Blackholing VS. Sinkholing: a Comparative Analysis

Anjali B Kaimal, Aravind Unnikrishnan, Leena Vishnu Namboothiri

ABSTRACT--- Distributed denial of service attack has caused major security problems all over the world. Be it small systems, or large organizations, DDoS attack can have severe impact on their functioning. It is a method used by the attacker to suspend services to that system for a period of time so that legitimate users cannot access services. Many techniques have been developed to reduce the effect of DDoS attack on the system. In this paper, we study about two different methods used to detect and prevent DDoS attacks: Blackholing and Sinkholing. The purpose of this study is to identify when to use blackholing and when to use sinkholing.

Keyword:Blackholing, Sinkholing, DOS, DDoS

1. INTRODUCTION

[1]Whenever a legitimate user is denied access to resources and services, we say denial of service occurs and it is termed as DOS attack. DOS attack can create many issues and few are disruption of services, exhaustion of the user's bandwidth and even denying access to a particular host. Denial of service attack has been around for a long time, but a distributed version of the attack has created widespread concern as it is more difficult to prevent. Here, the flooding occurs from many computers at a time, thus overwhelming the target easily. It uses the "many to one" version of DOS attack and it is called DDOS attack or distributed denial of service.

[2]The distributed denial of service attack has four components: victim, attack daemon agents, the control master program and the attacker himself. The victim is the targeted host which is attacked. The daemon agents are the components that actually carry out the attack on the victim. The master program coordinates the attack and attacker is the mastermind behind the attack. The daemon agents are infiltrated by the attacker to help carry out the attack.

The attacker sends "execute" command to the control program, and the control program triggers the daemon agents to carry out the attack on the target. The main work of the attacker is to infiltrate the host computers to make them daemon agents. Since the attack daemons are used, It becomes more difficult to trace the actual attacker.

There are countermeasures to reduce the effect of the attack, but no ways to avoid it altogether. Two of the known methods to mitigate a DDOS attack are blackholing and DNS sinkholing. Black holing redirects the malicious traffic to a"black hole" where it is dropped completely. Sinkholing routes the malicious traffic to another working IP address which checks the packets to find the faulty one. The following section describes in detail the working of blackholing and sinkholing methods.

2. BLACKHOLING

[3]It is a mitigation strategy for DDOS attacks. Here, the network traffic is directed into a "black hole" and these packets are lost/dropped. A black hole is a place where packets are destroyed or dropped and no information about the dropped packets is sent back to the source i.e we create an IP route that leads to nowhere. [7]This means that the packets are sent to a router that is disconnected and thus all the packets sent to it will be lost. A computer network consists of many routers which forward the packet that it receives to its destination and if the router does not work, these packets will be lost. In case of connection oriented protocol like TCP, a notification will be returned to the source if the packet is dropped. When an organization has no other ways or security measures lined up to block a DDOS attack, blackholing is a good option. For example when the victim under attack is facing the side effects of the attack, the users of this infrastructure also face the effects of the attack and thus when there is no other ways for the system to protect itself and its user, blackholing is used. It is a security measure against attackers that are known to us.

First, we define the destination of the malicious traffic. Then, we configure the static route to this destination to Null0 and the packets directed here are all lost. The most common form of black hole is an IP address that does not work or to which no host is assigned.

Remote triggered black hole filtering is a technique used for blackholing.

2.1. REMOTE TRIGGERED BLACK HOLE FILTERING

[5]It is a method used to drop malicious packets before it enters the network. Once an attack is detected in a network, the malicious packets can all be dropped at the edge of an ISP network based on destination address. It manipulates route tables at the edge using routing protocol updates to drop malicious traffic. The traffic is forwarded to Null0 interface. The Null0 interface is basically a trash can to route packets to and it cannot forward or receive any packets. It works effectively to stop DDoS attacks. Our main aim here is to stop the malicious traffic, identify the targeted destination IP and make the target return to service once the attack has disappeared. Here, we add a simple static route to the triggered device.

Revised Manuscript Received on May 29, 2019.

Anjali B Kaimal, PG Student, Department of Computer Science and IT, Amrita vishwa vidhyapeetham school of arts and sciences, Kochi, Kerala, India. (anjali.kaimal@gmail.com)

Aravind Unnikrishnan, PG Student, Department of Computer Science and IT, Amrita vishwa vidhyapeetham school of arts and sciences, Kochi, Kerala, India.. (aravind8896@gmail.com)

Leena Vishnu Namboothiri, Assistant Professor, Department of Computer Science and IT, Amrita vishwa vidhyapeetham school of arts and sciences, Kochi, Kerala, India.(vleena@gmail.com)

2.2. WORKING

A trigger is used to trigger the black hole and it is installed at the NOC. All the routers at the edge will have a iBGP peering relationship with the trigger. The trigger is set to redistribute static routes to its iBGP peers. These routes are sent by iBGP routing update. The Provider Edges (PE) must have a static route for unused IP address space. This means that this IP address is not actually deployed here. The admin adds a static route to the trigger. The trigger now redistributes the route to its iBGP peers. The PEs receives this update and next hop to the target IP is set to the unused IP which points to Null0 interface using static routing entry in the router configuration. All the traffic to the destination will now be sent to Null0 and will be dropped. When the threat disappears, the admin manually must remove the static route from the trigger which updates this with its iBGP peers. The PEs now removes the route for the target which is pointed to the unused IP.

2.3. DISADVANTAGES OF BLACKHOLING

Blackholing blocks all the traffic towards a website that is under attack without further considerations. At first, blackholing does seem like a perfect mitigation strategy to prevent DDOS attacks by routing all traffic to a null route. But now, we take a deeper look into what are the major limitations of blackholing.

- The problem with blackholing is that both malicious packets and legitimate packets will be sent to the null route and will be dropped. This means that anyone requesting services from our internet at that time is not processed and is dropped. For example, in case of credit union ISP which is under attack, blackholing is an unacceptable mitigation strategy. The credit union will completely be unable to access components like the internet, website, online banking facilities, email, credit card authorizations etc. for any business or organization that is based on the internet, this could create a problem.
- Blackholing must be carried out until the DDoS attack is over, or until the threat has disappeared. This could take hours, days, weeks or even months. Suspending the services of a system for this long could cause denial of service again. Customers accessing a website would no longer prefer using it if it stops working for a long period of time. The organization under attack could lose its reputation thus resulting in reputational risk. Reputational risk can break the trust that customers have in the organization. The organization is no longer productive if its services are suspended for a long period. DDOS attacks are often launched so that it can cover up a larger attack that is about to take place and an unresponsive system becomes easier to attack.
- When we use connectionless and unreliable protocols like UDP, it does not send a notification back to the source that it's packets were lost. If this was a legitimate user, they would never know that their packets have disappeared.
- When an attack occurs where the attacker uses IP address spoofing, this method can become useless.
- The problem is that good traffic is also dropped, and this was the actual aim of the attacker as well. We know that the attacker launches a DDOS attack with the aim of denying service to actual users. When we use a black hole to redirect all the traffic to a null route, we are actually doing the work for the attacker.
- The DDoS attack compromises the "availability" of the system but blackholing also does the same.

It can be useful when the target is a small site that is a part of a large network, in which case, it protects the larger network from the effects of the attack. Thus, we can conclude that blackholing results in more harm than good.

3. DNS SINKHOLING

[13]DNS sinkhole is used to detect and prevent DOS attacks and other malicious activity by redirecting all the bad traffic to an alternate server. Imagine we have two servers, one for our basic operations and another to back up data. If we are suddenly faced with a DOS/DDoS attack we can avoid it by having an extra server to redirect all the traffic to. This is what a sinkhole is. DNS is a service that is used to access the internet. A DNS sinkhole routes traffic to a valid IP address which analyzes the traffic and rejects the bad packets which is handled by researchers so that each of these packets can be later analyzed by them. In other words, it redirects the malicious traffic to a destination that is given by the security experts and researchers. This destination is what we call sinkhole. Sinkholes are usually used to analyze botnets which causes DDOS attacks by sending the malicious traffic from them to the sinkhole. This information helps the researchers understand more about the attack and the attacker. It is a standard DNS server which gives out addresses that cannot be routed so that the attacker can never get access to the actual website. Here, wrong information is given out about a domain name to prevent its use. It spoofs the authoritative DNS servers for the malicious hosts and domains. The DNS forwarder is made to return fake IP addresses to these hosts and domains. When the client requests to resolve this address, the sinkhole will send it an address that is not routable. This makes the connection to the target impossible. Whenever a new domain is added, it is under the control of the sinkhole admin and it is not possible to access the original domain. Using this method, attacked clients can be easily recognized.

One way that sinkholing prevents DDOS attack is by interrupting the names of the DNS that the botnets are designed to use in coordination. It stops the botnet from communicating with the original server while they are stuck in the sinkhole. DNS sinkhole can also be used by organizations to restrict access to various websites. Whenever a user try to access it, an error message will be shown. This reduces the risk of being attacked to a great extent as accidental clicks and opening of malicious websites is what allows an attacker to access a system to turn it into a zombie computer. Here the authoritative DNS server is impersonated and returns sinkholed addresses.

Essentially, a sinkhole is used when most of the system is almost completely compromised by the DDoS attack. It helps to get a detailed study of the DDoS attack to stop it from happening at other servers. It also helps to isolate the bad traffic so that it doesn't spread to other servers. The maintenance of a sinkhole is simple and more effort will

have to be spent researching on the data that is retrieved from the sinkhole. It is very inexpensive to set up and to maintain. Installing it on a virtual platform can further reduce costs. It is highly scalable and very effective.

3.1. WORKING

First, the system receives malicious packets. The compromised client resolves the malicious domain from these packets. The sinkhole now intercepts this malicious domain. The malware inside this client tries to connect to a known malicious domain which is configured in the DNS sinkhole. The request is sent to the sinkhole and it provides the client with an internal address. This address is a redirect to IP that is controlled by the admin. Now, the IDS gets a custom alert on suspicious activity with the help of snort IDS.

3.2. WANNACRY ATTACK & SINKHOLING

[14]WannaCry ransomware attack is a cyber attack that affected systems around the world in 2017. The attack was carried out by the WannaCry cryptoworm. It targeted the MS Windows operating systems and encrypted important data and files and demanded payments in bitcoins to decrypt the data back. The files would be deleted if the payment was not made. Marcus Hutchins started studying the attack to find flaws in it. He found out that the ransomware was programmed to check if a certain URL led to a website and noticed that the domain was not owned by anyone. He spent $10.69 and registered the domain himself. The ransom ware was checking to make sure that the domain was not active and to shut down if it was found active. The developers of the attack pointed the check to a domain that was static and not one that kept changing in random. Hutchins set up the domain and pointed it to sinholes set up by him to study the attack. The sinkhole could not decrypt the systems that were already affected but it bought them time to control the situation and for admins to patch their systems against attack.

3.3. DISADVANTAGES OF SINKHOLING

- [9]It has only a very limited effect in stopping botnets.
- The main limitation of a sinkhole is that it does not actually detect the malware or stop the attack, it only detects the indicators of the attack. These indicators are studied by the experts to know if the target is compromised.
- The sinkhole will be effective only if the malware uses the organization's DNS services and becomes ineffective is the attacker uses built in DNS services.
- Even though partial containment is done, the compromised computer might still try and attack the internal computers.
- It is usually used as a means of last resort when the system is almost completely compromised by the attack. Using it means that we have accepted defeat in protecting the system from the DDoS attack. It is not exactly a DDoS mitigation tool.
- They mostly help is fixing future DDoS attacks through research. It is a means of reacting to an attack, not preventing it.

4. CONCLUSION

Both blackholing and sinkholing have their advantages. Blackholing mechanism is best used when the target system under attack is a small part of a larger system. This will prevent the attack from affecting the larger system. Blackholing is best used when the system under attack is small. It causes minimum overheads.

Sinkholing is a means of admitting that we have given up. Sinkholing helps us to detect an attack but not prevent it. The systems that are infected cannot be cured of the attack, but studies can be done to further prevent the attack in the future. Sinkholing, though it is not a preventive mechanism, it helps us to develop prevention mechanisms against the attacker in the future so that the attack may not happen again. Thus sinkholing is best used as a research technique to study the attack.

REFERENCES

1. https://searchsecurity.techtarget.com/definition/denial-of-service
2. http://www2.ensc.sfu.ca/~ljilja/ENSC833/Spring01/Assignments/smc00_edited.pdf
3. https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/
4. https://en.m.wikipedia.org/wiki/Packet_drop_attack
5. https://www.cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf
6. http://www.networkers-online.com/blog/2009/02/black-hole-filtering/
7. https://www.techopedia.com/definition/23218/blackholing
8. https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/
9. "Botnets: A survey" by Sérgio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto, Ronaldo M. Salles
10. "A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques" by Usman Tariq, ManPyo Hong, Kyung-suk Lhee
11. "Distributed denial of service attacks" by F. Lau ; S.H. Rubin ; M.H. Smith ; L.Trajkovic
12. "Distributed Denial of Service Prevention Techniques" by B. B. Gupta, R. C. Joshi, Manoj Misra
13. https://en.wikipedia.org/wiki/DNS_sinkhole
14. http://theconversation.com/heres-how-the-ransomware-attack-was-stopped-and-why-it-could-soon-start-again-77745

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication