INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:40 UTC

# Storm-2561 SEO Poisoning Campaign Delivers Signed Trojanized VPN Installers to Harvest Enterprise Credentials

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0013 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | Ivanti Pulse Secure VPN (client installer), SonicWall VPN (client installer), Hanwha Vision (installer lure), Windows (RunOnce registry key for persistence); GitHub abused as delivery infrastructure |
| **Published** | 2026-03-13 |

## Executive Summary

Storm-2561, a tracked threat actor, has run a sustained campaign since at least May 2025 that poisons search engine results to redirect enterprise employees to attacker-controlled sites serving trojanized VPN installers for Ivanti Pulse Secure, SonicWall, and Hanwha Vision products. The installers deploy an information stealer and present a fake credential prompt, harvesting VPN credentials at the moment of installation. Organizations whose employees download VPN software outside of controlled software distribution channels face direct credential theft risk and potential enterprise network compromise.

## Technical Analysis

Storm-2561 stages digitally signed trojanized installers mimicking legitimate VPN clients (Ivanti Pulse Secure, SonicWall, Hanwha Vision) on attacker-controlled sites surfaced via SEO poisoning. Payload delivery relies on DLL sideloading (CWE-426, MITRE T1574.002) to execute the Hyrax information stealer. A fake credential UI (T1056.003) captures VPN credentials at install time. Malicious payloads were hosted on GitHub repositories (T1102, T1608.004) to abuse the platform's trusted reputation and bypass reputation-based controls (CWE-494, CWE-346). Persistence is established via the Windows RunOnce registry key (T1547.001, CWE-N/A). The code-signing certificate used to sign the lures was reported as revoked, and the associated GitHub repositories were taken down in January 2026. No CVE is assigned; the campaign exploits user trust and software supply chain weaknesses rather than a discrete technical vulnerability. Relevant MITRE techniques span resource development (T1608.001, T1608.004, T1608.006, T1588.003), supply chain compromise (T1195.002), web service abuse (T1102, T1567.001), credential access (T1555, T1056.003), user execution (T1204.002), and

persistence (T1547.001). The attack pattern itself remains viable: revocation of this certificate and repository removal do not retire the playbook.

## Action Checklist

1. Step 1, Immediate: Audit software distribution policy and confirm VPN client installers are sourced exclusively from vendor portals or internal software repositories; block ad-hoc downloads from unvetted sites via web proxy or endpoint DLP controls.
2. Step 2, Detection: Hunt endpoint logs and EDR telemetry for DLL sideloading events associated with VPN installer processes, unexpected RunOnce registry key entries created at or after software installation, and outbound connections to GitHub from installer processes or newly installed VPN client binaries.
3. Step 3, Assessment: Query identity and authentication logs for VPN credential use anomalies (new geo-locations, off-hours access, concurrent sessions) for users who installed or reinstalled VPN clients since May 2025; treat any flagged accounts as potentially compromised.
4. Step 4, Communication: Alert employees, particularly remote workers and IT help desk staff who commonly download VPN clients, to verify installer sources; issue internal guidance that legitimate VPN software will only be distributed via [your approved channel]; report suspicious installer activity to your threat intel or IR team.
5. Step 5, Long-term: Update acceptable use and software procurement policy to explicitly prohibit downloading security software from search engine results; evaluate application allowlisting controls that enforce code-signing certificate trust anchors; add detection rules for DLL sideloading patterns and RunOnce persistence to your SIEM or EDR.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to CISO/management immediately if any user account shows credential misuse post-compromise (Step 3 anomalies) or if organization-wide VPN client replacement is required; escalate to external IR firm if forensic analysis of trojanized installer reveals additional payload or persistence mechanisms not documented in public advisories. |
| **Recovery Notes** | After containment, initiate VPN credential reset for all users who installed software since May 2025 (cross-reference Step 2 and Step 3 findings). Force re-authentication with MFA for affected accounts and monitor for follow-on lateral movement (look for unexpected domain admin activities, remote access tool installations, or data exfiltration). Complete policy and detection rule updates within 30 days and perform tabletop exercise with IR team to test procedure against simulated trojanized installer. |

