INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 06:56 UTC

Hola Browser Windows Distribution Pipeline Compromised to Deliver Monero Cryptominer

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0413
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Hola Browser for Windows (Hola / Hola VPN)
Published	2026-06-04T17:27:25
Discovery Source	Rss

Executive Summary

Attackers compromised Hola Browser's Windows software distribution pipeline to silently install a Monero cryptocurrency miner on end-user machines. Any Windows user who installed or updated Hola Browser during the affected window received a trojanized build without any visible indication of tampering. The primary business risk is unauthorized use of corporate compute resources, potential policy and regulatory exposure on managed endpoints, and reputational risk if employee devices were affected.

Technical Analysis

Hola Browser's Windows distribution pipeline was compromised to deliver an undeclared Monero (XMR) miner alongside legitimate browser installations and updates. The attack was discovered by Sophos during AppEsteem certification checks and independently confirmed by Sygnia. No CVE has been assigned. Relevant weakness classifications: CWE-494 (Download of Code Without Integrity Check), CWE-345 (Insufficient Verification of Data Authenticity), CWE-506 (Embedded Malicious Code). MITRE ATT&CK techniques: T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain), T1543.003 (Create or Modify System Process: Windows Service), T1036.004 (Masquerading: Masquerade Task or Service), T1562.001 (Impair Defenses: Disable or Modify Tools), T1027 (Obfuscated Files or Information), T1496 (Resource Hijacking). Defense evasion mechanisms include: adding a Windows Defender exclusion for the miner binary, masquerading as a legitimate monitor service in process lists, and limiting execution to system idle periods. Patch status: users should uninstall Hola Browser for Windows and verify no miner artifacts remain; no patched version has been confirmed safe by an independent third party as of publication.

Action Checklist

1. Step 1: Containment, Identify all Windows endpoints in your environment where Hola Browser (Hola VPN) is installed. Block the Hola Browser installer and update URLs at the web proxy or firewall to prevent further trojanized builds from executing. Remove Hola Browser from your approved software list immediately (CIS 2.3, Establish and Maintain a Software Allowlist; CIS 2.1, Establish and Maintain a Software Inventory).
2. Step 2: Detection, Search endpoint logs for the following behavioral indicators: (a) Windows Defender exclusion additions for unfamiliar paths (Event ID 5007 in Microsoft-Windows-Windows Defender/Operational); (b) new services masquerading as monitor utilities with unusual parent processes; (c) high CPU usage during system idle periods attributed to unknown service processes; (d) outbound network connections to Monero mining pool infrastructure (common ports: 3333, 4444, 5555, 7777, 9999). Correlate with process creation logs (Event ID 4688 or Sysmon Event ID 1) for processes spawned by the Hola Browser installer. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence.
3. Step 3: Eradication, Uninstall Hola Browser from all affected Windows endpoints. After uninstall, manually verify: (a) no residual service entries mimicking monitor services remain in services.msc or via 'sc query'; (b) no Windows Defender exclusions added by the miner persist (check via PowerShell: Get-MpPreference | Select-Object -ExpandProperty ExclusionPath); (c) no scheduled tasks or startup entries reference the miner binary. Remove any identified miner artifacts and revoke Defender exclusions. Reference CIS 4.6 (Securely Manage Enterprise Assets and Software).
4. Step 4: Recovery, After removal, run a full Windows Defender scan with exclusions cleared. Monitor affected endpoints for recurrence of idle-time CPU spikes and unexpected outbound connections for a minimum of 14 days. Verify software inventory reflects Hola Browser removal (CIS 2.1). Re-enable any Defender exclusions that were legitimately in place before the compromise. Reference NIST AU-12 (Audit Record Generation) to confirm logging is intact post-remediation.
5. Step 5: Post-Incident, This incident exposes two control gaps: (a) absence of a software allowlist or application control policy permitting unvetted consumer browsers on managed endpoints (CIS 2.3; NIST AC-3, Access Enforcement); (b) insufficient integrity verification for software installed from third-party distribution pipelines (CWE-345 / CWE-494). Conduct a review of all consumer-grade software present on managed endpoints. Evaluate deployment of software allowlisting (CIS 2.3) and endpoint-based web server access mediation controls (D3-EBWSAM) to restrict unapproved installer execution. Where Windows Defender is the primary AV control, audit exclusion lists on a scheduled basis per NIST SI-4 (System Monitoring) cadence.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to CISO and legal counsel immediately if affected endpoints processed, stored, or transmitted regulated data (PII, PHI, PCI-DSS cardholder data) during the compromise window, as unauthorized code execution on those systems may trigger breach notification obligations under HIPAA, GDPR, or applicable state privacy laws; also escalate if the miner is discovered on endpoints with privileged access to production systems, as the compromised distribution pipeline may have enabled additional undiscovered payloads beyond the XMR miner.
Recovery Notes	After eradication, validate that Windows Defender exclusion lists have been fully restored to pre-compromise baselines on every affected endpoint before declaring systems clean, because the miner's self-protection mechanism specifically leveraged exclusion injection to survive on-access scanning. Monitor outbound traffic to Monero stratum pool infrastructure (ports 3333, 4444, 5555, 7777, 9999) and idle-time CPU utilization on previously affected hosts for a minimum of 14 days, as incomplete removal of the service-masquerading persistence mechanism may allow the miner to restart after system reboots. Update the software inventory (CIS 2.1) to reflect confirmed removal and establish a recurring quarterly audit of consumer-grade browser installations on managed endpoints to prevent recurrence via similar supply-chain-compromised distribution pipelines.
Forensic Artifacts	Windows Installer Application Event Log entries (Event ID 11707 — Installation completed successfully, Event ID 11724 — Removal completed) with source MsiInstaller, timestamped to identify which endpoints installed the Hola Browser build during the compromised distribution window | Microsoft-Windows-Windows Defender/Operational log Event ID 5007 entries recording exclusion path additions made by the miner dropper — the specific exclusion paths added (typically under %ProgramFiles%\Hola or %AppData%\Hola) are a high-fidelity indicator unique to this campaign's AV evasion technique | Windows Security Event Log Event ID 4688 (or Sysmon Event ID 1) process creation records showing the Hola installer process spawning sc.exe, reg.exe, or a miner binary executable, with full command-line arguments captured — requires 'Include command line in process creation events' GPO or Sysmon Process Create rule to be enabled | Sysmon Event ID 3 (Network Connection) or Windows Firewall log entries showing established outbound TCP connections from a service-named process to external IPs on ports 3333, 4444, 5555, 7777, or 9999 — these are Monero XMR stratum mining protocol ports and are not expected from any legitimate Hola Browser or system monitor service | SHA-256 hash and binary copy of the miner executable dropped to disk by the trojanized Hola Browser build, along with the Windows service registry key at HKLM\SYSTEM\CurrentControlSet\Services\ preserving the ImagePath, DisplayName, and ObjectName values used by the masquerading service for IOC documentation and cross-environment hunting

