INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:14 UTC

Google Disrupts NetNut Proxy Network Spanning 2 Million Infected Devices

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0628
Type	Threat Campaign
Severity	HIGH
Affected Products	NetNut proxy network; approximately 2 million compromised end-user devices used as residential proxy nodes
Published	2026-07-06
Discovery Source	Gemini

Executive Summary

Google disrupted NetNut, a residential proxy network that reportedly routed traffic through approximately 2 million compromised devices, severing those devices from the proxy infrastructure, according to reporting by BleepingComputer. Networks of this type are typically used to obscure the origin of malicious traffic for ad fraud, credential stuffing, and large-scale scraping operations. Organizations whose end-user devices were silently enrolled as proxy nodes face residual risk of malware persistence, bandwidth theft, and potential use of their network identities in downstream abuse campaigns.

Technical Analysis

NetNut operated as a residential proxy service by recruiting compromised end-user devices as exit nodes, routing client traffic through those hosts to mask its true origin. This model aligns with proxyware and malware-as-a-service architectures. Affected devices were enrolled without owner consent, likely via malware, bundled software, or deceptive applications (CWE-506: Embedded Malicious Code). Traffic from enrolled devices exited through standard web protocols (T1071.001: Application Layer Protocol, Web), enabling clients to conduct ad fraud, credential stuffing, and scraping while appearing to originate from legitimate residential IPs. Infrastructure techniques include use of compromised infrastructure (T1584), external proxy use (T1090.002: External Proxy), and acquisition of botnet infrastructure (T1583.008). Google's disruption severed device connections to the proxy control infrastructure; however, the underlying malware or enrollment mechanism on individual devices may persist. No CVE is associated with this campaign. Attribution of the threat actor(s) or commercial operator responsible for building and monetizing the infected device pool has not been confirmed in available source material. Confidence on the core disruption event is medium, primary reporting is from BleepingComputer (T2 source); Google's own public statement has not been independently confirmed in

available data. CWE references: CWE-668 (Exposure of Resource to Wrong Sphere), CWE-506 (Embedded Malicious Code).

Action Checklist

1. Step 1: Containment, Audit endpoint software inventories for unauthorized, bundled, or recently installed applications that may function as proxyware agents; prioritize devices used by remote workers or those with elevated network access. Reference CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.3 (Address Unauthorized Software).
2. Step 2: Detection, Monitor outbound traffic for unusual sustained connections to residential proxy infrastructure IP ranges, unexpected bandwidth spikes on end-user devices, and processes initiating outbound HTTP/HTTPS connections not associated with known applications. Review DNS query logs for domains consistent with proxy coordination. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). D3FEND countermeasure: D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to identify unauthorized persistent processes.
3. Step 3: Eradication, Remove any identified proxyware or malware components from affected endpoints. For devices where account authentication logs are available, revoke and rotate credentials for accounts that authenticated from affected devices, as those devices may have been observed by the proxy operator. Reference D3-CRO (Credential Rotation) and NIST IR-4 (Incident Handling).
4. Step 4: Recovery, Validate that removed software has not reinstalled via persistence mechanisms (scheduled tasks, startup entries). Monitor previously affected devices for renewed outbound proxy-pattern traffic for at least 30 days post-remediation. Reference D3-SICA (System Init Config Analysis) and NIST SI controls for ongoing monitoring.
5. Step 5: Post-Incident, Review software installation controls to prevent unauthorized or bundled applications from reaching endpoints (CIS 2.2, CIS 2.3). Assess whether endpoint detection tools are tuned to flag proxyware behavioral patterns. Document findings per NIST IR-8 (Incident Response Plan) and update playbooks to cover proxyware-as-a-service threat models.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately if proxyware-enrolled devices are confirmed to have authenticated to systems containing PII, PHI, or payment card data — triggering breach notification assessment under GDPR, HIPAA, or PCI DSS — or if the count of affected devices exceeds the IR team's remediation capacity within the defined containment SLA, requiring engagement of an external DFIR retainer.
Recovery Notes	After proxyware removal, verify endpoint integrity by confirming no proxy-pattern outbound traffic resumes within 72 hours using perimeter firewall egress monitoring; if it does, reimage rather than re-remediate. Monitor previously affected devices for 30 days minimum using Sysmon network connection telemetry, as some proxyware SDKs include watchdog processes that reinstall the agent if removed without also purging all persistence mechanisms. Confirm that all credentials authenticated from affected devices have been rotated and that no anomalous authentication events (e.g., logins from new geographies or devices) appear in identity provider logs in the two weeks following rotation.

Forensic Artifacts	Proxyware agent binary and working directory: files under %APPDATA%, %ProgramData%, or /var/lib/ belonging to the agent process — may include SQLite peer-node databases, cached proxy rotation configuration files, and installer logs identifying the delivery vector (e.g., bundled freeware installer name and version) | RAM image of affected host: volatile memory containing decrypted proxy coordination URLs, active peer-node IP lists, authentication tokens for the proxy operator's management infrastructure, and any in-flight HTTP CONNECT tunnel state present at time of capture | Perimeter and host-based DNS logs: query history showing repeated lookups to residential proxy SDK coordination domains (e.g., NetNut API endpoints or affiliate network domains) — high-frequency lookups with consistent TTL patterns are a distinguishing characteristic of proxy relay heartbeat traffic | Sysmon Event ID 3 (Network Connection) logs: records of the agent process establishing outbound TCP connections to diverse residential IP ranges — the volume, duration, and destination diversity of these connections distinguish proxy relay behavior from normal end-user browsing | Windows Security Event Log 4624/4648 and equivalent Linux auth logs: logon events from affected devices during the proxy enrollment window, used to enumerate all accounts that may have had credentials exposed to the proxy operator's infrastructure and to bound the scope of required credential rotation

Per-Action IR Details

Step 1: Containment — Audit endpoint software inventories for unauthorized, bundled, or recently installed applications that may function as proxyware agents; prioritize devices used by remote workers or those with elevated network access. Reference CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.3 (Address Unauthorized Software).

NIST Phase: Containment

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

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software)

Compensating: On Windows endpoints, run: `Get-WmiObject Win32_Product | Select-Object Name, InstallDate, Vendor | Sort-Object InstallDate -Descending | Export-Csv software_audit.csv` to surface recently installed software. Cross-reference output against a known-good baseline. On Linux, use `dpkg-query -l` or `rpm -qa --last` sorted by install date. Use osquery with `SELECT name, version, install_time FROM programs ORDER BY install_time DESC LIMIT 50;` to identify anomalous installs across a fleet without a commercial MDM.

Evidence: Before taking any containment action on a suspect device, capture: (1) running process list with parent-child relationships via `Get-CimInstance Win32_Process | Select-Object Name, ProcessId, ParentProcessId, CommandLine` or `ps auxf` on Linux; (2) active network connections via `Get-NetTCPConnection | Where-Object {$_.State -eq 'Established'}` or `netstat -ano` to identify live proxy relay sessions currently in progress; (3) recently modified files in `%APPDATA%`, `%TEMP%`, `C:\ProgramData`, and user startup folders (`%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup`) that may contain the proxyware agent. These connections and process states are destroyed the moment the agent is killed or the host is isolated.

Step 2: Detection — Monitor outbound traffic for unusual sustained connections to residential proxy infrastructure IP ranges, unexpected bandwidth spikes on end-user devices, and processes initiating outbound HTTP/HTTPS connections not associated with known applications. Review DNS query logs for domains consistent with proxy coordination. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). D3FEND countermeasure: D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to identify unauthorized persistent processes.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity's config to capture Event ID 3 (Network Connection) filtered for processes other than browsers and known business apps making sustained outbound connections on ports 80/443/8080. Use Wireshark or `tcpdump -i eth0 -w capture.pcap 'tcp and (port 80 or port 443)'` on a suspect device and inspect for high-frequency, low-payload HTTP CONNECT tunnel patterns characteristic of proxy relay traffic. For DNS, enable Windows DNS debug logging or query your router/firewall DNS logs for high-frequency lookups to dynamic DNS providers or domains with randomized subdomains consistent with proxy coordination infrastructure.

Evidence: Capture before analysis artifacts are rotated or overwritten: (1) DNS query logs from the endpoint resolver or perimeter DNS server covering the past 30 days — look for repeated lookups to domains associated with residential proxy SDKs (e.g., NetNut, Bright Data, IPRoyal affiliate domains); (2) Windows Security Event Log Event ID 4688 (Process Creation) for processes spawned by software installers or updaters that subsequently initiated network connections; (3) firewall or proxy egress logs showing sustained long-duration TCP sessions from end-user device IPs to diverse destination IPs — residential proxy relay traffic is distinctive for high connection counts to non-business destinations with consistent byte-transfer patterns.

Step 3: Eradication — Remove any identified proxyware or malware components from affected endpoints. Revoke and rotate credentials for accounts that authenticated from affected devices, as those devices may have been observed by the proxy operator. Reference D3-CRO (Credential Rotation) and NIST IR-4 (Incident Handling).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling)

Compensating: Before uninstalling the proxyware agent, capture a full memory image using WinPmem (free, open source) or `avml` on Linux to preserve in-memory configuration, C2 addresses, and session tokens the agent may hold. Then uninstall via standard Add/Remove Programs or `msiexec /x` and verify removal by re-running the process and startup audits from Step 1. For credential rotation on a budget, use Active Directory's 'Reset Password' for all domain accounts that logged into affected devices within the compromise window; for SaaS accounts, revoke all active sessions via each platform's admin console and force re-authentication with a new password plus MFA enrollment.

Evidence: BEFORE revoking credentials or uninstalling the agent — which destroys live state — capture: (1) full RAM image of the affected host to preserve any decrypted proxy coordination URLs, authentication tokens, or peer node lists held in the agent's process memory; (2) a copy of the agent's working directory (commonly under `%APPDATA%`, `%ProgramData%`, or `/var/lib/`) including any SQLite databases, configuration files, or cached peer lists that document the scope of proxy participation; (3) Windows Security Event Log events 4624/4648 (successful logon/explicit credential use) for the affected device over the compromise window to enumerate which accounts require credential rotation.

Step 4: Recovery — Validate that removed software has not reinstalled via persistence mechanisms (scheduled tasks, startup entries). Monitor previously affected devices for renewed outbound proxy-pattern traffic for at least 30 days post-remediation. Reference D3-SICA (System Init Config Analysis) and NIST SI controls for ongoing monitoring.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-5 (Incident Monitoring)

Compensating: Use Autoruns (Sysinternals, free) on each remediated host to enumerate all persistence points — scheduled tasks, Run/RunOnce registry keys, startup folders, service entries, and browser extensions — and verify none reference the removed proxyware agent or its installer path. To monitor for reinstallation, configure Sysmon Event ID 11 (File Creation) and Event ID 13 (Registry Value Set) with rules targeting the agent's known install paths and registry keys, forwarding alerts to a free ELK stack or a shared log directory reviewed daily. Set a 30-day Wireshark or `tcpdump` spot-check cadence on previously affected devices to confirm absence of proxy relay traffic patterns.

Evidence: At recovery validation, collect a clean-state snapshot for future comparison: (1) Autoruns output exported to CSV as a signed baseline; (2) a scheduled task export via `schtasks /query /fo CSV /v > tasks_baseline.csv`; (3)

registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` — these are the most common persistence paths used by proxyware SDKs bundled with freeware installers. If proxy-pattern outbound traffic resumes within the 30-day window, treat the device as re-infected and escalate to full reimaging rather than a second removal attempt.

Step 5: Post-Incident — Review software installation controls to prevent unauthorized or bundled applications from reaching endpoints (CIS 2.2, CIS 2.3). Assess whether endpoint detection tools are tuned to flag proxyware behavioral patterns. Document findings per NIST IR-8 (Incident Response Plan) and update playbooks to cover proxyware-as-a-service threat models.

NIST Phase: Post Incident

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

Controls: CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), NIST IR-8 (Incident Response Plan)

Compensating: Author a YARA rule targeting file characteristics common to proxyware SDKs (string patterns such as proxy rotation API calls, peer-list file structures, or specific SDK library names observed during eradication) and deploy it via ClamAV on a weekly scheduled scan. Submit findings and IOCs — including discovered proxy coordination domains, agent binary hashes, and persistence paths — to CISA's ISAC sharing channels or an internal threat intel feed so peer organizations can benefit. Use the documented findings to build a Sigma rule targeting the Sysmon network connection behavioral pattern (sustained high-frequency outbound connections from non-browser processes) for ongoing detection.

Evidence: For the lessons-learned record and playbook update, preserve: (1) all IOCs collected during the incident — agent binary SHA-256 hashes, proxy coordination domain names, C2 IP ranges, and registry/file persistence paths — formatted in STIX 2.1 or a flat IOC list for reuse; (2) a timeline reconstructed from DNS logs, firewall egress logs, and Sysmon Event ID 3 records showing the earliest evidence of proxy relay activity on each affected device, to establish dwell time; (3) the software inventory delta (new installs in the 30 days prior to detection) to identify the delivery vector — whether proxyware arrived via a bundled freeware installer, a browser extension, or an update mechanism — so the software allowlisting policy can be updated to block the specific delivery pathway.

Detection Guidance

Look for the following behavioral indicators on endpoint and network telemetry: (1) End-user devices initiating persistent, high-frequency outbound HTTPS connections to IP ranges not associated with known enterprise services, particularly to IPs flagged in residential proxy blocklists. (2) Processes on workstations or personal devices that maintain open network sockets outside of browser or known application activity, especially during off-hours. (3) Unexplained bandwidth consumption on individual endpoints inconsistent with user activity patterns. (4) DNS queries to domains associated with proxy coordination or proxyware command-and-control. (5) Presence of software not in the authorized application inventory (CIS 2.1) that requests persistent network access at startup. Log sources: endpoint EDR telemetry, DNS query logs, firewall/proxy egress logs, SIEM correlation rules for high-outbound-connection-count by non-server hosts. NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) apply. D3FEND: D3-SFA (System File Analysis) for unauthorized persistent binaries; D3-LAM (Local Account Monitoring) for unusual account-level network activity. No confirmed IOCs (malware hashes, C2 domains, or proxy infrastructure IP ranges) have been published in available source material. Organizations may request IOC data directly from Google or CISA if they suspect device enrollment.

Framework Mappings

MITRE-ATTACK

- **T1071.001** — Web Protocols
- **T1584** — Compromise Infrastructure
- **T1090.002** — External Proxy
- **T1583.008** — Malvertising

NIST-800-53R5

- **IA-2** — Identification and Authentication (Organizational Users)

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1584	Compromise Infrastructure	Resource-Development
T1090.002	External Proxy	Command-And-Control
T1583.008	Malvertising	Resource-Development

Sources

Source	URL	Tier
NetNut proxy network disrupted, 2 million infected devices ...	https://www.bleepingcomputer.com/news/security/netnut-proxy-network...	T2
NetNut proxy network disrupted, 2 million infected devices cut off	https://forum.ksec.co.uk/t/netnut-proxy-network-disrupted-2-million...	T3

Generated 2026-07-06 15:14 UTC by TJS Security Command Center