INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 08:39 UTC

Signed DAEMON Tools Installers Weaponized in Ongoing Supply-Chain Campaign Targeting Government and Industry

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0278
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	DAEMON Tools versions 12.5.0.2421 through 12.5.0.2434 (DTHelper.exe, DiscSoftBusServiceLite.exe, DTShellHlp.exe)
Published	2026-05-05T15:21:18
Discovery Source	Rss

Executive Summary

Threat actors compromised the official DAEMON Tools distribution channel beginning April 8, 2026 (discovered approximately one month later in early May 2026), embedding a multi-stage backdoor into digitally signed installers across versions 12.5.0.2421 through 12.5.0.2434. The campaign exploited code-signing trust to bypass security controls, with second-stage payloads selectively deployed against government, scientific, retail, and manufacturing organizations, primarily in Russia, Belarus, and Thailand, though infections reached over 100 countries. Any organization that installed DAEMON Tools during this window faces potential system compromise, data exfiltration, and persistent backdoor access; the campaign was discovered after approximately one month of undetected activity.

Technical Analysis

Threat actors compromised the official DAEMON Tools distribution channel to deliver trojanized installers carrying a multi-stage backdoor. Affected versions: 12.5.0.2421 through 12.5.0.2434. Malicious components embedded in DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe. The attack exploited three weaknesses: CWE-693 (protection mechanism failure via trusted code-signing bypass), CWE-506 (embedded malicious code), and CWE-494 (download without integrity verification). MITRE ATT&CK coverage spans the full intrusion chain, initial access via compromised supply chain (T1195.002), signed binary proxy execution (T1553.002), obfuscated files (T1027, T1140), persistence via registry run keys (T1547.001), process injection (T1055), command execution (T1059), system and network discovery (T1082, T1016), non-application layer C2

(T1095), standard application layer C2 (T1071), ingress tool transfer (T1105), masquerading (T1036), and process discovery (T1057). Second-stage payloads were selectively deployed only to high-value targets, suggesting active operator triage. Threat actor attribution remains unconfirmed as of 2026-05-05. Linguistic and operational indicators suggest possible Chinese-speaking operators, but confidence is insufficient for formal attribution. No CVE assigned. No vendor patch advisory confirmed at time of reporting. Campaign undetected for approximately one month.

Action Checklist

1. Step 1: Containment, Immediately identify all systems where DAEMON Tools versions 12.5.0.2421 through 12.5.0.2434 were installed between April 8, 2026 and the date of discovery. Isolate those endpoints from the network pending investigation. Block execution of DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe from the affected version range via application control policies.
2. Step 2: Detection, Query endpoint telemetry and EDR for process creation events involving DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe originating from DAEMON Tools installer directories. Hunt for T1547.001 persistence artifacts: new or modified HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalents created in the April 8 to present timeframe. Look for anomalous outbound connections (T1095, T1071) from DAEMON Tools process trees. Consult Securelist for published IOCs including file hashes and C2 indicators (search-retrieved resource - validate URL before use).
3. Step 3: Eradication, Uninstall affected DAEMON Tools versions (12.5.0.2421-12.5.0.2434) on all identified systems. Do not reinstall from cached or previously downloaded installers. Verify any replacement installer hash against a clean, post-incident release from the vendor before deploying. Remove persistence registry entries identified during detection. Terminate and remove any secondary payloads identified through EDR forensics.
4. Step 4: Recovery, Reimage or perform full forensic validation on any system confirmed to have received a second-stage payload before returning to production. On systems where only the trojanized installer was present but no second-stage activity is confirmed, validate clean state via EDR and integrity tooling before reconnecting. Monitor for re-establishment of C2 channels (T1095, T1071) and reappearance of registry persistence (T1547.001) for a minimum of 30 days post-remediation.
5. Step 5: Post-Incident, This campaign exposed a control gap in software supply chain verification (CWE-494). Implement or audit software allowlisting policies that validate installer hashes prior to execution. Evaluate whether your procurement process enforces integrity verification for third-party utilities, including those with valid code-signing certificates. Review privileged system inventories for non-essential utilities like disk imaging tools and consider restricting installation to approved, internally mirrored repositories.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior leadership, legal counsel, and relevant ISAC (e.g., MS-ISAC or sector-specific) immediately if any system confirmed to have received the second-stage payload stores PII, PHI, classified information, OT/ICS connectivity, or government contract data, as the selective targeting of government and scientific organizations in this campaign and the CVSS 9.5 rating indicate a high likelihood of data exfiltration objectives that may trigger breach notification obligations.
Recovery Notes	Systems with confirmed second-stage payload delivery must be fully reimaged from known-good media — forensic validation alone is insufficient given the multi-stage backdoor architecture, which may establish persistence mechanisms beyond the initial Run key entries. Post-reimage, re-enroll systems into endpoint monitoring and validate Sysmon telemetry is flowing before reconnecting to production segments. Maintain active monitoring for C2 re-establishment and T1547.001 registry persistence re-creation for a minimum of 30 days, as this campaign's selective deployment pattern suggests threat actors may retain knowledge of high-value targets and attempt re-infection through alternative vectors.
Forensic Artifacts	Trojanized installer binary on disk — typically retained in '%UserProfile%\Downloads\' or software deployment cache — SHA-256 hash must be collected and compared against Kaspersky-published IOC hashes for DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe from versions 12.5.0.2421–12.5.0.2434; the valid Disc Soft code-signing certificate on a malicious binary is itself a high-fidelity artifact of this specific supply-chain attack | Windows Prefetch files at '%SystemRoot%\Prefetch\' for DTHELPER.EXE, DISCSOFTBUSSERVICELITE.EXE, and DTSHELLHLP.EXE — prefetch timestamps establish first and last execution dates critical to scoping the infection window relative to the April 8, 2026 campaign start date | Sysmon Event ID 13 (Registry Value Set) and Windows Security Event ID 4657 (Registry Value Modified) entries in 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' and 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' created or modified between April 8, 2026 and discovery — these represent the T1547.001 persistence artifacts left by the backdoor's second stage | Network traffic pcap or Sysmon Event ID 3 (Network Connection) records showing outbound connections from DTHelper.exe, DiscSoftBusServiceLite.exe, or DTShellHlp.exe process trees — destination IPs, domains, ports, and protocols are the primary C2 infrastructure artifacts for this campaign (T1095/T1071) and required for IOC sharing and firewall blocking | Second-stage payload files dropped to '%AppData%\Roaming\', '%ProgramData%\', or '%Temp%\ 'by the backdoor post-installer execution — collect full file metadata (path, SHA-256, creation timestamp, owner) and any associated scheduled task XML files under '%SystemRoot%\System32\Tasks\' created after April 8, 2026, which represent the multi-stage persistence and execution infrastructure beyond the initial Run key

Per-Action IR Details

Step 1: Containment — Immediately identify all systems where DAEMON Tools versions 12.5.0.2421 through 12.5.0.2434 were installed between April 8, 2026 and the date of discovery. Isolate those endpoints from the network pending investigation. Block execution of DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe from the affected version range via application control policies.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SI-3 (Malicious Code Protection), CIS 2.3 (Address Unauthorized Software), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Use 'Get-WmiObject Win32_Product | Where-Object {$_.Name -like "*DAEMON Tools*"}' across endpoints via PSRemoting to enumerate installs. Cross-reference install timestamps against April 8, 2026 using

'Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*' for InstallDate fields. Block the three binaries via Windows Defender Application Control (WDAC) WDAC policy or Software Restriction Policies using their known paths: '%ProgramFiles%\DAEMON Tools Lite\DTHelper.exe', 'DiscSoftBusServiceLite.exe', and 'DTShellHlp.exe'. Isolate affected hosts using a host-based firewall rule: 'netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound' until investigated.

