Infoblox
NEXT LEVEL NETWORKING

JOINT SOLUTION BRIEF

Harnessing DNS for a Powerful Defense against Advanced Persistent Threats

FireEye

BloxOne™ Threat Defense integration with the FireEye NX Series appliance delivers a unique and powerful defense against advanced persistent threats (APTs) for business networks. This solution combines 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. It is the first solution in the marketplace that invokes powerful DNS-level control of FireEye APT detection events.

Background

An essential asset in today's connected enterprise, the Domain Name System (DNS) is also the number one service targeted by application-layer attacks (four out of five are DNS related). It is also the number one protocol used in amplification/reflection attacks. Such attacks on network security systems expose millions of records and cause significant financial damage to enterprises; the average cost per distributed denial of service (DDoS) attack is $2.5 million. 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.

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 was 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 BloxOne Threat Defense with the FireEye NX Series can help organizations leverage DNS, a powerful and ubiquitous enforcement point, for defending against APT malware and helping prevent data exfiltration. With our solution, they can elevate DNS security to the next level.

Challenges

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

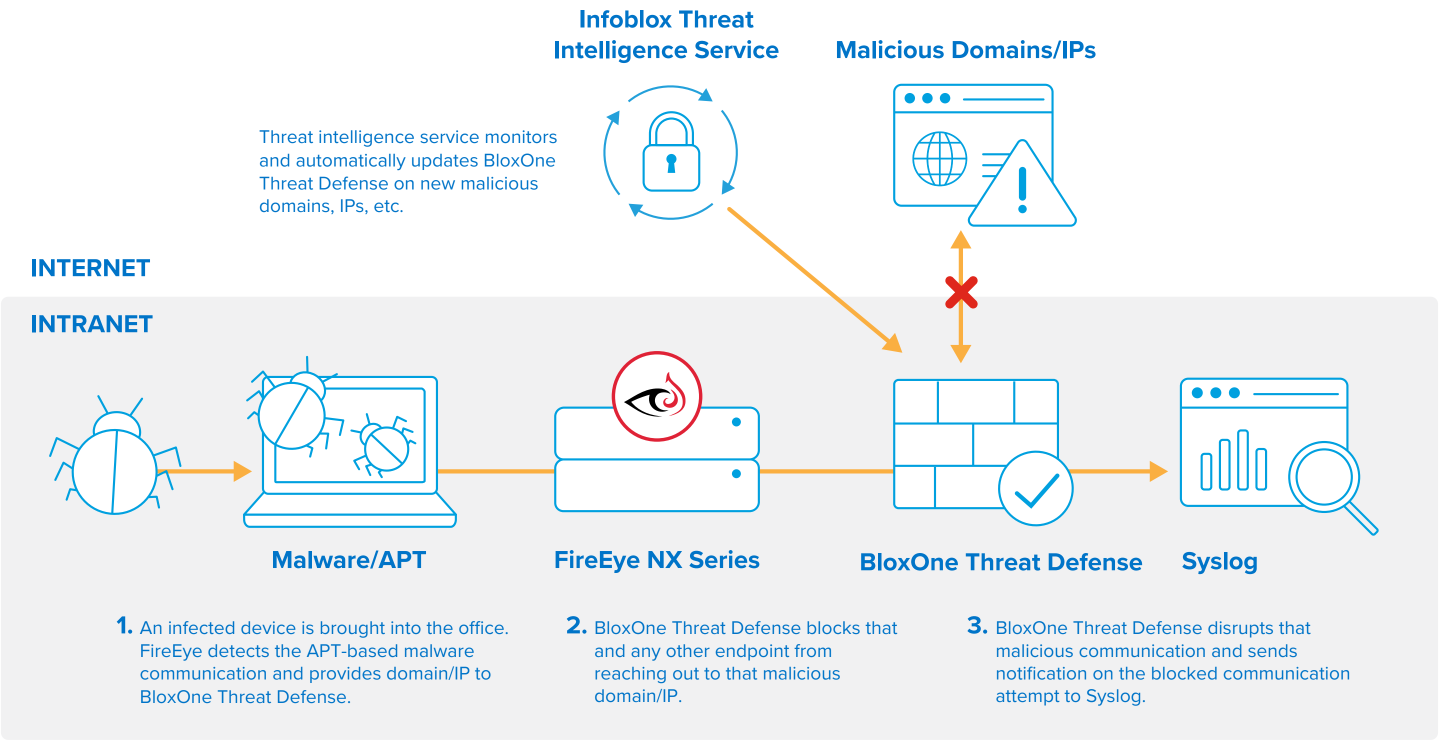
DNS is increasingly being used as a pathway for data exfiltration either unwittingly by malware-infected devices or intentionally by malicious insiders. According to a recent article in *SC Magazine*, a DNS security survey of 300 IT decision-makers revealed that nearly half—46 percent—had experienced DNS exfiltration.

Moreover, many companies have hundreds, if not thousands, of employees, each with two or more company-issued devices such as a laptop and cell phone, and each using several personal devices such as a smartphone and tablet, making it difficult and time consuming to find and clean up APT malware.

Solution

BloxOne Threat Defense and the 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 BloxOne Threat Defense–FireEye Adapter solution leverages alerts from the FireEye NX Series to block DNS queries at the domain and IP address level.
- **Flexible policy enforcement:** BloxOne Threat Defense supplies options for managing APT- and malware-based DNS queries. The ability to pass through, block or redirect such queries enables administrators to direct and act on malware DNS queries.
- **Identification of infected devices:** Infoblox helps expedite remediation by identifying infected devices by IP address, MAC address or user (through Infoblox Identity Mapping) and reporting this information to organizations through Infoblox Reporting and Analytics.



Threat intelligence service monitors and automatically updates BloxOne Threat Defense on new malicious domains, IPs, etc.

1. An infected device is brought into the office. FireEye detects the APT-based malware communication and provides domain/IP to BloxOne Threat Defense.
2. BloxOne Threat Defense blocks that and any other endpoint from reaching out to that malicious domain/IP.
3. BloxOne Threat Defense disrupts that malicious communication and sends notification on the blocked communication attempt to Syslog.

Figure 1: How the BloxOne Threat Defense–FireEye NX Series solution works

Benefits

Our joint solution provides advanced threat detection, security policy-defined action at the DNS level and rich reporting on infected devices that speed remediation and reduce expansion of attacks. Key benefits include:

- **Reduced risk of data exfiltration:** The BloxOne Threat Defense–FireEye Adapter leverages alerts from the FireEye NX Series to immediately and automatically disrupt DNS communication to botnets and command-and-control servers.
- **Flexible policy enforcement:** BloxOne Threat Defense 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.
- **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 FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 7,700 customers across 67 countries, including more than 50 percent of the Forbes Global 2000.

To learn more, visit: www.fireeye.com.

Infoblox
NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com