INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:12 UTC

Operation DragonReturn: China-Aligned Actors Target Indian Tax Season with DcRAT via DLL Sideloading and Steganography

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0624
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows systems; Indian Income Tax e-filing utility (spoofed); NVDA nvdaHelperRemote.dll (DLL sideloading vector); Windows Media Player directory (abused for payload staging); LINE installer (spoofed, ValleyRAT parallel campaign)
Published	2026-07-06T06:58:16
Discovery Source	Rss

Executive Summary

A suspected China-aligned threat cluster is running a targeted spear-phishing campaign, dubbed Operation DragonReturn, timed to India's income tax filing season. The campaign impersonates India's Income Tax Department using bilingual legal-themed lures to deliver DcRAT remote access malware through DLL sideloading and steganography-concealed payloads, targeting Indian taxpayers, tax professionals, and corporate finance teams. If successful, attackers gain full remote access to compromised Windows systems, enabling data theft, credential harvesting, and persistent access to sensitive financial and organizational data.

Technical Analysis

Operation DragonReturn is a spear-phishing campaign attributed with moderate confidence to a China-nexus threat cluster overlapping with the Silver Fox actor. Lures impersonate India's Income Tax Department with bilingual Hindi/English content and authentic legal citations to increase credibility. The delivery mechanism abuses DLL sideloading via legitimate signed binaries, specifically via a spoofed NVDA (NonVisual Desktop Access) helper binary, nvdaHelperRemote.dll, to load DcRAT (a .NET-based remote access trojan). Payloads are staged in the Windows Media Player directory and concealed via steganography (MITRE T1027.003), complicating static detection. The attack chain maps to: T1566.001 (spear-phishing attachment), T1574.002 (DLL side-loading), T1036.005 (masquerading as legitimate NVDA binary), T1027.003 (steganography), T1059

(command execution), T1055 (process injection), T1543.003 (Windows service persistence), T1113 (screen capture), T1041 (C2 exfiltration over application layer), T1071.001 (C2 over HTTP/S), T1562.001 (defense evasion via security tool impairment), and T1548.002 (UAC bypass). No CVE is associated; the campaign abuses legitimate signed binary behavior rather than disclosed software vulnerabilities. Relevant weaknesses: CWE-829 (inclusion of functionality from untrusted control sphere), CWE-506 (embedded malicious code), CWE-494 (download of code without integrity check). Infrastructure overlaps with parallel ValleyRAT campaigns spoofing LINE installers and targeting job seekers via Foxit PDF reader DLL sideloading, per Trend Micro research. Source quality is moderate (score 0.64); primary reporting is from The Hacker News (T2) corroborated by Trend Micro research (T1) on the parallel ValleyRAT campaign. Attribution to Silver Fox and direct linkage between DragonReturn and ValleyRAT infrastructure is reported by The Hacker News and has not been independently corroborated by a second T1 source as of analysis time.

Action Checklist

1. Step 1: Containment, Block execution of unsigned or anomalously placed DLLs in Windows Media Player directories and NVDA installation paths via application control policy (NIST CM-7, CIS 2.1). Alert on or block processes spawning from nvdaHelperRemote.dll outside of a verified, inventory-listed NVDA installation (CIS 1.1). Quarantine any endpoint that received Income Tax Department-themed email attachments during the filing season window.
2. Step 2: Detection, Query email gateway logs for lures referencing Indian Income Tax e-filing utilities, ITR forms, or Income Tax Department sender domains (AU-2, AU-6). Hunt for DLL loads of nvdaHelperRemote.dll from non-standard parent processes or paths outside Program Files. Search EDR telemetry for processes writing to or executing from %ProgramFiles%\Windows Media Player with non-media-player parent processes. Review for steganographic payload delivery: look for image files written to staging directories immediately before DLL load events (T1027.003 behavioral indicator). Pivot on known Silver Fox infrastructure IOCs if available from your threat intel feeds.
3. Step 3: Eradication, Remove any identified DcRAT implants and associated DLL sideload chains. Purge staged payloads from Windows Media Player directories. Revoke and rotate credentials for any accounts active on confirmed-compromised hosts (D3-CRO). Audit all NVDA installations against your software inventory (CIS 2.1) and remove unauthorized copies. Block delivery domains and file hashes associated with this campaign at the email gateway and endpoint.
4. Step 4: Recovery, Re-image confirmed-compromised endpoints before restoring to production. Validate restored systems against your secure configuration baseline (CIS 4.6). Monitor post-recovery for re-infection indicators: DLL anomalies in Windows Media Player paths, unexpected NVDA process activity, and outbound C2 patterns matching DcRAT (HTTP/S beaconing, T1071.001). Confirm audit logging is intact and alert rules for DLL sideloading are active (AU-12, CIS 8.2).
5. Step 5: Post-Incident, Review email security controls for spoofed government-sender detection; impersonation of tax authorities is a recurring lure class. Assess DLL sideloading exposure across your software inventory, identify other signed binaries susceptible to search-order hijacking (CIS 2.1, NIST CM-7, D3-CH). Evaluate whether user awareness training covers seasonal tax-themed lures, particularly for finance and accounting teams. Document control gaps against NIST AC-6 (least privilege for process execution) and CIS 7.1 (vulnerability management process) to inform next planning cycle.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if DcRAT keystroke logs, clipboard data, or file exfiltration artifacts confirm that taxpayer PII, corporate financial records, or ITR filing credentials were accessed or transmitted to Silver Fox C2 infrastructure, as this may trigger breach notification obligations under India's Digital Personal Data Protection Act 2023 or applicable sector regulations.
Recovery Notes	Re-image all confirmed-compromised endpoints from a validated clean baseline before returning them to production — do not attempt in-place remediation of a DcRAT-compromised host given the RAT's full remote access capability and potential for secondary persistence mechanisms beyond the initial DLL sideload chain. Post-recovery, maintain heightened monitoring of Windows Media Player directory DLL activity and outbound HTTP/S beaconing patterns for a minimum of 30 days, given that Operation DragonReturn is an active campaign timed to the Indian tax season (January–July) with high re-targeting probability. Validate that all rotated credentials from compromised accounts have not been reused on recovered systems, and confirm DMARC reject policies are enforced for all organizational email domains to reduce re-entry via the same spear-phishing vector.
Forensic Artifacts	Sideloaded nvdaHelperRemote.dll: Collect the malicious DLL from its non-standard load path (outside C:\Program Files (x86)\NVDA\) — hash, PE header analysis, and import table will reveal the DcRAT loader code masquerading as a legitimate NVDA helper library | Steganographic image carrier file: Recover the image file (PNG/JPG/BMP) written to %ProgramFiles%\Windows Media Player\ or a TEMP staging directory immediately before DLL load — binwalk or steghide analysis will extract the concealed DcRAT payload from the image data | DcRAT in-memory implant: RAM acquisition from the compromised process will contain the decrypted DcRAT configuration block including C2 server addresses, campaign ID, and any harvested credentials or keylog buffers staged for exfiltration | Email gateway logs with spoofed Income Tax Department headers: Full RFC 2822 headers from lure emails will document sender domain spoofing of incometax.gov.in, X-Originating-IP, and attachment filenames referencing ITR forms or e-filing utilities — critical for attributing initial access and identifying all targeted mailboxes | Windows Registry persistence and scheduled task artifacts: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and schtasks output from the compromised host will document any DcRAT persistence mechanism installed after the initial DLL sideload, which may survive removal of the staged payload files if not explicitly eradicated

Per-Action IR Details

Step 1: Containment — Block execution of unsigned or anomalously placed DLLs in Windows Media Player directories and NVDA installation paths via application control policy (NIST CM-7, CIS 2.3). Alert on or block processes spawning from nvdaHelperRemote.dll outside of a verified, inventory-listed NVDA installation (CIS 1.1). Quarantine any endpoint that received Income Tax Department-themed email attachments during the filing season window.

NIST Phase: Containment

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

Controls: NIST CM-7 (Least Functionality) — restrict execution of unsigned DLLs in %ProgramFiles%\Windows Media Player and NVDA paths, NIST AC-3 (Access Enforcement) — enforce authorized process execution boundaries for nvdaHelperRemote.dll, CIS 2.3 (Address Unauthorized Software) — block or quarantine unauthorized DLL instances outside inventoried NVDA installations, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — validate nvdaHelperRemote.dll presence against asset inventory before allowing execution

Compensating: Deploy Sysmon with EventID 7 (ImageLoaded) configured to alert on nvdaHelperRemote.dll loaded outside C:\Program Files (x86)\NVDA\. Use Windows Defender Application Control (WDAC) or Software Restriction Policies to block unsigned DLL execution from %ProgramFiles%\Windows Media Player. Run: Get-ChildItem 'C:\Program Files\Windows Media Player\' -Filter *.dll | Get-AuthenticodeSignature | Where-Object {$_.Status -ne 'Valid'} to enumerate unsigned DLLs immediately. Isolate flagged hosts by disabling their NIC via: Disable-NetAdapter -Name '*' -Confirm:$false.

