Reverse NS Lookup: Security Against DNS-Based Attacks

Posted on March 19, 2020

Given today's threat landscape, known threats or those that get publicized are quite hard to protect against. However, risks that come from unknown sources are even harder to detect and block. Domain Name System (DNS)-based attacks fall into the second category for a variety of reasons, the topmost of which is that once domains are up and running, their owners put their security in the background.

There are ways to avoid becoming the next victim of a DNS-based attack, though. One of them is using a reliable reverse name server (NS) solution such as Reverse NS Lookup. But before we delve into further details, let us first discern why attackers take advantage of inherent DNS weaknesses to get to their targets.

Why Attack DNS Servers?

There are several reasons why attackers choose to go after the DNS servers of their chosen targets, which include:

Traditional Firewall Use

Traditional firewalls typically leave port 53 open. This port takes care of all DNS queries. That said, even if companies use the best firewalls money can buy, they may not always be effective in thwarting DNS-based attacks.

Securing networks against DNS-based attacks requires extremely high computing performance. As such, deep inspection may be an impractical approach as the number of distribution points will definitely rack up costs.

Business Disruption

Any company whose DNS infrastructure gets attacked is likely to lose network connection. In that case, any attacker whose primary goal is to effectively render its target inoperational can easily do so with a successful denial-of-service (DoS) attack. The victim is sure to lose Internet connectivity, which leads to revenue loss, customer defection, and brand damage.

What Can Companies Do and How Can Reverse NS Lookup Help?

The best way to secure one's domain against attacks is through proper DNS hygiene. Here are a few tips that can help:

Audit DNS Zones

The first thing a company has to review apart from its DNS server's main configuration is its DNS zone, the portion of the DNS that it manages. Sadly, over time, we tend to forget about test domain names or subdomains that may run outdated software or is unsecured against attacks or has an exposed A record. An A record maps a domain name to its host's IP address.

Reverse NS Lookup can help with this dilemma. Just run all your name servers on it to see if all of the domains and subdomains that they point to (and belong to you) are active. Some of these may no longer be in use and are thus no longer secure. Keep in mind that attackers can take control of forgotten and insufficiently protected subdomains to infiltrate your network. That said, it may be a good practice to regularly check for inactive domains and subdomains and disconnect these from your infrastructure.

Keep DNS Servers Up-to-Date

The great thing about running your own name servers is that you can configure, test, and try things that you may not be able to do when you use the name servers given by your hosting provider.

If you decide to run your own DNS servers, however, make sure that you always patch its operating system (OS) and other software to prevent attackers from exploiting gaping vulnerabilities. Also, make sure that connected domains don't have security bugs that can negatively impact your DNS server's performance. As has been said, **Reverse NS Lookup** reveals all of the domains that run on your name servers.

Get Rid of Ill-Reputed Domains

One bad apple in a basket can sadly turn all others rotten, too. When your website shares a host with a malicious domain, malware infection on one site can spread to the others. Such an instance is what security experts call a "cross-site contamination." Cross-site contamination occurs when a site is negatively affected by neighboring sites within the same server due to poor isolation or account configuration.

Reverse NS Lookup can help prevent such an occurrence because you can quickly identify all of the domains you share a host with. You can then investigate all of them to see if any are malicious. If that's the case, you can ask your hosting provider to either remove the malicious site from your shared server or transfer your domain to a threat-free location.

Your name servers are the key to your website's visibility on the Internet. Without them, potential customers and site visitors in general will never be able to find you online. That's why they're such a tempting target for attackers who wish to cause your business or its customers harm. But justlike any other part of your infrastructure, there is a way to safeguard them and, ultimately, your company from threats. The trick is to submit your DNS to a regular hygiene check with the help of solutions which include Reverse NS Lookup.