Infoblox
CONTROL YOUR NETWORK

Global Consumer Health Products Company

CASE STUDY

One of the World's Largest Consumer Health Companies Combines Infoblox and FireEye to Defend against APTs.

Profile

The Customer:
A major provider of consumer health products, medical devices, biologics, and pharmaceuticals

The Challenge:
Protect a globally distributed network from 35,000 advanced persistent threats per day

The Solution:
- Infoblox DNS Firewall
- Infoblox Threat Intelligence Feed
- Infoblox Security Ecosystem
- Infoblox 2210 appliance

The Results:
- Ability to pinpoint the IP addresses of infected clients
- Added value from FireEye and Infoblox investments
- Significantly enhanced protection from APTs

The Customer

This large international company markets a wide range of health-related products—from medical devices to biologics to pharmaceuticals—to consumers and healthcare organizations. It has hundreds of operating companies around the world and more than 120,000 employees.

The Challenge

The company manages a vast, globally distributed network that serves all its operating companies, and advanced persistent threats (APTs) in particular keep network managers awake at night. FireEye Threat Prevention Platforms are deployed to guard against APTs at eight hub locations that carry 99 percent of the company's Internet traffic for EMEA, Asia-Pacific, and North America. And during a proof-of-concept test to demonstrate FireEye's effectiveness, the security team uncovered an alarming fact.

The FireEye software, which was configured on the side as a monitoring system rather than inline as a blocking system, was detecting from 35 to 40 thousand DNS requests every day going to or from domains associated with known malware products. But network managers had no way to identify the infected devices.

FireEye was identifying the company's Infoblox DNS servers, some of which were handling thousands of queries, as the source of the malicious communications—but what was actually going on was that Trojans, APTs, and other types of malware on infected clients were asking the DNS servers to phone home for them. And the FireEye alerts were identifying the Infoblox servers rather than the infected devices themselves as the source.

So while network managers could count the communications with malicious domains, they couldn't pinpoint the specific clients on their network that were sending them. And they asked Infoblox, "How can you help us see what we cannot see today?"

The Infoblox Solution

Infoblox handles all the company's DNS and DHCP management via an Infoblox Grid™ connecting appliances at the hubs where FireEye is deployed as well as at all the network endpoints. Infoblox and FireEye are technology partners, and FireEye named Infoblox Technology Alliance Partner of the Year in 2013.

While the Infoblox team was performing an upgrade of the DNS/DHCP system, they heard about the problem, and they proposed a solution. At the core of the Infoblox/FireEye partnership is the Infoblox Security Ecosystem, which integrates Infoblox DNS Firewall with FireEye NX Series appliances and combines FireEye APT detection with Infoblox DNS-level blocking and device fingerprinting.

Infoblox
CONTROL YOUR NETWORK

Global Consumer Health Products Company

CASE STUDY

With Infoblox servers already in place, the Security Ecosystem formed the ideal solution. It could be installed on a single Infoblox server and quickly pushed out to the servers at the end points via the Infoblox Grid™—supplying the missing piece in the company's threat protection and giving network administrators visibility into the IP addresses of the infected clients.

The Results

The company implemented DNS Firewall, the Security Ecosystem, and the Infoblox Threat Intelligence Feed, which delivers accurate and current data on emerging malware threats. The combined Infoblox/FireEye solution now delivers two layers of protection against APTs, makes it possible to pinpoint infected clients for quarantine and remediation, and blocks outbound communications to command-and-control servers and botnets, directing them instead to landing pages or walled gardens on internal servers for analysis and addition to blacklists.

And the Infoblox side of the solution extends threat protection beyond the APTs that FireEye focuses on to other forms of malware, further strengthening the company's defenses.

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