DNS-Based Attacks and How DNS Record Lookup Tools Can Prevent Them

Posted on December 9, 2019

The Domain Name System (DNS) is a fundamental cog in a company's network. It needs to function seamlessly for an entire network to run like a well-oiled machine; otherwise, it can bring your online portals to a screeching halt.

The problem is that not all organizations are aware how much of their digital ecosystem relies on a properly configured DNS environment. Most, especially small businesses, are guilty of not monitoring their DNS settings, paving the way for enterprising hackers to exploit undetected vulnerabilities. The DNS attacks featured in this post show the damage that poor DNS hygiene could inflict on businesses. Fortunately, solutions like DNS Lookup API can help.

Volumetric DDoS Attacks

A volumetric attack is a type of distributed denial-of-service attack (DDoS) that sends a high volume of queries to a target host to max out its bandwidth. The most infamous volumetric attacks seen to date are those against DYN (1.2 Terabytes per second (TBps) strong) and GitHub (1.35 TBps strong). Volumetric attacks have two subtypes:

- **DNS reflection attacks:** In these, attackers send large quantities of User Datagram Protocol (UDP) packets to a target host. Spoofed queries are sent to open DNS resolvers by using the target's IP address.

- **DNS amplification attacks:** In these, an attacker leverages the functionality of open DNS resolvers to overwhelm a target server or network with an amplified amount of traffic, rendering it and its surrounding infrastructure inaccessible.

Stealth or Slow-Drip DoS Attacks

Also known as the "water torture," a slow-drip attack is a denial-of-service (DoS) technique that targets networks with misconfigured or open resolvers. It often goes undetected due to its

complicated nature, but ultimately leads to resource exhaustion. It comes in three types:

- **Sloth domain attack:** In this, attackers channel queries to their authoritative domain, which returns responses at an extremely slow pace to overwhelm the target's recursive server.
- **Phantom domain attack:** This occurs when the victim's recursive server continues sending queries to forged or non-existent domains until it uses up the valuable resources.
- **Random subdomain attack:** This is similar to a phantom domain attack, except that the DNS queries are sent to non-existent subdomains of an existing domain. The authoritative DNS server attempts to satisfy requests until it can no longer handle other DNS lookups.

Vulnerability Exploit-Aided DNS Attacks

DNS server bugs and protocol- and application-layer vulnerabilities are a minefield for cyber attackers. And the threats that often work against insufficiently protected domains include:

- **DNS hijacking:** Also known as "domain hijacking," this occurs when a hacker redirects a website's traffic to a different website. Malware is often used to change a target's DNS router settings to hijack traffic.
- **Cache poisoning:** This occurs when an attacker sends a forged response to a DNS server that it inevitably stores in its cache. The negative caching can redirect users to an unauthorized IP address for the corrupted domain until the cache is flushed.
- **DNS tunneling:** This occurs when an adversary leverages the DNS protocol, such as Secure Shell (SSH) or Hypertext Transfer Protocol (HTTP) over DNS, to exfiltrate data. The computer sends queries to an open DNS resolver, which redirects it to a command-and-control (C&C) server. A covert channel is then established between the threat actor and the victim's computer.

How DNS Lookup API Can Help Against DNS-Based Attacks

DNS Lookup API allows security professionals to effectively validate daily changes to their DNS records and determine whether the risks are acceptable or not. Below are some other uses of our DNS record lookup product.

Detecting Unusual Behavior from Misconfigured Resource Records

Altered or wrong settings for your DNS protocol can expand your attack surface. Hackers can exploit, for instance, inherent bugs in the BIND signature to manipulate resource records and change authoritative nameservers. Our **DNS record lookup** tool enables you to adequately inspect your resource records to identify the root cause of packet anomalies resulting from such flaws.

Preventing Email Spoofing

Regularly perform a **DNS record lookup** to check if your Sender Policy Framework (SPF) record is present and if its TXT record contains correct values. The record should include your authorized IP addresses, mail servers, and allowed time to live (TTL) value to send emails on your domain's behalf.

Managing Your Corporate Domain Portfolio

Cyber attackers often use exploits in PHP or python script formats to scan the Web for expired domains still attached to apps and nameservers. A **DNS record lookup** can help website owners

verify if their domain nameservers are correctly set up and don’t have dangling pointers. It also ensures that expired top-level domains (TLDs) are detached from old applications that hackers could take advantage of.

DNS records play a central role in not just keeping websites online, but also an organization’s entire operations. Monitoring real-time changes to your nameserver records with **DNS record lookup** tools such as DNS Lookup API is critical to reducing risks of downtime and preventing attacks in the long term.