INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

# Typosquatting Campaign Trojanizes Popular Software Installers to Build Residential Proxy Botnet

**THREAT CAMPAIGN** | **MEDIUM** | CVSS 5.0

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0019 |
| **Type** | Threat Campaign |
| **Severity** | MEDIUM |
| **CVSS Base Score** | 5.0 |
| **Affected Products** | Windows hosts (SysWOW64 abuse); trojanized installers impersonating 7-Zip, HolaVPN, TikTok, WhatsApp, Wire VPN; Cloudflare (C2 traffic routing); iplogger.org (exfiltration endpoint) |
| **Published** | 2026-03-13 |

## Executive Summary

An active typosquatting campaign is distributing malware-laced installers impersonating widely used software including 7-Zip, WhatsApp, TikTok, HolaVPN, and Wire VPN. Windows users who download and run these installers unknowingly enroll their machines as nodes in a residential proxy botnet, providing threat actors with legitimate-looking IP addresses to conduct credential stuffing, phishing, and malware distribution at scale. Direct harm to individual endpoints is moderate, but organizational exposure includes potential use of corporate IP ranges in downstream criminal activity and reputational risk if company assets are implicated.

## Technical Analysis

The campaign operates through typosquatted domains serving trojanized Windows installers that mimic legitimate applications. Once executed, the payload abuses SysWOW64 to drop and run proxy agent components, establishes persistence via WMI subscriptions and Windows service creation (T1543.003), and modifies network configuration through netsh (T1562.004). C2 resolution uses DNS-over-HTTPS to bypass traditional DNS monitoring (T1071.001), and C2 traffic routes through Cloudflare infrastructure to blend with benign traffic (T1102). Control channel communications are XOR-obfuscated (T1027, T1573.001). The malware performs anti-VM checks before full execution to evade sandbox detonation (T1497.001). Registry modifications are used for persistence and configuration storage (T1112). The infected host is enrolled as a residential proxy node (T1090.002), contributing its IP to a pool used for downstream criminal operations. No CVE is associated;

relevant CWEs include CWE-506 (Embedded Malicious Code), CWE-693 (Protection Mechanism Failure), and CWE-799 (Improper Control of Interaction Frequency). No patch exists, this is a distribution campaign, not a software vulnerability. MITRE ATT&CK coverage spans initial access through T1583.001 (typosquatted infrastructure), T1553.002 (code-signing bypass), and T1195.002 (supply chain installer compromise pattern), with execution via T1059.001 (PowerShell) and discovery via T1082 (system information enumeration). Source quality score is 0.64 based on T3 secondary reporting; primary technical analysis has not been independently verified against a vendor advisory.

## Action Checklist

1. Step 1, Immediate: Block known typosquatted domains associated with this campaign at DNS and web proxy layers; enforce DNS-over-HTTPS inspection or block DoH endpoints not explicitly approved for enterprise use.
2. Step 2, Detection: Search endpoint logs and EDR telemetry for SysWOW64 process anomalies, unexpected WMI subscription creation, netsh execution by non-admin processes, and outbound connections to suspicious domains or Cloudflare-proxied destinations from non-browser processes.
3. Step 3, Assessment: Audit software installation sources across endpoints; identify any hosts where 7-Zip, HolaVPN, TikTok, WhatsApp, or Wire VPN were installed from non-official sources; compare installer hashes against vendor-published values.
4. Step 4, Communication: If proxy agent activity is confirmed on any corporate asset via behavioral indicators (Step 2), notify the security incident response team; assess whether affected IPs must be reported under applicable data protection or incident disclosure obligations before external communication.
5. Step 5, Long-term: Enforce application allowlisting or installer signing verification policies; implement software procurement controls requiring downloads only from vendor-official domains; add residential proxy botnet enrollment behaviors to threat hunting playbooks and scheduled hunt cadences.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to external IR firm or law enforcement if: (1) confirmed proxy botnet activity on >10 corporate endpoints, (2) evidence of data exfiltration to iplogger.org, (3) regulatory notification obligation triggered under GDPR/CCPA, or (4) indicators suggest lateral movement beyond initial infection vectors. |
| **Recovery Notes** | Post-containment: (1) Isolate and rebuild affected endpoints from clean media or approved backup snapshots; do not simply remove malware from infected systems. (2) Force password reset for all users who logged into affected hosts (malware may have harvested credentials). (3) Block all residential proxy botnet IP ranges at perimeter (query threat intelligence feeds for confirmed botnet IP space; block Cloudflare IP ranges used as C2 for 30 days while monitoring for false positives). (4) Conduct forensic deep-dive on 2-3 representative infected hosts to confirm malware capabilities and dwell time. (5) File security advisory internally with lessons learned; update security awareness training to warn against unofficial software sources. |

| | |
|---|---|
| **Forensic Artifacts** | Windows Event Log 4688 (Process Creation) and 4689 (Process Termination) — 7-day retroactive window \| Windows Event Log 11707 (Installer Started) and 11722 (Installer Completed) from Application log \| Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall and WOW6432Node\Uninstall (software inventory) \| Sysmon Event ID 1 (Process Create), ID 3 (Network Connection), ID 11 (File Created) — if available \| DNS query logs (Windows DNS Server or recursive resolver); firewall/proxy logs (egress connections to Cloudflare IPs and iplogger.org) \| Browser download history and cache (Chrome History database, Firefox places.sqlite, Edge WebCacheV01.dat) \| $UsnJrnl (NTFS journal) for installer file creation/modification timestamps \| Memory dumps of suspicious processes (rundll32.exe, explorer.exe spawning SysWOW64 children) via tasklist /v and Get-Process \| Network traffic capture (.pcap) filtered for DNS, HTTP/HTTPS to typosquatted domains and C2 endpoints |

### Per-Action IR Details

**Step 1, Immediate: Block known typosquatted domains associated with this campaign at DNS and web proxy layers; enforce DNS-over-HTTPS inspection or block DoH endpoints not explicitly approved for enterprise use.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.2.3

**Controls:** NIST 800-53 SC-7(5), CIS 4.8, CIS 13.2

**Compensating:** If no enterprise DNS/proxy: add known typosquatted domains to /etc/hosts (Windows: C:\Windows\System32\drivers\etc\hosts) on all endpoints; block DoH by configuring Windows Group Policy (Computer Configuration > Administrative Templates > Network > DNS Client > Configure DNS over HTTPS) to disable or restrict to approved resolvers; for unmanaged endpoints, distribute hosts file via GPO or manual distribution list.

**Evidence:** Capture current DNS resolver configuration (ipconfig /all on Windows; systemctl status systemd-resolved on Linux), proxy PAC/whitelist rules, and DoH endpoint allowlist before modification. Log all domain blocks in proxy/firewall (e.g., pfSense logs, Fortinet FortiGate syslog) with timestamp. Document baseline DNS query patterns 24 hours pre-block to establish normal traffic baseline for detection tuning.

**Step 2, Detection: Search endpoint logs and EDR telemetry for SysWOW64 process anomalies, unexpected WMI subscription creation, netsh execution by non-admin processes, and outbound connections to suspicious domains or Cloudflare-proxied destinations from non-browser processes.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2.1

**Controls:** NIST 800-53 SI-4(1), NIST 800-53 AU-12, CIS 8.2, CIS 13.6

**Compensating:** Without EDR: enable Windows Event Logging (auditpol.exe /set /subcategory:"Process Creation" /success:enable /failure:enable). Search Windows Event Log 4688 for: (1) Parent process = explorer.exe or rundll32.exe spawning C:\Windows\SysWOW64*.exe; (2) CommandLine = 'netsh' with CallingProcessName NOT System/Services; (3) WMI queries via WinRM Event Log 400. Parse with PowerShell: Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4688} | Where {$_.Properties[20].Value -match 'SysWOW64|netsh|WMI'}. Network detection: tcpdump/Wireshark filter (ip.src == && ip.dst == && dns.qry.name == 'typosquatted-domain') or netstat -ano to identify established connections from non-browser PIDs.

**Evidence:** Export Windows Event Log 4688 (Process Creation) for 7 days pre-detection; capture WMI Event Log Microsoft-Windows-WMI-Activity/Operational; extract network connections via netstat -ano output with timestamps; preserve memory dump of suspicious processes (tasklist /v, Get-Process). Capture DNS query logs if available (Windows DNS server logs at %SystemRoot%\System32\dns\DNS.log). Document process tree lineage (parent→child→grandchild) using WinLogBeat or Sysmon EventID 1.

**Step 3, Assessment: Audit software installation sources across endpoints; identify any hosts where 7-Zip, HolaVPN, TikTok, WhatsApp, or Wire VPN were installed from non-official sources; compare installer hashes**

**against vendor-published values.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2.2

**Controls:** NIST 800-53 SI-7(1), NIST 800-53 CM-5, CIS 2.3, CIS 6.1

**Compensating:** Query Windows Add/Remove Programs registry: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall and HKLM\SOFTWARE\WOW6432Node\Uninstall for InstallSource, InstallDate, PublisherURL. Cross-reference download folder (%USERPROFILE%\Downloads) for matching installer names; compute hash with certutil -hashfile SHA256 and compare against official vendor hash pages (7-Zip: 7-zip.org/download, WhatsApp: whatsapp.com/download, TikTok: tiktok.com/@tiktok/video). For all matches, check installer digital signature: Get-AuthenticodeSignature in PowerShell. Log any unsigned or self-signed binaries as high-priority. Document download source from browser history (Chrome/Firefox: Ctrl+H, look for download URLs) or $MFTEntry timestamps to infer approximate download time.

**Evidence:** Preserve installer binaries from %USERPROFILE%\Downloads and %ProgramFiles% before hash comparison (do not modify); export registry hives (HKLM\SOFTWARE and HCU SAM) using reg export. Capture browser history/downloads database (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History; Firefox: %APPDATA%\Mozilla\Firefox\Profiles*.default\places.sqlite). Document $MFT entry for each installer ($UsnJrnl to establish timeline). Preserve application event logs (Windows Event ID 11707 = installer started, 11722 = installer completed).

**Step 4, Communication: If proxy agent activity is confirmed on any corporate asset via behavioral indicators (Step 2), notify the security incident response team; assess whether affected IPs must be reported under applicable data protection or incident disclosure obligations before external communication.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.2.4

**Controls:** NIST 800-53 IR-4, NIST 800-53 IR-6, CIS 19.1

**Compensating:** Document incident scope in a spreadsheet: (1) Date/time of detection, (2) Affected host(s) (hostname, IP, MAC), (3) Evidence source (log name, event ID, query), (4) Behavioral indicator match (process name, domain, hash). Assess legal obligation by querying internal legal/compliance team on: jurisdiction of affected users, applicable regulations (GDPR, CCPA, HIPAA, etc.), customer notification thresholds (triggered if personal data of customers accessed). Create a communication tree: IR lead → CISO → Legal → Communications → affected stakeholders. Do NOT notify external parties (vendors, customers, regulators) until legal has documented the decision. Document the legal assessment and decision in a dated memo kept in the incident file.

**Evidence:** Preserve all behavioral indicators collected in Step 2 (event logs, netstat output, process memory dumps). Capture exfiltration evidence: traffic to iplogger.org (firewall/proxy logs, tcpdump), DNS queries to C2 domains (DNS logs, packet capture). Document the IP addresses of affected endpoints for breach scope assessment. Archive full incident timeline (when malware was detected, when it was confirmed active, when containment actions began).

**Step 5, Long-term: Enforce application allowlisting or installer signing verification policies; implement software procurement controls requiring downloads only from vendor-official domains; add residential proxy botnet enrollment behaviors to threat hunting playbooks and scheduled hunt cadences.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.2.5

**Controls:** NIST 800-53 CM-2, NIST 800-53 CM-5, NIST 800-53 SI-7, CIS 2.3, CIS 6.2, CIS 13.8

**Compensating:** Allowlisting without enterprise tools: use Windows AppLocker (gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker). Define rules: (1) Hash-based whitelist for approved installers (compute and store SHA256 of official 7-Zip, WhatsApp, etc.); (2) Path-based rule for C:\Program Files* and C:\Program Files (x86)*; (3) Publisher rule for Microsoft-signed binaries. Deploy via Group Policy. For procurement controls: create a Software Request Policy requiring employees to submit download URLs for approval before installation; maintain an approved-vendors list (7-zip.org, whatsapp.com, etc.) in a shared document. For threat hunting: add Sysmon EventID 1 query to detect SysWOW64 process spawn chains and quarterly run:

Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4688} | Where {$_.Properties[5].Value -match 'iplogger|cloudflare-c2-domains' -and $_.Properties[1].Value -notmatch 'chrome|firefox|edge'}.

**Evidence:** Baseline AppLocker policy settings and approved-vendor list before deployment for rollback capability. Capture BEFORE-state process execution logs (5 days minimum) to tune allowlisting rules and avoid false positives. Preserve all threat hunt results (queries, dates run, findings) in a hunt log for audit and continuous improvement.

