DEFENDING YOUR DNS INFRASTRUCTURE

NEW ATTACKS ON A VITAL RESOURCE

The Domain Name System (DNS) is a critical component of the Internet infrastructure. It is the means by which domain names (e.g. www.nsa.gov) are translated into Internet Protocol (IP) addresses (e.g. 23.214.23.29). In recent years, there have been a number of high profile, high impact attacks against DNS. In January, 2019, a wave of DNS hijacking attacks resulted in an emergency directive from the Department of Homeland Security (DHS) and multiple reports from cybersecurity experts, outlining how to secure DNS [1], [2].

HOW DOES DNS WORK?

When an end user types a domain name into a web browser, DNS uses countless DNS servers organized in a hierarchical fashion to convert these requests—called DNS queries—from names into IP addresses, which specify the server an end user will reach and which will, in turn, deliver the desired web content to the end user. In this way, the distributed DNS servers function like helpful neighbors, directing visitors to the correct addresses for whomever they want to visit.

Recursive DNS servers act as a middle man and get the DNS information on the user's behalf. If the recursive server has the DNS reference cached, then it will answer the DNS query. If not, it passes the query to the authoritative server to find the information. An Authoritative DNS server has the ultimate authority over a domain and is responsible for providing answers (i.e. IP address information) when the Recursive DNS servers forward a DNS query. Authoritative servers are usually managed by web-hosting companies. Both of these services work together to route an end user to the desired website or application. Figure 1 shows how these services work together to retrieve DNS information.

The top of the DNS hierarchy contains a root server. The servers immediately below the root server are called top-level domain name servers, and they include .com, .gov, .net, etc. The level below this is the name servers for domains like example.com. Each domain can then have their own lower level authoritative DNS servers. Each domain's DNS servers can resolve queries for hostnames of resources in that domain.

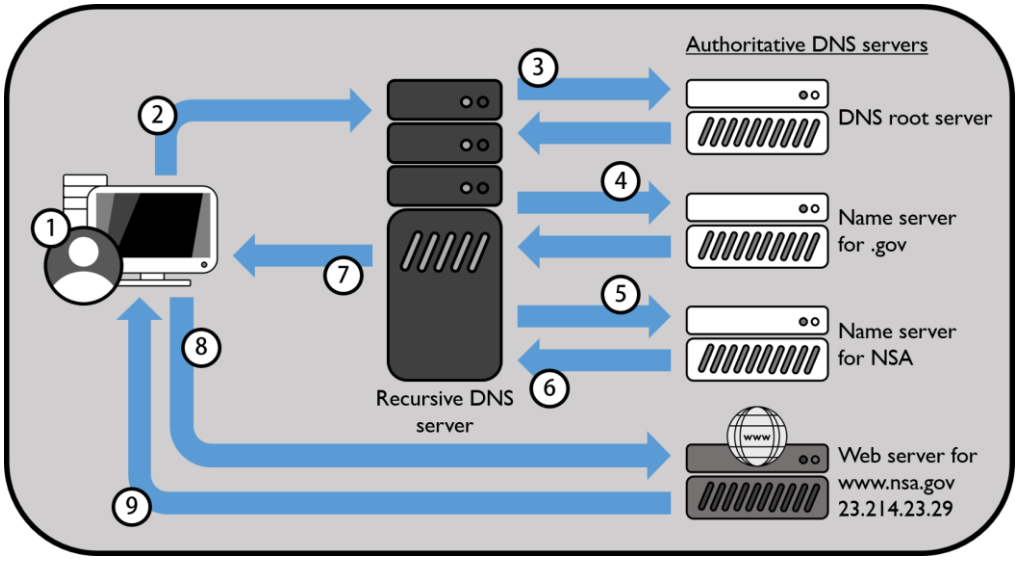

Figure 1: How DNS works

In the example depicted in Figure 1, a user wants to visit nsa.gov and types www.nsa.gov into the web browser. The request for www.nsa.gov is then routed to the recursive DNS server. The recursive server sends a request for www.nsa.gov to a DNS root server and receives a response: go to the name server for .gov. With that direction, the recursive server forwards the request to one of the

