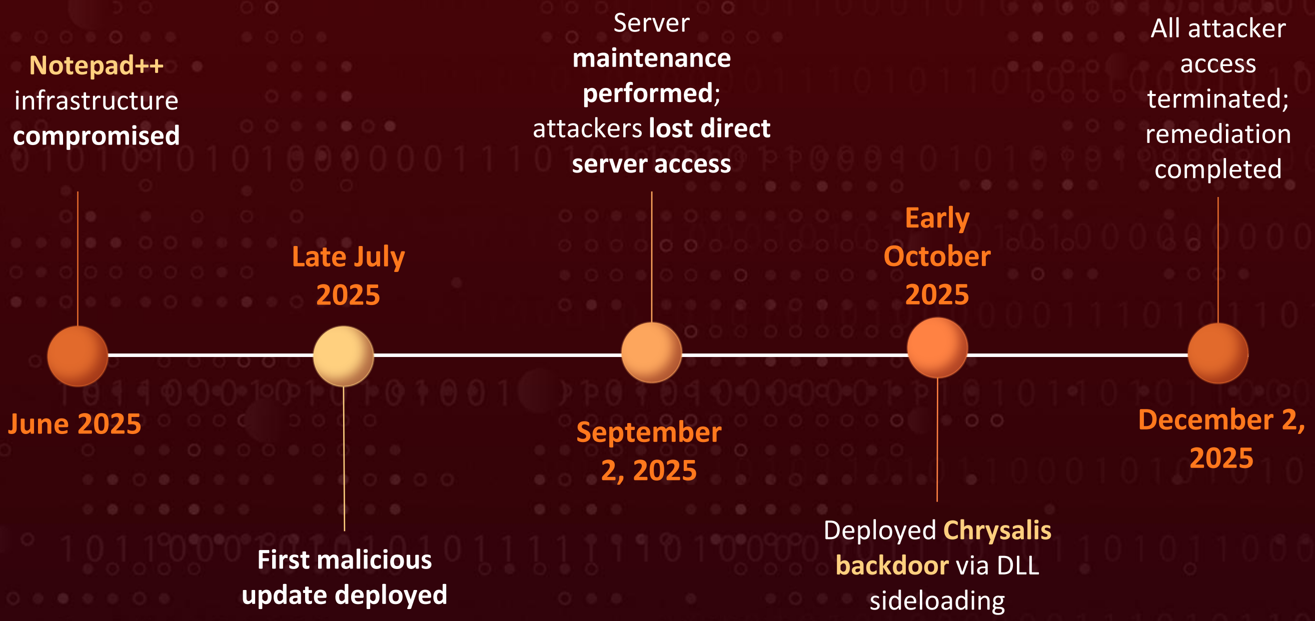
Chrysalis Backdoor: A Quiet Passenger in Notepad++ Updates

Date of Publication	Admiralty Code	TA Number
February 04, 2026	A1	TA2026034

Summary

First Seen: June 2025
Malware: Chrysalis Backdoor
Threat Actor: Lotus Blossom (also known as LOTUS PANDA, Billbug, Bronze Elgin, Spring Dragon, Raspberry Typhoon, Thrip)
Targeted Regions: Australia, Belize, Brunei, Cambodia, Costa Rica, El Salvador, Guatemala, Honduras, Indonesia, Laos, Malaysia, Myanmar, Nicaragua, Panama, Philippines, Singapore, Thailand, Timor-Leste, Vietnam
Targeted Industries: Government, Financial Services, Information Technology, Telecom, Aviation, Critical Infrastructure, Media
Targeted Platform: Windows
Targeted Product: Notepad++
Attack: A sophisticated supply chain attack attributed to the Chinese state-sponsored APT group Lotus Blossom, which compromised the infrastructure hosting Notepad++ to deliver a previously undocumented backdoor named Chrysalis. The attackers hijacked the update traffic of Notepad++ by compromising the hosting provider's infrastructure, selectively redirecting targeted users to malicious servers that served trojanized update packages containing malware payloads, including the Chrysalis backdoor, Cobalt Strike beacons, and Metasploit-based shellcode loaders.

