THE COVER UP

Incident response/log analyses challenge

[Publish Date]

European Cyber Security Challenge 2019

Bucharest, Romania

1. Initial Write-Up

Description:

As member of a computer network administration team you received a network traffic file recording a network communication. Your task is to analyse it help incident response by recreating the flow of event.

2. Challenge specifications

- Category: Network/traffic/log analysis
- Difficulty : medium
- Expected time to solve: 1 hour to solve (aprx)

3. Technical specifications

Description:

Challenge Technical Specification, data to set up and access to the environment.

- IP address: To be able to access to the machines, scenario, etc…
- Operating Systems
- Credentials
- Focus (Optional)
- Software used
- Important files to have in mind
- Other information
- Minimum setup requirements

1. Log file is provided in pcap format
2. Participant shall have software to open and analyse it (eg Wireshark)

4. Questions and answers

Description:

1. **CTF Specific questions:**

Q/A that can be directly introduced in a CFT format. This year upload of files can be included, also REGEXPs.

Question:

What is the IP address of the malicious server data has been transmitted to?

Answer:

172.16.83.101

Question:

To how many pieces the leaked data has been sliced during transmission?

Answer:

11

Question:

What kind of illness affects Ms. Susan Martin according to the leaked data??

Answer: diabetes

Question:

What is Ms. Dorothy Perez's birthdate according to the leaked data?

Answer:

28th January 1966

Question:

How can packets originating from 192.168.0.128/25 and sent to a TPlink device filtered?

Answer:

ip.src == 192.168.0.128/25 && eth.dst[0:3] == f4:f2:6d

2. Non-Flag specific:

Open Questions: Answers that may need a minimum development. (No suitable for CTF but useful for training and for a better understanding of the challenge) Multiple choice answer

Question:

What is the name of the technique used for data exfiltration?

Answer:

DNS tunneling

Question:

What is the most important decision before setting up a log server?

Answer:

To decide about the number of days, logs need to be kept about, and calculate the capacity.

Question:

What kind of packets are filtered with the following filter: eth.src[0:3] == 9C:1C:12

Answer:

Packets originating from Aruba devices

Question:

What kind of effect the following Wireshark filter causes: ip.addr == 192.168.100.27 ?

Answer:

Packets originating from and sent to 192.168.100.27 will be displayed.

5. Attack Scenario

The attached file contains recorded traffic from your organization's DMZ. Analyze the pcap file to investigate the events and figure out if there has been and data breach at the time of the incident.

6. Installation instructions

Setup for the organizers

Distribute the attached pcap file and topology with the task description.

7. Tools needed

Tools needed for the solution of the challenge:

- Wireshark

8. Artifacts provided

File	MD5	SHA256
network topology.PNG	2f475509c9dee5cec1e269dbd16121bf	4cf6b67362c38b10e435d8a149833aeca55905d4a74ddcf64aaf421a83a641cc

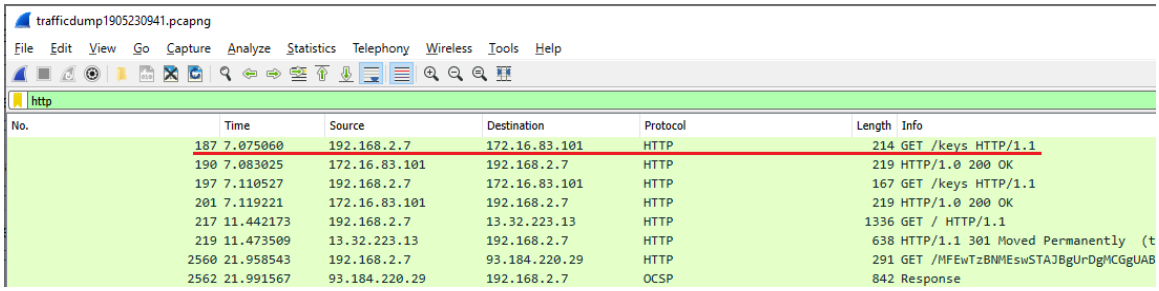
trafficdump1905230941.zip	0bbe7309acd0fef268c435cc28d68f47	9e63ce93e8c4d7f46266b339c4a39469d321f6e640f0e5c3a8e0692cf03100be

