infoblox

CASE STUDY

Large Internet Service Provider

THE CUSTOMER: LARGE INTERNET SERVICE PROVIDER

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

Mitigating Attacks on DNS Infrastructure that Hinder Performance and Impact Business Results

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 diagnose that the slow performance was not related to the servers but 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 send loads of DNS requests to force the DNS servers to resolve multiple non-existent domain names within the target domain. Each request comes 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 response 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.

Customer : Large Internet service provider

OBJECTIVES:

- Prevent DDoS attacks
- Improve DNS performance and its impact on customer experience
- Automate the detection of and response to legit traffic from malicious traffic

RESULTS:

- Blocking 100% of malicious DNS requests
- Saving significant time in several processes
- Eliminating extensive, repetitive, manual extensive repetitive manual tasks for skilled staff
- Maintaining customer experi- ence at the proper levels
- Preventing disruption to the business

PRODUCTS:

- NIOS DDI
- Advanced DNS Protection

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 SOLUTION

Fortunately, Infoblox could supply an effective solution, 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 the Infoblox 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 RESULT

A Success Story for Both Network Operations and Customers

Advanced DNS Protection automatically detects the pattern of incoming attacks and applies the blacklisting rules, blocking the false DNS requests before they reach the Infoblox DNS servers. The internet service provider has seen 100% success in blocking the attacks, which in turn yields multiple, tangible benefits.

The network operations team is free of time-consuming tasks, such as troubleshooting, analyzing, and manually applying blacklisting rules. Since rule changes were automatically applied, they no longer experience disruptive downtime caused by maintenance windows and reboots.

And most important, Advanced DNS Protection prevents the attacks from affecting legitimate requests; thereby, maintaining the appropriate level of customer experience. In other words, 100% success for the customer's defensive efforts resulted in 100% failure for the attackers.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240213v1