Threat of the Month: DNS Under Attack

What is DNS and DNS redirection?

The Domain Name System (DNS) is the core technology that directs users to different web sites and other locations on the internet. Think of it like asking a librarian for help locating a book. Only instead of asking about a book, you ask for a particular web site. DNS checks its records, and then tells your computer where the web site is located.

In the case of DNS redirection, an attacker manages to compromise the DNS process, altering the route to a legitimate website to lead to a malicious one, ultimately compromising the target. You ask for the IP address of a particular domain you want to visit, but the DNS records have been changed so that you are sent to a malicious IP address instead.

Attacking DNS

There are points where an attacker can compromise DNS records and change them:

- The DNS administrator may be phished.
- The DNS hosting may be compromised.
- The infrastructure along the DNS request chain could be compromised.

Further reading

- DNS Under Attack
- DNSpionage Campaign Targets Middle East
- DNSpionage brings out the Karkoff
- DNS Hijacking Abuses Trust In Core Internet Service
- Sea Turtle keeps on swimming, finds new victims, DNS hijacking techniques
- Covert Channels and Poor Decisions: The Tale of DNSMessenger
- Spoofed SEC Emails Distribute Evolved DNSMessenger
- Detecting DNS Data Exfiltration

07/19

DNSpionage

The attack began with a LinkedIn phishing message to a DNS administrator. The administrator clicked a malicious link in the message, which led to a malicious word document.

The administrator's machine was compromised as a result, allowing the attackers to steal DNS login information.

Having gained the ability to control the domain, the attackers subsequently redirected a webmail server to a malicious IP address, and registered valid certificates to "legitimize" the redirected domain. The malicious page impersonated the webmail interface and the atackers preceeded to steal login information.

Sea Turtle

While having a similar end-goal as DNSpionage—stealing information—the attackers behind Sea Turtle went after the network infrastructure where the TLD servers were hosted. Once the TLD servers where compromised, they modified the IP addresses of the name servers for particular domains.

This approach gave the attackers more control over the redirection. Setting up a malicious name server, the attacker can choose when requests for a particular domain is sent to the legitimate site or a malicious site.

Sea Turtle also changed records of webmail servers, where they can intercept and steal the information that they were after, and then send the target on to the legitimate system when done.

Umbrella Investigate	Duo Trusted Access
▪ Umbrella Investigate allows you to review DNS records to look for changes, legitimate or otherwise.	▪ Duo's multi-factor authentication can prevent arbitrary changes to DNS records without authentication.