Reference: https://blueteamlabs.online/home/challenge/network-analysis-ransomware-3dd520c7ec

Download the PCAP from the above link

In Linux with tcpdump

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ file ransom_traffic.pcapng
ransom_traffic.pcapng: pcapng capture file - version 1.0
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ sudo tcpdump -tttt -r ransom_traffic.pcapng -c 5
reading from file ransom_traffic.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
2021-01-31 12:59:57.361548 IP 10.0.2.4.49184 > 40.112.72.205.https: Flags [S], seq 1041143463, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
2021-01-31 12:59:57.361733 IP 10.0.2.4.49185 > 40.112.72.205.https: Flags [S], seq 1568426093, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
2021-01-31 12:59:57.362052 IP 10.0.2.1 > 10.0.2.4: ICMP host 40.112.72.205 unreachable, length 36
2021-01-31 12:59:57.362169 IP 10.0.2.1 > 10.0.2.4: ICMP host 40.112.72.205 unreachable, length 36
2021-01-31 13:00:00.376415 IP 10.0.2.4.49184 > 40.112.72.205.https: Flags [S], seq 1041143463, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$
```

Parsing IP

sudo tcpdump -tttt -r ransom_traffic.pcapng | cut -d " " -f 4 | cut -d "." -f 1-4 | sort | uniq -c | sort -nr

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ sudo tcpdump -tttt -r ransom_traffic.pcapng | cut -d " " -f 4 | cut -d "." -f 1-4 | sort | uniq -c | sort
-nr
reading from file ransom_traffic.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
    345 10.0.2.15
    328 10.0.2.4
     28 10.0.2.1
     10 Request
     10 Reply
      7 fe80::256b:4013:4140:453f.dhcpv6-client
      6 fe80::256b:4013:4140:453f
      4 10.0.2.3
      2 fe80::256b:4013:4140:453f.63876
      2 fe80::256b:4013:4140:453f.63512
      2 fe80::256b:4013:4140:453f.60468
      2 fe80::256b:4013:4140:453f.60398
      2 fe80::256b:4013:4140:453f.59588
      2 fe80::256b:4013:4140:453f.57915
      2 fe80::256b:4013:4140:453f.57493
      2 fe80::256b:4013:4140:453f.56509
      2 fe80::256b:4013:4140:453f.56424
      2 fe80::256b:4013:4140:453f.54561
```

So, the number of IP with count is shown above. Now we have to filter the output based on it.

