Emma Stensland

Reese Pearsall

CSCI 466

November 3, 2025

Evidence 4 - Emotet Trojan

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

0x15a29d64af3a0e5cceebfde7f4fc05241a18514b

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?

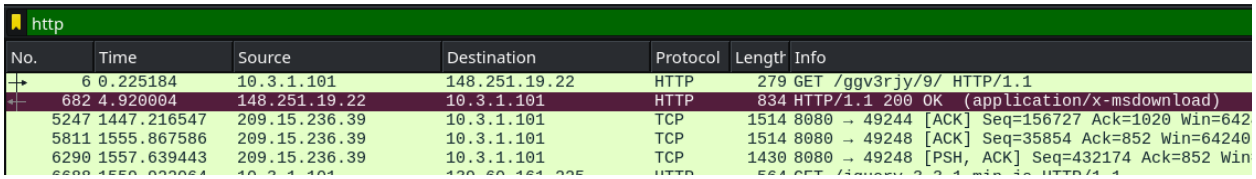
00:08:02:1c:47:ae

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



a. What is the filename of the malware?

B7tYH11h5gzY1sx.dll

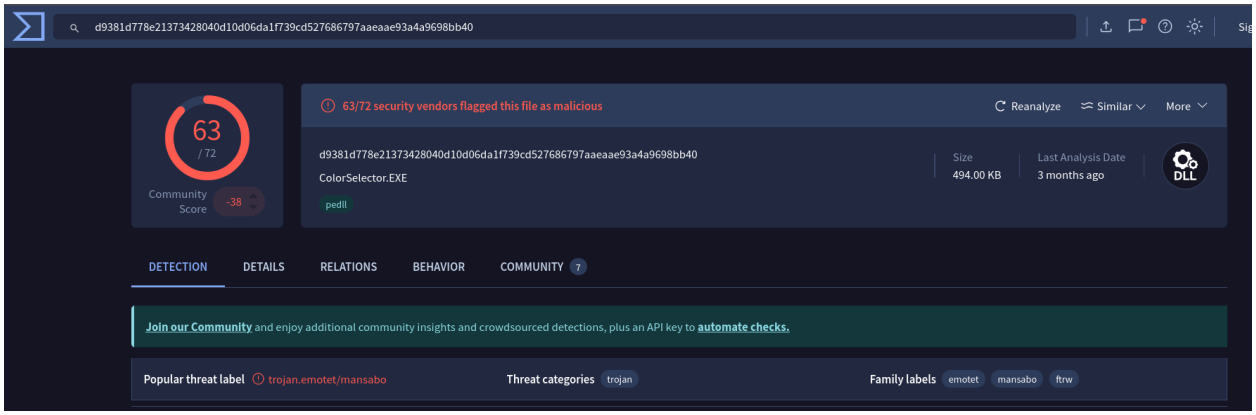
b. What is the file extension of the malware?

.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?

