Preventing Romance Fraud Caused by Automated Attacks

Case Study

Executive Summary

Zoosk is a relationship app with one goal—to help people connect and find romantic love. Rather than flings, and swipes, Zoosk helps real people find the real love they're looking for through a number of different means. Unfortunately, bad actors have seized on the popularity of Zoosk as an opportunity to scam unsuspecting users and commit fraud. Using automation, the bad actors commit account takeover and fake account creation attacks to build trust and convince users that their potential partner's request for a "loan" was real, when in fact it was fraud.

The Challenge

Challenge 1

Prevent romance scams that result in financial fraud averaging $12,000 per incident.

Challenge 2

Protect the Zoosk brand and reputation from damage caused by bad actors who victimize users.

Challenge 3

Protect all exposed APIs and web-based account login and registration applications with consistent security.

Why AWS

Zoosk migrated their applications onto Amazon Web Services (AWS) in 2017 with the goals of reducing operational overhead and adopting a more iterative application development methodology. Today, Zoosk has achieved their goal of being more iterative by publishing daily iPhone and Android mobile application updates. The Zoosk AWS deployment consists of a single Amazon VPC with between 40 and 100 Amazon EC2 instances running containerized PHP and Node-based micro-services, and an ECS cluster of 50-100 instances running Java-based micro-services. New apps and updates are deployed in an automated manner using custom-built orchestration tools integrated tightly with Slack and GitHub. Operationally, Zoosk developers can quickly prototype new features, spinning up, then taking down the compute, software, and storage related resources when the task is complete. This process is far less cumbersome than the traditional data center approach of working with IT, purchasing and internal approvals to buy, or gain access to the resources needed.

About Zoosk

Zoosk is a leading online dating company that personalizes the dating experience to help singles find the person and relationship that's just right for them. Zoosk's Behavioral Matchmaking technology is constantly learning from the actions of over 35 million members in order to deliver better matches in real time. With the #1 grossing online dating app in the Apple App Store, Zoosk is a market leader in mobile dating. Available in over 80 countries and translated into 25 languages, Zoosk is a truly global online dating platform.

"Cequence has virtually eliminated romance scams associated with automated account takeovers and fake account creation attacks targeting our mobile app APIs. Their agentless approach bakes security into our development workflow, allowing us to securely deploy new application updates every two weeks."

Conor Callahan, Technical Lead of Platform and Infrastructure, Zoosk

Why Cequence Security

Prior to choosing Cequence, Zoosk had implemented an alternative security solution that required JavaScript instrumentation for every web page and mobile SDK integration for iPhone and Android apps. This approach introduced significant delays in the development and deployment cycle, oftentimes disrupting their frequent software update cycles. In addition, the incumbent solution did not address direct-to-API attacks, where the bad actor decompiles the mobile app to find the login or registration APIs, then targets them directly with automation. Zoosk had discovered that roughly 90% of their attacks were targeting the mobile application APIs. Zoosk chose Cequence Security to replace their existing automated attack prevention solution for three reasons.

1. A unique AI-based, out-of-band approach that is developer friendly, eliminating JavaScript instrumentation and mobile SDK integration penalties such as application deployment delays, security gaps, and user dissatisfaction from slow page load times.

2. Automatic and continuous application discovery and visibility of all web, mobile and API-based applications, both current and newly deployed or updated.

3. Open, extensible platform that allows Zoosk to quickly discover and prevent automated attacks while the REST-based APIs allows them to export findings to their existing infrastructure for log analysis and reporting.

The Solution

The Cequence Application Security Platform with Bot Defense complements native AWS security by protecting the Zoosk web, mobile and API-based applications from automated bot attacks such as account take overs and fake account creation that may result in romance scams and fraud.

Zoosk has deployed Bot Defense as an NGINX plugin in their production Amazon VPC where all account and registration related transactions from any source – web, mobile or API – are analyzed and inspected by CQAI. Deployed out of band to ensure zero impact on user traffic, CQAI is a patented analytics engine that uses 150+ machine-learning-based indicators of automation to automatically discover all of the Zoosk web, mobile and API-based applications. The application transactions are then analyzed to detect automated attacks and if the intent of the transaction is malicious, then those attacks are blocked by a lightweight module that is deployed inline.

Results and Benefits

Zoosk has calculated that on average, romance scams result in $12,000 in theft and untold emotional damage to the unsuspecting victim. With Cequence Security deployed, Zoosk has virtually eliminating romance scams associated with automated account takeovers and fake account creation.

Benefit 1

Reduced infrastructure costs: Blocking automated attacks resulted in lower but higher quality of account signup and login traffic.

Benefit 2

Improved productivity: Security is baked into the application infrastructure, allowing app teams to securely maintain their application update productivity goals.

Benefit 3

Increased user confidence: Romance scams associated with automated attacks are virtually eliminated.

Benefit 4

Brand and reputation is maintained: Zoosk can focus on growing the business; as opposed to battling automated attacks.

CEQUENCE® SECURITY

aws partner network

About Cequence Security

Cequence Security is a Select Technology partner and one of the launch partners for the APN Global Startup Program. A venture-backed cybersecurity software company founded in 2015 and based in Sunnyvale, CA, Cequence Security is transforming application security by consolidating multiple innovative security functions within an open, AI-powered software platform that protects customers web, mobile, and API-based applications – and supports today's cloud-native, container-based application architectures. The company is led by industry veterans that previously held leadership positions at Palo Alto Networks and Symantec. Customers include F500 organizations across multiple vertical markets, and the solution has earned multiple industry accolades, including 2018 Gartner Cool Vendor. Learn more at www.cequence.ai.

aws partner network | global startup