INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-09 15:01 UTC

Lurking Lizard's Residential Proxy Machine: How Trojanized Software Becomes Monetized Infrastructure

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0638
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows, macOS, Android; trojanized: 7-Zip installer, WhatsApp installer, WireVPN app (1M+ downloads), fake TikTok/YouTube downloaders; impersonated proxy brands: IPIDEA, SmartProxy/Decodo, IP Royal, 911Proxy
Published	2026-07-09T00:01:49
Discovery Source	Rss

Executive Summary

A China-nexus threat actor tracked as Lurking Lizard has operated a multi-year campaign, active since at least August 2022, that silently converts victim devices into residential proxy exit nodes by distributing trojanized software including fake 7-Zip and WhatsApp installers and a WireVPN-branded Android app that surpassed one million downloads. Infected devices on corporate or consumer networks route arbitrary third-party traffic without user awareness, creating uncontrolled network egress, potential liability for traffic originating from company IP space, and a persistent foothold that is difficult to detect through conventional security tooling. Organizations face dual exposure: direct compromise of employee devices and the reputational and legal risk of their IP addresses appearing in proxy traffic logs associated with fraud, scraping, or other malicious activity.

Technical Analysis

Lurking Lizard operates an end-to-end proxyware monetization infrastructure spanning Windows, macOS, and Android. Initial access is achieved through trojanized installers distributed via lookalike download domains impersonating legitimate software titles (7-Zip, WhatsApp, WireVPN, TikTok/YouTube downloaders). The WireVPN-branded Android application reportedly exceeded one million downloads before removal. Once executed, the proxyware component silently enrolls the victim device as a residential proxy exit node; bandwidth is then resold through fraudulent proxy service brands impersonating IPIDEA, SmartProxy/Decodo, IP Royal,

and 911Proxy. No CVE is assigned; the campaign maps to CWE-494 (download of code without integrity check), CWE-506 (embedded malicious code/trojanized software), and CWE-693 (protection mechanism failure used to evade detection). MITRE ATT&CK techniques include T1204.002 (malicious file execution via user interaction), T1036.005 (masquerading as legitimate installer), T1090.002 (external proxy via residential proxy network), T1496 (resource hijacking for bandwidth resale), T1547 (boot/logon autostart for persistence), T1071.001 (C2 over HTTP/S), T1583.001 and T1608.001 (adversary-controlled infrastructure and staged capabilities), T1102 (web service abuse), and T1176 (browser extension abuse). China-nexus attribution and full infrastructure scope are assessed at medium confidence based on Infoblox primary sourcing with secondary corroboration; independent technical verification is pending. No vendor patch applies; remediation is detection- and policy-driven.

Action Checklist

1. Step 1: Containment, Block known Lurking Lizard distribution domains and impersonated proxy brand infrastructure at DNS and perimeter. Block outbound connections to known residential proxy port ranges (TCP 80, 443, 8080, 1080, and ephemeral ports used by proxyware C2) unless explicitly authorized per application whitelist. Isolate any endpoint where trojanized software execution is confirmed. Enforce CIS 4.4 and CIS 4.5 (server and endpoint firewall with default-deny outbound rules) to limit unauthorized egress.
2. Step 2: Detection, Query endpoint logs and DNS telemetry for connections to domains impersonating IPIDEA, SmartProxy/Decodo, IP Royal, or 911Proxy. Hunt for processes spawned by installer executables claiming to be 7-Zip, WhatsApp, or WireVPN that exhibit outbound network behavior post-installation. Review AU-2 (Event Logging) and AU-6 (Audit Record Review) coverage for process creation, network socket establishment, and autostart registry or launch daemon modifications consistent with T1547. Flag mobile device management (MDM) inventory for WireVPN or similarly named Android sideloaded applications per CIS 2.1 and CIS 2.3. Check for unexpected bandwidth consumption on endpoints as a behavioral indicator of T1496 resource hijacking.
3. Step 3: Eradication, Remove all identified trojanized applications and associated persistence mechanisms (autostart entries, scheduled tasks, launch agents/daemons). Verify software inventory against known-good hashes for 7-Zip, WhatsApp, and other impersonated titles using CIS 2.1 and CIS 2.2 controls; replace any unverifiable copies with vendor-signed binaries obtained directly from official sources. Enforce CM-14 (signed components) to prevent reinstallation of unsigned or unverified software. Revoke and rotate credentials for any account that authenticated on a confirmed compromised device per D3-CRO (Credential Rotation).
4. Step 4: Recovery, Validate that all identified proxyware processes are absent from affected endpoints via post-remediation endpoint scan. Confirm outbound traffic profiles have normalized; monitor DNS query logs and netflow data for residual C2 beaconing consistent with T1071.001 for a minimum of 30 days post-remediation. Ensure AU-12 (Audit Record Generation) is active and logging process creation and network events on remediated hosts. Re-image endpoints where full artifact confidence cannot be established.
5. Step 5: Post-Incident, Conduct a gap assessment against CIS 7.1 and CIS 7.2 (vulnerability and remediation management process) to evaluate whether software vetting controls would have detected trojanized installers prior to execution. Implement or strengthen software allowlisting (CM-7, Least Functionality) to restrict execution of unapproved applications on managed endpoints. Establish a documented process for validating installer integrity (CM-14) before deployment. Review third-party and