| | |
|---|---|
| **Forensic Artifacts** | Windows Security Event Log (Event ID 4688 for process creation, 4657 for registry modifications, 4624/4625 for authentication) \| Windows System Event Log (service installation, DLL load events, RunOnce registry key creation timestamps) \| NTUSER.DAT and SOFTWARE registry hives (RunOnce persistence keys, file associations, search history) \| VPN client installer file hashes, signatures, and sideloaded DLL artifacts from Program Files directories \| VPN server authentication logs (connection timestamps, source IPs, user accounts) covering 90-day lookback from incident discovery \| Proxy/firewall logs filtering for GitHub destination IPs and outbound connections from installer process IDs \| DNS query logs and netstat output capturing network artifacts from installation timeframe \| Browser download history and cache (edge://downloads, Chrome's Default/Download History SQLite database) |

### Per-Action IR Details

**Step 1, Immediate: Audit software distribution policy and confirm VPN client installers are sourced exclusively from vendor portals or internal software repositories; block ad-hoc downloads from unvetted sites via web proxy or endpoint DLP controls.**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2.1 (Preparation phase: tools and processes)

**Controls:** NIST 800-53 CM-5 (Access Restrictions for Change), NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), CIS 4.1 (Inventory and Control of Software Assets), CIS 4.6 (Address Unauthorized Software)

**Compensating:** Without DLP: configure Windows Firewall egress rules to block destination domains tied to Storm-2561 delivery (enumerate from threat intel). Use free proxy (Squid) with ACL to allowlist only vendor domains (ivanti.com, sonicwall.com, hanwha.com official download paths). Audit browser history weekly using PowerShell: Get-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedURLs' | Select-Object * | Export-Csv browser_urls.csv; correlate against approved vendor list.

**Evidence:** Capture current software distribution policy document, proxy/firewall allow/deny rules, and baseline of legitimate VPN installer download locations from vendor. Screenshot or export web proxy logs (last 90 days) filtering for VPN-related downloads to establish baseline of ad-hoc sources. Document integrity hash of legitimate installers (hash downloaded copies from official vendor portals).

**Step 2, Detection: Hunt endpoint logs and EDR telemetry for DLL sideloading events associated with VPN installer processes, unexpected RunOnce registry key entries created at or after software installation, and outbound connections to GitHub from installer processes or newly installed VPN client binaries.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2.4 (Analysis: Collection and examination of evidence)

**Controls:** NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-2 (Audit Events), CIS 8.2 (Configure Diagnostic Logging), CIS 8.5 (Collect Detailed Audit Logs)

**Compensating:** Without EDR: enable Windows Event Log auditing (Auditpol.exe /set /category:Object_Access /success:enable). Hunt manually using: (1) Autoruns from Sysinternals to enumerate RunOnce keys: reg query 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /s > runonce_baseline.txt; (2) File timestamps via Get-ChildItem -Path 'C:\Program Files\Ivanti\Pulse Secure' -Recurse -File | Get-FileHash > file_hashes.csv to detect sideloaded DLLs (compare against vendor manifest); (3) Netstat history: netstat -b -n -o > netstat_snapshot.txt at installation time, then weekly. Correlate with GitHub IP ranges (download from GitHub's public IP list).

**Evidence:** Collect Windows Event Log sources: Security (4688 for process creation, 4657 for registry modifications), System (DLL load events). Export Event Viewer logs: wevtutil qe Security /f:text > security_log_export.txt. Capture registry hive NTUSER.DAT and SOFTWARE hive from suspected machines (use Registry Editor or autoreg backup). Preserve netstat output and DNS query logs (if available from DNS server or proxy). Capture memory dump of VPN installer process if still running: Get-Process | Where-Object {$_.Name -like '*vpn*'} | Select-Object ProcessName, ID.

