DNS: A Unique and Powerful Defense against Advanced Persistent Threats

Infoblox
CONTROL YOUR NETWORK

FireEye

DNS Firewall integration with FireEye NX Series appliance using the FireEye Multi-Vector Virtual Execution (MVX) engine delivers a unique and powerful defense against advanced persistent threats (APTs) for business networks. This solution combines the power of FireEye APT detection and Infoblox DNS-level blocking and device fingerprinting to detect and disrupt APT malware communication and help pinpoint infected devices attempting to access malicious domains. This is the first solution in the marketplace that invokes powerful DNS-level control of FireEye APT detection events.

Background

In 2015, there were over 750 successful breaches with nearly 178 million records exposed (Identity Theft Resource Center, December 2015), costing businesses millions of dollars in remediation costs and infrastructure changes. Why? In 60 percent of cases, attackers can compromise an organization within minutes. And the proportion of breaches discovered within days falls well below that of time to compromise (Verizon 2015 Data Breach Investigations Report).

In July 2014, JPMorgan Chase discovered a breach of its systems that exposed the contact information of nearly 80 million consumers and 7 million small businesses. This data breach is considered one of the most serious intrusions into an American corporation's information system and one of the largest data breaches in history. One year later, U.S. and Israeli authorities arrested four people in Israel and Florida in connection with several fraud schemes tied to this breach. The average cost paid for each lost or stolen record containing sensitive and confidential information has increased from $145 in 2014 to $154 in 2015 (Ponemon 2015 Cost of Data Breach Study: Global Analysis). Integration of Infoblox DNS Firewall with FireEye NX Series can help organizations leverage DNS, a powerful and ubiquitous enforcement point, for defending against APT malware and helping prevent data exfiltration.

Challenges

APTs commonly target organizations with large amounts of sensitive information such as source code, industrial designs, trade secrets, and personally identifiable information—information that helps attackers gain a competitive and monetary advantage. Cybercrime has become a major threat to companies and financial institutions.

DNS is increasingly being used as a pathway for data exfiltration either unwittingly by malware-infected devices or intentionally by malicious insiders. According to an article in SC Magazine, a DNS security survey of 300 IT decision-makers in the U.S. and U.K. in November 2014 showed that 46 percent of respondents experienced DNS exfiltration.

Moreover, many companies have hundreds of employees, each with a minimum of two company-issued devices such as a laptop and cellphone, and each using another two or three personal devices such as a smartphone and tablet in the office, which makes finding and cleaning up APT malware time consuming and difficult.

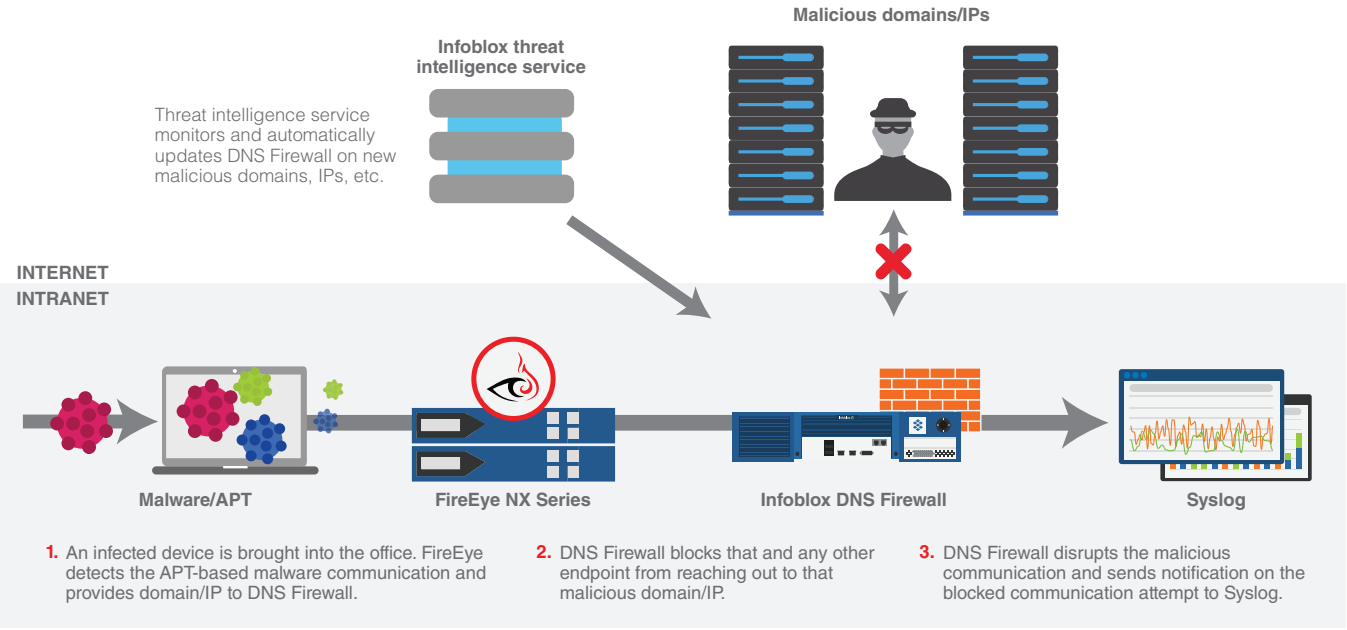
Solution

Infoblox DNS Firewall and FireEye NX Series work together to extend the value of threat intelligence on APTs with DNS-based security by providing:

- **Automatic DNS-level blocking of detected threats:** The Infoblox DNS Firewall – FireEye Adapter leverages alerts from FireEye NX Series to block DNS queries at the domain and IP address level.
- **Flexible policy enforcement:** DNS Firewall provides options for managing APT- and malware-based DNS queries. The ability to pass through, block, or redirect gives administrators the flexibility to direct and act on malware DNS queries
- **Identification of infected devices:** The identification of infected device by IP address, MAC address, or user (through Infoblox Identity Mapping) and reporting on this information with Infoblox Reporting and Analytics expedites remediation.

DNS: A Unique and Powerful Defense against Advanced Persistent Threats

Infoblox
CONTROL YOUR NETWORK



Key Capabilities of the Solution

Advanced threat detection, security policy-defined action at the DNS level, and rich reporting on infected devices expedites remediation and reduces expansion of attacks with these immediate benefits:

- **Reduced risk of data exfiltration:** The Infoblox DNS Firewall – FireEye Adapter leverages alerts from FireEye NX Series to immediately and automatically disrupt DNS communication to botnets and command and control servers.
- **Flexible policy enforcement:** DNS Firewall provides options for managing APT malware-based DNS queries. The ability to pass through, block, or redirect gives administrators the flexibility to direct and act on DNS queries.
- **Identification of infected devices:** The identification of infected device by IP, MAC address, or user (through Infoblox Identity Mapping) via Infoblox Reporting and Analytics expedites remediation.
- **Defense and remediation built into IT systems and processes:** No manual intervention is needed for 24x7 protection; and reporting automatically provides full audit trails.

To learn more, visit www.infoblox.com/securedns.

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