OpenDNS

OpenDNS is now part of Cisco.

The Sound of a New Frontier: OpenDNS Data Scientists Create a 'Sonar' System for Network Security

Data science is at the heart of a new era of enterprise security innovation, with developments in artificial intelligence leading the way. **OpenDNS Security Labs researchers are inventing new models to discover malicious attacks before they happen.**

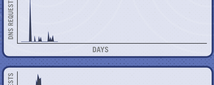
SPRank EXPLAINED: WHAT'S A SECURITY MODEL?

Using advanced data science, combined with security industry expertise, OpenDNS researchers have created a set of operations called algorithms to analyze large datasets. These algorithms, also known as models, automate the process of threat discovery and predicting malicious attacks.

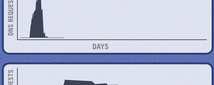
Spike Rank (SPRank) is a detection model that uses mathematical concepts more commonly used to analyze sound waves in real time — similar to how Pandora or Shazam analyze music. Instead of sound waves in a song, the model tracks patterns in network traffic, and listens for categorized malicious attack patterns. It functions like a sonar for security threats.

WHAT DOES AN ATTACK PATTERN SOUND LIKE?

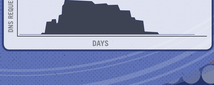
EXPLOIT KITS: A server-based toolkit used to automate attacks by targeting clientside vulnerabilities in browsers and other software.



DGA: Domains created by algorithms and used as command and control servers for botnets or malware.



DDoS: A domain targeted in a Denial of Service attack by one or more web servers.



HOW EFFECTIVE IS THIS MODEL?

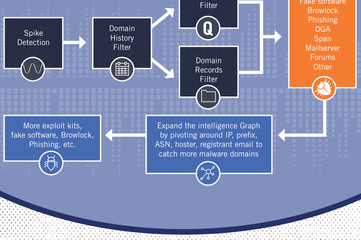
On average, only **16%** of security vendors catch the domains identified by SPRank

Of the **200** domains observed in a one hour period, **70** of the compromised domains had not been identified by any other vendor

SPRank has a **100%** success rate of discovering malicious domains before other security vendors (tested hourly against VirusTotal).

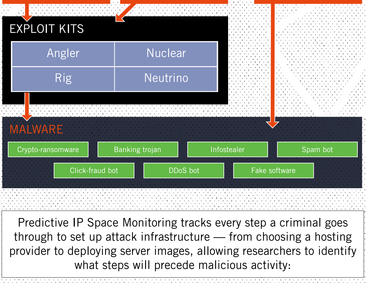
HOW DOES SPRank WORK?

SPRank analyzes worldwide Internet traffic for clues that indicate an attack is in progress.



DETECTING HACKER INFRASTRUCTURE

Another model developed by the OpenDNS Security Labs is Predictive IP Space Monitoring. Integrating 'clues' found by SPRank, this model categorizes patterns in malicious hosts to determine which domains will be the source of future malicious activity.



Predictive IP Space Monitoring tracks every step a criminal goes through to set up attack infrastructure — from choosing a hosting provider to deploying server images, allowing researchers to identify what steps will precede malicious activity:

HOW EFFECTIVE IS THIS MODEL?

For every **1** malicious domain identified by SPRank, Predictive IP Space Monitoring predicted **340** additional domains

Predictive IP Space Monitoring also uncovers the use of a criminal tactic called **Domain Shadowing**

Domain Shadowing uses a compromised subdomain of a legitimate website (e.g., "bad.opendns.com" instead of "opendns.com") as the base for launching an attack.

OpenDNS

OpenDNS is now part of Cisco.

FIND OUT MORE

To learn more about these security models and OpenDNS's research, read our Security Labs blog and follow us on Twitter **@OpenDNSLabs**.