Newly Active Domains (NAD)

The Security Challenge

Domains that were once live on the Internet and then abandoned are often purchased and reused by criminals in order to avoid immediate detection. The reuse of abandoned domains, that may have a good or neutral reputation/spam score, dramatically increase the probability of successfully delivering their intended criminal activities such as spam, malware distribution or botnets until spam and reputation engines get updated after a period of time.

Security teams need real-time information about domains that are reactivated on the Internet after a period of inactivity. With this information, security teams can apply rules to firewalls and mail servers to block inbound and outbound connections to these domains until more information is available about them.

The Farsight Solution

Farsight's Newly Active Domains (NAD) solution is a real-time data feed of domains that have become active after a period of inactivity (offline) for a period of at least ten (10) days. This data is very useful to detect and block domains used by threat actors who are patient enough to establish a harmless reputation for domain-name assets before use or reusing expired/abandoned domains that may have previously good reputations.

Farsight NAD leverages our real-time Passive DNS sensor array and cross-references that data with our industry leading DNSDB® historical DNS database.

Benefits

- **Phishing Protection**
  Reused domains are often used for malicious activity such as phishing attacks. Reactivated domains are especially dangerous because they may have positive or neutral reputations which greatly increases the probability of successfully bypassing existing spam and reputation services.

- **Malware Obstruction**
  Block any connections to newly active domains by leveraging NAD Response Policy Zones on DNS Servers; thus, disrupting techniques commonly used by modern malware.

- **Spam Filtering**
  Filter email of newly active domains by adding SpamAssassin rules that readily consume this DNSBL. Most email coming from reactivated domains is malicious and it’s good practice to protect users from these messages.
Protection from Newly Active Domains after a Period of Inactivity

Farsight observes millions of domains each day and detects that more than 100,000 of those are newly configured from the perspective of the historical DNSDB database. Leveraging more than 5TB of daily real-time Passive DNS data, Farsight NAD discovers newly reactivated domains that were inactive for at least ten (10) days.

Farsight NAD is available as a real-time stream aimed at blocking malware, phishing, and spam that leverage rapid domain reuse. It is delivered in a range of exclusion lists directly to recursive name servers, DNS firewall and email servers of your enterprise.

Delivery methods:
- RPZ - Response Policy Zone
- RBL - Real-time Block Lists
- RSYNC - Remote Sync
- NMSG - Network Messages
- BATCH - Batch Download via API or UI

Newly Active Domains
Provides Early Protection

Farsight NAD recognizes as soon as the domain is live again

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

About Farsight Security
Farsight Security is the world’s largest provider of historic and real-time DNS intelligence data. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Learn more about how we can empower your threat platform and security team with Farsight Security DNS intelligence solutions.