The Strategic Value of Passive DNS to Cyber Defenses and Risk Management

Dave Shackleford

SANS

A SANS Whitepaper

The Strategic Value of Passive DNS to Cyber Defenses and Risk Management

Written by **Dave Shackleford**

February 2021

Sponsored by:

Farsight Security

Introduction to DNS and Passive DNS

The Domain Name System (DNS) is arguably one of the most important services facilitating internet communications (and internal IT communications) today. Systems, applications, and users rely on DNS to resolve the names of services and sites they need to visit. Browsers and other clients and services, however, communicate via IP addresses. IP addresses are displayed as a series of numbers separated by dots. DNS is important because it translates domain names to IP addresses, and vice versa. DNS is usually associated with "records" of domain information (or resource record names) and related attributes (resource data).

Important DNS Record Types

There are numerous types of important DNS records, but here are some of the more commonly used ones:

- **`A` Records—**These records map domain names to traditional (**`IPv4`**) *dotted quad* addresses.

Example:

```
sans.org.          7200    IN      A       45.60.103.34
sans.org.          7200    IN      A       45.60.31.34
```

- **AAAA Records—***Quad A* records map domain names to IPv6 addresses.

Example:

```
google.com.             166     IN      AAAA    2607:f8b0:4002:c09::8b
google.com.             166     IN      AAAA    2607:f8b0:4002:c09::65
google.com.             166     IN      AAAA    2607:f8b0:4002:c09::71
google.com.             166     IN      AAAA    2607:f8b0:4002:c09::66
```

- **`CNAME` Records—**These records make it possible for one domain name to point to another domain name. This can be convenient for situations such as virtual hosting environments.

Example:

```
mail.google.com.        580612  IN      CNAME   googlemail.l.google.com.
```

- **`TXT` Records—`TXT`** records are something of a catchall record and are often used to share miscellaneous information about a domain. For example, **`TXT`** records are often used to share **`SPF`** details describing a domain's email sending policies.[1]

Example:

```
sans.org.               244     IN      TXT     "status-page-domain-verification=2w964jh22625"
sans.org.               244     IN      TXT     "v=spf1 include:sans.org._nspf.vali.email include:
%{i}._ip.%{h}._ehlo.%{d}._spf.vali.email ~all"
```

- **`MX` Records—**Such records define the **`Mail eXchanger`** records for a domain or where inbound mail for a domain should get directed.

Example:

```
sans.org.               10      IN      MX      0 sans-org.mail.protection.outlook.com.
```

- **`NS` Records—`NS`** records specify the name servers used by a domain.

Example:

```
sans.org.               167056  IN      NS      ns-1270.awsdns-30.org.
sans.org.               167056  IN      NS      ns-1746.awsdns-26.co.uk.
sans.org.               167056  IN      NS      ns-282.awsdns-35.com.
sans.org.               167056  IN      NS      ns-749.awsdns-29.net.
```

- **`PTR` Records—**Whereas **`A`** and **`AAAA`** records map domain names to IP addresses, **`PTR`** records go the other direction, mapping IP addresses to domain names. Unfortunately, these records are not always reliable and are often poorly maintained by many organizations.

Example:

```
8.8.8.8.in-addr.arpa.   29559   IN      PTR     dns.google.
```

[1] Sender Policy Framework, www.open-spf.org

Active DNS lookups and information exchange comprise the normal day-to-day DNS operations that most online activity relies on, but there's also value in storing historical DNS information and query data.

Passive DNS systems collect and store DNS resolution data over time so that you can reference past DNS records and information to uncover potential security incidents or discover malicious or suspicious adversary infrastructure. Although DNS is a very active protocol in most organizations, DNS records may change frequently. Without historical DNS records, it can be difficult or impossible to discover and investigate malicious asset DNS records from the past. Passive DNS helps security and operations teams analyze historical patterns and use predictive analysis to uncover unusual behaviors and possible attacks. In a relatively simple manner, teams can look for valuable historical information about a domain. For example, an incident response or forensics team can observe the date when a domain's A (name) record changed. This information can also tell them the previous name record and what its current value is. Passive DNS also has the advantage of stealth; unlike live DNS lookups where you're querying live records, you can avoid alerting adversaries to investigations.

Role in Security Detection and Investigations

Passive DNS has come to play a significant role in the realm of information security—and not just due to its mission-critical status for domain name resolution. Many security investigators and operations teams have come to rely on passive DNS for vital security functions that include detecting and blocking threats as early as possible in attack cycles, investigating and responding to threats, and rapidly identifying compromised infrastructure within their environments.

Passive DNS can provide numerous clues to attacker activity. Attacker campaigns and specific actions may interact with DNS in many places, as shown in Figure 1.

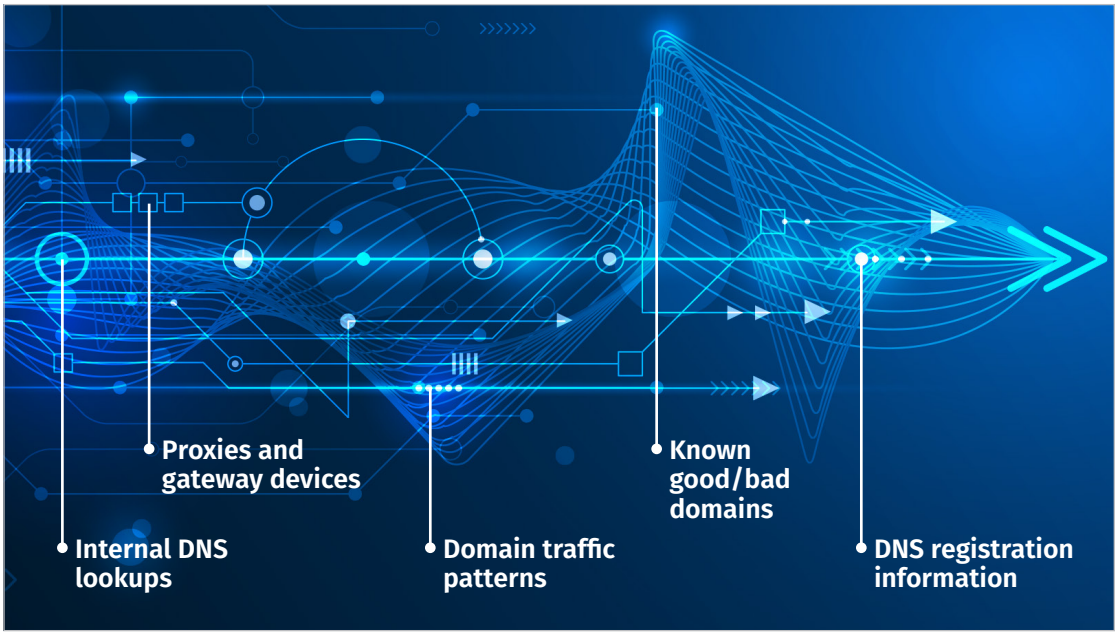

Figure 1. Places Where Attacker Campaigns May Interact with DNS

Passive DNS can be used to track and potentially help identify attack patterns and malicious infrastructure or attacker motivations. Domain reputation can also help identify bad actors and those associated with attacks in the past. Integrating reputation scoring and blocking/alerting actions can help in network defense. DNS can change rapidly, so organizations should, ideally, have a dedicated provider integrate these actions continuously.

Indicators of compromise (IoCs) related to DNS can help incident responders and forensics analysts to better detect unusual activity and respond more readily. Indicators might include:

- Local DNS queries
- Remote DNS queries
- DNS entry TTLs (time to live)
- Patterns of DNS lookups and access
- Logs in local and network devices

These IoCs can be used for investigations and building preventive controls such as blocking malicious domains.

The following sections provide a look at how passive DNS can be beneficial in incident response, forensics, security operations, threat hunting, and threat intelligence.

Incident Response

The goal of incident response in the context of DNS is to provide response to a variety of threats on the brand and domain of an organization. These threats are innumerable and could include ongoing and current inbound attacks, compromised internal systems, malware and bot activity, command and control traffic, phishing attempts, and other such malicious actions. Passive DNS queries and responses are among the best data sources that security teams can use during incident response investigations. Investigators rely on passive DNS because it can detect malicious activity earlier in the attack cycle than other security tools, in some cases, and provides a more extensive source of records related to a wide variety of malicious activity.

When an attack/infection occurs, investigators need tools that provide a holistic view of the extent and severity of the threat. Passive DNS domain/address investigations are one of the top tools investigators use to determine who in their organization was infected after an attack/infection occurs. In fact, passive DNS and malware analysis can be very effective in identifying what data and systems the attacker accessed. Investigators also find passive DNS helpful in their attempts to determine how much information the attacker accessed, especially when post-compromise data exfiltration has occurred.

The primary use case for passive DNS data for incident response is rapid investigation and analysis of suspicious activities that could help determine whether an incident or breach has actually occurred.

The primary use case for passive DNS data for incident response is rapid investigation and analysis of suspicious activities that could help determine whether an incident or breach has actually occurred.

Example Scenario for Incident Response

As an example of passive DNS data used for incident response, imagine that a network operations team reports that all the organization's firewalls of a certain type/brand began communicating to the same IP located in a foreign country.

Note: The SOC and IR teams do not want to scan this IP actively, potentially alerting the adversary that their presence has been detected.

Fortunately, passive DNS allows for remote threat actor domain investigations without touching the adversary's infrastructure at all. All the data queried by passive DNS is historical in nature.

During its initial queries, the security IR team first set out to understand the historical evolution of the infrastructure. In doing so, the team discovered that the targeted IP had not been in use for quite a long time. It also discovered:

- Every past use of the IP address was associated with a different single domain that consisted of the same name (the name of the firewall vendor followed by a number sequence that appeared to be the date the domain was first observed).
- All the domains were hosted on the same name servers.
- The name servers were hosted on similar domains named after different vendors pointing to different IPs in the same range as the suspect IP address.
- The last observed time was different for every domain, and some domains were still in use.

Further inspection of the firewalls revealed that internal devices had been remotely compromised via an unknown vulnerability.

Follow-Up Activities

- The IR team could notify other vendors about active campaigns against their customers, as well as notifying local government and law enforcement agencies.
- Block known malicious domains discovered during the investigation, an action that could be automated.

Forensics

Forensics and incident response are inextricably linked in most security teams. The goal of forensics is to analyze acquired evidence and data to determine what, when, and where a bad actor attempted or successfully gained access to the infrastructure; potentially provide testimony for prosecution; and help create mitigation strategies to prevent future attacks. Passive DNS is valuable in these endeavors due to the presence of forensic "markers" of activity, which can lead to actionable information for forensics teams (for example, past queries and responses or current domain information). In addition to identifying compromised resources on the network, another major element of forensics work with passive DNS is working to understand what resources point to an organization's infrastructure to help build better defenses.

Example Scenario for Forensics

In this scenario, an organization has just investigated a hijacking incident that occurred on its primary customer-facing website. The forensics team has been tasked with gathering evidence and investigating further.

At first glance, the site seemed to be working and every DNS record was accurate. However, there were consistent reports from customers that the site was asking them to re-enter credentials even though they were double-checked for accuracy numerous times. This process consistently happened over a period of several months and always during nighttime (off-business) hours.

The forensics team discovers that DNS server logs (primarily audit logs) are not readily accessible due to DNS being operated by a third-party provider that does not make these available. The team then turns to passive DNS data to look at the historical DNS records for the past six to eight weeks. They discover that DNS records indeed have been changed. They find that some DNS zone file settings were altered. After the previous settings lapsed, there were nightly changes to the DNS record for the site, causing it to resolve at different IP addresses all over the world. Some of the IP addresses still resolve to clones of the company site, and all exhibit the same behavior described in customers' complaints.

Follow-Up Activities

- Further investigation is needed. It may reveal that the company's DNS servers had been compromised and the adversary was using fraudulent DNS records to point to a cloned credential harvesting infrastructure they had created, likely to follow up with phishing and other attacks against customers directly.
- Law enforcement could then be notified, if desired or required.

Security Operations

Many types of activities in the realm of security operations align with the use of passive DNS. Security operations teams may perform any of the following types of activities that involve current and historical DNS data:

- Monitoring access attempts and sources
- Conducting proactive assessments/audits
- Red team/real-world assessments
- Blue team/enhanced and focused security controls

Most importantly, passive DNS can give security operations teams much needed visibility into which devices are making requests to connect to malicious destinations. This visibility allows the security team to sever those connections and protect the organization's entire infrastructure if needed.

Example Scenario for Security Operations

In this example, the response team identified several dozen IP addresses that participated in a mild DDoS attack with an unusual payload targeting an API gateway. This attack caused extended downtime and significant business impact on partners.

Security operations analysts were tasked with analyzing whether the attack was random or a coordinated effort. As the security operations team assessed historical DNS data, that data initially appeared as though all of the IP addresses involved in the attack randomly belonged to different ISPs in different geographic regions.

The analysts then noticed similarities among the host names that were pointing to the attacker IP addresses. The domains belonged to many different banks and the host names suggested all were similar API gateways.

Follow-Up Activities

- Further analysis of the payload is needed. The security operations team may learn that all API gateway systems might have been compromised through a common vulnerability and conclude that it was not a DDoS attack but rather a worm/bot attempt to compromise recently patched API gateways.
- Law enforcement and/or the other affected organizations could be notified, if desired or required.

Threat Hunting and Threat Intelligence

The primary goal of threat hunting with passive DNS data is to proactively search for network threats and indicators that may assist with and facilitate ongoing investigations. There are many possible use cases for threat hunting with passive DNS information. Hunting with passive DNS information allows threat researchers to:

- Pivot from single indicators to other DNS resources as needed, prior to following interesting or unusual queries, responses, and DNS information
- Use incomplete indicators to search for clues
- Help build preventive blocking measures in conjunction with security operations and others

Example Scenario for Threat Hunting

In this scenario, a peer organization within a particular vertical has reported, via intelligence-sharing channels, that it has experienced a variety of phishing attacks on its customers recently.

Based on intelligence, it appears that the phishing domains always contained each company's domain as a subdomain to disguise the malicious intent and confuse customers using mobile devices.

The threat hunting team, using the information provided by their industry peers, discovers that all malicious domains were hosted on the same set of name servers that were pointing to IPs distributed globally. While it appears that hosts on those IPs have been compromised to accommodate malicious websites, the fact that all malicious domains used the same name servers is noted for later investigation stages.

Follow-Up Activities

- Further investigation could yield more information. The organization may discover that the identified domains also had subdomains resembling the names of many different organizations in this sector. The discovery may uncover many unknown past phishing campaigns, including some for which the infrastructure was being prepared but were not yet known to be active.
- Notify law enforcement and/or share additional threat intelligence, which could lead to the prevention of potential future campaigns.

Threat intelligence, in general, relates to collecting and enriching threat data/details. Threat hunting can contribute to this effort, as can external threat intelligence data aggregation from peers and third-party organizations. Goals of building and developing threat intelligence include:

- Identifying current and future information on security threats
- Answering the "who, how, and why" for any given attacks
- Dissecting attack tactics, techniques, and procedures (TTPs)
- Evaluating attacker TTP relevance and impact in the business context
- Identifying opportunities to make high-level security architecture changes that will hinder an adversary's specific TTPs

Example Scenario for Threat Intelligence

An employee was contacted via a leading job search site to complete a survey. The employee viewed the survey and found some of the questions to be unusual and suspicious. Several questions revolved around a project that was currently not publicly disclosed and was known by only a limited number of senior stakeholders.

