Zero-hour Protection Against Newly Observed Domains with Infoblox and Farsight

PARTNER SOLUTION BRIEF

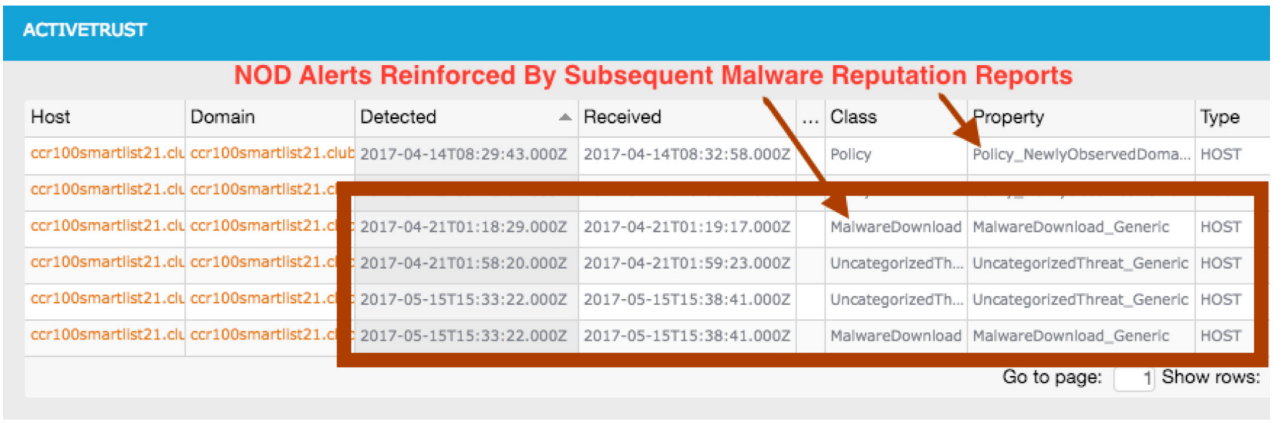
Overview

All organizations carry an inherently elevated level of exposure to attacks originating from new domains, and historically, a significant percentage of newly observed domains engage in malicious activity - either receiving exfiltrated content from previously injected malware or serving up phishing or malware-laden spam. Through integration with Infoblox Threat Intelligence Data Exchange (TIDE), Farsight Security's Newly Observed Domains (NOD) data service continuously alerts Infoblox ActiveTrust® platform users to the first-observed presence of domains in DNS.

Infoblox ActiveTrust technology allows customers to proactively detect, investigate, prioritize and protect against cyber threats. Infoblox ActiveTrust offerings bundle Infoblox DNS Firewall, Threat Insight in the Cloud, Infoblox Threat Intelligence Data Exchange (TIDE) and Infoblox Dossier® search tool. The solution enables organizations to prevent malware C&C communications and data exfiltration via DNS, centrally aggregate curated internal and external threat intelligence, distribute validated threat data to the customer's existing security infrastructure and enable rapid investigation to identify context and prioritize threats. ActiveTrust offerings are available in three tiers: ActiveTrust Standard includes just the DNS Firewall, Threat Insight in the Cloud, TIDE and Dossier.

Farsight's NOD feed identifies an average of 150,000 new domains each day, typically within 60 seconds of first appearance in the global DNS. Streamed at 1 Gb/second, Farsight NOD data is formatted to be ingested directly by the Infoblox TIDE platform, or queried directly for investigative purposes through Infoblox's Dossier service. By subscribing to Farsight Newly Observed Domains via TIDE, ActiveTrust Plus and Advanced customers benefit from a real-time incremental layer of defense to combat malware exfiltration, brand abuse, and spam-based attacks which originate or terminate at newly-launched domains.

Infoblox-Farsight Security Joint Solution



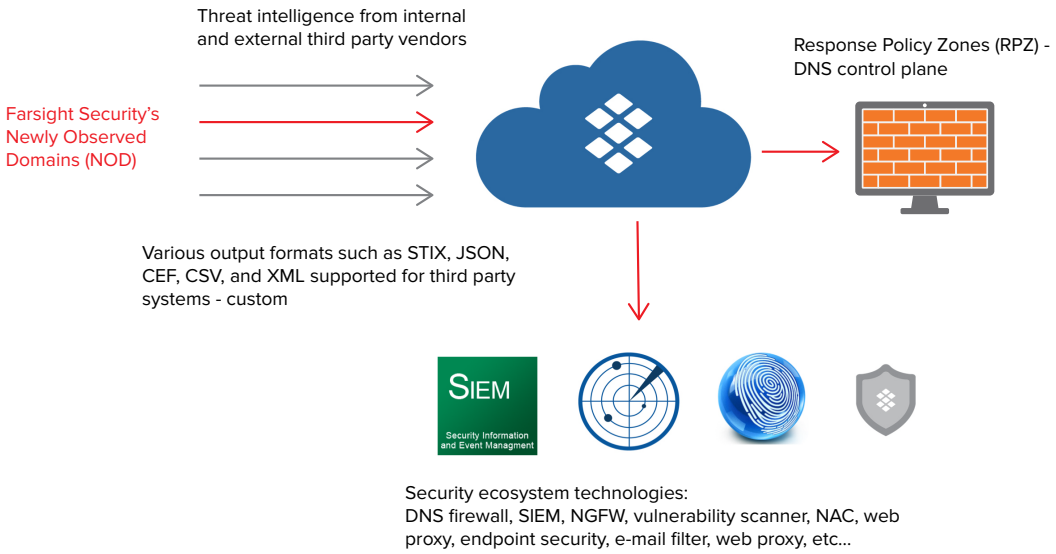
In the screen above, Farsight NOD identifies an average of 150,000 newly-active domains each day, continuously streaming sightings to the Infoblox TIDE platform (within ActiveTrust) enabling defensive blocking to be invoked. Then Infoblox's Dossier service can be leveraged for rapid threat investigation to trace the origin and relationship with other confirmed threat activity such as malware reputation reports signaling to ActiveTrust users whether the NODs are malicious (e.g. being used to distribute malware) or not.

Infoblox
CONTROL YOUR NETWORK

Zero-hour Protection Against Newly Observed Domains with Infoblox and Farsight

PARTNER SOLUTION BRIEF

How it Works – Infoblox TIDE and Farsight Security NOD



Background

Refusing traffic from all domains new to DNS for a brief period of time may sound excessive, but the tactic has been proven extremely effective in defending against quick strike attacks. The vast majority of entities operating reputable domains have no need to deliver email or serve web pages immediately after registering and activating a new domain. Threat actors however routinely exploit this short-lived window of opportunity to launch attacks from burner sites in the critical hours before reputation services can establish awareness and compute threat scores. Farsight Security has consistently found that when a network blocks the newest of new domains, even for a brief period of time - from a few minutes up to 24 hours - nothing of value is lost but much is gained in the way of security.

Challenges

1. Security analysts don't have a way to gather and analyze newly active domain information in a timely or practical manner because it is broadly distributed across name servers around the world.
2. Newly registered domain data is not a reliable predictor of impending attack as some threat actors register domains in bulk then park them for extended periods of time.
3. Reliance on top-level domain (TLD) zone files to block new domain-based attacks is prone to significant visibility and time gaps because not all TLDs offer ZFA (e.g. .EDU and .EU domains) and some registries only make new zone files available periodically during the day.

Infoblox
CONTROL YOUR NETWORK

Zero-hour Protection Against Newly Observed Domains with Infoblox and Farsight

PARTNER SOLUTION BRIEF

Key Capabilities

1. **Speed and Accuracy.** With multiple NOD offerings in the market, the operative question in evaluating which will provide the most comprehensive and accurate data set is "newly observed versus what?" Farsight operates the industry's most extensive global sensor array balanced across geographies, TLDs, and industries. Capturing in excess of 200,000 DNS observations/second and streaming at 1Gb/sec, domain observations are filtered against Farsight's proprietary passive DNS database, the most expansive historical pDNS database available containing > 100B DNS resolutions.
2. Apply threat intel data (NOD) in RPZ format at the DNS control plane, preventing malware communications with C&C sites and data exfiltration
3. **Enhance Security Infrastructure.** Distribute Farsight NOD information via ActiveTrust TIDE portal in various formats such as JSON, XML, CEF, CSV, and STIX to enhance existing security ecosystems such as next generation firewalls, IPS, web proxies, and SIEMs.

Joint Solution Benefits

1. **Malware Containment.** Protect against malware infection and exfiltration of intellectual property by blocking outbound connections to NODs at the DNS control plane. NOD information is made available via Infoblox TIDE in various formats for third party security vendors to take action.
2. **Brand protection.** Take immediate action in case of suspected brand phishing, confusion or dilution when NODs 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.
3. **Enhanced SPAM Filtering.** NOD coverage is focused and unique. It doesn't target the ~90+% of inbound SPAM caught by standard anti-spam solutions, but rather what they miss due to the newness of the attack source domain. With a half-life typically under 24 hours, NOD also complements and enhances the effectiveness of greylisting techniques without contributing to collateral damage.
4. **Rapid threat investigation.** Leverage Infoblox Dossier service to gain threat context to NODs when researching suspicious domains. For example, investigating a Farsight NOD using Dossier service could lead to organizations that have determined this NOD to be malicious thus providing the context and priority necessary to block it immediately.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com