top level domain name servers for the .gov domain and receives another response: go to the name server for nsa. The recursive server forwards the request a final time, this time to the nsa name server. The name server then looks in the nsa.gov hosted zone for the www.nsa.gov records, gets the associated values—such as the IP address for web server 23.214.23.29—and returns the IP address to the recursive server. The recursive server returns the newly acquired IP address to the web browser, and caches the IP address for nsa.gov for future queries. The user's web browser then sends the request for www.nsa.gov to the IP address that it received from the recursive server. Finally, the web server at 23.214.23.29 returns the requested webpage for www.nsa.gov to the web browser and the browser displays the page.

When a recursive DNS server is queried, it will first check its cached memory to see if the IP address for the requested domain was previously stored. If found, the recursive DNS server will immediately deliver the IP address back to the browser and the user is taken to the website. If the recursive DNS server does not have the IP address, it will reach out to the authoritative DNS server as described above, which will deliver the recursive server with information for the website. Enterprises can deploy DNS servers to contain hostname-to-IP address mappings for the resources in their domains, and utilize the DNS hierarchy to resolve queries for resources outside of their domains.

COMMON DNS ATTACKS

Some DNS attacks are aimed at taking down authoritative DNS servers to deny access to a domain. Other attacks attempt to either manipulate DNS to redirect traffic to malicious destinations or allow attackers to take control of the DNS infrastructure itself, with disastrous consequences to the server's domain and third parties.

Denial of Service Attacks

Attacks that aim to make DNS unavailable to clients on the internet, resulting in legitimate DNS queries going unanswered, are known as denial-of-service (DoS) attacks. These attacks halt the client's ability to reach their desired domains. Two common DoS attacks to DNS are NXDomain (also known as Phantom Domain) attacks and Flood attacks.

In an **NXDomain (Phantom Domain) attack**, the attacker sends a flurry of queries to the DNS server to resolve non-existent domains. When the DNS server cannot find the answers to the queries and answer back with an NXDOMAIN result, the recursive DNS server's cache data fills up with NXDOMAIN results, slowing down the response time for legitimate users.

DNS Protocol Attacks typically involve using malformed packets that cause an extra load in processing on the DNS server to the point where the server can no longer process legitimate queries.

Dropping any abnormal DNS queries and responses, or queries for which the DNS client is retransmitting a high volume of requests is one way to combat these attacks. Enforcing Time-to-Live (TTL), disallowing unsolicited DNS responses, or using DNS TCP transmission to force DNS clients to prove their legitimacy add additional protections.

Attacks on DNS Integrity

Attacks that result in the deliberate or inadvertent alteration of data are threats to DNS integrity. Some parts of data within DNS can lead to severe consequences, if altered (e.g. resource records that are stored in zone files, memory, etc.).

During ***Cache Poisoning, also known as DNS Poisoning***, an attacker causes the cache of a recursive DNS server to map a legitimate hostname to a malicious IP address. When a user attempts to access the resource associated with the legitimate hostname the recursive DNS server receives the query and resolves the hostname to the malicious IP address, causing the user to be redirected to the attacker's website. Because this resolution is stored in the DNS cache, the redirection can occur throughout the duration of the caching period.

Properly configuring DNS caching servers can help prevent DNS integrity attacks. Specifically, an enterprise should configure them to resolve only DNS queries for authorized networks, or to only cache resolutions from trusted DNS servers higher in the hierarchy, like the root and .com servers. Educating employees to verify website legitimacy and installing security controls on employee workstations to detect attempted DNS reconfiguration also help.

Attacks that Leverage DNS

Not all attacks are aimed at hampering the proper behavior of DNS; some attacks—like Reflection and Amplification attacks—leverage DNS to impact third party victims and systems, although the DNS server will still be impacted as a side-effect.

