Lurking Lizard

Target Bio

Names/Alias: Lurking Lizard

Affiliations: IPIDEA Proxy Provider

Motivation: Financial Gain

First Activity: Mid 2022

Structure: Cyber supply chain

Country of Basis: China

Targets: End-to-end users

Methodology: Lookalike domains, trojans, proxies

Most Recent Development: Fake 7-Zip Trojan Software to make remote proxies.

BLUF

Lurking Lizard, a China-based threat group, operates a sophisticated proxy-as-a-crime-service business that has already compromised hundreds of thousands of devices through trojanized software. Their established supply chain and cross-platform reach position them as a significant enabler of downstream cybercriminal activity with substantial economic impact on the global digital infrastructure.

Background

Operating from Wuhan, China, the threat group known as Lurking Lizard has actively maintained a massive malicious residential proxy network since mid-2022 [4]. Rather than deploying traditional ransomware or destructive malware, the group monetizes operations by trojanizing legitimate utility software like 7-Zip (7zip[.]com) to covertly recruit victim bandwidth and rent it out to other cybercriminals [2]. Their infrastructure spans over 230 lookalike domains spoofing services like HeroSMS, WireVPN, and major proxy firms such as SmartProxy and IPIDEA [5]. Analysis of these domains reveals overlapping registrant information and specific WHOIS metadata connecting the group's origins directly to Wuhan, China.

Summary (General Overview)

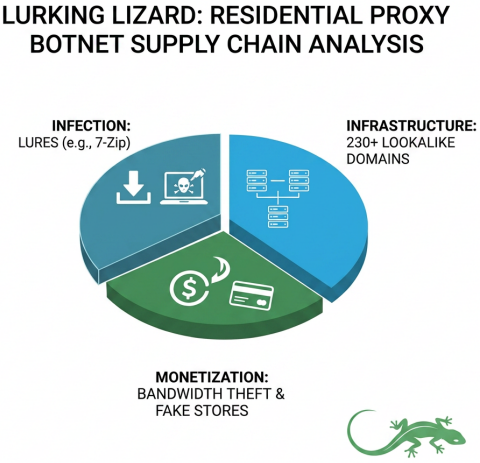
The Lurking Lizard threat group operates a sophisticated residential proxy network by deceiving users into installing trojanized versions of popular software tools and applications [1][2]. The group's primary infection vector involves creating convincing lookalike domains such as 7zip[.]com instead of the legitimate 7-zip.org and using search engine poisoning to direct unsuspecting users to counterfeit software installers [2][4]. Their targeted applications include 7-Zip, WhatsApp, WireVPN, and various TikTok and YouTube downloaders, with the operation expanding across Windows, macOS, and Android platforms [3][4]. When victims unknowingly download and execute these trojanized installers, silent malware integration converts their devices into proxy nodes that route third-party internet traffic without user knowledge or consent [1][2]. The group primarily targets individual end-users and consumers seeking legitimate software through web searches and mobile app stores, with the Android application "wirevpn - Fast Unlimited Proxy" accumulating over one million downloads on the Google Play Store [3][4]. Through their vertically integrated operation, Lurking Lizard monetizes this compromised infrastructure by reselling access to other cybercriminals under fraudulent commercial proxy service names.

Details and References

Analysis Summary

Lurking Lizard's vertically integrated criminal business model controlling everything from device acquisition through final monetization distinguishes it from standard malware operations and demonstrates sophisticated understanding of criminal supply chain economics [1][2]. The group's exploitation of user trust in established software brands through lookalike domains, search engine poisoning, and placement on legitimate mobile app stores represents a deliberate strategy to maximize victim acquisition [2][3][4]. The resilience of this business model suggests the threat group will likely continue scaling operations and may serve as critical infrastructure for a broader ecosystem of cybercriminal activity. By providing low-cost access to residential proxy nodes, the group enables downstream attacks including financial fraud, credential theft, and account takeovers that security systems cannot detect when routed through legitimate consumer IP addresses [1]. The economic implications extend beyond individual victims' enterprises cannot distinguish legitimate traffic from malicious third-party traffic routed through compromised consumer devices, creating cascading supply chain vulnerabilities that impact organizations globally [1][5].

Security researchers recommend prioritizing direct-source software acquisition as a primary defense, with users downloading applications exclusively from official, verified websites rather than relying on search results or third-party distribution channels [5]. Additionally, caution toward independent review platforms promoting obscure software is advised, as Lurking Lizard leverages fraudulent review sites to funnel users toward malicious storefronts [2]. Organizations should implement network monitoring to detect devices exhibiting proxy node behavior, such as unexplained outbound traffic patterns or multiple concurrent external connections and educate end-users on the risks of downloading software outside official distribution channels [2][5].



Resources

[1] https://www.zawya.com/en/press-release/research-and-studies/how-fake-7-zip-software-exposed-a-much-bigger-criminal-proxy-business-fr43efqj

[2] https://securityaffairs.com/194990/malware/fake-vpn-and-7-zip-apps-turn-victims-into-residential-proxy-nodes.html

[3] https://thehackernews.com/2026/07/fake-7-zip-installers-turn-devices-into.html

[4] https://blog.actipace.com/news/2026/07/lurking-lizard-uses-fake-software-installers-to-build-malicious-proxy-network/

[5] https://www.technadu.com/infoblox-report-details-residential-proxy-campaign-activity/630649/