National Cyber Security Centre
a part of GCHQ

Advisory: Ongoing DNS hijacking and advice on how to mitigate

12 July 2019

© Crown Copyright 2019

Introduction

In January 2019 the NCSC published an alert to highlight a large-scale global campaign to hijack Domain Name Systems (DNS).[1] DNS hijacking refers to the unauthorised alteration of DNS entries in a zone file on an authoritative DNS server, or the modification of domain configurations in relation to a domain registrar, by an attacker. These modifications can be used to achieve objectives such as redirecting traffic to capture sensitive information.

The previous alert described the two principal techniques that attackers use and provided Indicators of Compromise relevant to that campaign, as well as mitigation advice.

Details

The Domain Name System was designed as a hierarchical, delegated infrastructure. When a DNS resolver needs to establish a DNS record, it makes a series of queries through the chain of delegation. This "distributed database" design was primarily chosen for resilience and stability, but also to allow delegation subdomains to other entities. For example, delegation means that country code top level domains (ccTLDs) such as .uk or .fr can be delegated to the relevant nation.[2] A full list of terms and explanations can be found in the appendix.

The NCSC has observed various attacks which exploit the DNS system at different levels. Since the NCSC's alert in January further activity has been observed, with victims of DNS hijacking identified across multiple regions and sectors.[3]

Risks

Attackers may have a variety of motivations and objectives, ranging from taking down or defacing a website, to intercepting data. Some of the risks around DNS hijacking include:

Creating malicious DNS records - for example, to create a phishing website that is present within an organisation's familiar domain. This may be used to phish employees or customers.

Obtaining SSL certificates - domain-validated SSL certificates are issued based on the creation of DNS records; thus an attacker may obtain valid SSL certificates for a domain name, which could be used to create a phishing website intended to look like an authentic website, for example.

Transparent Proxying - one serious risk employed recently involves transparently proxying traffic to intercept data. The attacker modifies an organisation's configured

[1] https://www.ncsc.gov.uk/news/alert-dns-hijacking-activity

[2] For more information about DNS see https://www.cloudflare.com/learning/dns/what-is-dns/

[3] See https://blog.talosintelligence.com/2019/04/seaturtle.html

domain zone entries (such as “A” or “CNAME” records) to point traffic to their own IP address which is infrastructure they manage.

For example, users at an organisation may log in to webmail.company.com. The attackers will compromise the DNS for that record for that service, redirecting webmail.company.com to the attacker’s server. This server will often serve a legitimate domain validated SSL certificate (obtained because of the attacker’s control of the DNS). The server transparently proxies the users to the real webmail service, while intercepting credentials and sensitive data.[4]

Domain Hijack - an organisation may lose total control of their domain and often the attackers will change the domain ownership details making it harder to recover.

Protecting your organisation

Registrar Security

The most common DNS hijacking takes place at the registrar level, simply by gaining unauthorised access to a registrant’s account. ICANN have published an extensive best practices guide.[5]

Registrar accounts are compromised using familiar Account Take Over (ATO) techniques, including:

- Phishing;
- Credential stuffing;
- Social engineering.

To mitigate against these risks, follow NCSC’s phishing guidance and observe NCSC’s suggested password best practice, being sure to deploy Multi-Factor Authentication (MFA) when available

Additionally:

Account Access - regularly audit who can access the registrar control panel and make changes with the registrar.

Contact Information - domain registrations typically have four points of contact: the registrant, technical, administrative, and billing contacts. Ensure that all contact information is up to date - contact updates are often overlooked when organisations grow, shrink, move, or are acquired. A registrar may send certain types of communication to only one of those roles, and in some disputes, the registrant contact usually takes precedence.

Role account – it is not advisable to use individuals’ email addresses for any of the domain contacts, as this gives effective control to an individual who may leave or be absent. It is more effective to create role accounts e.g. hostmaster@ to receive these

[4] https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

[5] https://www.icann.org/en/system/files/files/sac-044-en.pdf

important messages and ensure these get distributed to all relevant parties. Ensure the members of the group are wary of phishing attacks. Ensure these email accounts are kept secure.