BYOD mobile device policies given the Android delivery vector. Assess whether CIS 6.3 and CIS 6.5 (MFA for external and administrative access) are enforced on accounts that may have been active on compromised devices.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, privacy counsel, and executive leadership if forensic analysis confirms that corporate network bandwidth was actively monetized as a residential proxy exit node routing third-party traffic, as this may constitute unauthorized network access by third parties and trigger breach notification obligations under applicable data protection regulations (e.g., GDPR Article 33, state breach notification laws) if sensitive internal traffic was exposed or exfiltrated through the proxy tunnel.
Recovery Notes	Post-containment, verify that all endpoints restored to production show normalized outbound bandwidth consistent with pre-infection baselines, specifically confirming absence of sustained high-volume TCP connections on ports 1080, 8080, and high ephemeral ranges that characterize Lurking Lizard proxyware tunneling. Monitor DNS query telemetry and netflow data continuously for a minimum of 30 days given the campaign's demonstrated persistence since August 2022, as re-infection via trojanized installers redistributed through the same social engineering channels remains a credible risk. Any Android BYOD devices that cannot be confirmed clean through MDM remote inspection should be treated as unmanaged and blocked from corporate network access until a verified factory reset and clean application install can be documented.
Forensic Artifacts	Trojanized installer binaries on disk: SHA-256 hash mismatches against official 7-Zip (7-zip.org/download.html), WhatsApp Desktop (whatsapp.com/download), and WireVPN release hashes, located in user Download directories (%USERPROFILE%\Downloads) or browser cache paths, indicating the impersonated software delivery vector | Windows autostart registry keys and scheduled tasks created by proxyware dropper: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon` entries referencing non-standard binary paths in %AppData% or %Temp%, and task XML files in `C:\Windows\System32\Tasks\` with creation timestamps post-installer execution | macOS LaunchAgent or LaunchDaemon plist files installed by the trojanized application in `~/Library/LaunchAgents/` or `/Library/LaunchDaemons/` with `RunAtLoad=true` and `ProgramArguments` pointing to a proxyware executable, paired with the associated binary in `~/Library/Application Support/` subdirectories | DNS query logs showing resolution attempts to domains impersonating IPIDEA, SmartProxy/Decodo, IP Royal, or 911Proxy infrastructure, capturable from Windows DNS Client Event ID 3006, Sysmon Event ID 22, or recursive resolver query logs, with timestamps correlating to the trojanized installer execution window | Outbound netflow or pcap data showing sustained high-volume TCP sessions from infected endpoints to residential proxy C2 infrastructure on ports 1080, 8080, or high ephemeral ranges, with anomalous data transfer volumes inconsistent with the endpoint's role — directly evidencing the resource hijacking and unauthorized proxy egress behavior characteristic of Lurking Lizard monetization infrastructure

Per-Action IR Details

Step 1: Containment — Block known Lurking Lizard distribution domains and impersonated proxy brand infrastructure at DNS and perimeter. Restrict outbound connections to known residential proxy port ranges

(typically TCP 80, 443, 8080, 1080, and high-range ephemeral ports used by proxyware C2). Isolate any endpoint where trojanized software execution is confirmed. Enforce CIS 4.4 and CIS 4.5 (server and endpoint firewall with default-deny outbound rules) to limit unauthorized egress.

