LODDOS

2018 Corero Trends Report

- 95% of the DDoS episodes performed are 5 Gbps or less in size. The rate of attacks on 10Gbps is 2%.

NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report

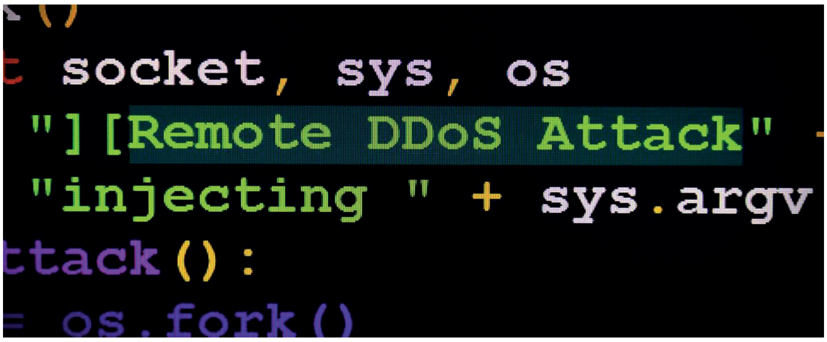
- 75.7% of the DDoS attacks performed are volumetric attacks.
- End Users, Financial Services, Cloud Services, and Public Services are the targets that are subject to DDoS attacks respectively.
- The cost of a successful DDoS attack on the target organization varies between $10,000 and $100,000

WHY TO PERFORM DDoS TESTS?

Generally, DDoS tests are performed to measure the efficiency and limits of the DDoS prevention products and services, and to improve these systems, as well as to measure and improve the efficiency and capabilities of the organization in case of a DDoS attack.

DDoS prevention systems and products are not plug-and-play systems; Organization's normal and abnormal network traffics, baselines and thresholds must be defined.

To define them correctly, engineers should test services protected against an actual DDOS attack and current solutions on the market are way out of being the tool needed for the job.

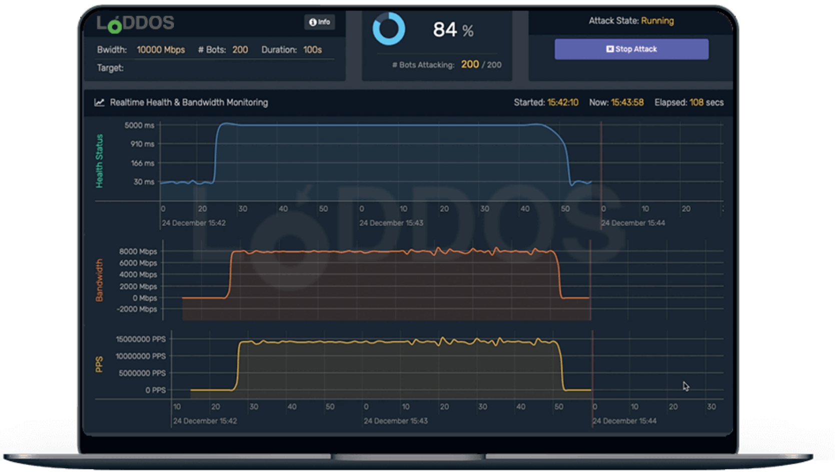


```
 ()
t socket, sys, os
 "][Remote DDoS Attack" -
 "injecting " + sys.argv
ttack():
= os.fork()
```

HOW TO PERFORM DDoS TESTS?

As of now, most DDoS tests are being done manually. The technical and administrative preparation stages of these tests take way too long. Security and IT teams must work together for a considerable amount of time to prepare and configure on premise traffic generator systems to perform DDoS tests. Performance of these operations leads to additional load in terms of time and cost. Real-time monitoring is usually not available during these tests and it takes time to issue reports after the tests are completed. Even if test is done, they are not re-usable most of the time.

WHAT IS LoDDoS?



Bwidth: 10000 Mbps # Bots: 200 Duration: 100s
Target:

84 %
Bots Attacking: 200 / 200

Attack State: Running

Started: 15:42:10 Now: 15:43:58 Elapsed: 108 secs

LoDDoS is a DDoS and Load Test platform offered as a service from the cloud. The platform creates real DDoS attacks against services via real attack parameters. It also measures the resilience of internet-enabled web applications against high traffic.

This enables organizations to test the limits and efficiency of DDoS prevention systems before a real DDoS attack. The tests can be stopped, restarted, recorded, reported anytime and the reports can be stored to investments can be easily monitored.

DDoS tests can be monitored in real-time by all parties and can be stopped at any time in case of an emergency. All tests can be replayed, and results can be compared. Reports are created instantly, and these reports can be saved for later evaluation.

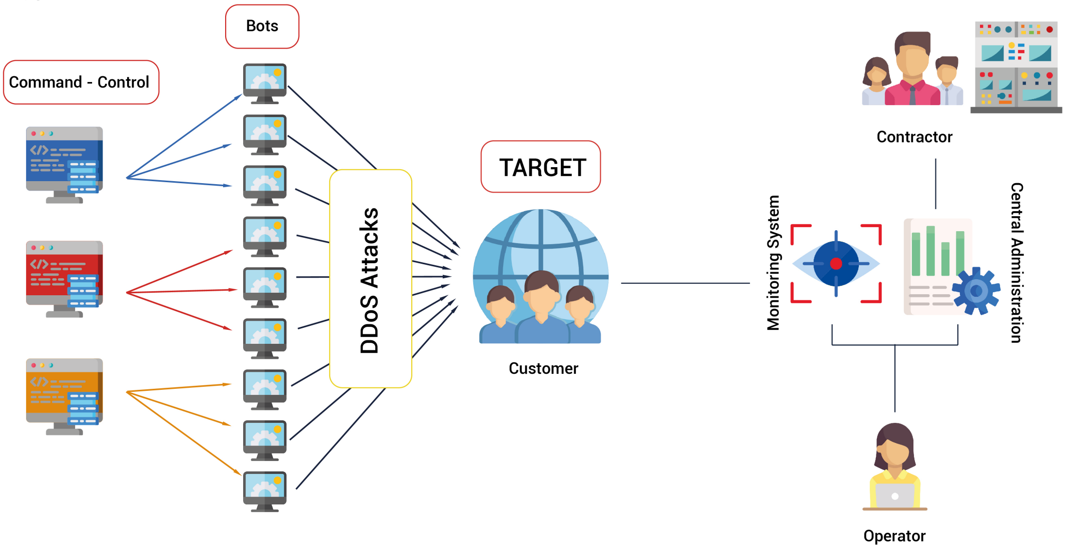
A high number of requests to web applications can be delivered by the help of load test future thus the limitations of these applications becomes visible. Load test helps to analyze real load situation of applications before it actually happens.

LoDDoS ARCHITECTURE

LoDDoS contains 3 main components. These components are;

1. Command and control center where the attacks performed are defined, managed, monitored and reported,
2. Bot networks where the attacks are conducted,
3. Monitoring system where the target system's health status is monitored.

Command and control center is controlled via a web interface. There are different user roles for management, operations and monitoring. DDoS tests performed after 2 phase security authorization based on these user's rights. Bot network runs on a cloud service provider and all the bots are managed by command and control center. The number of bots on the bot network, the geographical location of the bots, the bandwidth generated can be all controlled via command and control center based on the scope of the test. Bots are LODDOS managed cloud systems, not virus infected client systems of unaware end users. The monitoring type to be conducted by the monitoring component can also be controlled by the command and control center.



SUPPORTED DDOS TEST TYPES

Volumetric DDoS Tests

The main purpose of volumetric DDoS attacks is to consume network and system resources of target systems and to prevent these systems from serving to the users.

Mostly, it is intended to fill the line by sending packets more than of the Internet bandwidth of the target systems.

TEST TYPE	DESCRIPTION
TCP SYN Flood	High volume of SYN packets is sent to a TCP service serving on the target system, preventing the corresponding TCP service from serving.
TCP SYN-ACK Flood	High volume of the SYN-ACK packets is sent to a TCP service serving on the target system, preventing the TCP service from serving.
TCP ACK-FIN Flood	High volume of ACK-FIN packets is sent to a TCP service serving on the target system to prevent the corresponding TCP service from serving.
TCP RST Flood	High volume of RST packets is sent to a TCP service serving on the target system to prevent the corresponding TCP service from serving.
TCP PUSH ACK Flood	High volume of PUSH ACK packets is sent to a TCP service serving on the target system to prevent the corresponding TCP service from serving.
TCP All Flags Flood	High volume of full-flagged TCP packets is sent to a TCP service serving on the target system to prevent the corresponding TCP service from serving.
TCP No Flags Flood	High volume of none-flagged TCP packets is sent to a TCP service serving on the target system to prevent the corresponding TCP service from serving.
UDP Flood	High volume of UDP packets is sent to a UDP service serving on the target system to prevent the UDP service from serving.
UDP Fragmented Flood	High volume of fragmented UDP packets is sent to a UDP service serving on the target system and the UDP service is prevented from serving.
ICMP Flood	High volume of ICMP packets is sent to the target systems for testing.
SSL Negotiation Flood	High number of SSL/TLS handshakes are sent to an SSL/TLS service serving on the target system to prevent the service from serving.

DDoS Tests in Application Layer

The aim of the DDOS tests performed on the application layer is to open valid and real connections on the target systems and to force the limits of the systems and prevent them from serving.

TEST TYPE	DESCRIPTION
HTTP GET	High number of GET requests is sent to a HTTP service serving on the target system to prevent the service from serving.
HTTP POST	High number of POST requests is sent to an HTTP service serving on the target system to prevent the service from serving.

TEST TYPE	DESCRIPTION
HTTPS GET	High number of GET requests are sent to an HTTPS service serving on the target system to prevent the service from serving.
HTTPS POST	High number of POST requests are sent to an HTTPS service serving on the target system to prevent the service from serving.
Slowloris	A connection to an HTTP or HTTPS service serving the target system is established so that the connection remains open as long as possible. Thus, service is tried to be prevented. Slowloris is an effective attack on Apache web servers.
DNS Query	High number DNS requests is sent to a DNS service that serves on the target system, preventing the corresponding DNS service from serving.
DNS Random Query Flood	High number of random DNS requests are sent to a random DNS service that serves on the target system, preventing the corresponding DNS service from serving.

Test Volumes

BOTS	L3/4 TESTS (VOLUMETRIC) BANDWIDTH MBPS (UPTO)	L7 TESTS (APPLICATION) RUNNING USER (UPTO)
50	3.000	500.000
200	12.000	2.000.000
400	24.000	4.000.000
600	36.000	6.000.000

SECURITY

2-Stage Security

To perform a DDoS test; both the operator (the tester) and the customer (tested) must approve the relevant test. In this way, the test is guaranteed to be performed only to the party who wants to take the test.

Emergency Stop Button

The tests being performed can be stopped with one button if desired. In case of unexpected situations, tests can be stopped deliberately and restarted at any time.