How to Fend Off DNS Attacks with DNS Reverse Lookup Tools

Posted on January 18, 2020

You might be aware of how much Domain Name System (DNS) attacks can cripple organizations and their online properties. The 2019 Global DNS Threat Report by IDC confirms this, stating that the average cost of a DNS attack has risen by 49% since last year to $1.27 million. Companies also reported that it takes their teams more than a day to fix breaches, thus drastically affecting operations and revenues.

Today, we'll examine the worst DNS incidents to date and how a DNS reverse lookup tool like DNS Lookup API can help organizations build up domain intelligence against them.

DNS Attacks That Crippled Victims

The Dyn TCP SYN Flood Attack

One of the most massive DNS attacks in history was also the first to hit an Internet infrastructure provider — Dyn — in October of 2016. The multivector denial-of-service (DoS) attack started with a Transmission Control Protocol (TCP) SYN flood to port 53 of the company's DNS servers, followed by a subdomain attack. Hackers directed queries to the DNS servers of Dyn-issued domains to saturate their authoritative nameservers. Hackers then sent junk traffic amounting to 1.2 terabytes per second (TBps) to Dyn by using the Mirai botnet comprising over 100,000 Internet of Things (IoT) devices. The attack took several websites offline, including those owned by tech giants, and cost the victims $110 million.

The GitHub DDoS Attack

GitHub was the target of the most significant distributed DoS (DDoS) attack affecting a company in 2018 without the use of a single botnet. In what was a relatively new form of DDoS attack, threat actors spoofed the target's IP addresses and sent small requests to exposed memcached servers.

The technique amplified responses by a factor of 50, resulting in a 1.3 TBps-strong attack. GitHub worked with a security solution provider to mitigate the incident, allowing it to contain the attack in 15-20 minutes.

The Sea Turtle DNS Hijacking Campaign

Sea Turtle was the first registrar hijacking attack recorded that was tied to state-sponsored cyberespionage. The threat actors hacked into the infrastructures of nonprofit organizations as entry points. Once they had control of the domain registrar, they pointed its DNS records to the target's nameservers causing these to overload.

The attackers used spearphishing emails to compromise user accounts associated with the DNS records. They also exploited seven vulnerabilities that have been left unpatched since 2009.

The Occupy Central Attack

Independent news sites in Hong Kong were the targets of DDoS traffic during the Occupy Central protests in 2014. Five botnets sent trash traffic masquerading as legitimate requests to overwhelm Occupy Central's host. The campaign took popular pro-democracy sites, PopVote and Apple Daily offline. The size of the packet requests reached a peak of 500 Gbps.

Mafiaboy's Project Rivolta

There have been other noteworthy DNS-based attacks, but they pale in comparison with Project Rivolta in terms of downtime. The attack, which took place in 2000, was a precursor to today's more sophisticated DDoS attacks. University networks were used for as botnets and it affected the services of Yahoo!, E-Trade, Amazon, and eBay for a week.

DNS Reverse Lookup Tools Safeguard Organizations' Domain Infrastructures from Attacks

The scenarios above share a common denominator — a lack of thorough risk assessment or vulnerability testing. More often than not, vulnerabilities enable attackers to penetrate victims' networks. Our DNS Lookup API can help organizations reduce cyber risks by facilitating the following activities:

- **Keep track of domains and subdomains:** The tool lets you search for your domains' DNS records. It also allows you to review and update these records to make sure that discontinued or abandoned domains and subdomains can't be hacked and used for attacks.

- **Check domains' DNS configuration:** Security professionals can check if the correct resource record values are set for all domains. They can identify whether changes made to DNS configurations are authorized or not. This is easy to do by validating that all the details in DNS records match their organizations' assets and identifiers.

- **Identify malicious IP addresses:** Running a **DNS reverse lookup** on an IP address provides you with a list of the domains tied to it. From there, you can find out if the address is sending you legitimate requests during traffic surges. DNS Lookup API also helps uncover relationships between IP addresses for improving packet filtering rule sets.

The takeaway of these news stories? Always be on the lookout for vulnerabilities and unauthorized changes to your DNS records. While this sounds quite simple to do, the reality is that it requires concerted efforts to secure all endpoints and the entire network.

Adding a **DNS reverse lookup** tool such as DNS Lookup API to your arsenal can help your security team meet its goal — to protect against DNS attacks that could disrupt your business.