VexTrio Hackers Use Fake CAPTCHAs and Malicious Apps on Google Play

Data: 2025-08-13 12:10:08

Autor: Inteligência Against Invaders

Security researchers at Infoblox Threat Intel have revealed the complex workings of VexTrio, a highly skilled cybercriminal network that has been active since at least 2017. This discovery highlights the ongoing dangers in the digital economy.

Formerly known simply as VexTrio, this group now dubbed VexTrio Viper leverages advanced traffic distribution systems (TDSs), lookalike domains, and registered domain generation algorithms (RDGAs) to orchestrate global attacks.

Decade-Long Cybercrime Empire

By brokering traffic through the largest known cybercriminal affiliate program, VexTrio delivers malware, scams, and illicit content to users worldwide, making it one of the most pervasive threats observed in enterprise networks.

Their adept manipulation of DNS infrastructure enables seamless redirection chains, often embedding malicious smartlinks in compromised websites, social media platforms like Instagram and Facebook, and even email security tools.

This TDS trifecta not only cloaks landing pages to evade security analysis but also funnels victims into proprietary scam verticals, including dating, cryptocurrency, sweepstakes, and nutra industries, where VexTrio profits both as brokers and content creators.

At the heart of VexTrio's arsenal are deceptive mechanisms like fake CAPTCHA challenges, which have persisted in fraudulent activities for years, luring users into granting browser notification permissions or revealing personal data under the guise of verification.

These CAPTCHAs, often featuring infamous robot imagery, serve as gateways to persistent access, enabling spam and scam delivery.

Deceptive Tactics

The group's operations extend to malicious mobile applications distributed via Google Play and the Apple App Store, amassing over a million downloads collectively.

Under developer aliases such as HolaCode, LocoMind, Hugmi, Klover Group, and AlphaScale Media, apps like Hugmi, Cheri, WinkChat, Spam Shield, and Fast VPN masquerade as legitimate tools for dating, spam blocking, and virtual private networks (VPNs).

In reality, these apps bombard users with incessant advertisements, enforce hard-to-cancel subscriptions, and harvest email addresses through cost-per-action models.

Technical analysis reveals shared codebases and hosting overlaps with VexTrio's affiliates, including Prague-based Techintrade and Oilimpex, raising questions about blurred lines between the core group and its partners.

DNS records further tie these apps to VexTrio's dedicated IP ranges, such as those in AS5368, confirming control over scam toolkits that infringe on brands like Tinder, PornHub, and even high-profile figures including Elon Musk and Donald Trump in cryptocurrency fraud schemes.

Compounding the threat, VexTrio sustains a vicious spam-scam cycle by operating lookalike email marketing platforms that mimic services like SendGrid and MailGun, utilizing sender policy framework (SPF) records to authorize mass distributions from servers like mail.holaco.de.

Their domains, including datingcell.com and fidelitymail.com, boast access to over 220 million email addresses sourced from victim interactions on fraudulent sites and integrate third-party services like YNOT Mail for amplified outreach.

Spam emails, personalized with tracking links from trafficiq.com, redirect users to VexTrio-controlled landing pages hosting fake dating portals or investment scams, often resolved via Swiss data centers in AS5398.

This self-reinforcing loop not only feeds affiliate commissions but also expands their database for future campaigns.

Beyond digital fraud, VexTrio's key figures are linked to diverse enterprises, from solar energy investments in Bulgaria to unrelated micro-companies, highlighting the opaque boundaries of their global operations.

As of August 13, 2025, ongoing adaptations to industry reporting underscore VexTrio's resilience, urging enhanced DNS-based threat intelligence and app store vetting to mitigate this mega-threat.