RED BUTTON
DDoS Experts

DDoS Testing Report
EXAMPLE

Date: 10.11.2019
Time: 15:00 GMT

Authors:
Amos Jennings, DDoS Expert
Ziv Gadot, CEO

CONFIDENTIALITY & PROPRIETARY

This document contains information that is confidential and proprietary and that shall not be disclosed outside the customer (“the Customer”), transmitted, duplicated, or used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of the Customer is prohibited. Red Button makes no warranty that the information contained in this document is complete or error-free.

This report is solely for the information of the Customer and the Customer’s management and should not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document, without our prior written consent.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Test results

The following table summarizes the test results.

#	Attack Vector	Target	Rate	Result
01	UDP Flood	Router	1Gbps	**PASS**
02	SYN Flood	Website	1M PPS	**PASS**
03	ACK Flood	Website	1M PPS	**FAIL**
04	ICMP Hit-and-run	Website	1M PPS	**PASS**
05	HTTPS Flood	Website	5K RPS 50K RPS	**FAIL**
06	HTTPS Flood	API (REST)	5K RPS 50K RPS	**FAIL**

GENERAL INFORMATION

Checklist

Takes	Owner	Status / ETA
Test Planning Meeting Meet with customer to define test content.	All	Done
Fill Out Test Plan Document Fill out this document (‘Test Plan’ section).	Red Button	Done
Approval Customer to sign low, notify ISPs and hosting.	Customer	Done

DDOS TESTING	All parties	Done
Summary Report	Red Button	Done

Approvals

Company	Person	Approval date
Customer	Mr. [redacted] CISO	[redacted]
Customer	Mr. [redacted] CIO	[redacted]
Red Button	Mr. [redacted], test manger	[redacted]

General details

Test number	001
Test date	[redacted]
Test time	23:00
Motivation	Test vendor

Stop conditions

The test will be stopped at the following points (please select / fill)

Select	Criterion	Misc
✓	Test is over	
✓	Medium or high impact to production	
✓	Low impact that is not terminated as soon as attack terminates	

TEST PLAN

Test objective

The primary goal defines the attack vector and methodology off the entire test.

(select one)	Objective	Description
✓	**DDoS survey**	Map the strength and weakness of the DDoS defense layer, the balance between basic, medium and advanced attacks. Intended to produce a “snapshot” of the organization's ability with respect to DDoS attacks.
	Break-down test	Find any possible weak point that can be attacked. Use advanced attacks even if they are unrealistic or uncommon.
	POC	Evaluate a DDoS product or service.
	QA	Test that a new protection set is mitigated as expected.
	Measurement	Measure the actual capacity of network elements and defense layers

Test methodology

(select one)	Methodology	Description
✓	Free style	Customer and Red Button will define a test that is most appropriate for the customer resources. This methodology allows for the cost-effective surveying of main gaps.
	DRS	The test will follow the DRS (DDoS Resiliency Score) standard. This methodology follows an external objective stand and allows for the quantification of the DDoS posture into a numeric score.

Bots location

The bots can be found at the following locations.

Location	Number of bots
New York	30
San Francisco	30
Amsterdam	30
London	30
Frankfurt	30
Bangalore	30
Singapore	30
Total	**210**

Asset list

The following list describes the assets targeted during the test.

Name	URL/Address/IP	Description	Asset Monitoring
Organization Website	https://[redacted]	The organization primary website	✓
API (REST)	https://[redacted]	The organization API. This is the most critical resource.	✓
Organization router	[redacted]	The IP address of the organization router.	✓

ATTACK VECTORS

Summary test plan table

(by order of execution)

Time (IST)			Attack Vector	Botnet Size	Volume	Target
Hour	**Delta**	**Duration**				
		-00:30	Open bridge Receive GO from all stakeholders			
14:00	00:00	00:00	Test starts			
14:00	00:00	00:15	**UDP Flood**	80	10Gbps	[redacted]
14:15	00:20	00:05	Cool down			
14:30	00:35	00:15	**SYN Flood**	80	1M PPS	[redacted]
14:45	00:45	00:05	Cool down			
14:30	00:35	00:15	**ACK Flood**	80	1M PPS	[redacted]
14:45	00:45	00:05	Cool down			
14:50*	00:50	00:15	**HTTPS Flood**	80	5-50K RPS	https://[redacted]
15:05	01:05	00:05	Cool down			
15:10*	01:10	00:15	**HTTPS Flood**	80	5-50K RPS	https://[redacted]
15:25	01:25		Test ends			

