INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-12 06:02 UTC

Trusted Hardware Utility Site Weaponized: STX RAT Delivered via DLL Side-Loading in 19-Hour CPUID Compromise

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0168
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	CPUID CPU-Z, HWMonitor, HWMonitor Pro, PerfMonitor (cpuid.com downloads), all versions served during approximately 19-hour compromise window (April 9-10, 2026 UTC)
Published	2026-04-12T01:54:00
Discovery Source	Rss

Executive Summary

Between April 9-10, 2026, attackers breached cpuid.com for approximately 19 hours and replaced legitimate download links for CPU-Z, HWMonitor, HWMonitor Pro, and PerfMonitor with malware-laced installers. Any user or IT professional who downloaded these tools during that window likely received STX RAT, a remote access trojan giving attackers persistent control over the infected system. Organizations in retail, manufacturing, consulting, telecommunications, and agriculture are confirmed affected, with over 150 victims identified by Kaspersky; the primary business risk is unauthorized remote access to internal systems, credential theft, and potential lateral movement.

Technical Analysis

Threat actors compromised cpuid.com and substituted trojanized installers for four utilities: CPU-Z, HWMonitor, HWMonitor Pro, and PerfMonitor. The malicious installers deploy STX RAT via DLL side-loading (T1574.002 / CWE-426), placing a malicious DLL in a search-order-vulnerable load path used by a legitimate, signed executable. This technique abuses application trust to execute malicious code without triggering standard process-level detections. The infection chain also incorporates process injection (T1055), PowerShell execution (T1059.001), drive-by compromise via the weaponized site (T1189), supply chain compromise at the software distribution layer (T1195.002), keylogging or input capture (T1056), sandbox/VM evasion (T1497), and C2 over HTTP/S (T1071.001). Infrastructure and infection chain were reused verbatim from a prior FileZilla watering hole campaign, indicating operational reuse. Relevant CWEs: CWE-829 (inclusion of functionality from untrusted

control sphere), CWE-494 (download of code without integrity check), CWE-426 (untrusted search path). No CVE is assigned. The site has been remediated; no patch exists for the affected tools because the vulnerability was in the distribution channel, not the software itself. Confidence: HIGH, sourced from Kaspersky Securelist primary research.

Action Checklist

1. Containment: Immediately isolate any endpoint that downloaded CPU-Z, HWMonitor, HWMonitor Pro, or PerfMonitor from cpuid.com between April 9-10, 2026 UTC. Block outbound C2 connections at the perimeter by querying your DNS and proxy logs for domains and IPs associated with STX RAT (see Kaspersky Securelist report for IOC list). Revoke credentials stored or entered on suspected compromised hosts.
2. Detection: Search endpoint logs, EDR telemetry, and proxy/DNS logs for downloads from cpuid.com during the compromise window. Look for DLL side-loading indicators: unexpected DLLs loaded by CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe processes. Hunt for PowerShell child processes spawned by these executables (T1059.001). Cross-reference file hashes of installed binaries against known-good hashes published in the Kaspersky Securelist report.
3. Eradication: On confirmed-infected hosts: terminate and remove STX RAT and associated DLL. Uninstall all cpuid.com utilities downloaded during the compromise window. Re-download tools only from the current cpuid.com site after verifying file integrity against hashes published post-remediation. Rebuild hosts where full infection scope cannot be confirmed.
4. Recovery: After reimaging or cleaning affected hosts, reset all credentials that were entered on or accessible from those systems. Monitor for re-infection indicators for at least 30 days post-remediation. Validate that no persistence mechanisms (scheduled tasks, registry run keys, injected processes) remain. Confirm C2 blocking rules are active and generating no new hits.
5. Post-Incident: This attack exploited the absence of download integrity verification (CWE-494) and software distribution trust assumptions. Implement a software allowlist policy requiring hash verification before execution of downloaded utilities. Evaluate whether IT and engineering teams use hardware diagnostic utilities from unmanaged personal devices, which would fall outside EDR coverage. Consider requiring all utility software to be distributed through an internal, hash-verified repository rather than direct vendor download.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if any confirmed-infected host had access to PII, PHI, PCI-scoped systems, or privileged credentials (domain admin, service accounts), as STX RAT's persistent remote access capability creates a presumptive data exposure requiring breach notification assessment under applicable regulations (GDPR, HIPAA, state breach laws); also escalate if the blast radius cannot be bounded within 4 hours due to missing proxy/DNS log coverage.

