INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 13:40 UTC

Mustang Panda Deploys Updated LOTUSLITE Backdoor Against Asia-Pacific Financial and Diplomatic Targets

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0202
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	No specific CVEs identified; targets include Indian banking sector (HDFC Bank branding used as lure) and South Korean diplomatic organizations; attack chain involves CHM file delivery, DLL side-loading via dnx.onecore.dll, and dynamic DNS C2 (editor.gleeze[.]com)
Published	2026-04-22T03:58:00
Discovery Source	Rss

Executive Summary

Mustang Panda, a Chinese state-sponsored espionage group, has deployed an updated backdoor called LOTUSLITE against financial institutions and diplomatic organizations across India and South Korea. The campaign uses HDFC Bank branding as a social engineering lure, indicating deliberate targeting of personnel with access to sensitive financial and policy information. Organizations in Indo-Pacific finance and government sectors face elevated risk of persistent, undetected access to confidential systems and communications.

Technical Analysis

Mustang Panda (also tracked as TA416, RedDelta, Bronze President) has updated its LOTUSLITE backdoor for a campaign targeting Indian banking sector employees and South Korean diplomatic personnel. Initial access is achieved via spearphishing attachments (T1566.001) using CHM (Compiled HTML Help) files with HDFC Bank branding as lure content. Post-execution, the malware performs DLL side-loading through dnx.onecore.dll (T1574.002), abusing a trusted binary to load malicious code, mapped to CWE-426 (Untrusted Search Path) and CWE-494 (Download of Code Without Integrity Check). JavaScript execution within the CHM context is facilitated via T1218.001 (System Binary Proxy Execution: Compiled HTML File) and T1059.007. Command-and-control uses dynamic DNS infrastructure (editor.gleeze[.]com) via T1568.001 and T1583.001, enabling the actor to rotate infrastructure and evade static blocklist defenses. C2 communication occurs over

standard web protocols (T1071.001, T1071.004) with exfiltration via T1041. No CVEs are associated with this campaign; exploitation relies entirely on social engineering, trusted binary abuse, and dynamic infrastructure. No vendor patch is applicable; mitigation is detection and configuration-based. Technical claims should be validated against primary threat intelligence feeds before operationalizing IOCs.

Action Checklist

1. Containment: Block the known C2 domain editor.gleeze[.]com and its resolved IPs at perimeter firewalls, DNS resolvers, and proxy infrastructure. Isolate any endpoint that has initiated DNS queries or HTTP/S connections to this domain. Apply blocking to the broader gleeze[.]com dynamic DNS namespace as a precaution.
2. Detection: Hunt for CHM file execution events in endpoint telemetry (Event ID 4688 or Sysmon Event ID 1, process: hh.exe). Search EDR and SIEM for dnx.onecore.dll loaded by non-standard parent processes. Query DNS logs for queries to editor.gleeze[.]com and wildcard subdomains of gleeze[.]com. Flag outbound connections from hh.exe or unusual child processes spawned by it.
3. Eradication: Remove CHM-based email attachments at the mail gateway; configure email security controls to strip or quarantine .chm file types. Restrict execution of hh.exe via application control policy (e.g., Windows Defender Application Control or AppLocker) where it is not operationally required. Audit DLL search order configurations on endpoints to reduce side-loading exposure per CWE-426 guidance.
4. Recovery: Re-image any confirmed compromised endpoints. Rotate credentials for accounts that touched affected systems. Validate DNS sinkholing or blocking of gleeze[.]com is confirmed active across all egress paths. Monitor previously affected endpoints for re-infection indicators for a minimum of 30 days post-remediation.
5. Post-Incident: Review CHM file handling policies and email attachment filtering rules; this campaign exposed a gap if .chm files were permitted through mail gateways. Assess whether DLL side-loading prevention controls are deployed consistently across the endpoint fleet. Map detection coverage against T1574.002, T1218.001, and T1568.001 in your SIEM or EDR to identify and close visibility gaps.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and relevant financial sector regulatory contacts if any confirmed compromised endpoint belongs to a user with access to wire transfer systems, SWIFT infrastructure, customer PII, or diplomatic communications — the HDFC Bank lure targeting and Mustang Panda's established espionage mandate indicate likely intent to exfiltrate sensitive financial or policy data, triggering potential RBI breach notification obligations in India, FSS notification requirements in South Korea, and GDPR Article 33 obligations if EU citizen data is involved.