Attack Timeline



June 2025
Notepad++ infrastructure **compromised**

Late July 2025
First malicious update deployed

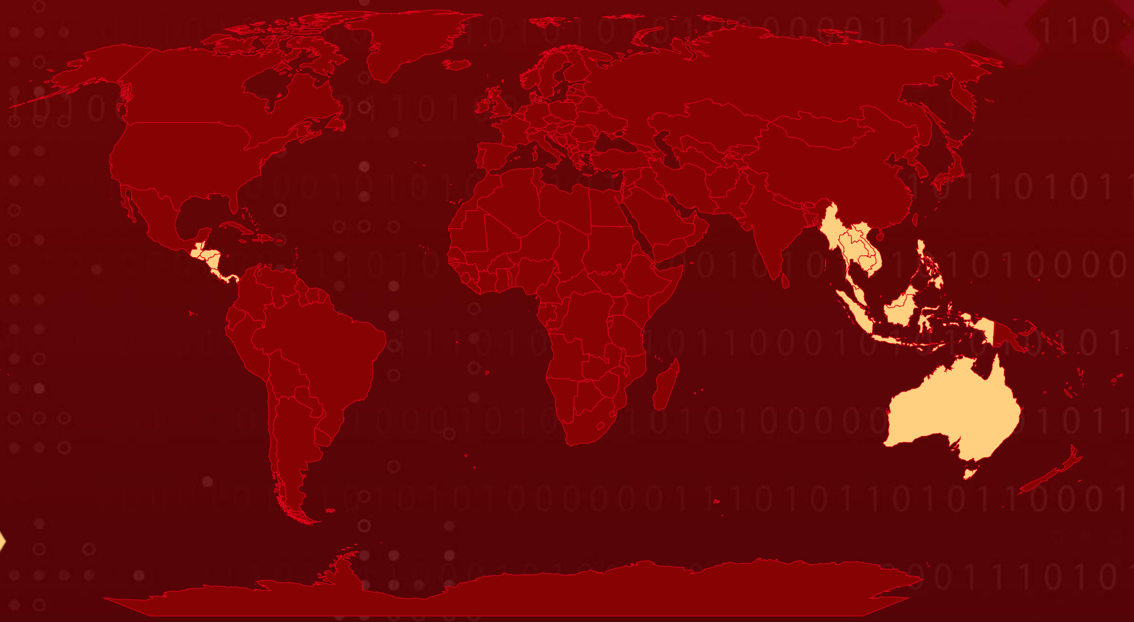
September 2, 2025
Server **maintenance performed**; attackers **lost direct server access**

Early October 2025
Deployed **Chrysalis backdoor** via DLL sideloading

December 2, 2025
All attacker access terminated; remediation completed

Attack Regions

Lotus Blossom



🟨 Targeted 🟥 Non-Targeted

Powered by Bing

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

Attack Details

#1

Notepad++ was affected by a supply-chain attack rooted in compromised hosting infrastructure, not in its source code. This attack campaign was attributed to the Chinese APT group Lotus Blossom. Attackers abused a former shared hosting provider to intercept and redirect software update traffic to malicious servers.

#2

The compromise began in June 2025, when attackers gained access to the hosting environment supporting the Notepad++ distribution domain. This access allowed them to selectively reroute update requests for notepad-plus-plus.org. Although server access was cut off during scheduled kernel and firmware updates on September 2, 2025, the attackers retained credentials to internal services until December 2, 2025, enabling continued traffic redirection. The attack specifically exploited weak update verification mechanisms present in older versions of Notepad++.

#3

The attack chain was triggered when users launched the legitimate GUP.exe updater. Instead of retrieving a valid update, the updater downloaded a malicious update.exe from an attacker-controlled infrastructure. This file was an NSIS installer, a delivery method frequently used by advanced threat actors. The installer created a hidden "Bluetooth" directory in AppData, deployed a renamed Bitdefender Submission Wizard binary, and placed a malicious log.dll alongside it. This setup enabled DLL sideloading, allowing the DLL to decrypt and execute the Chrysalis backdoor.

#4

The Chrysalis backdoor was highly capable. It employed heavy obfuscation, custom API hashing, RC4-encrypted configuration data, and HTTPS-based command-and-control traffic. It established persistence through Windows services or registry Run keys, collected detailed system information, and supported remote shell access, process execution, file management, directory enumeration, and self-removal.

#5

Multiple parallel attack chains were active between July and October 2025. The operators continuously rotated C2 domains, loaders, and payloads. Additional components included Metasploit shellcode that delivered Cobalt Strike beacons, in-memory loaders built with the Tiny C Compiler, and a notable loader that abused Microsoft’s internal Warbird protection framework. The campaign demonstrates a sustained, infrastructure-driven supply-chain attack characterized by evolving techniques and disciplined operational security.

Recommendations

Hunt for DLL Sideloading Artifacts: Search endpoints for suspicious BluetoothService.exe processes loading log.dll from %AppData%\Bluetooth directories, particularly where BluetoothService.exe matches the hash of the legitimate Bitdefender Submission Wizard binary but is located in non-standard paths.