NIST Phase: Containment

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

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Windows endpoints, run `netsh advfirewall firewall add rule name='Block Proxyware Egress' dir=out action=block protocol=TCP remoteport=1080,8080` to block SOCKS/HTTP proxy ports immediately. Use pfSense or OPNsense with a Response Policy Zone (RPZ) feed to DNS-sinkhole domains impersonating IPIDEA, SmartProxy/Decodo, IP Royal, and 911Proxy. For isolated endpoints, disable the NIC via `Disable-NetAdapter -Name '*' -Confirm:$false` in PowerShell before any further action to preserve volatile state.

Evidence: Before isolating any suspected host, capture: (1) full RAM image using Magnet RAM Capture or WinPmem to preserve proxyware process memory, injected threads, and C2 socket state; (2) active TCP/UDP connection snapshot via `Get-NetTCPConnection | Where-Object {$_.State -eq 'Established'} | Export-Csv connections.csv` and `netstat -ano` output; (3) running process list with parent-child relationships via `Get-Process | Select-Object Id,ProcessName,Path,StartTime | Export-Csv processes.csv`; (4) DNS cache via `ipconfig /displaydns > dnscache.txt` to capture any resolved impersonated proxy domains before network isolation flushes resolver state.

Step 2: Detection — Query endpoint logs and DNS telemetry for connections to domains impersonating IPIDEA, SmartProxy/Decodo, IP Royal, or 911Proxy. Hunt for processes spawned by installer executables claiming to be 7-Zip, WhatsApp, or WireVPN that exhibit outbound network behavior post-installation. Review AU-2 (Event Logging) and AU-6 (Audit Record Review) coverage for process creation, network socket establishment, and autostart registry or launch daemon modifications consistent with T1547. Flag mobile device management (MDM) inventory for WireVPN or similarly named Android sideloaded applications per CIS 2.1 and CIS 2.3. Check for unexpected bandwidth consumption on endpoints as a behavioral indicator of T1496 resource hijacking.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software)

Compensating: Deploy Sysmon with a SwiftOnSecurity-based config; hunt using Event ID 1 (Process Create) filtering on `Image` paths matching `7z*.exe`, `WhatsApp*.exe`, or `WireVPN*.exe` with `ParentCommandLine` not matching official update or system processes. Use Event ID 3 (Network Connection) to identify those same process images making outbound connections on TCP 1080, 8080, or high ephemeral ports (>49152). On macOS, use `log stream --predicate 'processImagePath contains "WireVPN"'` and inspect `~/Library/LaunchAgents/` and `/Library/LaunchDaemons/` for plist persistence. For Android, use `adb shell pm list packages` to identify WireVPN or lookalike package names and `adb shell dumpsys netstats` to quantify anomalous data throughput.

Evidence: This step is detection/analysis and does not alter live system state; however, log collection should precede any active process termination. Collect: (1) Windows Security Event Log Event ID 4688 (Process Creation with command line auditing enabled) filtering on installer binary names; (2) Sysmon Event ID 7 (Image Loaded) to detect DLL side-loading by trojanized installers; (3) DNS query logs from the resolver or endpoint (Windows Event ID 3006 if DNS Client logging is enabled, or Sysmon Event ID 22) for queries resolving to IPIDEA/SmartProxy/Decodo/IP Royal/911Proxy lookalike domains; (4) Windows Event ID 4698/4702 (Scheduled Task Created/Modified) and registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` for proxyware autostart entries; (5) Android MDM enrollment records and app installation timestamps for WireVPN package installs occurring after August 2022.

Step 3: Eradication — Remove all identified trojanized applications and associated persistence mechanisms (autostart entries, scheduled tasks, launch agents/daemons). Verify software inventory against known-good hashes for 7-Zip, WhatsApp, and other impersonated titles using CIS 2.1 and CIS 2.2 controls; replace any

unverifiable copies with vendor-signed binaries obtained directly from official sources. Enforce CM-14 (signed components) to prevent reinstallation of unsigned or unverified software. Revoke and rotate credentials for any account that authenticated on a confirmed compromised device per D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST CM-14 (Signed Components), NIST CM-7 (Least Functionality)

Compensating: Use `Get-FileHash -Algorithm SHA256 ` in PowerShell to compare hashes of installed 7-Zip and WhatsApp binaries against the official 7-Zip SHA-256 checksums published at 7-zip.org and WhatsApp's desktop release page; any mismatch confirms trojanization. Remove persistence via `schtasks /delete /tn /f` for scheduled tasks and manually delete identified `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` keys. On macOS, use `launchctl unload` on identified plist files before deleting them from `~/Library/LaunchAgents/`. For Android WireVPN, use `adb uninstall ` if MDM remote wipe of the app is unavailable. Use ClamAV with a YARA rule matching the proxyware dropper pattern to scan remaining endpoints before credential rotation.

