LODDOS

DDoS Attacks Evaluation Report

Abbreviations

DDoS : Distributed Denial of Service

IoT : Internet of Things

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

NTP : Network Time Protocol

SSDP : Simple Service Discovery Protocol

SMTP : Simple Mail Transfer Protocol

OSI : Open Systems Interconnection

CDN : Content Delivery Network

Gbps : Giga bit per second

PPS : Packet Per Second

WAF : Web Application Firewall

IPS : Intrusion Prevention System

DNS : Domain Name System

Executive Summary

As DDoS attacks become increasingly complicated, it gets much easier and cost-efficient to organize DDoS attacks. Attackers can organize DDoS attacks for quite low costs solely by entering destination addresses and easily disable organization systems. Such easy and low-cost DDoS attacks pose great risks for internet-driven organizations. Taken unawares by such DDoS attacks, organizations may fail to serve for hours, even for days.

DDoS attacks may be risky for all web-based organizations. It is of great importance to get prepared against such kind of attacks, to take any necessary technical and administrative measures and to test DDoS durability of systems on regular basis in order to improve defense mechanisms.

This report explains DDoS, types of DDoS, motives behind DDoS attacks, true stories of major DDoS incidents, approach of protection against DDoS attacks and the importance of DDoS tests.

What is a DoS/DDoS Attack?

Before describing the term “Distributed Denial of Service (DDoS)” Attack, it would be more appropriate to define the term Denial of Service (DoS) Attack. DoS attack targets to prevent legitimate users from accessing a targeted system. Such attacks exploit target system and applications or other sources used in accessing such system and applications to make the targets unavailable. In DDoS, attackers utilize multiple sources of distributed attacks for the same purpose. The use of multiple number and type of attack resources (computer, mobile phone, IoT etc.) targets both easily overcoming the easy prevention of attacks and faster and easier exploitation of targeted system. Attackers typically seize internet-connected information technology resources with malwares (zombie/bot) and prefer to deplete the resources of targeted systems through a number of mechanisms (Command and Control/C2/C&C), able to control such devices (botnet) in bulk.

Types of DDoS Attacks

Attackers typically use three types of DDoS attacks (Network, Protocol and Application) as defined below:

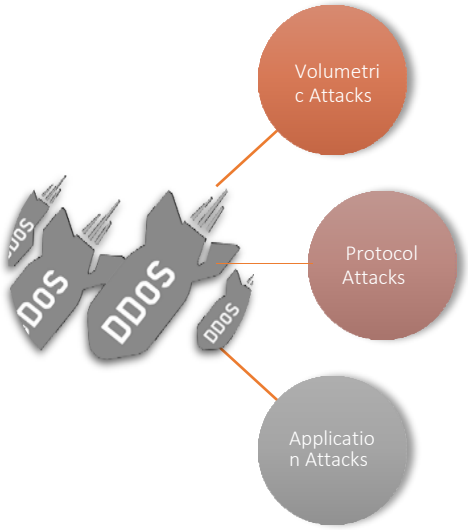

Figure 1

Volumetric Attacks (Network)

Volumetric attacks are the most preferred type of attack by the attackers and target to flood internet bandwidth used by targeted organizations. In this way, both the incoming and outgoing network traffic of an organization are affected and fail to respond any legitimate requests and eventually become unavailable. Finally, all parties that use the same internet infrastructure will be affected and all internet-connected services will be disabled.

Examples to volumetric attacks are TCP/UDP Flood, DNS/NTP/Memcached Amplification.

Amplification Attacks: Amplification attacks are those that use DNS, NTP, SSDP, Memcached etc. protocols on servers that serve large masses on the internet. While attacking victim (target) systems, attackers act like making requests from victim systems (spoof) and enable return packets access victim system to realize DDoS. In this type of attack, small queries are sent to servers, which are not safely configurated, to ensure that victim system is delivered large amount of inquiry packets. When victim systems fail to respond large-size and amplified amount of inquiries, it becomes inaccessible.

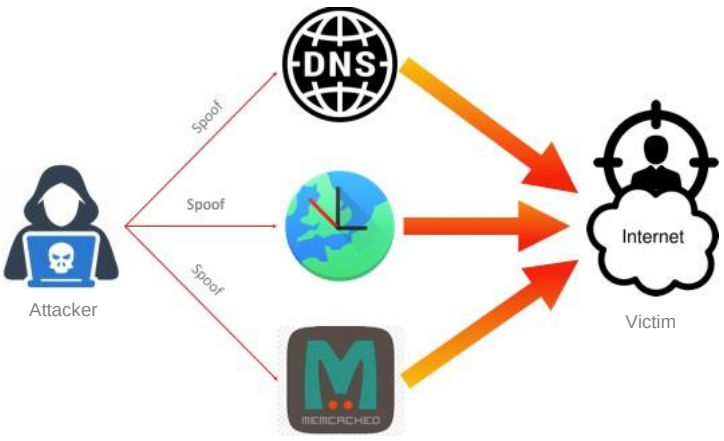

Figure 2

Protocol Attacks

These attacks typically target OSI L3/L4 protocols and use session information to target Firewalls, Load Balancers, Routers etc. systems. This type of attack makes multiple login requests and sends new inquiries before login is complete. In this way, it fills the session tables of network and security devices to make them inaccessible.

Examples to protocol attacks are SYN/SYN-ACK/ACK Flood, Ping of Death etc.

Application Attacks

These attacks target web applications, DNS, SMTP etc. OSI L7 application services. Targeted applications are overwhelmed by large range of inquiries beyond their capacities until their resources are depleted and eventually, the system becomes unavailable.

Examples to application attacks are Flood attacks to HTTP, HTTPS, DNS and SMTP services.

The aforementioned attacks may either be performed singly by attackers or simultaneously with multi-vector attacks. In this way, attackers make their attacks much more complexed while targeting both to hinder the response teams and to complicate the efforts of security devices for prevention.

Attack Motivations

It is likely that many motivation factors lie behind DDoS attacks. To address a few:

Money: The motivation that corresponds to an attack, which eventually leads to earning or losing money. The reasons may include, but not limited to, to gain advantage over competitors, racketing, decrease in share value etc.

Ideological: Due to political etc. reasons.

Attack Concealment: To prevent the original intention, i.e. detection of data leakage etc. by distracting the personnel and devices of a targeted organization.

These are typically mentioned motivations and may include any further different motives.

True Events

Many organizations are exposed to DDoS attacks every single day. This topic will address some of real attacks by their importance in the history.

Service Provider (Anonymous): 1.7 Tbps / 2018

NetScout reported that the largest DDoS attack was on March 5, 2018 of 1.7 Tbps size utilizing *Memcached Amplification* that targeted a customer of a U.S.-based service provider. It was confirmed that the attack had been avoided.

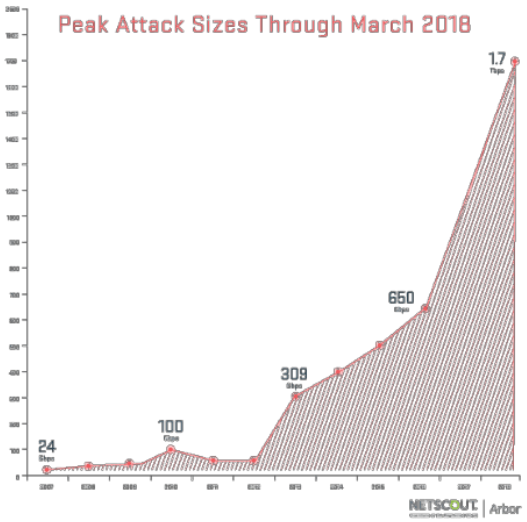

Figure 3

GitHub: 1.3 Tbps / 2018

GitHub, a platform where software developers store and share their applications, was the victim of a DDoS attack that peaked at 1.35 Tbps in 2018. The attack was mitigated after around 10 minutes of denial to website after which DDoS protection service was activated. The attackers used *Memcached amplification* attack.

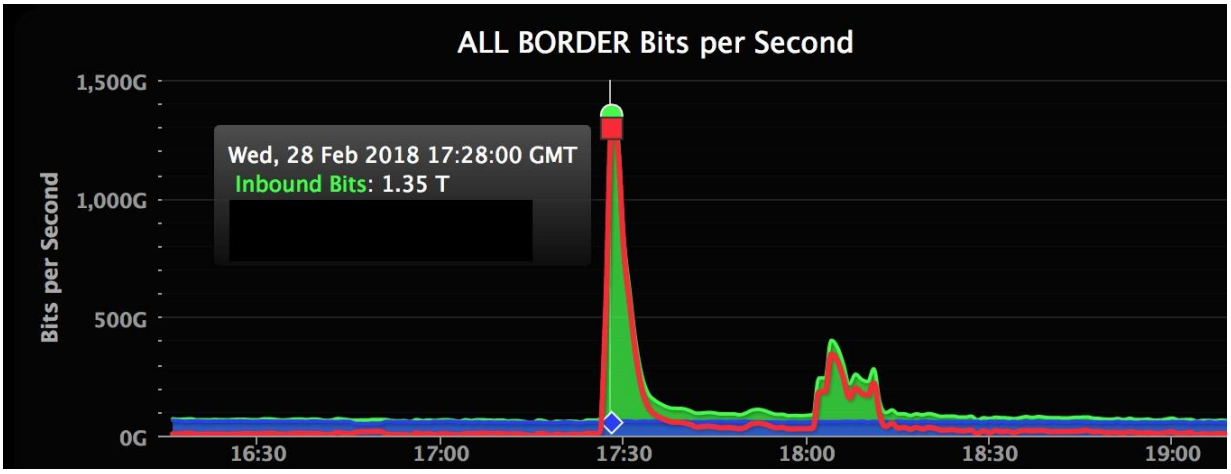

Figure 4

Dyn: 1.2 Tbps / 2016

Dyn, a DNS provider, was the victim of 1 Tbps-size DDoS attacks at several time periods on October 21, 2016. These attacks used *Mirai botnet*, largely made of IoT devices, and TCP and UDP traffic over port 53. The first attack could not be mitigated for 2,5 hours, after when only new attacks were encountered. Many websites suffered from accessibility during the attacks.

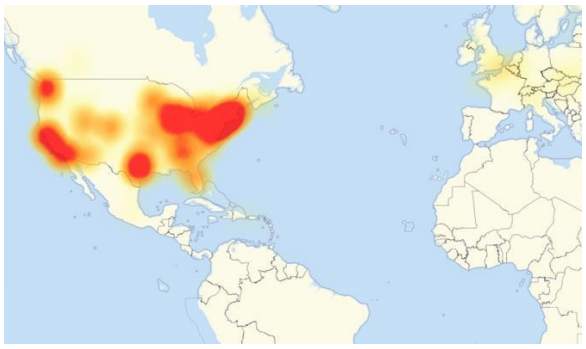

Figure 5

CloudFlare: 400 Gbps / 2014

CloudFlare is a Content Delivery Network (CDN) service provider. An organization serving on CloudFlare became the victim of a 400Gbps attack in 2014, which attack even affected CloudFlare's own systems. Such attack used Network Time Protocol (NTP), a networking protocol for clock synchronization between servers.

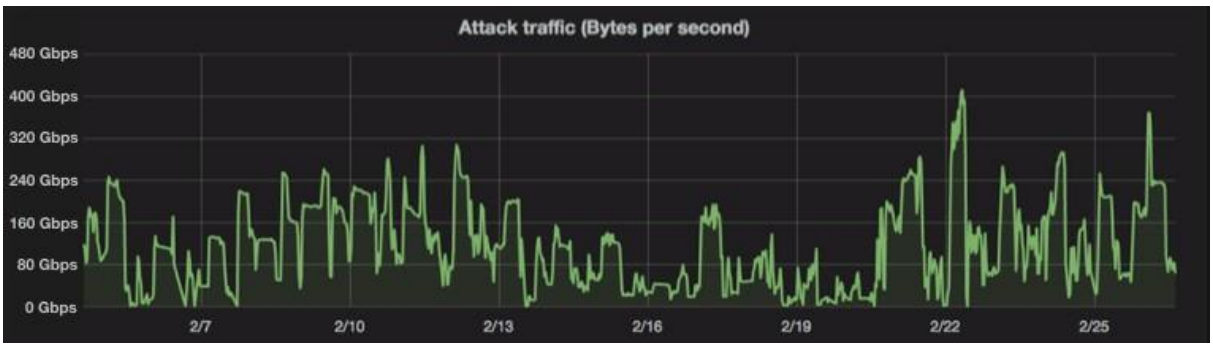

Figure 6

SpamHaus: 300 Gbps / 2013

In 2013, a 300 Gbps DDoS attack was launched against SpamHause, an anti-spam organization. The largest DDoS attack in history then, this attack was stopped by SpamHaus's service provider.

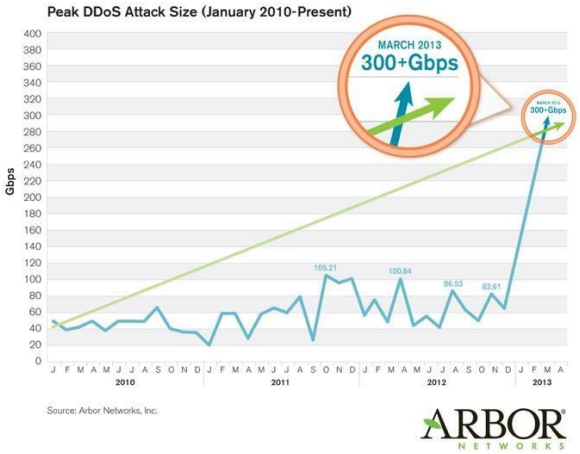

Figure 7

As seen in the incidents above, even security providers may be affected by massive DDoS attacks. The magnitudes of above attacks were tremendous, which sizes are rarely seen.

Various Statistics

The statistics obtained from a number of global reports published about DDoS attacks will be useful to profile DDoS attacks in general.

Two graphs in 2018 Corero Trends Report suggest that:

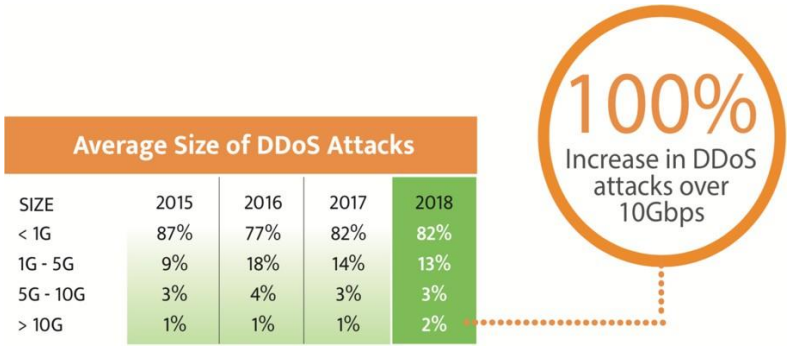

Figure 8

According to the graph above:

- 82% of DDoS attacks in 2018 were 1 Gbps or lower.
- The ratio of attacks between 1 Gbps and 10 Gbps is 16%.
- The ratio of attacks larger than 10 Gbps is 2% of total attacks.
- This ratio corresponds to an increase of 100% compared to 2017.

Figure 9

Another significant graph in 2018 Corero Trends Report is provided above. According to this graph:

- 81% of attacks in 2018 lasted for or less than 10 minutes

96% of DDoS attacks lasted for or less than 60 minutes.

Figure 10

According to Q4 2017 Global DDoS Threat Landscape Report, top targeted countries for DDoS attacks include US, South Korea and China. In addition, Turkey ranks amongst the top targeted countries with a ratio of 2.1%.

Figure 11

According to NETSCOUT Threat Intelligence Report published in 2018, 75.7% of DDoS attacks were volumetric, 12.4% were application layered and 11.8% were protocol attacks.

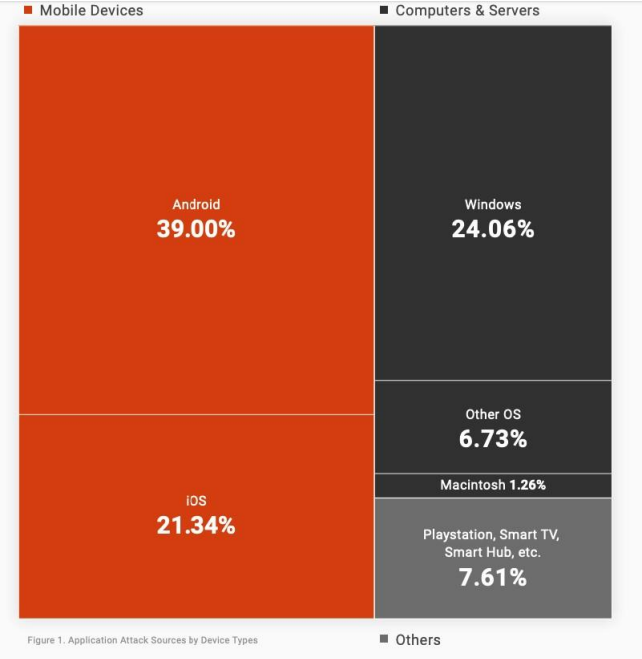

Figure 12

The increase of use of mobile phones, expansion of processors and memories of mobile phones and 24/7 availability of such devices make them vulnerable to active DDoS attacks. The graph above illustrates that around 60% of recent DDoS incidents include mobile phones as botnet members.

Protection Approach

As addressed in the topics above, DDoS attacks may be launched in various types and sizes. Unfortunately, no single device or method is readily available to prevent all DDoS types. The way to be resistant against DDoS attacks is to create a layered defense mechanism like in other security activities.

Gartner's "DDoS: A Comparison of Defense Approaches" report suggests a detection and prevention method consisting of multiple defense layers as given below about how a defense mechanism should be.

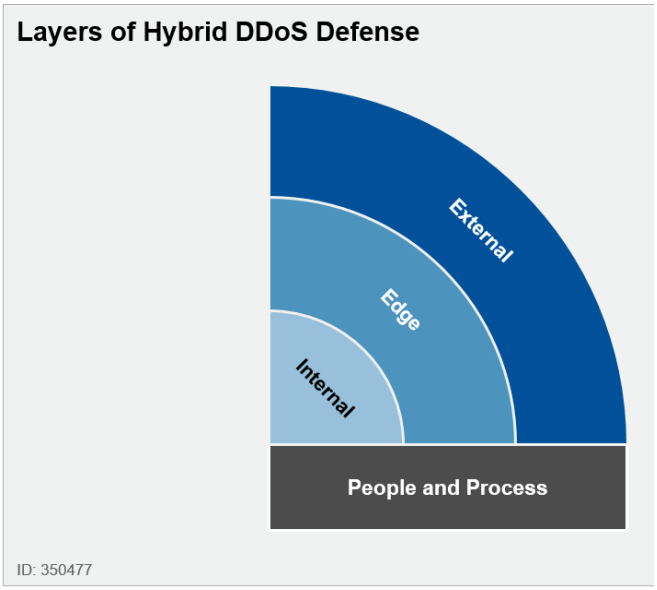

Figure 12

To address such layers;

External

We mentioned about the details of volumetric attacks above. If large size of volumetric attacks can reach the organization network, in such a case the security measures of organizations will unfortunately be poor to prevent the attack. Prevention or mitigation should be realized before such attacks reach out to the organization network. At this point, Internet Service Providers (ISP) or DDoS Protection Services provided by ISP's come into play. ISP's, which are able to process large-size traffics, get activated to mitigate the effects of DDoS attack in a short while (depending on ISP) after malicious traffic accesses the organization network.

From this point of view, it is of great importance for organization to adopt a DDoS Protection Service conforming to their business requirements.

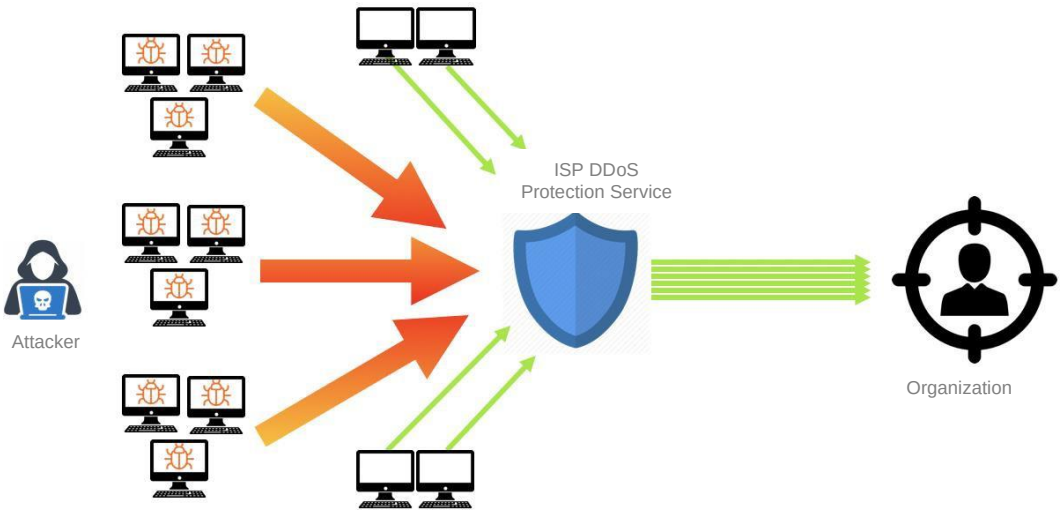

Figure 13

Edge

This layer consists of router, load balancer, firewall and similar edge network and security device of organizations. Attackers exhaust session tables of such devices through protocol attacks (TCP-SYN etc.) and may disable IP router, load balancer, firewall etc. devices.

DDoS Protection Devices, which have been developed to protect such networks and security devices, are currently available in cyber security market. These devices offer technologies that have been developed to prevent DDoS attacks launched against network and security devices on session basis.

In order to protect the organization systems in edge layer, these devices must be positioned at the external point of the organization nearest to the internet. Furthermore, certain DDoS protection devices ensure signaling with devices in ISP and offer DDoS protection service to enable a more effective DDoS protection mechanism.

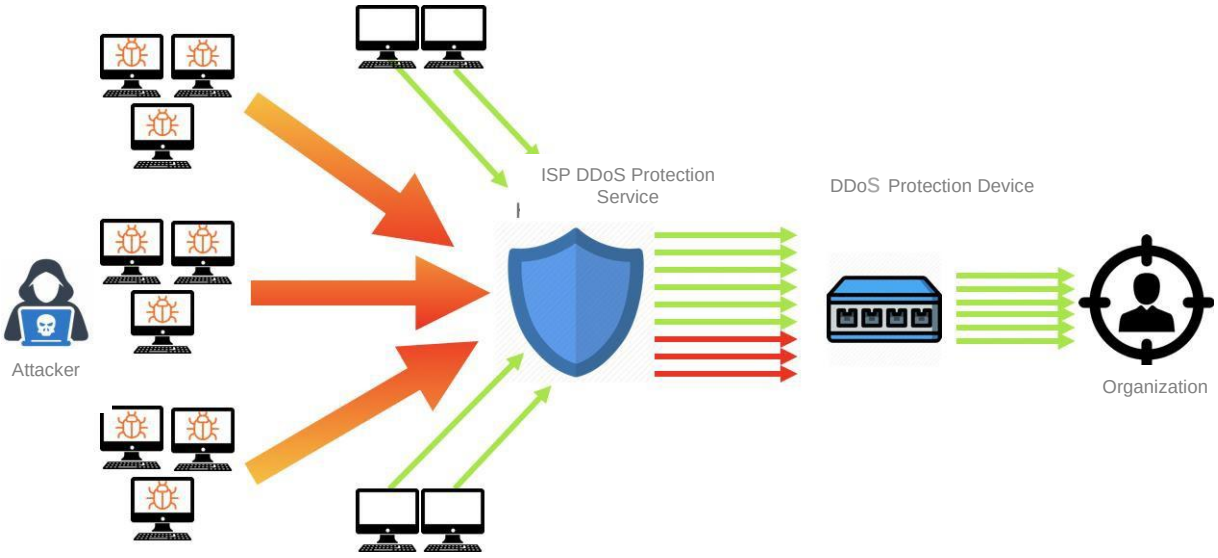

Figure 14

Internal

Probably the most dangerous of DDoS attacks in types of network, protocol and application is the application attack. These attacks are typically launched against web, e-mail, DNS etc. applications that directly serve the user and make related application become unavailable. If, in particular, DNS attack succeeds, all DNS-dependent applications will be inaccessible. IPS, WAF etc. devices are used for protection against internet-based applications. These devices help discover the configurations of applications and are capable of activating application-specific protection mechanisms.