9. Walkthrough (writeup)

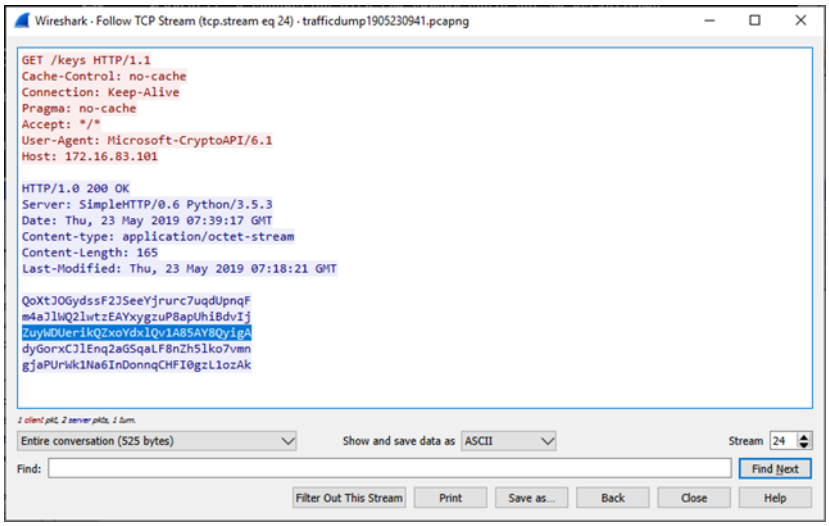
1., After opening the PCAP, loads of traffic can be seen from 192.168.2.7 to the internet: because everything goes over the INT-Gateway, in the DMZ all traffic seems to come from INT-Gateway, but in reality, they are originating from the 'Office LAN'.

2., Look for strange things:

Most of the traffic is TLS, but have a look at normal HTTP:

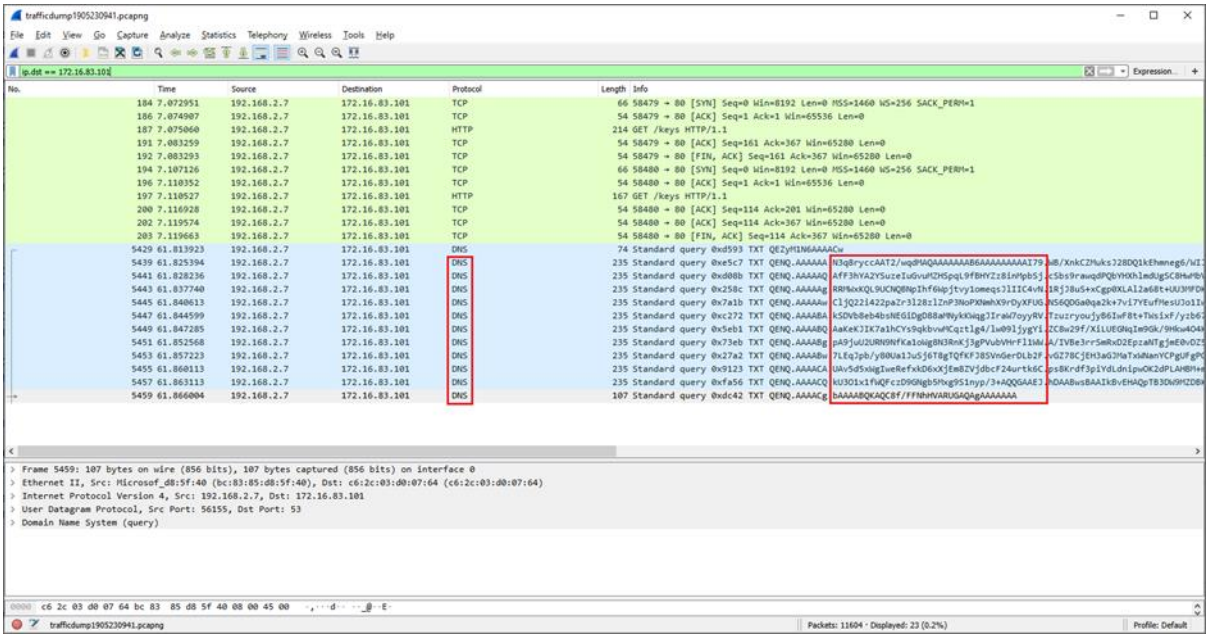


Investigate this traffic:

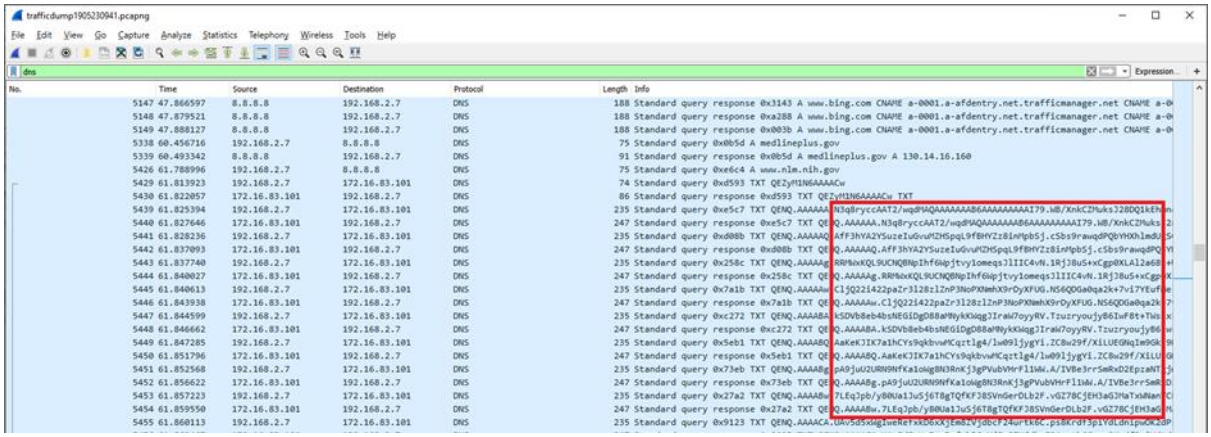


These can be useful later: can be keys for encryption

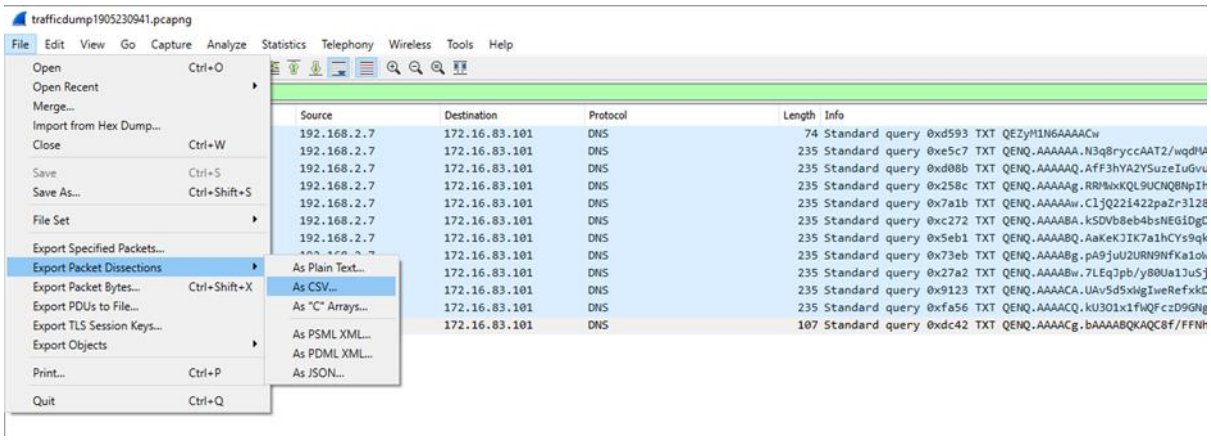
Following this IP gives interesting results:



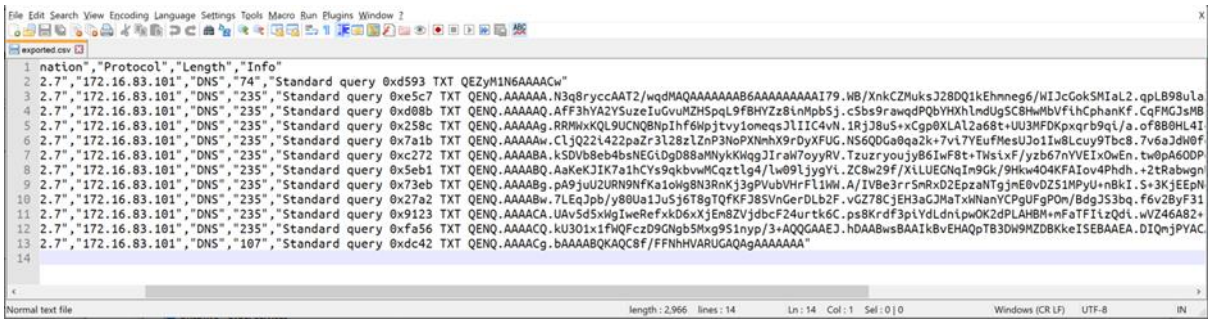
Another way: look first for DNS, and find the strange ones:



Narrow the filter to this address and DNS (ip.dst == 172.16.83.101 and dns) and export the data:



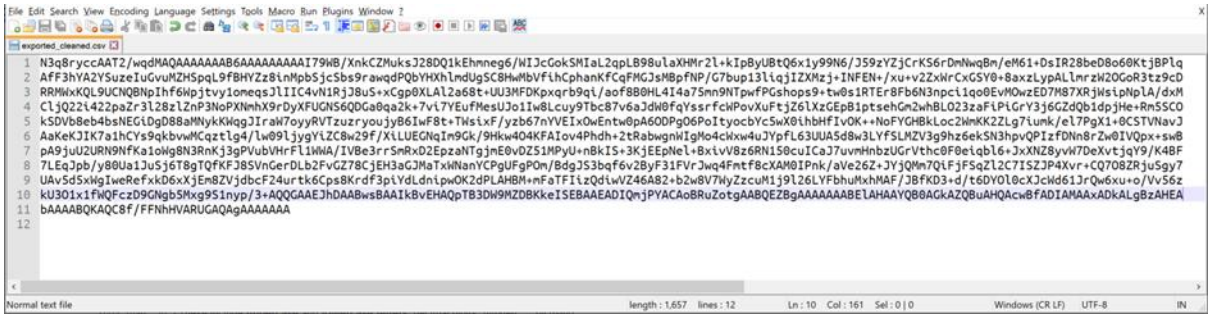
Open the exported file and investigate.



Looks like slices of data. There is some encoding or encryption used: capital and small letters, slash and plus sign is used. The answer is not trivial, but not even hard: base64.

https://rise4fun.com/Bek/tutorial/base64

Dots are not part of these, and the first 6 letters seem to be a counter. Remove all this and the citation marks:



Decode the base64 encoding:

certutil -decode exported_cleaned.csv extracted.bin

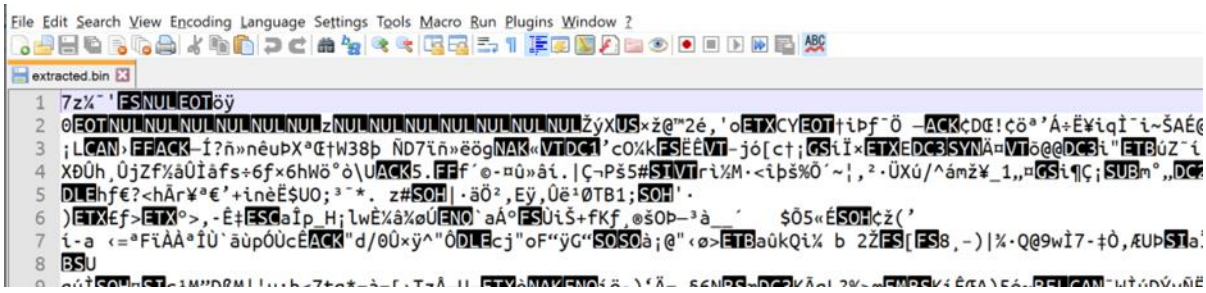
Input Length = 1657

Output Length = 1226

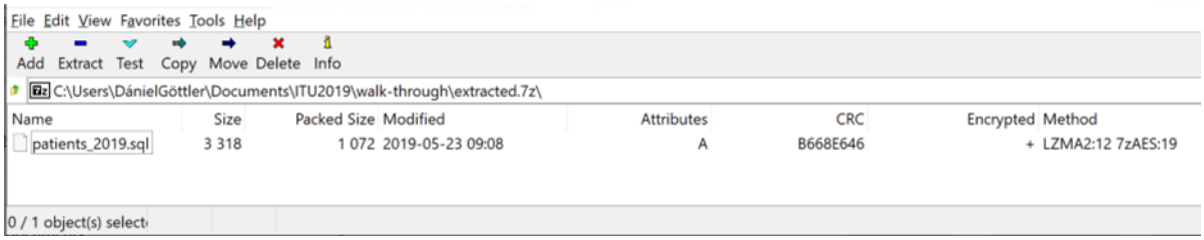
CertUtil: -decode command completed successfully.

(https://dmfrsecurity.com/2017/01/07/windows-base64-encoding-and-decoding-using-certutil/)

Looking at the file, it begins with 7z



Change the file extension to ‘7z’ and open it:



'patients_2019.sql' – that seems to be sensitive data, possibly from a healthcare organisation.

To open it, use the keys the malware has downloaded earlier:

QoXtJOGydssF2JSeeYjrurc7uqdUpnqF

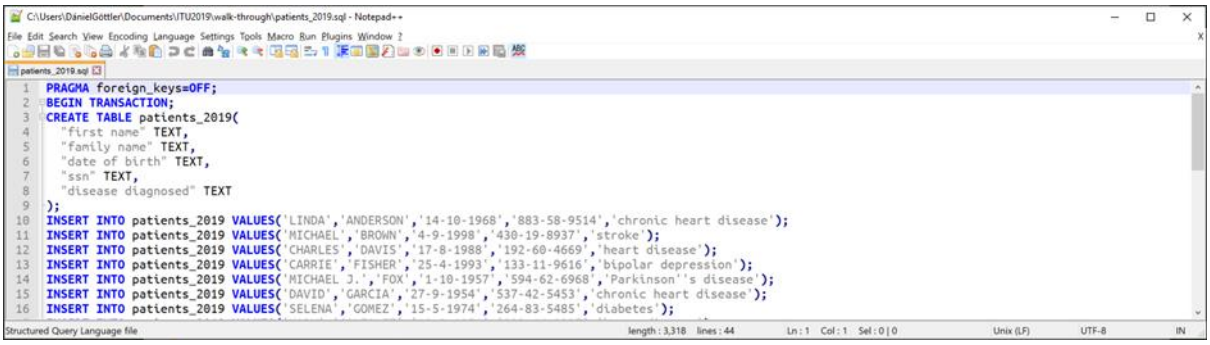
m4aJlWQ2lwtzEAYxygzuP8apUhiBdvIj

ZuyWDUerikQZxoYdxlQv1A85AY8QyigA

dyGorxCJlEnq2aGSqaLF8nZh5lko7vmn

gjaPUrWk1Na6InDonnqCHFI0gzL1ozAk

The third one helps:



Here is the proof of the data breach.