**Step 3, Assessment: Query identity and authentication logs for VPN credential use anomalies (new geo-locations, off-hours access, concurrent sessions) for users who installed or reinstalled VPN clients since**

**May 2025; treat any flagged accounts as potentially compromised.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2.3 (Determine the scope of the compromise)

**Controls:** NIST 800-53 AC-2 (Account Management), NIST 800-53 AU-12 (Audit Generation), CIS 5.3 (Configure Centralized Audit Logging)

**Compensating:** Without SIEM: extract VPN logs directly from VPN server (Ivanti/SonicWall appliance): export connection logs to CSV via admin console. Cross-reference with list of users who installed VPN client (from Step 2 registry/file timestamp data). Manually review logs for: (1) login timestamp anomalies (compare to user's historical pattern from Azure AD Sign-in or on-prem logs if available); (2) source IP geolocation using free GeoIP database (MaxMind GeoLite2 free tier); (3) concurrent sessions (multiple IPs logged in simultaneously for one user account). Document findings in spreadsheet: user | install_date | first_anomalous_login | geo | time_of_day | action_taken.

**Evidence:** Export VPN authentication logs (minimum 90 days back): request from VPN appliance admin. Capture Azure AD Sign-in logs (if cloud-connected) or on-prem Active Directory logon events (Event ID 4624, 4625). Preserve email metadata for users flagged as installing software (check with help desk for ticket records, or search email for 'vpn install' / 'vpn download' keywords). Document baseline user access patterns (time of day, geography) from 6 months prior to May 2025.

**Step 4, Communication: Alert employees, particularly remote workers and IT help desk staff who commonly download VPN clients, to verify installer sources; issue internal guidance that legitimate VPN software will only be distributed via [your approved channel]; report suspicious installer activity to your threat intel or IR team.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 (Containment strategy and execution)

**Controls:** NIST 800-53 IR-4 (Incident Handling), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), CIS 1.2 (Assign Cybersecurity Responsibility)

**Compensating:** No alternative needed for this step — communication is procedural, not tool-dependent. However, document communication chain: (1) draft alert email template with installer signature/hash verification instructions; (2) distribute via email, internal wiki, and Slack/Teams; (3) request IT help desk log all received 'installer reports' in shared spreadsheet (time | user | installer_source | action_taken); (4) escalate any reported downloads to IR team within 1 hour of report.

**Evidence:** Before sending communication, preserve baseline of current IT help desk ticket system status. After communication, collect: email delivery receipt logs (MX logs or email gateway logs showing alert distribution), employee acknowledgment tracking if survey/attestation is used, and help desk ticket log for incoming installer reports (establishes post-alert baseline for measuring campaign exposure).

**Step 5, Long-term: Update acceptable use and software procurement policy to explicitly prohibit downloading security software from search engine results; evaluate application allowlisting controls that enforce code-signing certificate trust anchors; add detection rules for DLL sideloading patterns and RunOnce persistence to your SIEM or EDR.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.4 (Post-incident activities: lessons learned)

**Controls:** NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), NIST 800-53 CM-5 (Access Restrictions for Change), NIST 800-53 IA-5 (Authentication and Identification Controls), CIS 2.1 (Maintain Inventory of Authorized Software), CIS 4.6 (Address Unauthorized Software)

**Compensating:** Without enterprise allowlisting (AppLocker/Device Guard): (1) use free PowerShell AppLocker policies (built into Windows 10/11 Pro and above) to enforce code-signing: create XML policy requiring VPN installer binaries to carry valid Authenticode signature from Ivanti/SonicWall; deploy via Group Policy. (2) For detection rules without EDR: write Sysmon rules (free, open-source) to alert on registry writes to RunOnce hives and DLL loads from unexpected parent processes (e.g., msiexec.exe loading unsigned DLLs). (3) Export rules to SIEM/log aggregator (ELK Stack, Splunk free tier, or Graylog) for correlation. Template: EventID=13 (registry write) AND TargetObject CONTAINS

'RunOnce' AND User NOT IN (admin_list) → Alert.

**Evidence:** Document current acceptable use policy version and distribution date. Archive baseline code-signing certificates for Ivanti Pulse Secure and SonicWall (download from vendor PKI documentation). Preserve AppLocker/Sysmon rule creation date and test results (rule should fire on test installers before deployment). Create detection rule audit log showing rule effectiveness on historical logs (e.g., rule triggered X times on confirmed Storm-2561 samples).

## Detection Guidance

Focus detection on three behavioral clusters. First, DLL sideloading at install time: look for installer processes (setup.exe, installer.exe, or VPN vendor binary names) loading DLLs from unexpected paths, particularly user-writable directories or the same directory as the installer executable, EDR process tree and image load telemetry are the primary signal. Second, RunOnce persistence: query registry event logs (Event ID 4657 or Sysmon Event ID 13) for RunOnce key writes (HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce or HKLM equivalent) created within the timeframe of VPN installer execution. Third, credential harvesting indicators: look for fake UI processes spawning alongside installer processes, or installer processes making network connections that do not match the legitimate vendor's update or telemetry infrastructure. For GitHub-hosted payload delivery (T1102), look for installer or dropper processes initiating HTTPS connections to raw.githubusercontent.com or github.com during or immediately after installation. Baseline: compare against clean installations of the legitimate vendor installers to identify behavioral delta. No public IOCs (hashes, domains, IPs) are confirmed in the source data available for this session; treat any IOC list from external feeds as requiring validation before blocking.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `github.com / raw.githubusercontent.com (abused infrastructure)` | GitHub repositories used to host Hyrax stealer payloads; specific repository paths not available in source data. Repositories taken down January 2026. Monitor for installer processes making unexpected connections to GitHub delivery paths. | MEDIUM |

## Framework Mappings

### MITRE-ATTACK

- **T1608.001** — Upload Malware
- **T1195.002** — Compromise Software Supply Chain
- **T1598.003** — Spearphishing Link
- **T1588.003** — Code Signing Certificates
- **T1608.004** — Drive-by Target
- **T1102** — Web Service

- **T1547.001** — Registry Run Keys / Startup Folder
- **T1567.001** — Exfiltration to Code Repository
- **T1056.003** — Web Portal Capture
- **T1608.006** — SEO Poisoning
- **T1204.002** — Malicious File
- **T1574.002** — DLL Side-Loading
- **T1555** — Credentials from Password Stores

**NIST-800-53R5**

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

**OWASP-TOP10-2021**

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

**CIS-V8**

- **2.5**
- **2.6**
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers

**HIPAA-SECURITY**

- **164.312(d)** — Person or Entity Authentication

**SOC2-TSC**

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

**ISO-27001-2022**

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

**NIST-CSF-2**

- **GV.SC-01** — Cybersecurity supply chain risk management program

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1608.001 | Upload Malware | Resource-Development |
| T1195.002 | Compromise Software Supply Chain | Initial-Access |
| T1598.003 | Spearphishing Link | Reconnaissance |
| T1588.003 | Code Signing Certificates | Resource-Development |
| T1608.004 | Drive-by Target | Resource-Development |
| T1102 | Web Service | Command-And-Control |
| T1547.001 | Registry Run Keys / Startup Folder | Persistence |
| T1567.001 | Exfiltration to Code Repository | Exfiltration |
| T1056.003 | Web Portal Capture | Collection |
| T1608.006 | SEO Poisoning | Resource-Development |
| T1204.002 | Malicious File | Execution |
| T1574.002 | | |
| T1555 | Credentials from Password Stores | Credential-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://thehackernews.com/2026/03/storm-2561-spreads-trojan-vpn-cli... | T3 |
| **VPN flaws allowed Chinese hackers to compromise dozens of Ivanti ...** | https://techcrunch.com/2026/02/23/vpn-flaws-allowed-chinese-hackers... | T2 |
| **Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation** | https://cloud.google.com/blog/topics/threat-intelligence/ivanti-con... | T3 |
| **Ivanti VPN Chain Exploitation: The Two-Vulnerability Knockout** | https://medium.com/@instatunnel/ivanti-vpn-chain-exploitation-the-t... | T3 |
| **Ivanti VPN Vulnerability: What You Need to Know** | https://www.paloaltonetworks.com/cyberpedia/ivanti-VPN-vulnerabilit... | T3 |

Generated 2026-03-29 18:40 UTC by TJS Security Command Center