Recovery Notes	Re-imaged endpoints should be rebuilt from a known-good baseline image predating the campaign's earliest confirmed delivery date; validate image integrity using SHA256 hash against the golden image repository before deployment. Post-recovery, maintain elevated logging verbosity (Sysmon Event IDs 1, 3, 7, 22 at minimum) on all rebuilt hosts and any hosts that accessed the same network segments as compromised systems for a minimum of 30 days, alerting on any recurrence of hh.exe execution, unsigned DLL loads from user-writable paths, or DNS queries to gleeze.com or newly registered dynamic DNS providers. Given Mustang Panda's pattern of re-targeting previously compromised organizations with updated tooling, subscribe affected sector organizations to CISA advisories and FS-ISAC threat feeds and re-run the full IOC hunt at 30-day and 90-day intervals.
Forensic Artifacts	Malicious dnx.onecore.dll dropped in a user-writable or application directory (not %SystemRoot%\System32\) — collect full path, SHA256 hash, PE metadata, and code-signing certificate details; absence of a valid Microsoft signature is definitive evidence of side-loading abuse (T1574.002) | CHM lure file and its unpacked artifacts in %TEMP%\hh\ — the unpacked directory contains the HTML/JavaScript dropper logic and may include embedded executables or encoded LOTUSLITE staging payloads; preserve directory structure and file timestamps intact before antivirus remediation destroys them | Sysmon Event ID 22 (DNS Query) records for *.gleeze.com queries — timestamp, querying process PID/name, and returned IP address establish the C2 communication timeline and confirm which processes initiated beacon activity, directly attributing LOTUSLITE callback behavior to the side-loaded DLL | Windows Prefetch files for hh.exe (%SystemRoot%\Prefetch\HH.EXE-.pf) — prefetch records the last 8 execution times and up to 128 files referenced during execution, allowing reconstruction of which .chm file was opened and what files were accessed during the LOTUSLITE staging process even after the original files are deleted | Scheduled task XML definitions (%SystemRoot%\System32\Tasks\ or exported via schtasks /query /xml) and HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry keys — LOTUSLITE establishes persistence via one or both mechanisms during the CHM execution phase; task definitions will reference the side-loaded DLL or a dropped executable with a plausible system-sounding name

Per-Action IR Details

Containment — Block the known C2 domain editor.gleeze[.]com and its resolved IPs at perimeter firewalls, DNS resolvers, and proxy infrastructure. Isolate any endpoint that has initiated DNS queries or HTTP/S connections to this domain. Apply blocking to the broader gleeze[.]com dynamic DNS namespace as a precaution.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-4 (System Monitoring), CIS 13.7 (Deploy a Host-Based Intrusion Detection Solution)

Compensating: On Windows DNS servers, run: Get-DnsServerQueryResolutionPolicy to check for existing blocks, then Add-DnsServerQueryResolutionPolicy -Name 'BlockGleeze' -Action DENY -Fqdn 'eq,*.gleeze.com' to sinkhole the entire dynamic DNS namespace. On Linux resolvers using BIND, add 'zone gleeze.com { type redirect; masters { 127.0.0.1; }; };' to named.conf. Use PowerShell to pull DNS query logs: Get-WinEvent -LogName 'DNS Server' \| Where-Object { $_.Message -match 'gleeze' } to identify endpoints that have already beaconed. For host-level blocking without a proxy, push a Windows Firewall rule via GPO: netsh advfirewall firewall add rule name='Block LOTUSLITE C2' dir=out action=block remoteip=.

Evidence: Before isolating any endpoint, capture: (1) Full DNS resolver cache (ipconfig /displaydns > dns_cache_HOSTNAME_DATE.txt) to record the resolved IP of editor.gleeze[.]com at time of incident. (2) Active

network connections (netstat -ano > netstat_HOSTNAME_DATE.txt) to identify established or TIME_WAIT sessions to C2 IPs. (3) Windows DNS Server debug logs (%SystemRoot%\System32\dns\dns.log) or Sysmon Event ID 22 (DNS Query) filtering on 'gleeze' for historical beacon timing. (4) Firewall session logs showing outbound HTTP/S from hh.exe or the side-loaded dnx.onecore.dll process PID to C2 infrastructure. (5) Preserve memory image of any process holding an active C2 connection before isolating — LOTUSLITE's updated variant may store C2 configuration and staging payloads only in memory.

