INDUSFACE™

CASESTUDY

Nullifying Targeted DDoS Attacks on a Canadian Auto Giant

SOLUTION HIGHLIGHTS:

- An automobile giant's website was brought down in **a 3-step DDoS attack** by an anonymous hacktivist group.
- The website downtime led to **losses** of hundreds to **thousands of dollars** for the company
- WAF/WAAP with **core + custom rules** (user-level tracking, honeypots, anomaly policies and more) provided **advanced protection from DDoS attacks** and the business faced 0 downtimes in the past year

Customer Testimonial

"We have entered an era in which cyber-attacks can be more than disruptive and expensive. Investing in decent WAF DDoS Protection can save you time, money and frustration down the road."

- CISO

KEY CHALLENGES:

- A Canadian automobile giant faced a severe DDoS attack threat orchestrated by a determined hacktivist group
- The attacks disrupted the business's online operations and posed significant financial risks, potentially costing the company thousands of dollars.
- The attackers, identified as Anonymous, employed a multi-stage strategy to launch DDoS attacks that led to downtime
- This Anonymous hacktivist group launched the DDoS attacks in 3 major steps.
    - **Prestrike Doxing:** At this stage, the attacker sends a threatening message attributed to an anonymous person, demanding money from the customer by sharing some stolen customer details.
    - **Slow DDoS Attack:** Over the course of a week, the attacker regularly threatened the customer by targeting their website with a slow DDoS attack, leading to the site's slowness and irregular availability.
    - **Large DDoS Attack:** In the third step, the attacker blocked the website access completely through a direct high-volume DDOS attack.
    - After the last attack, the **website went down & the customers started losing deals running through their online portal application.** Here are some of the major effects faced by the customer after the DDoS attack:
    - Inability to reach the client-server during a DDoS attack.
    - Unable to receive customer information from the dealerships through their online portal.
    - Inability to publish new deals/offers & for the clients, as the clients cannot visit the site and perform any payments or transactions.
- This spoilt the customer experience and led to too much inconvenience for the dealers as the attacks were targeted for over a week.
- The customer tried to block these attacks with their internal firewalls but couldn't scale with their solution and felt the urgent need for a cloud-WAF solution with better detection and protection capabilities.

STRATEGY & RECOMMENDED SOLUTION

After understanding the above attack details, Indusface immediately deployed Apptrana WAAP/WAF in block mode and provided threshold-based protection with the default/core rules, which reduced the attacks by 60%.

For complete protection, the below-mentioned custom policies were deployed to protect from the DDoS attack:

- As the customer had the immediate need to make the website available during the downtime, AppTrana Cloud WAAP was made to **auto-scale for the incoming traffic.** This made sure that the business started running again smoothly.
- As a next step, the inbuilt **rate-limiting** with auto-suggestion of limits was enabled to control the frequency of requests by a user. This ensured that the attacker, even using multiple nodes/user agents, could make only a few requests, and each request was blocked quickly.
- Apptrana also performed **IP reputation checks** and blocked anything that was marked malicious as per our threat intelligence database.
- Further adding to the security levels, the solution provided advanced protection, including policies such as **user-level tracking, honeypots, advanced input validation, and anomaly policies.**

With the combination of all the above layers of defense, Apptrana WAAP made sure that the site was continuously running and mitigated all sorts of attacks in the run-time.