TLP:WHITE

NCCIC

DNS Infrastructure Hijacking Campaign

Original release date: January 10, 2019 | Last revised: January 11, 2019

The National Cybersecurity and Communications Integration Center (NCCIC), part of the Cybersecurity and Infrastructure Security Agency (CISA), is aware of a global Domain Name System (DNS) infrastructure hijacking campaign. Using compromised credentials, an attacker can modify the location to which an organization's domain name resources resolve. This enables the attacker to redirect user traffic to attacker-controlled infrastructure and obtain valid encryption certificates for an organization's domain names, enabling man-in-the-middle attacks.

NCCIC encourages administrators to review the FireEye and Cisco Talos Intelligence blogs on global DNS infrastructure hijacking for more information. Additionally, NCCIC recommends the following best practices to help safeguard networks against this threat:

- Implement multifactor authentication on domain registrar accounts, or on other systems used to modify DNS records.
- Verify that DNS infrastructure (second-level domains, sub-domains, and related resource records) points to the correct Internet Protocol addresses or hostnames.
- Search for encryption certificates related to domains and revoke any fraudulently requested certificates.

TLP:WHITE