Detection — Hunt for CHM file execution events in endpoint telemetry (Event ID 4688 or Sysmon Event ID 1, process: hh.exe). Search EDR and SIEM for dnx.onecore.dll loaded by non-standard parent processes. Query DNS logs for queries to editor.gleeze[.]com and wildcard subdomains of gleeze[.]com. Flag outbound connections from hh.exe or unusual child processes spawned by it.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 13.6 (Collect Network Traffic Flow Logs)

Compensating: Without SIEM/EDR, deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config) and run these targeted PowerShell queries on each host: (1) Hunt hh.exe execution: Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'hh\.exe'} | Select-Object TimeCreated,Message | Export-Csv hh_executions.csv. (2) Hunt dnx.onecore.dll side-loading: Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 7 -and $_.Message -match 'dnx.onecore.dll'} | Select-Object TimeCreated,Message. (3) Hunt DNS queries: if DNS debug logging is enabled, run: Select-String -Path C:\Windows\System32\dns\dns.log -Pattern 'gleeze' -List. Use the Sigma rule 'proc_creation_win_hh_chm_execution' (SigmaHQ detection-rules repository) converted to a Windows Event Log query as a baseline detection. Use osquery: SELECT name,path,pid,parent FROM processes WHERE name='hh.exe'; to identify active instances.

Evidence: Before pivoting on detection findings: (1) Collect Sysmon Event ID 1 (Process Create) records for hh.exe, including full command-line showing the .chm file path and parent process (likely Outlook.exe, winword.exe, or a browser — consistent with HDFC Bank lure delivery). (2) Collect Sysmon Event ID 7 (Image Load) records for dnx.onecore.dll, recording the loading process name and full image path — legitimate dnx.onecore.dll should reside in %SystemRoot%\System32\; a path in a user-writable directory is definitive evidence of side-loading. (3) Preserve the original .chm lure file from %TEMP%, %APPDATA%, or Downloads — CHM files unpack to %TEMP%\hh\; recover these unpacked HTML/JS/script components as they contain the dropper logic. (4) Extract Sysmon Event ID 3 (Network Connect) from hh.exe or its child processes to document initial C2 contact. (5) Collect Event ID 4688 child process tree under hh.exe — LOTUSLITE campaigns frequently spawn cmd.exe or PowerShell for persistence staging immediately after CHM execution.

Eradication — Remove CHM-based email attachments at the mail gateway; configure email security controls to strip or quarantine .chm file types. Restrict execution of hh.exe via application control policy (e.g., Windows Defender Application Control or AppLocker) where it is not operationally required. Audit DLL search order configurations on endpoints to reduce side-loading exposure per CWE-426 guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), NIST CM-6 (Configuration Settings), CIS 2.5 (Allowlist Authorized Software), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 9.6 (Block Unnecessary File Types)

Compensating: For teams without commercial mail gateway controls: (1) In Exchange Online/on-prem, add a transport rule: New-TransportRule -Name 'Block CHM Attachments' -AttachmentExtensionMatchesWords 'chm' -DeleteMessage $true -StopRuleProcessing $true. (2) For AppLocker on Windows 10/11 Pro without Intune — deploy via GPO: Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Executable Rules; add a Deny rule for %SYSTEMROOT%\System32\hh.exe for all users except a defined exception

group. (3) To audit DLL search order exposure for dnx.onecore.dll specifically, run on each endpoint: where.exe dnx.onecore.dll — any result outside %SystemRoot%\System32\ indicates a hijackable path. Use Sysinternals Process Monitor with a boot-time capture filter on 'PATH NOT FOUND' + 'dll' to map all DLL search order gaps across the system.

