

Mustang Panda Strikes India and South Korea with Updated LOTUSLITE Backdoor in Espionage Campaign

By Secure Blink

Archived: 2026-05-22 02:01:34 UTC



Mustang Panda



China-linked Mustang Panda targets India banks & S.Korea policy via LOTUSLITE backdoor

22-Apr-2026

4 min read

A China-linked threat group known as Mustang Panda has launched a dual-faced espionage campaign targeting India's banking sector and South Korea's policy circles, according to new research from the Acronis Threat Research Unit (TRU).

The group is deploying an updated version of the LOTUSLITE backdoor (v1.1) that uses legitimate Microsoft-signed executables to bypass security checks and gain persistent access to victim systems.

The campaign, first observed in March 2026, represents a significant geographic and sectoral shift for Mustang Panda. The group has previously focused on U.S. government entities using geopolitical lures tied to Venezuela, but has now expanded its reach to India's financial sector and South Korean diplomatic circles.

HDFC Bank-Themed Lures

In India, the attackers used a malicious CHM (Compiled HTML) file named **Request for Support.chm** to trick employees in the banking sector. The file contained a pop-up window that mentioned **HDFC Bank Limited** to appear legitimate.

When a user clicked the file, it triggered a chain of events that downloaded a malicious JavaScript payload called **music.js** from the domain `cosmosmusic[.]com`.

The malware also created fake pop-up windows designed to look like real [HDFC Bank](#) software.

While victims believed they were interacting with a banking app, the LOTUSLITE backdoor was silently establishing a foothold on their systems.

South Korean Policy Circles: Impersonating a Diplomatic Figure

In the second prong of the campaign, Mustang Panda impersonated **Victor Cha**, a former Director for Asian Affairs at the U.S. National Security Council. Using a fake Gmail account (victorcha707@gmail.com) featuring Mr. Cha's real photo, the group sent Google Drive links to folders named "March 30." Inside were fake invitation letters crafted to infect the computers of policy-makers.

"What stands out is the broadening of the group's targeting, from U.S. government entities with geopolitical lures, to India's banking sector through implants embedded with HDFC Bank references, and now to South Korean and U.S. policy circles through the impersonation of a prominent figure in Korean peninsula diplomacy," the Acronis researchers noted.

LOTUSLITE v1.1

The updated LOTUSLITE variant introduces several incremental improvements designed to evade detection while maintaining its core espionage functions:

- **Changed magic packet value:** The internal code marker used to identify network traffic has been rotated from **0x8899AABB** to **0xB2EBCFDF**.
- **New command flag:** The old flag `--DATA` has been replaced with a new one, `--ZoneMAX`.
- **Runtime API resolution:** The malware now resolves APIs through `ntdll.dll` chains, making static analysis more difficult.

Despite these updates, the backdoor retains residual code names from older versions, including **KugouMain** and **DataImporterMain** — a clear sign that the same developer continues to maintain the tool.

DLL Sideloaded Abusing Trusted Binaries

The infection chain relies on a technique called **DLL sideloading**. The attackers take a legitimate file signed by Microsoft — such as **Microsoft_DNX.exe** — and place their own malicious DLL right next to it. The computer trusts the Microsoft signature, allowing the infected file to execute without raising suspicion.

“The backdoor communicates with a dynamic DNS-based command-and-control server over HTTPS and supports remote shell access, file operations and session management, indicating a continued espionage-focused capability set rather than financially motivated objectives,” said [Acronis](#) researchers Subhajeet Singha and Santiago Pontiroli.

Infrastructure Reuse Attribution

The attackers used a service called **Gleeze** to communicate with their command-and-control server at `editor[.]gleeze[.]com`. This is the same infrastructure observed in previous Mustang Panda attacks, helping researchers link the new activity to the group.

The Acronis Threat Research Unit assessed attribution to Mustang Panda with **moderate confidence**, based on:

- Shared code lineage and identical command structures
- Overlapping infrastructure (Dynu Systems dynamic DNS provider)
- Consistent operational patterns and OPSEC mistakes

In a notable touch, the threat actor even left a message in the code mentioning a security researcher who has been tracking them — a recurring habit of leaving identity markers in their implants.

The campaign underscores how Mustang Panda continues to refine well-tested techniques while broadening its targeting to financial and diplomatic sectors across multiple geopolitical regions.

While the malware does not appear focused on immediate financial theft, it aligns with espionage-driven objectives — long-term access, surveillance, and data exfiltration.

Researchers emphasize the importance of staying skeptical of unexpected emails or files, even if they appear official. The group’s constant upgrading of impersonation tactics and use of trusted software to lure users makes vigilance essential.

Source: <https://www.secureblink.com/cyber-security-news/mustang-panda-strikes-india-and-south-korea-with-updated-lotuslite-backdoor-in-espionage-campaign>