Per-Action IR Details

Step 1: Containment — Identify all Windows endpoints in your environment where Hola Browser (Hola VPN) is installed. Block the Hola Browser installer and update URLs at the web proxy or firewall to prevent further trojanized builds from executing. Remove Hola Browser from your approved software list immediately (CIS 2.3 — Address Unauthorized Software; CIS 2.1 — Establish and Maintain a Software Inventory).

NIST Phase: Containment

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

Controls: CIS 2.1 (IG1/IG2/IG3) — Establish and Maintain a Software Inventory, CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, NIST AC-4 — Information Flow Enforcement

Compensating: Run the following PowerShell one-liner against all domain-joined endpoints via WinRM or PSExec to enumerate Hola installations: `Invoke-Command -ComputerName (Get-ADComputer -Filter *).Name -ScriptBlock {

Get-ItemProperty 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall*','HKLM:\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall*' | Where-Object { $_.DisplayName -like '*Hola*' } | Select-Object PSComputerName, DisplayName, InstallDate }`. Block Hola update domains (client.hola.org, updates.hola.org, client2.hola.org) at the perimeter firewall with an explicit deny rule and log all matches for later review.

Evidence: Before blocking, capture proxy or firewall logs showing outbound connections to Hola Browser update infrastructure (client.hola.org, updates.hola.org) to establish which endpoints pulled the trojanized build and during which time window. Preserve Windows Installer event logs (Event ID 11707/11724 in Application log, source MsiInstaller) on affected hosts to document installation timestamps of the compromised Hola build.

Step 2: Detection — Search endpoint logs for the following behavioral indicators: (a) Windows Defender exclusion additions for unfamiliar paths (Event ID 5007 in Microsoft-Windows-Windows Defender/Operational); (b) new services masquerading as monitor utilities with unusual parent processes; (c) high CPU usage during system idle periods attributed to unknown service processes; (d) outbound network connections to Monero mining pool infrastructure (common ports: 3333, 4444, 5555, 7777, 9999). Correlate with process creation logs (Event ID 4688 or Sysmon Event ID 1) for processes spawned by the Hola Browser installer. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 — Audit Record Review, Analysis, And Reporting, NIST AU-2 — Event Logging, NIST AU-3 — Content Of Audit Records

Compensating: Deploy Sysmon with a configuration that includes NetworkConnect events (Event ID 3) filtering on DestinationPort values 3333, 4444, 5555, 7777, 9999 to Monero pool IP ranges. Use the following PowerShell to extract Defender exclusion change events: `Get-WinEvent -LogName 'Microsoft-Windows-Windows Defender/Operational' | Where-Object { $_.Id -eq 5007 } | Select-Object TimeCreated, Message | Format-List`. For process ancestry, run `Get-WinEvent -LogName Security | Where-Object { $_.Id -eq 4688 } | Where-Object { $_.Message -match 'hola' }` to find child processes spawned by the Hola installer. Use Wireshark or netstat (`netstat -b -n -o`) on suspect hosts to confirm live connections to mining pool ports.