Registry and Registrar Lock – many registries offer a "registrar lock" service. This lock prevents the domain being transferred to a new owner, without the lock being removed. A "registry lock" (which sometimes involves a fee) is considered an additional level of protection whereby changes cannot be made until additional authentication has taken place which usually involves a call to the owner.

For example, Nominet, the .uk registry, offers a service called "Domain Lock" which:

- Prevents the nameservers from being changed;
- Prevents domain registrant and / or contact details being changed;
- Prevents the domain from being transferred to another registrar.

Domain Management Monitoring - if you operate a critical domain, consider monitoring for domain transfers, WHOIS data changes, and nameserver changes. Explore monitoring services which may be offered by your registrar or hosted DNS provider. Consider monitoring for changes to records related to critical services e.g. MX (mail delivery) records.

Keep evidence - in case your entire domain is hijacked, you'll need to appeal to your registry for help. Keep extensive records which can be used to prove ownership.

Nameserver Security

Change Control – if operating your own DNS infrastructure, consider robust change control processes to manage any changes to your zone file. Ideally you should use a DNS zone file that is managed through a version control system, such as git. This will provide a backup of your DNS records, allow change-auditing and easy rollback. Enforce levels of organisational approval which is monitored before changes are made.

Access Control – employ strict access controls to infrastructure hosting DNS zone files or providing DNS services for your domain.

Monitoring and auditing – monitor and periodically audit entries configured in your zone files to ensure what is present is expected. Monitor and record access to critical infrastructure hosting DNS services.

SSL Monitoring – use open source tools like crt.sh to monitor for the creation of SSL certificates created that match your organisations domain name(s).

DNSSEC – consider configuring DNSSEC on your zone so queries are cryptographically signed. This provides a level of origin integrity for a client given a response to a query from your DNS server would be cryptographically signed with a private key and can be verified by a client with your public key. It is important that controls are put in place to secure your private key.

Web Application Security

Web Services Access Log Monitoring – in the case of an attacker using a transparent proxy technique as described to steal credentials or other data, internet traffic would come via the proxy the attacker manages. Typically, this traffic will be forwarded to an organisation's web facing application from the proxy and thus would likely originate from a single or small pool of IP addresses. Monitoring access or authentication logs for an internet facing web application for traffic coming from a single or small pool of internet facing IP address(es) en mass could be an indicator of this technique in use.

Appendix: key terms

Root nameservers – these are operated by ICANN (a non-profit organisation involved with managing the overall operations of the internet). The root nameservers list all the top-level domains (e.g. .com, .uk, .net) and delegate those to a registry.[6]

Registry – registries are responsible for maintaining the database of all domain names and registrant information for the top-level domains that they operate. For example, In the UK, Nominet is the registry responsible for .uk domains and some sub-delegations like .co.uk. Their database lists all domains, such as bbc.co.uk, as well as the authoritative nameservers these are delegated to. Usually registries do not sell domain registrations directly, they instead rely on registrars to do so.

Registrars - registrars are companies which sell domains to *Registrants* and manage the ownership of domain names**.** They act as a sort of intermediary to a *Registry*. Registrars could be thought of as the 'shop fronts' for domain names, providing the sales channel to the end domain owner.

Registrants – an individual or organisation that owns and operates a domain. Registrants own domains and ultimately have control over the DNS, including deciding what authoritative nameservers to use.

Authoritative Nameservers – these servers are the last stop in a DNS query, and store the final source of trust for a DNS record. For example, it will provide the mapping between a full domain (e.g. www.bbc.co.uk) and the relevant IP address.

Registrars often offer additional services such as providing an authoritative nameserver service for the domains which are purchased/managed through them. Most customers will manage DNS record changes for their domains through the Registrar. However, many organisations may select an unrelated supplier to operate the authoritative nameservers, or may operate authoritative nameservers themselves.

[6] For more details see https://whois.icann.org/en/dns-and-whois-how-it-works