FireEye
SECURITY REIMAGINED

FireEye and Infoblox®

Disruption of Advanced Targeted Attack Communications at the DNS Level

SOLUTION BRIEF

SECURITY REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

- **The reduced risk of information exfiltration:** Alerts from the FireEye Network Threat Prevention Platform (NX Series) immediately result in DNS Firewall disrupting DNS communication to botnets and command-and-control servers.
- **Malicious domains and IP addresses reporting:** Data reporting sent from FireEye provides IT security personnel with a greater understanding of APT attacks.
- **Defense and remediation built into IT systems and processes:** No need for manual intervention for 24x7 protection. Reporting automatically provides full audit trails.

OVERVIEW

As more and more information becomes available and stored in electronic form, Advanced Persistent Threat (APT) actors will increasingly focus on breaching data treasures found on networks and systems.

Many of the attacks and hacks these days are using DNS queries to 'phone home' and exfiltrate information. Organizations need to remove DNS queries as an avenue for threats to communication and information exfiltration to protect IT infrastructure from ever-changing attacks and hacks.

THE CHALLENGE

Threat actors behind APTs commonly target organizations with large amounts of sensitive information such as source code, industrial designs, trade secrets, and personally identifiable information that help them gain a competitive and monetary advantage. The challenge for IT professionals is to prevent these sophisticated attacks without disrupting business operations.

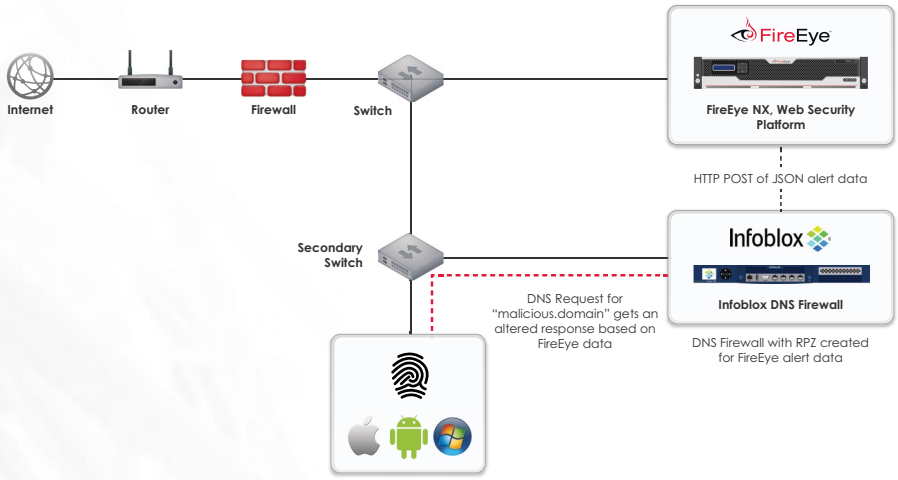
Infoblox®
CONTROL YOUR NETWORK

THE INTEGRATED SOLUTION

The FireEye Infoblox joint solution combines the power of FireEye detection and Infoblox DNS level blocking and device fingerprinting to detect and disrupt threat communications and help pinpoint infected devices attempting to access malicious domains. This joint solution improves response time and accelerates remediation by enabling customers to take an action at the DNS level to disrupt advanced targeted attack communications and pinpoint infected devices.

The integration enables:

- **Automatic DNS-level blocking of detected threats:** DNS Firewall leverages alerts from the FireEye Network Threat Prevention Platform (NX Series) to block DNS queries at the domain and IP level by leveraging a Response Policy Zone (RPZ) for enforcement.
- **Flexible policy enforcement:** DNS Firewall provides options for managing APT-based DNS queries. The ability to pass through, block, or redirect gives administrators the flexibility to direct and act on threat-directed DNS queries. The joint solution enforces policy to block web exploitation, dropper, and callback.
- **Identification of infected devices:** FireEye blocks the advanced targeted attack call back attempts. The identification of the infected device by IP or MAC address, and user via Infoblox expedites remediation.
- **Disruption:** APT heavily leverages DNS at various stages. Infoblox DNS Firewall contains the threat from progressing by cutting off the communication and prevents the attack from propagating.
- **Pinpointing:** Infoblox Reporting, DHCP Fingerprinting, and IPAM solution provides faster identification of source, significantly reducing incident response times.



FIREEYE PRODUCT AND VERSION

FireEye Network Threat Prevention Platform (NX Series) v 7.5

INFOBLOX PRODUCT AND VERSION

Infoblox DNS Firewall

HOW THE JOINT SOLUTION WORKS TOGETHER

Once the targeted attack initiates a callback to a command-and-control server for more instructions or to exfiltrate information, FireEye detects and detonates the malicious software within its Multi-vector Virtual Execution (MVX) engine on the FireEye Network Threat Prevention Platform (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 attack initiates a DNS query (domain) to find home. DNS Firewall does not resolve the DNS query, thereby disrupting communications. DNS Firewall sends information about infected devices that make DNS queries to malicious domains or IP addresses to Infoblox Reporting. Then it cross-correlates the IP address, lease, user of the device and device fingerprint (type) to create a report that helps the security team identify devices for cleanup.

At the time of attack 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.

THE VALUE OF THIS PARTNERSHIP

FireEye and Infoblox have partnered to integrate our solutions and help our joint customers protect their organizations and valuable data from today's increasing threats. The FireEye Network Threat Prevention Platform (NX Series) integration with Infoblox DNS Firewall delivers a unique and powerful defense against advanced persistent threats for business networks.

The partnership delivers a joint solution that is:

Proactive: DNS Firewall—FireEye Adapter enables automated disruption of DNS communication by FireEye detection of advanced targeted threats. This quick action reduces the risk of information exfiltration outside of the business network.

Timely: DNS Firewall and Infoblox Reporting server provide visibility into malicious domains and IP addresses from FireEye. It provides additional clarity on external communication attempts to understand the attack scope better.

Tunable: Tuned DNS Firewall policies can manage advanced persistent threats-based DNS queries. The ability to pass through, block, or redirect to landing pages gives administrators the flexibility to direct and view the APT DNS queries within their security frameworks.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

ABOUT INFOBLOX

Infoblox (NYSE:BLOX) 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 reduces the risk and complexity of networking.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**