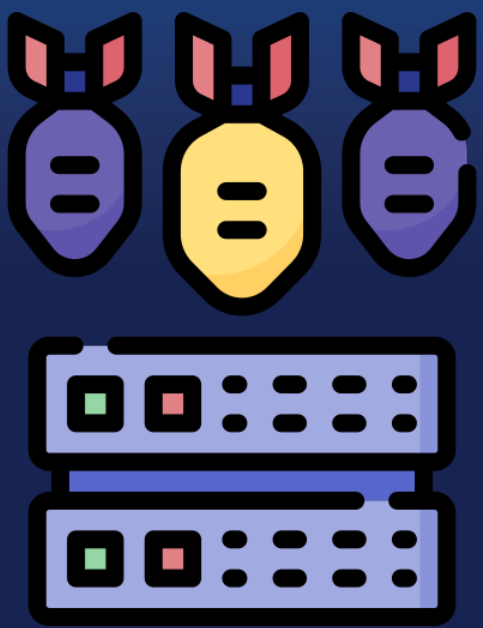


DDoS Mitigation

Overview

One of our prospect contacted Prophaze Technologies regarding their high bandwidth utilization and unavailability of their servers randomly. The client needs to processes thousands of requests prior to weekends. Server down time is a critical issue which comes under the three security pillars (CIA triad). As per the discussion with their prospect IT support Team, we got an overview of the incident.

Offenders were trying to hit the servers with thousands of requests from different IPs which makes their servers down on Fridays at the business peak hours. After analysis, we also confirmed that this was done using the bots.

Prophaze cloud security platforms offers protection from bots with the AI- based Behaviour detection. Then we on boarded the prospect for a pilot session for 2 days. Success criteria of the pilot is to mitigate this specific attack and Prophaze was successful in mitigating this attack.

The Challenges that they experienced

The security challenges includes HTTP flood attacks and DDoS attacks that takes the website down. The attacks are done using malicious robots. The prospect requires protection against bots that could flood the website traffic.

The Prospect suspected that they were under bot attack. But they were not sure, into what level of HTTP request traffic was real versus that generated by bots. This creates a troublesome to analyse a legitimate user's traffic on their sites.

BOT Protection and scalability are the important things that they were looking for. The prospect chose Prophaze Kubernetes WAF because this offers the security and scalability as the company expected. Knowing how critical web application security is to the fabric of their business, they need protection against potential attack factors.

The Results

Our Kubernetes WAF solution has the ability to meet the challenges the company faced:

1. Our products and services help them to analyse, do inbound/outbound content analysis, compliance and powerful policy configuration into a single solution.

2. We tend to leverage known-bad IP lists to go with our proprietary Parsing technology, to form quick, inline decisions to identify and block malicious requests.

3. Provides a lot of innovative approach to automatic detection and blockage of potential attacks in production environment

4. Increased security against malicious activities and is up-to-date on securing itself against IP offenders and they are automatically blocked.

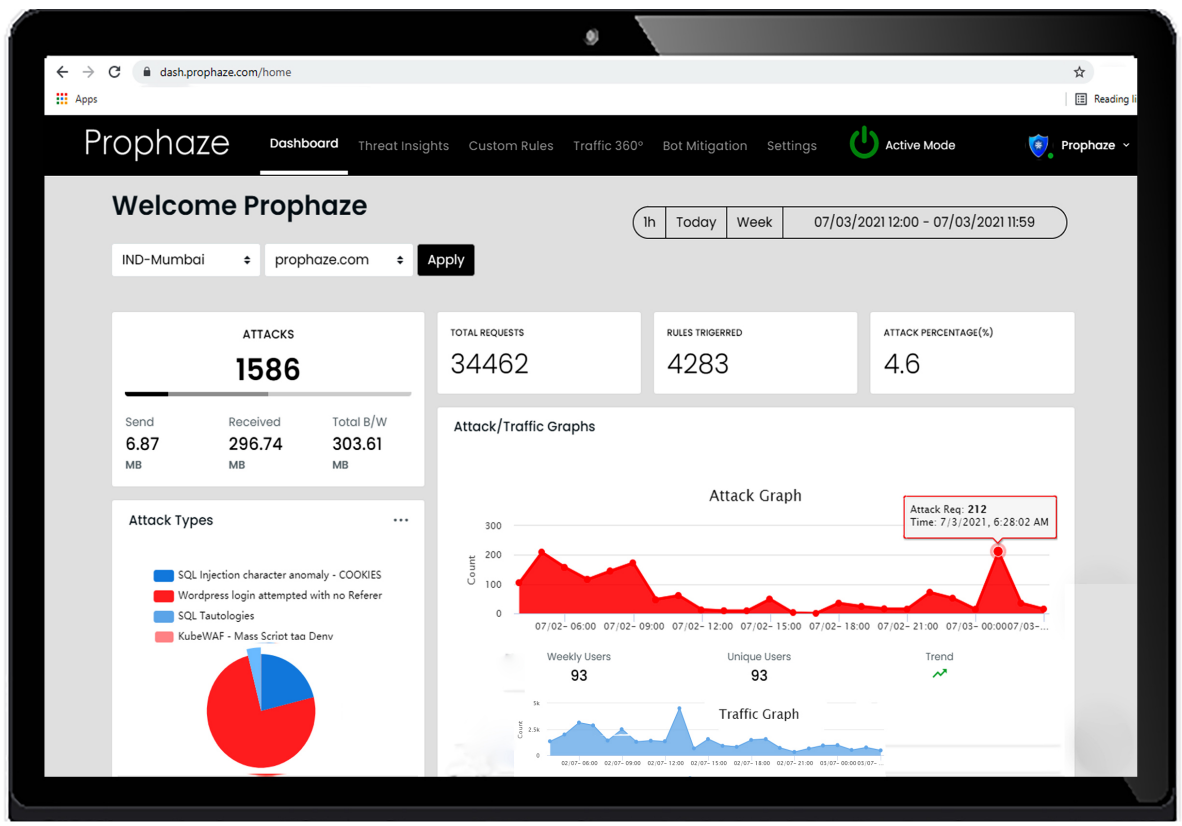
5. Automatically scales to handle its increased security needs and reliable security without the false positives.

6. The protection is much easier, better and scalable.

7. Delivers faster incident-response time

8. Provided scalable performance and centralized visibility into traffic and attacks at the web attack layer

Advanced Dashboard



Real time Reports