Major Financial Institution Stops Data Breach by Defending Against High Volume SQL Injection Attack

The Situation

A large global asset manager headquartered in the United States faced a large scale SQL injection attack, which originated from Nigeria.

The Challenge

SQL injection passes SQL common web application's legitimate SQL code with the common objective of downloading valuable information such as user passwords, account numbers, and other personal information. The extracted data can then be used to commit fraudulent fund transfers, credit card purchases, and ATM withdrawals. In this example, the SQL injection attack attempted to probe for SQL vulnerabilities and extract data from a large asset management firm. While Nigeria has been a historical source of fraudulent web attacks and the firm could have employed Akamai's services to block all traffic from the country, this was not a viable option because the firm has valued customers in Nigeria.

The Goal

- Protect both client and corporate data by preventing a data breach.
- Maintain performance and availability of services during the attack.
- Avoid requirement to divert IT staff to fight attack traffic and conduct post-attack recovery.

Why Akamai

Kona Site Defender automatically and immediately denied the SQL injection traffic. No action was required on the part of the customer. The financial firm's team received an automated alert and was able to observe both the attack characteristics and the activated defenses using Kona's security monitor, which provided near real-time visibility. In comparison, with some security offerings, the customer would not have even been notified that the attack was in progress.

In total, more than 15,000 malicious requests were identified by the Akamai security defense during the roughly thirty minutes of the attack's duration. At the edge of the Internet, far from the customer's data center, Akamai's Intelligent Platform™ denied more than 14,000 of the malicious SQL injection attempts. Akamai also served cached content to the balance of the malicious requests, and none of the attack traffic reached the customer's datacenter.

This attack occurred inside SSL based requests. Akamai decrypts each SSL request, inspects the request for known attacks and, if none are found, re-encrypts the request and sends it to the customer's data center. This highly distributed defense helps to ensure that the attack traffic inside of the SSL request is blocked far away from the customer data center. Akamai SSL servers are a special subset of the Akamai Intelligent Platform that is fully PCI compliant.

With more than 120,000 servers positioned in more than 80 countries, the Akamai Intelligent Platform is designed to offer unmatched scale and highly distributed capacity to stop even the largest cyber-attacks.

INDUSTRY

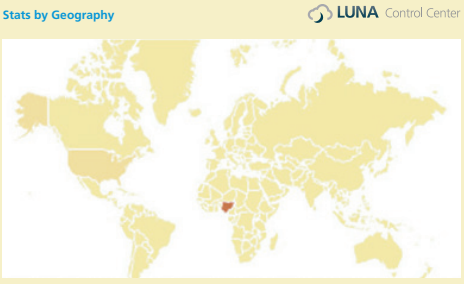
Financial Services

SECURITY SOLUTIONS

- Web Application Firewall
- Security monitor
- DDoS defense
- Cached content delivery

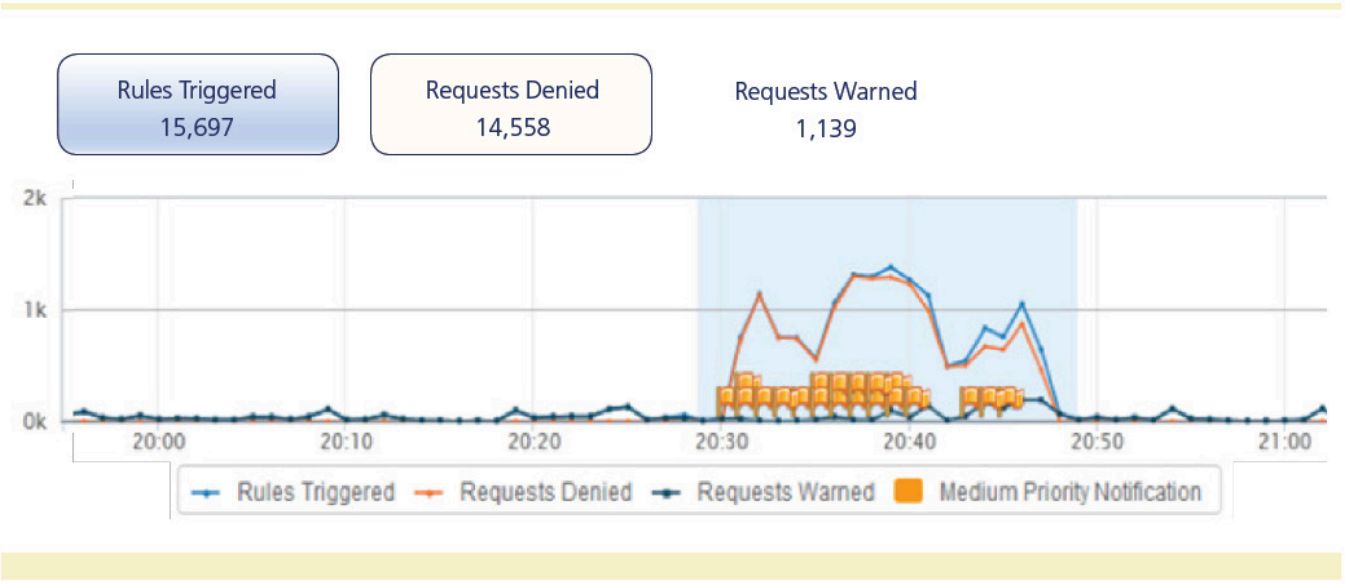
KEY IMPACTS

- More than 14,000 attack requests were denied.
- Always-on defense initiated automatically.
- Customer was alerted and had full visibility into the attack data and defenses employed.
- No customer staff resources were diverted to attack defense or recovery.



Akamai's Luna Control center provides attack statistics and a visual representation of the geographical source of attack traffic. In this particular case study, Nigeria is highlighted in red.

Major Financial Institution Stops Data Breach



Akamai FASTER FORWARD

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.