Monitor for NSIS Installer Artifacts: Detect NSIS installer activity by monitoring for the creation of %LocalAppData%\Temp\ns .tmp directories and investigating the origin of any identified NSIS installers, especially those spawned from update processes.

Implement Application Allowlisting: Deploy application control policies to prevent execution of unauthorized binaries from AppData directories and other non-standard locations commonly abused by threat actors for persistence.

Detect System Information Gathering Commands: Alert on sequential execution of reconnaissance commands (whoami, tasklist, systeminfo, netstat -ano) particularly when output is redirected to files, as this pattern was consistently observed across multiple execution chains.

Monitor for temp.sh File Upload Activity: Detect and investigate any network traffic or DNS resolutions involving the temp.sh file hosting service, which is rarely observed in legitimate corporate environments and was used by attackers to exfiltrate system information.

Verify Third-Party Software Sources: Implement controls to verify the integrity and authenticity of all third-party software and updates, considering the use of cryptographic verification beyond basic certificate validation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
	T1106: Native API	
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	T1543.003: Windows Service
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL
	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
	T1140: Deobfuscate/Decode Files or Information	
	T1036: Masquerading	
	T1055: Process Injection	
	T1620: Reflective Code Loading	
	T1480: Execution Guardrails	T1480.002: Mutual Exclusion

Tactic	Technique	Sub-technique
Discovery	T1083: File and Directory Discovery	
	T1082: System Information Discovery	
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1070: Indicator Removal	T1070.004: File Deletion

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//59[.]110[.]7[.]32[:]8880/uffhxpSy, hxxp[:]//59[.]110[.]7[.]32[:]8880/api/getBasicInfo/v1, hxxp[:]//59[.]110[.]7[.]32[:]8880/api/Metadata/submit, hxxp[:]//124[.]222[.]137[.]114[:]9999/3yZR31VK, hxxp[:]//124[.]222[.]137[.]114[:]9999/api/updateStatus/v1, hxxp[:]//124[.]222[.]137[.]114[:]9999/api/Info/submit, hxxps[:]//api[.]wiresguard[.]com/users/system, hxxps[:]//api[.]wiresguard[.]com/api/getInfo/v1, hxxps[:]//api[.]wiresguard[.]com/api/Info/submit, hxxp[:]//45[.]76[.]155[.]202/update/update[.]exe, hxxp[:]//45[.]32[.]144[.]255/update/update[.]exe, hxxp[:]//95[.]179[.]213[.]0/update/update[.]exe, hxxp[:]//95[.]179[.]213[.]0/update/install[.]exe, hxxp[:]//95[.]179[.]213[.]0/update/AutoUpdater[.]exe, hxxp[:]//45[.]76[.]155[.]202/list, hxxps[:]//self-dns[.]it[.]com/list, hxxps[:]//45[.]77[.]31[.]210/users/admin, hxxps[:]//cdncheck[.]it[.]com/users/admin, hxxps[:]//safe-dns[.]it[.]com/help/Get-Start, hxxps[:]//45[.]77[.]31[.]210/api/update/v1, hxxps[:]//45[.]77[.]31[.]210/api/FileUpload/submit, hxxps[:]//cdncheck[.]it[.]com/api/update/v1, hxxps[:]//cdncheck[.]it[.]com/api/Metadata/submit, hxxps[:]//cdncheck[.]it[.]com/api/getInfo/v1,