Evidence: Capture Microsoft-Windows-Windows Defender/Operational log (Event ID 5007) entries showing exclusion path additions timed to the Hola Browser installation window — the miner drops its binary to a path it then excludes to evade on-access scanning. Collect Sysmon Event ID 1 or Security Event ID 4688 records showing the Hola installer process (hola_setup.exe or equivalent) spawning unexpected child processes such as service registration commands (sc.exe create) or miner executables. Export netstat output or Sysmon Event ID 3 network connection logs showing established connections from service-named processes to Monero stratum pool ports 3333/4444/5555.

Step 3: Eradication — Uninstall Hola Browser from all affected Windows endpoints. After uninstall, manually verify: (a) no residual service entries mimicking monitor services remain in services.msc or via 'sc query'; (b) no Windows Defender exclusions added by the miner persist (check via PowerShell: Get-MpPreference | Select-Object -ExpandProperty ExclusionPath); (c) no scheduled tasks or startup entries reference the miner binary. Remove any identified miner artifacts and revoke Defender exclusions. Reference CIS 4.6 (Securely Manage Enterprise Assets and Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 4.6 (IG1/IG2/IG3) — Securely Manage Enterprise Assets and Software, CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, NIST SI-2 — Flaw Remediation

Compensating: Run the following command sequence on each affected host to verify full miner removal: (1) `sc query type= all state= all | findstr -i monitor` — compare output against known-good baseline to identify masquerading service names. (2) `schtasks /query /fo LIST /v | findstr -i 'Task To Run\|Status\|Task Name'` — review for tasks referencing paths in %AppData%, %Temp%, or Hola installation directories. (3) `Get-MpPreference | Select-Object -ExpandProperty ExclusionPath` — any path under Hola's install directory (typically %ProgramFiles%\Hola or %AppData%\Hola) that was not present before the incident should be removed with `Remove-MpPreference

-ExclusionPath "`. Use Autoruns (Sysinternals) to enumerate all persistence mechanisms and filter by the Hola installation path.

Evidence: Before executing uninstall, image or snapshot the miner binary on disk (typically dropped under %ProgramFiles%\Hola or %AppData%\Hola subdirectory) and record its SHA-256 hash for IOC sharing. Capture the full output of `sc qc ` for any masquerading service to preserve the binary path, start type, and account context. Export the current Defender exclusion list via `Get-MpPreference` and the scheduled tasks export (`schtasks /query /xml`) as timestamped forensic artifacts before removal.

Step 4: Recovery — After removal, run a full Windows Defender scan with exclusions cleared. Monitor affected endpoints for recurrence of idle-time CPU spikes and unexpected outbound connections for a minimum of 14 days. Verify software inventory reflects Hola Browser removal (CIS 2.1). Re-enable any Defender exclusions that were legitimately in place before the compromise. Reference NIST AU-12 (Audit Record Generation) to confirm logging is intact post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 2.1 (IG1/IG2/IG3) — Establish and Maintain a Software Inventory, NIST AU-12 — Audit Record Generation, NIST AU-6 — Audit Record Review, Analysis, And Reporting

Compensating: Schedule a full Defender scan via PowerShell: `Start-MpScan -ScanType FullScan` on all previously affected hosts after exclusions are cleared. Set up a recurring Sysmon + PowerShell monitoring job for the 14-day window that alerts on any process establishing connections to TCP ports 3333, 4444, 5555, 7777, or 9999, and on any new exclusion path additions (Event ID 5007). Use `Get-Counter '\Processor(_Total)\% Processor Time' -SampleInterval 60 -MaxSamples 1440` logged to CSV via Windows Task Scheduler to capture CPU usage during off-hours (23:00–05:00 local) where idle-time mining would surface.

Evidence: Confirm that Windows Security Event Log (Event ID 4688 or Sysmon Event ID 1) and the Microsoft-Windows-Windows Defender/Operational log are actively generating events post-remediation to establish that logging was not disabled by the miner or its installer. Retain the pre-remediation Defender exclusion export and post-remediation exclusion state as a before/after record. Document the full Defender scan results log (%ProgramData%\Microsoft\Windows Defender\Support\MPLog-*.log) from the post-eradication scan as evidence of clean state.

