DDoS Testing Case Study

Dutch Retail Bank

DDoS testing exposes critical mis-configuration error in managed service provider mitigation set-up

Introduction

Our client is a leading and relatively new retail bank, with more than 500 thousand customers, operating principally over the Internet. Primarily based in the Netherlands, the bank also has operations in many other European regulatory areas.

The bank has several data centres each with a common ISP that also provides a managed DDoS mitigation solution based on Arbor equipment.

As part of normal operational procedure it sought to test the capability of each data centre within a single long maintenance window. This would test both the ability to repel a range of DDoS attack types and confirm whether it had the ability to continue operation to Internet based customers in the live active: active configuration it had adopted.

With a significant monthly sum being spent on mitigation, as part of a long term contract, a DDoS test programme was critical to help validate this investment.

The task

The mitigation solution on test was an on-premise, LAN based, traffic pass-through, with in-Service Provider cloud flood protection.

The managed service provider was notified ahead of time that a simulated attack was to take place but not given details of the attack parameters.

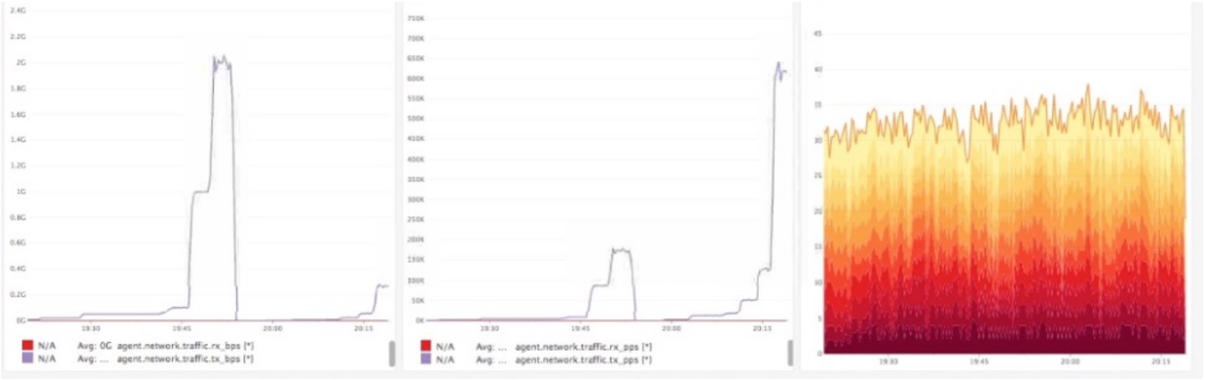
Testing was done to a test VMWare image at each data centre which mimicked typical Internet services but with traffic passing across the Internet from the multiple test nodes to each data centre.

Test Duration
Six hours, starting at 00:00 CET

DDoS Attack Simulation
Layer 3 TCP & UDP, and Layer 7 HTTP/HTTPS attacks were deployed to a customer selected maximum of 2Gbs, ramped up over the test cycle

Test Sequence
First test cycle complete. Further test cycles scheduled Q3 2016

The Testing Platform In Operation



The test

Starting with a UDP based attack, almost immediately it was discerned that no mitigation alerts were being sent to the customer and as traffic levels increased it was apparent that no mitigation had been brought into play by the service provider.

Our customer called their service provider who confirmed that this was due to a mis-configuration on their part. This was rectified but importantly the fix was not adopted by the service provider to the other data centres until a further request was sent by our customer.

Testing moved to a TCP based pattern and it was clear that the service provider had been using a simplistic strategy with IP based blocks since probes showed the target traffic was not seen. The agents were moved to a different geolocation and the attack traffic easily bypassed the mitigation equipment. The service provider SOC was not able to confirm whether mitigation was active and what blocking strategy was in place.

HTTPS GET tests showed the on-premise devices being unable to determine whether to block or pass the traffic. The devices were not able to consistently report their mitigation status in real-time. The device did build an IP based blacklist but the managed service provider SOC was unable to clear the blacklist on request.

Final tests with TCP SYNs showed good mitigation and alerting but the last test with a UDP payload showed inconsistent blocking by protocol with no marking of the originating IP addresses as suspect for other forms of traffic. This allowed a lower volume HTTP attack from those same agents to pass without mitigation, albeit that alerts were sent for the UDP component.

Whilst the customer data centre hosted banking sites were slowed or made unavailable due to the traffic volumes, the test had been designed to attack a single data centre at a time so some customer service was still available even through the maintenance window.

Result summary:

There is naturally an expectation of competence, safety, and security from the customers of a financial institution. The risks of reputational loss are of paramount concern if an impact to operations as a consequence of a Denial of Service becomes public knowledge.

Metrics & Reporting: Several recommendations were made by activereach as a consequence of the tests. During smaller volume attacks, and with on-premise equipment that has been properly tested, it is reasonable to expect there to be automatic mitigation. However, and as a matter of course for larger attacks, there must be real-time alerting to internal staff of the occurrence of the attack so that the relevant internal procedures can be adopted.

The accuracy of the reporting from the on-premise equipment during the attack was, at best, questionable, and in some tests, wholly inaccurate.

Changes Implemented: We advised the customer that their service provider should be using blocking by network range as the last resort because of the likelihood of false positives. Tuning and testing of the mitigation process on these on-premise devices is the best way to have a predictable outcome, and familiarity with the interface was a necessity within their service provider.

The fact that the service provider SOC could not provide information on the nature of blocking, or whether mitigation was actually occurring, is unacceptable in a managed service.

The customer accepted that their own external monitoring of access to banking applications needed to be changed as a result of the tests. We also advised further internal monitoring of key statistics that might provide valuable insight into the initial ramping of an attack.

Raza Rizvi, Technical Director activereach, commented:

“Every DDoS test shows something different to the customer. In this case, it was a long test but with a well-defined plan to test similar multiple environments with a customer that was confident they had protection for their Internet facing service.

They were surprised that their managed service provider did not provide the protection they needed. Now armed with the test results they had the basis to ensure that the protection they needed, and indeed were paying for, was put in place, correctly.”

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