DRDoS

João Pedro Novo Antunes

Universidade de Coimbra
Portugal

I. Introduction

Distributed Reflective Denial-of-Service (DRDoS) is a form of Distributed Denial-of-Service (DDoS) attack. This type of attack relies on public services accessible through UDP servers, these servers are then used for their Bandwidth Amplification Factors (BAFs) and Distribution capabilities in order to flood a targeted systems with colossal amounts of UDP traffic.

II. User Datagram Protocol

The aformentioned attacks rely on UDP traffic for the attacks. UDP stands for User Datagram Protocol, this protocol is connection-less, what this means is that there is no need for a connection to be established for the server to send packets, the server simply sends packets to the end user with no regards for reliability. This features make UDP to be much faster than, for example, TCP, in terms of the ability to transfer data at much higher speeds. This quicker data transfer capacity makes it much more dangerous when the objective to saturare a target system with network traffic.

III. UDP Protocols

When some UDP services or protocols receive certain commands, this can originate responses substantialy bigger than the bandwidth of the original packet. Some common UDP services, such as DNS, NTP and SNMP, can provide this amplifying factor for attackers. When an attacker forgers the IP address of a victim, the destination server will respond to the target chosen by the threat actor, this creates a Reflected Denial-of-Service attack. In addition to this, the malicious user can also make use of services that generate packets hundreds of times the original packet bandwidth. This is called an Amplification attack, and when combined with Reflective Denial-of-Service attacks this translates massive amounts of traffic being generated to target a victim. Three protocols that provide this possibility to attackers are the following.

A. Network Time Protocol

Network Time Protocol, or NTP, is a protocol used for the synchronization of clocks between computer systems, this procotol is UDP based and functions on port 123. This protocol has a considerable Bandwidth Amplification Factor of 557. An attacker makes use of the publically accsessible vulnerable NTP servers to send a *get monlist* request with the spoofed source IP address. This command makes the NTP server send a list of the last 600 IP addresses that have connected to it to be sent to the victim. Since the size of the response is much bigger than the initial request, the threat actor is able to amplify the volume of traffic with ease.

B. CharGEN

Character Generator Protocol, or CharGEN, is a protocol used to send data containing a random number (between 0 and 512) of characters without any regard for the received datagram, typically used as a debugging and measuring tool. The CharGEN protocol is UDP based and listens for UDP datagrams on port 19. It has a Bandwidth Amplification Factor of 359. Since a response to the character generation request is sending a random number of characters, this generates a reply with a bandwidth much larger than the request. When an attacker sends a request to one of these servers with the source IP address spoofed, the server will send it is reply to the victim's system creating large amounts of traffic.

C. SNMPv2

Simple Network Management Protocol, or SNMP, is a protocol used to collect and organize information about managed devices on IP networks and to modify that information to modify its behavior. This protocol listens on port 161 and 162. An attacker can send a GetBulk request to an SNMP server, this will cause the SNMP manager to obtain large tables of data by performing multiple GetNext request commands, generating considerable amounts of data that will be sent via network. If an attacker sends the GetBulk request using a spoofed source IP address, these high loads of traffic will be redirected to the target's system.

IV. The Common Denominator

These types of attacks use services that share impactful common characteristics that power them, allowing for devastating effects on targeted systems.

A. 1st Characteristic

The first common characteristic is the choice of the Transport Layer protocol, UDP, this protocol allows for a rapid cadence of packets being sent accross the Internet, overwhelming a system that is targeted.

B. 2nd Characteristic

The second main characteristic is the use of services that allow for the functioning of the Internet. These services are trusted, allowing the attacker to flood with unwanted traffic a victim. This characteristic ties with three other "sub-characteristics" that allow for these attacks to have such disastrous effects.

1) Geography: These services are supported by servers distributed across the whole planet, allowing for even quicker and more effective attacks.

2) Number: The high number of servers offering the services is what concedes the Distributed nature for this type of attack.

3) Bandwidth: These servers have the necessary high bandwidth for the attacker to be able to overload the victim's system with network traffic.

C. 3rd Characteristic

The third important characteristic is the Bandwidth Amplification Factor. DRDoS attacks make use of commands that produce much larger bandwidth being sent in the reply, than the one being sent in the original request. What this permits is the amplification of an attacker capacity to flood a targeted system with massive amounts of network traffic. In conclusion, services that allow for bigger Amplification Factors are the most likely to be used by an attacker.

V. Mitigation

DRDoS attacks bring the necessity for new strategies to mitigate these attacks. But, tradition DDoS mitigation techniques can apply and will help in the mitigation of the more damaging DRDoS attacks.

Small Businesses can adopt some mitigation techniques that can help in case of a DRDoS attack.

A. Reflexive Access Control Lists

For small businesses, this is a great solution since it acts as a stateful firewall. This will only allow traffic that is initiated within the network and deny other packets coming from outside the network. Altough this could make, for example, Web Servers unavailable until the attack ceases, the business equipement will not be overwhelmed by the traffic and it will be able to still have access to the internet.

B. Segmentation of the Network

The separation and distribution of assets inside a network is crucial. The distribution of different servers and databases is a good practice, aswell as restricting access from servers to other types of machines.

Mitigation techniques to protect large services, can include the following.

C. SDN Approach

In this solution, it is required the use of two *Differentiators* that provides basic logic to classify specific types of traffic. Traffic from the target host (requests) will be divided into UDP or TCP, TCP traffic will be allowed to exit the network towards the internet, however, UDP traffic will go through a NAT based solution that will provide an alias IP address. This result of this will be that, traffic incoming from the internet (response) will be split between UDP and TCP traffic, the TCP traffic will be allowed to enter the network, on the other hand, UDP traffic will be redirected to a *DRDoS Mitigiation System*, this will then filter the traffic based on if the destination address is the alias IP address or the real IP address of the target host. If the IP in that packet is in fact the real one, this responses will be dropped, if it is the alias IP address in the packet this will be classified as a legitimate UDP response.

D. Remotely Triggered Blackhole

This will have the best effect when working in coordination with ISPs. RTBH routing will block at the edge all inbound traffic destined for the victim, this is the most effective way to stop a DRDoS attack, however this will cut off all the communication to the internet since the victim is now unreachable. But the most important factor here is the protection of internal infrastructure and other costumers from the flood of traffic, this will also allow for time to investigate and analyze so better solutions to that attack can be put in place to mitigate it.

VI. DRDoS vs. Stuxnet

A. Knowledge and Availability

DRDoS attacks can be easily bought as a service on the internet, these attacks are relatively cheap and do not require much expertise in order to have devastating effects on the targeted system's. Publicly available services are exploited for these attacks to happen, the amplification factor that these services (such as DNS, SNMPv2) provide, increases the effects of traditional DDoS attacks, allowing for hundreds of times more traffic generated. On the other hand, the Stuxnet worm required a very high level of knowledge and expertise, this had to be created and developed from scratch. As it is evident, there's a big difference in the knowledge required for someone to launch an attack and the availability, since DRDoS can easily be bought on the internet as a service.

B. How does it happen?

Distributed Reflected Denial-of-Service attack is launched via the internet, it does not require direct access to a system, it only requires that the victim's system is online. Stuxnet was only activated under specific conditions, since the target was offline, this required that the payload had to be injected directly into the targeted systems.

C. Objectives

It is possible to make the case that both of these attacks have a common objective, make an asset unavailable. DRDoS attacks make the system unavailable and has the devastating effects immediately after the attack launching successfully. This is not the case with Stuxnet, the objective was to damage the equipment slowly, not giving away any signs of its actions.

D. Effects

These attacks have very different effects on the targeted systems. Systems targeted by DRDoS attacks are affected only when the attack is ocurring, when the attacks is stopped, the systems will be able to process the information and start functioning normally again. However, Stuxnet had the intention of permanently damaging equipment, making them unusable.

References

[1] Cybersecurity and Infrastructure Security Agency, Jan. 2014. Accessed on: April, 2022. [Online] Available: https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

[2] CloudFlare Learning. Accessed on: April, 2022. [Online] Availabe: https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

[3] Professor Aiko Pras, Forschungsinstitut Cyber Defendce, June 2017. Accessed on: April, 2022. [Online] Available: https://www.youtube.com/watch?v=XRZ1vreWrM0

[4] Internet Engineering Task Force, June 2010. Accessed on: April, 2022. [Online] Available: https://datatracker.ietf.org/doc/html/rfc5905

[5] Cybersecurity and Infrastructure Security Agency, Oct. 2016. Accessed on: April, 2022. [Online] Available: https://www.cisa.gov/uscert/ncas/alerts/TA14-013A

[6] Internet Engineering Task Force, May 1983. Accessed on: April, 2022. [Online] Available: https://datatracker.ietf.org/doc/html/rfc864

[7] ThousandEyes Learning (Cisco). Accessed on: April, 2022. [Online] Available: https://www.thousandeyes.com/learning/techtorials/snmp-simple-network-management-protocol

[8] Thomas Lukaseder, Stephan Kleber, Benjamin Erb, Frank Kargl, August 2018. Accessed on: April, 2022. [Online] Available: https://arxiv.org/pdf/1808.01177.pdf

[9] PacketLife, stretch, July 2009. Accessed on: April, 2022. [Online] Available: https://packetlife.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing/