INDUSFACE™

CASESTUDY

Mitigating Targeted Browser-Based Bot Submission Attacks

SOLUTION HIGHLIGHTS:

- Over **200,000** false **insurance claim submissions were blocked**
- **Bot attacks from 100,000+ IPs/Day and browser-based automated tools**
- Deployed AI-recommended, time-based rate-limiting measures to block hackers from submitting forms at **abnormal rates**

ABOUT THE CUSTOMER:

The customer is a decade-old firm based in California, USA, specializing in legal, fiduciary, and administrative services. They specialize in Corporate Restructuring, Mass Tort, Settlement Administration, and Trustee and Fiduciary Services.

KEY CHALLENGES:

- The behavioural AI model found anomalies with the “Insurance Settlement Administration” page, where a hacker was persistently submitting bot-driven insurance claims
- This was relayed out to the customer in real-time to check the veracity of the findings. The customer confirmed and noted that this could have resulted in hundreds of thousands of claim submission requests flooding the system in a short time, making it difficult for employees to process claims and identify legitimate requests
- The hacker had carefully designed the bots to mimic human behavior, filling out all required details on the claim page accurately
- Additionally, identifying the bots was challenging because they were deployed through browser-based automated tools rather than command-line interface (CLI) tools
- The hacker utilized over 100,000 IP addresses, submitting more than 200,000 claims
- The attack evolved every day and the rules had to be tuned regularly while eliminating false positives

SOLUTION:

The customer already used the behavioural bot module on AppTrana WAAP.

Once the anomaly alert triggered, the 24/7 SOC team took a quick confirmation from the customer and deployed the mitigation mechanisms.

The summary of the mitigation approach includes:

- Deploy a very low tolerance for requests per URI. Any URI exceeding this threshold was blocked
- Any signs of malicious bot activity-regardless of tools, geography, or device-were met with CAPTCHA or tarpit challenges first, and if suspicious behaviour persisted, users were blocked for extended periods
- Accept traffic solely from the geographical locations where insurance claims were permitted, blocking requests from all other locations
- Deploy time-based rate-limiting rules to block any user who filled out the form at a significantly faster rate, calculated by the behavioural AI model, than normal or submitted multiple forms within a specified time-frame
- Prevent the exploitation of any business logic vulnerabilities in the claim process, ensuring that user input-from insurance numbers to other details-was more specific and unique

The AI model on AppTrana WAAP continuously evolved with the hackers' methods and the attacks stopped within a couple of days.

This is a classic case of human (Indusface 24/7 SOC and customer's DevOps team) and AI (behavioural bot module) working together to ensure that attacks are thwarted with minimal false positives.

AppTrana successfully blocked over 2 million targeted attacks, leading zero cases of false claims registered on the customer's site.

RESULTS:

- Over **2 million attacks blocked** in a couple of days
- Prevented potential losses of hundreds of hours and thousands of dollars lost in processing fraudulent claims
- Achieved **zero false claim submissions** with AppTrana WAAP
- Strengthened security measures, reducing vulnerability to future attacks