IMPORTANT CYBERSECURITY NEWS: THREAT ACTORS USE TYPO DGA TO EVADE DETECTION IN MALWARE

Vairav Cyber Security News Report

Date: March 10, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Unit 42 researchers have identified a new malware campaign that leverages typo-squatting domain generation algorithms (DGAs) to distribute potentially unwanted Android applications. The campaign involves newly registered domains (NRDs) mimicking legitimate websites with intentional typographical errors. By employing a rapid domain turnover strategy, attackers evade traditional security filters, redirecting users to malicious landing pages that promote unwanted software and adult content.

INCIDENT ANALYSIS

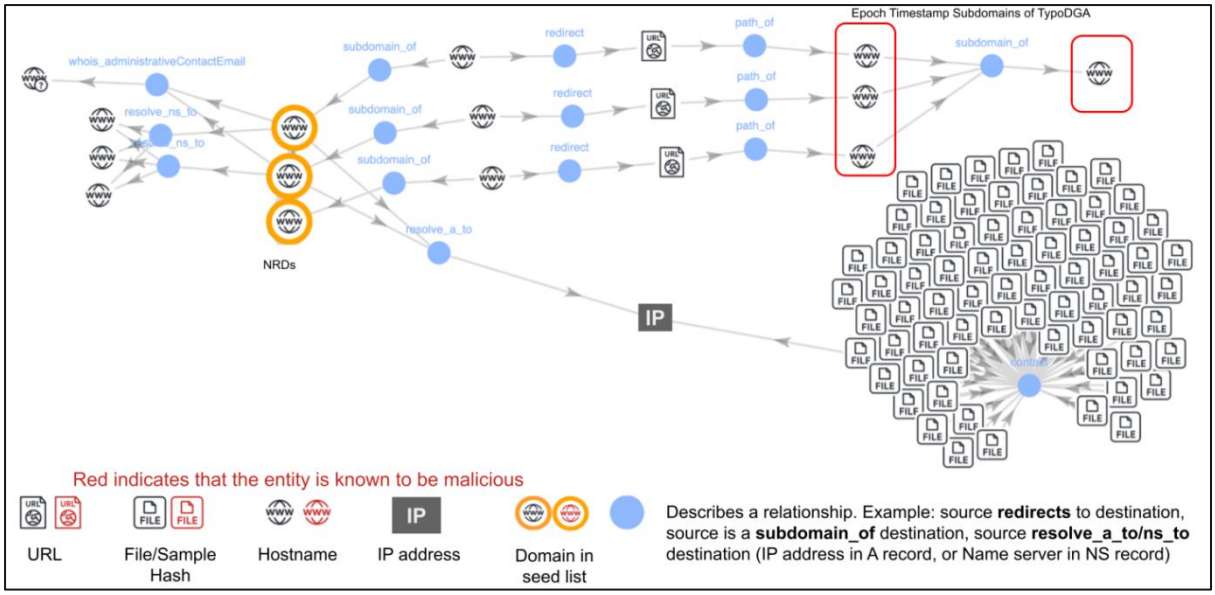

Figure 1: Part of the campaign depicting three NRDs redirecting to typo DGA subdomains

Attackers are leveraging typo-squatting domain generation algorithms (DGAs) to create domains with subtle misspellings, such as "*pictidentifyive[.]pro*," to evade detection by security filters.

Shared WHOIS Information

Researchers linked 6,057 NRDs to a single entity using the email address *fangyuanhenry20230927@outlook[.]com*. Domain registrations spiked in October 2024 (2,634 domains) before declining in November (1,172 domains).

