DNS Infrastructure Hijacking Campaign | CISA

Published: 2019-02-13 · Archived: 2026-04-05 12:50:41 UTC

Summary

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.

See the following links for downloadable copies of open-source indicators of compromise (IOCs) from the sources listed in the References section below:

- IOCs (.csv)
- IOCs (.stix)

Note: these files were last updated February 13, 2019, to remove the following three non-malicious IP addresses:

- 107.161.23.204
- 192.161.187.200
- 209.141.38.71

Technical Details

Using the following techniques, attackers have redirected and intercepted web and mail traffic, and could do so for other networked services.

1. The attacker begins by compromising user credentials, or obtaining them through alternate means, of an account that can make changes to DNS records.
2. Next, the attacker alters DNS records, like Address (A), Mail Exchanger (MX), or Name Server (NS) records, replacing the legitimate address of a service with an address the attacker controls. This enables them to direct user traffic to their own infrastructure for manipulation or inspection before passing it on to the legitimate service, should they choose. This creates a risk that persists beyond the period of traffic redirection.
3. Because the attacker can set DNS record values, they can also obtain valid encryption certificates for an organization's domain names. This allows the redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.

Mitigations

NCCIC recommends the following best practices to help safeguard networks against this threat:

- Update the passwords for all accounts that can change organizations' DNS records.
- Implement multifactor authentication on domain registrar accounts, or on other systems used to modify DNS records.
- Audit public DNS records to verify they are resolving to the intended location.
- Search for encryption certificates related to domains and revoke any fraudulently requested certificates.

References

- Cisco Talos blog: DNSpionage Campaign Targets Middle East
- CERT-OPMD blog: [DNSPIONAGE] – Focus on internal actions
- Global DNS Hijacking Campaign: DNS Record Manipulation at Scale | Mandiant | Google Cloud Blog
- Crowdstrike blog: Widespread DNS Hijacking Activity Targets Multiple Sectors

Revisions

January 24, 2019: Initial version
February 6, 2019: Updated IOCs, added Crowdstrike blog
February 13, 2019: Updated IOCs
