Why DNS History Matters: 5 Key Use Cases of Passive DNS

When Florian Weimer introduced the passive Domain Name System (DNS) replication technology in 2005, his goal was to provide a source of name resolution data distilled from actual DNS query traffic. He also saw the necessity to find a way to look at **DNS history** as a safeguard against the ease with which anyone can control and modify DNS records.

Where did things go from there? Passive DNS has been around for a decade and a half, but there is still confusion as to what it is and how it can help organizations. So, this article aims to distinguish passive from active DNS. By extension, we explored some reasons why a passive DNS database that gives users access to **DNS history** can be very beneficial.

Active DNS Versus Passive DNS

The whole domain name system is a distributed database consisting of zone files as primary sources and cached data. And when we talk about active DNS, we refer to DNS responses to deliberate DNS queries. Looking into the system, therefore, gives you a list of DNS servers that are reachable by IPv4 or IPv6. The DNS data it provides is helpful when users want to change their DNS server settings.

The tricky part is that several people can add DNS records if given permission to change the zone file, as well as to add a new hostname for a given IP address. Furthermore, it’s easy to create new zones.

The challenge, however, is that the domain name system on its own does not contain historic records stemming from successive active DNS queries. So, you cannot tell what the hostname of a host was 2 weeks ago if it has been modified in the meantime. Because of that, there are attacks against the maintenance mechanisms, notably cache poisoning, which can lead to the malfunction of DNS.

By keeping logs of the DNS traffic, passive DNS provides an answer to this problem. It keeps track of DNS history and serves as a kind of an independent data source that can reveal cache poisoning or other inconsistencies. Millions of DNS queries made over the Internet, along with their corresponding responses, are therefore recorded as a backup thanks to passive DNS. In turn, a passive DNS database gives users a glimpse of a tremendous amount of historical DNS queries and responses. Each modification also has a timestamp.

With this glaring difference in mind, we conclude that passive DNS is an essential requirement when it comes to threat hunting and defense and cybercrime investigation, among others. The succeeding sections will explain why that is so.

5 Cybersecurity Uses of Passive DNS Data (That Isn’t Possible with Active DNS Information)

1. Deter Malware Attacks

Malware applications and files often have domain names hard-coded into them. To hide their primary node, however, threat actors use stealth techniques such as fast fluxing, which is easy to detect with passive DNS data. By looking at logged DNS information, security teams can see that a domain name resolves to an unusual number of IP addresses, and changes IP addresses at a high frequency. This can be a telltale sign of a malware attack, which also effectively identifies infected computer networks.

2. Identify Domain Associations

When a malicious domain is detected, it's easy to report it so it can be removed from a server or submitted to a blacklist authority to alert everyone. But it's only a matter of time before a threat actor strikes again using another domain name. Quite often, cyber attackers even use multiple domains in simultaneous attacks.

However, it's common for cybercriminals to reuse at least some of their infrastructure, thus tracing their digital footprint using passive DNS data can sometimes be possible. Therefore, security teams can determine which domains are associated with a malicious domain by looking at a **DNS history** database. Once all associated domains are retrieved, it's only a matter of deciding whether to block all domains or further investigate each of them before taking the appropriate action.

3. Detect Phishing Attacks

In phishing attacks, threat actors use domain names that sound and look like those of well-known companies or brands. Usually, there's only a one-letter difference or an unnoticeable typo. When organizations have an updated passive DNS database, however, they can check for domains that may be used in phishing attempts. They can then compare the **DNS history** records of these suspicious domains with those of legitimate domains to see if they match.

4. Uncover Possible Trademark Infringement

In the same way, users detect possible phishing vectors, and brand owners can check for potential cases of trademark infringement by getting hold of a passive DNS database. They can look for domains that use their trademarked names in any way.

5. Recover Zone Data

Passive DNS makes it possible to restore lost zone data at a specific date since it contains time-stamped DNS history records. It also comes in handy as a guide when there are incorrect records that require removal.

Compared to active DNS, passive DNS is often more effective in battling prevalent cybersecurity issues such as phishing, malware attacks, and domain or brand infringement. **DNS history** allows cybersecurity professionals to enhance their threat hunting and detection capabilities. For more information on both active and passive DNS, you can also check our domain name system primer.