Attackers are using DNS for data theft, denial-of-service, and other malicious activity. Proactive monitoring of DNS activity can help network administrators quickly detect and respond to these threats.

About the Domain Name System (DNS)

The Domain Name System (DNS) provides a hierarchy of names for computers and services on the Internet or other networks. Its most noteworthy function is the translation of domain names such as example.com into IP addresses. DNS is required for the Internet to function, operates on a global scale, and is massively distributed.

DNS servers normally accept messages on UDP port 53. The DNS protocol has two message types, queries and replies; both use the same format. These messages are used to transfer resource records (RRs). A RR contains a name, a time-to-live (TTL), a class (normally IN), a type, and a value. For example, an A-type resource record specifies the IPv4 address associated with a domain. The domain name space is divided into DNS zones and a server is considered authoritative if it has authority for a particular zone.

An "A" resource record for example.com

| example.com | 3600 | IN | A | 93.184.216.34 |

A DNS request involves the following parts (in the common case):

Recursing resolver

The resolver receives the request from the client and makes further requests as necessary to obtain the authoritative record.

Root nameserver

A root nameserver can be queried to acquire more information about a particular top-level domain (TLD), such as com.

TLD nameserver

A TLD nameserver provides information about domains ending in a particular TLD.

Authoritative nameserver

Finally, an authoritative nameserver is one that contains the actual DNS records for a particular DNS zone.
Example 1. DNS request and resolution

For example, consider a user attempting to connect to a website at example.com. Before attempting to connect, the system must acquire the IP address for that domain (an A record for IPv4). Here is the basic process for resolving an uncached record:

![DNS Request and Resolution Diagram]

DNS security concerns

When the Domain Name System was designed, security was not a major consideration. Now, malicious actors are using DNS for data theft, denial-of-service attacks, command-and-control, and other malicious activity. According to an EfficientIP survey for 2018[^1], the average cost of a DNS attack was $715,000 (57% higher than in 2017) and 77% of organizations were subject to DNS attack.

Common types of DNS attacks include:

DNS hijacking

An attacker can perform DNS hijacking by manipulating either user workstations or DNS servers. In the first case, malware is used to modify a workstation’s configured name servers, causing DNS requests to be sent to malicious servers instead. Alternatively, a DNS server may be compromised and configured to return incorrect replies. Either way, users are directed to an attacker’s site, allowing the attacker to steal user credentials (phishing), generate traffic (pharming), distribute malware, or publish a defaced version of the website.

In early 2019, FireEye identified a DNS hijacking campaign[^2] of “unprecedented scale” that has had a “high degree of success” targeting victims across the globe. Soon after, the United States Cybersecurity and Infrastructure Security Agency released Emergency Directive 19-01, which outlines actions for mitigating the risk of DNS hijacking—including DNS auditing and monitoring. The recent Sea Turtle[^3]...
campaign is a state-sponsored DNS hijacking attack that has targeted at least 40 different organizations across 13 different countries, using man-in-the-middle attacks to harvest user credentials.

**DNS tunneling**

DNS queries and responses can contain data payloads capable of transporting malware, stolen data, command-and-control information, or bidirectional protocols such as SSH. DNS traffic is often considered benign and not monitored. Therefore, DNS tunneling may be of particular interest to an attacker as a covert communication channel.

Many types of client malware make use of DNS tunneling, including point of sale (PoS) malware like MULTIGRAIN[^4], remote backdoors such as DNSMessenger[^5] and DNSpionage[^6], and botnets like JAKU[^7]. There are also several open-source DNS tunnel implementation examples: [dnscat2](https://github.com/dnscat/dnscat2), [iodine](https://iodine.im/), and [Heyoka](https://www.heyoka.net).

**Various denial-of-service (DoS) attacks**

There are several different types of denial-of-service attacks that are used against DNS servers, including NXDOMAIN, phantom domain, and domain lock-up attacks. In each case, the attacker’s goal is to increase load on the server to the point where it is unable to answer legitimate requests.

One of the largest of these attacks was the 2016 Dyn distributed DoS (botnet) attack[^8], which brought down many major sites in the United States and Europe.

