Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

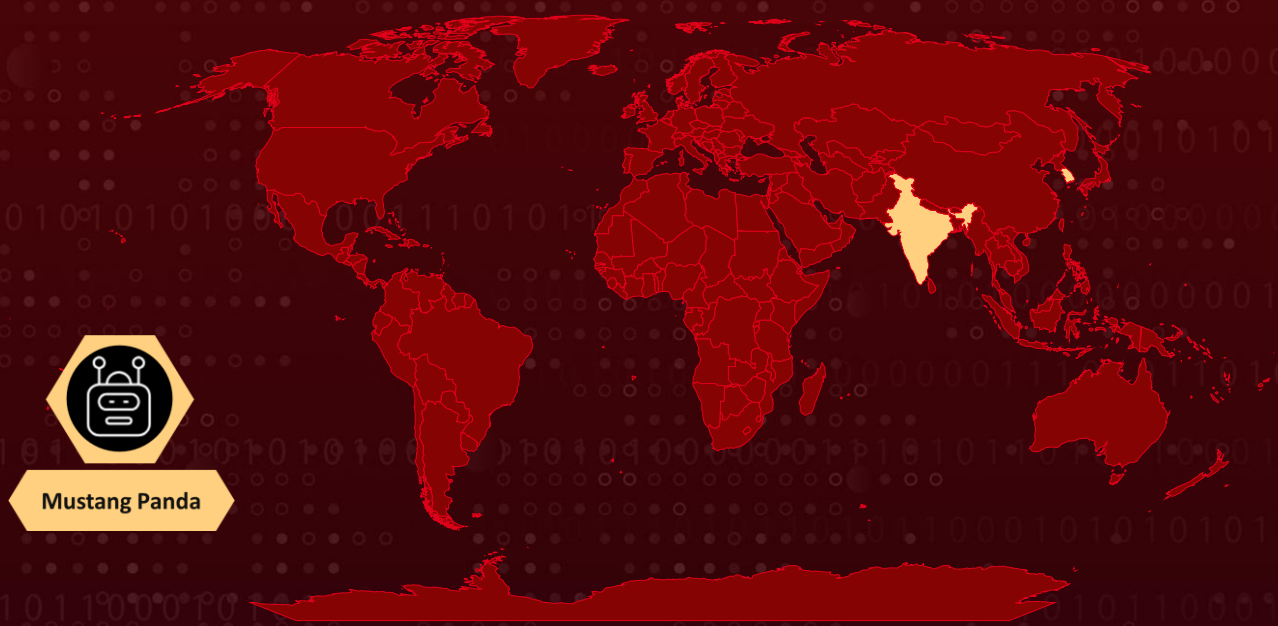
LOTUSLITE v1.1: Enhanced Evasion Meets Banking-Themed Social Engineering

Date of Publication	Admiralty Code	TA Number
April 23, 2026	A1	TA2026110

Summary

First Seen: March 2026
Targeted Regions: India, South Korea
Targeted Platforms: Windows
Targeted Industries: Banking and Financial Services, Government, Diplomatic, and Policy Organizations
Threat Actor: Mustang Panda (also tracked as Bronze President, Earth Preta, Stately Taurus, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, PKPLUG, Twill Typhoon, Hive0154) - attributed with medium confidence
Malware: LOTUSLITE backdoor (v1.1)
Attack: A newly evolved LOTUSLITE campaign is leveraging banking-themed social engineering to quietly infiltrate targeted systems, starting with a deceptively simple CHM file disguised as a support request. With a single click, the attack chain unfolds, triggering a hidden JavaScript loader that abuses trusted Windows components to deploy its payload. By sideloading a malicious DLL through a legitimate Microsoft-signed binary, the malware executes under the radar while employing advanced API resolution techniques to evade detection and analysis. Once established, it secures persistence, blends its network traffic with normal HTTPS communications, and enables full backdoor capabilities. The campaign's overlap with parallel operations targeting geopolitical policy experts highlights a broader, coordinated effort, underscoring LOTUSLITE's continued evolution into a stealthy and adaptable cyber espionage tool.

Attack Regions



Attack Details

#1

A newly observed campaign has introduced an updated variant of the LOTUSLITE malware, cleverly packaged around a theme tied to India's banking sector to enhance its credibility. The attack chain begins with a well-crafted spear-phishing email delivering a Compiled HTML Help (CHM) file titled "Request for Support.chm", a name deliberately chosen to mimic legitimate helpdesk or ticketing workflows commonly seen in financial institutions. Once opened, the file displays a seemingly benign prompt urging the user to click "Yes," but this interaction quietly triggers the download and execution of a malicious JavaScript payload, music.js, hosted on a remote domain. This script acts as the orchestrator of the infection, abusing trusted Windows utilities like hh.exe and leveraging ActiveX components such as ShortcutCommand, alongside Scriptlet.TypeLib, to bypass built-in security controls and initiate execution without raising suspicion.

#2

Once executed, the JavaScript extracts embedded payloads into a public directory on the system, including a legitimate Microsoft-signed binary (Microsoft_DNX.exe) and a malicious DLL (dnx.onecore.dll), which constitutes the LOTUSLITE v1.1 implant. The attackers exploit DLL sideloading by relying on the signed binary's behavior of dynamically loading libraries at runtime without strict path validation or authenticity checks. This allows the malicious DLL to execute under the guise of a trusted application. Notably, this variant introduces enhanced anti-analysis techniques, rather than statically importing APIs, it dynamically resolves them at runtime via ntdll.dll, using functions like LdrLoadDll and RtlInitUnicodeString. This approach minimizes detectable indicators in the import table, significantly complicating static analysis and reverse engineering efforts.