Evidence: BEFORE quarantining any endpoint, capture: (1) full RAM acquisition using WinPmem or Magnet RAM Capture to preserve in-memory DcRAT implant artifacts and injected shellcode; (2) netstat -ano output to document active C2 connections from DcRAT HTTP/S beaconing; (3) tasklist /svc and Get-Process output to record all running processes and their parent PIDs; (4) full directory listing of %ProgramFiles%\Windows Media Player\ and the NVDA installation path including file timestamps and hashes (Get-FileHash); (5) email attachment artifacts from the user's mailbox or quarantine folder referencing ITR forms or Income Tax Department lures, including full email headers for sender domain spoofing evidence.

Step 2: Detection — Query email gateway logs for lures referencing Indian Income Tax e-filing utilities, ITR forms, or Income Tax Department sender domains (AU-2, AU-6). Hunt for DLL loads of nvdaHelperRemote.dll from non-standard parent processes or paths outside Program Files. Search EDR telemetry for processes writing to or executing from %ProgramFiles%\Windows Media Player with non-media-player parent processes. Review for steganographic payload delivery: look for image files written to staging directories immediately before DLL load events (T1027.003 behavioral indicator). Pivot on known Silver Fox infrastructure IOCs if available from your threat intel feeds.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging) — ensure email gateway, endpoint, and DLL load events are captured in audit logs, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — actively analyze email gateway and endpoint telemetry for Operation DragonReturn lure patterns and DLL anomalies, NIST AU-3 (Content of Audit Records) — verify log records include parent process, full image path, and timestamps for DLL load events, CIS 8.2 (Collect Audit Logs) — confirm audit logging is enabled on endpoints to capture DLL sideload activity in Windows Media Player directories

Compensating: Without EDR, deploy Sysmon EventID 7 (ImageLoaded) with a rule targeting nvdaHelperRemote.dll and any DLL loaded from %ProgramFiles%\Windows Media Player\. Use Sysmon EventID 11 (FileCreate) to catch image files (*.png, *.jpg, *.bmp) written to staging directories within 60 seconds before a DLL load event. Query email gateway MTA logs with: grep -iE '(income.?tax|ITR|efiling|incometax\.gov\.in)' mail.log to surface lure-themed messages. Use the Sigma rule for DLL sideloading detection (sigma/rules/windows/image_load/image_load_side_load_non_standard_path.yml) converted to Windows Event Log format for teams without a SIEM.

Evidence: This is a detection step that does not alter live state; however, preserve all log artifacts before any downstream containment action: (1) email gateway logs with full headers, attachment filenames, and sender domains impersonating incometax.gov.in; (2) Sysmon Event ID 7 records showing nvdaHelperRemote.dll loaded from a non-standard path; (3) Sysmon Event ID 11 records of image files (steganographic carriers) written to %ProgramFiles%\Windows Media Player\ or TEMP directories immediately preceding DLL load events; (4) Windows Security Event Log Event ID 4688 (Process Creation) filtered for processes spawned from Windows Media Player or NVDA paths with anomalous parent processes; (5) network flow logs or DNS query logs showing outbound connections to Silver Fox-associated C2 infrastructure during or after DLL load timestamps.

Step 3: Eradication — Remove any identified DcRAT implants and associated DLL sideload chains. Purge staged payloads from Windows Media Player directories. Revoke and rotate credentials for any accounts active on confirmed-compromised hosts (D3-CRO). Audit all NVDA installations against your software inventory (CIS 2.1) and remove unauthorized copies. Block delivery domains and file hashes associated with this campaign at the email gateway and endpoint.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management) — revoke and rotate credentials for all accounts active on DcRAT-confirmed hosts, NIST AC-6 (Least Privilege) — audit and restrict accounts whose credentials may have been harvested by DcRAT keylogging or credential theft modules, CIS 2.1 (Establish and Maintain a Software Inventory) — diff all NVDA installations against the authorized software inventory; remove unauthorized or tampered copies, CIS 2.3 (Address Unauthorized Software) — remove unauthorized DLL sideload components (spoofed nvdaHelperRemote.dll) and DcRAT payload files from Windows Media Player directories

Compensating: Use Get-FileHash on all DLLs in %ProgramFiles%\Windows Media Player\ and compare against known-good hashes from a clean Windows installation. Remove anomalous files with Remove-Item -Force. For credential revocation without enterprise tooling, use net user /domain to disable accounts and force password reset via Active Directory Users and Computers. Block campaign file hashes at the endpoint using Windows Defender: Add-MpPreference -ExclusionPath is insufficient — instead add them as indicators via: Add-MpPreference -ThreatID or deploy YARA rules scanning for DcRAT's known string artifacts and C2 configuration patterns in memory and on disk.