TYPE	VALUE
URLs	hxxps[:]//cdncheck[.]it[.]com/api/FileUpload/submit, hxxps[:]//safe-dns[.]it[.]com/resolve, hxxps[:]//safe-dns[.]it[.]com/dns-query, hxxps[:]//api[.]skycloudcenter[.]com/a/chat/s/70521ddf-a2ef-4adf-9cf0-6d8e24aaa821, hxxps[:]//api[.]wiresguard[.]com/update/v1, hxxps[:]//api[.]wiresguard[.]com/api/FileUpload/submit, hxxp[:]//124[.]222[.]137[.]114:9999/3yZR31VK, hxxp[:]//124[.]222[.]137[.]114:9999/api/updateStatus/v1
SHA1	8e6e505438c21f3d281e1cc257abdbf7223b7f5a, 90e677d7ff5844407b9c073e3b7e896e078e11cd, 573549869e84544e3ef253bdba79851dcde4963a, 13179c8f19fbf3d8473c49983a199e6cb4f318f0, 4c9aac447bf732acc97992290aa7a187b967ee2c, 821c0cafb2aab0f063ef7e313f64313fc81d46cd, 06a6a5a39193075734a32e0235bde0e979c27228, 9c3ba38890ed984a25abb6a094b5dbf052f22fa7, ca4b6fe0c69472cd3d63b212eb805b7f65710d33, 0d0f315fd8cf408a483f8e2dd1e69422629ed9fd, 2a476cfb85fbf012fdbe63a37642c11afa5cf020, d7ffd7b588880cf61b603346a3557e7cce648c93, 94dffa9de5b665dc51bc36e2693b8a3a0a4cc6b8, 21a942273c14e4b9d3faa58e4de1fd4d5014a1ed, 7e0790226ea461bcc9ecd4be3c315ace41e1c122, f7910d943a013eede24ac89d6388c1b98f8b3717, 73d9d0139eaf89b7df34ceeb60e5f8c7cd2463bf, bd4915b3597942d88f319740a9b803cc51585c4a, c68d09dd50e357fd3de17a70b7724f8949441d77, 813ace987a61af909c053607635489ee984534f4, 9fbf2195dee991b1e5a727fd51391dcc2d7a4b16, 07d2a01e1dc94d59d5ca3bdf0c7848553ae91a51, 3090ecf034337857f786084fb14e63354e271c5d, d0662eadbe5ba92acbd3485d8187112543bcfbf5, 9c0eff4deeb626730ad6a05c85eb138df48372ce
Domains	api[.]skycloudcenter[.]com, api[.]wiresguard[.]com
IPv4	95[.]179[.]213[.]0, 61[.]4[.]102[.]97, 59[.]110[.]7[.]32, 124[.]222[.]137[.]114
File Paths	%appdata%\ProShow\load, %appdata%\Adobe\Scripts\alien.ini, %appdata%\Bluetooth\BluetoothService

References

https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/

https://notepad-plus-plus.org/news/hijacked-incident-info-update/

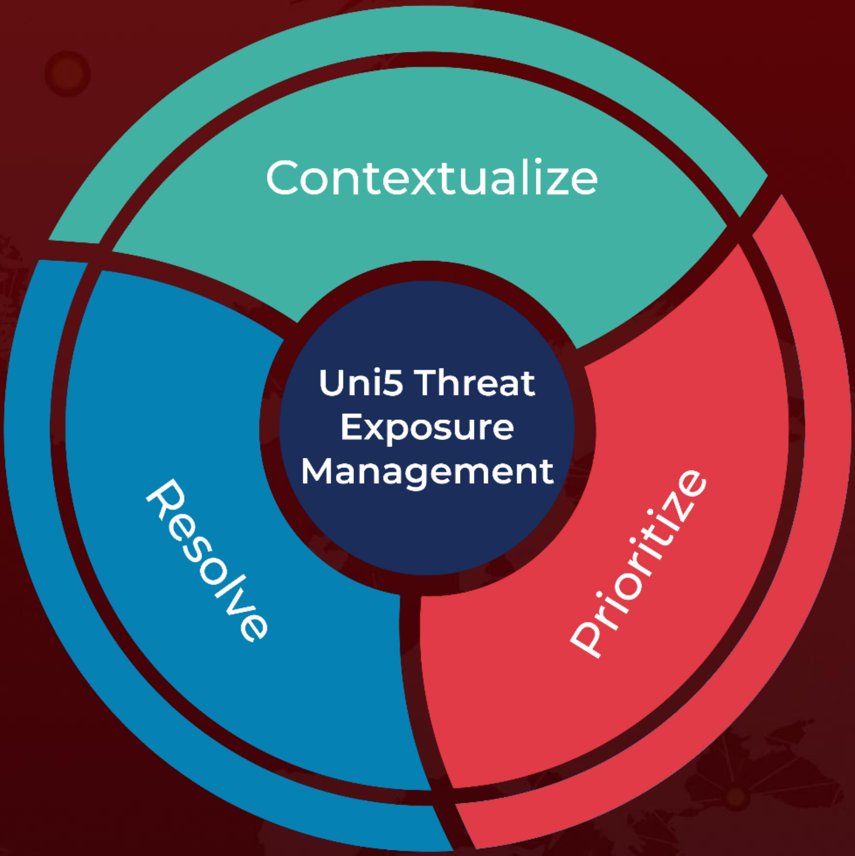
https://socradar.io/blog/notepad-infrastructure-hijacked/

https://securelist.com/notepad-supply-chain-attack/118708/

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

February 04, 2026 • 06:30 AM

More at www.hivepro.com