# Understanding and Securing Your DNS Records with a DNS History Lookup Resource

Posted on February 7, 2020

The Domain Name System (DNS) is commonly abused because successfully attacking it reaps great rewards for threat actors and cybercriminals. Domain hijacking, for instance, can allow attackers to siphon off personally identifiable information (PII) and confidential corporate data from compromised domains. And since not all security solutions and technologies monitor DNS packets, threat actors can exploit this to infiltrate target networks.

Not all is lost, however, as regularly checking your DNS records for anomalies is an excellent proactive security measure. A **DNS history lookup** resource such as DNS Database Download can provide you with actionable threat intelligence.

But before we dive in and establish how to go about DNS record protection, let us first discuss the various types of DNS records that need protecting.

## DNS Record Types and Their Uses and How They Can Be Abused

### A Record

In a nutshell, the A record contains the IPv4 address that a domain name points to. Google.com's A record, for instance, would contain the IP address 172.217.11.78.

Attackers can modify or hijack a domain's A record to redirect users to malicious sites that they own and operate. These malicious sites can be phishing pages designed to steal visitors' login credentials or malware-hosting sites that automatically drop malicious files onto victims' systems.

### AAAA Record

An AAAA record is the IPv6 equivalent of an A record. It is susceptible to the same attacks as its

IPv4 counterpart.

### PTR Record

A PTR record is the exact opposite of an A or AAAA record. While A and AAAA records point domain names to IP addresses, PTR records resolve IP addresses to domain names. Like A and AAAA records, however, they may also be subject to the same attacks.

### CNAME Record

Canonical names are also known as “aliases.” Domains that share a single IP address use a CNAME record. That way, an A record does not have to be created for each host.

### MX Record

A mail exchange (MX) record indicates which mail servers should handle emails for a specific domain. It also specifies the order in which mail servers handle communications.

When your DNS infrastructure is compromised, attackers can intercept email communications directed to your organization and point these to their own mail servers instead. Such an attack may cause the leakage of confidential information to unauthorized recipients, which could severely impact your business.

### NS Record

A name server (NS) record distinguishes the subzones of your DNS servers. Each NS record must

be in a separate zone for redundancy purposes. Organizations typically have more than one NS in case issues arise, such as their primary NS being rendered inaccessible.

Unauthorized changes to one NS record (most websites have at least two) allow attackers to take control of a victim's DNS server and serve results as they wish or set custom time-to-live (TTL) timing, among others.

### SOA Record

A start of authority (SOA) record acts as storage for information on your DNS zone. Details like its administrator and data source server name, among others, are contained in an SOA record.

While SOA records are not usually attacked, when improperly configured and left outdated, they may reduce NS bandwidth, decrease your site access speed, and won't be able to keep your site up when its primary DNS server is down.

### TXT Record

A text (TXT) record contains additional information about a domain in a human-readable or plain-text format.

## How to Secure DNS Records

When cybercriminals and threat actors abuse weaknesses in your DNS infrastructure and consequently hijack your domains, they can turn your web properties into malware hosts or point your visitors to harmful sites. In more unfortunate cases, attackers can gather administrator account credentials that allow them to move laterally throughout your network to exfiltrate

corporate secrets. You can, however, prevent DNS-based attacks by:

- Regularly applying patches for software and firmware vulnerabilities. Patch management is critical to prevent exploitation from affecting your network. Once attackers get inside it, they can easily modify your DNS records and thus wreak greater havoc.
- Monitor your DNS records regularly, not only for irregularities but also for possible exposure. Plug all gaps in your DNS records and make sure you don't leave any of them dangling.
- Make sure your domain registrar is reliable and trustworthy. Choose one that has security measures in place.

## Why Use a Passive DNS Database?

A passive DNS database such as DNS Database Download is a means to look at the entire history of a domain name. Such a repository may shed light on the makeup and health of a domain's infrastructure. All of the changes DNS records have undergone, for instance, could point to when the attack started. Knowing that may lead to the identification of attack vectors that should be blocked and so on.

Our **DNS history lookup** database contains pertinent information on 1 billion domains and 2 billion hostnames. It is a product of more than a decade of scouting the web for domain information.

Would you like to know more about how DNS Database Download can aid you? Contact us at support@whoisxmlapi.com.