Recovery Notes	After reimaging or cleaning, reinstall CPUID utilities exclusively from hashes published by cpuid.com post-incident and verify with Get-FileHash before first execution — do not trust any installer cached locally or on file shares during the April 9–10 window. Monitor all previously infected hosts for 30 days using Sysmon Event ID 7 (Image Loaded) and Event ID 1 (Process Create) for recurrence of the DLL side-loading pattern, as STX RAT may have established secondary persistence mechanisms not removed during initial eradication. Validate that all STX RAT C2 IOC blocking rules at the DNS and perimeter firewall layers are generating zero new resolution or connection hits before closing the incident.
Forensic Artifacts	Malicious installer files: SHA-256 hashes of CPU-Z, HWMonitor, HWMonitor Pro, or PerfMonitor installers downloaded from cpuid.com between April 9–10, 2026 UTC — compare against Kaspersky Securelist known-bad hashes to confirm trojanized versions were received. | DLL side-loading evidence: files in the CPUID application install directories (e.g., '%ProgramFiles%\CPUID\CPU-Z\', '%ProgramFiles%\CPUID\HWMonitor\') that are not signed by CPUID SA or that have SHA-256 hashes matching STX RAT-associated DLLs listed in the Kaspersky Securelist report. | Process ancestry logs: Sysmon Event ID 1 or Windows Security Event ID 4688 entries showing PowerShell.exe, cmd.exe, or unknown executables spawned as child processes of CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe — this parent-child relationship is the behavioral signature of the DLL side-loading execution chain. | Network C2 artifacts: DNS query logs (Sysmon Event ID 22 or DNS server query logs) and proxy access logs showing outbound connections to STX RAT C2 infrastructure domains and IPs sourced from the Kaspersky Securelist IOC list, with timestamps correlating to or following the CPUID utility download event. | Persistence registry keys and scheduled tasks: contents of 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' and 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run', plus output of 'schtasks /query /fo LIST /v' filtered for tasks created on or after April 9, 2026, referencing paths associated with the STX RAT executable or its dropped DLL.

Per-Action IR Details

Containment — Immediately isolate any endpoint that downloaded CPU-Z, HWMonitor, HWMonitor Pro, or PerfMonitor from cpuid.com between April 9–10, 2026 UTC. Block outbound C2 connections at the perimeter by querying your DNS and proxy logs for domains and IPs associated with STX RAT (see Kaspersky Securelist report for IOC list). Revoke credentials stored or entered on suspected compromised hosts.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), CIS 12.8 (Establish and Maintain Dedicated Computing Resources for All Administrative Work), CIS 13.4 (Perform Traffic Filtering Between Network Segments)

Compensating: For teams without NAC or enterprise EDR: use Windows Firewall to hard-block the host at the OS level via 'netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound' on suspect endpoints while investigation proceeds. For perimeter C2 blocking without a SIEM, extract STX RAT IOC domains and IPs from the Kaspersky Securelist report and push them as deny rules to your perimeter firewall or DNS resolver (e.g., add NXDOMAIN overrides in BIND or Windows DNS for known C2 hostnames). Use 'netstat -ano' on isolated hosts to capture active connections before blocking to preserve evidence of live C2 channels.

Evidence: Capture before isolating: full memory dump of any process spawned by CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe (use ProcDump: 'procdump -ma '); browser download history confirming cpuid.com download URL and timestamp within the April 9–10 UTC window; Windows proxy/DNS logs showing outbound resolution of STX RAT C2 domains at time of infection; 'netstat -ano' output preserving active C2 connections tied to the malicious process PID; and Windows Security Event Log Event ID 4688 (Process Creation) filtered on the

four affected executables as parent processes.

Detection — Search endpoint logs, EDR telemetry, and proxy/DNS logs for downloads from cpuid.com during the compromise window. Look for DLL side-loading indicators: unexpected DLLs loaded by CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe processes. Hunt for PowerShell child processes spawned by these executables (T1059.001). Cross-reference file hashes of installed binaries against known-good hashes published in the Kaspersky Securelist report.

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 a SwiftOnSecurity or Olaf Hartong config to capture Event ID 7 (Image Loaded) — filter on DLLs loaded by CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe where the DLL path does not match the expected application install directory. Use Sysmon Event ID 1 (Process Create) to detect PowerShell spawned as a child of any of the four affected executables (MITRE T1059.001). For hash verification without EDR, run 'Get-FileHash -Algorithm SHA256 ' in PowerShell against the installed binaries and compare against Kaspersky Securelist published known-bad hashes. For proxy log hunting without SIEM, use 'findstr /i cpuid.com' against exported proxy or Squid access logs scoped to April 9–10, 2026 UTC timestamps.

