radware

CASE STUDY: **BANKING**

U.S. Credit Union Relies on Cloud-Based Protection to Ensure a Superior Banking Experience

OVERVIEW

This credit union has been serving customers throughout the Southeastern United States for over 75 years. With over 300,000 members and $4 billion in assets, it is one of the largest credit unions in the region.

Like most financial service organizations, this credit union is heavily dependent on various online platforms, including its website and customer banking portal, to provide a superior digital experience for its customers.

THE CHALLENGES

Several years ago, the credit union's online platforms came under attack and customers were unable to access the portal and/or complete banking transactions, resulting in dissatisfied customers. This necessitated the implementation of a cloud-based web application firewall (WAF). The credit union selected Imperva's Cloud WAF.

Unfortunately, several months later, the credit union was still suffering from various application-based attacks, including a series of new bot-based, account takeover attacks. While Imperva's WAF proved successful in blocking these attacks, it came at an unacceptable cost. Imperva was reactionary and manual-driven, requiring the credit union's security team to identify attack traffic themselves. This cost the credit union time when under attack and tied up limited security resources.

The credit union, which had previously inquired about Radware's DDoS protection solutions, reached out a second time to discuss application protection. Radware and Cisco, a Radware alliance partner, presented a joint solution to provide comprehensive protection against an array of network and application attack vectors.

THE SOLUTION

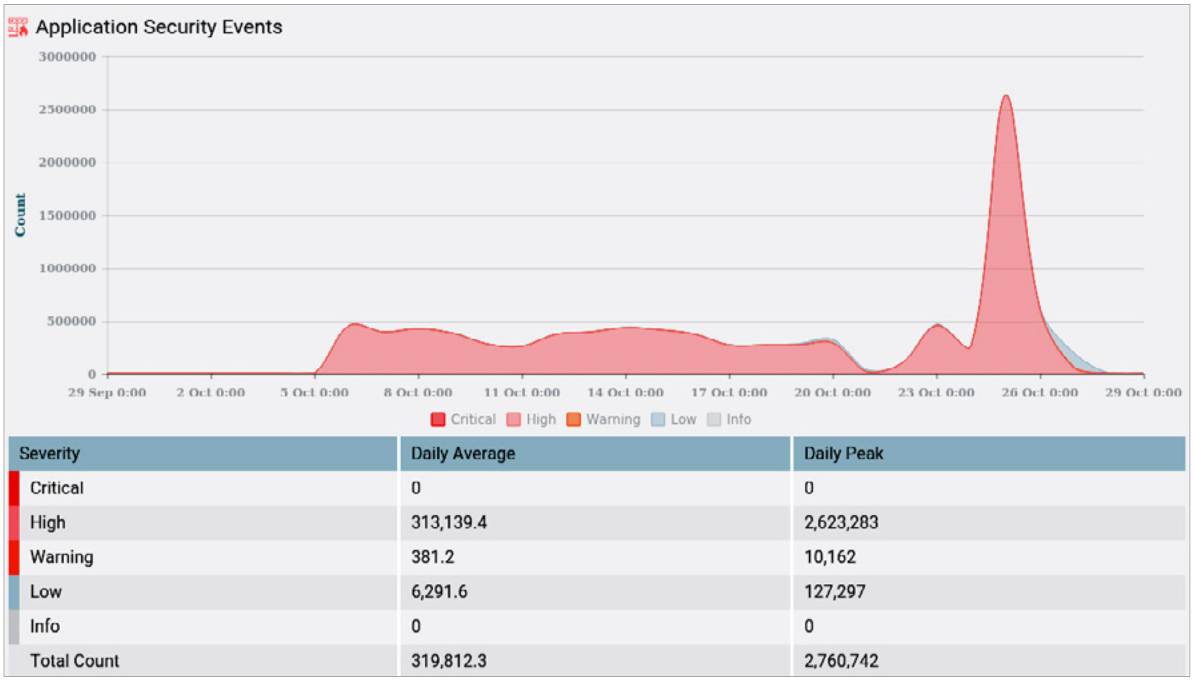
The solution comprises several Radware security solutions, starting with Cloud WAF Service for protection against OWASP Top-10, zero-day assaults and other attack application-layer attacks. The credit union particularly values the automatic policy generation capabilities of the Cloud WAF Service, which adapts security policies to new threats and changes to applications and websites, saving the security team time and operational costs.

It also includes Radware Bot Manager, which safeguards the credit union's web and mobile applications and APIs from automated threats by distinguishing malicious bots from legitimate traffic.

Lastly, DDoS attack protection will be provided by leveraging a hybrid implementation that includes DefensePro, Radware's on-premise DDoS mitigation appliance, and Radware's Cloud DDoS Protection Service for protection against distributed denial-of-service attacks, network Layer 3/Layer 4 and application-Layer 7 attacks and SSL protection.

STAYING IN BUSINESS WHILE UNDER ATTACK

In October 2020, the credit union was the target of advanced application and bot attacks which nearly crippled their application and network infrastructure. From October 17-21, the credit union experienced access control violations of their websites, followed by website application attacks which peaked at 2.5 MPPS on October 24th. A series of malicious bot attacks against the credit union websites, totaling 57.43 million hits, started on October 25th (See Figure 2).



Severity	Daily Average	Daily Peak
Critical	0	0
High	313,139.4	2,623,283
Warning	381.2	10,162
Low	6,291.6	127,297
Info	0	0
Total Count	319,812.3	2,760,742

Figure 1. Application Security Events Experienced (Oct. 1 - Nov. 1)

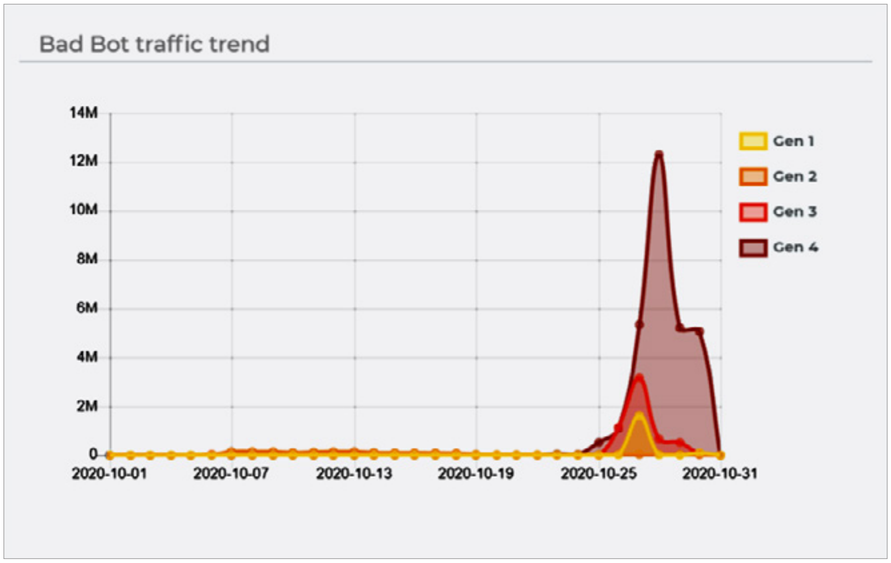


Figure 2. Bad Bot Traffic by Generation (Oct.1- Oct. 31). Gen 1- Basic script bots mitigated through blacklists. Gen 2- Headless browser bots blocked via fingerprint. Gen 3-Bots simulating basic human like interactions blocked by keystroke or mouse movement analysis. Gen 4-Bots simulating advanced human like interactions blocked using Radware's intent-based deep behavioral analysis.

At the time of these assaults, the credit union was still using Imperva Cloud WAF, which was incapable of fully mitigating the attacks. This resulted in high call volumes since many users were unable to access their accounts via the mobile application.

Radware expedited the implementation and onboarding of Radware Cloud WAF Service and Bot Manager. Both solutions mitigated the assaults and restored availability and security for the credit union's mobile and web applications. The VP of IT stated that the credit union's security team was impressed with speed and effort of the implementation and the ability of Radware professional services to address the credit union's issues.

MOVING FORWARD

Radware's Cloud WAF Service and Bot Manager have successfully safeguarded the credit union's application from a series of high-volume application and bot attacks, allowing the company to guarantee uninterrupted service for its customers.

Because Radware's application security tools use automation and behavioral learning to adapt to new threats, the credit union security team has more time to do proactive planning for the next evolution of threats. Next on the agenda for the credit union is implementing Radware's Hybrid DDoS protection service.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.