Evidence: Before isolating, capture: full memory dump using ProcDump or WinPmem ('winpmem_mini_x64.exe memdump.raw') to preserve any in-memory second-stage payload resident in DTHelper.exe or DiscSoftBusServiceLite.exe process space; Windows Prefetch files at '%SystemRoot%\Prefetch\DTHELPER.EXE-*.pf' and equivalents for the other two binaries to establish first and last execution timestamps; installer file hash ('Get-FileHash -Algorithm SHA256 ') compared against known-bad hashes from the Kaspersky/Securelist advisory; and current active network connections from affected processes ('Get-NetTCPConnection | Where-Object {$_.OwningProcess -in (Get-Process DTHelper,DiscSoftBusServiceLite,DTShellHlp).Id}') before network isolation severs C2 visibility.

Step 2: Detection — Query endpoint telemetry and EDR for process creation events involving DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe originating from DAEMON Tools installer directories. Hunt for T1547.001 persistence artifacts: new or modified HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalents created in the April 8 to present timeframe. Look for anomalous outbound connections (T1095, T1071) from DAEMON Tools process trees. Check Securelist (https://securelist.com/tr/daemon-tools-backdoor/119654/) for published IOCs including file hashes and C2 indicators — treat as search-retrieved URLs requiring human validation.

NIST Phase: Detection Analysis

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a config that captures Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Value Set). Query Sysmon operational log: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -match "DTHelper|DiscSoftBusServiceLite|DTShellHlp"}'. For T1547.001 registry persistence, run: 'reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run' and 'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and filter entries with timestamps post-April 8, 2026 using 'reg query' combined with autoruns.exe (Sysinternals) with '/accepteula /a /c /h /s' to export and diff against a known-good baseline. For C2 hunting (T1095/T1071) without EDR, capture 10-minute pcap per suspect host using 'tshark -i -w daemontools_suspect.pcap -f "host "' and filter for non-browser processes making HTTP/S or raw TCP connections. Write a YARA rule targeting the trojanized installer by hashing DTHelper.exe from the affected version range and scanning with 'yara64.exe rule.yar C:\Program Files\DAEMON Tools Lite\'.

Evidence: Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on parent processes matching DTHelper.exe, DiscSoftBusServiceLite.exe, or DTShellHlp.exe to identify any child processes spawned by the backdoor — unexpected cmd.exe, powershell.exe, or rundll32.exe children are high-fidelity indicators. Export Sysmon Event ID 13 (Registry Value Set) entries targeting 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' and 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' with timestamps between April 8, 2026 and discovery date. Extract Windows DNS Client Event Log (Microsoft-Windows-DNS-Client/Operational) for resolution of domains made by DAEMON Tools process PIDs — this campaign's C2 infrastructure would appear as DNS queries from the DTHelper.exe process space. Collect Sysmon Event ID 3 (Network Connection) records for outbound connections initiated by any of the three affected binaries, noting destination IP, port, and protocol to identify T1095 (non-application-layer protocol) or T1071 (application-layer protocol) C2 channels.

Step 3: Eradication — Uninstall affected DAEMON Tools versions (12.5.0.2421–12.5.0.2434) on all identified systems. Do not reinstall from cached or previously downloaded installers. Verify any replacement installer hash against a clean, post-incident release from the vendor before deploying. Remove persistence registry

entries identified during detection. Terminate and remove any secondary payloads identified through EDR forensics.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Uninstall via 'wmic product where name="DAEMON Tools Lite" call uninstall /nointeractive' and confirm removal with 'Get-WmiObject Win32_Product | Where-Object {$_.Name -like '*DAEMON*'}'. Verify no DTHelper.exe, DiscSoftBusServiceLite.exe, or DTShellHlp.exe binaries remain under '%ProgramFiles%', '%ProgramFiles(x86)%', '%AppData%', or '%Temp%' using 'Get-ChildItem -Path C:\ -Recurse -Filter "DTHelper.exe" -ErrorAction SilentlyContinue'. Before deploying any replacement installer, compute SHA-256 ('certutil -hashfile SHA256') and compare against the vendor-published hash from the official Disc Soft release announcement post-April 8, 2026 incident — do not trust any installer downloaded prior to vendor confirmation of a clean build. Remove identified Run key persistence entries with 'reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v /f'. For second-stage payloads identified in memory or on disk, use ClamAV ('clamscan -r --remove=yes C:\ --log=clamscan_output.txt') as a secondary sweep after manual removal.

