ultraviolet

THREAT ADVISORY

CPUID Compromise

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
April 13, 2026
TLP:GREEN

Executive Snapshot

The CPUID distribution channel compromise demonstrates how quickly a trusted software source can become an effective malware delivery mechanism and why software supply chain incidents continue to present outsized risk to enterprises. In this case, users seeking common hardware diagnostic utilities were reportedly served trojanized installers that leveraged DLL sideloading to deploy STX RAT, a capable remote access trojan associated with credential theft, remote control, persistence, and follow-on payload delivery. For organizations, the key concern is that routine software downloads from legitimate vendors can bypass normal user suspicion and create an initial foothold on technical workstations, support systems, or administrative endpoints that may hold elevated access or sensitive data. This incident reinforces the need to treat third-party software distribution paths as part of the attack surface and to respond to even short-lived vendor compromises as potential enterprise credential exposure and lateral movement events.

- Identify and investigate any systems that downloaded or executed CPU-Z, HWMonitor, HWMonitor Pro, or PerfMonitor during the suspected exposure window, and isolate affected hosts pending triage.
- Assume possible credential theft on impacted systems by resetting user passwords, rotating privileged credentials, revoking active sessions, and considering full reimaging where malware execution is confirmed.
- Reduce future supply chain exposure by restricting software installation rights, distributing approved utilities through managed repositories, validating hashes and signatures before deployment, and monitoring for DLL sideloading and anomalous outbound activity from trusted tools.

TIDE Team Analysis

The compromise of CPUID's software distribution channel is a reminder that trusted utilities can become effective malware delivery vehicles with very little warning. Attackers reportedly abused a compromised secondary API on CPUID's website and caused users seeking CPU-Z, HWMonitor, HWMonitor Pro, and PerfMonitor to receive trojanized downloads instead of clean installers. While CPUID indicated that its signed original files were not directly modified, the operational risk to organizations remained significant because users downloading software from a legitimate vendor site were instead served attacker-controlled payloads during the compromise window.

What makes this incident strategically important for Security Leadership is not just the malware family involved, but the delivery mechanism. CPU-Z and HWMonitor are widely trusted diagnostic tools used by administrators, engineers, support staff, and technical users. When a familiar vendor and a normal software download workflow are leveraged to stage malware, traditional user skepticism becomes far less effective, and a routine action can quickly become an initial access event inside the enterprise.

The reported intrusion window appears to have been relatively short, but even a brief exposure can create outsized enterprise risk when popular software is involved. A short-lived compromise of a widely used download channel can still result in dozens or hundreds of infected systems across multiple sectors before defenders are fully aware of the issue. This reflects the broader danger of software supply chain compromises, where trust in the source accelerates infection and limits the warning signs that users and defenders would normally expect to see.

Technically, the attack appears to have paired legitimate signed executables with a malicious DLL named CRYPTBASE.dll in order to trigger DLL sideloading. In practice, that means the expected application may still launch and appear normal to the user while a malicious library is loaded in parallel. This is particularly dangerous in enterprise environments because the visible behavior of the software may not immediately signal compromise, allowing the malware to establish itself before help desk teams or endpoint users recognize that anything is wrong.

The final payload, STX RAT, materially increases the severity of the incident because it is not a nuisance implant but a capable remote access platform. Public reporting has described the malware as supporting remote control, hidden virtual network computing functionality, in-memory execution of additional payloads, credential theft, data theft, persistence, anti-analysis measures, and encrypted command-and-control traffic. From a business risk perspective, this means a single compromised workstation can become a foothold for credential harvesting, lateral movement, further malware deployment, and deeper compromise of internal systems.

Organizations should treat any CPUID software downloaded during the suspected exposure period as potentially hostile until proven otherwise. Security teams should identify systems where CPU-Z, HWMonitor, HWMonitor Pro, or PerfMonitor were downloaded or executed during the relevant timeframe, isolate those hosts, and perform forensic triage. Review should focus on browser download history, process execution telemetry, DLL load activity involving CRYPTBASE.dll, suspicious outbound connections, and signs that credentials or locally stored secrets may have been accessed by the malware.

Containment and recovery efforts should assume credential exposure, rather than treating the issue solely as a malware cleanup event. Because STX RAT reportedly includes infostealer and remote access capabilities, affected organizations should reset passwords associated with impacted users, revoke active sessions where possible, rotate privileged credentials that may have been exposed, and strongly consider reimaging affected systems rather than attempting partial remediation. Security teams should also validate that endpoint controls are able to detect DLL sideloading, anomalous child processes spawned by trusted utilities, anti-sandbox behavior, and unusual outbound

traffic from workstations that do not normally initiate remote-control activity.

The broader lesson is that software trust must be continuously verified rather than assumed. Organizations can reduce future exposure by restricting which users may install diagnostic utilities, distributing approved tools through managed internal repositories, validating software hashes and signatures before deployment, and monitoring vendor-originated downloads as a distinct supply chain risk category. This incident reinforces the need for rapid coordination between security, IT, and endpoint operations, because compromise of a legitimate vendor site can bypass the instincts and controls that normally protect users from malicious downloads.

Why It Matters

The CPUID compromise matters because it turned a trusted software source into an initial access channel with almost no friction for the end user. Public reporting indicates attackers tampered with CPUID's download workflow for CPU-Z, HWMonitor, HWMonitor Pro, and PerfMonitor and used DLL sideloading to deliver STX RAT to victims across multiple industries. For enterprise defenders, that is the core lesson: even a short-lived compromise of a legitimate vendor can bypass normal user suspicion, evade casual IT review, and create footholds on systems that may already have administrative access, browser-stored credentials, or privileged network reach.

Tools like CPU-Z and HWMonitor are also more sensitive in enterprise environments than they appear at first glance because they operate close to the hardware and, in some cases, rely on kernel-mode components to gather low-level system information. That matters because ring 0, or kernel-level access, is the most privileged execution layer in the operating system, and abuse at that layer can enable privilege escalation, defense evasion, and deeper system manipulation. The historical record reinforces the concern: NVD documents a prior CPU-Z kernel-driver vulnerability that allowed arbitrary physical memory reads and potential elevation of privilege, while broader research on driver-based attacks shows why adversaries prize kernel-level pathways when they want to disable or subvert security controls. In practice, even legitimate hardware utilities can become high-consequence software in enterprise fleets because compromise of the vendor, installer, or driver path can expose defenders to far more than ordinary user-space malware.

Historically, incidents like this deserve attention because they fit a well-established pattern in which trusted software channels are abused to reach downstream victims at scale. The 2017 CCleaner compromise, the ASUS Live Update incident, SolarWinds, and the 3CX compromise all demonstrated variations of the same problem: once attackers gain influence over a legitimate software distribution path, they inherit the trust relationships that enterprises have already built around that vendor or product. The CPUID event is smaller in scale than some of those landmark cases, but it belongs in the same strategic category. It reinforces that software supply chain risk is not limited to major enterprise platforms; even niche or operational utilities can become effective delivery vehicles when they are broadly trusted, commonly installed, and granted deep system access.

How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Perform a software inventory of user edge devices to understand where Ring0 tools like HWMonitor and CPU-Z are installed.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a Red Team or Purple Team engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---