Stopping Bots & Malware with Anti-DDoS

haltdos

Let's take a peek into how an industry leading Finance Bank for Infrastructure development blocks malware and bots with HaltDos' DDoS Mitigation Solution

What happens when one of the leading banks becomes a victim of network and low & slow DDoS attacks leaving its online banking fried and end customers frustrated during the peak of COVID-19 pandemic and country lock down?

Well, such was the case who chose Haltdos Anti-DDoS solution to ensure 24×7 uptime for their online infrastructure. But this case study is a testament to ingenuity and forward thinking on part of the bank to make efficient and effective use of existing resources to maximize defense against growing cyber attacks on Banking Industry.

For sake of anonymity, lets call this bank – “Smart Bank”

Findings

On installing Haltdos’ Anti-DDoS solution, the situation became clear. In Haltdos, we created multiple rules to count the number of packets of established TCP connection with varying payload size belonging to TOR exit nodes and bad IP reputation IP addresses.

The following were the rules:

1. Monitoring Frequency of packets with payload in range 1-50
2. Monitors the frequency of TCP packets with payload in range 51-100
3. Monitor the frequency of connections packets with payload in range 101-200
4. Monitors the frequency of connection packets with payload in range 200-300

These rules confirmed:

Low and Slow DDoS Attack: The solution observed continuous Low and Slow DDoS attacks that started to peak during the end of the month until mid of the first week of the month.

Continuous Bot Activity: During the same period, there was heightened Bot activity with automated traffic though we noticed continuous bot activity throughout the month.

Solution

The solution was as simple as putting anti-DDoS in Mitigation mode with Machine Learning enabled. The solution started blocking all Low and Slow DDoS attacks and blocking malicious IPs and TOR exit nodes.

Completing the Loop

While the problem of attack on online banking was stopped, Smart Bank CISO got a brilliant idea. DDos mitigation solution works in transparent mode at the very edge of the network. This means, the CISO now had a solution to block any unwanted traffic before it even entered the network.

The SOC team at the Bank was already tracking malicious IPs trying to spam, malware or infect Bank’s infrastructure – including BYOD devices (as most employees were working from home due to COVID-19 Lockdown). Using Splunk, the SOC team started pushing all the discovered malicious IPs trying to attack the Bank and feeding them into Haltdos solution.

With a little bit of customization, Haltdos put these feed of IPs on high alert watch list and started blocking them IPs upon misbehavior.

This completion of the loop by taking events from various security solutions and feeding into Haltdos solution became an ingenious way to block attacks at the Edge and ensure smooth business operations.

While we detected multiple attacks including Network DDoS attack, the attacks were automatically blocked by Haltdos solution. We discovered more than 60,000 new IP addresses that were not in any threat intelligence feeds. The Bank SOC team alerted the authorities on the discovered malicious list and are continuing to do so – a few thousand every month since then.