The next morning, the employee reported the survey website to the company's information security team. However, it appeared the website was no longer available. This type of scenario can prove vexing to security investigators, especially because few conventional methods offer any insight into what has happened.

Follow-Up Activities

- Further investigation can yield more information. The threat hunting and intelligence teams may discover that the domain pointing to the survey website was only active for several days prior to the reported incident. They may also discover a similar pattern with dozens of subdomains that were live for no longer than a few days. All of the domains may point to the same IP, which was not active outside the specific live campaigns noted.
- The threat intelligence team should contact the vendors. They may discover that one of them recently noticed suspicious activity that may have been a compromise—and that all discovered subdomains resemble names of other organizations in the same sector as well as common vendors typically partnered with these organizations. Notify all organizations using this supplier (some of which may consequently discover they have been compromised for quite some time already).
- Notify law enforcement and/or share additional threat intelligence, which could lead to prevention of potential future campaigns.

Additional Passive DNS Utility

Passive DNS is most likely to be used frequently by security operations teams, incident handlers, threat hunters, and similar security-related disciplines. However, there's immense value in DNS information regarding just about all facets of IT and organization/brand protection, and these priorities will apply to many other types of stakeholders within any organization. First, passive DNS information can assist IT audit teams by providing accurate historical and current domain and infrastructure details. If the audit team needs to see how DNS records and internal system lookups have changed over a period of time, DNS records are the primary source of information.

For IT operations teams, passive DNS information can prove invaluable in many ways. First, teams can identify legacy or older DNS records and infrastructure to help in resolving incidents or outages. Additionally, they can help identify suspect internal assets or systems communicating in unusual ways, possibly indicating misconfiguration or other issues.

Numerous other teams and stakeholders can also benefit from passive DNS data, including:

- **Business units (mergers and acquisitions)—**Business units can evaluate potential merger and acquisition targets to determine any operations history that may be relevant in investment decisions. This evaluation might include third-party relationships expressed in `CNAME` and `SRV` records (in outsourcing arrangements, for example).
- **Anti-fraud—**Fraud activities may be due to deliberate actions on the part of malicious actors who seek to manipulate DNS records or set up false sites to trick/lure prospective victims. Passive DNS can help reveal these trends and specific issues in many cases.
- **Brand protection—**Any malicious domains engaging in impersonation and fraudulent activity can be targeted for legal takedown attempts. Anti-piracy and anti-counterfeit teams can also benefit from the same types of investigations and processes.
- **Security management—**Security management benefits from all the aforementioned security practices and use cases, but it will particularly benefit from the development of attack trends and metrics related to historical DNS use and abuse. As security teams use passive DNS more comfortably, additional operational and financial benefits will become more readily apparent over time.

Conclusion

The variety of information security capabilities and processes needed to effectively prevent, detect, and respond to incidents and attacks today is broad and varied. However, a number of operational concepts and technologies can offer enormous value to security teams and many others simply by virtue of their significance and importance. In fact, passive DNS may help detect and prevent many attacks that other security tools cannot. Passive DNS data can help to identify these items and much more:

- Assets that may be compromised
- External actors seeking to develop malicious sites and content that may harm the organization
- Active attacks that rely on DNS for phishing
- "Water hole" style attacks that lure victims to malicious sites
- Counterfeit and fraud scenarios
- Command and control or data exfiltration activities

Passive DNS may help detect and prevent many attacks that other security tools cannot.

Passive DNS should be considered as part of a comprehensive threat solution that increases security and operational coverage, potentially reducing the costs of correlation and overall threat management.

About the Author

Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director, and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and as CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

FORESIGHT SECURITY