Newly Observed Hostnames (NOH)

The Security Challenge

Millions of hostnames are created every day as part of the Domain Name System (DNS). Often, bad actors use hostnames to impersonate other organizations.

Security teams need to know when new hostnames are put into use in real-time. Unfortunately, this insight is not readily available because it is broadly distributed across many recursive and authoritative name servers around the world.

The Farsight Solution

Farsight’s Newly Observed Hostnames (NOH) solution provides organizations with visibility of new hostnames or Fully Qualified Domain Names (FQDNs) – when they are first active. Using NOH, security teams can leverage real-time, actionable insights based on new hostnames that target their domains as well as their partners; thus ensuring end-to-end security.

NOH provides security teams the following capabilities:

- **Phishing and brand protection**
  Organizations can watch for and discover infringing domains and phishing hostnames targeting their users and partners.

- **Unexpected DNS additions**
  By monitoring the DNS worldwide, organizations can see newly added websites in their own domains. They can also learn about unexpected DNS changes within minutes; allowing for quick action and investigation.

- **Situational awareness for sensitive environments**
  Organizations often have internal hosts that should never be accessed from the Internet. Security teams can know when someone, either internal or external, is attempting to resolve these hosts.

- **Penetration test assistance**
  Internal and external penetration testers can use this feed of new systems and hosts for legitimate pen testing engagements.

“Farsight’s NOH is very valuable for malware discovery.”

Senior Security Analyst, Fortune 500 Investment Manager
Newly Observed Hostnames

Benefits

- Discover the existence of new hostnames within minutes of when they are first resolved.
- Identify “wildcarded” and uniquely tagged hostnames, which are often used in phishing attempts or to evade domain name-focused investigations.
- Monitor potentially infringing websites (e.g., rolex.acme.com, prada-sale.acme.biz).
- Detect potentially malicious websites used in phishing attacks targeting the organization or its customers (e.g., lloydsbank.co.uk, www.beatsbydrewholesale.com).
- Discover “domain shadowing” — when adversaries hijack legitimate domains to create subdomains to distribute malicious content (e.g., apple.hackedsite.com, paypal.secureserver.hackedsite.com).

Newly Observed Hostnames Discovered in Real Time

NOH leverages more than 5 TB of real-time Passive DNS data to detect hundreds of millions of hostnames per day. Farsight validates that more than 25 million of those hostnames are newly configured from the perspective of the historical DNSDB database.

NOH is available in the following formats: nmsg, CSV.

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.