Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

AUGUST 2022

Domain Name Service (DNS) Tampering

ITSAP.40.021

DNS queries are required for almost everything you do with network applications and online activity. Threat actors frequently target DNS services in order to direct legitimate web traffic to malicious domains, which enables them to compromise not only your systems, but those of your customers as well. Threat actors can use a variety of attacks against your DNS systems that tamper with DNS settings and caches on your infrastructure, or your organization's DNS registry entries. The guidance and mitigation measures provided in this publication are presented two-fold: by addressing DNS tampering attacks on hosting servers (e.g. registry compromise) and tampering attacks on DNS resolution (e.g. poisoning, hijacking, and pharming).

What is DNS?

DNS is a protocol that translates user-friendly web addresses, such as “cyber.gc.ca”, into machine-readable internet protocol (IP) addresses, such as 20.151.96.73. It is often referred to as the address book for the Internet. DNS is used for both human-initiated actions (e.g. visiting a website) and machine-initiated actions (e.g. running an update). This translation process is called DNS resolution. A DNS resolver searches for requested domains until it finds an authoritative name server that provides the IP address for the domain.

What is DNS Tampering?

DNS tampering attacks are focused on redirecting users to malicious content. Threat actors do this by either compromising user credentials associated with accessing or maintaining your internal DNS infrastructure or by injecting erroneous DNS entries through vulnerabilities in the DNS protocol. Compromised credentials allow threat actors to access your DNS and make changes to your DNS nameserver.

DNS Nameserver Compromise

Threat actors can compromise administrative DNS credentials for a domain and change the legitimate DNS records. They are able to redirect user traffic to their own infrastructure or obtain domain validated certificates containing a rogue key. Threat actors may then serve malicious websites or launch a person-in-the-middle attack to decrypt transport layer security (TLS) connections to that domain. It is important your organization implements the following mitigation measures to protect against a compromise of your DNS nameserver records:

- Implement multi-factor authentication (MFA) if available for nameserver accounts.
- Audit user accounts that have access to the DNS registrar and nameserver.
- Monitor certificate transparency (CT) logs related to your domain certificates to assess any new certificates added.
- Implement “client lock/change lock/registry lock” programs offered by your domain name registrar to add additional controls/ protections on changes to your DNS entries.

DNS Security (DNSSEC)

DNSSEC is a method of improving data integrity and authentication security.

DNSSEC secures data exchanged in DNS and helps protect sensitive information stored in your DNS records. It provides cryptographic authentication of DNS data. It also provides authenticated denial of existence by allowing a DNSSEC-enabled resolver to confirm that a particular domain exists. DNSSEC also improves data integrity.

DNSSEC enhances the security of DNS servers and is an effective mitigation measure to protect your organization from DNS tampering attacks, specifically DNS spoofing and hijacking. It eliminates a vector for threat actors to exploit other potential vulnerabilities in your DNS infrastructure.

Cat. No. D97-1/40-021-2022E-PDF
ISBN 978-0-660-44753-7

Canada

Mitigation Measures for Common Tampering Attacks on DNS Resolution

DNS tampering can be done through various attack methods targeting DNS resolution. The following attack methods are prevalent and the associated mitigation measures should be implemented to better protect your DNS resolution.

DNS Spoofing (Cache Poisoning)

Threat actors can gain access and insert domain name associations to malicious IP addresses. They can "poison" your DNS cache with a malicious domain, which could lead to the cache maintaining the incorrect association for future DNS server queries from your end users.

- Implement DNSSEC to validate DNS resolutions.
- Disable local hosts files.
- Use a virtual private network (VPN).
- Flush your DNS cache periodically.
- Use DNS over TLS (DoT) to encrypt DNS queries to external DNS resolvers.
- Disable use of DNS over HTTPS (DoH) in the web browser configuration.

DNS Hijacking

Threat actors can redirect users to malicious recursive DNS servers which then redirects them to malicious sites. Typically this is done by compromising an endpoint or networking device to change their networking configurations.

- Implement MFA on accounts and systems used to modify your DNS registry.
- Run anti-virus and anti-malware software on endpoints and servers.
- Implement firewall rules that limit DNS queries to access only DNS resolvers you trust.
- Adopt robust change control protocols for performing changes to internal DNS resolvers.

Pharming

Threat actors can compromise a router and manipulate the DNS cache, or modify the DNS settings to point to alternative DNS resolvers.

- Change the default name and password of your routers to use strong passphrases or passwords, and implement MFA if available.
- Check the DNS configuration settings of your router regularly to spot possible changes to DNS configurations.
- Apply firmware patches to your router to ensure all security fixes have been addressed.

DNS Security Actions

The following security actions are recommended to better protect your organization against DNS attacks, including DNS tampering:

- Block domain names or IPs that could be malicious or pose a threat to your organization.
- Set up rules around DNS queries that are suspicious.
- Implement restrictions on your networks for the length, type, or size of outbound or inbound DNS queries.
- Harden your operating systems by patching and updating regularly. (e.g. patch and update).
- Understand name resolution capabilities and determine their search order.
- Conduct continuous system monitoring and user behaviour analytics to automatically detect anomalies.
- Install protective DNS to protect your users from visiting potentially malicious domains.

Learn More

- *Protective Domain Name System (DNS) (ITSAP.40.019)*
- *Protecting Your Organization Against Denial of Service Attacks (ITSAP.80.100)*
- *Secure Your Accounts and Devices With Multi-Factor Authentication (ITSAP.30.030)*
- *Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101)*
- *Top 10 IT Security Actions to Protect Internet Connected Networks and Information (ITSM.10.089)*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**