# CLDAP Reflectors On The Rise Despite Best Practice

Black Lotus Labs



Posted On October 24, 2022

## Executive Summary

The sophistication of threat actors' DDoS strategy and tactics continues to evolve rapidly in response to improved mitigation-side efforts. Actors have complicated filtering and firewalling by bringing a more diverse set of vectors to the attack, attacking at multiple network layers at the same time and automating changes to the mix of vectors at attack time – perhaps even in response to the ongoing mitigation efforts. Much of this growing sophistication centers around increasing the number of ingredients employed in an attack. A year ago, Black Lotus Labs wrote about our work

tracking UDP reflectors. In that article, we explained that despite the industry's firm understanding of the mechanics of UDP reflection, as well as the fact that most of these UDP services vulnerable to reflection are accidental configurations, we continue to find plenty of vulnerable services out there, ready and waiting to generate a voluminous stream of junk traffic directed at a DDoS target of choice.

While many vectors of UDP reflection would be nullified entirely with broad adoption of well-known best practices, this simply has not happened broadly enough to counter the threat. By leveraging our unique visibility into internet traffic, Black Lotus Labs is working to collect more data on these UDP reflection vectors with an eye towards informing next-generation mitigation strategy.

One of the most common UDP services in these multi-vector attacks is the Connectionless Lightweight Directory Access Protocol (CLDAP). With a high Bandwidth Amplification Factor (BAF) of 56 to 70x and common deployment onto systems provisioned with healthy bandwidth, CLDAP reflectors reliably add traffic volume to the DDoS recipe. Hopefully, the internet community can eventually clean up these exposed services. In the meantime, we can analyze and report on the span of open CLDAP reflectors on the internet today, as well as some of our findings related to the strategy and tactics behind their use in DDoS attacks.

## The CLDAP Service

CLDAP is a UDP implementation of the LDAP protocol. While the LDAP protocol is an open standard implemented by a variety of services, the full CLDAP specification was never completely implemented in any successful product. Microsoft's Active Directory service features a partial CLDAP implementation that exposes only a single command, the LDAP ping. This command is not a directory-related command; it's used by Windows clients attempting to discover a service via which they may authenticate users. While it's hard to imagine why someone would design their network topology such that a client would need to discover a local authentication service over the open internet, it happens. The motivations of the deployment are less salient than the simple fact that, when exposed to the public internet, the service is open to reflection.

When the first report about a new UDP reflection vector, CLDAP, was published, there were tens of thousands of CLDAP instances available for reflection with observed rates, via just the CLDAP vector, of up to 24 Gbps. Since then, CLDAP usage in DDoS attacks has trended up and down, as

have the total numbers of them available. After their discovery, the total count of open CLDAP reflectors dropped, likely due to the awareness brought by media attention. However, the spike in DDoS that occurred during the beginning of the pandemic in 2020 brought with it a return of CLDAP reflection.

## Current CLDAP Numbers

Black Lotus Labs leverages visibility across the Lumen network, one of the largest and most deeply peered global IP backbones, to identify, track and disrupt malicious – or in this case, misused – infrastructure. By isolating the traffic pattern of CLDAP activity, we created a validator to flag suspected reflectors in our global telemetry. In addition to locating and validating CLDAP instances, we then pivot to monitoring their behavior over time to baseline normal traffic against anomalous traffic. When we see traffic that looks like DDoS, we return to our telemetry to better assess the attack and enhance our validation models to continue tracking the evolving morphology of DDoS strategy and tactics. We then notify the likely unsuspecting owners of these vulnerable services of the problematic activity. With this in mind, we are tracking the current set of open CLDAP reflectors on a daily basis, and our analysis shows they are on the rise again: we've observed a more than 60% increase over the last 12 months, moving from the 7K range to over 12K. Below are some of our other recent findings.

### Open CLDAP Reflectors

Wondering about the lifecycle of an open CLDAP reflector, we looked at the longevity of the instances we track. Interestingly, we see some of these CLDAP reflectors live for a long time, while others disappear quickly. The following shows a recent snapshot of the percentages of open CLDAP reflectors by age.

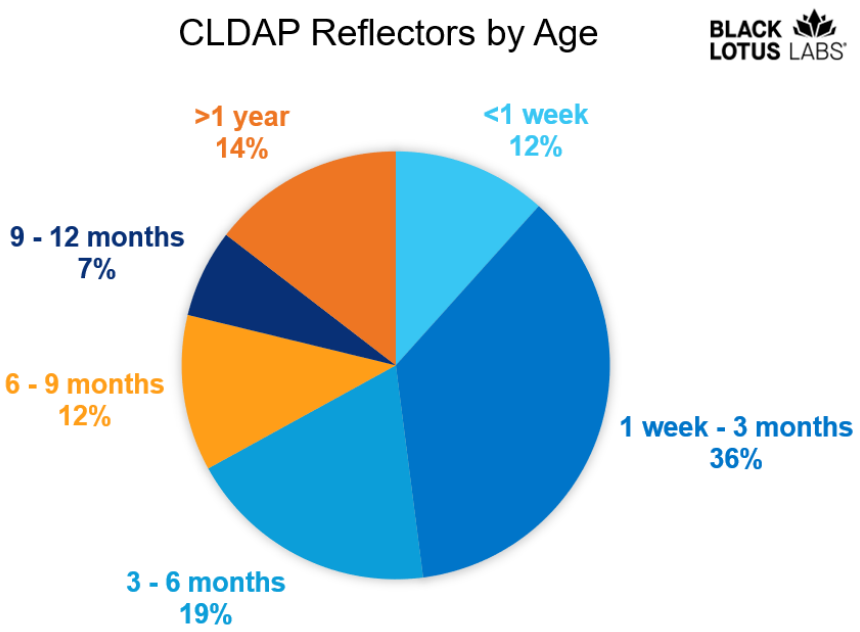


Figure 1: Percentages of confirmed CLDAP instances by age as of Oct. 1, 2022

| Age | Percentage |
|---|---|
| < week | 12% |
| Week to 3 months | 36% |
| 3 to 6 months | 20% |
| 6 to 9 months | 11% |
| 9 months to year | 6% |
| More than one year | 15% |
| TOTAL | >12K |

As you can see, roughly 14% have been around longer than a year. On the other hand, the generation less than a week old is similar in size. On the whole, these 12,142 reflectors average 131 days in age. Based on our current analysis, we assess there are two types of open CLDAP reflectors: accidental deployments and intentional deployments. In this case, an intentional deployment would mean that the system we track as an open CLDAP reflector is also a legitimate Domain Controller for an organization's MS network domain; these we would expect to be long-lived, hence a large count in the oldest age bin. At the other end of the spectrum, we observe an accidental deployment that is a trivial instance stood up for some non-production reason, perhaps a network engineer playing with some feature as part of a discovery or POC effort, then forgetting to decommission the instance.

## Veteran Reflectors

Since some reflectors can live so long, might they also be seasoned veterans of many DDoS campaigns? In our humble opinion, some of these

venerable CLDAP services have earned a well-deserved retirement. Looking back at the dozen or so largest DDoS events containing a productive CLDAP vector, we do see significant re-use of reflectors. In fact, the levels of re-use are so high that we assess the bit rates achieved towards a specific target are blunted by virtue of the reflectors being leveraged simultaneously by separate attackers.

In our recent data, we can easily find instances of long-lived reflectors participating in multiple DDoS events over time. As a case study, let's consider a CLDAP service hosted on an IP address associated with telecommunications provider in North America. This CLDAP instance has been a confirmed reflector in our reputation system for a full year, putting it well into the long-lived category. Focusing on recent months, we see this reflector directing problematic amounts of traffic towards a range of targets. The specific targets change, but the reflector dutifully directs several Gbps of traffic when called to do so. Sometimes the target is a single IP, sometimes a whole network prefix. Sometimes the targets change in a matter of hours; other times the same targets are hit for days or even weeks.

The graph in Figure 2 shows the repeated use of this reflector in DDoS events over the past three months.

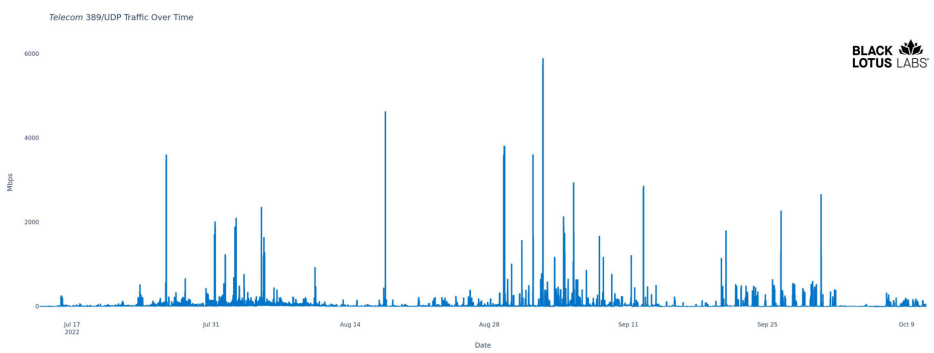


Figure 2: North American Telecom Associated Reflector's repeated DDoS activity July – October 2022

Looking at the graph, the baseline traffic rate is down around 20 Mbps or less, but we see plenty spikes of up to 300 times the baseline traffic. In addition to the fact that spikes stand out so proudly above the baseline, indicating highly anomalous traffic rates, we can further corroborate these as actual DDoS events by looking at the targets of the anomalous traffic rates. This is, in fact, how we found this hard-working reflector: it was located by first looking for targets that received the highest incoming traffic from 389/UDP. After noting this IP's role in one of these strong attacks, we then analyzed all the traffic generated by it against all

destinations. As we expected, a well-provisioned, long-lived reflector sees repeated use as a weapon in DDoS.

If we zoom in on a specific time range, we can get a clearer picture of how this reflector is used. In early September, we see the IP sending as much as 6 Gbps at a single target system, a game hosting provider in South America. This is the highest bit rate achieved by the reflector this past summer, and it's high enough to make us wonder about the key ingredients in leveraging an array of these reflectors for maximal power: we have a single reflector generating up to 6 Gbps. Even if the average reflector has only a fourth of the bandwidth as this particular host, the quick math suggests that marshalling even 10% of existing CLDAP reflectors in an attack could generate traffic in the Terabits per second range (1.5 Gbps x 1000 = 1.5 Tbps). Let's hope all of the CLDAPs out there aren't as heavily provisioned as this one.

## Geographic Distribution of Open CLDAP Reflectors

One question we sought to address was whether there are any discernable hotspots for CLDAP reflectors. Below is the geographic distribution of the open CLDAP reflectors we track.

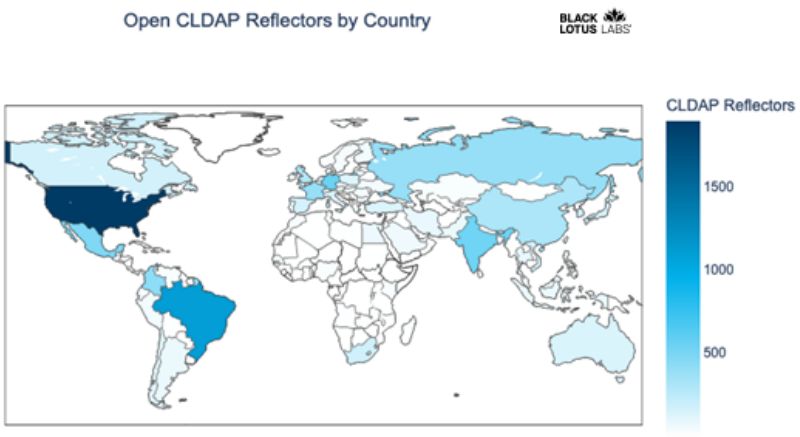


Figure 3: Geographic distribution of known open CLDAP instances

As you can see, the spread of CLDAP reflectors spans the globe, with the greatest distributions located in the U.S. and Brazil, followed at some distance by Germany, India and Mexico. While we are not able to produce summary data on the whole set of reflectors yet, initial ad hoc analysis suggests a strong correlation between age of reflector and frequency of use in DDoS. It appears that new reflectors are unknown to the attackers for some period of time. Once the reflector is discovered, its frequency of usage rises over time.

## Profiles of Some Top Talkers

As with many other reflection vectors, it's hard to imagine a valid reason for these CLDAP services to be exposed to the open internet. This makes us wonder about the nature of these systems. Lumen tracks known threats observed and detected by both our own analysts, machine learning algorithms, honeypots and third-party intelligence. If we take this data into account, we see that many of the reflectors have been observed being abused in other ways.

One of the more sensible patterns we see suggests a specific profile for the reflector system. We start with knowing that these reflectors are MS Domain Controllers hosting Active Directory services. We can build on this story by enriching the profile with reputation data. Let's look at a couple of the more active CLDAP reflectors to see what else we can surmise.

First, let's consider a host associated with a regional retail business in North America. We've been tracking this confirmed CLDAP reflector for more than nine months, during which time we have observed a repeated habit of it throwing Gigabits per second of traffic at an array of targets. As seen below, this reflector has participated in numerous DDoS events, as evidenced by numerous spikes of 389/UDP traffic of more than 1,000x the baseline traffic rates.

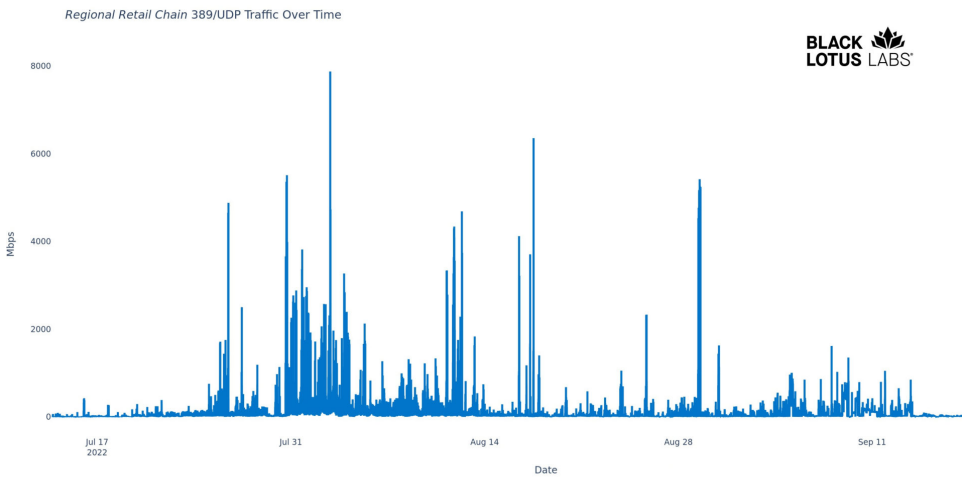


Figure 4: Regional retail reflector's repeated DDoS activity July – September 2022

This data includes peak moments where the service is emitting up to 7.8 Gbps of CLDAP traffic, thus making it a particularly potent reflector. When we look through our reputation data, we find a litany of suspicious behaviors. Turns out, it's also open to DNS reflection, and running RDP and SMB services vulnerable to exploitation. It has, on occasion, presented certain bot-like behaviors; RDP and SMB vulnerabilities are common

vectors for bot takeover. Trying to build a story out of these facts leads us to see this system as the MS Domain Controller in a small organization. Small sites might only have a single data center, and they would also likely host SMB, DNS and RDP. Additionally, it's inherent that smaller organizations, on the whole, will have less sophisticated security practices, thus suggesting more likelihood of being infected with bot malware.

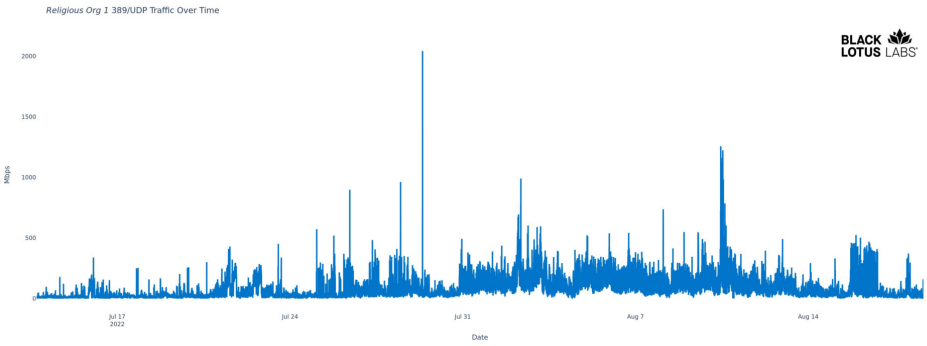


Figure 5: Religious organization reflector's DDoS activity July – August 2022

This pattern repeats in our data; Figure 5, above, depicts the extracurricular activity of a reflector associated with an IP owned by a religious organization in North America. As a case study in reflectors, this is almost identical to the previous one. This 18-month-long member of our confirmed reflector list has demonstrated strong pipes with a peak bit rate, during the last few months alone, of more than 2 Gbps. This one has also been tagged as an open DNS reflector, and as a bot for multiple malware families based on bidirectional communications with confirmed C2s on the expected C2 ports. This pattern does not hold across all the reflectors we see, but it's strong among the more powerful reflectors.

Speaking of more powerful reflectors, we saved the best for last. The following reflector, also affiliated with a religious organization, routinely generates more than 10 Gbps of traffic. Our reputation data again suggests a well-provisioned MS Domain Controller with the same set of issues as the others.

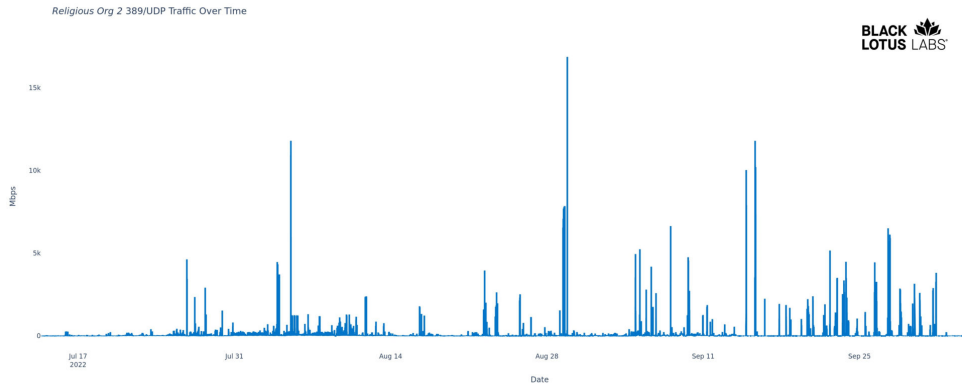

Figure 6: Religious organization reflector's high traffic DDoS activity July – September 2022

The four biggest spikes in Figure 6 exceed 10 Gbps, and the big one approaches 17 Gbps. This traffic is perhaps strong enough to DoS some less well provisioned servers all by itself. In theory, a hundred of these, working in unison, could generate a Terabit per second of attack traffic.

We have been confirming this IP as an open CLDAP reflector since late June. Our reputation data includes reports of the system being an open DNS reflector, having a vulnerable SMB service exposed and having bi-directional communications with confirmed C2s for multiple malware families.

With the reflectors we analyzed, we see a strong pattern of increased frequency of anomalous spikes the longer the open reflector exists. As we suggested earlier, it appears that frequency of use in DDoS increases with age. This makes sense as we would expect that attackers would need some time to locate new reflectors and update their arsenal.

# Conclusion

The past has shown when the industry comes together to address broad and significant threats, we can work together to make an impact. With CLDAP reflectors once again on the rise, and the potential for CLDAP reflectors to generate record-setting bit rates, now is the time for a similar effort in addressing CLDAP reflection.

Black Lotus Labs has notified the owners of vulnerable CLDAP services exposed to the internet in the Lumen IP space and we will continue to track and analyze vulnerable CLDAP reflectors at large, as well as feed this intelligence into the Lumen Connected Security portfolio. We are working to expand notification to third-party legitimate hosts of CLDAP reflection activity and to block long-lived CLDAP reflector traffic from traversing the Lumen global backbone. We encourage the community to monitor for and alert on known CLDAP reflectors. We also advise the following:

- Network administrators: Consider not exposing CLDAP service (389/UDP) to the open internet.
  - If exposure of the CLDAP service to the open internet is absolutely necessary, take pains to secure and defend the system:
    - On versions of MS Server supporting LDAP ping on the TCP LDAP service, turn off the UDP service and access LDAP ping via TCP.
    - If MS Server version doesn't support LDAP ping on TCP, rate limit the traffic generated by the 389/UDP service to prevent use in

DDoS.
    - If MS Server version doesn't support LDAP ping on TCP, firewall access to the port so that only your legitimate clients can reach the service.
- Network defenders: Implement some measures to prevent spoofed IP traffic, such as Reverse Path Forwarding (RPF), either loose or, if feasible, strict. For more guidance, the MANRS initiative offers in depth discussion of anti-spoofing guidelines and real-world applications.

If you would like to collaborate on similar research, please contact us on Twitter @BlackLotusLabs.

This analysis was performed by Chad Davis.



BLACK LOTUS LABS CLDAP DDOS DDOS ATTACK DDOS REFLECTION