Evidence: Before eradicating components: (1) Hash and preserve any identified .chm lure file (Get-FileHash -Algorithm SHA256) and submit to VirusTotal or an internal sandbox for dynamic analysis — the unpacked CHM may reveal additional payload staging URLs or embedded executables beyond the known LOTUSLITE binary. (2) Export the full DLL load history for the side-loaded dnx.onecore.dll process from Sysmon Event ID 7, capturing ImageLoaded path, SHA256 hash, and signing status — the malicious dnx.onecore.dll will be unsigned or signed with an anomalous certificate. (3) Collect scheduled tasks (schtasks /query /fo LIST /v > scheduled_tasks.txt) and run keys (reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run run_keys.txt) before removal — LOTUSLITE variants establish persistence via scheduled tasks or run keys written during the CHM execution phase. (4) Pull AppLocker or WDAC audit logs (Event IDs 8003/8004 in Microsoft-Windows-AppLocker/EXE and DLL channel) to identify all systems where hh.exe executed without policy enforcement.

Recovery — Re-image any confirmed compromised endpoints. Rotate credentials for accounts that touched affected systems. Validate DNS sinkholing or blocking of gleeze[.]com is confirmed active across all egress paths. Monitor previously affected endpoints for re-infection indicators for a minimum of 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without automated credential rotation tooling: (1) Force immediate password reset for all accounts with interactive logon to compromised systems using: Get-ADUser -Filter {LastLogonDate -gt (Get-Date).AddDays(-90)} | Set-ADAccountPassword -Reset — then scope to accounts with EventID 4624 (Logon) on compromised hosts in the 60-day lookback window. (2) Verify DNS blocking completeness by running nslookup editor.gleeze.com from a controlled test host — any non-sinkhole response indicates a resolver gap. (3) Post-re-image, deploy a Sysmon + YARA scanning cron using ClamAV with a custom LOTUSLITE signature (based on preserved malicious dnx.onecore.dll SHA256 and known LOTUSLITE string artifacts) to run nightly: clamscan -r --max-filesize=50M --include='*.dll' C:\ -l lotuslite_scan.log. (4) For the 30-day monitoring window, run daily osquery scheduled queries targeting hh.exe process creation and unsigned DLL loads from user-writable paths.

Evidence: Before re-imaging: (1) Acquire a full forensic disk image (using FTK Imager Lite or dc3dd) and memory image (using WinPmem) of each confirmed compromised host — LOTUSLITE's updated features may include novel persistence or data staging mechanisms not yet fully documented, and these images are required for retrospective analysis. (2) Export the full Security event log (wevtutil epl Security C:\IR\Security_HOSTNAME_DATE.evtx), Sysmon operational log, and PowerShell ScriptBlock log (Event ID 4104) before wiping. (3) Document all accounts that authenticated to compromised systems via Event ID 4624/4648 in the 90-day lookback — this scopes the credential rotation requirement and identifies potential lateral movement targets. (4) Capture the contents of %APPDATA%, %TEMP%, and all user profile Startup folders as LOTUSLITE may stage secondary payloads or exfiltration queues in these locations.

Post-Incident — Review CHM file handling policies and email attachment filtering rules; this campaign exposed a gap if .chm files were permitted through mail gateways. Assess whether DLL side-loading prevention controls are deployed consistently across the endpoint fleet. Map detection coverage against T1574.002, T1218.001, and T1568.001 in your SIEM or EDR to identify and close visibility gaps.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST RA-3 (Risk Assessment), CIS 7.1

(Establish and Maintain a Vulnerability Management Process), CIS 17.6 (Train Workforce Members on Identifying Social Engineering Attacks)

Compensating: For teams mapping ATT&CK coverage without a commercial SIEM: (1) Use the free ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to mark T1574.002 (DLL Side-Loading), T1218.001 (Compiled HTML File), and T1568.001 (Fast Flux DNS) — overlay your current Sysmon + Windows Event Log detection capability to visualize gaps. (2) Pull community Sigma rules for all three techniques from the SigmaHQ repository and convert to Windows Event Log XML queries using sigmac or pySigma for no-cost deployment. (3) Conduct a targeted tabletop exercise simulating a Mustang Panda-style CHM lure delivery to HDFC Bank-branded email targets — use this campaign's actual TTPs (CHM delivery, dnx.onecore.dll side-load, gleeze.com dynamic DNS) as the scenario to validate your updated playbook. (4) Document lessons learned using the NIST 800-61r3 §4 after-action template and share relevant IOCs (gleeze.com namespace, dnx.onecore.dll hashes, CHM file hashes) with sector ISACs (FS-ISAC for financial, relevant government CERTs for diplomatic sector peers).

