

Emma Stensland

Reese Pearsall

CSCI 466

November 3, 2025

### Evidence 4 - Emotet Trojan

#### 1. What is the hash of the evidence PCAP file?

0x15a29d64af3a0e5ccee bfde7f4fc05241a18514b

#### 2. What is the IP address of the infected machine? Is this a public or private IP address?

10.3.1.101

#### 3. What is the MAC address of the infected machine?

00:08:02:1c:47:ae

#### 4. What is the IP address of the DNS server that is used by the infected machine?

10.3.1.3

#### 5. Find the initial piece of malware. Take a screenshot of the malicious packet/event.

Arrival Time: Mar 1, 2022 11:38:19.845463000 MST

http						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.225184	10.3.1.101	148.251.19.22	HTTP	279	GET /ggv3rjy/9/ HTTP/1.1
682	4.920004	148.251.19.22	10.3.1.101	HTTP	834	HTTP/1.1 200 OK (application/x-msdownload)
5247	1447.216547	209.15.236.39	10.3.1.101	TCP	1514	8080 → 49244 [ACK] Seq=156727 Ack=1020 Win=642
5811	1555.867586	209.15.236.39	10.3.1.101	TCP	1514	8080 → 49248 [ACK] Seq=35854 Ack=852 Win=64240
6290	1557.639443	209.15.236.39	10.3.1.101	TCP	1430	8080 → 49248 [PSH, ACK] Seq=432174 Ack=852 Win=

#### a. What is the filename of the malware?

B7tYH11h5gzY1sx.dll

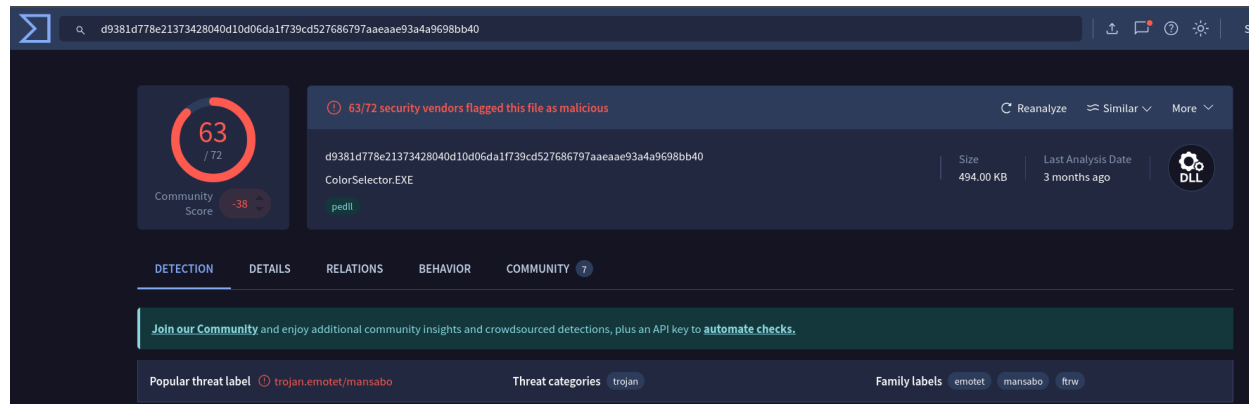
#### b. What is the file extension of the malware?

.dll

#### c. What is the hash of the malware?

99f59e6f3fa993ba594a3d7077cc884d

## 6. Plug the hash value into VirusTotal and take a screenshot. Is the file malicious?



It's malicious :(

## 7. What is the "name" associated with this malware?

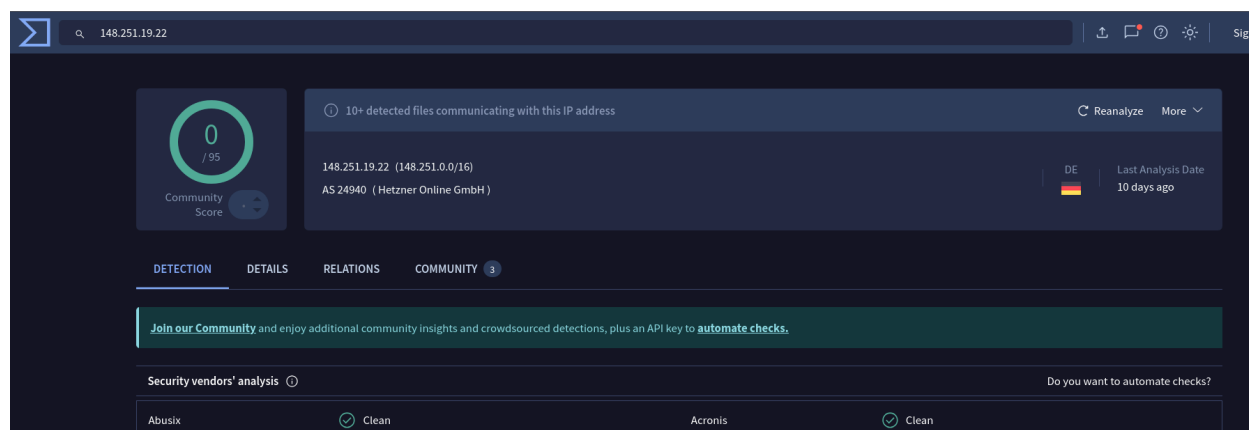
Emotet

## 8. What type of malware is it? (You can google common malware types if you don't know what this question is asking)

Trojan

## 9. What IP address did the malware come from? Plug the IP address into VirusTotal and take a screenshot. Is it a malicious IP address?

148.251.19.22



Not malicious.

**10. This IP address came from a DNS query. What is the hostname associated with this IP address? Plug the hostname into VirusTotal and take a screenshot.**

Query at: Mar 1, 2022 11:38:14.925459000 MST

To: diacrestgroup.com

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.3.1.101	10.3.1.3	DNS	77	Standard query 0x69c5 A diacrestgroup.com
2	0.005358	10.3.1.3	10.3.1.101	DNS	93	Standard query response 0x69c5 A diacrestgroup.com A 148.251.19.22
3	0.006547	10.3.1.101	148.251.19.22	TCP	60	48183 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.224886	148.251.19.22	10.3.1.101	TCP	58	80 → 49183 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.225033	10.3.1.101	148.251.19.22	TCP	54	49183 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

10/95 security vendors flagged this domain as malicious

Reanalyze More

diacrestgroup.com

Registrar: NAMECHEAP INC | Creation Date: 13 years ago | Last Analysis Date: 11 days ago

Malicious (alphaMountain.ai) | spyware and malware | Malware Sites | top-1M

DETECTION | DETAILS | RELATIONS | COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Malicious hostname associated with spyware.

**11. Use a WHOIS tool (there are tons of these tools online) to find out who is registered under that IP address and take a screenshot.**

The IP is from a German Data Center, Hetzner Online GmbH (Just a randomly provided IP)

### Whois IP 148.251.19.22

Updated 5 hours ago

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '148.251.19.0 - 148.251.19.31'

% Abuse contact for '148.251.19.0 - 148.251.19.31' is 'abuse@hetzner.com'

inetnum:        148.251.19.0 - 148.251.19.31
netname:        HETZNER-fsn1-dc11
descr:          Hetzner Online GmbH
descr:          Datacenter fsn1-dc11
country:        DE
admin-c:        HOAC1-RIPE
tech-c:         HOAC1-RIPE
status:         LEGACY
remarks:        INFRA-AW
mnt-by:         HOS-GUN
mnt-lower:      HOS-GUN
mnt-routes:     HOS-GUN
created:        2018-03-15T14:40:56Z
last-modified:  2018-03-15T14:40:56Z
source:         RIPE
```

## 12. Is there any evidence of communication with a command and control (C2) server?

Yes.

Mar 1, 2022 11:38:32.003299000 MST a connection with 147.139.134.226, a self-signed server, was requested from the infected machine. Connection ended on Mar 1, 2022

12:23:17.380554000 MST. This is shown to be a malicious IP address on VirusTotal:

```
ts: 2022-03-01T18:38:32.812897Z,
uid: "CxmuVm18hcmCbUigWa",
id: > {orig_h: 10.3.1.101, orig_p: 49188 (port=(uint16)), resp_h: 147.139.134.226, resp_p: 443 (port=(uint16))},
fuid: "FTAb7R2H1y52AF0JIa",
file_mime_type: null,
file_desc: null,
proto: "tcp" (zenum),
note: "SSL::Invalid_Server_Cert" (zenum),
msg: "SSL certificate validation failed with (self signed certificate)",
sub: "CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB",
src: 10.3.1.101,
dst: 147.139.134.226,
```

9/95 security vendors flagged this IP address as malicious

139.60.161.225 (139.60.160.0/22)  
AS 395839 (HOSTKEY-USA)

US | Last Analysis Date: 26 days ago

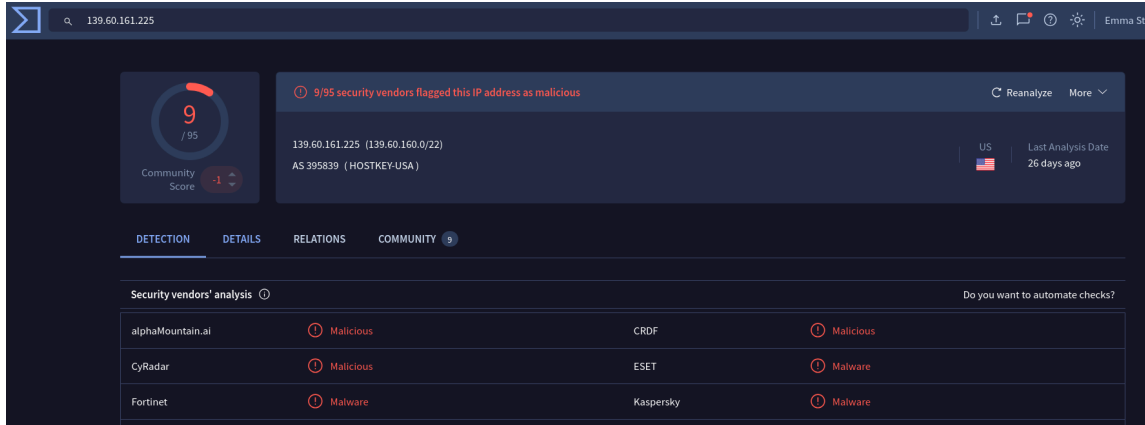
DETECTION DETAILS RELATIONS COMMUNITY (9)

Security vendors' analysis

alphaMountain.ai	Malicious	CRDF	Malicious
CyRadar	Malicious	ESET	Malware
Fortinet	Malware	Kaspersky	Malware

Do you want to automate checks?

Mar 1, 2022 12:04:14.768003000 MST a connection with 139.60.161.225 was requested from the infected machine. Connection was maintained to the end of the trace. This is shown to be a malicious IP address on VirusTotal:



139.60.161.225

9 / 95  
Community Score -1

9/95 security vendors flagged this IP address as malicious

139.60.161.225 (139.60.160.0/22)  
AS 395839 (HOSTKEY-USA)

US Last Analysis Date 26 days ago

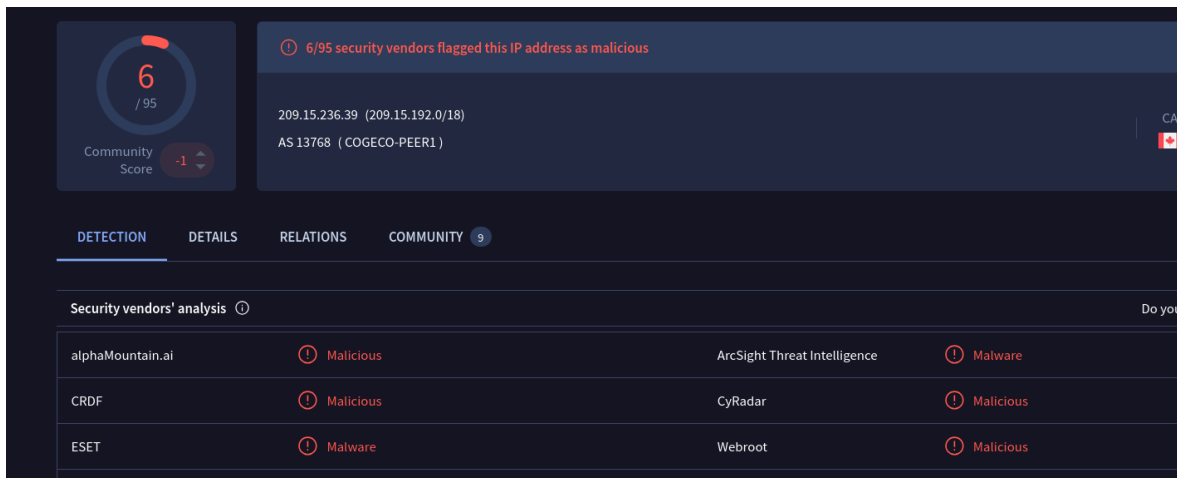
DETECTION DETAILS RELATIONS COMMUNITY 9

Security vendors' analysis

alphaMountain.ai	Malicious	CRDF	Malicious
CyRadar	Malicious	ESET	Malware
Fortinet	Malware	Kaspersky	Malware

Lastly, on Mar 1, 2022 11:38:26.842452000 MST, the connection to 209.15.236.39 was made. Connection was maintained until Mar 1, 2022 12:25:07.400187000 MST. This connection was also to an insecure IP:

```
{
  _path: notice,
  ts: 2022-03-01T18:38:27.175288Z,
  uid: "CuakM14VHT15oN0itd",
  id: {orig_h: 10.3.1.101, orig_p: 49184 (port=(uint16)), resp_h: 209.15.236.39, resp_p: 8080 (port=(uint16))},
  fuid: "Fh7Ner3FT9h2kxTdI8",
  file_mime_type: null,
  file_desc: null,
  proto: "tcp" (zenum),
  note: "SSL::Invalid_Server_Cert" (zenum),
  msg: "SSL certificate validation failed with (self signed certificate)",
  sub: "CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB",
  src: 10.3.1.101,
  dst: 209.15.236.39,
  p: 8080 (port=(uint16)),
  n: null,
}
```



209.15.236.39 (209.15.192.0/18)  
AS 13768 (COGECO-PEER1)

6 / 95  
Community Score -1

6/95 security vendors flagged this IP address as malicious

DETECTION DETAILS RELATIONS COMMUNITY 9

Security vendors' analysis

alphaMountain.ai	Malicious	ArcSight Threat Intelligence	Malware
CRDF	Malicious	CyRadar	Malicious
ESET	Malware	Webroot	Malicious

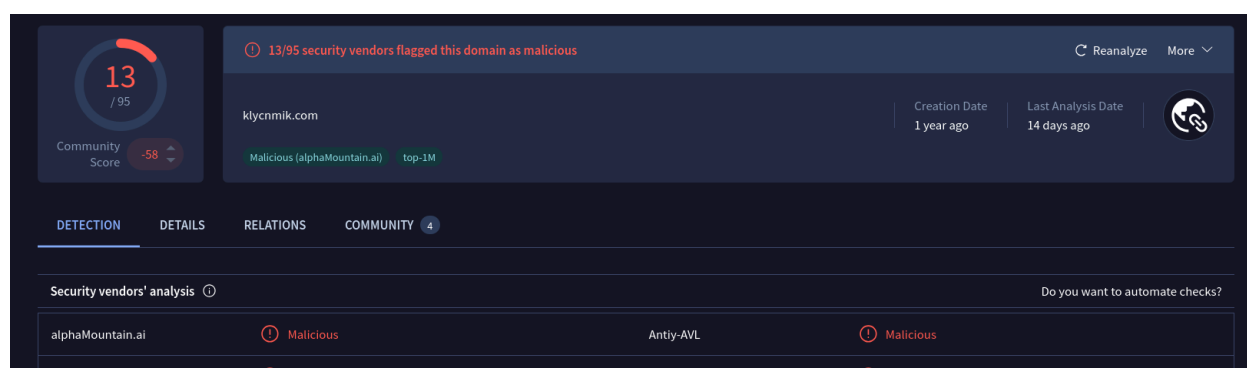
TLS was used to send encrypted data. The first server and last server seemed to exclusively receive data from the infected machine, while the second server seemed to exchange data to the infected machine and conduct HTTP GET requests.

### 13. What is the IP address of the C2 server?

139.60.161.225 is the IP where the Cobalt Strike occurs.

### 14. Did this IP address come from a DNS query? What is the hostname associated with that IP address?

Yes, 139.60.161.225 came from klycnmik.com which was flagged as malicious.



The third server, 209.15.236.39, came from irdayu.com, which was not flagged as malicious.

### 15. What types of messages were exchanged with the C2 server?

The first server, 147.139.134.226, and the last server, 209.15.236.39, appeared to exfiltrate data.

The second server, 139.60.161.225 appears to be exchanging data. All the data is encrypted over TLS so the exact data sent is uncertain.

### 16. Did the infected machine download any files from the C2 server?

Multiple javascript executables GET requests occur from 139.60.161.225, but don't appear to do anything. Nothing seems to be explicitly downloaded from the C2 server.

## 17. Are there any other suspicious files you can see from the trace? Do you think they are malicious?

A .zip file is set over SMTP at the end of the trace. Due to the previous behavior of the infected machine attempting to message multiple mailing services, it is plausible that this is a phishing email from Emotet. It is not listed as malicious over VirusTotal, though.

## 18. What does this malware typically do? (ie what are the common behaviors for this malware?)

Emotet is primarily used as a banking trojan and is often delivered via phishing emails, but can drop password grabber modules. Powershell is used to retrieve the malicious payload and download additional resources. Emotet can also brute force user accounts and scrape email addresses/local logins. To maintain persistence, it creates new services, is within the autostart folder for Windows boot, and is a scheduled task. Emotet also uses encrypted C2 traffic.

Within the trace itself, potential behavior of Emotet could be seen through a large amount of DNS requests and EHLO messages from the infected machine over STMP, made to different mailing services in a very short period of time:

11531 2393.185518	10.3.1.3	10.3.1.101	DNS	160 Standard query response 0x5208 No such name A wpad.norealdomain.net SO
27948 2853.881395	10.3.1.3	10.3.1.101	DNS	92 Standard query response 0x52fe A mail.gnine.co.th A 203.150.224.90
19645 2782.485683	10.3.1.3	10.3.1.101	DNS	124 Standard query response 0x5420 A smtp.mx9.ttcn.ne.jp CNAME smtp2.cm.dr
26598 2847.921640	10.3.1.3	10.3.1.101	DNS	114 Standard query response 0x556f A smtp.rediffmailpro.com A 202.137.236.
4438 453.491625	10.3.1.3	10.3.1.101	DNS	179 Standard query response 0x5621 A geo.prod.do.dsp.mp.microsoft.com CNAME
4378 451.971861	10.3.1.3	10.3.1.101	DNS	179 Standard query response 0x5675 A fe3cr.delivery.mp.microsoft.com CNAME
25202 2840.266781	10.3.1.3	10.3.1.101	DNS	99 Standard query response 0x5771 A pop.emai.rojinhome.info A 157.7.144.1
24409 2829.475327	10.3.1.3	10.3.1.101	DNS	145 Standard query response 0x599c No such name A mail.hasegawashouten.co.
25267 2840.556905	10.3.1.3	10.3.1.101	DNS	101 Standard query response 0x5b0e A smtp.frontier-japan.co.jp A 211.13.20
4783 592.962341	10.3.1.3	10.3.1.101	DNS	151 Standard query response 0x5c37 No such name A wpad.localdomain SOA a.r
23882 2824.536995	10.3.1.3	10.3.1.101	DNS	106 Standard query response 0x5e7d A imap.gmail.com A 142.250.115.108 A 14
1786 162.165697	10.3.1.3	10.3.1.101	DNS	211 Standard query response 0x617d A self.events.data.microsoft.com CNAME
38776 2878.983971	10.3.1.3	10.3.1.101	DNS	112 Standard query response 0x62d3 A smtp.shalme.co.jp CNAME mail.shalme.c
984 69.587196	10.3.1.3	10.3.1.101	DNS	231 Standard query response 0x642a A nti.store.microsoft.com CNAME sfd-pro

19822 2783.484997	10.3.1.101	183.90.228.45	SMTP	76 C: EHLO [173.66.46.112]
19967 2784.221335	10.3.1.101	59.157.128.15	SMTP	76 C: EHLO [173.66.46.112]
21542 2798.548247	10.3.1.101	66.96.131.143	SMTP	76 C: EHLO [173.66.46.112]
21550 2798.595669	10.3.1.101	161.34.19.8	SMTP	76 C: EHLO [173.66.46.112]
21622 2799.129224	10.3.1.101	203.183.70.150	SMTP	76 C: EHLO [173.66.46.112]
21707 2799.391258	10.3.1.101	142.250.113.108	SMTP	76 C: EHLO [173.66.46.112]
21753 2799.610973	10.3.1.101	183.90.228.45	SMTP	76 C: EHLO [173.66.46.112]
21775 2799.645584	10.3.1.101	183.181.90.20	SMTP	76 C: EHLO [173.66.46.112]
21791 2799.829740	10.3.1.101	210.129.90.38	SMTP	76 C: EHLO [173.66.46.112]
21795 2799.835849	10.3.1.101	106.187.245.237	SMTP	76 C: EHLO [173.66.46.112]
21840 2800.055936	10.3.1.101	183.181.89.133	SMTP	76 C: EHLO [173.66.46.112]
21862 2800.161433	10.3.1.101	210.130.202.106	SMTP	76 C: EHLO [173.66.46.112]
21933 2800.543261	10.3.1.101	188.94.250.245	SMTP	76 C: EHLO [173.66.46.112]
