Amazon Web Services DDoS Attack 2020

Shona Start
Northumbria University, KF7002
shona.start@northumbria.ac.co.uk

Abstract - *The largest reported DDoS was conducted using CLDAP Reflection. This type of attack exploits vulnerable CLDAP servers using address spoofing to flood a victims' network with amplified packets. AWS Shield was able to mitigate this attack, however many other countermeasures and corrective measures could be implanted.*

Index Terms— CLDAP Reflection; DDoS; Amazon Web Service; LDAP Reflection.

I. Introduction

In February 2020 the largest reported distributed denial-of-service (DDoS) attack was mitigated by Amazon Web Services (AWS). This attack lasted for three days and peaked at 2.3 terabytes per second, a size approximately 44% larger than any network event previously detected on AWS. The attack targeted an AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection (Bisson, 2020). This technique has been used since at least 2016 (NHS, 2017) and is a highly sought-after protocol for DDoS attacks due to its ability to amplify DDoS traffic by 56 to 70 times its initial size (Shin, 2018). This report will outline the mechanism and exploits used to perform a CLDAP Reflection DDoS. It will also discuss the countermeasures and corrective measures that could have been taken to minimize this attack.

II. CLDAP Reflection DDoS

CLDAP is a UDP-based directory lookup protocol that is used as an alternative to the Lightweight Directory Access Protocol (LDAP). LDAP is an application protocol that was developed to connect, search, and modify shared internet directories. This protocol is one of the most widely used protocols for accessing username and password information in databases (Zeilenga, 2006). CLDAP was designed as a more efficient version to reduce overheads when retrieving data from these databases. However, the protocol was designed with security vulnerabilities, including a lack of integrity protection, missing confidentiality protection and anonymous access (Young, 1995) (Zeilenga, 2003). When a CLDAP server is incorrectly configured it has the potential to respond to any requests it receives, because of this CLDAP servers can be exploited by DDoS attackers.

A CLDAP Reflection DDoS attack relies on using address spoofing. Address spoofing is the use of packets to either hide the identity of the sender or/and to impersonate another IP address (Touch, 2007). This technique is often used in DDoS attacks, as attackers will impersonate their victim to send multiple queries to vulnerable CLDAP servers. The CLDAP server will not determine where the query was sent from or if the destination IP addresses is legitimate. So, on receipt of the requests the servers will send large, amplified response packets to the victims IP. CLDAP reflection attacks are often deployed using attack scripts. These scripts define the IP address of the victim, a list of CLDAP servers that are used for the attack and the time limit of attack. Using this method attackers can generate a massive number of requests (Choi & Kwak, 2017).

The first step of contracting a DDoS attacks is to first detect that an attack is in action, there are two main strategies for detection, these are inline detection and out-of-band detection. Out-of-band detection is the use of monitoring tools to passively analyze packet data from outside of the direct traffic flow. An example of out-of-band security would be an Intrusion Detection System (IDS). Out-of-band detection can take several minutes to identify an attack giving attackers a chance to adapt. On the other hand, inline DDoS techniques can detect attacks in seconds. This type of detection uses network devices such as routers, switches, and firewalls which are placed directly in the traffic to actively analyze packet data. An example of in-line security would be an Intrusion Prevention System (IPS) (Dillard , 2020).

The attack on AWS was reportedly detected and mitigated using "AWS Shield" (Cimpanu , 2020). AWS Shield is a protective service set up for AWS that is designed to minimize DDoS attacks. The standard shield is provided to all AWS customers and protects against common network and transport layer DDoS attacks. However, the advanced shield provides further protection, including protection against application layer attacks and integration with AWS web application firewall (WAF). During an attack, the advance shield deploys network access control lists (ACL's) to network borders; doing this can provide protection against larger amounts of traffic by limiting the size of packets (AWS, 2021). It is not clear if the common or advanced shield was used but, because the advanced AWS shield can mitigate against large and sophisticated DDoS attacks it is likely this shield was used.

The AWS shield is a form of victim network defence. This means that the defense mechanism is deployed at the source network, from this location the defence mechanism can directly respond to an attack at its highest impact point. Other deployment locations include the intermediate network and the source network (Mirkovic & Reiher, 2004).

One method of source network attack prevention is port filtering; this is the control of network packets into or out of a network based on their port number. A port number is a 16-bit integer stored in the header of a packet. This number identifies the way packets are handled once they reach a network (Cotton, et al., 2011). CLDAP uses UDP port 389 (Touch, et al., 2021) blocking this port can be effective, as the network is not expected to receive CLDAP responses from the internet. However, if the port needs more advance filtering, such as rate limiting, port traffic will be needed.

Rate limiting port traffic allows for a limit to be applied to a ports traffic. This slows down all traffic and can affect normal port function as no traffic will be able to exceed the set limit; so low limits are not advisable on frequent ports (Wong, et al., 2005). Another method of port filtering is IP filtering. IP filtering is the blocking or allowing of specific IP addresses through a port. Threat intelligence companies provide data on vulnerable servers, theoretically a tactic of prevention could be to block all the known IP addresses, however, there are thousands of known vulnerable CLDAP servers (A10, 2021). Alternately, a system could block all IP, except those of known servers (Arteaga & Mejia , 2017).

Another method of mitigating CLDAP Reflection DDoS attacks is to use an algorithm to check and control packet size. The paper "A Study on Reduction of DDoS Amplification Attacks in the UDP-based CLDAP Protocol" proposes an algorithm that detects CLDAP DDoS attacks by scanning servers to establish if a packet was sent from a vulnerable source. The algorithm then scans the packet to determine if an attack signature is present and sets a limit on the packet size in order to control the bandwidth of the CLDAP packets. This method should stabilise network during a DDoS attack (Choi & Kwak, 2017). This algorithm is an example of a reactive mechanism.

Reactive mechanisms are designed to quickly detect DDoS attacks and respond to them immediately, with minimal false positives. There a several types of reactive mechanisms, including signature detection and anomaly detection (Mirkovic & Reiher, 2004). Signature detection, sometimes called pattern detection, mechanisms use the signatures of known attacks and compare all packets for similar configurations. This type of detection can only uncover known attack types but has a very low false positive count. This method is often used by anti-virus software (Hussain & Sharma, 2019). On the other hand, anomaly-based detection uses a model of the standard traffic and system performance expected from a network in order to detect packets that are out size of normal system operation. This method is generally considered the more advanced option due to its ability to detect newer and more complex attacks, however, it does have higher false positive count (Purwanto, et al., 2014) . An example of anomaly-based detection is the IDS, Hogzilla (GuardianKey Cybersecurity, 2019).

III. Conclusion

Although AWS Shield was able to mitigate the CLDAP DDoS attack this service is only available to protect AWS customers so other countermeasures and corrective measures are needed. There are many options available, which can be used solo or in combination with each other. Detection of DDoS attacks is vital so that defence mechanisms can be activated. There are two main options for this: inline detection e.g., IDS and out-of-band detection e.g., IPS. Port filtering and rate limiting port traffic are effective ways of controlling traffic so that DDoS attacks cause less damage, however they can reduce the quality of normal network use if left in place permanently. Reactive mechanisms are an effective detection and defense system to have in place. Signature detection may cause less false positives but its inability to defend against new or altered attacks makes it lacking compared to anomaly detection.

IV. References

A10, 2021. *DDoS Weapons Intelligence Map.* [Online] Available at: https://threats.a10networks.com/

Arteaga, J. & Mejia , W., 2017. *CLDAP Reflection DDoS,* s.l.: Akamai.

AWS, 2021. *How AWS Shield works.* [Online]
Available at:
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html

Bisson, D., 2020. *Amazon Web Services Mitigated a 2.3 Tbps DDoS Attack.* [Online]
Available at: https://www.tripwire.com/state-of-security/security-data-protection/amazon-web-services-mitigated-a-2-3-tbps-ddos-attack/

Choi , S.-J. & Kwak, J., 2017. *A Study on Reduction of DDoS Amplification Attacks in the UDP-based CLDAP Protocol.* Kuta Bali, Indonesia, 4th International Conference on Computer Applications and Information Processing Technology (CAIPT).

Cimpanu , C., 2020. *AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever.* [Online]
Available at: https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/#:~:text=Amazon%20said%20its%20AWS%20Shield,in%20mid%2DFebruary%20this%20year.&text=The%20Netscout%20and%20GitHub%20DDoS,servers%20to%20reach%20massive%20bandwidth

Cotton, M. et al., 2011. *RFC 6335: Internet Assigned Numbers Authority (IANA) Procedures for the Management,* s.l.: Internet Engineering Task Force.

Dillard , J., 2020. *The 101 Series: Out-of-Band vs Inline Network Security.* [Online]
Available at:
https://www.garlandtechnology.com/blog/the-101-series-out-of-band-vs-inline-network-security

GuardianKey Cybersecurity, 2019. *Hogzilla IDS.* [Online]
Available at: https://ids-hogzilla.org/

Hussain, A. & Sharma, P. K., 2019. Efficient Working of Signature Based Intrusion Detection Technique in Computer Networks. *International Journal of Scientific Research in Computer Science Engineering and Information Technology,* pp. 60-64.

Mirkovic, J. & Reiher, P., 2004. A Taxonomy of DDoS Attackand DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communications Review,* 34(2), pp. 39-54.

NHS, 2017. *CLDAP Used in DDoS Attacks.* [Online]
Available at: https://digital.nhs.uk/cyber-alerts/2017/cc-1333

Purwanto, Y., Kuspriyanto & Rahardjo , B., 2014. Traffic Anomaly Detection in DDos Flooding Attack. *8th International Conference on Telecommunication Systems Services and Applications (TSSA),* pp. 1-6.

Shin, D., 2018. *How to Defend Against Amplified Reflection DDoS Attacks.* [Online]
Available at:
https://www.a10networks.com/blog/how-defend-against-amplified-reflection-ddos-attacks/

Touch, J., 2007. *RFC 4953: Defending TCP Against Spoofing Attacks,* s.l.: Network Working Group.

Touch, J. et al., 2021. *Service Name and Transport Protocol Port Number Registry.* [Online]
Available at:
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=

Wong, C., Bielski, S. & Wang, C., 2005. Empirical Analysis of Rate Limiting Mechanisms. *International Workshop on Recent Advances in Intrusion Detection,* Volume 3858, pp. 22-42.

Young, A., 1995. *RFC 1798: Connection-less Lightweight X.500 Directory Access Protocol,* s.l.: Network Working Group.

Zeilenga, K., 2006. *RFC 4510: Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map,* s.l.: Network Working Group.

Zeilenga, Z., 2003. *RFC 3352: Connection-less Lightweight Directory Access Protocol (CLDAP) to Historic Status,* s.l.: Network Working Group.