# Why Domain DNS Lookups Matter as Part of Preventing DNS Attacks

Posted on March 3, 2020

When they proposed the Domain Name System (DNS) in 1983, computer scientists Paul Mockapetris and Jon Postel never intended it to become an attractive means for hackers to commit crimes. As a trust-based communications protocol, the DNS was first implemented in the early 1980s to connect devices to the Internet. It works by mapping domain names to IP addresses.

Unfortunately, it wasn't long before unscrupulous actors found the protocol's design and components easy to abuse. Open DNS resolvers abound on the Internet, and the same goes for the exploit kits that criminals can deploy even without any technical knowledge.

Flash forward to 2019, DNS attacks are on the rise. Anyone could become a victim: in the past month alone, a distributed denial-of-service (DDoS) attack hit the U.K.'s Labour Party. Cloud infrastructure provider Amazon Web Services and antivirus vendor Avast also fell victim to similar attacks.

In the wake of these recent attacks, we rounded up a list of the worst DNS attacks in history, and what possible lessons cybersecurity professionals can glean from them. We also briefly discussed how **domain DNS lookup** tools like DNS Lookup API can potentially help to prevent such attacks.

## Limit DNS recursion from external IP addresses

Spamhaus is a non-profit organization that supplies blocklists to Internet service providers (ISPs), corporations, and cybersecurity companies. It's no wonder then why it's a red-hot target for hackers, who aimed one of the most massive packet floods in history at it.

Attackers sent open DNS resolvers forged requests for a zone file for ripe[.]net by spoofing Spamhaus's IP address. Each response was around 2.5Mbps, way below the baseline. Due to 30,000 open DNS resolvers, however, it was severely amplified. A 100Gbps flood initially brought down the antispam organization's server, after which it was bombarded again with 300Gbps in a subsequent attack.

**The solution:** Spamhaus sought external help to mitigate the DNS reflection attack, as it was impossible to handle with an onsite solution. Through load balancing, the request were redirected among 20+ data centers for scrubbing, which enabled to lower Spamhaus's network congestion significantly and restore its services.

The responsibility of closing open DNS resolvers rests on the shoulders of network providers and web administrators. The ideal scenario would be for them to conduct regular network cleanup to identify open DNS resolvers or to implement stricter network ingress filtering rules. One way is to limit servers from performing recursive lookups for uncommon addresses. As part of that process, users can rely on DNS Lookup API to verify IP addresses and queries.

## Enable multi-factor authentication (MFA) and DNS Security Extensions (DNSSEC)

In 2008, Turkish hackers defaced several domains owned by the Internet Corporation for Assigned Names and Numbers (ICANN) and its subsidiary, the Internet Assigned Numbers Authority (IANA). The hijacked domains, which included icann[.]com, icann[.]net, iana[.]com, and iana-servers[.]co, were used as mirror servers.

The multivector attack redirected users visiting these domains to atspace[.]com, which showed the message: "You think that you control the domains, but you don't! Everybody knows wrong. We control the domains including ICANN! Don't you believe us?" The hijacking lasted for 20 minutes until ICANN and IANA regained control of their sites.

**The solution:** To guard against domain hijacking, it's recommended to activate MFA and DNSSEC as countermeasures. A location-based factor in MFA, for instance, can prevent threat actors from signing in from outside a corporate network. Meanwhile, DNSSEC validates DNS lookups by authenticating the source of the record with a digital signature. It also stops users from being misdirected when DNS records undergo unauthorized changes. Besides, organizations can use DNS Lookup API to make sure that their DNS records only point to authorized IP addresses.

## Never underestimate good network and endpoint protection

Last year, Cisco's Talos Intelligence Group uncovered a multipronged DNS hijacking campaign that affected over 50 government agencies and private companies in Lebanon and the United Arab Emirates (U.A.E.). Based on the attackers' tools, tactics, and procedures (TTPs), the campaign used malware called "DNSpionage" to infect target hosts and steal data. The second stage of the attack was a DNS redirection campaign for the name servers of the Lebanese Finance Ministry, Middle East Airlines (MEA), and U.A.E. government domains.

The infection vector was a malware-ridden job application form hosted in two fake job listing websites. The form came as a downloadable Microsoft Word document laced with a malicious macro. The macro downloaded the payload onto the victim's computer then created a covert channel connected to the attackers' command-and-control (C&C) server via the DNS. Through this channel, the attackers may have been able to siphon off email credentials and sensitive data from the victims and send commands to the malware.

**The solution:** The best and up-to-date malware solutions and next-generation firewalls (NGFWs) provide a good layer of protection against DNSpionage-type attacks. Intrusion prevention systems (IPSs) can also defend networks against nefarious activities, emails, and domains. Users can also integrate DNS Lookup API into IPS tools to provide additional intelligence that can be compared with threat data to identify connected domains and name servers that need monitoring, further investigation or blocking.

We're bound to see more DNS attacks as long as there is a way for hackers to attack the protocol.

By plugging all security loopholes in the DNS, companies can stand a chance against such costly attacks. **Domain DNS lookup** tools like DNS Lookup API can help prevent incidents by providing infosec professionals with accurate and near-real-time threat intelligence.