UNIT 42
BY PALO ALTO NETWORKS

The Next Level: Typo DGAs Used in Malicious Redirection Chains

Executive Summary

We have uncovered a new campaign in which an attacker leverages newly registered domains (NRDs) and introduces a new variant of domain generation algorithms (DGAs) potentially designed to avoid detection. We found this through our novel graph-intelligence based pipeline. The system infers attack campaigns by correlating domain registrations with hosting infrastructure, passive DNS and WHOIS data.

This campaign used over 6,000 NRDs that redirected to similar paths on domains resembling those generated by dictionary-based DGAs. Dictionary DGAs are a DGA variant that combines dictionary words to create domain names resembling legitimate ones, thus hindering detection by security systems.

These NRDs redirected users to URLs that lead to advertisements of potentially unwanted Android applications. Analysis of files contacting the NRDs' IP address revealed that 96% (89 of 92) were malicious.

Broadening the scope of our investigation, we found that there were 444,898 NRDs belonging to the same actor. These NRDs redirected to 178 domains exhibiting dictionary DGA-like characteristics.

We identified a new pattern in these 178 domains, which we call typo DGAs: dictionary DGA domains containing typographical errors. For example, `pictidentifyive[.]pro` is a typo DGA that could be a combination of the words “picture,” “identify” and “five” with some letters deleted. This typo DGA pattern suggests a new dictionary DGA variant designed to evade traditional detection methods.

Palo Alto Networks customers are better protected through the following products and services:

Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.

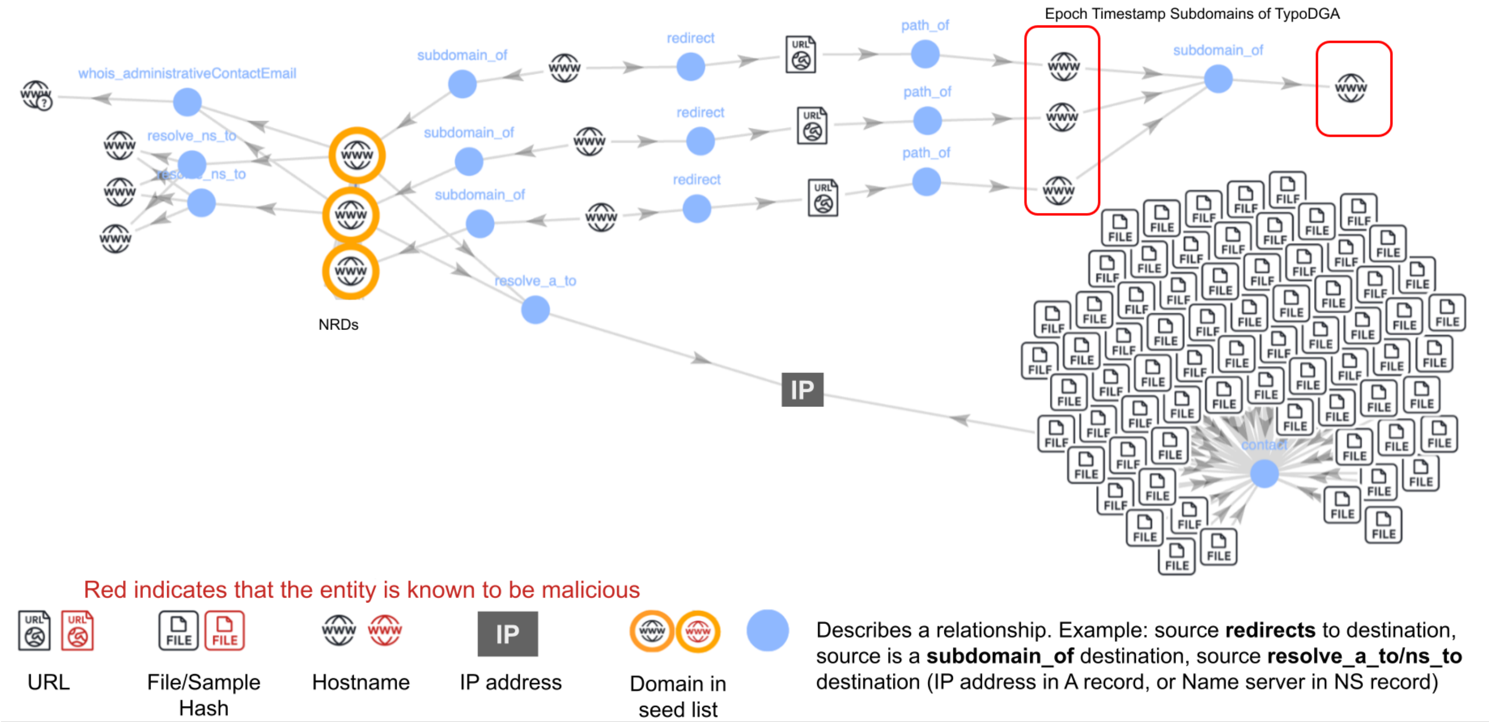
If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics	**DNS**

The Typo DGA and Redirection Campaign

Our graph-intelligence based detection system, described in our article TLD Tracker: Exploring Newly Released Top-Level Domains, has uncovered a new campaign. This campaign has used 6,057 newly registered domains, each redirecting to paths under various dictionary DGA-like domains.

Figure 1 illustrates a portion of the campaign, specifically three NRDs redirecting to typo DGA subdomains. These subdomains resolve to a malicious IP address that many malicious file samples contacted.



Describes a relationship. Example: source **redirects** to destination, source is a **subdomain_of** destination, source **resolve_a_to/ns_to** destination (IP address in A record, or Name server in NS record)

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

Shared WHOIS Information

The 6,057 NRDs were alphanumeric strings resembling DGAs, with five to six characters. These domains all shared the same WHOIS information including registrant email address (`fangyuanhenry20230927@outlook[.]com`), which confirms that the same entity registered them.

Figure 2 shows that all the NRDs logged at the time of campaign detection were registered between August-November 2024.

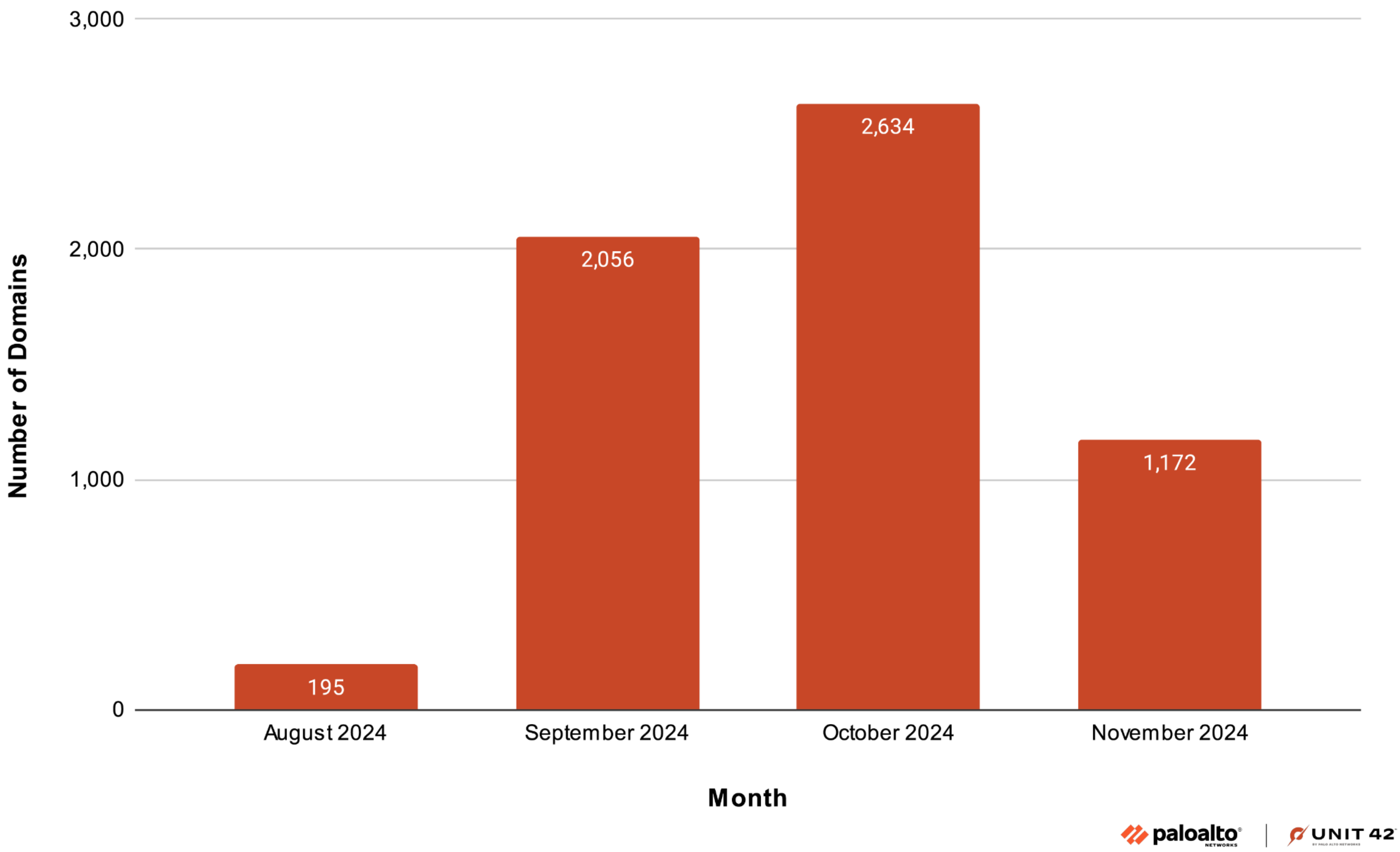


Figure 2. Creation dates of all 6,057 NRDs found in the campaign.

Shared Hosting Infrastructure

We identified this campaign because these NRDs share the same malicious hosting infrastructure and resolve to the same IP address `91.195.240[.]123`.

Redirection to URLs Under Typo DGA Subdomains

Subdomains of these NRDs redirected to URLs under typo DGAs. In this campaign, the typo DGA subdomains used epoch timestamps. These timestamps correspond to the observed redirection times. For example, we observed `hxxps://121.y1ly6n[.]us` redirecting to `hxxps://1731804190472.gratsuccessfic[.]pro` on Nov. 17, 2024, at 00:45:19 UTC.

The epoch timestamp 1731804190472 represents a time two minutes earlier. These epoch timestamp subdomains suggest that the NRD domain registrations and redirections might have been automated and scheduled to trigger at certain times of the day.

Landing Pages

The NRDs' landing pages presented adult Android app download pages (shown in Figure 3). The NRDs all resolved to the same IP address mentioned above, `91.195.240[.]123`. Furthermore, over 96% of the samples (89 of 92) contacting this IP address were malicious executable files.