A **Reflection attack** employs an unwitting intermediary machine in order to affect the actual target system. A DNS **Amplification attack** is a form of reflection attack that takes advantage of an insecure DNS server to launch a flood attack on a third party victim. The attacker generates spoofed DNS requests using the IP address of the target. The DNS server then sends the response message to the target. The attacker can then flood the recursive DNS server with spoofed requests. Because the response messages are larger than the requests, this form of attack amplifies the attacker's ability to flood the victim. The victim of the attack will think that the attack is originating from the DNS Server, even though the DNS server only acts as a relay. From the DNS server perspective, the attack seems to come from the victim itself since the requests appear to originate from the victim's IP address. Administrators may not even notice that there are abnormal incoming requests to the DNS server.

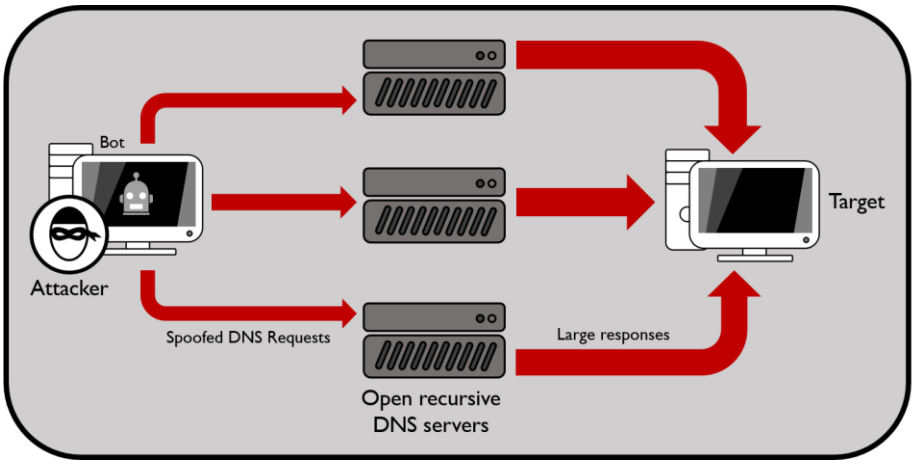

Figure 2: Amplification attack

DNS Tunneling Attacks are used to steal data from a network. The attacker infects a target system with malware, which opens a tunnel to the attacker's machine through the recursive DNS server using DNS traffic. This server is normally located within the target's network and bypasses the client's network firewall. Once the attack is successful, HTTPS traffic can be exchanged through the tunnel, disguised as DNS query responses, thereby evading the firewall while maintaining the secrecy of the exfiltrated data from any security device on the client's network. Even though DNS tunneling is not considered an attack on DNS itself, it is an attack that leverages DNS to exfiltrate data.

Attacks on DNS Management

During ***Domain Hijacking*** an attacker takes control of an enterprise's domain. Domain hijacking could occur when the enterprise's third-party DNS provider has internal security issues that are beyond the control of the enterprise, or when an attacker compromises the credentials to the organization's DNS administration account. Domain hijacking allows the attacker to imitate an administrator and make changes that affect the entire domain. When deciding to use a third-party DNS provider to register their domains, enterprises must select reputable DNS providers with rigorous security in place. Enterprises must also protect access to DNS administration accounts and credentials used to access those accounts.

DNSSEC

The original DNS specifications did not provide authentication or integrity controls. Without authentication and integrity controls, corrupting the address resolution process is easy. DNS Security Extensions (DNSSec) was developed to aid in thwarting this type of attack. DNSSec allows a DNS server to use cryptographic keys and signatures to authenticate other DNS servers before accepting their query replies. A DNS server configured with DNSSec permits the server to generate its key and signature. The root DNS server uses its key to sign a lower level DNS server, and that lower level DNS server uses its key to sign the next lower level DNS server. This forms a trust chain, where each DNS server can assess the signature in a query response to verify that the replying DNS server is who they claim to be. Since this trust chain occurs throughout the DNS hierarchy, enterprises must properly configure DNSSec on DNS servers at each domain level to utilize the hierarchical trust chain, authenticate DNS query responses, and prevent attacks like DNS poisoning.