**DNS cache poisoning**

Cache poisoning (or spoofing) occurs when a DNS resolver accepts an invalid resource record due to a vulnerability. An attacker may use a long time-to-live (TTL) value, during which time the data is retained in the resolver’s cache and the resolver is considered “poisoned”. The result is similar to DNS hijacking. DNS cache poisoning is mitigated by cryptographic signatures such as those implemented by the Domain Name System Security Extensions (DNSSEC), but DNSSEC is not yet universally deployed.

By proactively monitoring DNS audit logs and query traffic, IT personnel can more quickly identify and respond to a DNS attack, reducing its impact.

## DNS data that can be collected and monitored

There are many different DNS-related events that can be collected from a DNS server. The actual data available is dependent on the DNS server in use. Events that may be available for collection include, but are not limited to:

**Dynamic updates**

If a DNS server is configured to allow DNS updates via Dynamic DNS (DDNS), these events should be available for auditing, including approval and denial of update requests.
Zone transfers

DNS databases can be replicated between DNS servers with zone transfers (the AXFR query type). These transfers, inbound and outbound, should be logged.

Rate limiting

A DNS server may implement rate limiting to help mitigate various types of DNS attacks, including response rate limiting (RRL) and client rate limiting. When rate limiting takes effect, some queries are ignored (for RRL) or client requests cannot be resolved.

DNS signing

Events may be logged for DNS transaction signing protocols including DNSSEC and TSIG.

Query logs

DNS servers often provide some form of query logging, also referred to as analytical logging. These events detail all requests that are handled by the server.

Resolution queries

Events may also be available for recursive lookups performed in order to resolve client queries. These logs may provide destination IP addresses and other details associated with these queries. These also could be categorized with analytical logs and may be included as part of query logging.

This metadata may be available for query logging (analytical) events:

Client IP address

Source addresses can help administrators identify devices that may be compromised on a local network, or malicious actors on the public Internet.

Domain name queried

The domain name in requests can be compared with a list of known malware domains. Esoteric domain names or repeated lookups may indicate the presence of malware.

Record requested

The types of records requested may be an indicator of malicious activity. For example, the TXT record in particular is often used for command-and-control or DNS tunneling.

Request flags

There are several status flags associated with a DNS message, including whether the message is a request or response, whether the query is recursive, DNSSEC status, etc.
BIND 9 name server logging

There are two types of logging to consider for BIND 9 servers:

BIND 9 logging

The standard BIND 9 logging system uses *channels* and *categories*. Each channel logs messages to a specified Syslog facility or file. All log messages are organized into categories, which range from security related (such as *update-security*) to analytical (such as *queries*). Each category specifies one or more channels to use for log messages in that category. For more information and a full list of categories, see the BIND 9 Administrator Reference Manual.

**BIND 9 query log sample**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Client IP</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-May-2019</td>
<td>info</td>
<td>client @0x7f82bc11d4e0</td>
<td>10.80.0.1#53995 (google.com)</td>
<td>query: google.com IN A +E(0) (10.80.1.88)</td>
</tr>
</tbody>
</table>

Configuration monitoring

File integrity monitoring can also be implemented for the BIND 9 configuration files (for example, in the `/etc/bind/` directory). This could be done as part of a system-wide DNS server auditing plan.

Windows DNS Server logging

There are four types of logging available for Windows DNS Server events.

**Analytical logging**

DNS analytical logging uses the Event Tracing for Windows (ETW) system to provide high-performance logging of all DNS transactions. The logs can be collected from the `Microsoft-Windows-DNSServer` provider. This functionality is available beginning with Windows Server 2016, or as a hotfix for Server 2012 R2, and is the preferred method for collecting DNS Server transaction logs. DNS Server performance should not be affected except during very high query rates. For more information, see DNS Logging and Diagnostics on Microsoft Docs. For the Server 2012 R2 hotfix 2956577, see Update adds query logging and change auditing to Windows DNS servers on Microsoft Support.

**Native DNS auditing**

DNS auditing was also introduced alongside the analytical DNS logging changes—with Windows Server 2016, or 2012 R2 with hotfix 2956577—and is enabled by default. These audit logs are written to the `Microsoft-Windows-DNS-Server/Audit` log in the Windows EventLog. This is the preferred method for collecting DNS audit logs.

**Debug logging**

For Windows DNS Server versions prior to Windows Server 2012 R2, or on 2012 R2 without hotfix
2956577, “debug logging” can be enabled to record DNS queries and replies to a log file. This type of logging can affect DNS Server performance and is not intended to be enabled permanently. However, without support for analytical logging, DNS debug logging is the only way to collect DNS transaction information from Windows DNS Server. For more information about debug logging, see [Using server debug logging options on Microsoft Docs](#).

**DNS Server debug log sample**

```
4/21/2017 7:52:03 AM 06B0 PACKET 0000000028657F0 UDP Snd 10.2.0.1        6590 R Q
[8081   DR NOERROR] A      (7)example(3)com(0)
```

**Active Directory auditing**

On systems without native DNS auditing (prior to 2012 R2, or 2012 R2 without hotfix 2956577), DNS changes can be audited by enabling AD Directory Services auditing. These events are written to the **Microsoft-Windows-Security-Auditing** log in the Windows EventLog. For more information, see the [AD DS Auditing Step-by-Step Guide](#) on Microsoft Docs and [Who Moved the DNS Cheese? Auditing for AD-Integrated DNS Zone and Record Deletions](#) on Microsoft Tech Community.

**How NXLog Enterprise Edition can help with DNS monitoring**

NXLog Enterprise Edition provides several unique features for collecting and processing DNS logs:

**Native ETW collection**

NXLog includes an `im_etw` input module that implements an ETW consumer. This allows NXLog to collect DNS analytical logs directly from ETW, without requiring events to be first written to disk.

**Parsing of DNS debug logs**

The `xm_msdns` module offers built-in parsing of log messages read from Windows DNS Server debug logging files.

**Multiple types of Windows EventLog collection**

NXLog can be configured to collect Windows EventLog data as a local agent or remotely. NXLog can also use Windows Event Forwarding to collect EventLog data remotely while running on Linux. As a result, there are a variety of options for collecting DNS Server audit logs or Active Directory audit logs from a Windows DNS Server. See the [Windows EventLog](#) chapter in the NXLog User Guide for more details.

**File integrity monitoring**

NXLog can be used to implement several types of checksum-based and real-time file integrity monitoring. This can be used to monitor BIND 9 configuration files or any other system files that are related to DNS. For more information, see [File Integrity Monitoring](#).
Parsing and structured logging

NXLog provides many tools for parsing event messages, and is designed around the concept of structured logging. Log data that is structured at the source can be retained as structured data, reducing the need for further processing. By handling and forwarding logs as structured data, events can be easily filtered, classified, and correlated as required for monitoring. For an introduction to NXLog's handling of event data, see Event Records and Fields.

Output integrations

Once log data has been collected and parsed, the structured data can be forwarded to another NXLog agent for centralized log collection or to a log analytics solution for monitoring and analysis. NXLog offers a range of extension and output modules capable of converting log data and forwarding it to other systems. NXLog supports a variety of SIEM [9] products and many MSSPs [10]. See Integration in the NXLog User Guide.

For more information about using these features to implement DNS logging for specific DNS servers, see the DNS Monitoring chapter in the NXLog User Guide.

NXLog Ltd. develops multi-platform log collection tools that support many different log sources, formats, transports, and integrations. The tools help administrators collect, parse, and forward logs so they can more easily respond to security issues, investigate operational problems, and analyze event data. NXLog distributes the free and open source NXLog Community Edition and offers additional features and support with the NXLog Enterprise Edition.

This document is provided for informational purposes only and is subject to change without notice.

[6] DNSpionage Campaign Targets Middle East, Cisco Talos Intelligence Group, Talos Blog, retrieved 2019-05-14
[8] DDoS attack that disrupted internet was largest of its kind in history, experts say, The Guardian, retrieved 2019-05-14
[9] SIEM: Security information and event management
[10] MSSP: Managed security service provider