A Large Internet Service Provider

Infoblox
CONTROL YOUR NETWORK

Profile

The customer:

A large Internet service provider

The challenge:

Prevent NXDomain attacks that were slowing performance and damaging customer experience

The solution:

- Infoblox Grid™ technology
- Infoblox DNS Caching Appliances
- Infoblox Advanced DNS Protection

The results:

- Blocked 100 percent of malicious DNS requests
- Saved significant time in several processes
- Eliminated extensive repetitive manual tasks for skilled staff
- Maintained customer experience at the proper levels
- Prevented disruption to the business

The Customer

The customer is one of the more than 150 service providers that use Infoblox solutions to manage mission-critical networks serving millions of customers. Like all service providers today, the company is a potential target of distributed-denial-of-service (DDoS) attacks.

The Challenge

This service provider had problems with DNS performance and service outages—problems that can directly impact customer satisfaction, revenue, and reputation. These difficulties also burdened the operations staff, which was spending a lot of time diagnosing perceived performance issues.

After extensive troubleshooting attempts involving manually reviewing server logs, they contacted Infoblox support staff, who helped them determine that there was no problem with the servers and that the slow performance was being caused by a growing DNS threat—the non-existent domain (NXDomain) attack, also called the “phantom domain” attack. Phantom domain is a type of DDoS attack that causes extreme stress on the DNS infrastructure and can lead to loss of Internet service.

The customer’s DNS infrastructure was under attack by a series of random clients that sent multiple DNS requests to force the DNS servers to resolve multiple non-existent domain names within the target domain. Each request came from a different source IP address.

Since the non-existent domains were not cached, the DNS servers requested recursion across the Internet to resolve the domain locations—getting no responses and causing the overall level of traffic to and from the caching servers to increase by a factor of five. As the caching servers started to become saturated, DNS performance for legitimate queries slowed down, degrading the customer web experience.

To mitigate the attacks, the network operations team started manually reviewing DNS server log files and then manually applying new blacklisting rules to block DNS requests for the non-existent domains. This involved rebooting the system, and had to take place during maintenance windows, disrupting services. And within a couple of days, the attackers hit again with new non-existent domain names, and the network team had to start over again. Multiple cycles of this activity over several months caused considerable disruption.

The Infoblox Solution

Fortunately, Infoblox could supply an effective solution—called Infoblox Advanced DNS Protection—that the customer could quickly plug into its existing Infoblox Grid™ architecture.

Running on Infoblox Advanced Appliances with next-generation programmable processors designed for threat mitigation, Advanced DNS Protection intelligently distinguishes legitimate traffic from malicious traffic generated by DNS attacks like DDoS, DNS exploits, and vulnerabilities. It automatically drops the attack traffic while responding to legitimate traffic.

In addition, it receives regular automatic updates based on threat data uncovered by our threat research team. The team mines petabytes of data daily from different locations, resulting in new analytics algorithms that determine bad and phantom domains used in this class of attack.

The Results

The Infoblox Advanced DNS Protection solution was able to automatically detect the pattern of incoming attacks and apply the blacklisting rules, blocking the false DNS requests before they reached the Infoblox DNS servers. There was 100 percent success in blocking the attacks, which in turn yielded multiple tangible benefits.

The network operations team was freed from the time-consuming efforts they had been pouring into troubleshooting, analysis, and manual application of blacklisting rules. Since rule changes were automatically applied, there was no longer a need for disruptive downtime caused by maintenance windows and reboots.

And most important, Advanced DNS Protection prevented the attack from affecting legitimate requests so that the customer experience was maintained at the appropriate levels. In other words, 100 percent success for the customer's defensive efforts resulted in 100 percent failure for the attackers.

About Infoblox

Infoblox (NYSE:BLOX), headquartered in Santa Clara, California, delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 7,000 enterprises and service providers around the world to transform, secure, and scale complex networks. Infoblox (www.infoblox.com) helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime.