INDUSFACE™

CASESTUDY

Mitigating Carding Attacks for a US-Based Leading Jewellery Company

SOLUTION HIGHLIGHTS:

Carding attacks were carried out from **varying IP addresses**

16,000+ attacks using stolen credit card details were blocked

Human-mimicking bot attacks

"Zero" fake **orders** punched

KEY CHALLENGES:

- The customer faced persistent and frequent carding attacks (also known as credit card stuffing/card verification attacks) on their application.
- A carding attack is an attack where attackers **use stolen/fake credit card information** and try to make online purchases.
- Similarly, in this situation, the attacker(s) utilized multiple bots to enter fake/stolen credit card details, randomly generated fake email addresses, and tried to make a purchase.
- A worrisome concern for the customer was that by using this bot automation, the attacker could even place around **15 fake orders** from their site by following this process.
- While the orders didn't go through, the jeweller was facing the risk of getting blacklisted by 3rd party payment providers for the volume of fake orders
- In the event of a successful blacklisting, the jeweller faced potential losses of hundreds and thousands of dollars per day

STRATEGY & RECOMMENDED SOLUTION:

- The customer contacted the Indusface team and was able to deploy the AppTrana solution within 60 minutes of the request
- The **AI engine** of AppTrana was immediately activated to find any anomalies in the incoming traffic
- Within a few minutes, the AI engine identified a **unique bot pattern in the traffic that appeared to mimic human behaviour** (and had unique IDs and cookies associated with them). This indicated that the bots were not generated by standard automated tools but were browser-based bots designed exclusively by the hackers.
- These bots executed all processes and functions just like a normal user, from selecting a product to making a payment, making it difficult to differentiate between normal users and hackers.
- The attacker even made sure to use different IP addresses from various countries during each attempt, further complicating detection efforts.
- The AI engine tracked user behavior and identified patterns of the bot attacks based on historical data, highlighting **randomizations in parameters such as Bank Identification Number (BIN) and credit card details.**
- Following the AI engine's recommendations, the managed services team deployed custom rules to monitor and block any users attempting to alter standard parameters linked to the carding attack.
- It was ensured that any parameter deviations made by the user for up to a specific number of attempts within a specific time frame were logged, and all the attempts exceeding those attempts were blocked.
- AppTrana's AI engine ensured that IP addresses (series) used for the carding attacks were blocked to prevent further access for a defined period
- Furthermore, if the user/attacker belonged to a geolocation where the customer had no scope of doing business, then the AI capability of the AppTrana WAAP blocked such requests immediately.
- All the above rules were deployed within a **48-hour time** frame, while working with the customer to continuously remove false positives
- In spite of the reduction in attacks, Indusface's 24*7 managed services **constantly monitored the AI-suggested tuning recommendations** and adjusted the defence mechanisms on an ongoing basis
- Since the deployment of the AppTrana WAAP, the customer has punched **zero fake orders due to carding attacks** over the past year.

RESULTS:

- **Successful mitigation of carding attacks** within 48 hours of request
- Significant reduction in fraudulent transactions and **zero fake orders**
- Regained **control over the brand reputation**
- Efficient and **quick response to prevent disruptions** caused by carding attacks