Radware Bot Manager Protects Leading US-Based Financial Institution from ATO Attacks

CUSTOMER:
Leading US-Based Financial Institution.

INDUSTRY:
Financial Technology.

CHALLENGES FACED:

- ATO attacks via credential stuffing and cracking.
- Scalability challenges for new client applications.
- High false positives impacting user experience.
- Poor visibility into mobile app vulnerabilities.

Overview

This leading US-based financial institution is a global provider of financial technological (fintech) solutions, serving banks, credit unions, insurance companies, and leasing companies in over 100 countries. The company processes and facilitates billions of payment transactions annually, which made its platform an attractive target for cybercriminals running malicious bots to carry out attacks such as Account Takeover (ATO), which jeopardized user accounts, sensitive data, and business operations.

WHY RADWARE BOT MANAGER?

- Seamless API-based scalability.
- Real-time detection and preemptive mitigation.
- AI-powered behavioral analysis.
- Flexible CAPTCHA-less mitigation options.
- Mobile app-specific protections.

RESULTS:

- Over 5 billion bad bot hits mitigated in 3 months.
- $155M in potential breach losses prevented.
- 100+ hours saved in manual security efforts.
- Seamless protection for over 5,000 applications.

Challenges

The company was targeted with increasingly sophisticated bot attacks on the login workflow of their client applications, particularly brute-force ATO attacks including both credential stuffing and credential cracking techniques.

Their existing application security was built around a competing security vendor to manage incoming traffic and mitigate bot activity. However, with the rapid expansion of their client base and the evolving bot threat landscape, several critical limitations quickly became apparent:

Poor Scalability: The existing solution required extensive configuration for each new client integration, creating significant operational bottlenecks as the company continued to expand its client base.

Inconsistent Bot Detection: The existing solution struggled to differentiate between legitimate traffic and malicious bots, causing high false positives and disrupting critical transactions, while sometimes not detecting sophisticated attacks.

Ineffective Mitigation: The existing solution's limited bot mitigation options caused friction, as security measures could not be tailored to user behavior, dynamic attack patterns, or threat levels—leading to disruption of critical workflows.

Bad User Experience: Legitimate customers sometimes faced delays or disruptions due to unnecessary security challenges caused by high false positive rates. This impacted the overall user experience, leading to frustration and harming our client's reputation.

Operational Inefficiencies: The company's internal security team spent significant time to manually adjust settings, manage false positives, and handle policy updates for new clients, which diverted focus from other key security initiatives and strategic improvements.

Poor Integration with Mobile App Protection Solutions: The existing solution provided limited visibility and inconsistent security coverage in detecting and mitigating bot threats on mobile platforms, exposing critical APIs to significant vulnerabilities.

The company had even taken internal rate limiting defense measures, which proved ineffective against advanced credential stuffing attack patterns.

Solution

Faced with rising bot threats and the ineffectiveness of existing defenses against sophisticated ATO attacks, the company sought a more effective solution. After evaluating several vendors, the company chose Radware Bot Manager, p**art of Radware's Cloud Application Protection Services, to effectively address its challenges and deliver comprehensive AI-driven protection tailored to the firm's needs**.

The key features that differentiated Radware Bot Manager from the client's earlier security solution were:

Seamless Scalability: Radware's API-based cloud-native approach enabled the company to seamlessly extend protections to new applications and clients without manual intervention.

Real-time Bot Detection: Bot Manager's patented machine learning algorithms detected and analyzed malicious activity in real-time, flagging suspicious behavior and preemptively blocking known bad bot traffic and malicious sources before they even hit the client's applications.

Behavioral-based Mitigation: Radware's AI-powered behavioral-based detection algorithms analyzed incoming traffic on the client applications' login workflows to accurately distinguish between legitimate users and sophisticated humanlike bad bots without causing false positives. Bot Manager provided robust protection against even large-scale distributed ATO attacks by swiftly detecting anomalies and automatically creating attack signatures in real-time.

Cross-module Correlation: Deploying Bot Manager as part of Radware's broader Cloud Application Protection Services allowed our AI-based correlation engine to analyze security events on applications from across all active security modules, including our Web Application & API Protection (WAAP) suite. This cross-correlation helped block nefarious source IPs across all protected applications with complete visibility, enabling accurate security and lower overheads on infrastructure and security costs.

Flexible Mitigation Methods: Radware Bot Manager provided a wide variety of mitigation methods out-of-the-box, which did not require any customization on the company's part. From conventional mitigation methods such as blocking and CAPTCHA challenges, to Radware's innovative CAPTCHA-less Crypto Challenge-based mitigation technique, our client now had the flexibility to mitigate bad bots based on its unique needs without disrupting the user experience.

Mobile App-Specific Protection: Radware's proprietary Secure Identity Engine and mobile attestation for devices blocked bot attacks on native mobile apps before they even materialized, and ensured complete, real-time visibility into mobile threats.

Benefits

Radware's Bot Manager implementation process focused on addressing the client's specific needs while ensuring minimal disruption to their existing operations. With the solution deployed, the fintech company realized significant improvements across multiple areas:

Scalable Security: As the company continued to grow and handle more complex transaction volumes, Bot Manager seamlessly scaled its protection to cover over 5000 applications, providing enhanced protection while offering bulk onboarding support for new applications and clients without additional overheads.

Accurate Bot Detection: Over three months following its deployment, Bot Manager blocked over 5 billion bad bots in real-time from hitting over 5,000 onboarded applications. Though Radware's preemptive protection techniques mitigated a good share of this traffic, our AI-powered behavioral detection techniques were the key driver in detecting and mitigating over 90% of these bad bot hits that included sophisticated bots emulating human-like browsing behavior.. Radware's SDKs for Android and iOS devices also ensured device authenticity, blocking emulators, modified apps, and unauthorized devices from launching attacks.

Improved User Experience: With Radware's accurate bot detection and advanced mitigation, legitimate users were no longer impacted by unnecessary security checks caused by false positives. CAPTCHA-less mitigation techniques such as our Crypto Challenge proved to be highly effective in throttling bad actors without affecting reals users.

High ROI on Data Breach Protection: Successful ATO attacks can have far-reaching consequences on data security and privacy implications due to theft of personally identifiable information (PII). For two critical applications alone, Radware Bot Manager helped our client avoid over $155 million in potential losses from data breaches.

Operational Efficiency: Bot Manager helped the company's internal teams save over 100 work-hours and over $20,000 on human resource costs in securing its critical applications through its automated detection and mitigation capabilities that greatly reduced the need for manual intervention.

By adopting Radware Bot Manager, this major fintech company successfully overcame scalability, security, and user experience challenges. The success of this implementation, along with the responsiveness and consistent support from Radware's team—including the onboarding of over 5000 client applications—has convinced the company to recommend Radware Bot Manager to all their clients. As the company continues to grow, it now has a solid foundation including the right tools and capabilities to proactively prevent future threats while maintaining a positive, seamless experience for its users.

To learn more about how Radware solutions such as Bot Manager, Cloud Application Protection Services, and our other solutions comprehensively protect your organization from cyber-attacks, click here to contact us.