Challenges in Inferring Domain Hijacks at Scale (Abstract)

Gautam Akiwate
gakiwate@cs.ucsd.edu
UC San Diego

The correct and efficient working of DNS relies upon vital configuration data. Thus, control over DNS configuration of a domain affords complete control over the domain. Typically, attackers leverage previously compromised user credentials to gain privilege to modify DNS configurations for a domain at the registrar. The attackers can then update A, MX, or NS records to direct traffic towards their own infrastructure. This hijacked traffic could then be forwarded to the legitimate services to avoid detection [2, 3, 4]. Furthermore, DNS is increasingly used for other purposes like automatically issuing SSL certificates [1]. Attackers can thus not only hijack the domain name to inject malicious resolutions, but also obtain SSL certificates which can allow masquerading of legitimate websites with no browser warnings. Recognizing these risks, in January 2019 DHS issued an emergency directive that urged IT administrators of government domains to audit their DNS configurations [3].

Given the potential for abuse, identifying instances of domain hijacking, both historically and operationally, is important. We are investigating using a robust set of features to identify instances of domain hijacking. But accurate identification of domain hijacking, and thus features that can identify it, requires correlation across multiple disparate data sources, including passive and active DNS measurements, BGP routing data, Certificate Transparency (CT) logs, blacklists, and WHOIS data. Enabling integrated analytics on such data sets requires significant investment to establish and maintain. This barrier demonstrates the need for sustained open data sets to effectively identify security threats, vulnerabilities, and harmful behavior.

At the DINR workshop we will present our strategy for identifying domain hijacking and the data sets that we are using. We also hope that discussion at the workshop can help us identify additional techniques for detecting hijacks, and sources for collecting and sharing relevant data.

References

[1] R. Barnes, J. Hoffman-Andrews, D. McCarney, and J. Kasten. Automatic certificate management environment (acme). RFC 8555, Mar 2019.

[2] Talos Intelligence. Dnspionage campaign targets middle east, Nov 2018.

[3] Department of Homeland Security. Emergency directive 19-01: Mitigate dns infrastructure tampering, Jan 2019.

[4] Fire Eye Research. Global dns hijacking campaign: Dns record manipulation at scale, Jan 2019.