## Detection Guidance

Key behavioral indicators: (1) SysWOW64 child processes spawned by installer executables outside standard update workflows; (2) WMI event subscription creation via wmic.exe or PowerShell referencing non-standard namespaces or scripts; (3) netsh invocations modifying firewall or interface configuration from user-context processes; (4) outbound HTTPS connections to proxy or exfiltration endpoints from non-browser processes; (5) DoH queries to resolvers not in your approved list, particularly from newly installed or unknown processes; (6) registry write activity in Run/RunOnce or service control paths immediately following installer execution. SIEM query focus: correlate process creation events (Sysmon Event ID 1) for netsh.exe and wmic.exe with parent processes matching installer naming patterns; alert on anomalous outbound connections from newly installed processes (Sysmon Event ID 3). EDR behavioral rules: flag XOR-pattern encoded outbound payloads and VM-check API calls (CPUID, registry checks for VM artifacts) occurring within 60 seconds of installer execution. Note: specific file hashes and domain IOCs are not confirmed in available T3 source reporting; treat the behavioral patterns above as primary detection layer until authoritative IOC lists are published.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `iplogger.org` | Exfiltration endpoint used by proxy agent for data reporting; outbound connections from non-browser processes to this domain should be treated as high-confidence malicious indicator | MEDIUM |
| URL | `Typosquatted domains impersonating 7-zip.org, holavpn.com, tiktok.com, whatsapp.com, wire.com, specific domain values not confirmed in available source reporting` | Initial distribution infrastructure; specific domains not extracted from T3 sources available at configuration time, monitor DNS for lookalike registrations using common typosquat patterns (transposition, homoglyph, hyphen insertion) | LOW |
| DOMAIN | `Cloudflare-proxied C2 endpoints, specific hostnames not confirmed in available source reporting` | C2 traffic routed through Cloudflare to blend with legitimate traffic; behavioral detection preferred over domain blocking given shared infrastructure risk | LOW |

## Framework Mappings

**MITRE-ATTACK**

- **T1583.001** — Domains
- **T1553.002** — Code Signing
- **T1195.002** — Compromise Software Supply Chain
- **T1071.001** — Web Protocols
- **T1573.001** — Symmetric Cryptography
- **T1112** — Modify Registry
- **T1566.002** — Spearphishing Link
- **T1562.004** — Disable or Modify System Firewall
- **T1543.003** — Windows Service
- **T1059.001** — PowerShell
- **T1102** — Web Service
- **T1027** — Obfuscated Files or Information
- **T1082** — System Information Discovery
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1497.001** — System Checks
- **T1090.002** — External Proxy

### 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
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-2** — Identification and Authentication (Organizational Users)

### CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

### HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

### SOC2-TSC

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

### ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

- **A.5.23** — Information security for use of cloud services

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1583.001 | Domains | Resource-Development |
| T1553.002 | Code Signing | Defense-Evasion |
| T1195.002 | Compromise Software Supply Chain | Initial-Access |
| T1071.001 | Web Protocols | Command-And-Control |
| T1573.001 | Symmetric Cryptography | Command-And-Control |
| T1112 | Modify Registry | Defense-Evasion |
| T1566.002 | Spearphishing Link | Initial-Access |
| T1562.004 | Disable or Modify System Firewall | Defense-Evasion |
| T1543.003 | Windows Service | Persistence |
| T1059.001 | PowerShell | Execution |
| T1102 | Web Service | Command-And-Control |
| T1027 | Obfuscated Files or Information | Defense-Evasion |
| T1082 | System Information Discovery | Discovery |
| T1036.005 | Match Legitimate Resource Name or Location | Defense-Evasion |
| T1497.001 | System Checks | Defense-Evasion |
| T1090.002 | External Proxy | Command-And-Control |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/malicious-7-zip-site... | T3 |
| **Fake 7-Zip downloads are turning home PCs into proxy nodes** | https://radar.offseq.com/threat/fake-7-zip-downloads-are-turning-ho... | T3 |
| **Laced 7-Zip installers turn home PCs into residential proxy nodes** | https://cyberinsider.com/laced-7-zip-installers-turn-home-pcs-into-... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Trojanized ScreenConnect installers evolve, dropping multiple RATs ...** | https://www.acronis.com/en/tru/posts/trojanized-screenconnect-insta... | T3 |
| **Weekly Recap: Proxy Botnet, Office Zero-Day, MongoDB Ransoms ...** | https://thehackernews.com/2026/02/weekly-recap-proxy-botnet-office-... | T3 |



Generated 2026-03-29 18:42 UTC by TJS Security Command Center