SOLUTION NOTE

PROTECTION AGAINST NEWLY OBSERVED DOMAINS WITH INFOBLOX AND DOMAINTOOLS

OVERVIEW

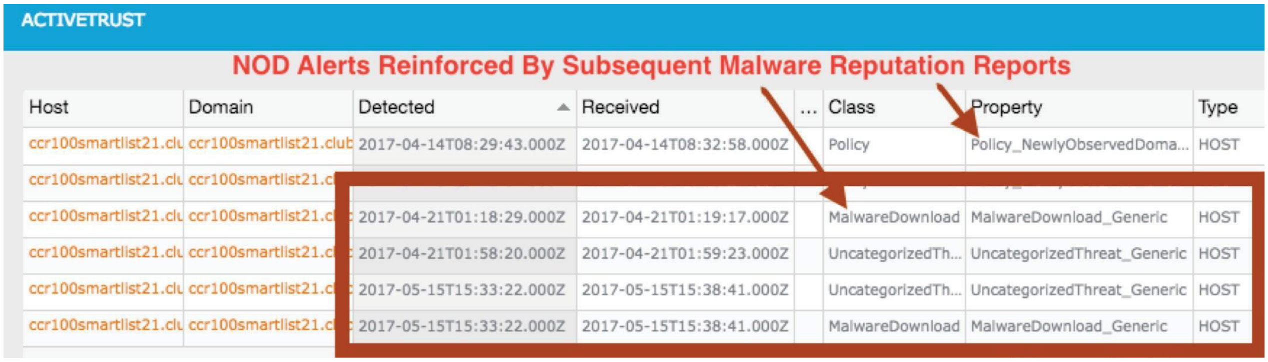
All organizations carry an inherently elevated level of exposure to attacks originating from new domains, and historically, a significant percentage of bad actors utilize newly observed domains to engage in malicious activity – serving up phishing or malware-laden websites, delivering spam, or even used as part of a malware'scommand-and-control (C2) infrastructure.

Through integration with Infoblox Threat Intelligence Data Exchange (TIDE), part of BloxOne® Threat Defense, the Farsight Newly Observed Domains (NOD) data service continuously alerts Infoblox BloxOne Threat Defense platform users to the first-observed presence of domains in DNS.

BloxOne Threat Defense strengthens and optimizes an organization's security posture from the foundation up. It uses a hybrid architecture for pervasive, inside-out protection against today's advanced malware threats, data exfiltration, lookalike domain threats, DGAs and more. The solution also powers security orchestration, automation and response (SOAR) solutions by providing rich network and threat context, optimizes the performance of the entire security ecosystem and reduces the total cost of enterprise threat defense.

The Farsight NOD Feed typically identifies over 200,000 new domains each day, typically within 60 seconds of first appearance in the global DNS. Streamed in near-real-time, 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, part of BloxOne Threat Defense. By subscribing to Farsight NOD via TIDE, BloxOne Threat Defense 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

