**Network-based Cybersecurity Incident**

In February 2020, ​Amazon Web Services​ (AWS), the 800-pound gorilla of everything cloud computing, was hit by a gigantic Distributed Denial of Service (DDoS) attack. This was the most extreme DDoS attack in recent history, and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim’s IP address by 56 to 70 times.

The attack lasted for three days and peaked at an astounding 2.3 terabytes per second. While the ​disruption caused by the AWS DDoS Attack​ was far less severe than it could have been, the sheer scale of the attack and the implications for AWS hosting customers potentially losing revenue and suffering brand damage are significant.

**1.​** ​**The link below is to an article that discusses the AWS DDoS attack in more detail. https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-t**

**bps/**

As you read through it, pay special attention to how the attackers were able to abuse CLDAP to carry out a ​reflection attack and combine it with an amplification attack to deny access to the target container.

**2.​** ​**Answer the following questions regarding the attack itself:**

What is CLDAP and what is it normally used for?

* Connection-less Lightweight Directory Access Protocol is an addition to the TCP-based LDAP protocol that uses an UDP-based directory lookup protocol. On Microsoft Active Directory networks, where clients typically use it to retrieve server information, CLDAP is most frequently encountered.

What are the ​two primary benefits to threat actors of amplification attacks?

* These attacks have two benefits: first, the attacker's payload can be amplified to generate 5x, 10x, or 100x the traffic from their requests; second, they can use spoofing to mask the attacker's identity while directing the payloads at a chosen target.

What are the five DDOS weapons that are even more prevalent than CLDAP?

* TFTP
* DNS Resolver
* Portmap
* SNMP
* SSDP

What is meant by a “zero trust model?”

* The principle of zero trust is based on the idea that companies should just not expect to trust anything that is either inside or outside the network perimeter. Any attempt to connect to the network must be validated before access is permitted.

How can enterprises protect themselves from these kinds of attacks?

* An efficient DDoS mitigation technique to counter the CLDAP reflection and amplification attack is to block or rate-limit traffic on port 389 across the internet. Alternate configurations include TCP and encrypted LDAP.
* The shared-responsibility approach should be used in cloud environments.
* Using a zero-trust model, businesses should actively safeguard applications in multi-cloud environments.
* Another layer of a zero-trust system that can report on network anomalies, block undesired traffic, and lessen attacks is DDoS protection.