INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-08 19:04 UTC

DAEMON Tools Supply Chain Attack Deploys Backdoors to High-Value Targets

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0294
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	DAEMON Tools versions 12.5.0.2421 through 12.5.0.2434 (patched in 12.6.0.2445)
Published	2026-05-08
Discovery Source	Gemini

Executive Summary

Attackers compromised the official DAEMON Tools distribution channel between April 8, 2026 and the release of version 12.6.0.2445, embedding backdoors in legitimate software installers. The campaign selectively delivered advanced malware only to high-value targets in government, retail, scientific research, and manufacturing sectors across Russia, Belarus, and Thailand, indicating a disciplined, intelligence-driven operation rather than opportunistic mass infection. Organizations that installed affected versions (12.5.0.2421 through 12.5.0.2434) from the official source may have persistent, undetected access present on their systems.

Technical Analysis

Kaspersky researchers identified trojanized DAEMON Tools installers distributed from the official vendor website beginning April 8, 2026. Affected versions span 12.5.0.2421 through 12.5.0.2434. The attack chain exploits the software supply chain (T1195.002) by replacing legitimate installers with modified builds containing embedded malicious code (CWE-506). Payloads employed obfuscation (T1027, CWE-693), command-and-control communications over application-layer protocols (T1071), scripting engine abuse for execution (T1059), and masquerading techniques (T1036). Staged delivery (CWE-494) ensured advanced backdoors reached only pre-selected high-value targets, reducing forensic visibility across the broader victim pool. No official CVSS or CVE identifier has been assigned; qualitative severity is assessed editorially as 'high' based on scope and targeting. No confirmed threat actor attribution is available. The vendor released a remediated version, 12.6.0.2445, to address the compromise. Primary investigative reporting from Kaspersky; published reporting available through T3 news aggregation sources cited below. Direct access to Kaspersky's official threat intelligence advisory is recommended for operational use. Human verification against the

authoritative Kaspersky advisory is mandatory before production action.

Action Checklist

1. Containment. Immediately isolate any host where DAEMON Tools versions 12.5.0.2421 through 12.5.0.2434 was installed from the official website after April 8, 2026. Treat these systems as potentially compromised. Block outbound communications from affected hosts pending investigation, referencing C2 indicators published in the Kaspersky advisory.
2. Detection. Query endpoint telemetry and EDR logs for DAEMON Tools installer execution events dated April 8, 2026 onward. Review process trees spawned by the DAEMON Tools installer process for unexpected child processes (T1059), anomalous network connections (T1071), and masquerading artifacts (T1036). Cross-reference file hashes of installed binaries against known-good hashes from version 12.6.0.2445 or pre-April 8 builds. Pull any IOCs published in the Kaspersky report and run retroactive SIEM queries.
3. Eradication. Upgrade all installations to DAEMON Tools 12.6.0.2445 from the vendor's official channel, verifying installer integrity via hash before execution. On hosts confirmed or suspected to have run a trojanized installer, assume persistent access and conduct full forensic triage before re-imaging or restoring from a pre-April 8, 2026 clean backup.
4. Recovery. After re-imaging or upgrading affected systems, validate that no scheduled tasks, registry run keys, or service entries associated with the backdoor payload persist. Monitor outbound network traffic from previously affected hosts for at least 30 days for C2 reconnection attempts. Confirm software inventory reflects only version 12.6.0.2445 or later.
5. Post-Incident. Review software procurement and update processes to require hash verification against vendor-published values before installer execution. Evaluate whether software allowlisting or application control policies would have blocked the trojanized installer. Assess whether third-party software ingestion paths (automated deployment pipelines, IT provisioning scripts) bypass manual integrity checks, and close that gap.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if any host confirmed to have executed a trojanized DAEMON Tools installer (versions 12.5.0.2421–12.5.0.2434 installed after April 8, 2026) is identified as processing PII, PHI, classified government data, or intellectual property, as the intelligence-driven targeting profile of this campaign suggests exfiltration of high-value data may have occurred, triggering breach notification obligations under GDPR, HIPAA, or applicable national regulations.

Recovery Notes	Re-image all confirmed and suspected hosts from verified pre-April 8, 2026 backups rather than attempting in-place remediation, as the backdoor's persistence mechanisms and full capability set may not yet be fully characterized in public reporting. Monitor outbound network connections from all previously affected hosts for a minimum of 30 days post-recovery, with daily review of DNS queries and TCP connections against Kaspersky's published C2 indicator set, watching specifically for low-and-slow beaconing patterns consistent with an intelligence-driven APT maintaining dormant access. Verify clean state on recovered hosts by re-running hash checks against all DAEMON Tools binaries and auditing scheduled tasks, services, and registry Run keys immediately after reimaging and again at 7-day intervals for the first month.
Forensic Artifacts	Trojanized DAEMON Tools installer binary: Recover from %USERPROFILE%\Downloads\, Windows Installer cache (%WINDIR%\Installer\), or browser download history; compute SHA-256 and compare against Kaspersky-published malicious installer hashes for versions 12.5.0.2421–12.5.0.2434 distributed after April 8, 2026. | Sysmon Event ID 1 (Process Create) and Windows Security Event ID 4688 process creation records: Filter on parent processes matching the DAEMON Tools installer executable to identify backdoor dropper child processes spawned during or after installation, with timestamps between April 8, 2026 and detection date. | Windows registry persistence keys: Examine HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, and HKLM\SYSTEM\CurrentControlSet\Services for entries created within 60 minutes of the trojanized installer execution timestamp, as the backdoor payload would establish persistence through one of these standard mechanisms. | Memory image of affected host (captured via WinPmem before isolation): Analyze for injected backdoor shellcode or DLLs loaded into legitimate processes (e.g., DTAgent.exe or svchost.exe) using Volatility3 plugins `windows.malfind` and `windows.dlllist`, which would reveal in-memory backdoor components not present on disk if a fileless stage was used. | Network traffic PCAP from the affected host's egress interface (captured via Wireshark or tcpdump before isolation): Filter on outbound connections from DTAgent.exe PID or its child processes to identify C2 beacon traffic, focusing on periodic outbound HTTP/HTTPS connections to non-DAEMON Tools infrastructure or DNS queries to domains matching Kaspersky-published indicators from this campaign.

Per-Action IR Details

Containment — Immediately isolate any host where DAEMON Tools versions 12.5.0.2421 through 12.5.0.2434 was installed from the official website after April 8, 2026. Treat these systems as potentially compromised. Block outbound communications from affected hosts pending investigation, referencing C2 indicators published in the Kaspersky advisory.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without enterprise NAC, use Windows Firewall via GPO or local PowerShell to block all outbound traffic on affected hosts: `New-NetFirewallRule -DisplayName 'DAEMON-C2-Block' -Direction Outbound -Action Block -Enabled True`. Simultaneously null-route Kaspersky-published C2 IPs/domains at the perimeter firewall or DNS layer using your router's ACL. For Linux hosts: `iptables -I OUTPUT -j DROP && iptables -I INPUT -j DROP` — keep only management SSH open for forensic access.

Evidence: Before isolating, capture a full volatile memory image using WinPmem (free) to preserve any in-memory backdoor code injected by the trojanized DAEMON Tools installer. Run `netstat -ano` and document all active

outbound connections, paying specific attention to established sessions from DTAgent.exe, DTShellHlp.exe, or any process spawned by the DAEMON Tools installer PID. Export the current Windows Security Event Log and capture all DNS query logs from the host's resolver cache (`ipconfig /displaydns`) before network isolation severs DNS resolution evidence.

Detection — Query endpoint telemetry and EDR logs for DAEMON Tools installer execution events dated April 8, 2026 onward. Review process trees spawned by the DAEMON Tools installer process for unexpected child processes (T1059), anomalous network connections (T1071), and masquerading artifacts (T1036). Cross-reference file hashes of installed binaries against known-good hashes from version 12.6.0.2445 or pre-April 8 builds. Pull any IOCs published in the Kaspersky report and run retroactive SIEM queries.

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), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR, deploy Sysmon with SwiftOnSecurity's config and query Event ID 1 (Process Create) filtering on ParentImage paths matching the DAEMON Tools installer executable (typically `%ProgramFiles%\DAEMON Tools Lite\` or the installer temp extraction path under `%TEMP%`). Use Get-WinEvent in PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'daemon'}`. Compute SHA-256 hashes of all files in the DAEMON Tools installation directory using `Get-FileHash -Algorithm SHA256 -Path 'C:\Program Files\DAEMON Tools Lite\*' -Recurse` and diff against the Kaspersky-published IOC hash list. Write a YARA rule targeting the trojanized installer's embedded backdoor dropper based on Kaspersky's published string indicators.

Evidence: Query Windows Security Event Log for Event ID 4688 (Process Creation) or Sysmon Event ID 1 filtering on processes spawned by the DAEMON Tools installer PID (DTLiteInstaller.exe or similar) between April 8, 2026 and the date of version 12.6.0.2445 deployment. Capture Sysmon Event ID 3 (Network Connection) records showing outbound connections from DTAgent.exe or any child process spawned by the installer. Retrieve the original installer binary from browser download history paths (`%USERPROFILE%\Downloads\`), Windows Installer cache (`%WINDIR%\Installer\`), or Prefetch entries (`%WINDIR%\Prefetch\DTLITEINSTALLER*.pf`) to hash-verify against the Kaspersky-published malicious installer hashes. Check Windows Event ID 7045 (New Service Installed) for any service registered within 60 minutes of the trojanized installer execution.

Eradication — Upgrade all installations to DAEMON Tools 12.6.0.2445 from the vendor's official channel, verifying installer integrity via hash before execution. On hosts confirmed or suspected to have run a trojanized installer, assume persistent access and conduct full forensic triage before re-imaging or restoring from a pre-April 8, 2026 clean backup.

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-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Verify the SHA-256 hash of the DAEMON Tools 12.6.0.2445 installer before execution using `certutil -hashfile DTLite12.6.0.2445.exe SHA256` (Windows) or `sha256sum DTLite12.6.0.2445.exe` (Linux/WSL) and compare against the value published on the Disc Soft official site. For confirmed-compromise hosts, do not attempt in-place remediation — preserve a forensic disk image using FTK Imager (free) or `dd` before wiping. Restore from a verified pre-April 8, 2026 backup snapshot and use osquery to confirm no persistence mechanisms remain: `SELECT * FROM scheduled_tasks; SELECT * FROM services; SELECT * FROM registry WHERE key LIKE 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run%';`

Evidence: Before re-imaging, capture the full registry hive set (SYSTEM, SOFTWARE, NTUSER.DAT for all user profiles, SAM, SECURITY) using `reg export` or FTK Imager's logical acquisition to preserve backdoor persistence keys written by the DAEMON Tools trojanized installer payload. Document all scheduled tasks (`schtasks /query /fo

LIST /v > tasks_before_wipe.txt`) and Windows services (`sc query type= all state= all > services_before_wipe.txt`) as the backdoor likely established persistence via one of these mechanisms. Collect the full contents of `%APPDATA%`, `%LOCALAPPDATA%`, and `%PROGRAMDATA%` directories for any files written by the malicious installer payload within 24 hours of its execution timestamp, using `forfiles` or a timeline built with Eric Zimmerman's MFTECmd against the $MFT.

Recovery — After re-imaging or upgrading affected systems, validate that no scheduled tasks, registry run keys, or service entries associated with the backdoor payload persist. Monitor outbound network traffic from previously affected hosts for at least 30 days for C2 reconnection attempts. Confirm software inventory reflects only version 12.6.0.2445 or later.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Run osquery on restored hosts to verify clean state: `SELECT name, path, source FROM scheduled_tasks;` and `SELECT name, path, start_type FROM services WHERE path LIKE '%appdata%' OR path LIKE '%temp%';`. Configure Sysmon Event ID 3 (Network Connection) logging with output to a local EVTX file, then use a daily PowerShell cron job to extract and review outbound connections to IPs/domains matching the Kaspersky C2 indicator list for 30 days post-recovery. Use `Get-Package` or `wmic product get name,version` to audit the DAEMON Tools version across all hosts and confirm no 12.5.0.2421–12.5.0.2434 installs remain.

Evidence: Query Sysmon Event ID 22 (DNS Query) on recovered hosts for 30 days post-reimaging, specifically filtering on domains matching Kaspersky-published C2 infrastructure associated with this campaign — C2 reconnection is expected if any persistence mechanism was missed during eradication. Review Windows Security Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) post-recovery to catch any re-establishment of backdoor persistence. Validate software inventory by computing SHA-256 of the DTAgent.exe binary on each recovered host and confirming it matches the vendor-published hash for version 12.6.0.2445.