Evidence: BEFORE revoking credentials or removing any files, capture: (1) a full memory dump of any process hosting the DcRAT implant (identify via Sysmon EventID 7 or netstat C2 connection PID) using ProcDump: procdump.exe -ma dcrat_memdump.dmp — DcRAT stores its C2 config, stolen credentials, and keylog buffers in memory; (2) a forensic image or hash-verified copy of all files in %ProgramFiles%\Windows Media Player\ including the steganographic image carrier and sideloaded DLL before deletion; (3) the full Windows Registry run keys and scheduled tasks on the compromised host (reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and schtasks /query /fo LIST /v) to document DcRAT persistence mechanisms before eradication; (4) any files in %APPDATA% or %TEMP% directories associated with the DcRAT implant's working directory, including exfiltrated data staging artifacts.

Step 4: Recovery — Re-image confirmed-compromised endpoints before restoring to production. Validate restored systems against your secure configuration baseline (CIS 4.6). Monitor post-recovery for re-infection indicators: DLL anomalies in Windows Media Player paths, unexpected NVDA process activity, and outbound C2 patterns matching DcRAT (HTTP/S beaconing, T1071.001). Confirm audit logging is intact and alert rules for DLL sideloading are active (AU-12, CIS 8.2).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation) — verify audit logging is re-enabled and generating records for DLL load and process creation events post-reimage, CIS 4.6 (Securely Manage Enterprise Assets and Software) — validate restored endpoints against a documented secure configuration baseline before returning to production, CIS 8.2 (Collect Audit Logs) — confirm audit log collection is active and forwarding to a central store post-recovery, specifically for Windows Media Player path and NVDA process activity, NIST AC-17 (Remote Access) — review and re-validate remote access configurations on recovered systems to ensure DcRAT did not establish a persistent remote access channel that survives reimaging via credential reuse

Compensating: For teams without enterprise imaging infrastructure, use DISM or a validated WIM image to restore the OS. Post-reimage, run: sfc /scannow and DISM /Online /Cleanup-Image /RestoreHealth to verify OS integrity. Immediately deploy Sysmon post-reimage with EventID 7 rules for nvdaHelperRemote.dll and EventID 3 (Network Connection) filtered for DcRAT C2 port patterns. Use Wireshark with a BPF filter for HTTP POST traffic to known Silver Fox C2 IP ranges to confirm no residual beaconing. Verify no rogue scheduled tasks or Run keys were restored with user profile data: schtasks /query and reg query HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Evidence: Before reimaging, ensure all previously specified volatile captures (RAM, process list, network state, DcRAT working directory, registry persistence keys) have been completed and are hash-verified in evidence storage. Post-recovery, the evidence focus shifts to integrity validation: (1) hash all DLLs in %ProgramFiles%\Windows Media Player\ on the restored system and compare against Microsoft's known-good file manifest; (2) confirm Sysmon is generating EventID 7 and EventID 3 telemetry by running a controlled test process; (3) validate that no DcRAT-associated file hashes or IOC domains appear in DNS query logs or proxy logs for 72 hours post-recovery as a re-infection watchpoint.

Step 5: Post-Incident — Review email security controls for spoofed government-sender detection; impersonation of tax authorities is a recurring lure class. Assess DLL sideloading exposure across your software inventory — identify other signed binaries susceptible to search-order hijacking (CIS 2.1, NIST CM-7, D3-CH). Evaluate whether user awareness training covers seasonal tax-themed lures, particularly for finance and accounting teams. Document control gaps against NIST AC-6 (least privilege for process execution) and CIS 7.1 (vulnerability management process) to inform next planning cycle.

NIST Phase: Post Incident

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

Controls: CIS 2.1 (Establish and Maintain a Software Inventory) — enumerate all signed binaries in the software inventory susceptible to DLL search-order hijacking similar to NVDA's nvdaHelperRemote.dll, NIST AC-6 (Least Privilege) — document and remediate gaps where standard user processes had execution rights in Windows Media Player directories enabling DcRAT staging, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate DLL sideloading exposure scanning into the vulnerability management cycle, CIS 7.2 (Establish and Maintain a Remediation Process) — update remediation process to include DLL sideloading risk as a tracked finding class following Operation DragonReturn, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — schedule recurring review of DLL load telemetry and email gateway logs during future Indian tax season windows (January–July) when this campaign class is most active

Compensating: Run the open-source tool Robber or a PowerShell DLL hijacking enumeration script against your software inventory to identify other signed binaries with writable DLL search paths — prioritize applications installed in user-writable directories. For email spoofing detection without a commercial email security gateway, verify DMARC reject policy (p=reject) is configured for your domain and test with: nslookup -type=TXT _dmarc.yourdomain.com. Use the open-source PhishTool or MxToolbox email header analyzer to build a runbook for finance team staff to identify spoofed incometax.gov.in sender domains. Document all findings in a lessons-learned report referencing NIST 800-61r3 §4 and schedule a tabletop exercise simulating a tax-season DLL sideloading scenario before the next filing season.

Evidence: Post-incident evidence requirements shift to documentation and improvement: (1) compile all IOCs from this campaign (nvdaHelperRemote.dll hashes, steganographic image file hashes, C2 domains, sender domains spoofing Income Tax Department) into a structured threat intelligence report for sharing with sector peers and CERT-In; (2) produce a DLL search-order hijacking exposure report listing all software inventory entries with writable sideload paths, prioritized by privilege level; (3) retain all incident evidence (memory dumps, email artifacts, DcRAT samples) in a hash-verified evidence repository for a minimum period consistent with your data retention policy (NIST AU-11) and any applicable Indian IT Act obligations; (4) document timeline discrepancies between initial email delivery and first DcRAT C2 beacon to calculate dwell time and inform detection gap analysis.

Detection Guidance

Focus detection on three behavioral pillars: (1) DLL sideloading anomalies, alert on nvdaHelperRemote.dll loaded by any process outside a verified NVDA installation path; flag DLL loads from Windows Media Player directories by non-media processes; use EDR to detect signed binary execution with anomalous child processes (maps to T1574.002, T1036.005). (2) Steganographic staging, look for image files written to user or temp directories immediately preceding DLL load or process injection events; correlate file-write and process-spawn events within a short time window (T1027.003, T1027.001). (3) DcRAT C2 behavior, hunt for periodic HTTP/S beaconing to low-reputation or newly registered domains; flag screen capture API calls (T1113) combined with outbound data transfers (T1041); monitor for Windows service creation or modification by non-admin processes (T1543.003). Email gateway: filter for Income Tax Department impersonation lures with Hindi/English mixed content and attachments spoofing ITR utilities. Enrich alerts with Silver Fox infrastructure indicators from current threat intel feeds. Reference AU-2 for event logging scope and AU-6 for review cadence. D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) are applicable countermeasures.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	not disclosed in source material	C2 infrastructure attributed to Silver Fox / DragonReturn — obtain current IOC feed from threat intel provider; The Hacker News reporting did not publish specific domains at analysis time	LOW
HASH	not disclosed in source material	DcRAT payload and spoofed NVDA binary hashes not published in available sources — check Trend Micro ValleyRAT research and current threat intel platforms for associated hashes	LOW

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1105** — Ingress Tool Transfer
- **T1562.001** — Disable or Modify Tools
- **T1113** — Screen Capture
- **T1041** — Exfiltration Over C2 Channel
- **T1574.002** — DLL Side-Loading
- **T1566.001** — Spearphishing Attachment
- **T1543.003** — Windows Service
- **T1548.002** — Bypass User Account Control
- **T1055** — Process Injection
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1204.002** — Malicious File
- **T1059** — Command and Scripting Interpreter
- **T1027.003** — Steganography
- **T1071** — Application Layer Protocol
- **T1027.001** — Binary Padding

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness

- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **CM-7** — Least Functionality
- **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

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1105	Ingress Tool Transfer	Command-And-Control
T1562.001	Disable or Modify Tools	Defense-Evasion
T1113	Screen Capture	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration
T1574.002	DLL Side-Loading	Persistence
T1566.001	Spearphishing Attachment	Initial-Access
T1543.003	Windows Service	Persistence
T1548.002	Bypass User Account Control	Privilege-Escalation
T1055	Process Injection	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1204.002	Malicious File	Execution
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1027.003	Steganography	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1027.001	Binary Padding	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/suspected-china-nexus-hackers-use...	T2
DLL Sideloading Attacks: Signed Malware Risks - Ontinue	https://www.ontinue.com/resource/blog-signed-sideloaded-compromised/	T3
PureRAT Campaign Targets Job Seekers, Abuses Foxit PDF ...	https://www.trendmicro.com/en_us/research/25/l/valleyrat-campaign.html	T1
ValleyRAT Targets Job Seekers via Foxit DLL Sideloading	https://socprime.com/active-threats/valleyrat-malware-detection/	T3

Generated 2026-07-06 15:12 UTC by TJS Security Command Center