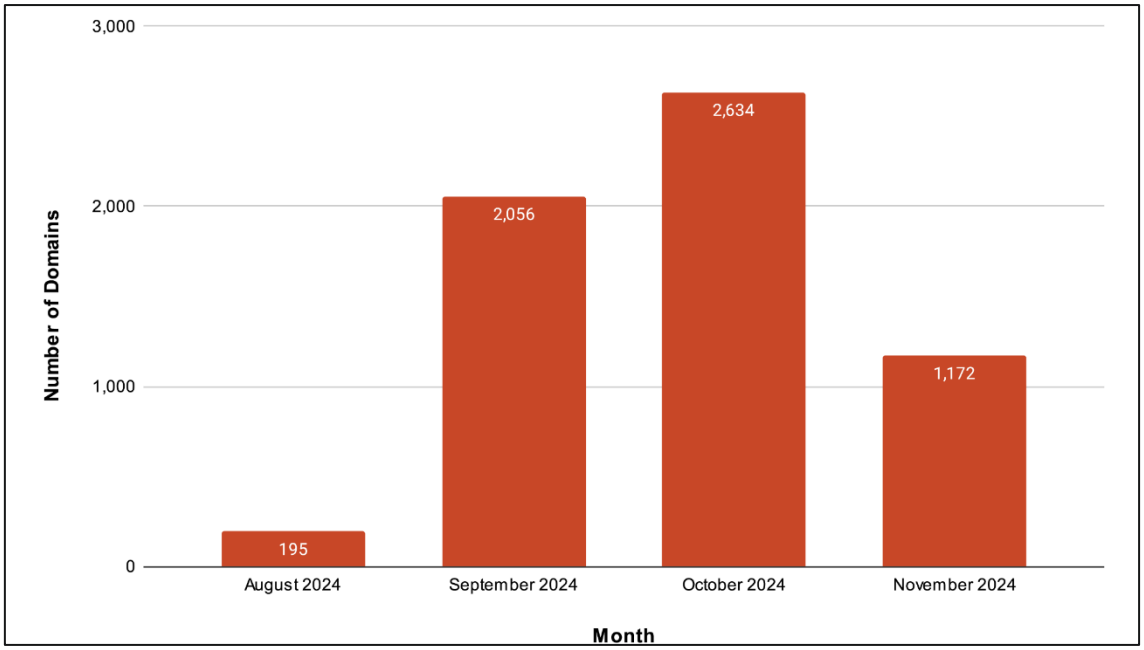

Figure 2: Creation dates of all 6,057 NRDs found in the campaign

Shared Hosting & Redirection

All NRDs resolved to *91.195.240[.]123*, enabling centralized control. The automated attack strategy relies on epoch timestamps to trigger redirections *hxxps://121.y1ly6n[.]us* → *hxxps://1731804190472.gratsuccessfic[.]pro* at scheduled intervals, allowing attackers to quickly swap domains and minimize detection windows.

Landing Pages

These short-lived landing pages enable attackers to continuously register and abandon domains, making it difficult for security systems to track and block them. Ultimately, victims are redirected to malicious websites promoting unwanted Android applications and adult content. Over 96% of the related samples were malicious executables, highlighting the campaign's high-risk nature.

Detection Through Threat Actor Infrastructure

Researchers identified 444,898 domains linked to the same registrant email, with 99.98% resolving to *91.195.240[.]123*, indicating a vast malicious network. The domains followed a pattern of bulk registrations and rapid turnover, that redirects to 178 typo DGA. While no direct link to the NRD operator was found, the consistent use of the *.pro* TLD suggests further investigation. Each typo DGA domain averaged 67 unique subdomains.

Figure 3: Example landing page with adult content distributing potentially unwanted applications

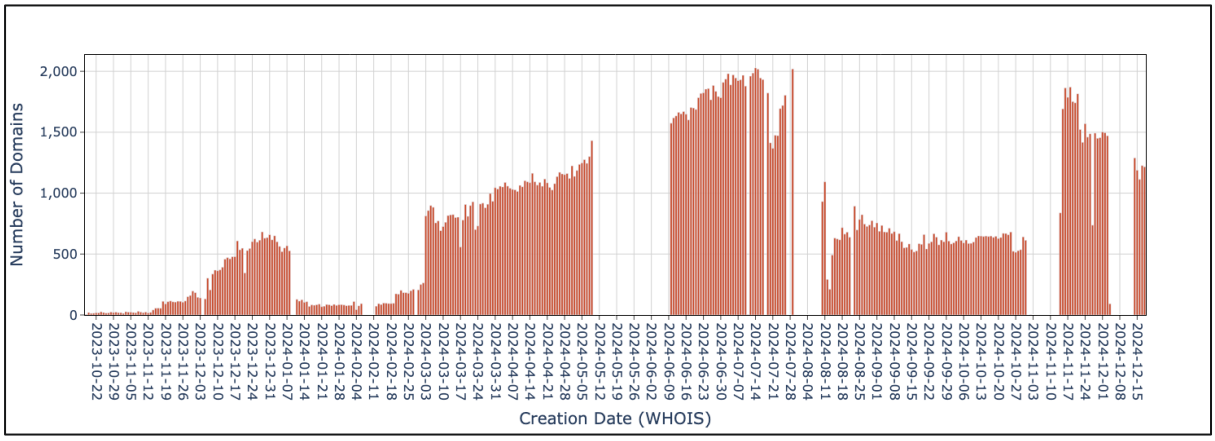

Figure 4: Creation dates of 444,898 domains belonging to the same actor

The emergence of typo DGAs in malware campaigns showcases threat actors' adaptability in bypassing security controls. Proactive cybersecurity measures mitigate these evolving threats, including real-time domain monitoring and user awareness.

RECOMMENDED ACTIONS

- Implement DGA detection models to identify and block typo-squatted domains.
- Organizations should restrict access to newly registered and suspicious domains to minimize exposure.
- Educate users to avoid clicking unknown links and verify URLs before downloading applications.
- Leverage AI-powered security tools to detect and analyze fast-changing attack infrastructures.

RESOURCES

https://securityonline.info/typo-dgas-a-new-tactic-in-malicious-redirection-campaigns/

https://unit42.paloaltonetworks.com/typo-domain-generation-algorithms/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com