Evidence: Before revoking credentials or removing persistence mechanisms, capture: (1) a forensic image or at minimum a file system timeline of `%AppData%`, `%ProgramData%`, and `%Temp%` directories where the trojanized 7-Zip or WhatsApp installer would have dropped proxyware components; (2) export all scheduled tasks via `schtasks /query /fo CSV /v > tasks_before_removal.csv`; (3) registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, and `HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` before deletion; (4) on macOS, copy all plist files from LaunchAgents/LaunchDaemons directories before `launchctl unload`; (5) document all account authentication events (Windows Security Event ID 4624/4625) on the compromised host for the period since initial infection to determine lateral movement or credential exposure scope before rotating.

Step 4: Recovery — Validate that all identified proxyware processes are absent from affected endpoints via post-remediation endpoint scan. Confirm outbound traffic profiles have normalized; monitor DNS query logs and netflow data for residual C2 beaconing consistent with T1071.001 for a minimum of 30 days post-remediation. Ensure AU-12 (Audit Record Generation) is active and logging process creation and network events on remediated hosts. Re-image endpoints where full artifact confidence cannot be established.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST CP-10 (System Recovery And Reconstitution), CIS 8.2 (Collect Audit Logs)

Compensating: Run a post-remediation osquery query — `SELECT name, path, pid FROM processes WHERE path LIKE '%AppData%' OR path LIKE '%Temp%'` — to confirm no proxyware processes remain resident in non-standard directories. Use Wireshark or `tcpdump -i any -w post_remediation.pcap port 1080 or port 8080` for 72 hours post-remediation to detect any residual outbound proxy tunneling. Set up a Sigma rule (sigma/rules/network) matching DNS queries to known Lurking Lizard infrastructure patterns and pipe it against local DNS server query logs. For re-imaged hosts, restore only from backups predating August 2022 or from clean vendor media, as the campaign has been active since that date.

Evidence: Before re-imaging any endpoint, ensure a full forensic disk image has been acquired using a write blocker (e.g., `dc3dd if=/dev/sda of=host_image.dd hash=sha256`) to preserve the complete artifact record for potential legal or regulatory purposes. Confirm that memory acquisition from containment phase is retained. Post-recovery, verify baseline process and network telemetry is captured via Sysmon Event ID 1 and 3 on the restored host for the first 30 days as a clean behavioral baseline against which any proxyware re-infection can be detected.

Step 5: Post-Incident — Conduct a gap assessment against CIS 7.1 and CIS 7.2 (vulnerability and remediation management process) to evaluate whether software vetting controls would have detected trojanized installers prior to execution. Implement or strengthen software allowlisting (CM-7, Least Functionality) to restrict execution of unapproved applications on managed endpoints. Establish a documented process for validating installer integrity (CM-14) before deployment. Review third-party and BYOD mobile device policies given the Android delivery vector. Assess whether CIS 6.3 and CIS 6.5 (MFA for external and administrative access) are enforced on accounts that may have been active on compromised devices.

NIST Phase: Post Incident

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST CM-7 (Least Functionality), NIST CM-14 (Signed Components), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Implement Windows Defender Application Control (WDAC) or AppLocker policies to allowlist only publisher-signed binaries from official 7-Zip, Meta (WhatsApp), and known VPN vendors — blocking unsigned or self-signed executables that impersonate these brands. Create a pre-deployment integrity checklist requiring SHA-256 hash verification against the vendor's official release page before any installer is permitted on managed endpoints. For BYOD Android devices, enforce an MDM policy (e.g., Microsoft Intune free tier or Google Workspace endpoint management) prohibiting sideloaded APKs (sources outside Google Play) and flagging WireVPN or similarly named applications. Document lessons learned in a post-incident report referencing the August 2022 campaign start date to quantify the organization's exposure window.

Evidence: No volatile evidence capture is required at this phase as active threat activity has been eradicated. Retain all forensic artifacts, memory images, disk images, log exports, and network captures from prior phases for a minimum retention period consistent with NIST AU-11 (Audit Record Retention) and applicable regulatory requirements. Compile the full artifact timeline from August 2022 campaign onset through remediation to support gap analysis, regulatory notification assessment, and intel sharing with ISACs if corporate network egress was used as a residential proxy exit node for third-party traffic.

Detection Guidance

Primary detection signals center on three behavioral patterns: (1) Outbound proxy traffic, hunt for sustained outbound TCP sessions on ports 80, 443, 1080, 8080, or high-range ephemeral ports from endpoints that do not have a documented proxy role; correlate against netflow or firewall session logs for anomalous bandwidth volume per host (T1496, T1090.002). (2) Suspicious installer execution, query EDR process creation logs for parent-child relationships where a file claiming to be a legitimate installer (7-Zip, WhatsApp, WireVPN) spawns an unexpected secondary process or drops a binary to a non-standard path; apply D3-SFA (System File Analysis) to monitor for post-install file drops in startup or temp directories. (3) Persistence mechanisms, search for new autostart registry keys (HKCU/HKLM Run), scheduled tasks, or macOS LaunchAgent/LaunchDaemon plist entries created in proximity to a software installation event, consistent with T1547; apply D3-SICA (System Init Config Analysis). For DNS-layer detection, flag resolutions of domains associated with the impersonated proxy brands (IPIDEA, SmartProxy/Decodo, IP Royal, 911Proxy) and any newly registered lookalike domains impersonating major software download sites. Mobile: query MDM for Android applications installed outside the official Play Store with names or package identifiers matching WireVPN or similar VPN-branded apps. Note that IOC-based detection alone is insufficient given the campaign's use of residential IP infrastructure and domain impersonation to blend traffic; behavioral analytics on outbound session volume and process lineage are the higher-confidence detection path.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`wirevpn[.]com (impersonation variant — verify exact lookalike domain via Infoblox report)`	Distribution domain associated with trojanized WireVPN-branded Android app exceeding 1M downloads; exact lookalike domain strings should be sourced directly from Infoblox advisory	MEDIUM
DOMAIN	`Impersonated proxy brand domains (IPIDEA, SmartProxy/Decodo, IP Royal, 911Proxy lookalikes)`	Campaign infrastructure impersonates legitimate proxy service brands to resell victim bandwidth; specific domain strings not enumerated in available source summaries — obtain full IOC list from Infoblox primary report	MEDIUM
URL	`Lookalike download domains impersonating 7-Zip and WhatsApp official sites`	Used for trojanized installer distribution; specific URLs not available in source summaries — reference Infoblox primary report for enumerated infrastructure	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1102** — Web Service
- **T1090.002** — External Proxy
- **T1583.001** — Domains
- **T1608.001** — Upload Malware
- **T1204.002** — Malicious File
- **T1496** — Resource Hijacking
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1547** — Boot or Logon Autostart Execution
- **T1071.001** — Web Protocols
- **T1176** — Software Extensions

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **AT-2** — Literacy Training and Awareness
- **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
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **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
T1102	Web Service	Command-And-Control
T1090.002	External Proxy	Command-And-Control
T1583.001	Domains	Resource-Development
T1608.001	Upload Malware	Resource-Development
T1204.002	Malicious File	Execution
T1496	Resource Hijacking	Impact
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1071.001	Web Protocols	Command-And-Control
T1176	Software Extensions	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/fake-7-zip-installers-turn-device...	T2
Proxyware actor behind fake 7-Zip is bigger than you think!	https://www.infoblox.com/blog/threat-intelligence/fake-installers-f...	T3
Fake 7-Zip and WireVPN Installers Built a Residential Proxy ...	https://www.mallory.ai/stories/019f435a-f725-7dc3-9618-3659ae96d590	T3
Fake 7-Zip Installer Drops Proxyware Trojan	https://www.smarttech247.com/threat-intel-reports/fake-7-zip-instal...	T3
Lurking Lizard Uses Fake 7-Zip Installers to Turn Victim ...	https://cybersecuritynews.com/lurking-lizard-uses-fake-7-zip-instal...	T3

Generated 2026-07-09 15:01 UTC by TJS Security Command Center