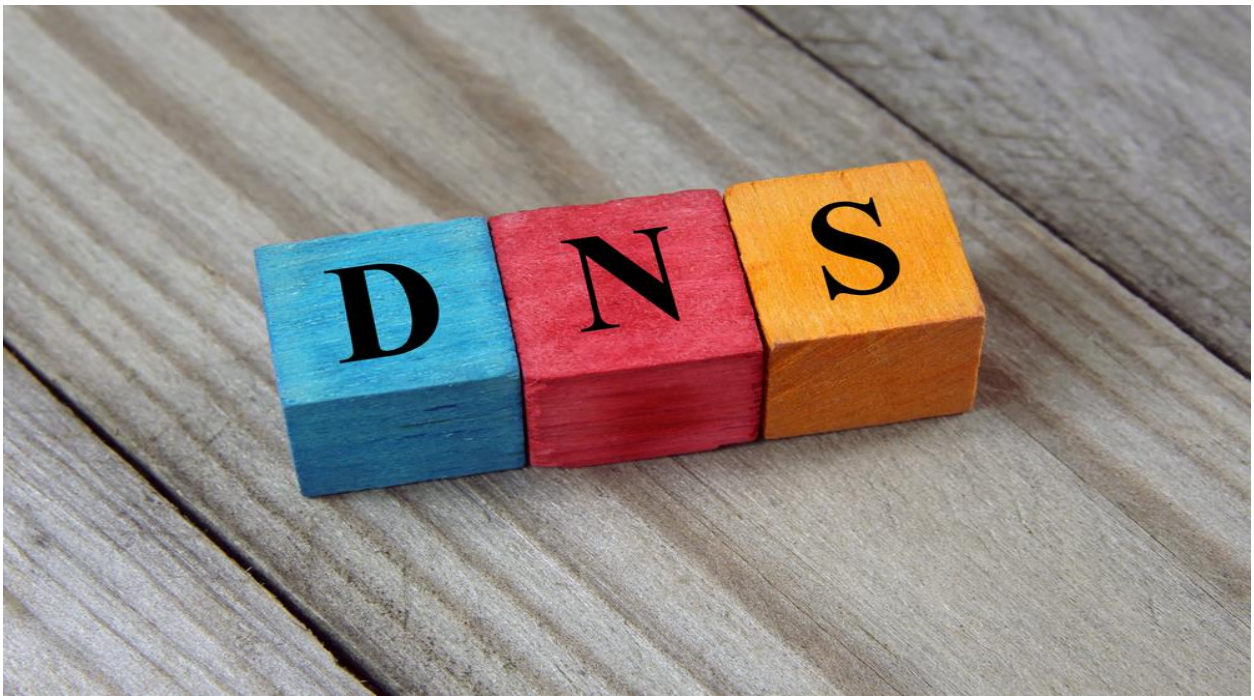
H E A D Q U A R T E R S
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

This is How Dangling Domains are Becoming a Prevalent Threat



A recent study claims that an unnoticed threat—dangling DNS records—could be easily used for domain hijacking. According to the study, there are multiple types of dangling DNS records and several techniques to exploit them.

The dangling domains

A DNS record is a pointer (for resource record name or rrname) that points to the network resource (in rdata). When the associated resource is moved or removed, the DNS record becomes dangled and the rrname is called a dangling domain.

If the released or abandoned resource could potentially be managed by any other individual instead of the actual owners of the rrname, this dangling DNS record is labeled as open to hijacking and may lead to a disaster.

When any network resource is removed, its corresponding DNS record should be removed from its DNS zone to ensure security. However, domain owners usually forget to remove, leading to dangling DNS records.

The study focused on three such records: CNAME (an alias for the canonical name rdata), MX (the mail server used for accepting emails on behalf of the domain), and NS (an authoritative name server).

Statistically speaking

Using a dangling domain detector, around 317,000 unsafe dangling domains have been spotted. Further analysis reveals that out of these dangling domains, around 63.1% were expired rdata, 36.9% were from GitHub, while around 0.1% were from WordPress.

The distribution of DNS record types disclosed that most of these records were CNAME (99.4%), while a small percentage were NS (0.6%). No dangling was detected in the MX records.

According to the study, several thousand dangling domains are being queried every single day. Two spikes were spotted on 6 and 12 September, caused by a single domain linked to 11,000 unique dangling subdomains.

Researchers had aggregated all 317,000 dangling domains by TLDs and then presented the top 60 TLDs. The top TLD is com, which accounted for around 55.2% of all dangling domains.

The TLDs gov/edu are believed to be well-managed DNS zones, although they still account for 197 and 13 dangling domains.

Additionally, researchers checked if the dangling domains are subdomains of Tranco's top 1 million domains. They found that 12% of domains are under the top 1 million domains, where 4,767 fell in the top 2000 ranks.

Conclusion

A forgotten set of dangling DNS records could be a recipe for disaster for any organization. Therefore, organizations are suggested to use appropriate DNS security measures and advanced URL filtering. Moreover, organizations should conduct security audits and self-reconnaissance of their IT assets on a regular interval to keep a check on any loose ends.

References:

https://cyware.com/news/this-is-how-dangling-domains-are-becoming-a-prevalent-threat-f34186de
https://unit42.paloaltonetworks.com/dangling-domains/
https://www.haktechs.com/latest-vulnerability/this-is-how-dangling-domains-are-becoming-a-prevalent-threat/
https://unit42.paloaltonetworks.com/dns-rebinding/
https://unit42.paloaltonetworks.com/proactive-detector/