Evidence: Before uninstalling, image the full installer binary ('DTSetup.exe' or equivalent) from its download cache location — typically '%UserProfile%\Downloads\' or '%Temp%\' — and preserve SHA-256 hash as evidence of the trojanized version. Capture the complete registry export of both Run key hives ('reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run run_hkcu_pre_eradication.reg') prior to deletion to document persistence mechanisms. Enumerate and hash all files dropped by the secondary payload in '%AppData%\Roaming\', '%ProgramData%\', and any scheduled task XML files under '%SystemRoot%\System32\Tasks\' that were created or modified after April 8, 2026, as the multi-stage backdoor would have staged additional components in these locations. Document all active scheduled tasks ('schtasks /query /fo LIST /v > scheduled_tasks_pre_eradication.txt') before removal.

Step 4: Recovery — Reimage or perform full forensic validation on any system confirmed to have received a second-stage payload before returning to production. On systems where only the trojanized installer was present but no second-stage activity is confirmed, validate clean state via EDR and integrity tooling before reconnecting. Monitor for re-establishment of C2 channels (T1095, T1071) and reappearance of registry persistence (T1547.001) 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 SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For systems requiring forensic validation rather than reimage, run Sysinternals Autoruns ('autorunsc.exe -a * -c -h -s -user * > autoruns_post_eradication.csv') and diff against a known-good baseline to confirm no residual T1547.001 persistence. Validate binary integrity of OS system files using 'sfc /scannow' and 'DISM /Online /Cleanup-Image /RestoreHealth'. For 30-day post-remediation monitoring without EDR, schedule a daily Sysmon log export and PowerShell script to alert on any new Run key entries or outbound connections from DAEMON Tools install paths: 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational -FilterXPath "*[System[EventID=13] and EventData[Data[@Name=\'TargetObject\'] and contains(.,\'CurrentVersion\\Run\')]]]'". Deploy a YARA rule scanning '%AppData%', '%ProgramData%', and '%Temp%' weekly for second-stage payload signatures derived from Kaspersky IOCs.

Evidence: Capture a post-eradication memory dump on any system that received a confirmed second-stage payload, using WinPmem, to verify no resident implant survives in process space before reconnection. Run 'netstat -anob > netstat_post_recovery.txt' at reconnection and at 24-hour intervals for the first week to detect any re-establishment of C2 channels characteristic of this campaign's T1095/T1071 infrastructure. Preserve Windows Event Log archives (Security, System, Sysmon Operational) from the full April 8, 2026 through remediation window as chain-of-custody

evidence — export with 'wevtutil epl Security Security_archive.evtx' — before log rotation discards them.

Step 5: Post-Incident — This campaign exposed a control gap in software supply chain verification (CWE-494). Implement or audit software allowlisting policies that validate installer hashes prior to execution. Evaluate whether your procurement process enforces integrity verification for third-party utilities, including those with valid code-signing certificates. Review privileged system inventories for non-essential utilities like disk imaging tools and consider restricting installation to approved, internally mirrored repositories.

NIST Phase: Post Incident

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

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST SA-12 (Supply Chain Protection), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Establish an internally mirrored software repository (Nexus Repository OSS is free) for approved third-party utilities including disk imaging tools, and enforce downloads exclusively from the mirror. Implement a pre-execution hash verification script: 'certutil -hashfile SHA256' compared against a manually curated allowlist CSV maintained by the security team. Configure WDAC or AppLocker to block any executable not matching a known-good publisher certificate AND hash — this directly addresses the attack vector here, where a valid Disc Soft certificate was abused, meaning certificate trust alone is insufficient and hash pinning is required. Add a Sigma rule (free, community-supported) for Sysmon that alerts on any new installer execution from '%UserProfile%\Downloads\' or '%Temp%\' matching DAEMON Tools naming patterns. Document the procurement gap in the lessons-learned report and require the IT procurement policy to mandate SHA-256 hash verification against vendor-published values for all new third-party utility installations.

Evidence: Produce a full timeline of installer distribution and execution across the environment — correlate Software Inventory logs, Windows Installer Event Log (Event ID 1040/1042 in Application log), and deployment system records (SCCM/Intune if available, or manual PSRemoting query results) to establish scope of exposure for the lessons-learned report. Document the code-signing certificate serial number from the trojanized DTHelper.exe ('sigcheck.exe -i DTHelper.exe') to inform future certificate-pinning and allowlisting policies and to share as an IOC with ISACs or CISA if applicable. Archive all forensic artifacts — memory dumps, registry exports, pcap files, Sysmon logs, and hashes — with chain-of-custody documentation per NIST IR-4 (Incident Handling) requirements before case closure.

Detection Guidance

Primary hunt targets: process trees spawned by DTHelper.exe, DiscSoftBusServiceLite.exe, and DTShellHlp.exe in DAEMON Tools version directories installed between April 8, 2026 and present. Look for child process creation (T1059), injection into other processes (T1055), and outbound network connections (T1071, T1095) originating from these binaries. Check for registry modifications under HKCU and HKLM run keys (T1547.001) timestamped to the installation window. Query file system for dropped executables in temp or appdata paths created shortly after DAEMON Tools installer execution. Review DNS and proxy logs for anomalous domains contacted by DAEMON Tools process trees. Kaspersky's Securelist published technical indicators for this campaign; consult https://securelist.com/tr/daemon-tools-backdoor/119654/ for current IOC sets including file hashes and C2 infrastructure (search-retrieved URL; validate before use). SIEM rule tuning should prioritize detection of masquerading (T1036) and obfuscated payload execution (T1027, T1140) in the context of trusted installer processes.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`[See Securelist publication for confirmed file hashes — not reproduced here to avoid transcription error]`	Malicious DTHelper.exe, DiscSoftBusServiceLite.exe, DTShellHlp.exe from affected installer versions 12.5.0.2421–12.5.0.2434	HIGH
DOMAIN	`[See Securelist publication for confirmed C2 domains]`	Command-and-control infrastructure used by the backdoor for non-application and application layer C2 (T1095, T1071)	HIGH
URL	`https://securelist.com/tr/daemon-tools-backdoor/119654/`	Kaspersky Securelist primary technical analysis — source for confirmed IOCs including hashes and C2 indicators. Search-retrieved URL — validate before use.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1055** — Process Injection
- **T1027** — Obfuscated Files or Information
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1082** — System Information Discovery
- **T1016** — System Network Configuration Discovery
- **T1095** — Non-Application Layer Protocol
- **T1140** — Deobfuscate/Decode Files or Information
- **T1553.002** — Code Signing
- **T1195.002** — Compromise Software Supply Chain
- **T1105** — Ingress Tool Transfer
- **T1036** — Masquerading
- **T1071** — Application Layer Protocol
- **T1057** — Process Discovery
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes

- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **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
- **8.2** — Collect Audit Logs

ISO-27001-2022

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

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1055	Process Injection	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1082	System Information Discovery	Discovery
T1016	System Network Configuration Discovery	Discovery
T1095	Non-Application Layer Protocol	Command-And-Control
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion
T1553.002	Code Signing	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1036	Masquerading	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1057	Process Discovery	Discovery
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/daemon-tools-trojani...	T3
Government, Scientific Entities Hit via Daemon Tools Supply Chain ...	https://www.securityweek.com/government-scientific-entities-hit-via...	T3
DAEMON Tools Supply Chain Attack Compromises Official Installers ...	https://thehackernews.com/2026/05/daemon-tools-supply-chain-attack....	T3
Popular Daemon Tools utility exploited in supply chain attack	https://www.techzine.eu/news/security/141034/popular-daemon-tools-u...	T3
Popular DAEMON Tools software compromised | Securelist	https://securelist.com/tr/daemon-tools-backdoor/119654/	T3

Generated 2026-05-06 08:39 UTC by TJS Security Command Center