NETACEA / CASE STUDY

Protecting a top ten global video game publisher against account takeover bots

NETACEA

Protecting a top ten global video game publisher against account takeover bots

THE CHALLENGE | THE SOLUTION | THE OUTCOME

CUSTOMER PROFILE

- Top ten video game publisher
- Turnover of $2billion+ and global headcount of 5,000+
- Nearly 500m games sold worldwide

RESULTS

- Sophisticated, distributed “low and slow” attacks mitigated using machine learning techniques
- 75 malicious login attempts detected having bypassed two other layers of security
- Discovery and profiling of credential stuffing tool built specifically to target the client’s login page

THE CHALLENGE

The client is a top ten global video games developer and publisher, with over 5,000 employees around the world. They are known for releasing some of the best-loved video game franchises dating back nearly 50 years.

The company offers its customers added value via an online membership, where gamers can access account services and purchase additional content. These accounts store not just payment information like card details, but also credits and in-game assets.

These assets make user accounts a prime target for criminals. Just as with bank accounts, crooks use sophisticated methods such as advanced account takeover bots (automated programs) to gain access to these accounts so they can spend, transfer or compromise the credits held in them, or steal payment details to use elsewhere.

The business was set to launch an exciting new franchise from a popular entertainment brand, raising their public profile – and attracting attention from fraudsters looking to exploit their growing user base. With the new series of games attracting a younger customer base, many of whom may not take password hygiene seriously, the business needed to ensure their user accounts platform was as secure as possible.

Although they were already using a Web Application Firewall (WAF) plus a client-side security layer built in-house, they wanted a frictionless security layer against malicious account takeover attacks, which Netacea’s agentless bot protection uniquely provides.

THE SOLUTION

Netacea provided an agentless implementation for its advanced bot management solution, which identifies a wide range of sophisticated bot attacks including credential stuffing and fake account creation.

The client’s central database is used by all players to authenticate logins across over 200 games. All requests made to the user login page via web, mobile and API were fed directly into Netacea’s data pipeline, before being processed through the Netacea Intent Analytics™ engine to identify bot activity. Because Netacea Bot Management collects data from the server side, even console endpoints could be monitored, not just browser-based requests.

Netacea’s Intent Analytics engine used a variety of machine learning techniques to build a unique profile for each visitor and their interaction with the system (where they come from, how they identify themselves and what activity they have undertaken) as well as profiling the aggregation of all visitor activity. This enabled Netacea to identify known bad actors as well as attack patterns.

ABOUT NETACEA

Netacea provides an innovative bot management solution that solves the complex problem of web scraping and malicious bot activity for its customers, in a scalable, agile and intelligent manner, across websites, mobile apps and APIs.

Our Intent Analytics™ engine is driven by machine learning to provide an in-depth analysis into all traffic to your site. This gives us an incredibly fast and comprehensive understanding of human and automated traffic behavior, enabling us to identify and block bots in real time with unparalleled accuracy.

With machine learning at the heart of our approach, our technology provides an innovative and profoundly effective solution that is configurable to your environment and adapts to changing threats.

FREE TRIAL

Find out how Netacea's unique approach to bot management can help your business keep bad bots at bay. Get a personalized demo of Netacea Bot Management for your business and get control over your website traffic.

THE OUTCOME

In a short period of time, Netacea's Intent Analytics engine identified 75 successful breaches of user accounts by account takeover bots. This is significant as the bots showed a high level of sophistication, avoiding a volumetric approach in favor of a "low and slow" strategy to bypass two other layers of defense, before being successfully detected by Netacea Bot Management.

Attack overview:

- 2,655 malicious login attempts flagged (1.3% of total login requests)
- Flagged requests distributed between 65 datacenters, 185 IP addresses and 15 countries
- 75 successful logins by bad actors identified

The malicious login attempts originated from various datacenters, IP addresses and user agents, as well as being rotated from multiple countries (China, Russia and Indonesia being the most common). Although this distribution was likely to be an attempt to mask the malicious activity, and managed to fool two layers of security, these attacks were successfully identified and verified using Netacea's patented Intent Clustering technology.

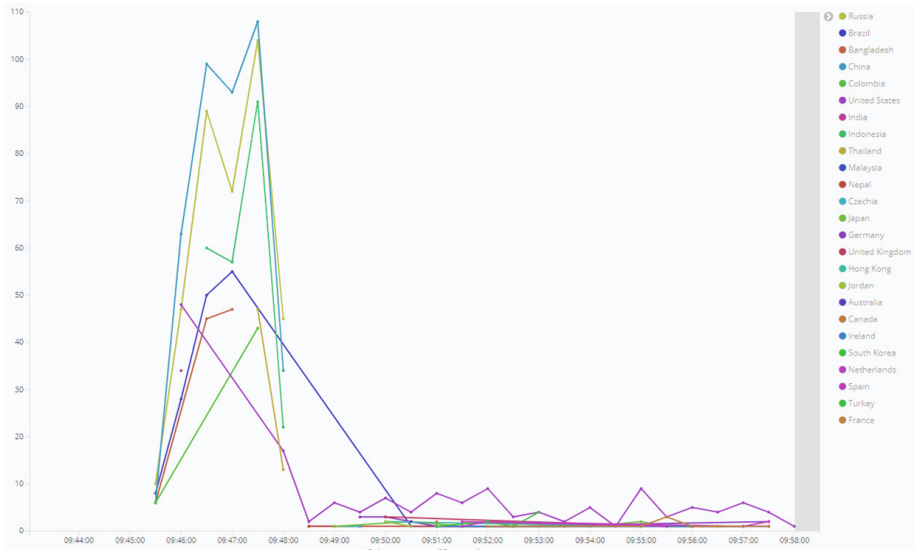

Fig 1: Malicious login attempts identified from multiple countries

Netacea's Bot Experts performed further analysis on the traffic, delivering actionable recommendations to the client. All results were passed into the client's SIEM solution via a direct integration with Splunk, allowing the business to quickly take corrective action, from resetting passwords through to enforcing multi-factor authentication.

Netacea's Threat Research team also uncovered and profiled a credential stuffing tool available online that was specifically built to target the client business's accounts login page.

Netacea's advanced, agentless bot management technology categorized incoming traffic instantly using finely tuned machine learning techniques. Augmented by a team of Bot Experts and Threat Researchers, Netacea Bot Management identified sophisticated attacks that the client's WAF and custom-built client-side security layer missed.

Without mitigation, such breaches could lead to the loss of customer data, including payment details, credits and in-game assets. This negated a potentially damaging financial and reputational fallout during the launch of a new game franchise.