* If time allows

UDP Flood @ Organization Router

Name	UDP Flood against organization router
Attack Vector	UDP Flood port 80
Target	[redacted]
Rate	10 Gbps
Expected Mitigation	Mitigation by ISP
Log	Time Event 14:16 UDP flood started site goes down 11:22 Site is up (6 minutes down) The following sites are also accessible https://employee.[redacted] https://partners.[redacted] 14:35 Stopping the attack
Results	At first the site was down but after 6 minutes ISP mitigated the attack and the site was alive again.

SYN Flood @ Organization Website

Name	SYN Flood against Organization website
Attack Vector	SYN Flood port 443
Target	https://[redacted]
Rate	1M PPS (packets per seconds)
Expected Mitigation	Mitigated by ISP
Log	Time Event 14:45 SYN Flood started sites were slow at first but quickly were fully available 14:50 Stopping the attack
Results	Attack mitigated by ISP

ACK Flood @ Organization Website

Name	ACK Flood against Organization website

Attack Vector	ACK Flood port 443
Target	https://[redacted]
Rate	1M PPS (packets per seconds)
Expected Mitigation	ISP
Log	Time Event 14:50 ACK Flood started Site is down 14:55 Stopping the attack
Results	Not mitigated

ICMP Hit-and-run @ Organization Website

Name	ICMP Hit-and-run against Organization website
Attack Vector	ICMP Hit-and-run
Target	https://[redacted]
Rate	1M PPS (packets per seconds)
Expected Mitigation	Not mitigated
Log	Time Event 15:00 ICMP Flood started No impact 15:01 Stop 15:02 Start 15:03 Stopping the attack
Results	Attack mitigated by ISP

HTTPS Flood @ Organization Website

Name	HTTPS Flood against Organization Website
Attack Vector	HTTPS
Target	https://[redacted]
Rate	5,000 RPS (requests per second) and increasing up to 50,000

Expected Mitigation	None. ISPs are typically unable to mitigate HTTPS because of the service certificate and they cannot scrutinize the traffic.
Log	Time Event 15:14 Attack started Site is slow and even very slow 15:18 Doubling the size of the attack to 10,000 RPS Website not responding 15:25 Stopping the attack
Results	Outage. Attack was not mitigated. At the original rate (5K RPS) site was slow and at in higher rate (10K RPS)

HTTPS Flood @ Organization API

Name	HTTPS Flood against Organization API
Attack Vector	HTTPS
Target	https://
Rate	5,000 RPS (requests per second) and increasing up to 50,000
Expected Mitigation	None. ISPs are typically unable to mitigate HTTPS because of the service certificate and they cannot scrutinize the traffic.
Log	Time Event 15:37 Attack started API not responding 15:50 Stopping the attack
Results	Outage. Attack was not mitigated even at the starting rate (5K RPS)

RELEVANT RED BUTTON SERVICES

Following is a list of Red Button services that may be relevant for the future.

Recommendation	Description	Comments
DDoS Testing	***"DDoS mitigation without DDoS Testing is like software without QA"*** Red Button's DDoS Testing service enhances your DDoS readiness by simulating attacks in a secured, controlled manner. Using proprietary cloud technology, our DDoS test simulation specialists generate multi-vector DDoS attacks and try to breach your defense systems.	Recommend that Ages perform another test as a validation step after recommendations and actions have been executed.
DDoS Consulting	DDoS Architecture and Design Consulting, including DDoS hardening, vendor selection, and basic training.	Ages can use this service if it decides to harden ISP DDoS mitigation or in the case of additional vendor selection.
DDoS Readiness Platinum	An all-inclusive, fully managed DDoS protection program: **Professional services**: assessment, gap analysis, design, POC, game plan, mitigation technology review and selection, integration, procedures, training, DDoS simulation, war game, emergency response. **Dedicated DDoS engineer**: 10 full days per quarter. Software-based services: DDoS testing (unlimited), DDoS monitoring (unlimited), DDoS protection status page.	Ages should use this if it wishes to be fully ready for DDoS attacks and to reach a score of 6.0.