radware

CASE STUDY: **E-COMMERCE**

Multinational Online Retailer Turns to Radware for 360-Degree DDoS Detection and Protection

THE CHALLENGES

An increasingly wide range of cyberthreats began to threaten the online availability of e-commerce sites. In addition to negatively impacting consumer quality of experience, any resulting data breaches that compromised personal information would undermine consumers' trust in the company and brand.

THE SOLUTION

Radware's Attack Mitigation Solution (AMS) is a hybrid system that integrates on-premise DDoS mitigation capabilities with cloud-based scrubbing centers.

WHY RADWARE

AMS provided the best 360-degree protection from a wide array of attack vectors, including volumetric, encrypted and application-layer attacks, for the company's e-commerce sites without blocking legitimate traffic.

BENEFITS

The e-commerce retailer has successfully mitigated a series of volumetric and network-layer cyberattacks, solving the challenges associated with distinguishing legitimate traffic from malicious traffic and ensuring no negative impact on legitimate customers.

This e-commerce retailer is a cable, satellite and broadcast shopping conglomerate that specializes in televised home shopping and owns several sister channels in seven countries around the globe.

THE CHALLENGES

Two cornerstones of this company's e-commerce business were high availability of its e-commerce services/websites and security of its customers' data. The company had numerous e-commerce sites that served millions of customers worldwide. A wide range of cyberthreats began to threaten the online availability of these sites, and any resulting data breaches of customer personal information would undermine consumers' trust in the company to keep their data secure.

A series of cyberattacks underscored these concerns. First, the company experienced several DDoS attacks that leveraged HTTP/HTTPS Floods, which it had difficulty mitigating. Next, the company received a ransom letter threatening a large-scale volumetric attack from the Armada Collective. It became clear that the organization needed to strengthen its DDoS mitigation capabilities against a wider array of attack vectors, specifically volumetric floods.

The organization was already an existing customer of Radware and leveraged its on-premise DDoS mitigation device, DefensePro. DefensePro was very effective at detecting and mitigating nonvolumetric attacks by using behavioral analytics and automated signature creation. The threat of volumetric attacks meant the organization required a hybrid DDoS strategy, one that combined on-premise with cloud-based scrubbing centers.

Complicating this new DDoS mitigation strategy was the fact that, several years earlier, to cope with Layer 7 application-based attacks, the e-commerce retailer had purchased the Imperva WAF, only because this is the actual, licensed name for a competitive product. which the retailer did not want to replace. In addition, some cyberattacks were embedded within the organization's CDN service, which was provided by Akamai. The e-commerce retailer could not determine the source of the attacks, which appeared to be coming from the CDN vendor's IP address.

As a result, the retailer had a series of technical requirements for the new hybrid DDoS mitigation solution:

- Ability to ensure that legitimate, clean network traffic was not blocked due to false positives and did not suffer from high latency, thereby impacting the quality of experience for customers
- Ability to differentiate attack traffic from legitimate traffic when they have the same source address as the CDN
- SSL traffic inspection for protection from encrypted attacks (at least 10,000 CPS)
- Tight integration between the multiple components of the DDoS mitigation solution
- Minimal to no network latency

THE SOLUTION

To satisfy these business needs, Radware recommended a hybrid DDoS system, the Attack Mitigation Solution (AMS), to protect the online retailer from potential volumetric attacks. Radware worked with the CDN provider to allow AMS to provide accurate detection and mitigation of embedded attack traffic coming from the CDN.

AMS integrated a series of web application and network security products into a single solution. This included integrating the existing DefensePro with Radware's Cloud DDoS Protection Service; Radware's on-premise web application firewall, AppWall; and SSL traffic inspection capabilities.

This integrated solution is able to provide complete 360-degree protection from a wide array of attack vectors, including volumetric attacks, encrypted attacks by performing SSL traffic inspection and application-layer protection via Layer 7 defense capabilities. The integrated solution also has the added benefit of having decreased operational and management requirements for the security team.

Finally, to assist the online retailer's operations team with service installation and day-to-day solution monitoring and management, the customer elected to purchase additional assistance from Radware's professional services team.

Prior to implementing Radware AMS, the e-commerce company consulted with Akamai to see if the CDN vendor could provide this same level of protection, but Akamai was unable to differentiate legitimate traffic from malicious traffic that was processed via the CDN.

"This is a great example as to why we implemented Radware. Shortly after implementing Radware, we successfully mitigated a massive volumetric DDoS attack by diverting to Radware's cloud-based scrubbing center."

— Operational VP of IT security at e-commerce retailer

BENEFITS AND NEXT STEPS

Since implementing AMS, the e-commerce retailer has successfully mitigated a series of volumetric and network-layer cyberattacks and has solved the challenges associated with distinguishing legitimate traffic from malicious traffic, including network traffic originating from its CDN. This has enabled it to ensure minimal latency with no negative impact on legitimate customers leveraging its numerous e-commerce sites. Cyberattacks are now mitigated in real time by leveraging AMS' machine-learning capabilities to detect traffic anomalies and automatically create new attack signatures.

Moving forward, the retailer has decided to allow the daily operations and maintenance of AMS (including security policy updates, product updates/patches, etc.) to be fully managed by Radware's team of security experts, the Emergency Response Team. Finally, as the company's licenses for Imperva WAF expire, it is replacing Imperva WAF with Radware AppWall to ensure it has a fully integrated attack mitigation system in place.

MERGER AND ACQUISITION

In 2018, this e-commerce retailer was purchased by a larger, multinational home shopping company. At the time, this larger home shopping company was evaluating its own DDoS protection capabilities. Following the acquisition, the global director of information security strategy and architecture at the e-commerce retailer became an internal champion of Radware, and as a result, the large home shopping company has elected to implement Radware as well to make it the cornerstone of its DDoS mitigation strategy.