INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 18:51 UTC

Trojanized DAEMON Tools Lite Installers Backdoored Thousands of Systems Across 100+ Countries in Confirmed Supply Chain Breach

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0280
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	DAEMON Tools Lite v12.5.0.2421-12.5.0.2434 (free version, Disc Soft Limited); DAEMON Tools Pro and DAEMON Tools Ultra reported unaffected
Published	2026-05-06T12:43:30
Discovery Source	Rss

Executive Summary

Attackers compromised the build environment of Disc Soft Limited and distributed backdoored installers for DAEMON Tools Lite (versions 12.5.0.2421-12.5.0.2434) through the official vendor website from April 8 to May 5, 2026. The trojanized installers carried a valid digital signature, enabling distribution to potentially thousands of systems across more than 100 countries. Organizations whose users installed the free version of DAEMON Tools Lite during that window should treat affected systems as potentially compromised and begin containment and investigation immediately.

Technical Analysis

Disc Soft Limited confirmed a build environment intrusion resulting in malware-laced installers for DAEMON Tools Lite versions 12.5.0.2421-12.5.0.2434 (free tier only; Pro and Ultra reported unaffected). Installers were signed with the vendor's legitimate certificate (CWE-345: insufficient verification of data authenticity via subverted code signing), included undisclosed malicious functionality (CWE-506), and were delivered via the official download channel without integrity verification mechanisms detectable by end users (CWE-494). The malware is described as multi-stage. Confirmed MITRE ATT&CK technique mapping includes: supply chain compromise via software dependency (T1195.002), code signing abuse enabling trusted installer delivery (T1553.002), command and control over application layer protocol HTTP/S (T1071.001), ingress tool transfer (T1105), process injection (T1055), command and scripting interpreter (T1059), exfiltration over C2 channel (T1041), boot/logon autostart persistence (T1547), system owner/user discovery (T1033), process discovery

(T1057), system information discovery (T1082), and malicious file execution by user (T1204.002). Specific C2 infrastructure, payload hashes, and full post-exploitation capability details are not confirmed in available source data as of 2026-05-06. No CVE has been assigned. A clean replacement installer (v12.6.0.2445) has been released by Disc Soft. Threat actor attribution remains unknown.

Action Checklist

1. Step 1: Containment. Immediately isolate any endpoint on which DAEMON Tools Lite was installed or updated between April 8 and May 5, 2026. Query software inventory (SCCM, Intune, endpoint agent) for installed versions 12.5.0.2421 through 12.5.0.2434. Block outbound connections from affected hosts pending investigation. Do not allow these systems to access sensitive internal resources or authentication infrastructure until cleared.
2. Step 2: Detection. Search EDR telemetry for execution of DAEMON Tools Lite installer binaries during the April 8-May 5, 2026 window (event type: process creation; parent process: installer executable). Look for anomalous child processes spawned by the installer, unexpected scheduled tasks or autostart registry entries (HKLM\Software\Microsoft\Windows\CurrentVersion\Run), unexplained outbound HTTP/S connections to new or low-reputation destinations, and signs of process injection (T1055) such as remote thread creation into legitimate host processes. Query SIEM for file download events from disc-soft.com or mirror domains in the exposure window. No confirmed IOC hashes or C2 addresses are available in current source data; behavioral detection is the primary method.
3. Step 3: Eradication. Uninstall DAEMON Tools Lite versions 12.5.0.2421-12.5.0.2434 from all affected systems. Do not reinstall from cached or previously downloaded media. Download v12.6.0.2445 exclusively from the official Disc Soft channel and verify the installer's digital signature before execution. On systems where malware indicators are detected (anomalous processes, persistence artifacts, or C2 connections), treat full reimaging as the baseline remediation given the multi-stage malware description and unconfirmed payload scope. Remove any persistence mechanisms identified during detection (scheduled tasks, autostart registry keys, injected DLLs).
4. Step 4: Recovery. After reimaging or confirmed eradication, validate that no residual persistence artifacts remain (autostart registry, scheduled tasks, service entries). Reset credentials for any accounts used on affected systems, including domain credentials if the host had access to Active Directory. Monitor reinstated systems for 30 days for anomalous outbound connections, new scheduled tasks, or lateral movement indicators. Confirm v12.6.0.2445 install integrity via vendor-provided checksum if published.
5. Step 5: Post-Incident. Audit software procurement and update workflows to determine how trojanized installers bypassed existing controls. Implement or enforce file hash verification for third-party software installers prior to execution. Evaluate whether endpoint controls would have detected code-signing abuse (T1553.002) or anomalous installer behavior at execution time. Review vendor vetting processes: confirm whether Disc Soft or comparable vendors are subject to periodic supply chain risk assessments per NIST SP 800-161r1. Document findings for future GRC reviews.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if forensic analysis confirms credential harvesting, lateral movement to Active Directory infrastructure, or data exfiltration from any affected host — or if the organization operates in a regulated industry (HIPAA, PCI-DSS, GDPR) where confirmed installation of the backdoored DTLite versions on systems processing PII, PHI, or cardholder data triggers mandatory breach notification timelines.
Recovery Notes	Reinstated hosts must be monitored via Sysmon and centralized log collection for a minimum of 30 days post-recovery, with specific alerting on new outbound connections, scheduled task creation (Event ID 4698), and service installation (Event ID 4697), as multi-stage backdoor payloads may include time-delayed or conditional secondary stagers that survive initial eradication if reimaging was not performed. All domain accounts active on affected hosts during the April 8–May 5 exposure window must be treated as potentially harvested and require password resets and Kerberos TGT invalidation before those hosts are returned to production. Confirm v12.6.0.2445 installer integrity via vendor-published SHA-256 checksum prior to deployment, and do not deploy from any internally cached copy of the installer downloaded before May 6, 2026.
Forensic Artifacts	DTLiteInstaller.exe binary cached in %TEMP% or user Downloads folder with file creation timestamp between April 8 and May 5, 2026 — SHA-256 hash this file and compare against Disc Soft's post-incident advisory for known-bad hashes once published; this is the primary artifact confirming trojanized installer delivery. | Windows Sysmon Event ID 1 (Process Create) logs showing DTLiteInstaller.exe spawning unexpected child processes (cmd.exe, powershell.exe, wscript.exe, msiexec.exe with non-standard arguments) — these child process chains are the behavioral signature of the embedded backdoor dropper executing during installation. | Windows Registry hive export of HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKCU equivalent, filtered for entries with creation timestamps matching the DTLite installer execution window — persistence keys written by the backdoor component would appear here outside the expected DTLite installation footprint (C:\Program Files (x86)\DAEMON Tools Lite\). | Sysmon Event ID 3 (Network Connection) and DNS Client Event Log (Event ID 3006/3010) records from affected hosts during and after the April 8–May 5 window — the backdoor's C2 beacon traffic would appear as outbound HTTP/S connections to domains not previously seen in the organization's DNS history, likely with low TTLs or newly-registered certificates, attributable to the DTLite process or an injected host process. | Windows Security Event Log Event IDs 4768 and 4769 (Kerberos TGT and service ticket requests) from affected hosts during the exposure window — if the backdoor included a credential harvester, anomalous Kerberos ticket requests (unusual service SPNs, off-hours authentication, ticket requests for sensitive services like CIFS on domain controllers) from compromised host machine accounts would indicate lateral movement attempts originating from the trojanized DTLite installation.

Per-Action IR Details

Step 1: Containment — Immediately isolate any endpoint on which DAEMON Tools Lite was installed or updated between April 8 and May 5, 2026. Query software inventory (SCCM, Intune, endpoint agent) for installed versions 12.5.0.2421 through 12.5.0.2434. Block outbound connections from affected hosts pending investigation. Do not allow these systems to access sensitive internal resources or authentication infrastructure until cleared.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and

Manage a Firewall on End-User Devices)

Compensating: Run the following PowerShell command on all Windows endpoints (or push via PSRemoting) to identify affected installs without SCCM/Intune: Get-WmiObject -Class Win32_Product | Where-Object { $_.Name -like '*DAEMON Tools Lite*' -and ($_.Version -ge '12.5.0.2421' -and $_.Version -le '12.5.0.2434') } | Select-Object Name, Version, InstallDate. For network isolation on a tight budget, apply a Windows Firewall outbound block rule via GPO or local policy targeting affected hosts: netsh advfirewall firewall add rule name='DTLite-Quarantine' dir=out action=block. If osquery is deployed, use: SELECT name, version, install_date FROM programs WHERE name LIKE '%DAEMON Tools%'.

Evidence: Before isolating, capture a live memory snapshot and active network connections from the affected host using ProcDump (sysinternals) and netstat -ano to preserve any in-memory backdoor artifacts and active C2 connections. Collect the installed DAEMON Tools Lite binary (DTLite.exe) and installer cache (typically %TEMP%\DTLite*.exe or C:\Users\\Downloads\DTLiteInstaller.exe) for hash comparison and static analysis. Pull SCCM/Intune software inventory logs showing the specific version installed and the installation timestamp to confirm exposure within the April 8–May 5, 2026 window.

Step 2: Detection — Search EDR telemetry for execution of DAEMON Tools Lite installer binaries during the April 8–May 5, 2026 window (event type: process creation; parent process: installer executable). Look for anomalous child processes spawned by the installer, unexpected scheduled tasks or autostart registry entries (HKLM\Software\Microsoft\Windows\CurrentVersion\Run), unexplained outbound HTTP/S connections to new or low-reputation destinations, and signs of process injection (T1055) such as remote thread creation into legitimate host processes. Query SIEM for file download events from disc-soft.com or mirror domains in the exposure window. No confirmed IOC hashes or C2 addresses are available in current source data — behavioral detection is the primary method.

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)

Compensating: Deploy Sysmon (config: SwiftOnSecurity baseline minimum) if not present and collect Event ID 1 (Process Create) for DTLiteInstaller.exe as parent process, Event ID 3 (Network Connection) for outbound connections from DTLite.exe or any child process it spawned, and Event ID 8 (CreateRemoteThread) for process injection indicators against common host processes (svchost.exe, explorer.exe, lsass.exe). Query Windows Security Event Log for Event ID 4698 (Scheduled Task Created) and Event ID 4697 (Service Installed) filtered to the April 8–May 5 install window using: Get-WinEvent -LogName Security | Where-Object { $_.Id -in @(4698,4697) -and $_.TimeCreated -ge '2026-04-08' -and $_.TimeCreated -le '2026-05-05' }. For network detection without a SIEM, run Wireshark or tcpdump with a capture filter for outbound port 80/443 traffic from the affected host and inspect SNI fields for low-reputation or newly-registered domains. Develop a Sigma rule targeting DTLiteInstaller.exe spawning cmd.exe, powershell.exe, or wscript.exe as child processes for retroactive log hunting.

Evidence: Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on parent processes matching DTLiteInstaller.exe (any version string 12.5.0.2421–12.5.0.2434) between April 8 and May 5, 2026, to identify any anomalous child process chain. Review Sysmon Event ID 11 (File Create) for files dropped by the installer outside expected DAEMON Tools installation paths (default: C:\Program Files (x86)\DAEMON Tools Lite\). Inspect the Windows Registry at HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\Microsoft\Windows\CurrentVersion\Run for entries created during the installer execution window that do not correspond to legitimate DTLite components. Pull DNS query logs (Windows DNS Client Event Log, Event ID 3006/3010 or resolver cache via ipconfig /displaydns) from affected hosts for any external domains resolved during or shortly after installer execution. Given that the installer carried a valid Disc Soft digital signature, also query SIEM or Sysmon Event ID 7 (Image Loaded) for signed DLLs loaded from unexpected paths, as the trojanized installer may have sideloaded a malicious signed component.

Step 3: Eradication — Uninstall DAEMON Tools Lite versions 12.5.0.2421–12.5.0.2434 from all affected systems. Do not reinstall from cached or previously downloaded media. Download v12.6.0.2445 exclusively

from the official Disc Soft channel and verify the installer's digital signature before execution. On confirmed-compromise hosts, treat full reimaging as the baseline remediation given the multi-stage malware description and unconfirmed payload scope. Remove any persistence mechanisms identified during detection (scheduled tasks, autostart registry keys, injected DLLs).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-1 (Policy and Procedures — Configuration Management), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For hosts where full reimaging is not immediately feasible, perform the following manual eradication sequence: (1) Uninstall DTLite via wmic product where 'name like "%DAEMON Tools Lite%"' call uninstall /nointeractive; (2) Remove residual scheduled tasks: schtasks /query /fo LIST /v | findstr /i 'daemon' and delete any hits with schtasks /delete /tn /f; (3) Scrub autostart registry keys: reg delete HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v /f and repeat for HKCU path; (4) Scan for injected DLLs in running processes using Sysinternals Process Explorer (Check VirusTotal integration) — look for unsigned or mis-pathed DLLs loaded into svchost.exe or explorer.exe post-installer execution; (5) Verify the v12.6.0.2445 installer digital signature via PowerShell: Get-AuthenticodeSignature -FilePath .\DTLiteInstaller.exe before execution. Use ClamAV with an updated signature database to scan the full installation directory and %TEMP% path prior to reimaging decision.

Evidence: Before uninstalling, preserve the full DAEMON Tools Lite installation directory (default: C:\Program Files (x86)\DAEMON Tools Lite\) as a forensic copy, including all DLLs, executables, and any files with creation timestamps matching the April 8–May 5 installer execution window. Export current scheduled tasks (schtasks /query /xml > scheduled_tasks_snapshot.xml) and the full HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKCU equivalent registry hive exports (reg export HKLM\Software\Microsoft\Windows\CurrentVersion\Run run_keys_snapshot.reg) before removal to preserve evidence of persistence mechanisms. If process injection (T1055) was identified in Step 2, capture a full memory image using WinPmem or Magnet RAM Capture before rebooting, as injected payloads will not survive a reboot and cannot be recovered post-eradication.

Step 4: Recovery — After reimaging or confirmed eradication, validate that no residual persistence artifacts remain (autostart registry, scheduled tasks, service entries). Reset credentials for any accounts used on affected systems, including domain credentials if the host had access to Active Directory. Monitor reinstated systems for 30 days for anomalous outbound connections, new scheduled tasks, or lateral movement indicators. Confirm v12.6.0.2445 install integrity via vendor-provided checksum if published.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Validate persistence clearance on reinstated hosts using Sysinternals Autoruns (run as Administrator, hide Microsoft entries, scan for unsigned or suspicious entries in the Logon, Scheduled Tasks, and Services tabs) — export baseline as autoruns_baseline__.arn for 30-day comparison. For credential resets without an enterprise PAM tool, force domain password resets via: Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force) and immediately revoke any Kerberos TGTs: klist purge on affected hosts. For 30-day monitoring without EDR, configure Sysmon Event ID 3 (Network Connection) forwarding to a central Windows Event Collector (WEC) server and alert on new outbound connections from reinstated hosts to non-whitelisted destinations. Run a weekly osquery scheduled query against reinstated hosts: SELECT name, path, source FROM startup_items to catch re-emergent persistence.

Evidence: Before returning a reimaged host to production, run Sysinternals Autoruns and compare output against a known-good baseline from a similarly-configured, unaffected host to confirm no residual persistence from the DTLite

backdoor survived the reimage. Pull Active Directory authentication logs (Windows Security Event Log Event ID 4624, 4625, 4768, 4769) for accounts that were active on affected hosts during the April 8–May 5 window to establish whether credential harvesting occurred prior to containment — this is especially relevant given that the trojanized installer had valid code signing and could have operated undetected for weeks. Verify the SHA-256 hash of the v12.6.0.2445 installer against any checksum published in the Disc Soft vendor advisory before deployment to reinstated hosts.

Step 5: Post-Incident — Audit software procurement and update workflows to determine how trojanized installers bypassed existing controls. Implement or enforce file hash verification for third-party software installers prior to execution. Evaluate whether endpoint controls would have detected code-signing abuse (T1553.002) or anomalous installer behavior at execution time. Review vendor vetting processes: confirm whether Disc Soft or comparable vendors are subject to periodic supply chain risk assessments per NIST SP 800-161r1. Document findings for future GRC reviews.

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-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SA-12 (Supply Chain Protection), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Implement mandatory hash verification for all third-party installers using a simple PowerShell wrapper enforced via GPO software restriction policy: (Get-FileHash -Path .\installer.exe -Algorithm SHA256).Hash — document expected hashes in a version-controlled text file in your software repository before any installer is approved for deployment. To detect future code-signing abuse (MITRE T1553.002) without commercial tooling, configure Sysmon Event ID 7 (Image Loaded) to alert on signed executables where the signer does not appear on an internal approved-publisher allowlist, and develop a YARA rule targeting installer PE structures that contain embedded secondary payloads (polyglot PE patterns, appended data sections). For supply chain vendor assessment without a formal TPRM platform, create a lightweight annual questionnaire aligned to NIST SP 800-161r1 Appendix D (C-SCRM practices) for all critical software vendors — flag Disc Soft and similar utility-software vendors as Tier 2 supply chain risks given this incident.

Evidence: Compile a full incident timeline from software inventory logs, SCCM/Intune deployment records, and any download proxy logs showing when disc-soft.com was accessed during April 8–May 5, 2026 — this establishes the precise exposure window for regulatory breach notification analysis and GRC documentation. Preserve all forensic artifacts collected across Steps 1–4 in a documented chain-of-custody package, including memory images, registry exports, scheduled task snapshots, and network connection logs, as these may be required for regulatory reporting or law enforcement referral given the confirmed supply chain breach affecting 100+ countries. Review proxy or DNS logs for any downloads from disc-soft.com mirror or CDN domains during the exposure window to identify endpoints that may have been missed by the SCCM/Intune software inventory query.

Detection Guidance

No confirmed IOC hashes, C2 IP addresses, or domain indicators are available in current source data as of 2026-05-06. Detection must rely on behavioral and inventory-based methods. (1) Software inventory: query for installed DAEMON Tools Lite versions 12.5.0.2421-12.5.0.2434 across all managed endpoints. (2) Process execution history: search EDR or Windows Event Logs (Event ID 4688 with command-line logging enabled) for execution of DAEMON Tools Lite installer binaries between April 8 and May 5, 2026. (3) Persistence: audit HKLM and HKCU autostart registry keys and scheduled tasks created in the April 8-May 5 window, particularly on systems where the installer ran. (4) Network: review proxy and firewall logs for outbound connections to unfamiliar destinations initiated by installer or post-install processes; flag HTTP/S sessions (T1071.001) with low-reputation or newly registered domains. (5) Process injection indicators: review EDR alerts for remote

thread creation or suspicious memory writes to legitimate host processes (T1055). Flag any findings for immediate escalation. Update detection rules when vendor or Kaspersky release confirmed hashes or C2 infrastructure.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`Not confirmed in available source data as of 2026-05-06`	Malicious DAEMON Tools Lite installer binary hashes not yet published by Disc Soft or Kaspersky	LOW
DOMAIN	`Not confirmed in available source data as of 2026-05-06`	C2 infrastructure domains not disclosed in current reporting	LOW
URL	`disc-soft.com — official distribution channel confirmed as the delivery vector during April 8–May 5, 2026`	Trojanized installers were served via the legitimate vendor website; any installer download from this domain in the exposure window should be treated as suspect	HIGH

Framework Mappings

MITRE-ATTACK

- **T1547** — Boot or Logon Autostart Execution
- **T1041** — Exfiltration Over C2 Channel
- **T1055** — Process Injection
- **T1071.001** — Web Protocols
- **T1195.002** — Compromise Software Supply Chain
- **T1033** — System Owner/User Discovery
- **T1204.002** — Malicious File
- **T1057** — Process Discovery
- **T1553.002** — Code Signing
- **T1036.001** — Invalid Code Signature
- **T1082** — System Information Discovery
- **T1059** — Command and Scripting Interpreter
- **T1105** — Ingress Tool Transfer

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring

- **SC-7** — Boundary Protection
- **AC-6** — Least Privilege
- **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

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **15.1** — Establish and Maintain an Inventory of Service Providers

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

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1547	Boot or Logon Autostart Execution	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1055	Process Injection	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1195.002	Compromise Software Supply Chain	Initial-Access
T1033	System Owner/User Discovery	Discovery
T1204.002	Malicious File	Execution
T1057	Process Discovery	Discovery
T1553.002	Code Signing	Defense-Evasion

Technique ID	Technique Name	Tactic
T1036.001	Invalid Code Signature	Defense-Evasion
T1082	System Information Discovery	Discovery
T1059	Command and Scripting Interpreter	Execution
T1105	Ingress Tool Transfer	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/daemon-tools-devs-co...	T3
	https://www.bleepingcomputer.com/news/security/daemon-tools-devs-co...	T3
	https://www.bleepingcomputer.com/news/security/chinese-hackers-brea...	T3
	https://www.bleepingcomputer.com/news/security/cloudflare-hacked-us...	T3
DAEMON Tools Software Hacked to Deliver Malware in a Supply ...	https://cybersecuritynews.com/daemon-tools-software-hacked/	T3

Generated 2026-05-06 18:51 UTC by TJS Security Command Center