Infoblox
CONTROL YOUR NETWORK

Q1 2016 INFOBLOX SECURITY ASSESSMENT REPORT

Introduction

Infoblox, an industry leader in securing Domain Name System (DNS) infrastructure, delivers advanced technologies that prevent DNS-based data exfiltration; disrupt advanced persistent threat (APT) and malware communications; and provide context around attacks and infections on the network.

To help our customers and prospective customers discover whether their organizations have been exposed to malicious DNS-based activity, Infoblox offers free security assessments. These assessments identify DNS queries inside an organization's network that are attempting to reach known malicious or suspicious domains. External threat data from these assessments is anonymized and aggregated to create the Infoblox Security Assessment Report. For details, see the Methodology section below.

DNS is a unique and ubiquitous protocol, and can also be a powerful enforcement point within the network. When suspicious DNS activity is detected, network administrators and security teams can use this information to quickly identify and remediate infected devices—and can use DNS firewalling as well to prevent malware inside the network from communicating with command-and-control servers or exfiltrating data.

Results

In the first quarter of 2016, **519** files capturing DNS traffic were uploaded by **235** customers and prospects for security assessments by Infoblox. The results: **83%** of all files uploaded showed evidence of suspicious activity (429 files).

Evidence of the following specific threats was identified in the uploaded files:

Botnets – 54% (280 files)
A botnet is a set of infected computers communicating with each other and working together to either spread malware or participate in denial-of-service attacks. They can use command-and-control/ peer-to-peer communication to achieve their goals.

Protocol anomalies – 54% (282 files)
Protocol anomalies are malformed DNS packets, including unexpected header and payload values, sent to a targeted server. They make use of software bugs in protocol parsing and processing implementation. The server stops responding by going into an infinite loop, or crashes.

DNS tunneling – 18% (93 files)
DNS tunneling enables cybercriminals to insert malware or pass stolen information through DNS, thereby using DNS as a covert communication channel to bypass firewalls. Service providers have seen this technique being used to evade billing systems, impacting their revenues. While there are legitimate uses of DNS tunneling, many instances of tunneling are malicious. There are several off-the-shelf tunneling toolkits readily available on the Internet.

ZeuS – 17% (87 files)
ZeuS is malware designed to capture keystrokes and/or grab web forms on the infected device to steal user credentials such as banking information. The stolen information can then be used to divert funds to criminal accounts. Zeus has been used to create peer-to-peer botnets and to drop in malware such Cryptolocker. ZeuS is very difficult to track due to its stealthy nature, and uses DNS to communicate with command-and-control servers and avoid detection by firewalls.

DDoS – 15% (80 files)
Distributed-denial-of-service (DDoS) attacks use hundreds or even thousands of hosts to flood a target with traffic, such as DNS requests, with a goal of knocking the targeted site offline. Some DNS-based DDoS attacks use "phantom domains" to either keep a DNS resolver engaged by making it wait for responses or by sending random packets. The DNS resolver consumes valuable resources while waiting for valid responses, leading to poor or no response to legitimate queries.

CryptoLocker – 13% (69 files)
Cryptolocker is a form of "ransomware" that primarily targets Windows-based computers. It can be spread via email where the attached malware is disguised as a PDF or voice-mail audio file. It can also be downloaded by Trojans that are already present in an infected device. Once the malware is on a machine, Cryptolocker encrypts files on the local hard drive or mapped network drives by getting an encryption key from an Internet-based server. The user is then asked to pay a ransom to retrieve the data. One way to stop CryptoLocker is by blocking access to the encryption servers by preventing DNS queries to them.

Amplification and reflection – 12% (63 files)
Reflection attacks use one or more third-party DNS servers, usually open resolvers on the Internet, to propagate a DDoS attack on the victim's server. The attacker spoofs the DNS queries he sends to open resolvers by including the victim's IP address as the source IP. The resolvers send all responses to the victim's server, thereby overwhelming it and potentially creating a denial of service. Amplification is an attack where the queries are specially crafted to result in a very large response. Cybercriminals typically use a combination of amplification and reflection to maximize impact on the victim server.

Heartbleed – 11% (55 files)
Heartbleed is a security vulnerability discovered in April 2014 in certain versions of OpenSSL that has a severe memory-handling defect. This defect can be exploited by attackers to read the memory of systems, allowing for theft of users' session cookies and passwords.

Methodology

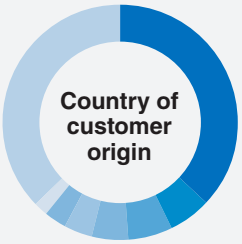
Participants in Infoblox security assessments submit a packet capture (PCAP) file containing recent DNS traffic on their networks. The uploaded PCAP files are then run through the Infoblox DNS Firewall and Infoblox Advanced DNS Protection products to flag suspicious activity.

Suspicious activity is an indicator of a specific threat being present on the network. In some cases, these indicators could be false positives or could point to activity that is already contained by the network's existing security solutions.

The results of each security assessment are listed in a document that is sent to the participant. The Infoblox Security Assessment Report anonymizes and aggregates these individual security assessments to show the extent of suspicious DNS activity across a diverse range of organizations.

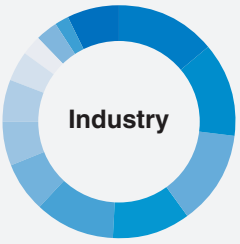
Organizations seeking a free Infoblox security assessment should visit www.infoblox.com/free-malware-report. More information on Infoblox security solutions is available at www.infoblox.com/security.

Demographics



37% United States
6% Mexico
6% Spain
5% France
4% Canada
3% Germany
2% United Kingdom
37% Other

19% 10,000 or more
18% 5,000 to 10,000
21% 2,000 to 5,000
22% 1,000 to 2,000
20% Under 1,000



14% Education
13% Financial services
13% Healthcare
11% Government
11% Telecommunications service provider
7% Manufacturing
6% Information technology
6% Transportation
4% Media and entertainment
3% Hospitality
3% Retail
2% Construction
7% Other

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of networks around the world. As the industry leader in DNS, DHCP, and IP address management, known as DDI, Infoblox reduces the risk and complexity of networking, lowers costs, and increases uptime. Our Infoblox Grid™ ensures availability and provides authoritative data, and Secure DNS solutions defend against a wider range of threats than any other product.

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