Evidence: For the post-incident review: (1) Compile a complete IOC report from the incident — all observed gleeze.com subdomains with resolved IPs and first-seen timestamps, SHA256 hashes of the CHM lure file and malicious dnx.onecore.dll, and any additional payloads staged by LOTUSLITE — to build a Mustang Panda campaign-specific threat intelligence profile. (2) Pull email gateway logs for the 90 days prior to detection to identify all .chm file delivery attempts — including blocked ones — to determine whether earlier campaign waves were missed and to reconstruct the full targeting scope against HDFC Bank-branded lures. (3) Extract the full process execution timeline from preserved Sysmon logs across all affected hosts to reconstruct dwell time and map all lateral movement or data access that occurred between initial compromise and containment — this determines whether a breach notification obligation exists under applicable financial sector regulations.

Detection Guidance

Primary detection targets: (1) Process execution, hunt for hh.exe (Microsoft HTML Help executable) spawning child processes, particularly JavaScript interpreters or network-connected processes; log source: Sysmon Event ID 1 or Windows Security Event ID 4688 with command-line logging enabled. (2) DLL side-loading, search for dnx.onecore.dll loaded from non-standard paths or by unexpected parent processes; log source: Sysmon Event ID 7 (ImageLoad) with DLL load monitoring enabled. (3) DNS telemetry, query DNS logs for resolutions of editor.gleeze[.]com or any subdomain of gleeze[.]com; flag endpoints generating these queries for immediate investigation. (4) Network traffic, alert on outbound HTTP/S connections initiated by hh.exe or processes spawned from CHM file execution contexts; log source: proxy logs, firewall flow data, EDR network telemetry. (5) Email gateway, flag inbound emails containing .chm attachments, particularly those using financial institution branding (HDFC Bank); log source: mail gateway attachment-type telemetry. MITRE ATT&CK coverage check: verify your detection stack has rules mapped to T1218.001, T1574.002, and T1568.001.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`editor.gleeze[.]com`	Dynamic DNS C2 domain used by LOTUSLITE backdoor for command-and-control communications (T1568.001, T1583.001)	MEDIUM
DOMAIN	`gleeze[.]com`	Parent dynamic DNS provider namespace; broader blocking recommended given actor use of subdomains for C2 rotation	MEDIUM

Type	Value	Context	Confidence
URL	`hh.exe spawning child process`	Behavioral IOC — CHM file execution via Microsoft HTML Help executable (T1218.001); flag any hh.exe child process in endpoint telemetry	MEDIUM
URL	`dnx.onecore.dll loaded from non-standard path`	Behavioral IOC — DLL side-loading technique (T1574.002, CWE-426); flag unexpected load events for this DLL	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1566.001** — Spearphishing Attachment
- **T1071.001** — Web Protocols
- **T1071.004** — DNS
- **T1568.001** — Fast Flux DNS
- **T1583.001** — Domains
- **T1105** — Ingress Tool Transfer
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1041** — Exfiltration Over C2 Channel
- **T1059.007** — JavaScript
- **T1218.001** — Compiled HTML File
- **T1574.002** — DLL Side-Loading

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T1071.004	DNS	Command-And-Control
T1568.001	Fast Flux DNS	Command-And-Control
T1583.001	Domains	Resource-Development
T1105	Ingress Tool Transfer	Command-And-Control
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059.007	JavaScript	Execution
T1218.001	Compiled HTML File	Defense-Evasion
T1574.002	DLL Side-Loading	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/mustang-pandas-new-lotuslite-vari...	T3
HDFC Bank Security Rating, Vendor Risk Report, and Data Breaches	https://www.upguard.com/security-report/hdfc-bank	T3
Threat Actors Abusing Chrome DLL Side-Loading Vulnerability for ...	https://rewterz.com/threat-advisory/threat-actors-abusing-chrome-dl...	T3
In-Depth Analysis of July 2023 Exploit Chain Featuring CVE-2023 ...	https://unit42.paloaltonetworks.com/new-cve-2023-36584-discovered-i...	T3

Source	URL	Tier
ThreatsDay Bulletin: PQC Push, AI Vuln Hunting, Pirated Traps ...	https://thehackernews.com/2026/03/threatsday-bulletin-pqc-push-ai-v...	T3

Generated 2026-04-22 13:40 UTC by TJS Security Command Center