

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

Network Analysis - Ransomware

ABC Industries worked day and night for a month to prepare a tender document for a prestigious project that would secure the company's financial future. The company was hit by ransomware, believed to be conducted by a competitor, and the final version of the tender document was encrypted. Right now they are in need of an expert who can decrypt this critical document. All we have is the network traffic, the ransom note, and the encrypted tender document. Do your thing Defender!

Wireshark TShark TCPDump

Points	Difficulty	Solves	OS
20	Medium	5043	Windows/Linux

 **Network Log**
998 KB

Password
btlo (inner ZIP: infected)

Download File

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
-r
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.

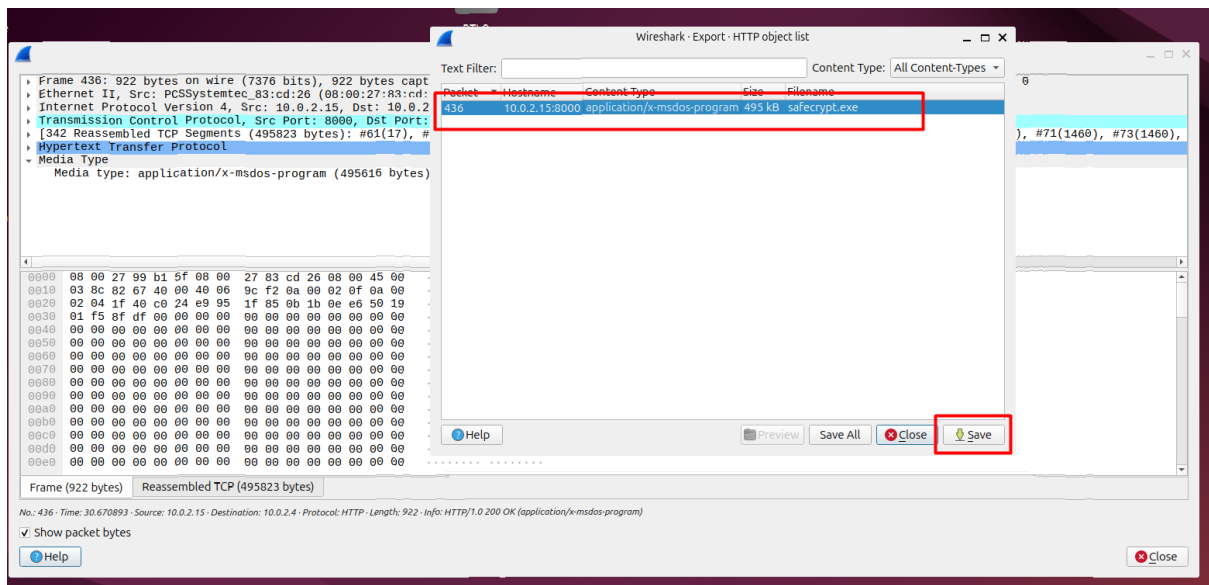
Filter out with the suspicious IP we get:

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

```
saf-lx@Saf-Ubuntu: ~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ sudo tcpdump -nn -A -r ransom_traffic.pcapng 'host 10.0.2.15 and tcp' | grep "GET"
reading from file ransom_traffic.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
...S.0.....P.0)....GET /safecrypt.exe HTTP/1.1
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$
```

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

```
extracted_help_recover_instructions.HTM help_recover_instructions.png help_recover_instructions.TXT ransom_traffic.pcapng safecrypt.exe Tender.pdf.micr
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ file safecrypt.exe
safecrypt.exe: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$
```

Generate the hash and check its reputation.

```
safecrypt.exe: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$ sha256sum safecrypt.exe
7004af389d633b82c3ee67055ecb0f9accac5dc0a53721da66c76825ece528f8 safecrypt.exe
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/BTLO Network Analysis - Ransomware/Challenge Files$
```

Let's check its reputation in virustotal.

Sha256 hash -> 7004af389d633b82c3ee67055ecb0f9accae5dc0a53721da66c76825ece528f8

67
/ 72

Community Score -228

67/72 security vendors flagged this file as malicious

7004af389d633b82c3ee67055ecb0f9accae5dc0a53721da66c76825ece528f8

safecrypt.exe

Size 484.00 KB

Last Analysis Date 16 days ago

peexe checks-user-input persistence runtime-modules checks-disk-space nxdomain malware detect-debug-environment direct-cpu-clock-access long-sleeps

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 20+

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

Popular threat label trojan,teslacrypt/bqcs

Threat categories trojan ransomware virus

Family labels teslacrypt bqcs bitman

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Teslacrypt.R590247	Alibaba	Ransom:Win32/Tescript.756898dd
AliCloud	Virus:Win/Tescript.E	ALYac	Trojan.Ransom.TeslaCrypt
Arcabit	Trojan.Agent.BQCS	Arctic Wolf	Unsafe
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	TR/Injector.qhju	Baidu	Win32.Trojan.Filecoder.k
BitDefender	Trojan.Agent.BQCS	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Ransomware.TeslaCrypt-10019632-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.teslacrypt	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Encoder.3722

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