DNS Errors and NXDOMAINS

The Security Challenge

Every day, hundreds of billions of Domain Name System (DNS) queries are made as Internet users visit websites. While most queries are successful and return the requested answer, sometimes the DNS request results in a “non-zero” error code, signaling that the specific domain name cannot be resolved successfully.

Suspicious activity is often a factor for these errors, and may indicate brand infringement, misuse of domains to enable malware campaigns or botnet activity. Security teams need fast access to accurate data about DNS errors so they can understand and investigate the reasons for domain names not resolving successfully.

The Farsight Solution

Farsight Security offers two channels in the Farsight Security Information Exchange (SIE) platform to help organizations identify the cause of certain types of errors that prevent successful resolution of domain names: DNS Errors (Channel 220) and NXDOMAINS (Channel 221).

DNS Errors

The DNS Errors channel is a real-time feed of DNS query responses which have a valid or completely absent checksum and a non-zero response code. These include NXDOMAIN, SERVFAIL, REFUSED, and other DNS error codes.

The DNS Errors channel provides:

+ Visibility into global SERVFAIL and REFUSED messages that are otherwise difficult to obtain for monitoring name servers. Network managers can determine when the name servers under their responsibility are causing problems in real-time.

+ The ability for security analysts to monitor for indications that DNS response policy zones (RPZ) or other “DNS firewall” technologies are in selective use; since those methods normally result in error conditions being returned locally for names that are actually currently defined.

“Farsight’s error channels enable valuable dumpster-diving for intelligence on my domains.”

Information Security Manager,
National Financial Institution

sales@farsightsecurity.com • +1-650-489-7919 • www.farsightsecurity.com
**NXDOMAINS**

The NXDOMAINS channel is derived from the DNS Errors channel and consists solely of query traffic receiving a DNS RCODE=3 (NXDOMAIN).

The NXDOMAINS channel provides:

+ The ability to empirically characterize user mistakes and identify potentially valuable brand protection opportunities with similar domain names.
+ Identification of unregistered Web Proxy Autodiscovery (WPAD) Protocol servers for security teams to address.

**Benefits**

Together, the DNS Errors channel and NXDOMAINS channel offer organizations the following capabilities:

**Operational Monitoring**

An easy way to monitor domain names for unexpected errors - including those due to authoritative name server problems.

**Brand Protection**

Brand infringement campaigns often begin with DNS reconnaissance with malicious actors probing for unregistered domain names similar to those of targeted brands. Watching NXDOMAIN traffic is a simple way to detect the emergence of these campaigns.

**Domain Protection**

Security-conscious organizations often register commonly misspelled variations of their domain names to prevent cybercriminals from registering those domains and employing them in malware campaigns. The NXDOMAINS channel delivers a real-time view of misspelled variations of domain names so organizations can move quickly to register them before malicious actors do.

**Detection of Botnets and Domain Generation Algorithms (DGAs)**

Botmasters have avoided takedowns by coding and deploying DGAs. Through this approach, botnet-infected systems will attempt and fail to resolve a large number of random-appearing domain names. The DNS Errors and NXDOMAINS channels give threat analysts and security researchers visibility into DGA-related DNS traffic.

---

**How to Subscribe**

For more information, contact sales@farsightsecurity.com or call +1-650-489-7919.

**About Farsight Security**

Farsight Security provides the world’s largest real-time actionable threat intelligence on changes to the Internet. Leveraging proprietary technology with more than 200,000 observations/second, Farsight provides security teams with the Internet’s view of an organization’s presence and how it is changing - whether purposely, inadvertently or maliciously. The world’s most security-conscious organizations use Farsight threat intelligence to protect their users and infrastructure.