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ sudo tcpdump -r ransom_traffic.pcapng | cut -d " " -f 3 | cut -d "." -f 1-4 | sort | uniq -c | sort -nr
reading from file ransom_traffic.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
    345 10.0.2.15
    328 10.0.2.4
     28 10.0.2.1
     10 Request
     10 Reply
      7 fe80::256b:4013:4140:453f.dhcpv6-client
      6 fe80::256b:4013:4140:453f
      4 10.0.2.3
      2 fe80::256b:4013:4140:453f.63876
      2 fe80::256b:4013:4140:453f.63512
      2 fe80::256b:4013:4140:453f.60468
```

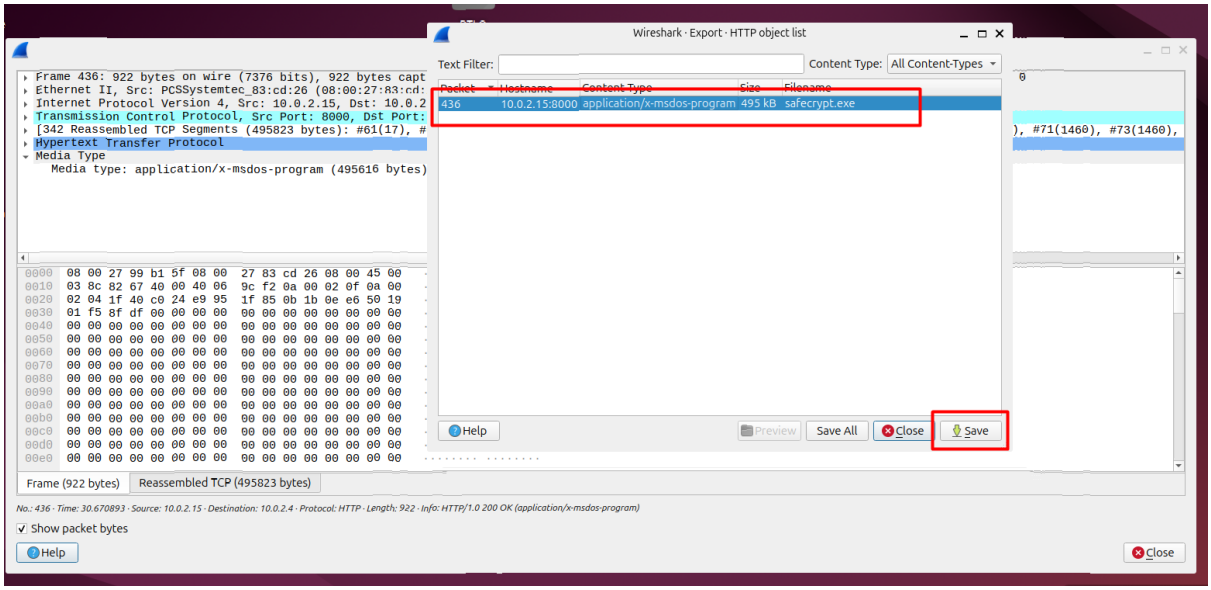
This IP looks suspicious as it is making lots of request.

Filter out with the suspicious IP we get:

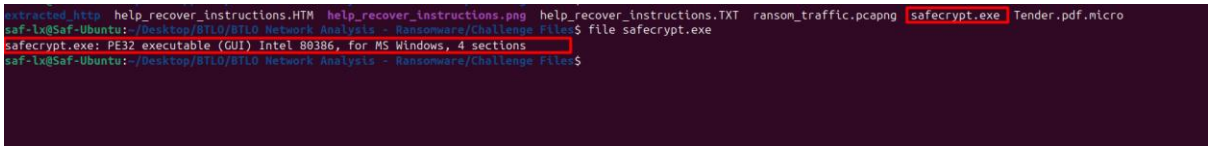
sudo tcpdump -nn -A -r ransom_traffic.pcapng 'host 10.0.2.15 and tcp' | grep "GET"

We can see the .exe file which is kind of suspicious. Let's extract it.

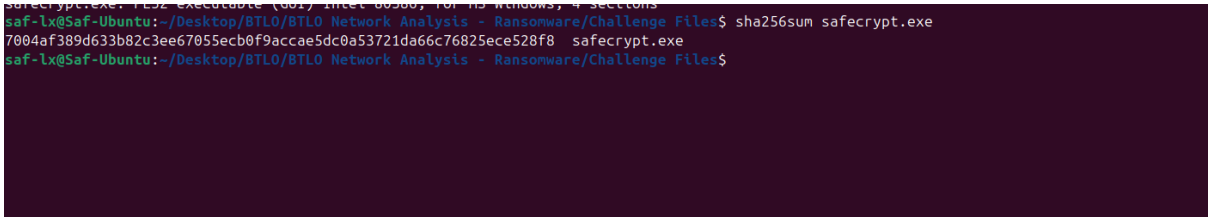
Since we can't download the file with tcpdump, we will use wireshark to do that.



Download and check the file type

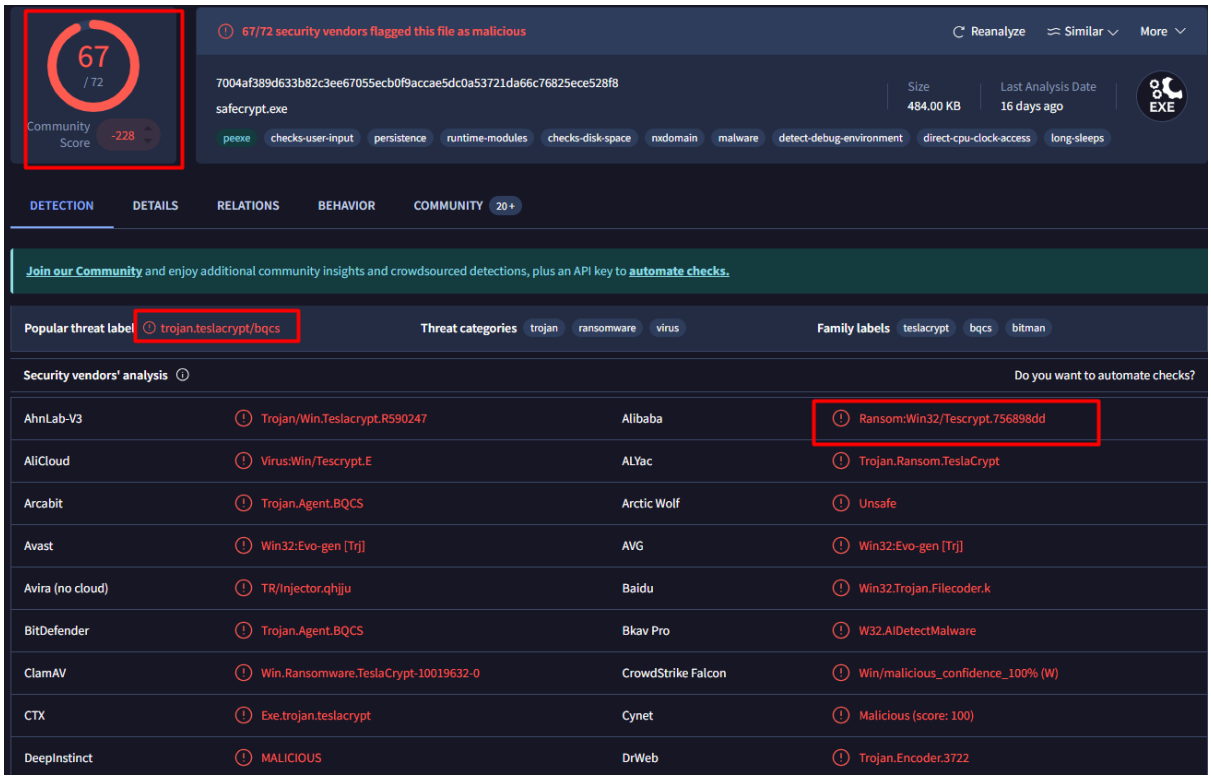


Generate the hash and check its reputation.



Let’s check its reputation in virustotal.

Sha256 hash -> 7004af389d633b82c3ee67055ecb0f9accae5dc0a53721da66c76825ece528f8



From here we can find the other details of the ransomeware executable file.