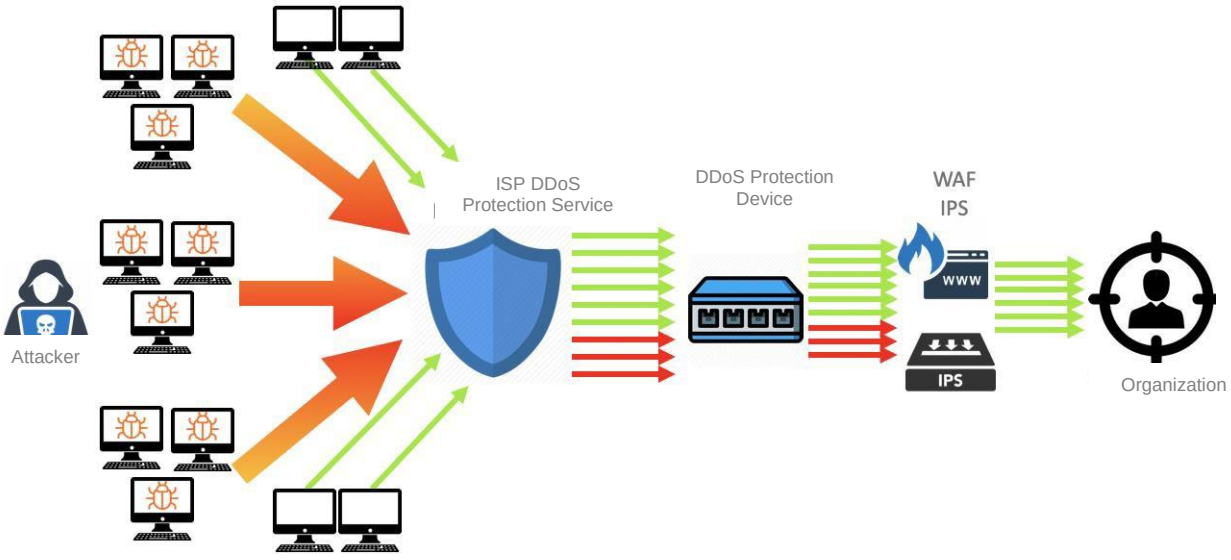

Figure 15

People and Process

Even if top-quality DDoS protection services and devices (state-of-the-art technology) are adopted, all People-Process-Technology components should be cohesively used for an effective cyber defense. At this point, People and Process factors are of great importance in DDoS protection approach. In case of a DDoS attack, an incident management process should have been soundly realized for an accurate and effective response. In a similar manner, the response team and the team responsible from recovery in case of a failure should be competent and prepared. Therefore, Emergency Action Plans must be prepared and checked for currency and validity through regular drills.

DDoS Tests

DDoS tests include the activities, which are conducted to test the aforementioned DDoS protection activities at certain intervals and/or after any major system/application changes and to improve any performed protection activities according to such test results.

The activities, which are most appropriate to minimum exposure to DDoS attacks, were mentioned under DDoS protection approach heading. The aforementioned people-process-technology activities require not only time and money but also investment. It is quite important to measure how such investments are effective and efficient in case of a real attack and to remove any detected deficiencies. In this context, it will be necessary to test the internet-connected services of the organization by generating large amount of traffic (bandwidth and pps) through multiple bots across different geographic regions around the world, like real attackers do. In particular, internet-connected applications must be tested consistently and such tests must be repeated in case of any changes in existing applications or starting new applications.

LoDDoS

It takes time and effort to conduct the necessary preparations to run DDoS tests. Technical and administrative preparation phases of such tests take a long time. Both security and IT teams should work in collaboration in order to prepare and configure the systems to be used in DDoS testing. Upon completion of preparations, no instant watch is possible during the implementation phase of testing and it takes time to generate reports after tests are completed. Whether a test is conducted once or consistently, preparation phase of each test is performed

from the very beginning. Therefore, it became imperative to obtain automation for such preparation and implementation phases through an application.

At this point, LoDDoS is a DDoS Simulation and Load Testing platform offered as a service. This platform simulates any possible DDos attacks to an organization with real-attack parameters. Moreover, it measures the resilience of internet-connected web applications to high traffic.

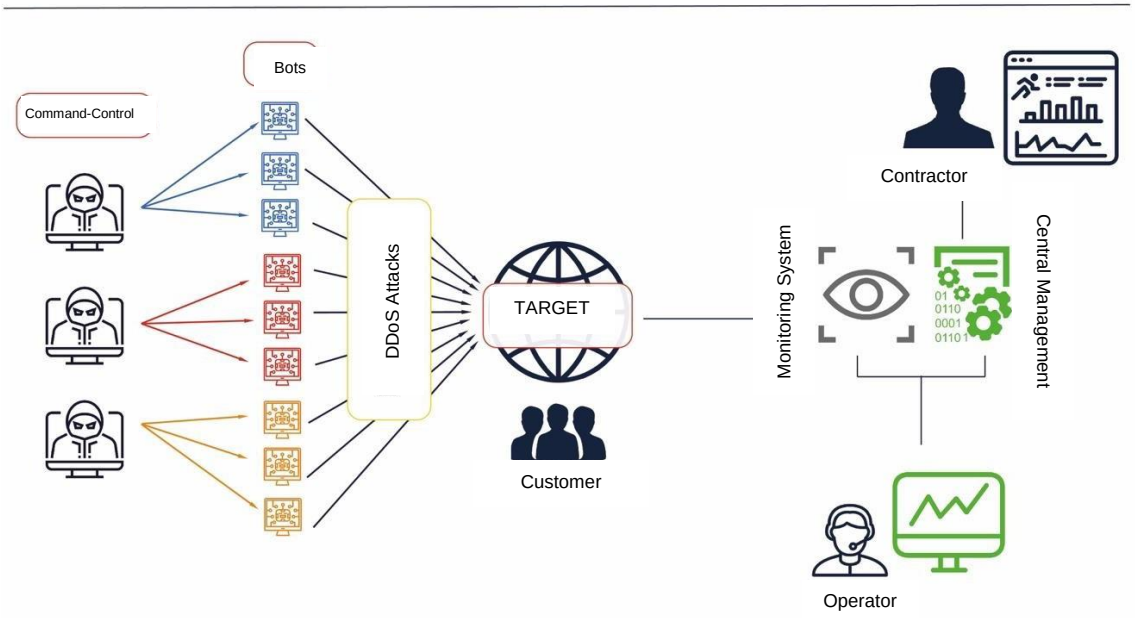

Figure 16

DDoS Simulation helps organizations test the limits and abilities of their DDoS prevention systems without being exposed to a real DDoS attack. Tests can be monitored live, and can be stopped at any time in a controlled manner, started over, reported instantly and reports may be saved for further evaluation.

Load Testing helps quantifying to what extent the infrastructures may fulfill large number of requests to web applications and performing any necessary improvements before a real load occurs.

Conclusions

DDoS attacks become increasingly complicated and reach massive sizes. Even though it is not inevitable for organizations to sustain DDoS attacks, they are not unavoidable. No matter how large and complicated such attacks are, it is possible to be affected the least by such attacks if necessary and sufficient preparations are in place. Case studies described under the heading 'True Events' are the best examples to this. Planned defense actions on the axis of People-Process-Technology will have importance in corroborating the resilience of organizations against DDoS attacks.

To summarize the main topics about DDoS protection and defense:

- To ensure, to consistently monitor and to improve the security service and components necessary at external, edge and middle layers;
- To create and to keep up-to-date processes, procedures and directives for DDoS protection;
- To make sure that the personnel responsible from DDoS protection is technically and administratively trained;
- To test the systems and applications for DDoS and load testing after any major changes or before commissioning any new applications or periodically; and
- To test the components of people-process-technology through drills and to apply any necessary improvements.

Mustafa Kemal Mahallesi.
Dumlupınar Bulvarı No:164,
Kerıtpark Ofis, Kat:4 Daire:06
Çankaya/Ankara

Phone: +90 (312) 235 44 41
Fax: +90 (312) 235 44 51
E-mail: bilgi@barikat.comtr

Nida Kule Alaşehir Kuzey İş Merkezi,
Barbaros Mahallesi, Begonya Sokak. No:3,
Daire: 71/72 Alaşehir/İstanbul

Phone: +90 (216) 504 53 30
Fax: +90 (216) 504 53 32
E-mail: bilgi@barikalcom.tr

Millenium Tower Floor 29.
Radarweg 29 1045 XN
Amsterdam/Netherlands

Phone: •3120 854 6146
E-mail: info@barikatbv.com