What is CLDAP and what is it normally used for?
CLDAP is an acronym for Connectionless Lightweight Directory Access Protocol which is a DDoS reflection attack
What are the two primary benefits to threat actors of amplification attacks?

The 2 primary benefits are that the CLDAP is able to amplify their payload which can multiply the traffic from their request, and they are able to spoof and essentially hide themselves among the traffic to hide their tracks while targeting the payload at a specific target of their choice. This reminds me of playing the original assassins creed trilogy with the main character Ezio Auditore and throwing gold coins to attract people to a specific location so you can hide among them to not attract the guards so they dont notice you.

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

The top 5 DDoS weapons are from top to bottom According to the article “AWS hit by Largest Reported DDoS Attack of 2.3 Tbps” are from top to bottom : Portmap, SNMP, SSDP, DNS Resolver, and TFTP.

What is meant by a “zero trust model?”

To basically trust no one inside and outside the network. The Zero trust model would have a set of rules such as The network is always assumed to be hostile, External and internal threats exist on the network at all times, Every device user, and network flow is authenticated and authorized, Policies must be dynamic and calculated from as many sources of data as possible. This is what the Zero trust network would assume to help secure the network from a DDos attack, the source “Online Gaming Needs a Zero-Trust DDoS Defense” gives in great detail on how a zero trust network would be implemented and how it would work.

How can enterprises protect themselves from these kinds of attacks?
Enterprises are able to protect and prevent these attacks by following the guidelines the article “AWS hit by Largest Reported DDoS Attack of 2.3 Tbps” lists so you aren't the next headline in a DDoS attack “ Blocking or rate-limiting port 389 traffic from the internet is an effective DDoS protection method to mitigate the CLDAP reflection and amplification attack, especially if it is not expected to receive CLDAP responses from the internet. Alternatively, TCP or encrypted LDAP configurations can be used. it’s important to ensure that you have baselines for your traffic, practice zero-trust DDoS defense best practices, and keep up to date on the latest DDoS attack trends.”

Link to the websites :
https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/
Online Gaming Needs a Zero-Trust DDoS Defense | A10 Networks