"Ten thousand people ordered pizza at the same time, so nobody got pizza"

Denial-of-Service Attacks, and what you can do about them

November, 2020

DoS basics

CISA definition of denial-of-service (DoS) attack:

"…legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor"

- Normally because a server is bombarded with an unmanageable volume of data requests
- Directly harms organisations by taking networks and websites offline, and can indirectly upset physical systems such as energy grids and production processes via ICS (Industrial Control Systems)
- Sometimes launched to distract attention from a more subtle attack (e.g. ransomware insertion)
- Other motivations behind DoS attacks include extortion, 'hacktivism' based on political/social interests, business competition and state-sponsored cyber warfare

Distributed Denial of Service (DDoS):

Many machines (normally a botnet) mount a coordinated DoS attack simultaneously

Botnet:

Large network of internet-connected devices that have been penetrated and compromised by malware and are controlled by an attacker/criminal group (see e.g. Trickbot, Mirai)

sEptu

A brief history of DoS

1974: First recorded DoS attack

David Dennis, who was just 13 years old at the time, wrote a program that sent a certain command to all the computers on a network at the University of Illinois. The command exploited a vulnerability on the computers that caused 31 users to shut down immediately

1988: The Morris worm:

An infamous example of early malware written by Robert Morris at Cornell University. Created with the intention of calculating the size of the precursor to the Internet (ARPANET), it propagated rapidly throughout the network of 60,000 machines. Multiple infections of around 10% of the computers caused so many unwanted processes to run that they broke down

1999: (One of) the first recorded DDoS attacks

An unknown hacker sent an instruction to some computers on a network at the University of Minnesota, which in turn sent further instructions to other 'daemon' machines. These machines overwhelmed target IP addresses with data packets (a 'UDP flood'), shutting down the network for two days

2001: Code Red

A worm that propagated among computers running the Microsoft IIS web server, infecting 359,000 hosts. The intention of the hackers behind this malware was apparently to use it to launch a DoS attack on US government websites including the White House website, but a patch was discovered and applied before this happened

2017: Biggest recorded DDoS so far

In October of this year, Google claimed that – in 2017 – they resisted a DDoS attack of 2.5Tbps (terabits/sec)

sEptu

Some examples of network DoS attacks against infrastructure such as servers, firewalls and load balancers

UDP flood

The victim's server is bombarded with data packets of the type associated with the 'UDP protocol' – one of the main standardised methods for transferring data between computers

Unlike the TCP protocol, there is no initial 'handshake connection' to check validity, and the receiving server attempts to allocate each packet to an application, finds none and then sends out a 'Destination Unreachable' packet. It's hard to manage this type of attack with a normal firewall, and it was the most commonly used DDoS vector in 2019*

SYN flood

The attacker abuses the initial TCP protocol connection or 'handshake' between users of services (clients) and providers (servers) by sending a massive volume of initial contact (SYN) packets to a targeted server. The victim responds (with 'SYN-ACK' packets), using up available ports and awaiting final counter-responses ('ACK'), which never come

*Source: Imperva Global DDoS Threat Landscape 2019

sEptu

Further examples of network DoS attacks

Ping (ICMP) flood

An internet layer attack on devices using the 'ping' function, which tests reachability of a host on a network. The attacker's botnet sends a flood of ping requests to the target, which becomes overwhelmed by the requirement to respond to all of the requests

Ping, SYN and similar attacks are quantified by the number of packets per second (pps)

Amplification attacks using DNS and NTP servers

The amount of data that floods the victim is far greater than the initial output from the attacker's botnet. In the case of a DNS attack, the botnet sends UDP packets from a false ('spoofed') IP address to a group of DNS servers. In fact, the false IP is the IP of the victim, and the DNS servers reply to this address with much larger responses, amplifying the original attack size. This is also known as a reflection attack, as it is 'reflected' off the DNS servers, and can also be achieved by abusing Network Time Protocol (NTP) servers.

Amplification attacks are a form of Volume-Based ('Volumetric') attack which is normally measured in bits per second or bps (in fact typically Gbps or even Tbps). The Amplification Factor shows the ratio between the number of packets that the victim has to manage compared to what the attacker sends out. It can be over 500 in the case of an NTP attack*

*A recent form of attack (that can be mitigated by disabling UDP on relevant servers) called 'Memcached Amplification' can reach a ratio of over 50,000X

sEptu

Some examples of application or Layer 7 DoS attacks against websites and web applications

- Layer 7 attacks on websites take advantage of the asymmetry between the resources used to make a request to a web server, and the work that needs to be done in order to generate a response and deliver a webpage

HTTP flood

The targeted server is overwhelmed by HTTP requests (e.g. HTTP GET requests for some file or other asset) from a botnet. As with other Application Layer Attacks, the intensity is measured in requests per second (RPS)

Randomised HTTP flood

A type of HTTP flood where the attacker uses a range of different IP addresses, URLs, agents and so on in order to confuse the victim's defences

Slowloris

Named after a type of nocturnal animal that 'moves slowly and deliberately', this form of attack combines simplicity with elegance and efficiency. It doesn't require much bandwidth as it works by sending a series of incomplete HTTP requests to the targeted web server at regular (but not rapid) intervals. The server keeps the connections open while it awaits the rest of each request, with the result that all connections quickly become blocked and it cannot operate normally any more

sEptu

Denial-of-service – current activity

- Attack sizes

  Headline-making volumetric DDoS attacks peak at over 1Tbps nowadays (1Tbps is the equivalent of about 40,000 people simultaneously streaming Netflix Ultra HD). However, this type of attack remains rare: the average attack size in 2019 seems likely to have been in the 10-40Gbps area, with over half below 10 Gbps

  Very large attacks in terms of data packets hit levels of 600Mpps+ but this type of protocol attack is normally measured at 50Mpps or below

  Application layer DDoS attacks have been known to reach an intensity of over 200,000 requests per second but generally are in the range 100-1000RPS, which can be enough to bring down a 'mid-size' website

- DDoS for hire ("DDoS as a service")

  Some botnet operators offer their capacity to organise DDoS attacks as a service, relabelling themselves as 'stressers' that can test the resilience of networks as a form of penetration testing

sEptu

Denial-of-service – current activity

- **Multi-vector attacks**

  There is a trend towards more frequent 'Multi-Vector' DDoS attacks that combine and/or alternate different attack methods. For example, the attack may start with a UDP flood, then switch over to an NTP Amplification Attack combined with an SSDP attack that uses IoT devices such as cameras and vending machines to generate a reflected, amplified wave of data

  It appears that in 2019, more than half of DoS attacks exploited two or more vectors, and in 10% of cases, four or more vectors were used. Rapid changing of vector type and intensity makes it much harder to mitigate this type of attack

- **DDoS and Ransomware**

  In October of this year it was reported that a ransomware operation ('SunCrypt') used a DoS or DDoS attack against one of their victims after they became frustrated with 'stalling' payment negotiations

sEptu

Mitigation of DoS attacks

- Most defence against DoS and DDoS attacks is based around routing traffic through the network of another company that specialises in DDoS mitigation. As it passes through this network, it is inspected with the aim of identification and control of malicious data flows at ‘the edge’ of your own organisation’s network

- Tactics used to detect potential DoS traffic include identification of excessive requests from one source, watching for known attack types or ‘signatures’ and machine learning-based methods

- In the case of application layer DDoS, the functionality may be linked to a web application firewall (WAF)

- An important goal of DoS mitigation is to avoid false positives – i.e. not to block friendly traffic

- Volume-based attacks (e.g. reflected, amplified DNS attacks) are managed by using a third party that has resources (‘content distribution network (CDN)-based DDoS mitigation services’) that can cope with huge data flows and ‘scrub’ them of any malicious component

- One increasingly common approach to website DoS and to web security generally is ‘bad bot management’. This uses WAFs and visitor behaviour analytics with machine learning, that considers IP address, time, device type, operating system etc to help them spot and manage malicious automated visitors - ‘bad bots’

For more information: **robin.long@septu.tech**