Evidence: Sysmon Event ID 7 (Image Loaded) entries showing DLLs loaded from unexpected paths by the four affected CPUID executables — specifically any DLL in the application directory that does not match vendor-signed baselines; Sysmon Event ID 1 or Windows Security Event ID 4688 showing PowerShell.exe or cmd.exe with a parent process of CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe; browser download history (Chrome: 'AppData\Local\Google\Chrome\User Data\Default\History', Edge: 'AppData\Local\Microsoft\Edge\User Data\Default\History') confirming download URL and timestamp; SHA-256 hashes of all binaries in the CPUID install directories for comparison against Kaspersky Securelist known-bad hashes; Windows DNS client cache ('ipconfig /displaydns') or Sysmon Event ID 22 (DNS Query) for STX RAT C2 domain resolutions.

Eradication — On confirmed-infected hosts: terminate and remove STX RAT and associated DLL. Uninstall all cpuid.com utilities downloaded during the compromise window. Re-download tools only from the current cpuid.com site after verifying file integrity against hashes published post-remediation. Rebuild hosts where full infection scope cannot be confirmed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without enterprise endpoint management: use Autoruns (Sysinternals) to enumerate and remove STX RAT persistence entries — specifically check the 'Logon', 'Scheduled Tasks', and 'AppInit DLLs' tabs for entries referencing the malicious DLL or STX RAT executable paths identified in the Kaspersky Securelist report. Run 'taskkill /F /IM ' to terminate the RAT before removal. Verify DLL removal by checking the CPUID application install directory for any DLL not present in the post-remediation clean installer. Scan with ClamAV using an updated signature database as a secondary confirmation before re-allowing the host on the network. If Autoruns reveals persistence that cannot be cleanly removed (e.g., injected into a system process), treat as full-rebuild required.

Evidence: Before eradication, image the infected disk using FTK Imager or 'dd' to preserve forensic evidence for post-incident review; capture Autoruns output as a CSV ('autorunsc -a * -c > autoruns_output.csv') documenting all persistence mechanisms left by STX RAT; collect the malicious DLL file and STX RAT binary with SHA-256 hashes for IOC sharing; export Windows Security Event Log and Sysmon logs covering the full infection timeline before any remediation actions alter the evidentiary record; document all registry run keys and scheduled tasks associated with STX RAT persistence (registry paths: 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run', 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run').

Recovery — After reimaging or cleaning affected hosts, reset all credentials that were entered on or accessible from those systems. Monitor for re-infection indicators for at least 30 days post-remediation. Validate that no persistence mechanisms (scheduled tasks, registry run keys, injected processes) remain. Confirm C2 blocking rules are active and generating no new hits.

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 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without SIEM for 30-day re-infection monitoring: configure a Sysmon + Windows Event Forwarding (WEF) pipeline to a central Windows Event Collector server (no-cost, built into Windows Server) and write a Sigma rule detecting the specific DLL side-loading pattern (CPUID executables loading unsigned or unexpected DLLs) for ongoing alerting. For credential reset validation without PAM tooling, use 'net user' and Active Directory Users and Computers to confirm password resets on all accounts identified as accessible from affected hosts. Schedule a weekly PowerShell cron job ('schtasks') to re-run Get-FileHash against all reinstalled CPUID utilities and compare against post-remediation known-good hashes to detect re-compromise.

Evidence: Post-recovery validation artifacts to retain: Autoruns clean-state CSV captured immediately after rebuild or cleaning confirming no STX RAT persistence entries remain; firewall/DNS blocking logs showing STX RAT C2 IOC rules are active with zero new hit events over the 30-day monitoring window; credential reset confirmation records for all accounts that were logged into or stored on affected hosts (document account names, reset timestamps, and authorizing administrator); Sysmon Event ID 7 baseline log from the clean reinstalled CPUID tools documenting expected legitimate DLL load paths for future anomaly comparison.

Post-Incident — This attack exploited the absence of download integrity verification (CWE-494) and software distribution trust assumptions. Implement a software allowlist policy requiring hash verification before execution of downloaded utilities. Evaluate whether IT and engineering teams use hardware diagnostic utilities from unmanaged personal devices, which would fall outside EDR coverage. Consider requiring all utility software to be distributed through an internal, hash-verified repository rather than direct vendor download.

NIST Phase: Post Incident

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

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-11 (User-Installed Software), NIST SA-12 (Supply Chain Protection), NIST IR-8 (Incident Response Plan), 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: For teams without enterprise software distribution infrastructure: establish a SharePoint or internal file share as an interim verified repository — host only CPUID utilities (and other hardware diagnostic tools) whose SHA-256 hashes have been manually verified against vendor-published post-incident hashes, and document the verification date and verifying analyst in a simple spreadsheet. Implement a AppLocker or Windows Defender Application Control (WDAC) policy (both free, built into Windows) to block execution of any unsigned or hash-unrecognized executable from user download directories (Downloads, Temp, Desktop). Create a one-page IT policy requiring hardware diagnostic tools to be pulled from the internal repository only, and include a BYOD/personal device exception acknowledgment form to capture the unmanaged device risk identified in this incident.

Evidence: Lessons-learned documentation artifacts: a timeline reconstruction of which endpoints downloaded from cpuid.com during the April 9–10 window (sourced from proxy/DNS logs), used to validate blast radius assessment accuracy; a gap analysis record documenting which affected endpoints lacked EDR or Sysmon coverage — specifically identifying any personal/unmanaged devices that were used — to quantify the BYOD visibility gap exposed by this campaign; final IOC list derived from Kaspersky Securelist report (STX RAT hashes, C2 domains, DLL names) formatted for import into your DNS blocklist, firewall, and any future YARA/Sigma detection rules as institutional memory of this specific supply chain compromise.

Detection Guidance

Note: Full IOC values (domains, IPs, file hashes) must be retrieved directly from the Kaspersky Securelist report; key indicators are summarized below, but operational detection requires complete data.

Primary detection surface is endpoint and network telemetry. In EDR: search for DLL loads from non-standard paths by CPU-Z.exe, HWMonitor.exe, HWMonitor_x64.exe, or PerfMonitor.exe. Alert on PowerShell processes with these executables as parent. In proxy and DNS logs: query for connections to cpuid.com between 2026-04-09T00:00Z and 2026-04-10T19:00Z (approximate window) with HTTP response bodies indicating a binary download. For file-based detection: compare SHA-256 hashes of installed cpuid.com binaries against clean hashes from the Kaspersky Securelist report (https://securelist.com/tr/cpu-z/119365/). Behavioral indicators include: unexpected network beaconing from hardware utility processes, input capture activity (keylogger artifacts in temp directories), and injection into legitimate processes following hardware tool execution. YARA and Sigma rules, if published by Kaspersky for STX RAT, should be loaded into your SIEM and endpoint tooling.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://cpuid.com (download endpoints, April 9–10 2026 UTC window)`	Legitimate site was weaponized during compromise window; downloads from this site during the window should be treated as malicious	HIGH
HASH	`[Retrieve from Kaspersky Securelist: https://securelist.com/tr/cpu-z/119365/]`	File hashes for trojanized CPU-Z, HWMonitor, HWMonitor Pro, and PerfMonitor installers and associated STX RAT DLLs are published in the Securelist primary report; not reproduced here to avoid transcription error	HIGH
DOMAIN	`[Retrieve from Kaspersky Securelist: https://securelist.com/tr/cpu-z/119365/]`	STX RAT C2 domains are documented in the Securelist IOC table; not reproduced here to avoid transcription error	HIGH
IP	`[Retrieve from Kaspersky Securelist: https://securelist.com/tr/cpu-z/119365/]`	STX RAT C2 IP addresses are documented in the Securelist IOC table; not reproduced here to avoid transcription error	HIGH

Framework Mappings

MITRE-ATTACK

- **T1090** — Proxy
- **T1056** — Input Capture

- **T1497** — Virtualization/Sandbox Evasion
- **T1574.002** — DLL Side-Loading
- **T1059.001** — PowerShell
- **T1608.004** — Drive-by Target
- **T1059** — Command and Scripting Interpreter
- **T1055** — Process Injection
- **T1189** — Drive-by Compromise
- **T1071.001** — Web Protocols
- **T1071** — Application Layer Protocol
- **T1195.002** — Compromise Software Supply Chain

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **CA-7** — Continuous Monitoring
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **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
T1090	Proxy	Command-And-Control

Technique ID	Technique Name	Tactic
T1056	Input Capture	Collection
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1574.002	DLL Side-Loading	Persistence
T1059.001	PowerShell	Execution
T1608.004	Drive-by Target	Resource-Development
T1059	Command and Scripting Interpreter	Execution
T1055	Process Injection	Defense-Evasion
T1189	Drive-by Compromise	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control
T1195.002	Compromise Software Supply Chain	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/cpuid-breach-distributes-stx-rat-...	T3
CPU-Z & HWMonitor, cpuid.com, Watering Hole Attack | Securelist	https://securelist.com/tr/cpu-z/119365/	T3
HWMonitor and CPU-Z developer CPUID breached by unknown ...	https://www.tomshardware.com/tech-industry/cyber-security/hwmonitor...	T3
DO NOT DOWNLOAD HWMonitor, CPU-Z AND OTHER ... - Reddit	https://www.reddit.com/r/AMDHelp/comments/1shh7ch/do_not_download_h...	T3
CPUID hijacked to serve malware as HWMonitor downloads	https://www.theregister.com/2026/04/10/cpuid_site_hijacked/	T3

Generated 2026-04-12 06:02 UTC by TJS Security Command Center