CISA
CYBER+INFRASTRUCTURE

CISA INSIGHTS CYBER

Mitigate DNS Infrastructure Tampering

AT-A-GLANCE RECOMMENDATIONS

- Review DNS Records
- Change DNS Account Passwords
- Add Multi-Factor Authentication to DNS Accounts
- Monitor Certificate Transparency Logs

CYBERSECURITY THREAT

In late 2018, cybersecurity organizations across the globe started to detect an increase in malicious activity targeting the Domain Name System (DNS) infrastructure on which we all rely. Using common tactics, outlined below, the attackers were able to redirect and intercept web and email traffic, and could have achieved the same for other networked services.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages its State, Local, Tribal and Territorial (SLTT) government partners, as well as private sector owners of critical infrastructure, to use this guide to learn more about this threat and associated mitigation activities. This guidance is derived from Emergency Directive 19-01 – Mitigate DNS Infrastructure Tampering and includes lessons learned and additional considerations for non-federal entities seeking to implement actions in line with federal civilian departments and agencies, as directed by CISA.

ATTACK BREAKDOWN

How It Works

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. 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.**

Why It's Effective

- Frequently, different domain and DNS records are owned and managed by different parts of an organization. This means that many **organizations lack central visibility** into all domains that belong to them or associated DNS records.
- This **decentralization of the DNS ecosystem** and the organizational governance processes make it difficult to monitor and secure domains.

RECOMMENDED ACTIONS

To address the significant risks to organizational information and information systems posed by DNS tampering, CISA directed federal civilian agencies to undertake the following series of near-term actions and encourages non-federal organizations to do the same:

Action 1: Review DNS Records

- For all organization owned/managed domains:
  a. Review all public domain records with domain registrars to verify the associated NS records are delegated to intended DNS servers; and
  b. Review all DNS records on all authoritative and secondary DNS servers to verify they resolve to their intended destination.
- Any discovered discrepancies should be investigated immediately and treated as a potential security incident.

Action 2: Change DNS Account Passwords

- Immediately update passwords for all accounts on systems that can make changes to your organization's DNS records, including accounts on organization-managed DNS server software, systems that manage that software, third-party DNS operators' administration panels, and DNS registrar accounts.

Action 3: Add Multi-Factor Authentication to DNS Accounts

- Implement and enforce multi-factor authentication (MFA) for all accounts on systems that can make changes to your organization's DNS records including accounts on organization-managed DNS server software, systems that manage that software, third-party DNS operators' administration panels, and DNS registrar accounts.
- If MFA is not supported for records hosted by third party providers, CISA strongly encourages organizations to consider migrating to providers that support strong access controls and MFA.
- If MFA is not supported on legacy system hosted by organizations internally, compensating controls can be introduced to temporarily harden access controls (e.g. require physical console access, disable remote access, limit remote access to management network only, etc.).

Action 4: Monitor Certificate Transparency Logs

- Monitor Certificate Transparency (CT) log data for newly added certificates issued to organization-owned domains that have not been authorized/requested by the organization.

Scope of Recommendations

- The focus of these recommendations is on external/public/internet facing domain and DNS records. The recommendations are not concerned with internal infrastructure.
- The scope of these recommendations transcends DNS infrastructure itself and requires a comprehensive approach that includes associated services. To capture this scope, CISA

uses the term DNS ecosystem to include: root zones, top level domain registries, domain registrars, domain registrants, and authoritative DNS servers. Disparate organizational units may be responsible for managing these services and successful outcomes depend on their close coordination.

LESSONS LEARNED AND ADDITIONAL CONSIDERATIONS

Lessons Learned

- Many organizations lack a DNS-specific policy to guide DNS-related activities at the operational level that specify security protocols and activities related to the protection of the DNS ecosystem. Even basic steps that can be taken to maintain awareness of DNS infrastructure, such as the documentation of a domain inventory, are not consistently or effectively acted upon across organizations.
- Organizations need better top-level control of the acquisition, management, and reporting of domains (e.g. preventing anyone with a corporate purchase card from registering a domain). To successfully protect their infrastructure from DNS tampering, it is critical that organizations have accurate and up-to-date inventories of all domain names that are owned or operated on their behalf.
- Without a clear understanding of an organization's environment, it is not only difficult to identify anomalies, risks, and misconfigurations but it is impossible to defend against what one does not know.

Implementation Considerations

- Performing historical analysis of past record changes (passive DNS) may be prudent, but it will not stop current hijacking from occurring, it may only indicate whether a hijack has occurred in the past.
- Certificate Transparency logs record all SSL certificates issued by publicly trusted certificate authorities. While those certificates are not directly issued for DNS services, logs can alert you that an unauthorized certificate was issued for a domain you manage. To take full advantage of CT log monitoring, organizations must **1) have a comprehensive inventory of domains they manage**, and **2) the ability to confirm that a certificate request was actually *authorized by your organization.***
- In large organizations with multiple operating divisions, the process of obtaining a certificate may not be centrally managed, and a single entity may not be aware that a given certificate was requested.
- To monitor CT logs, organizations may use various free or commercial CT monitoring services.

Resource Considerations

- From a federal perspective, gaining central visibility into all domains owned by an organization proved to be the most labor intensive and challenging process. Organizations with a strong grasp on all domain related records and/or central visibility had to invest significantly less effort to meet the same requirements. A coordinated effort by all organizational units throughout the enterprise is essential for a successful outcome.
- Organizations with a large number of domain names and domain name records may want to prioritize domain names and records associated with key services offered to organizational users (for example, websites that are central to the organization's mission, MX records, or other services with high utilization).

HELPFUL LINKS AND REFERENCE MATERIALS

CISA Emergency Directive 19-01 – Mitigate DNS Infrastructure Tampering and FAQ:
https://cyber.dhs.gov/ed/19-01/

CISA Current Activity: DNS Infrastructure Hijacking Campaign:
https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

Sources of Certificate Transparency (CT) logs (and passive DNS records):
https://www.entrust.com/ct-search
https://crt.sh
https://sslmate.com/certspotter
https://transparencyreport.google.com/https/certificates?hl=en

Auditing DNS records and Certificate Transparency (CT) logs using Splunk:
https://www.splunk.com/blog/2019/01/25/cisa-emergency-directive-19-01-doing-things-the-easy-way-in-splunk.html.

For guidance on MFA, organizations should consult National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management:
https://csrc.nist.gov/publications/detail/sp/800-63b/final

When utilizing MFA, organizations should consider using additional factors that are resilient to phishing. Consistent with NIST SP 800-63B, Short Message Service (SMS)-based MFA is not recommended.