21985 2800.052228	10.3.1.101	200.50.463.80	SMTP	76 C: EHLO [173.66.46.112]

**19. Using your answer from question 7, how is this malware typically distributed? (ie how do machines get infected with this malware to begin with?)**

This malware is typically distributed over email. Then for lateral movement within a network, Emotet brute forces the local admin password and uses Admin\$ share. This is shown below, when at Mar 1, 2022 12:05:44.533188000 MST it appears as though the infected device attempts to gain root access and search for other devices on the network.

Time	Source IP	Destination IP	Protocol	Details
7051 1649.596263	10.3.1.101	10.3.1.3	DCERPC	798 Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (64bit NDR)
7052 1649.596414	10.3.1.3	10.3.1.101	TCP	54 49667 → 49257 [ACK] Seq=1 Ack=2197 Win=2102272 Len=0
7053 1649.596972	10.3.1.3	10.3.1.101	DCERPC	338 BindAck: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate A.
7054 1649.597412	10.3.1.101	10.3.1.3	DCERPC	274 Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)
7055 1649.597714	10.3.1.3	10.3.1.101	DCERPC	159 Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
7056 1649.599487	10.3.1.101	10.3.1.3	DRSUAPI	322 DsBind request
7057 1649.599715	10.3.1.3	10.3.1.101	DRSUAPI	258 DsBind response
7058 1649.600936	10.3.1.101	10.3.1.3	DRSUAPI	338 DsCrackNames request
7059 1649.600934	10.3.1.3	10.3.1.101	DRSUAPI	450 DsCrackNames response
7060 1649.600966	10.3.1.101	10.3.1.3	DRSUAPI	194 DsUnbind request
7061 1649.600966	10.3.1.3	10.3.1.101	DRSUAPI	194 DsUnbind response
7062 1649.602314	10.3.1.101	10.3.1.3	EPH	222 Map request, DRSUAPI, 32bit NDR
7063 1649.602501	10.3.1.3	10.3.1.101	EPH	226 Map response, DRSUAPI, 32bit NDR
7064 1649.603006	10.3.1.101	10.3.1.3	DRSUAPI	258 DsBind request
7065 1649.603186	10.3.1.3	10.3.1.101	DRSUAPI	258 DsBind response
7066 1649.603463	10.3.1.101	10.3.1.3	DRSUAPI	338 DsCrackNames request
7067 1649.603745	10.3.1.3	10.3.1.101	DRSUAPI	450 DsCrackNames response
7068 1649.604016	10.3.1.101	10.3.1.3	DRSUAPI	194 DsUnbind request
7069 1649.604241	10.3.1.3	10.3.1.101	DRSUAPI	194 DsUnbind response
7070 1649.606815	10.3.1.101	10.3.1.3	TCP	66 49258 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7071 1649.606953	10.3.1.3	10.3.1.101	TCP	66 389 → 49258 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7072 1649.607104	10.3.1.101	10.3.1.3	TCP	54 49258 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
7073 1649.607729	10.3.1.101	10.3.1.3	LDAP	404 searchRequest(1) "c=dc" baseObject
7074 1649.608041	10.3.1.3	10.3.1.101	TCP	1514 389 → 49258 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP PDU reassembled in 7075]
7075 1649.608050	10.3.1.101	10.3.1.3	LDAP	1405 searchResEntry(1) "c=dc"   searchResDone(1) success [4 results]
7076 1649.608188	10.3.1.101	10.3.1.3	TCP	54 49258 → 389 [ACK] Seq=351 Ack=2812 Win=262656 Len=0
7077 1649.609299	10.3.1.101	10.3.1.3	TCP	1514 49258 → 389 [ACK] Seq=351 Ack=2812 Win=262656 Len=1460 [TCP PDU reassembled in 7078]
7078 1649.609309	10.3.1.101	10.3.1.3	LDAP	681 bindRequest(3) "c=dc" sasl
7079 1649.609409	10.3.1.3	10.3.1.101	TCP	54 389 → 49258 [ACK] Seq=2812 Ack=2438 Win=2102272 Len=0
7080 1649.610091	10.3.1.3	10.3.1.101	LDAP	264 bindResponse(3) success
7081 1649.611236	10.3.1.101	10.3.1.3	LDAP	293 SASL GSS-API Integrity: searchRequest(4) "CN=DESKTOP-CLIENT1,CN=Computers,DC=norealdomain,DC=net" baseObject
7082 1649.611474	10.3.1.3	10.3.1.101	LDAP	227 SASL GSS-API Integrity: searchResEntry(4) "CN=DESKTOP-CLIENT1,CN=Computers,DC=norealdomain,DC=net" searchResDone(4) success ...
7083 1649.612115	10.3.1.101	10.3.1.3	LDAP	208 SASL GSS-API Integrity: searchRequest(5) "CN=DESKTOP-CLIENT1,CN=Computers,DC=norealdomain,DC=net" baseObject
7084 1649.612304	10.3.1.3	10.3.1.101	LDAP	185 SASL GSS-API Integrity: searchResEntry(5) "CN=DESKTOP-CLIENT1,CN=Computers,DC=norealdomain,DC=net" searchResDone(5) success ...
7085 1649.612613	10.3.1.101	10.3.1.3	LDAP	292 SASL GSS-API Integrity: searchRequest(6) "CN=DESKTOP-CLIENT1,CN=Computers,DC=norealdomain,DC=net" baseObject
7086 1649.612822	10.3.1.3	10.3.1.101	LDAP	238 SASL GSS-API Integrity: searchResEntry(6) "CN=DESKTOP-CLIENT1,CN=Computers,DC=norealdomain,DC=net" searchResDone(6) success ...
7087 1649.614968	10.3.1.3	10.3.1.101	TCP	226 [TCP Retransmission] 135 → 49254 [PSH, ACK] Seq=109 Ack=329 Win=2102816 Len=172
7088 1649.615018	10.3.1.3	10.3.1.101	TCP	194 [TCP Retransmission] 49607 → 49255 [PSH, ACK] Seq=1622 Ack=3620 Win=2100736 Len=140

**20. Using all the evidence you have collected, build a basic timeline with the important events that transpired during the cyber attack. Be sure to include a timestamp for each event.**

- Before Trace: User most likely received an email or accessed a website with this unsafe link or attachment.
- Mar 1, 2022 11:38:14.925459000 MST: User accessed diacrestgroup.com
- Mar 1, 2022 11:38:19.845463000 MST: User downloaded Emotet Trojan from diacrestgroup.com
- Mar 1, 2022 11:38:26.842452000 MST: C2 Server 209.15.236.39 Begins Exfiltrating Data



- Mar 1, 2022 11:38:32.003299000 MST: C2 Server 147.139.134.226 Begins Exfiltrating Data
- Mar 1, 2022 12:04:14.768003000 MST: Cobalt Strike starts using C2 Server 139.60.161.225
- Mar 1, 2022 12:05:44.533188000 MST: Infected machine gains initiates lateral movement across the local network.
- Mar 1, 2022 12:22:09.160729000 MST: Infected machine gains root access initiates lateral movement across the local network again.
- Mar 1, 2022 12:23:17.380554000 MST: C2 Server 147.139.134.226 is disconnected
- Mar 1, 2022 12:25:07.400187000 MST: C2 Server 209.15.236.39 is disconnected
- Mar 1, 2022 12:26:11.253264000 MST: Massive amount of DNS requests sent to different domains related to outlook, smtp, and other mailing services.
- Mar 1, 2022 12:26:15.780124000 MST: Successfully logs into an email and sends an email with a .zip file.