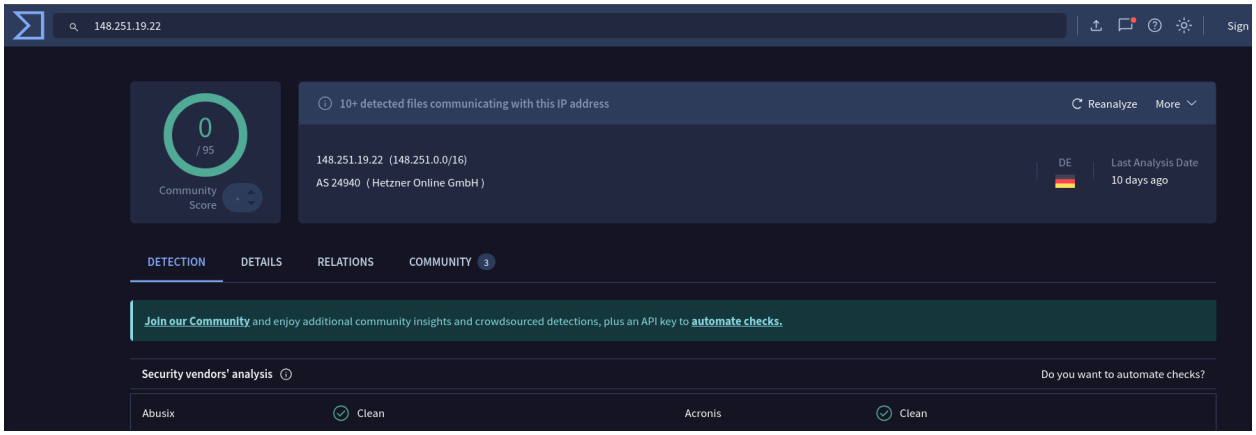
Emotet

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



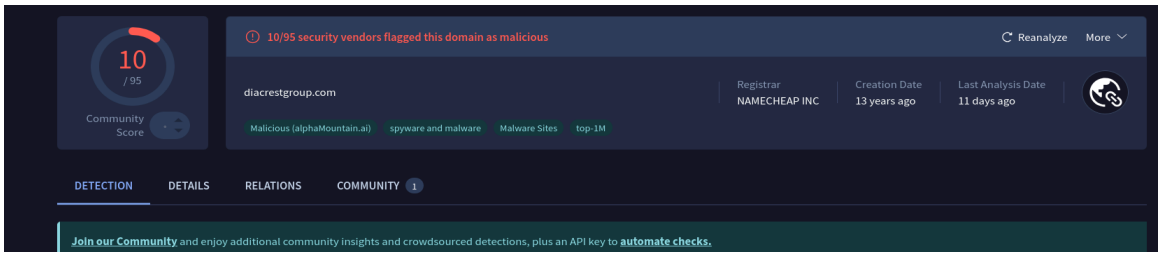
Not malicious.

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	0.065358	10.3.1.3	10.3.1.101	DNS	93	Standard query response 0x69c5 A diacrestgroup.com A 148.251.19.22
3	0.066547	10.3.1.101	148.251.19.22	TCP	66	49183 → 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



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

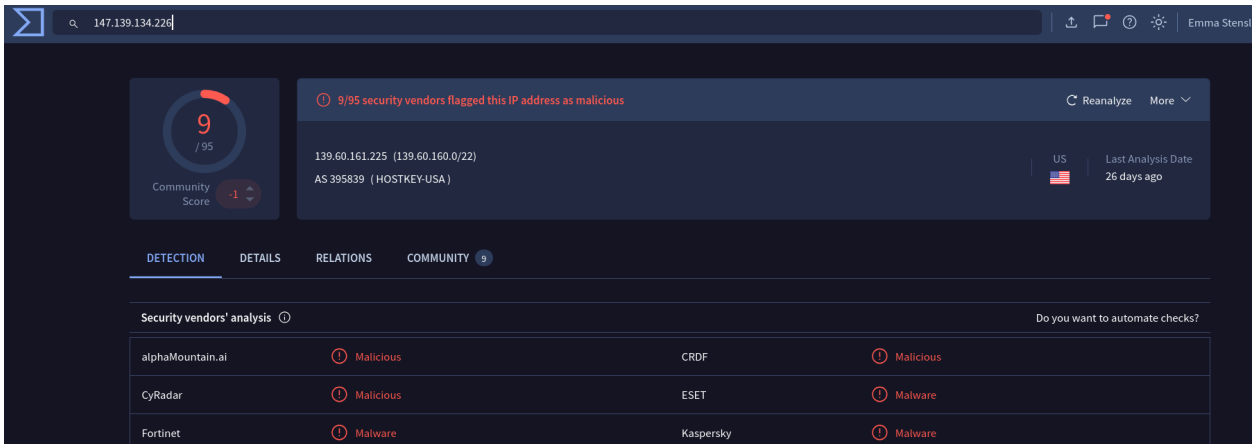
```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% 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?

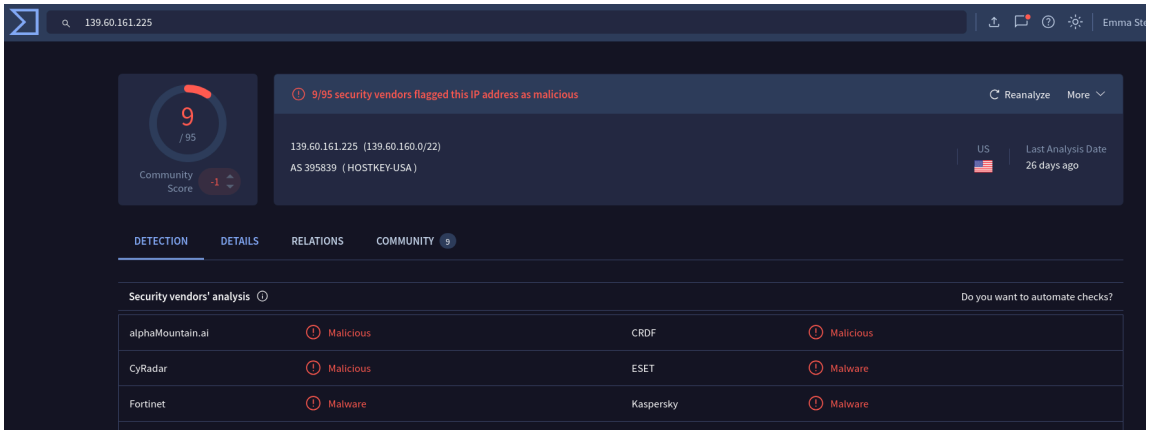
Yes.

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:

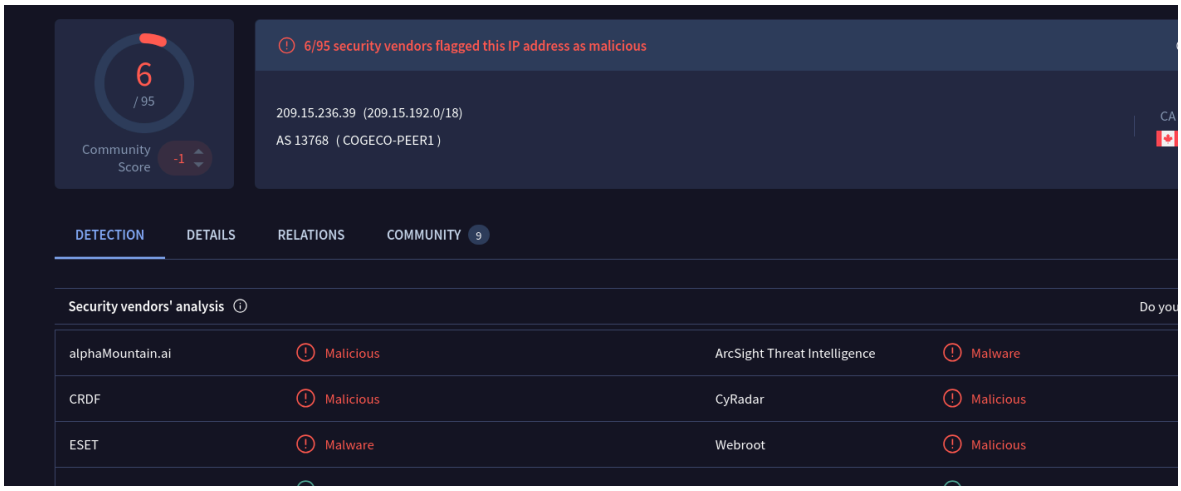

```
ts: 2022-03-01T18:38:32.812897Z,
uid: "CxmuVm18hcmCbUigWa",
id: > {orig_h: 10.3.1.101, orig_p: 49188 (port=(uint16)), resp_h: 147.139.134.226, resp_p: 443 (port=(uint16))},
fuid: "FTAb7R2H1y52AFOJIa",
file_mime_type: null,
file_desc: null,
proto: "tcp" (zenum),
note: "SSL::Invalid_Server_Cert" (zenum),
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,
```

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:



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:



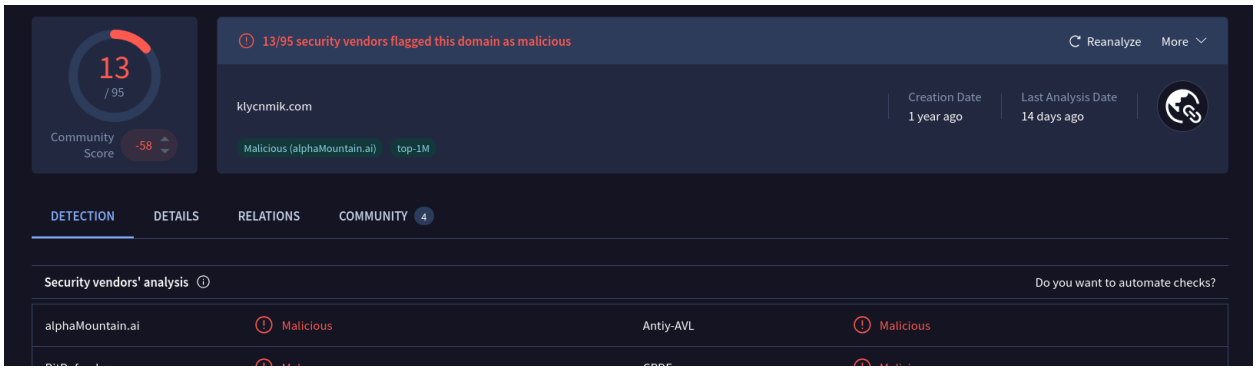
TLS was used to send encrypted data. The first server and last server seemed to exclusively receive data from the infected machine, while the second server seemed to exchange data to the infected machine and conduct HTTP GET requests.

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?

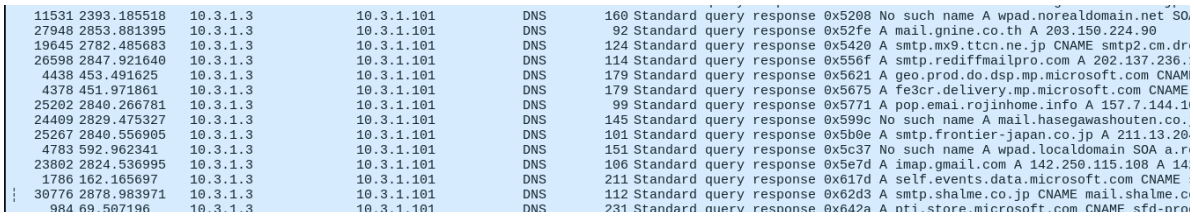
Multiple javascript executables GET requests occur from 139.60.161.225, but don't appear to do anything. Nothing seems to be explicitly downloaded from the C2 server.

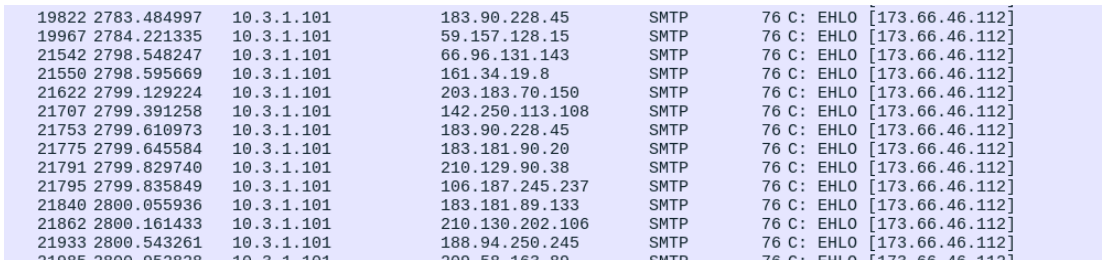
17. Are there any other suspicious files you can see from the trace? Do you think they are malicious?

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?)

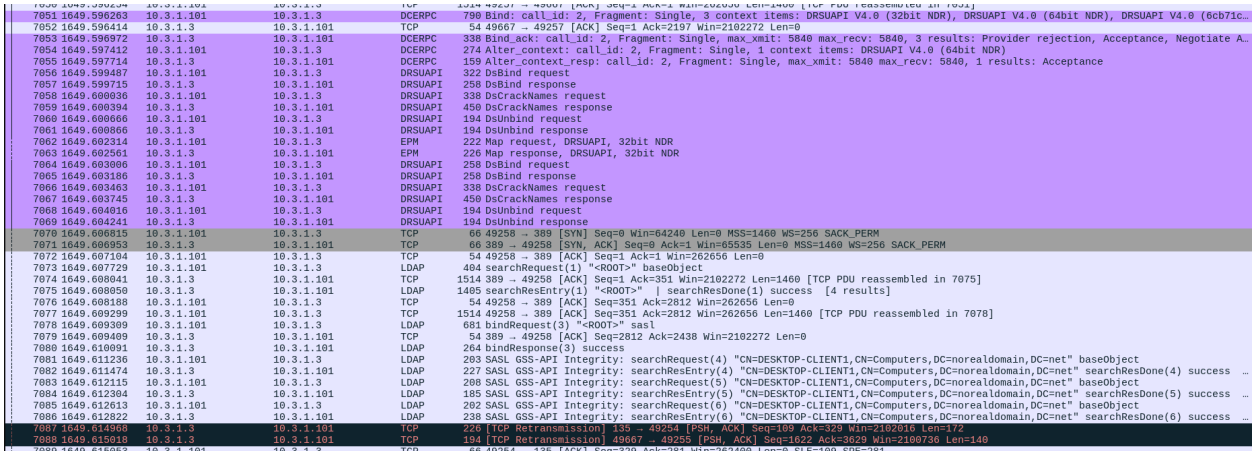
Emotet is primarily used as a banking trojan and is often delivered via phishing emails, but can drop password grabber modules. Powershell is used to retrieve the malicious payload and download additional resources. Emotet can also brute force user accounts and scrape email addresses/local logins. To 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:





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.



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.