Infoblox
CONTROL YOUR NETWORK

Infoblox Threat Intelligence Feed for Infoblox DNS Firewall

OVERVIEW

Infoblox DNS Firewall is the leading DNS-based network security solution that helps businesses contain and control malware that uses DNS to communicate with command and control servers (C&Cs) and botnets. DNS Firewall proactively detects infections and blocks malware communications, effectively stopping them in their tracks and preventing data theft. It works by employing DNS Response Policy Zones (RPZs) timely threat intelligence, and the optional Infoblox Threat Insight to prevent data exfiltration (behavioral approach). This document explains the threat intelligence offered by Infoblox, called Infoblox Threat Intelligence Feed.

Sources

Infoblox's automated threat intelligence feed is designed to keep DNS Firewall updated on new and evolving malicious hostnames. The Infoblox threat intelligence feed uses over 300 distinct classifications to help provide context and insight on threats:

- Top malicious hostnames with which devices attempted to communicate
- Detailed threat information to enable operators to quickly understand the nature of the threat they are experiencing

This comprehensive intelligence of observed and verified hostnames known to be used by cybercriminals is leveraged by DNS Firewall (via automatic updates to its RPZ policy) to enforce policies set by the user to block unwanted IP communications. The sources of threat intelligence are reviewed, the data correlated, and whitelists applied to minimize false positives.

Policy Enforcement

Infoblox provides multiple feed types (sets of blacklists of hostnames) that can be applied to the RPZ policy.

1. **Base feed** – enables protection against known malicious threats that are dangerous as destinations.
2. **Malware feed** – enables protection against known malicious threats that can take action/control of your system.
3. **Ransomware feed** – enables protection against ransomware that restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying.
4. **Bogon feed** – enables protection against bogons, which are commonly found as the source addresses of DDoS attacks. Many ISPs and end-user firewalls filter and block bogons, because they have no legitimate use, and usually are the result of accidental or malicious misconfiguration.

Out-of-the-box Blacklists

Examples of sources of threat intelligence available using the **Base feed** include:

- APT (Advanced Persistent Threat) – set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity; purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period.
- Compromised Host/Domain – compromised host is a computer connected to the Internet that has been compromised by a hacker, computer virus, or Trojan horse and can be used to perform malicious tasks of one sort or another under remote direction; compromised domain refers to a DNS server being compromised by a hacker.
- Exploit Kits – Software kits designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with the kits, and discovering and exploiting vulnerabilities to upload and execute malicious code on the client.
- Malicious Name Server – compromised or malicious DNS servers; this may cause inaccurate DNS responses for the domain requested (e.g., the client is sent to a phishing site or served malicious code).
- Sinkholes – list of servers that are used by malware researchers and law enforcement organizations to sinkhole botnets that have been taken down.

Infoblox
CONTROL YOUR NETWORK

Infoblox Threat Intelligence Feed for Infoblox DNS Firewall

OVERVIEW

Examples of sources of threat intelligence available using the **Malware feed** include:

- Malware C2 – Command and Control servers are used by attackers to maintain communications with compromised systems within a target network.
- Malware Download – domains used for malicious software download execution aka, “drive-by-downloads”.
- Phishing – domains used in phishing attacks.

Examples of sources of threat intelligence available using the **Ransomware feed** include:

- Ransomware Locky – when installed on a victim system, it encrypts victims’ personal files and the file names turn into a sequence of numbers and characters followed by the .Locky extension. The compromised user has to pay to have the files decrypted.
- Ransomware CryptoLocker – when installed on a victim system, it encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware’s control servers. The malware then displays a message which offers to decrypt the data if a payment is made by a stated deadline, and threatens to delete the private key if the deadline passes.
- Ransomware Dircrypt – when installed on a victim system, Dircrypt sweeps through files, targeting documents, images and archive files. The suffix of the affected files is changed to ‘.enc.rtf’. Upon clicking on a file, instead of its original contents, an RTF document opens with instructions on how to pay the ransom.
- Ransomware CryptoWall – when installed on a victim system, it encrypts a wide variety of files using public/private key encryption with a strong 2048-bit RSA key. It then asks the user to pay to have the files decrypted.

Examples of sources of threat intelligence available using the **Bogon feed** include:

- Bogon IPs – Bogus IP addresses from the Bogon space, which is a set of IP addresses not yet officially assigned to any entity by the Internet Assigned Number Authority (IANA) or a regional Internet registration institute. Bogon space IP addresses are not normally visible over the Internet or on any computer network, but they are still exploited, mostly for illegal or fraudulent activities. Hackers manipulate the source IP address to a Bogon IP, giving the receiver the impression that the packet is arriving from a reliable source.

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

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