INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 14:30 UTC

Hola Browser Supply Chain Compromise Delivers Cryptominer via Windows Service

THREAT CAMPAIGN | **HIGH** | CVSS 7.8

SCC Item ID	SCC-CAM-2026-0469
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.8
Affected Products	Hola Browser for Windows (specific version(s) not confirmed in available sources)
Published	2026-06-08
Discovery Source	Gemini

Executive Summary

Hola Browser for Windows was compromised through its software distribution or update mechanism, resulting in a malicious cryptominer being silently installed on user systems as a persistent Windows service. The attacker also disabled Windows Defender exclusions to avoid detection, leaving affected machines exposed to ongoing resource abuse and potential further compromise. Organizations and individuals running Hola Browser on Windows should treat any installed instance as potentially compromised and take immediate action to remove it.

Technical Analysis

A supply chain compromise (MITRE T1195.002) targeting Hola Browser for Windows resulted in a malicious executable being distributed to users via the browser's update or build distribution mechanism. The payload installs itself as a persistent Windows service (T1543.003, Create or Modify System Process: Windows Service), mines cryptocurrency on victim hardware (T1496, Resource Hijacking), and adds Windows Defender exclusions to suppress detection (T1562.001, Impair Defenses: Disable or Modify Tools). Relevant CWEs: CWE-506 (Embedded Malicious Code), CWE-494 (Download of Code Without Integrity Check), CWE-693 (Protection Mechanism Failure). No CVE has been assigned. No specific compromised version has been confirmed in available sources. Threat actor attribution is unconfirmed. The exact number of affected users is unknown pending vendor disclosure. No vendor patch advisory with a specific version remediation path has been confirmed in available sources at the time of this writing. Specific technical details remain unconfirmed pending vendor disclosure. Treat this guidance as precautionary until Hola publishes an official advisory.

Action Checklist

1. Step 1: Containment. Immediately identify all Windows endpoints running Hola Browser using your asset inventory (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory). Isolate or block network access for any confirmed Hola Browser installations until the software is removed and the system is verified clean. Block Hola Browser update domains at the perimeter firewall and DNS layer.
2. Step 2: Detection. Query endpoint logs for new Windows services created around the time Hola Browser was installed or updated (Event ID 7045, A new service was installed in the system). Search for Windows Defender exclusion additions via Event ID 5007 (Windows Defender configuration changed) and registry path HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions. Monitor for anomalous CPU usage patterns consistent with cryptomining (sustained high CPU on endpoints with no corresponding user workload). Review scheduled tasks and service entries for unknown executables in Hola Browser's installation directory. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence.
3. Step 3: Eradication. Uninstall Hola Browser from all enterprise endpoints. Verify removal of any Windows services created by the malicious payload, delete any unrecognized services registered from Hola's install path. Remove all Windows Defender exclusions added by the malware. Run a full endpoint scan with updated definitions after re-enabling Defender protections. Reference CIS 2.3 (Address Unauthorized Software) for process guidance on removing unauthorized software from enterprise assets.
4. Step 4: Recovery. After removal, verify no persistence mechanisms remain: confirm no rogue scheduled tasks, no residual services, and no unauthorized registry modifications. Re-enable and validate Windows Defender is fully operational with no remaining exclusions from the incident. Monitor affected endpoints for 14 days post-remediation for anomalous outbound connections or CPU spikes. Reference NIST AU-6 for ongoing audit review post-recovery.
5. Step 5: Post-Incident. This incident exposes a gap in software supply chain integrity verification (CWE-494). Review NIST SP 800-161r1 (Supply Chain Risk Management) with your procurement and GRC teams to strengthen controls at the download and installation level. Assess your software allowlist policy against CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.3 (Address Unauthorized Software) to prevent unapproved browsers from running in the enterprise. Evaluate whether automated patch management processes (CIS 7.3, CIS 7.4) include integrity verification of distributed packages. Document this event in your lessons-learned record and update your supply chain risk assessment accordingly.

Detection Guidance

Primary detection signals on Windows endpoints: (1) Event ID 7045 in the System event log, filter for new services registered from Hola Browser's installation directory or from unexpected paths. (2) Event ID 5007 in the Microsoft-Windows-Windows Defender/Operational log, look for exclusion additions not corresponding to approved IT changes. (3) Registry key monitoring: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths and \Processes for entries added at or after Hola Browser installation. (4) Sustained anomalous CPU utilization (sustained >80% on endpoints with no user-intensive workload), correlate with process telemetry to identify the consuming process. (5) Outbound network connections from unknown processes to mining pool domains or IPs, mining pools commonly use ports 3333, 4444, 14444, or 45560, though specific IOCs for this campaign have not been confirmed in available sources. Reference NIST AU-2

(Event Logging) to ensure these event types are captured in your logging baseline. Ensure system monitoring controls per your GRC framework are in place to capture these signals; note that endpoint detection and response (EDR) capabilities beyond native Windows logging may be required for comprehensive coverage. D3FEND countermeasures applicable: D3-SFA (System File Analysis) to monitor Hola's installation directory for unauthorized executables; D3-LAM (Local Account Monitoring) to detect service account creation; D3-SICA (System Init Config Analysis) to review service startup configuration changes.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not confirmed in available sources`	Malicious executable delivered via Hola Browser update/distribution mechanism — no confirmed hash values in available sources at time of writing	LOW

Framework Mappings

MITRE-ATTACK

- **T1543.003** — Windows Service
- **T1195.002** — Compromise Software Supply Chain
- **T1496** — Resource Hijacking
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **CM-7** — Least Functionality
- **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
- **SI-4** — System Monitoring

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
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1543.003	Windows Service	Persistence
T1195.002	Compromise Software Supply Chain	Initial-Access
T1496	Resource Hijacking	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
gemini	https://research.checkpoint.com/2026/8th-june-threat-intelligence-r...	T3
Hola Browser for Windows compromised to deliver cryptominer	https://www.bleepingcomputer.com/news/security/hola-browser-for-win...	T3
Hola VPN Support Center: Setup Guides & Help	https://hola.org/faq	T3
Hola browser extension should be uninstalled, researchers say	https://www.pcworld.com/article/427797/hola-browser-extension-shoul...	T3
Hola Browser for Windows compromised to deliver cryptominer	https://www.reddit.com/r/InfoSecNews/comments/1txg1fl/hola_browser_...	T3

Generated 2026-06-15 14:30 UTC by TJS Security Command Center