THREAT ADVISORY

CLDAP Reflection DDoS

Risk Factor: Medium

TLP: Green

Authors: Jose Arteaga & Wilber Mejia

Akamai

Issue Date: 4.3.17

1.0 / Overview / On October 14, 2016, the Akamai Security Operation Center (SOC) began mitigating attacks for what was suspected to be Connection-less Lightweight Directory Access Protocol (CLDAP) reflection. This new reflection and amplification method has since been confirmed by the Akamai Security Intelligence Response Team (SIRT) and has been observed producing Distributed Denial of Service (DDoS) attacks, comparable to Domain Name System (DNS) reflection in that most exceed 1 Gbps.

Similarly to many other reflection and amplification attack vectors, this is one that would not be possible if proper ingress filtering was in place. Potential hosts are discovered using internet scans, and filtering User Datagram Protocol (UDP) destination port 389, to eliminate the discovery of another potential host fueling attacks. This advisory will cover the distribution of these sources, methods of attack, and target industries observed.

2.0 / Attack Timeline / Since October 2016, Akamai has detected and mitigated a total of 50 CLDAP reflection attacks. Of those 50 attack events, 33 were single vector attacks using CLDAP reflection exclusively. Figure 1 provides a timeline of attacks, showing attack size and detailing if the attack was single or multi-vector.

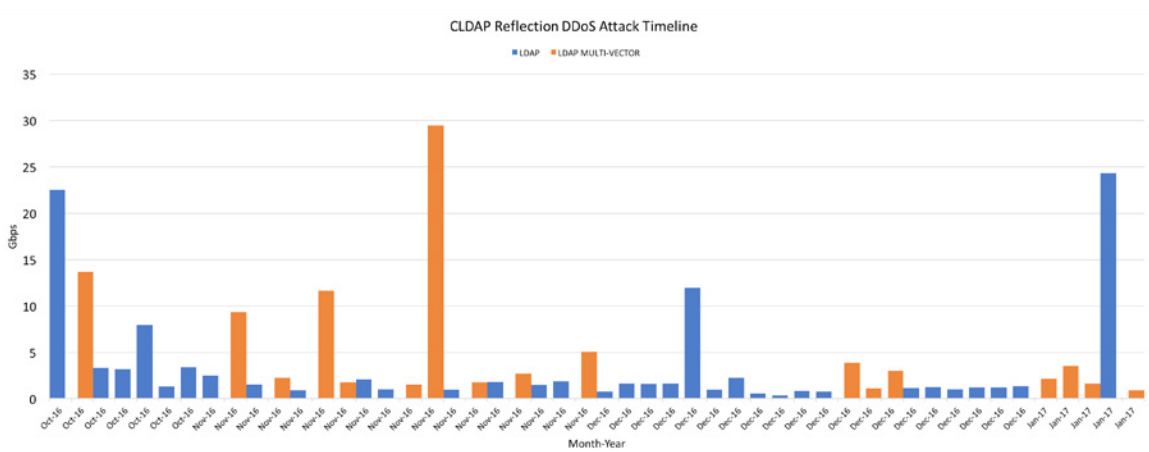

Figure 1: CLDAP reflection attacks from October 14, 2016 – January 13 2017. Attacks with additional vectors are orange.

While the gaming industry is typically the most targeted industry for attacks, observed CLDAP attacks have mostly been targeting the software & technology industry along with six other industries.

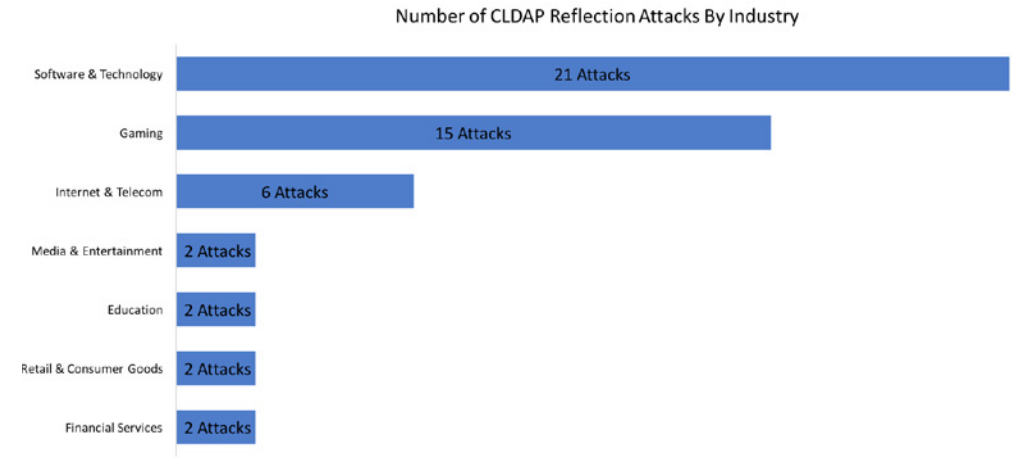

Figure 2: Target industry count for DDoS attacks containing CLDAP reflection.

2.1 / Highlighted Attack Attributes / On January 7, 2017, the largest DDoS attack using CLDAP reflection as the sole vector was observed and mitigated by Akamai. Attributes of the attack were as follows:

- Industry Vertical: Internet & Telecom
- Peak Bandwidth: 24 Gigabits per second
- Peak Packets per Second: 2 Million Packets per second
- Attack Vector: CLDAP
- Source Port: 389
- Destination Port: Random

```
CLDAP Reflection Attack – Largest Observed Response is 3,662 Bytes:

17:35:25.728099 IP A.A.A.A.389 > Z.Z.Z.Z.46414: UDP, bad length 3006 > 1472
17:35:25.728102 IP B.B.B.B.389 > Z.Z.Z.Z.38980: UDP, bad length 3662 > 1472
17:35:25.728106 IP A.A.A.A > Z.Z.Z.Z: ip-proto-17
17:35:25.728110 IP A.A.A.A > Z.Z.Z.Z: ip-proto-17
17:35:25.728115 IP B.B.B.B > Z.Z.Z.Z: ip-proto-17
17:35:25.728127 IP B.B.B.B > Z.Z.Z.Z: ip-proto-17
```

Figure 3: CLDAP reflection attack signature with 3,006 and 3,662 of respective response data.

Signatures of this attack reveal that it is capable of impressive amplification factors. After the first few waves of attacks using CLDAP, Akamai SIRT was able to obtain sample malicious Lightweight Directory Access Protocol (LDAP) reflection queries. The query payload is only 52 bytes and is discussed further in the "ATTACK & CLDAP OVERVIEW" section. This means that, the Base Amplification Factor (BAF) for the attack data payload of 3,662 bytes, and a query payload of 52 bytes, was 70x , although only one host was revealed to exhibit that response size. Post attack analysis showed that the average amplification during this attack was 56.89x.

This 24 Gbps attack was the largest mitigated by Akamai to date. In contrast, the smallest observed attack Akamai has seen using this vector was 300 Mbps, and the average attack bandwidth for a CLDAP attack has been 3 Gbps.

2.2 / ATTACK & CLDAP OVERVIEW / First described in RFC 1798, CLDAP has had additional functionality added by Microsoft. It was intended as an efficient alternative to LDAP queries over Transmission Control Protocol (TCP). Consequently, CLDAP does not support the full features available in LDAP.

During the initial stages of this attack, Akamai SIRT observed the following malicious CLDAP queries attempting to reflect LDAP response data to various targets. Figure 4 contains the queries observed during an actual CLDAP reflection attack. These were sourced from a handful of servers (the intended targets) destined for a few LDAP hosts.

```
13:55:57.962697 IP X.X.X.X.57852 > X.X.X.X.389: UDP, length 52
13:55:57.963784 IP X.X.X.X.33850 > X.X.X.X.389: UDP, length 52
13:55:57.964392 IP X.X.X.X.47097 > X.X.X.X.389: UDP, length 52
13:55:57.965226 IP X.X.X.X.47728 > X.X.X.X.389: UDP, length 52
```

Figure 4: Malicious CLDAP queries sent to destination port 389. Only 52 bytes of data per query.

Using the same data payloads observed above, this query could be easily reproduced using a tool such as Scapy. Lab tests were conducted using a virtualized instance of Windows Server and Linux with Scapy. Sending the query from the Linux host to the Windows server initially produced no response. However, once the Windows server was setup as a domain controller, and began to listen on UDP and TCP port 389, the following transaction was captured.

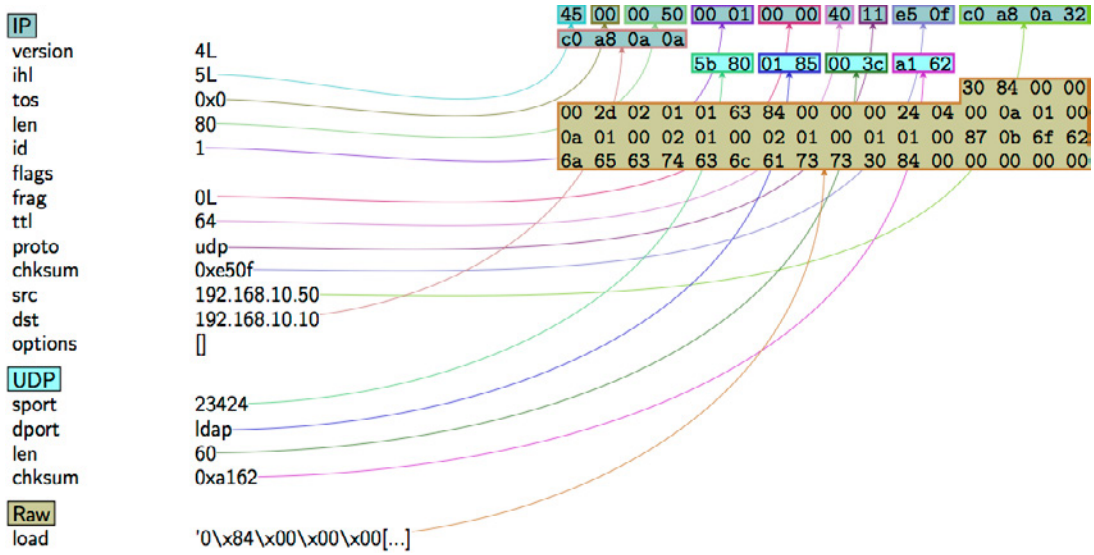

Figure 5: CLDAP query packet.

CLDAP Query Test and Response in a Lab Test

```
11:37:04.281079 IP linux_host.23424 > windows_server.389: UDP, length 52
11:37:04.282207 IP windows_server.389 > linux_host.23424: UDP, bad length 2962 > 1472
11:37:04.282223 IP windows_server > linux_host: ip-proto-17
11:37:04.282227 IP windows_server > linux_host: ip-proto-17
```

CLDAP Sample of Printable Response Text

Packet 1

```
2[`0vdm0e0&currentTime120170213163705.0Z0WsubschemaSubentry1><CN=Aggregate,CN=Schema,CN=Configu-
ration,DC=locallab,DC=local0
dsServiceName1zxCN=NTDS
Settings,CN=WIN-U5K3VOF1HE3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,D-
C=locallab,DC
<snip>
```

Packet 2

```
<snip>
WIN-U5K3VOF1HE3.locallab.local0GldapServiceName10.locallab.local:win-u5k3vof1he3$@LOCALLAB.LOCAL0{
serverName1igCN=WIN-U5K3VOF1HE3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=locall
ab,DC=local0supportedCapabilities11.2.840. 113556.1.4.8001.2.840.113556.1.4.16701.2.840.113556.1.4.17911.2.840.
113556.1.4.19351.2.840.113556.1.4.20801.2.840.113556.1.4.22370isSynchronized1TRUE0"isGlobalCatalogReady1TR
UE0domainFunctionality160forestFunctionality160(domainControllerFunctionality160e
```

Figure 6: CLDAP query to Windows 2012 server with 2,962 byte reply.

The first 2 response payloads contained most of the data at a size of 1,472 bytes and 1,480 respectively. The last fragment contained the remaining 10 bytes. This is from a fresh instance of Windows Server 2012 R2, with no other option or setting adjustment. Other versions may produce different payload sizes.

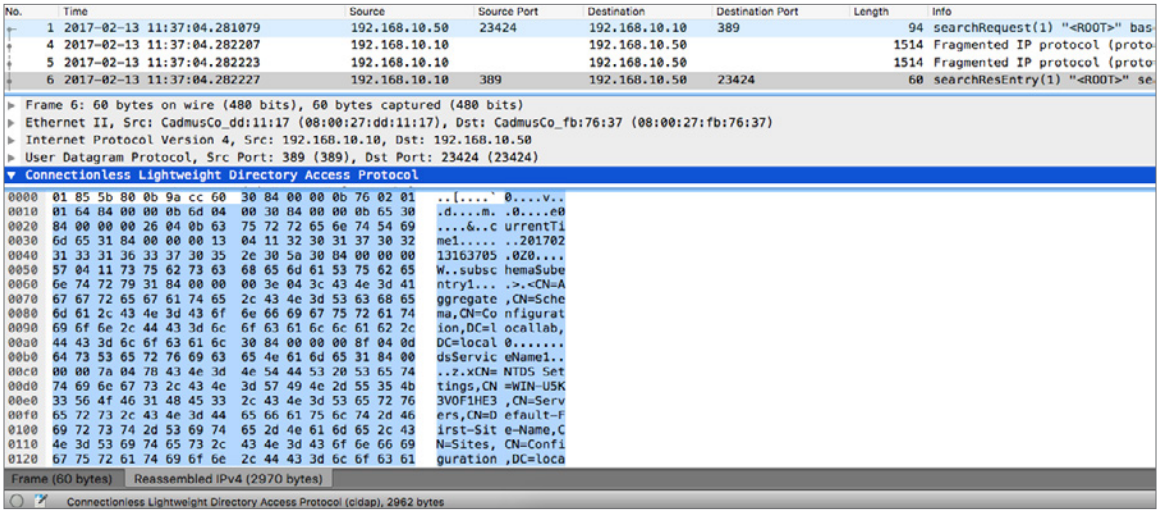

Figure 7: CLDAP lab generated response payload of 2,962 bytes.

The message size and contents can vary from what was observed during these attacks. This includes server configuration parameters and other settings.

The observed reflection-based attacks are launched using so called "attack scripts". These attack scripts are usually written using the C-programming language, and are very similar from one vector to another. In fact, there is minimal effort required to adapt one attack script to a completely different attack vector like CLDAP reflection. The options commonly available with these attack scripts are target_ip, target_port, list of reflectors, and time limit. When executed, the target IP becomes the source of all of the 52 byte query payloads. These are then sent rapidly to every server in the supplied reflector list. From there, the CLDAP servers do as they are designed and reply to the query. As a result, the target of this attack must deal with a flood of unsolicited CLDAP responses.

2.3 / Source Distribution / Combined with sources collected from both the Prolexic (PLX) routed mitigation solution and Akamai perimeter firewall, a total of 7,629 unique CLDAP reflectors were observed in attacks. The largest concentration of these were located within the U.S. This is based only on sources collected during actual CLDAP reflection attacks. The usable pool of CLDAP reflectors is larger as revealed by internet scanning.

Country	Count
Unites States	1,871
Germany	487
United Kingdom	484
France	436
Canada	376
Other	3,975

Figure 8: CLDAP reflector source country

Akamai SIRT also conducted an internet-wide scan for hosts exposed to CLDAP reflection abuse. This scan resulted in a total of 78,531 unique IP responses. While not as high as the number of hosts available with other reflection vectors with CLDAP, almost every host is a usable reflector.

In fact, 78,071 of those hosts responded with more than 1,500 bytes of data. The range of response sizes was anywhere from 1 byte to the max observed in attacks of 3,662 bytes. All hosts combined averaged 2,693.67 bytes of response for a 51.8x amplification factor.

2.4 / Top Countries With CLDAP Reflectors / (Internet Scan)

Country	Count
United States	17,980
Brazil	6,005
France	3,542
United Kingdom	3,495
Germany	3,426
China	3,177
Russian Federation	2,582
Canada	2,207
Colombia	2,072
India	1,987
Other	32,058

Figure 9: CLDAP unique source concentration by country.

2.5 / Top ASNs With CLDAP Reflectors / (Internet Scan)

ASN	Count
AS7922	2,787
AS16276	2,633
AS8075	2,443
AS18881	1,345
AS28573	1,122
AS4134	893
AS3215	884
AS8151	839
AS7018	825
AS24940	764
Other	64,302

Figure 10: CLDAP unique source centration by ASN.

3.0 / Mitigation / Mitigation for CLDAP reflection begins with filtering of the port in question. The attack is fueled by the number of servers on the Internet with UDP port 389 open and listening. Once a server is identified as a viable source for a CLDAP reflection attack, it will be added to a list of reflectors. Ingress filtering of the CLDAP port from the Internet will prevent discovery and subsequent abuse of this service. Most reflection methods, except DNS and NTP, do not require these ports to be exposed. An alternative is to apply an IDS rule, such as the snort rule below. This is specific to the requests observed so far but can be adapted to a more generic LDAP search request. This rule is suitable for alerting rather than mitigating and is intended to provide an indicator of an attempt to use your systems as part of a CLDAP reflection attack.

```
alert udp $EXTERNAL_NET any -> $HOME_NET 389 \
(msg: "CLDAP DDoS Abuse request"; \
flow: to_server; \
content: "|30840000002d02010163840000002404000a01000a0100020100020100010100870b-
6f626a656374636c6173733084000000000|"; dsize:52<>52; \
classtype:Reflection-Abuse; \
sid: 201700001; rev:1;)
```

Figure 11: Sample signature for detection of CLDAP abuse for potential reflectors.

4.0 / Conclusion / UDP based reflection attacks consistently comprise more than 50% of all attacks. With new vectors being discovered regularly and many persisting for years, it's a problem that won't likely go away anytime soon. One of the primary solutions, is filtering by the organizations hosting these services, and by Internet Service Providers (ISPs) providing home user Internet access. Unless there is a legitimate need for an organization to have CLDAP available over the Internet, there should be no reason to compound the DDoS reflection problem by exposing this protocol. External auditing policies are one means to provide reporting of services that can be potentially exploited as reflection attacks. For CLDAP, hosts aren't in the millions, as initially discovered with other reflection vectors, but the amplification factor has been enough to produce significant attack bandwidth with fewer hosts. Based on similarities shared by UDP reflection attack scripts, it is likely that CLDAP has been included, or will be included, into a full attack script, and integrated into the booter/stresser infrastructure. If it has yet to be included, we may have not seen the worse of these attacks.

5.0 / References /

- *https://www.scmagazine.com/zero-day-ddos-attack-vector-leverages-ldap-to-amplify-malicious-traffic/article/568309/*
- *https://packetstormsecurity.com/files/139561/LDAP-Amplication-Denial-Of-Service.html*
- *https://tools.ietf.org/html/rfc1798*
- *https://msdn.microsoft.com/en-us/library/gg593144.aspx*
- *https://www.us-cert.gov/ncas/alerts/TA14-017A*

Non-customers can submit inquiries through Akamai's hotline at 1-877-425-2624, the contact form on our website at *http://www.akamai.com/html/forms/sales_form.html*, the chat function on our website at *http://www.akamai.com/*, or on Twitter *@akamai*.

To access other white papers, threat advisories, and research publications, please visit our *Security Research and Intelligence section* on the Akamai Community.