Why DNS Attacks Prevail and How to Mitigate Them with a DNS Lookup API

Posted on February 18, 2020

Over the past five years, cyber attackers have been ramping up campaigns targeting the Domain Name System (DNS) as a primary attack vector. The reason? The DNS is a critical part of any organization's operations because it is responsible for properly resolving domain names to IP addresses. In a nutshell, it directs visitors or even potential customers to the right websites.

However, despite the crucial role that DNS servers play, businesses have yet to recognize the need to secure them. Why is that? Let's take a closer look to answer this question, starting with why DNS attacks are typically successful.

Reasons Behind the Success of DNS Attacks and How These Can Be Addressed with DNS Lookup API

DNS Was Not Built with Security in Mind

The DNS was designed for efficiency. When it was created, security and privacy were not yet salient requirements, and so years after, it has repeatedly proven its susceptibility to attacks. Even today's firewalls are usually not equipped to check for DNS traffic. They cannot validate queries nor require authentication for DNS requests and responses.

Because of this, without regularly monitoring DNS records to check if their domains point to the right IP addresses with tools like DNS Lookup API, organizations may not discover malicious connections until it is too late.

Lack of Awareness About the Importance of DNS Server Security

Despite the numerous attacks targeting DNS servers, only 64% of organizations recognize the need for DNS security. Companies do not seem to realize how vital DNS servers are for business

continuity (BC) and data confidentiality. Although they use data loss prevention (DLP) tools, intrusion prevention systems (IPSs), firewalls, and gateway security solutions, these may not be able to help when it comes to securing DNS servers.

What they need instead is a way to ensure the integrity of their domain-to-IP resolutions. A tool like **DNS Lookup API**, for instance, can identify if their domains resolve to the right IP addresses and not those owned by threat actors.

No Proactive Countermeasures in Place

Due to the absence of proactive security measures, enterprises are just reacting to attacks when they hit. In 2016, for instance, when Dyn's servers were taken down by a distributed denial-of-service (DDoS) attack, even the sites of prominent establishments like The New York Times, Twitter, Reddit, Spotify, and Airbnb were rendered inaccessible. And though Dyn addressed the attack, two more waves hit it. Imagine how costly and time-consuming the situation was for its IT and security staff. They needed to shut down applications, processes, and servers that were essential to the business operation. That downtime may have impacted sales and web traffic as well.

Organizations can perform DNS logging regularly to prevent a similar disaster. A DNS log can help them detect security incidents and start acting on an incident response plan. They can monitor DNS logs by looking at them to check for malicious activity or analyzing anomalies in the volumes, frequency, and types of requests and responses.

Placing Too Much Trust on Site Visitors

Another option would be employing the zero-trust model, which requires microlevel authentication. In a nutshell, that means scrutinizing every piece of communication that comes in and goes out of your network.

In DNS's case, every bit of traffic should be vetted before being allowed to pass through. Integrating a **DNS API** into existing perimeter security solutions to identify every time who is behind the domains attempting to communicate with yours may be one way to go about it. It can help screen suspicious entities before they can even connect to your network. But more importantly, it can help you screen your DNS records to make sure nothing is amiss or misconfigured, therefore reducing the likelihood of threat actors' entry into your network.

Absence of Business Continuity and Disaster Recovery Strategies

And if mitigation measures fail, having a BC and disaster recovery (DR) plan in place is highly recommended. You can rely on DNS services along with hardware solutions to redirect traffic while you address a threat to backup servers usually located in external data centers. This approach may, however, be hampered by time-to-live (TTL)-related delays.

While workarounds may do when dealing with DNS attacks, employing a more proactive approach to securing DNS servers could be of great help. Doing so may reduce the likelihood of operations downtime that can lead to a loss of customers and ultimately hurt your bottom line. Bolstering the security of your organization's DNS infrastructure and employing countermeasures with the help of a **DNS Lookup API** can also reduce the risk of becoming the next DNS attack headliner.

Would you like to know more about how DNS Lookup API can help beef your organization's DNS security? Feel free to contact us at sales@whoisxmlapi.com.