Infoblox DNS Firewall – FireEye Adapter

Infoblox
CONTROL YOUR NETWORK

Product Summary

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

- **Automatic DNS level blocking of detected APTs:** 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-malware-based DNS queries. The ability to pass through, block, or redirect gives administrators the flexibility to direct and act on malware DNS queries within their security frameworks.
- **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.
- **Reporting of malicious domains and IP addresses:** Reporting on data sent from FireEye provides IT security personnel with greater understanding of APT attacks.

Using DNS to Protect Against Advanced Persistent Threats

APT Attacks Are on the Rise.

In 2012 there were 855 successful breaches with 174 million records exfiltrated (Ponemon Institute Report, June 2013), costing businesses millions of dollars in remediation costs and infrastructure changes. Why? Because 84 percent of businesses didn't find they were under attack until weeks or months after information had been exfiltrated. (Verizon 2012 Security Report).

APT targets are commonly organizations with large amounts of sensitive information—such as source code, industrial designs, trade secrets, or personally identifiable information, and so forth—that will help the attacker gain a competitive advantage or identify a weakness.

In many cases, APT attacks are about theft for economic gain. Cybercrime has become a major threat to companies and financial institutions. In July 2013, U.S. federal prosecutors charged five men responsible for a hacking and credit-card fraud spree that cost companies more than $300 million.

With many companies having hundreds of employees, each with a minimum of two company-issued devices such as laptop computers and cellphones, and each using another two or three personally owned devices such as smartphones and tablets in the office, finding and cleaning up APT malware is time-consuming and difficult.

Defense in Depth: Disruption of APT Malware Communication at the DNS Level

Infoblox and FireEye have partnered to integrate our solutions to help our joint customers protect their organizations and valuable data from advanced persistent threats (APTs). Infoblox DNS Firewall integration with FireEye NX series delivers a unique and powerful defense against 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 and only solution in the marketplace that invokes powerful DNS-level control on FireEye APT detection events. The joint solution enables customers to detect APTs, leverage DNS to disrupt malware communication, and pinpoint infected devices for improved response time and faster remediation.

How the Solution Works

As shown in Figure1, the solution works as follows:

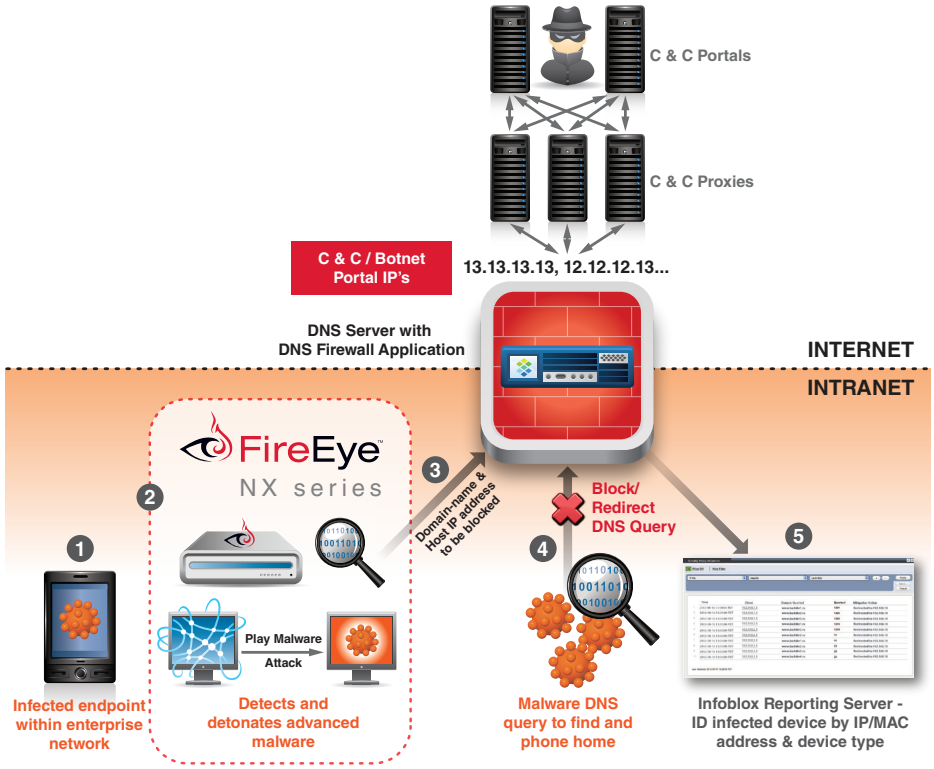
1. A rogue organization or person infects an Internet-based domain web server frequented by employees of the targeted organization or breaches the network perimeter and inserts malware onto various servers, laptops, or desktops. The malware initiates a callback to a command-and-control server for more instructions or to exfiltrate information.
2. FireEye detects and detonates the advanced malware within its Multi-Vector Virtual Execution (MVX) engine on FireEye NX series. It determines that the activity is malicious and therefore should be blocked.
3. 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.
4. The APT malware initiates a DNS query (domain) in order to find home. DNS Firewall does not resolve the DNS query, thereby disrupting communication.
5. 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.

Infoblox DNS Firewall – FireEye Adapter

Infoblox
CONTROL YOUR NETWORK

Product Benefits

- **Reduced risk of information exfiltration:** Alerts from FireEye immediately result in DNS Firewall disrupting DNS communication to botnets and command-and-control servers.
- **Minimization of resources spent on APT and malware remediation:** Infoblox Reporting server identifies infected devices to enable fast cleanup and visibility into security risks by device types.
- **APT defense and remediation built into IT systems and processes:** After setup, no manual intervention is needed for 24x7 protection. Reporting automatically provides full audit trails as well as reports of infected devices suitable for inclusion into IT task queues.



Why the Infoblox Solution Is Unique

Infoblox DNS Firewall integration with FireEye Malware Protection System delivers a unique and powerful defense against advanced persistent threats for business networks. This solution combines the power of FireEye 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. Infoblox DNS Firewall is first and only solution in the marketplace that invokes powerful DNS-level control upon FireEye detection events.

Proactive

DNS Firewall – FireEye Adapter enables automated disruption of DNS communication by FireEye detection of APT malware. This quick action reduces the risk of information exfiltration outside of the business network.

Timely

DNS Firewall and Infoblox Reporting server provide visibility into APT malware domains and IP addresses from FireEye to provide additional clarity on external communication attempts to help better understand the attack scope.

Tunable

DNS Firewall policies can be tuned for managing APT/malware based DNS queries. The ability to pass through, block, or redirect to landing pages gives administrators the flexibility to direct and view the APT-malware DNS queries within their security frameworks.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.

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