FireEye Fuel Technology Alliances

FireEye and Infoblox

Disruption of APT Malware Communication at the DNS Level

Key Benefits

- **Reduced risk of information exfiltration:** Alerts from FireEye immediately result in DNS Firewall disrupting DNS communication to botnets and command-and-control servers.
- **Reporting of malicious domains and IP addresses:** Reporting on data sent from FireEye provides IT security personnel with greater under- standing of APT attacks.
- **Defense and remediation built into IT systems and processes:** No manual intervention is needed for 24x7 protection. Reporting automatically provides full audit trails.

Integrated Solution

- **Automatic DNS-level blocking of detected threats:** DNS Firewall leverages alerts from FireEye to block DNS queries at the domain and IP 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:** Malware call back attempts are blocked by FireEye and identification of infected device by IP or MAC address via Infoblox expedites remediation.

Infoblox
CONTROL YOUR NETWORK

DNS Firewall—FireEye Adapter enables disruption of DNS queries by malware and advanced persistent threats (APT) that "calls home" in order to expand attacks and exfiltrate information.

Defense in depth against rising apt malware attacks

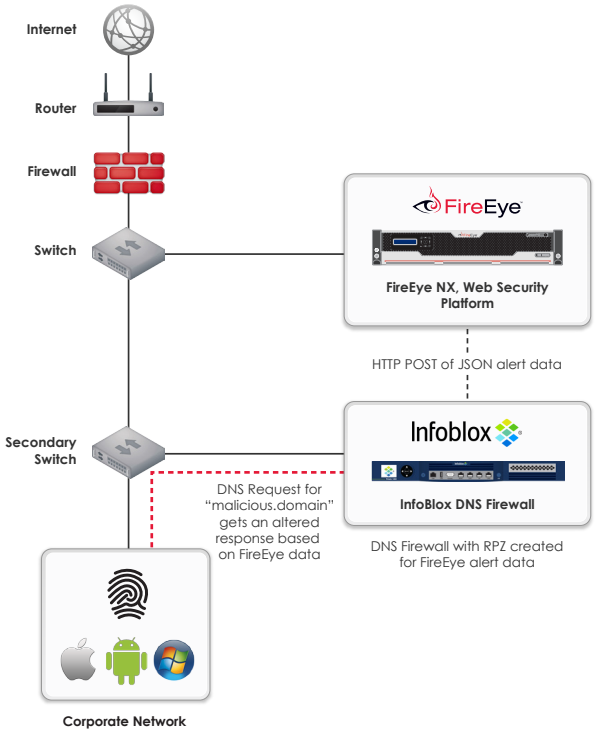
Threat actors behind APTs commonly target organizations with large amounts of sensitive information—such as source code, industrial designs, trade secrets, personally identifiable information that help them gain a competitive and monetary advantage.

FireEye and Infoblox have partnered to integrate our solutions to help our joint customers protect their organizations and valuable data from today's increasing threats. FireEye® NX series integration with Infoblox DNS Firewall delivers a unique and powerful defense against malwares and APT's for business networks.

This solution combines the power of FireEye detection and Infoblox DNS level blocking and device fingerprinting—to detect and disrupt malware communication and help pinpoint infected devices attempting to access malicious domains. The joint solution enables customers to DNS to disrupt malware communication and pinpoint infected devices for improved response time and faster remediation.

How the joint solution works

Once the malware initiates a callback to a command-and-control server for more instructions or to exfiltrate information, FireEye detects and detonates the advanced malware within its Multi-Vector Virtual Execution (MVX) engine on FireEye NX series. FireEye sends an alert to DNS Firewall with the malicious domain and host IP address. DNS Firewall Server adds the domain and host IP address to its blocked domain table. The APT malware initiates a DNS query (domain) in order to find home. DNS Firewall does not resolve the DNS query, thereby disrupting communication. DNS Firewall sends information on infected devices that make DNS queries to malicious domains or IP addresses to Infoblox Reporting, which cross-correlates the IP address, DHCP lease, and device fingerprint (type) to create a report that helps the security team identify devices for cleanup.



Identification of infected devices
At the time of malware callback attempt, identification of infected device by IP or MAC address and by device fingerprint via Infoblox Reporting expedites remediation and reduces expansion of attacks.

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,500 customers across more than 40 countries, including over 100 of the Fortune 500.

About Infoblox

IInfoblox (NYSE:BLOX) delivers essential technology to help customers control their networks. Our patented Grid™ technology helps businesses automate complex network control functions to reduce costs and increase security and uptime.

Infoblox solutions help over 6,100 enterprises and service providers in 25 countries make their networks more available, secure and automated.

For more information, contact Alliances@FireEye.com