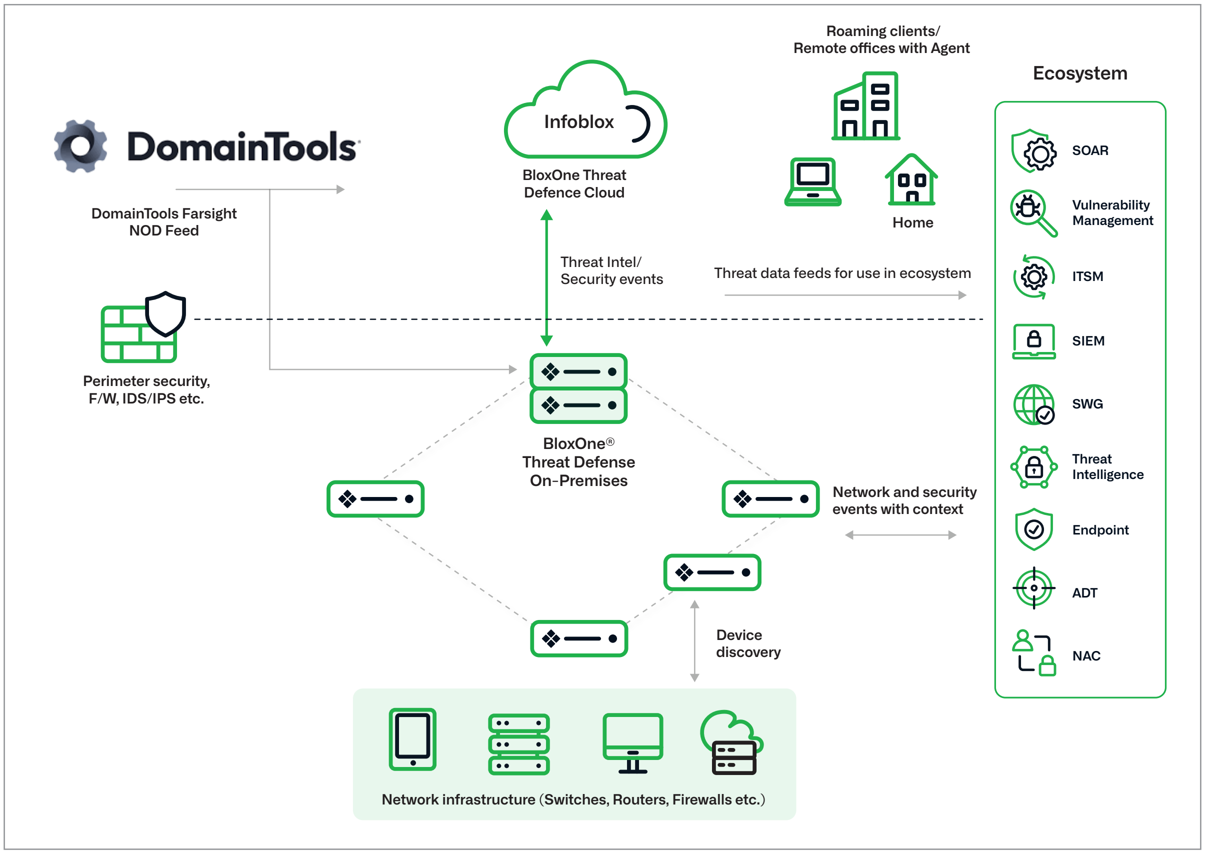


ACTIVETRUST

NOD Alerts Reinforced By Subsequent Malware Reputation Reports

Host	Domain	Detected	Received	...	Class	Property	Type
ccr100smartlist21.clu	ccr100smartlist21.club	2017-04-14T08:29:43.000Z	2017-04-14T08:32:58.000Z		Policy	Policy_NewlyObservedDoma...	HOST
ccr100smartlist21.clu	ccr100smartlist21.cl						
ccr100smartlist21.clu	ccr100smartlist21.cl	2017-04-21T01:18:29.000Z	2017-04-21T01:19:17.000Z		MalwareDownload	MalwareDownload_Generic	HOST
ccr100smartlist21.clu	ccr100smartlist21.cl	2017-04-21T01:58:20.000Z	2017-04-21T01:59:23.000Z		UncategorizedTh...	UncategorizedThreat_Generic	HOST
ccr100smartlist21.clu	ccr100smartlist21.cl	2017-05-15T15:33:22.000Z	2017-05-15T15:38:41.000Z		UncategorizedTh...	UncategorizedThreat_Generic	HOST
ccr100smartlist21.clu	ccr100smartlist21.cl	2017-05-15T15:33:22.000Z	2017-05-15T15:38:41.000Z		MalwareDownload	MalwareDownload_Generic	HOST

In the screen above, Farsight NOD is continuously streaming sightings to the Infoblox TIDE platform 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 BloxOne Threat Defense users whether the NODs are malicious (e.g. being used to distribute malware) or not.


DomainTools
DomainTools Farsight NOD Feed
Perimeter security, F/W, IDS/IPS etc.
Infoblox
BloxOne Threat Defence Cloud
Threat Intel/ Security events
BloxOne® Threat Defense On-Premises
Roaming clients/ Remote offices with Agent
Home
Threat data feeds for use in ecosystem
Network and security events with context
Device discovery
Network infrastructure (Switches, Routers, Firewalls etc.)
Ecosystem
SOAR
Vulnerability Management
ITSM
SIEM
SWG
Threat Intelligence
Endpoint
ADT
NAC

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 always 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.

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 500,000 DNS observations/second, domain observations are filtered against Farsight’s proprietary passive DNS database, the most expansive historical pDNS database available, containing over 35 billion DNS resolutions.
2. **Enhance Security Ecosystems.** Distribute Farsight NOD information via BloxOne Threat Defense TIDE portal with DNS RPZ or in other various formats 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. NOD information is made available via the TIDE platform in various formats for third party security vendors to take action.
2. **Brand protection.** New domains are often used to trick users by impersonating known brands and hosting lookalike websites. 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. Farsight 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.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20231025v1