activereach helps global information provider put on-premise DDoS mitigation solution to the test

Introduction

The British Library is a world-renowned UK government organization that serves information to businesses, researchers, academics and students. With a growing amount of that information being provided online, the global reputation of the organisation is increasingly at risk from online attacks - particularly Distributed Denial of Service (DDoS).

Our customer had recently deployed an on-premise DDoS mitigation appliance to protect critical IP assets. These assets were held within multiple data centres each with separated high capacity Internet links. This mitigation solution represented a significant investment in protection against the threat of DDoS, but the system was unproven in the deployed environment and its performance under attack had not been verified.

The key objective of doing a DDoS attack test was to validate the operational effectiveness of these mitigation devices under a real attack scenario.

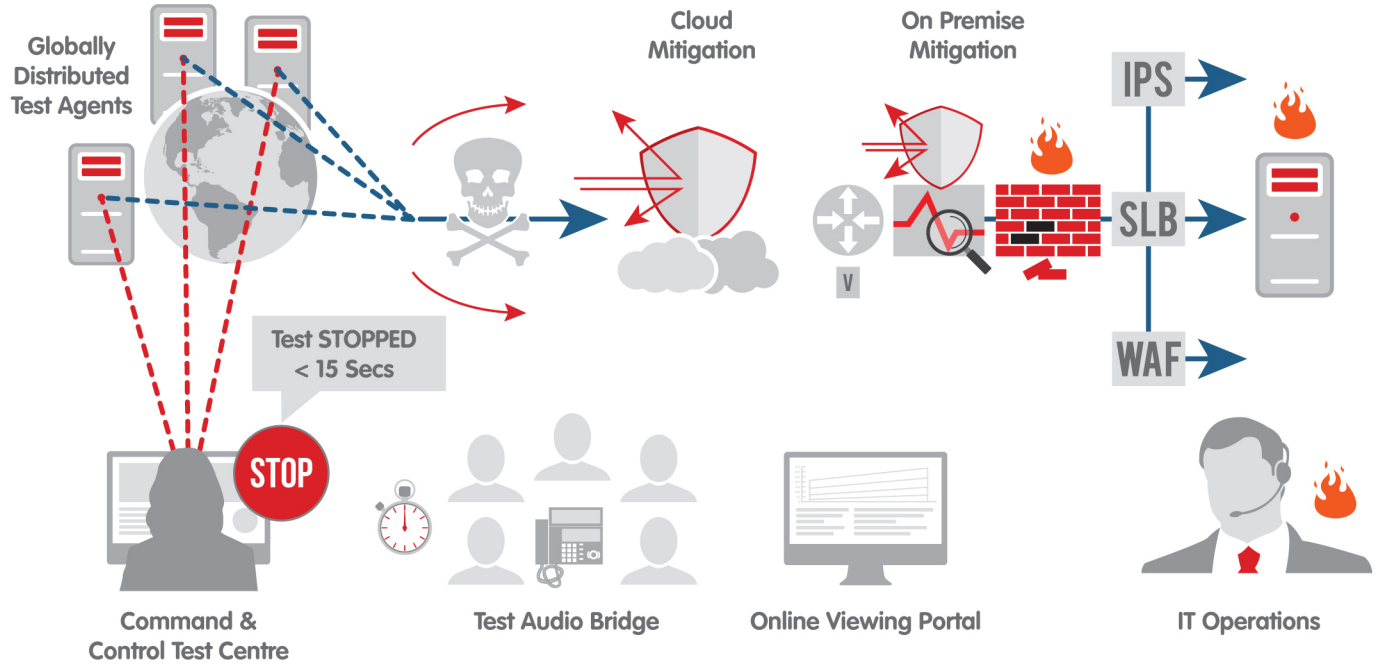
The task

activereach was selected as the supplier of choice to provide a number of 90 minute DDoS tests. The duration of the tests ensured they could be conducted inside normal maintenance windows. Running multiple tests meant that the mitigation could be tuned between tests, and the improvement in security posture measured. Once NDAs and commercial agreements were completed, activereach engineers conducted a detailed technical consultation phase. This phase establishes a number of key test parameters.

Key Test Parameters

1. Required compliance to code of best practice
2. Test objectives
3. Systems, people and risk assessment review
4. DDoS attack types and parameters

The Testing Platform In Operation



The test

The customer had the option of selecting the DDoS attack types from our extensive library (www.activereach.net/support/ddos-dict/) with our advice to form the test patterns. Whilst bespoke attacks can be created in 3-5 days depending on the complexity of the requirement, this was not deemed to be necessary to test the capabilities of their deployed web and Internet applications. Therefore for this set of tests, the standard dictionary had the ideal attack patterns to demonstrate interesting behaviours from the mitigation systems.

A maintenance window was selected for each test event and publicised internally through the normal change control process. A sacrificial target server was deployed, 3rd party service providers notified and key monitoring points were set up. A test working party was formed of stakeholders from all critical areas of the IT infrastructure and final DDoS types and parameters were confirmed and verified.

On the test date all key stakeholders connected to a live web conference allowing clear communication with the activereach operations team and visibility of the DDoS attack test portal. At any time during the test the customer was very aware that they could activate the emergency stop procedure, halting the test within seconds.

The tests were conducted with three different attack types, and at 25%, 50%, and 105% of Internet bandwidth.

Result Summary:

The tests showed that the mitigation device coped well with a number of the tests; however it also successfully highlighted some scenarios where further work was required within the British Library.

Following these initial tests, the information discovered was used to improve procedures.

A repeat test at a later date confirmed that issues had been corrected satisfactorily.

The overall test results provided significant value to the organization, particularly in the following areas:

- Identification of potential weaknesses
- Preparation of people in the event of an attack
- Indicating improvements to the 'Cyber Attack Run Book'
- Providing a simulated attack scenario that provided management with real data to model business effects

Mark Dawson, Head of Service Assurance, commented:

"We learnt a huge amount as a result of doing the DDoS test simulation. It was better doing this in a controlled manner instead of waiting until we are hit for real. We now understand a lot more about our systems and our people have gained useful experience, which has only improved our readiness for a real attack.

We certainly see the real value of doing this on a regular basis in a similar way to testing our fire alarm system so that people and systems operate under real scenarios efficiently"

activereach Ltd.
4 Cliveden Office Village, Lancaster Road, High Wycombe, Bucks. HP12 3YZ.
Tel: 0845 625 9025 / Fax 01494 980 255 / Email: contactus@activereach.net