ISSUES WITH SECURING DNS

Securing the DNS infrastructure can be an overwhelming task. Some vulnerabilities are beyond a network administrator's ability to mitigate, such as when an enterprise lacks control over the third-party DNS provider through which they register their domains and create name records. The mitigations covered in the previous sections of this paper are useless if adversaries access the DNS provider's account. Compromised DNS provider accounts enable mapping of malicious IP addresses to legitimate DNS names. This can allow attackers to stand up websites identical to the original ones, fooling users and harvesting their passwords. It can also allow attackers to acquire valid TLS certificates to make these masquerades more realistic. To mitigate the risk of adversarial modification of DNS provider records, enterprises must establish DNS security requirements prior to selecting a DNS provider, and insist on contractual language to clearly state the responsibilities and security requirements the DNS provider must meet. Specifically, enterprises should ensure that DNS providers offer access control lists (ACL) and out-of-band notifications. The ACLs can be configured to allow access to the DNS provider account only to specified IP addresses, while the notifications can alert authorized enterprise administrators of high risk changes to the DNS account.

Third-party recursive DNS providers can act as a first line of defense against attacks such as phishing, drive-by downloads, botnet command and control, and any others that leverage DNS domains. Generally, ISPs do not filter DNS requests to block domains that support malware, gambling, pornography, and other forms of potentially unwanted content, since such decisions vary by customer. Third-party DNS recursive services are intended to allow such filtering based on organizational policies and threat reputation services (TRS). In addition, DNSSec may not yet be implemented on an ISP's recursive DNS server to ensure that DNS requests are securely signed and accurate, whereas third-party recursive DNS providers (e.g. Umbrella, Quad9, and OpenDNS) may offer this feature. Many third-party recursive DNS providers will perform a more in-depth analysis of a DNS packet if it is deemed suspicious.

CONCLUSION

DNS plays an important role in Internet infrastructure. If enterprises don't conduct regular DNS audits and properly configure their DNS servers, attackers will see this as a real opportunity to perform malicious attacks against their network. It is crucial to keep DNS servers well maintained and remain vigilant in identifying any abnormal DNS traffic. For a comprehensive breakdown of standards and guidelines for securing DNS, please refer to NIST Special Publication 800-81-2, "Secure Domain Name System (DNS) Deployment Guide [3].

REFERENCES

[1] "Mitigate DNS Infrastructure Tampering." Department of Homeland Security, 2019 January 22. [Online] Available: https://cyber.dhs.gov/ed/19-01/#fn:1

[2] M. Hirani, S. Jones, and B. Read, "Global DNS Hijacking Campaign: DNS Record Manipulation at Scale." FireEye, 2019 January 9. [Online] Available: https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

[3] Chandramouli, R., & Rose, S. "SP 800-81-2 Secure Domain System (DNS) Deployment Guide," (pp. 1 – 130). U.S. Department of Commerce, National institute of Standards and Technology, 2013. http://dx.doi.org/10.6028/NIST.SP.800-81-2

[4] "Types of DNS Attacks and Tactics for Security." Geeks for Geeks, 2018 August 14. [Online] Available: http://www.geeksforgeeks.org/types-of-dns-attacks-and-tactics-for-security/

[5] Liska, A., & Stowe, G. (2016). DNS Security: Defending the domain name system. Cambridge, MA: Syngress.

[6] "The Most Popular Types of DNS Attacks." Security Trails, 2018 November 22. [Online] Available: https://securitytrails.com/blog/most-popular-types-dns-attacks

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

CONTACT INFORMATION

Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov