**What is CLDAP and what is it normally used for?**

CLDAP, or Connection-less Lightweight Directory Access Protocol, is a [UDP-based directory lookup protocol](https://www.rfc-archive.org/getrfc.php?rfc=1798#gsc.tab=0) complementing the TCP-based LDAP protocol. CLDAP is designed to reduce the connection overheads at retrieving organizational resource information from a directory service database when using LDAP.

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

These attacks have two primary benefits: first, amplification of the attacker’s payload could generate 5x, 10x or 100x the traffic from their requests, and second, they can spoof to hide the attacker’s tracks while targeting the payloads at a specific target of their choice.

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

Portmap, SNMP, SSDP,DNS Resolver,TFTP

**What is meant by a “zero trust model?”**

Enterprises should tightly secure applications in multi-cloud environments using a [zero-trust model](https://www.a10networks.com/blog/online-gaming-needs-zero-trust-ddos-defense/), for example, to decide what should and should not be exposed. [DDoS protection](https://www.a10networks.com/solutions/network-security/ddos-protection/) is another layer in a zero-trust model that can report on network anomalies, stop unwanted traffic, and mitigate attacks. In cloud environments, the shared-responsibility model should be employed as security is not just the provider’s responsibility. This, again, points to the need for a zero-trust security approach and mindset.

**How can enterprises protect themselves from these kinds of attacks?**

Since the reflected CLDAP packets all come with UDP port 389 as the UDP source port, 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.