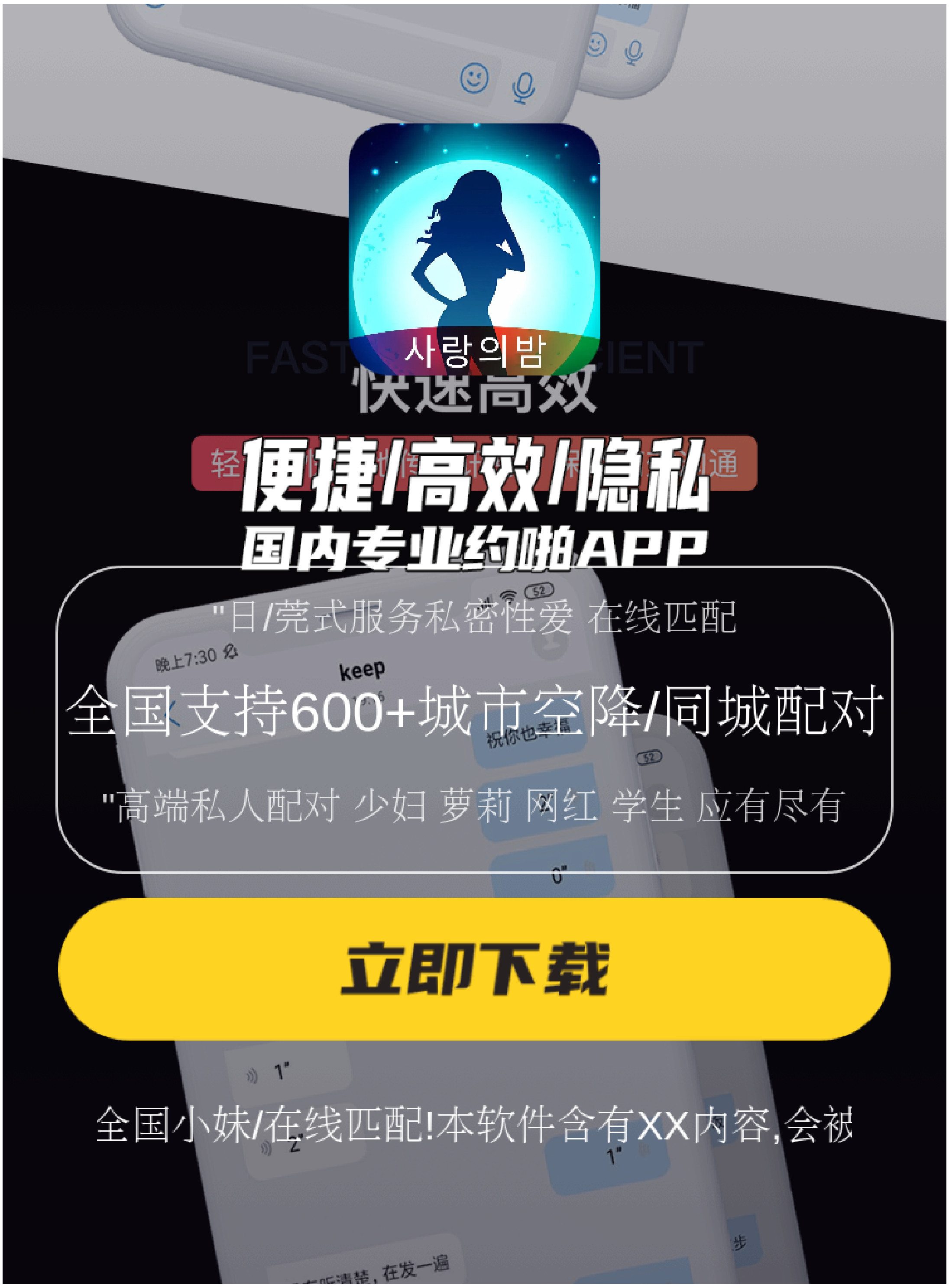

사랑의밤
FAST IENT
快速高效
轻 通
便捷/高效/隐私
国内专业约啪APP
"日/莞式服务私密性爱 在线匹配
全国支持600+城市空降/同城配对
"高端私人配对 少妇 萝莉 网红 学生 应有尽有
立即下载
全国小妹/在线匹配!本软件含有XX内容,会被

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

Using the Threat Actor’s Infrastructure to Expand Detection

We used our graph-intelligence pipeline to search for domains with similar characteristics, expanding the coverage of the campaign. Using the same registrant email address identified above, we identified 444,898 domains. Our passive DNS data shows that nearly all of these (99.98%, or 444,827 domains) resolved to the same IP address (`91.195.240[.]123`). This strong correlation suggests a broader network of potentially malicious activity, even if not all domains are directly involved in this campaign.

Figure 4 shows that the distribution pattern of the domain creation dates suggests that the attacker registered several thousand domains over multiple weeks, followed by periods of reduced activity. The short lifespan of the landing pages and redirection behavior suggests a rapid domain turnover strategy.

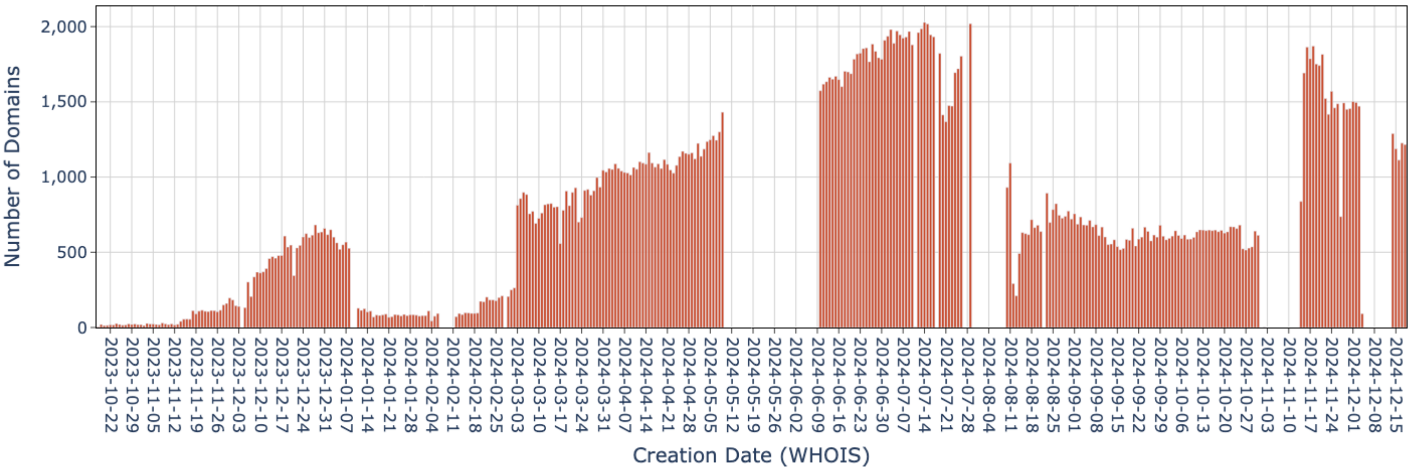


Figure 4. Creation dates of 444,898 domains belonging to the same actor.

Many of these NRDs redirected to 178 distinct typo DGA domains, also employing epoch timestamps in their subdomains. We haven't found direct evidence linking these typo DGA domains to the same actor controlling the NRDs (e.g., shared WHOIS or hosting). However, the consistent use of the less common `.pro` TLD across all 178 domains warrants further investigation.

Furthermore, we found an average of 67 different epoch timestamp subdomains under each typo DGA root domain, which suggests at least that many distinct redirection events.

Conclusion

Our analysis revealed a campaign using typo DGAs, which is a novel dictionary DGA variant designed to evade detection. This campaign highlights the need for advanced detection capabilities like our graph intelligence pipeline. We are actively monitoring and blocking the malicious infrastructure in the campaign we described (tracked as **'typodga_redir'**).

Palo Alto Networks customers are better protected through the following products and services:

Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

NRDs

- `zgi8ij[.]us`
- `ord8w1[.]us`
- `mg77bi[.]us`
- `wnsukh[.]us`
- `y1ly6n[.]us`
- `fdca5[.]us`
- `xwc30[.]us`
- `sloe2[.]us`

IP Address

- `91.195.240[.]123`

Typo DGA Domains

- `pictidentifyive[.]pro`
- `gratsuccessfic[.]pro`
- `emesispushship[.]pro`
- `everybodyform[.]pro`
- `brontalreadyture[.]pro`

Additional Resources

- Fast Flux 101: How Cybercriminals Improve the Resilience of Their Infrastructure to Evade Detection and Law Enforcement Takedowns — Unit 42, Palo Alto Networks
- Newly Registered Domains: Malicious Abuse by Bad Actors – Unit 42, Palo Alto Networks
- Threat Brief: Understanding Domain Generation Algorithms (DGA) – Unit 42, Palo Alto Networks
- TLD Tracker: Exploring Newly Released Top-Level Domains – Unit 42, Palo Alto Networks