Bi-Directional DDoS Protection

What happens when you become the source of DDoS Attacks

Managing a large data center involves multiple operations. Sometimes, however, you end up finding yourself as a victim of cyber attack.

If you want to block all traffic from North Korea or Iran, that's easy with a simple Geo IP rule. But what if the attack is originating on your own turf or from your friendly neighbors?

State sponsored cyber attacks use this approach to perpetrate their attacks. State sponsored hackers infecting systems not to attack your IT network but to piggyback on your data center resources to launch attacks to other targets.

This case study talks about how Haltdos solution uncovered a covert operation using a Government Data Center to launch attacks on Banks and Enterprise of the country.

The Problem

The problem started when the IT Security team approached Haltdos informing that the Data Center's IP addresses have been blacklisted by ISP for perpetrating the attack. Despite trying hands with the firewall, the Security team could not figure out what might be going wrong.

As an auditor and OEM, Haltdos team inspected their network and found many inconsistencies and vulnerabilities, which indicated infection in some parts of the network. But the urgent problem was – all websites hosted in the Data Center were down – a new kind of denial of service!

Observation

We quickly deployed Haltdos anti-DDoS solution in the network and started observing. We noticed bursts of high volume attack originating from within the network to different targets – sometimes bank and other times, enterprises.

Haltdos anti-DDoS solution is a bi-directional solution – i.e. it can detect and mitigate attack originating from the Internet or some compromised machines within the network. Depending upon its placement, the solution can also determine infected IP addresses within the network launching the attack.

After initial few days of observation, we put Haltdos in mitigation mode. We observed the following:

1. **Midnight attacks:** On 5 consecutive days, Haltdos detected 5 DDoS attacks from four compromised machines launching simultaneous attacks exactly at 5 minutes past midnight. In a data center of 1 Gbps lease line, the highest attack was over 600 Mbps.
2. **Malware Identification:** On identifying the compromised machines, we inspected and found malware that was taking commands from a VM in Amazon Web Services (AWS). All the four machines were desktops running old unpatched version of Windows XP – but were not taken out of the network.

Mitigation

The mitigation was straight forward – deploy anti DDoS solution in Mitigation mode with Machine Learning enabled. The infected machines were first patched and then put back into the network.

Attackers soon realized that their bot network was breached. Soon, the VM in AWS was taken down and over the course of the next few months, multiple DDoS attacks occured – this time from the Internet; as a show of anger. Luckily, Haltdos auto-pilot detected and blocked the attacks without requiring any human intervention.

Summary

The IT security team used multiple security solutions (Firewall, IPS / IDS, Anti-virus, etc) but lacked visibility into the network. Firewall misbehaving, IP blacklisting were all symptoms of infected machines that came to light only with visibility.