#3

To maintain persistence, the malware modifies the Windows Registry under the HKCU Run key, again using obfuscated API resolution techniques to evade detection. It copies itself into C:\ProgramData\Microsoft_DNX* and leverages a modified command-line argument to control execution flow, either establishing persistence or initiating communication with its command-and-control (C2) server. A mutex named "mdseccoUk" ensures only a single instance runs at a time. The DLL's export table has also been expanded to include functions such as HDFCBankMain, which displays a decoy message box referencing "HDFC Bank Limited" to reinforce the banking-themed disguise. Meanwhile, legacy artifacts such as KugouMain persist, providing strong evidence of lineage from earlier LOTUSLITE versions.

#4 On the network side, the implant communicates with a hardcoded C2 endpoint hosted on a dynamic DNS subdomain, using TCP port 443 to blend seamlessly with normal HTTPS traffic. The communication protocol relies on a custom binary TLV structure, updated with a new magic header value, signaling iterative development. Functionally, the backdoor retains its core capabilities, including remote shell access, file manipulation, and session control, mirroring the command structure of earlier versions.

#5 Further investigation reveals that this activity is not isolated. A actor is also targeting policy experts and individuals engaged in Korean Peninsula and Indo-Pacific security discussions. In this case, threat actors employed a spoofed Gmail account impersonating a well-known U.S.-Korea policy figure to distribute malicious files via Google Drive. This overlap in targeting and tooling suggests a broader, coordinated effort, with LOTUSLITE continuing to evolve both technically and operationally to support targeted cyber espionage campaigns. With moderate confidence, this activity is attributed to Mustang Panda based on shared code lineage, overlapping infrastructure, residual build artifacts and consistent behavioral patterns observed across all three campaigns.

Recommendations

Block Known C2 Infrastructure: Immediately block network communication to the domains editor[.]gleeze[.]com and www[.]cosmosmusic[.]com at the firewall, proxy, and DNS levels. Add the associated IoC hashes to endpoint detection blocklists to prevent execution of known LOTUSLITE v1.1 artifacts.

Restrict CHM File Execution: Deploy Group Policy restrictions to prevent the execution of Compiled HTML (.chm) files from untrusted sources, particularly those arriving via email attachments or web downloads. Monitor for unexpected invocations of hh.exe, which is abused in this campaign as a file extraction mechanism.

Harden DLL Sideloading Defenses: Implement application control policies that prevent unsigned or untrusted DLLs from being loaded alongside legitimate signed executables. Monitor for the execution of Microsoft_DNX.exe and kwpswnsserver.exe outside of expected development contexts, as these legitimate binaries are abused for sideloading in this campaign.

Monitor Registry Persistence Mechanisms: Deploy detection rules for registry modifications under HKCU\Software\Microsoft\Windows\CurrentVersion\Run, specifically watching for entries pointing to executables staged in C:\ProgramData\ subdirectories. Alert on the creation of the mutexes "mdseccoUkFuiCkTrump" and "1ac5e7ee1a107499" as direct indicators of LOTUSLITE activity.

Deploy Network Detection Signatures: Create network intrusion detection rules to identify the LOTUSLITE custom binary packet structure, specifically monitoring for the magic value 0xB2EBCFDF in packet headers on TCP port 443. Also retain detection for the legacy magic value 0x8899AABB from v1.0 to ensure coverage across both variants.

Implement JavaScript Execution Controls: Restrict the execution of JavaScript files (.js) via Windows Script Host in environments where such functionality is not operationally required. Monitor for the creation and execution of JavaScript files in user-writable directories, particularly those triggered by CHM file interactions.

Implement Network Segmentation for Financial Systems: Isolate banking and financial application servers from general-purpose endpoints to limit lateral movement opportunities if a LOTUSLITE implant achieves initial compromise. Ensure that sensitive financial systems are accessible only through hardened jump servers with multi-factor authentication.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spear-Phishing Attachment
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
	T1218: System Binary Proxy Execution	T1218.001: Compiled HTML File
	T1204: User Execution	
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1106: Native API	
	T1027: Obfuscated Files or Information	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1095: Non-Application Layer Protocol	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	af31ebe9085df408bedcf8f027fb60389897e5c8d3b0e9695fea29774f9d3aec, cc0ff7e25ea686171919575916e2d9ebaeb5800a063f370a6980ea791f8851b8, 7beede15ecdc7d3f01db4b699e5fe5f4f2e7c79cd7ef0e918ed0583bf621de7d, 9bf2f3b15a621789f898f9bd7710ba857e3f238a4937b64fdc47ef9a92e0b05d, 18bc0e0f627d90fb283aa243055b46d0bfb5d85a7240d8f63ec2d1c8a2c15893, 6d22d50634c2c2fc853bfd2b564e1837d51087aa684a9c4415634c8c13c44135
Domains	editor[.]gleeze[.]com, www[.]cosmosmusic[.]com
Mutex	mdseccoUkFuiCkTrump, 1ac5e7ee1a107499
File Path	C:\ProgramData\Microsoft_DNX\

References

https://www.acronis.com/en/tru/posts/same-packet-different-magic-mustang-panda-hits-indias-banking-sector-and-korea-geopolitics/

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 Demo of **HivePro**.

REPORT GENERATED ON

April 23, 2026 • 8:30 AM

More at www.hivepro.com