DDoS Testing Case Study

Public Utilities: Middle East

DDoS attack simulation uncovers ISP mitigation failure and misconfiguration of on-LAN WAF

Introduction

Our client is a public services infrastructure company located in the Middle East.

In order to protect their critical online assets, websites and data centre, the organization had invested in cloud-based, always-on mitigation - provided as a managed service by their Internet service provider (ISP).

Our client had previously experienced DNS-based attacks which they had failed to mitigate. As part of normal operational procedure, the utilities company sought to test the capability of its mitigation service as well as its on-premise web application firewall within a single 120-minute maintenance window. This would test their ability to repel a range of Layer 3, Layer 7 and DNS-based attack types and confirm their capacity and capability to continue operation in the event of a real attack.

The mitigator, a market leader in the ISP market, was not made aware of the DDoS test in advance of the procedure.

The task

Our client was initially unsure of attack types and targets to be tested. Following consultation, activereach proposed a series of 6 tests including application, volumetric and DNS based attacks, designed to stress different aspects of their mitigation service, DNS servers, web servers and firewall.

A 2-hour test window was allocated to deliver 104 minutes of attack traffic against 3 different targets. In order to accurately simulate traffic in the wild, 4 botnet armies were utilized covering 120 bots across 21 different global geo-locations.

Test Duration

- 120 minutes, conducted outside normal operational hours at 22:00 GST

DDoS Attack Simulation

- HTTP Slow Post
- Randomised DNS Request Flood
- UDP Flood
- Dynamic HTTP Flood
- ACK Flood
- Tsunami SYN Flood

Test Sequence

- 6 individual tests including a blended attack

The Testing Platform In Operation

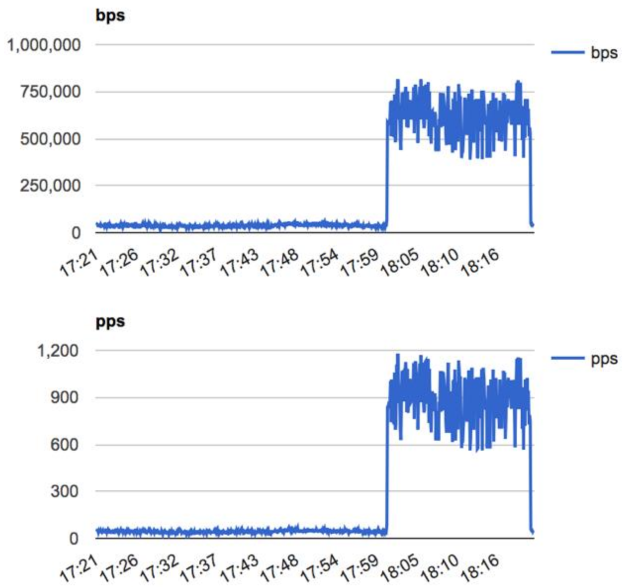

Fig 1: HTTP Slow Post Attack: A small volume DDoS attack can still have a significant impact on connected services.

> **“Almost immediately it was discerned that no mitigation alerts were being sent to the customer and the ISP did not detect the attack.”**

The test

Starting with a gentle **HTTP Slow Post attack** (screenshot above) the client’s server did not appear to be unduly affected. However, the SIEM was overloaded with event logs and was at risk of “falling over” as a consequence of the attack on part of their infrastructure.

Testing moved to a **DNS Req Flood** which caused the DNS Server to stop responding. The mitigator saw the attack but reported it as a false positive. Furthermore, other hosts in their subnet were brought down by the attack.

The third test involved a **UDP Flood** on a dedicated website. The site became slow before becoming unavailable. Almost immediately it was discerned that no mitigation alerts were being sent to the customer and the ISP did not detect the attack.

Tests four and five were deliberately run at the same time in a **blended attack** on multiple layers of mitigation. Test 4 was a **Dynamic HTTP Flood** which sent random URL requests to the main website. This was NOT detected by the ISP or WAF – which we would have expected to flag either the returned 404s or the increase in the rate of connections. In test 5, an **ACK Flood** caused severe over-mitigation bringing multiple websites and the VPN down. This was a severe failure on the part of the ISP which neglected to spot the specific attacks or issue alerts.

Finally, a **Tsunami SYN Flood** completed the test sequence. In response, our client dropped all traffic from outside of the country. Although traffic was blocked it still looked like a “successful” denial of service to the outside world.

Result summary:

The test highlighted some real concerns for our client with the failure of their Internet service provider to recognise or report the attacks. In addition, the mitigation service neglected to stop a number of the attacks and in some instances caused “bystander fallout” of unintended targets on their network.

Metrics & Reporting: Every operations member in the live test team was provided with a login to the dashboard displaying attack traffic. Notes were taken in real-time, allowing the test team to record discrepancies as they appeared.

Recommendations: Although our client had invested in advanced telemetry techniques, suggestions for further analysis and parsing of traffic logs were made. In addition, measures to implement real-time alerting to relevant internal staff for emergency incident escalation were recommended. Finally, it was recommended that our client engage with their ISP to understand why their protection services had failed.

Next Steps: A second round of tests is being scheduled further to implementing the recommended changes. The tests will be run at least once a year for a ‘main-test’ of each 3rd party mitigator, followed by re-tests to ensure that any deficiencies have been addressed and that test coverage extends to all critical targets.

As security best practice, even if compliance does not dictate regular DDoS testing, it can be a strong indicator to auditors, investors and customers that a company takes its responsibility to service availability very seriously.

Raza Rizvi, Technical Director activereach, commented:

“Whilst our client was better prepared than most, they were let down by their mitigator and the misconfiguration of their on-premises WAF.

They were surprised that their Internet service provider did not provide the protection they needed, and were paying for. Now armed with the DDoS test results and a comprehensive report they have a good baseline for more targeted simulations in a subsequent round of testing.”

For more information call 0845 625 9025, email contactus@activereach.net or visit our website www.activereach.net

Ref: CS.CNIME.2019.1