Post-Incident — Review software procurement and update processes to require hash verification against vendor-published values before installer execution. Evaluate whether software allowlisting or application control policies would have blocked the trojanized installer. Assess whether third-party software ingestion paths (automated deployment pipelines, IT provisioning scripts) download and execute binaries without integrity verification, and close that gap.

NIST Phase: Post Incident

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

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST SI-2 (Flaw Remediation), NIST IR-8 (Incident Response Plan), NIST CM-3 (Configuration Change Control), 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), CIS 2.3 (Address Unauthorized Software)

Compensating: Implement a mandatory pre-execution hash verification step in all deployment scripts by wrapping installer invocations in a PowerShell function that computes SHA-256 and compares against a hardcoded expected value before allowing execution — abort and alert if mismatch is detected. Deploy AppLocker (built into Windows Enterprise/Education) or Windows Defender Application Control (WDAC) with a publisher-based rule requiring code-signing certificates from Disc Soft Ltd; the trojanized DAEMON Tools installers in this campaign may share the same Authenticode signature as legitimate builds, so also enforce hash-pinning for this specific application. Codify the hash verification procedure in a runbook stored in your ITSM tool so every software deployment — manual or scripted — follows the same integrity gate.

Evidence: Retrieve deployment pipeline logs, IT provisioning scripts, and any SCCM/Ansible/Chef/Puppet job histories that executed DAEMON Tools installer downloads between April 8 and the patching date to determine the blast radius of automated deployment paths that lacked hash verification — this establishes whether the trojanized installer was distributed enterprise-wide via tooling rather than individual user downloads. Review software allowlisting policy logs

(AppLocker event log: `Applications and Services Logs\Microsoft\Windows\AppLocker`) to determine whether a policy existed and whether it would have permitted or blocked the trojanized installer based on its Authenticode signature or file path.

Detection Guidance

Primary detection pivot: identify hosts where a DAEMON Tools installer (versions 12.5.0.2421-12.5.0.2434) executed between April 8, 2026 and the patch date. In EDR/SIEM, query for process creation events where the parent is the DAEMON Tools installer and children are cmd.exe, powershell.exe, wscript.exe, or other scripting hosts (T1059). Look for outbound connections from dtlite.exe or associated installer processes to non-DAEMON Tools infrastructure (T1071). Flag any file writes to startup locations, scheduled task creation, or service installation events tied to the installer process chain (T1036, T1027). Hash comparison: pull SHA-256 hashes of installed DAEMON Tools binaries and compare against vendor-published hashes for 12.6.0.2445. Mismatches in the affected version range are high-confidence indicators. Retrieve and operationalize IOC lists (file hashes, domains, IPs) from the Kaspersky advisory directly; specific IOC values are not independently verified in available T3 sources and should not be assumed complete.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Official DAEMON Tools website (daemontools.com installer distribution path)`	Trojanized installers for versions 12.5.0.2421–12.5.0.2434 were distributed from the official vendor site beginning April 8, 2026. Specific malicious URLs not independently verified from available T3 sources — retrieve from Kaspersky advisory.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1027** — Obfuscated Files or Information
- **T1071** — Application Layer Protocol
- **T1059** — Command and Scripting Interpreter
- **T1036** — Masquerading
- **T1195.002** — Compromise Software Supply Chain

NIST-800-53R5

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

- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **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
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **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
T1027	Obfuscated Files or Information	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1059	Command and Scripting Interpreter	Execution
T1036	Masquerading	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access

Sources

Source	URL	Tier
gemini	https://industrialcyber.co/kaspersky-uncovers-targeted-daemon-tools...	T3

Source	URL	Tier
Government, Scientific Entities Hit via Daemon Tools Supply Chain ...	https://standbywithme.blog/2026/05/75693175.html	T3
BeyondMachines :verified: (@beyondmachines1@infosec.exchange)	https://infosec.exchange/@beyondmachines1	T3
A new malware has been discovered that can turn network devices ...	https://www.instagram.com/p/DW650v_k9re/	T3
InfoSec Briefing - May 06, 2026	https://briefing.workshop1.net/html/briefing-2026-05-06.html	T3

Generated 2026-05-08 19:04 UTC by TJS Security Command Center