Newly Observed Domains (NOD)

The Security Challenge

New domains are created and published every day as part of the Domain Name System (DNS) – but not all of them are created for legitimate purposes. Bad actors use new domains for criminal activities such as spam, malware distribution or botnets within the first minutes of creating them.

Security teams need real-time information about new domains so they can apply rules to firewalls and mail servers to block access to those domains until the security community has time to better understand them. Security analysts don’t have a way to gather and analyze information about new domains in real-time or in a timely manner because this domain information is broadly distributed across name servers around the world.

The Farsight Solution

Farsight’s Newly Observed Domains (NOD) solution provides organizations with real-time actionable insights based on the newness of a domain. This enables them to protect their users from newly configured and used domains until those domains are better understood by the rest of the security industry such as spam filters and reputation providers— thereby materially improving their risk profile.

NOD leverages Farsight’s real-time Passive DNS sensor array and cross-references that data with its industry-leading DNSDB™ historical Passive DNS database.

Benefits

+ **Malware Obstruction**
  Block outbound connections to newly used domains by leveraging NOD Response Policy Zones on DNS Servers; thus, disrupting techniques commonly used by modern malware.

+ **Brand Protection**
  Take immediate action in case of suspected brand phishing, confusion or dilution when new names are detected. New domains are often used to trick users by creating a lookalike site. These domains are dangerous until they are classified and blocked. They can be blocked for periods of time by leveraging NOD Response Policy Zones on DNS Servers.

+ **Spam Filtering**
  Filter email of very young domains (e.g., five minutes old or newer, 30 minutes old or newer, etc.) by adding SpamAssassin rules that readily consume this DNSBL. Most email coming from new, look-alike domains can be malicious. It’s good practice to protect users from these messages.

“Farsight’s NOD protected, on average, each of my users at least once a day.”

**CISO**
35,000-student U.S.-based university

sales@farsightsecurity.com · +1-650-489-7919 · www.farsightsecurity.com
Protection from Unknown Domains

Farsight observes millions of domains each day and detects that more than 100,000 of those as newly configured from the perspective of the historical DNSDB database. Leveraging more than 5TB of daily real-time Passive DNS data, NOD discovers newly configured domains when they are first used/resolved. This is a great contrast to the typical 17 hours after first use with other discovery methods such as TLD Zone File Access, spam filters or WHOIS.

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

The NOD Solution can be consumed in real-time using:

- RPZ - Response Policy Zone
- RBL - Real-time Black Lists
- RSYNC - Remote Sync
- NMSG - Network Messages

This provides network security managers with the ability to block connections to domains based on their age such as those that are less than 3 minutes old to be blocked for the first 24 to 48 hours.

Attacking are opportunistic and will remain active as long as they can operate undetected: According to a January 2016 Ponemon Institute Survey, 37 percent of attackers quit if they can't yield value after a delay of 10 hours.

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.