Step 5: Post-Incident — This incident exposes two control gaps: (a) absence of a software allowlist or application control policy permitting unvetted consumer browsers on managed endpoints (CIS 2.3; NIST AC-3 — Access Enforcement); (b) insufficient integrity verification for software installed from third-party distribution pipelines (CWE-345 / CWE-494). Conduct a review of all consumer-grade software present on managed endpoints. Evaluate deployment of software allowlisting (CIS 2.3) and endpoint-based web server access mediation controls (D3-EBWSAM) to restrict unapproved installer execution. Where Windows Defender is the primary AV control, audit exclusion lists on a scheduled basis per NIST SI-4 (System Monitoring) cadence.

NIST Phase: Post Incident

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

Controls: CIS 2.3 (IG1/IG2/IG3) — Address Unauthorized Software, CIS 2.2 (IG1/IG2/IG3) — Ensure Authorized Software is Currently Supported, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 7.2 (IG1/IG2/IG3) — Establish and Maintain a Remediation Process, NIST AC-3 — Access Enforcement, NIST AU-9 — Protection Of Audit Information

Compensating: Implement Windows AppLocker or WDAC (Windows Defender Application Control) in audit mode first, using the built-in publisher rules to block execution of unsigned or consumer-signed installers from paths outside %ProgramFiles% and %Windows%. Export AppLocker audit events (Event ID 8003/8004 in Microsoft-Windows-AppLocker/EXE and DLL log) to identify additional unauthorized software before enforcing block mode. Schedule a monthly PowerShell audit of Defender exclusion lists across all endpoints via WinRM and diff against a known-good baseline stored in version control to detect future unauthorized exclusion additions — a

technique directly relevant to how this miner evaded on-access detection.

Evidence: Produce a lessons-learned artifact documenting the delta between the software inventory at time of compromise and the approved software list — this gap is the root cause enabling the Hola Browser installation to proceed undetected. Preserve the timeline of Hola Browser installation dates (from MsiInstaller Event IDs 11707/11724) correlated against the known trojanized build window to determine total exposure period and number of affected endpoints. Archive the miner binary hash, the Defender exclusion paths it added, and the mining pool domains/IPs it contacted as organizational IOCs for future threat hunting and detection rule development.

Detection Guidance

Primary detection signals: (1) Windows Defender exclusion modifications, query Microsoft-Windows-Windows Defender/Operational Event ID 5007 for ExclusionPath additions coinciding with Hola Browser install or update activity; (2) new Windows services with display names resembling legitimate monitor utilities but with unusual binary paths or parent processes, cross-reference Sysmon Event ID 7 (ImageLoad) and Event ID 4697 (Service Installed); (3) sustained CPU utilization during system idle attributed to an unrecognized service process, Windows Resource Monitor or EDR process telemetry; (4) outbound TCP connections to Monero mining pool ports (3333, 4444, 5555, 7777, 9999) from non-server workstations, query firewall or proxy logs for connections to these ports from endpoints with Hola Browser installed; (5) process masquerading, compare service executable paths against known-good monitor service baselines (D3-SFA: System File Analysis). No confirmed file hashes or C2 infrastructure IOCs have been publicly released by Sophos or Sygnia as of the sources available for this item. Detection confidence for behavioral indicators is medium because the malware employs obfuscation and evasion tactics; confirm detections with EDR telemetry and cross-reference against known-good baselines before escalating.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`no confirmed IOCs published`	Neither Sophos nor Sygnia have released file hashes, C2 domains, or IP indicators in the sources available for this item. Do not fabricate. Monitor for mining pool port activity as a behavioral proxy.	LOW

Framework Mappings

MITRE-ATTACK

- **T1036.004** — Masquerade Task or Service
- **T1027** — Obfuscated Files or Information
- **T1195.002** — Compromise Software Supply Chain
- **T1562.001** — Disable or Modify Tools
- **T1543.003** — Windows Service
- **T1496** — Resource Hijacking

NIST-800-53R5

- **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
- **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
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

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

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1036.004	Masquerade Task or Service	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1562.001	Disable or Modify Tools	Defense-Evasion
T1543.003	Windows Service	Persistence
T1496	Resource Hijacking	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hola-browser-for-win...	T3
Hola VPN Support Center: Setup Guides & Help	https://hola.org/faq	T3
How bad is Hola and what are there alternatives? : r/VPN - Reddit	https://www.reddit.com/r/VPN/comments/39cdgn/how_bad_is_hola_and_wh...	T3
Hola VPN Review: Is It Safe to Download & Use in 2026? - vpnMentor	https://www.vpnmentor.com/reviews/hola-vpn/	T3
Misadventures with Hola service, or A lot of strings attached	https://www.kaspersky.com/blog/misadventures-with-hola-service-or-a...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-05 06:56 UTC by TJS Security Command Center