



# 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	2f475509c9dee5cec1e269dbd	4cf6b67362c38b10e435d8a149833aeca55905d4a74ddcf64
topology.PNG	16121bf	aaf421a83a641cc

trafficdump1905	0bbe7309acd0fef268c435cc28	9e63ce93e8c4d7f46266b339c4a39469d321f6e640f0e5c3a
230941.zip	d68f47	8e0692cf03100be

# 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:

🚄 trafficdump1905230941.pcapng								
Eile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>I</u> ools <u>H</u> elp								
🛋 🔳 🔬 🔘 🖡 🚵 💁 ۹. 👳 📾 🗑 👲 🚍 🧮 ۹. ۹. ۹. 9.								
R http								
No.	Time	Source	Destination	Protocol	Length Info			
1	87 7.075060	192.168.2.7	172.16.83.101	HTTP	214 GET /keys HTTP/1.1			
1	90 7.083025	172.16.83.101	192.168.2.7	HTTP	219 HTTP/1.0 200 OK			
1	97 7.110527	192.168.2.7	172.16.83.101	HTTP	167 GET /keys HTTP/1.1			
2	01 7.119221	172.16.83.101	192.168.2.7	HTTP	219 HTTP/1.0 200 OK			
	17 11.442173	192.168.2.7	13.32.223.13	HTTP	1336 GET / HTTP/1.1			
2	19 11.473509	13.32.223.13	192.168.2.7	нттр	638 HTTP/1.1 301 Moved Permanently (t			
25	60 21.958543	192.168.2.7	93.184.220.29	нттр	291 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUAB			
25	62 21.991567	93.184.220.29	192.168.2.7	OCSP	842 Response			

Investigate this traffic:

Wireshark - Follow TCP Stream (tcp.stream eq 24) - trafficdump1905230941.pcapng	-	
GET /keys HTTP/1.1		
Cache-Control: no-cache		
Connection: Keep-Alive		
Pragma: no-cache		
Accept: */*		
User-Agent: Microsoft-CryptoAPI/6.1		
Host: 172.16.83.101		
HTTP/1.0 200 OK		
Server: SimpleHTTP/0.6 Python/3.5.3		
Date: Thu, 23 May 2019 07:39:17 GMT		
Content-type: application/octet-stream		
Content-Length: 165		
Last-Modified: Thu, 23 May 2019 07:18:21 GMT		
QoXtJOGydssF2JSeeYjrurc7uqdUpnqF		
m4aJ1WQ21wtzEAYxygzuP8apUhiBdvIj		
ZuyWDUerikQZxoYdxlQv1A85AY8QyigA		
dyGorxCJlEnq2aGSqaLF8nZh5lko7vmn		
gjaPUrWk1Na6InDonnqCHFI0gzL1ozAk		
clent pkt, 2 server pkts, 1 turn.		
Entire conversation (525 bytes) 🗸 Show and save data as ASCII		Stream 24
ind:		Find New
Filter Out This Stream Print Save as Back O	lose	Help

These can be useful later: can be keys for encryption

Following this IP gives interesting results:

				🖾 📼 🔹 Expression
Time	Source	Destination	Protocol	Length Info
184 7.072951	192.168.2.7	172.16.83.101	TCP	66 58479 + 80 [5170] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
186 7.074907	192.168.2.7	172.16.83.101	TCP	54 58479 → 80 [ACK] Seq*1 Ack*1 Win*65536 Len*0
187 7.075060	192.168.2.7	172.16.83.101	HTTP	214 GET /keys HTTP/1.1
191 7.083259	192.168.2.7	172.16.83.101	TCP	54 58479 → 80 [ACK] Seq=161 Ack=367 Win=65280 Len=0
192 7.083293	192.168.2.7	172.16.83.101	TCP	54 58479 → 80 [FIN, ACK] Seq=161 Ack=367 Win=65280 Len=0
194 7.107126	192.168.2.7	172.16.83.101	TCP	66 58480 + 80 [SYN] Seq=0 Win=8192 Len=0 MS=1460 WS=256 SACK_PERM=1
196 7.110352	192,168,2.7	172.16.83.101	TCP	54 58480 + 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
197 7.110527	192.168.2.7	172.16.83.101	HTTP	167 GET /keys HTTP/1.1
200 7.116928	192.168.2.7	172.16.83.101	TCP	54 58480 = 80 [ACK] Seq=114 Ack=201 Win=65280 Len=0
202 7.119574	192.168.2.7	172.16.83.101	TCP	54 58480 + 80 [ACK] Seq=114 Ack=367 Win+65280 Len=0
203 7.119663	192.168.2.7	172.16.83.101	TCP	54 58480 * 80 [FIN, ACK] 5eq=114 Ack=367 Win+65280 Len=0
5429 61.813923	192.168.2.7	172.16.83.101	DNS	74 Standard query exd593 TXT QEZyHIMAAAACu
5439 61.825394	192.168.2.7	1/2.16.83.101	UNS	255 Standard query twesc/ 1X1 QENC, Advance regery ccar 12/ngdrigQAAAAAAbabaAAAbabaAAAAabaA1/5 ams/Xnic.2/nix5/2280Q1kemine
5441 01.020230	192.100.2.7	1/2.10.03.101	UNS	255 Standard query exceed 1X1 geng Awway artisticated unitropiq stont to intro 50 cost and or gen and or generation of the store of the
5443 61.837740	192.168.2.7	172.10.83.101	DNS	255 Standard query W250C IX1 QEW2.Awwwg KRIWKQL90CHQ00plinteip]TVy10Heg5111L4VH IX7305+KgDWLA12805+0
5445 01.040015	192,100.2.7	172.10.03.101	DNG	235 Standard guery 6x7410 KA geng Awwell C19gez14zpez151zez1zh Skorwalitarityk og ASOgodadgezer/17/10/165
5447 01.044579	192.100.2.7	172.16.63.101	DNG	255 Standard query WKC2/2 IAI QEW, ANNAL AND STATES OF STATES AND
5445 01.047205 EAE1 61 EE1E60	102.100.2.7	172.10.03.101	DWG	235 Standard uptry 0x501 TAT (CR) ANALY and STATATIC SEQUENCE (1897) 10051 (STATATIC CONTRACT) ALLOCATION AND A STATATIC CONTRACT AND A STATATICA A
5453 61 857333	192.100.2.7	172.16.83.101	DNS DNS	255 School and Unity 0x7500 XX1 QERQ, Reveals proj poutointent nationgorisers jog vuorint riske av stops trainen av stops trainen av stops and the stops of th
5455 61 860113	192.168.2.7	172.16.83.101	INIS	235 Standard oper y 0x27a (A) QER Added (A) Address (A
5457 61 863113	192 168 2 7	172 16 83 181	DNS	235 Standard query 8x555 TYT 0E0 ALLATO MISOLYTUP/CECEDBIOSTANDARD SAMOSALT MARKANING TRANSPORT
5459 61.866004	192.168.2.7	172.16.83.101	DNS	107 Standard overv Bydra2 TXT OFIO Adalate hadalatokaOr87/JFIN-bydali/Solaeddadada

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

a trafficdump	1905230941.pcapng				- 🗆 X
Ela Eda Ma	- Go Casture Assture Sta	tistics Telephones Wire	iters Teals Male		
Los Tou Ye	a So Pabinic Branza Sta	The second the	pere Trois Eleh		
			a a 11		
R drs					Expression +
No.	Time	Source	Destination	Protocol	Length Info
	5147 47.866597	8.8.8.8	192.168.2.7	DNS	188 Standard guery response 0x3143 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME a-0
	5148 47.879521	8.8.8.8	192.168.2.7	DNS	188 Standard query response 0xa288 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME a-0
	5149 47.888127	8.8.8.8	192.168.2.7	DNS	188 Standard query response 0x003b A www.bing.com CNAME a-00001.a-afdentry.net.trafficmanager.net CNAME a-0
	5338 60.456716	192.168.2.7	8.8.8.8	DIVS	75 Standard query 0x0b5d A medlineplus.gov
	5339 60.493342	8.8.8.8	192.168.2.7	DNS	91 Standard query response 0x0b5d A medlineplus.gov A 130.14.16.160
	5426 61.788996	192.168.2.7	8.8.8.8	DNS	75 Standard query 0xe6<4 A www.nlm.nih.gov
	5429 61.813923	192.168.2.7	172.16.83.101	DNS	74 Standard guery 0xd593 TXT QEZyM1N6AAAACw
	5430 61.822057	172.16.83.101	192.168.2.7	DNS	86 Standard guery response 8xd593 TXT QEZyHIN6AAAACw TXT
	5439 61.825394	192.168.2.7	172.16.83.101	DNS	235 Standard query 0xe5c7 TXT QENQ.AAAAAA N3q8ryccAAT2/wqdMAQAAAAAAB6AAAAAAAI79.NB/XnkC2Nwks328DQ1kEh n
	5440 61.827646	172.16.83.101	192.168.2.7	DNS	247 Standard guery response 0xeSc7 TXT QE Q.AAAAAA.N3qBryccAAT2/wqdMAQAAAAAAB6AAAAAAAAAAA79.NB/XnkC2Muks 2
	5441 61.828236	192.168.2.7	172.16.83.101	DNS	235 Standard guery 0xd08b TXT QENQ.AAAAAQ AfF3hYA2YSuzeIuGvuM2HSpqL9f8HYZz8iAMpb5j.cSbs9rawqdPQbYHXhlmdu S
	5442 61.837093	172.16.83.101	192.168.2.7	DNS	247 Standard guery response 0xd08b TXT QE Q.AAAAAQ.AFF3hYA2YSuzeIuGvuHZHSpqL9f8HYZz8inRpbSj.cSbs9rawqdPQ YI
	5443 61.837740	192.168.2.7	172.16.83.101	DNS	235 Standard query 0x258c TXT QENQ.AAAAAg RRMixKQL9UCNQ8Nplhf6Wpjtvylomeqs3lIIC4vN.1Rj38uS+xCgp0XLAl2a68 +
	5444 61.840027	172.16.83.101	192.168.2.7	DNS	247 Standard query response 0x258c TXT QE Q.AAAAAg.RRMWxKQL9UCNQ8Nplhf6wpjtvylomeqs3lIIIC4vN.1Rj38u5+xCgp X
	5445 61.840613	192.168.2.7	172.16.83.101	DNS	235 Standard query 0x7a1b TXT QENQ.AAAAAw C1jQ221422paZr3128z1ZnP3NoPXMmhX9rOyXFUG.N56QDGa0qa2k+7v17YEuf e
	5446 61,843938	172.16.83.101	192.168.2.7	DNS	247 Standard guery response 0x7alb TXT QE Q.AAAAAw.CljQ221422paZr3128z12nP3NoPXNmhX9rDyXFUG.NS6QDGa0qa2k 7
	5447 61.844599	192.168.2.7	172.16.83.101	DNS	235 Standard query 0xc272 TXT QENQ.AAAABA KSDVb8eb4bsNEGiDgD88aMNykKNqgjIraW7oyyRV.Tzuzryoujy861wF8t+TWs x
	5448 61.846662	172.16.83.101	192.168.2.7	DNS	247 Standard query response 0xc272 TXT QE Q.AAAABA.kSDVb8eb4bsNEGiDgD88a/WykKNqgJIraW7oyyRV.Tzuzryoujy86 w
	5449 61.847285	192.168.2.7	172.16.83.101	DNIS	235 Standard query 0xSeb1 TXT QENQ.AAAABQ AaKeKJIK7a1hCYs9qkbvu/Cqrtlg4/lw09ljygYi.ZC8w29f/XiLUEGNqIm9Gk 9
	5450 61.851796	172.16.83.101	192.168.2.7	DNS	247 Standard query response 0x5eb1 TXT QE Q.AAAA8Q.AaKeKJIK7a1hCYs9qkbvuMCqzt1g4/lw09ljygYi.ZC8w29f/XiLU G
	5451 61.852568	192.168.2.7	172.16.83.101	DNS	235 Standard query 0x73eb TXT QENQ.AAAABg pA9juU2URN9NfKaloNgBN3RnKj3gPVubVHrF11WW.A/IVBe3rrSmRxD2EpzaNT j
	5452 61.856622	172.16.83.101	192.168.2.7	DNS	247 Standard query response 0x73eb TXT QE Q.AAAA8g.pA9juU2URN9NfKaIoNg8N3RnKj3gPVubVHrFl1NN.A/IVBe3rr5mR_D
	5453 61.857223	192.168.2.7	172.16.83.101	DNS	235 Standard query 0x27a2 TXT QENQ.AAAA8w 7LEq3pb/y80Ua13u5j6T8gTQfKF385VnGerOLb2F.vGZ78CjEH3aG3MaTxHNan C
	5454 61.859550	172.16.83.101	192.168.2.7	DWS	247 Standard query response 0x27a2 TXT QE Q.AAAABw.7LEq3pb/yB0Ua13uSj6T8gTQfKF38SVnGerDLb2F.vGZ78CjEH3aG M
	5455 61.860113	192.168.2.7	172.16.83.101	DNS	235 Standard guery 0x9123 TXT QENQ.AAAACA UAv5d5xigIweRetxkD6xXjEm8ZVjdbcF24wrtk6C.ps8krdf3p1YdLdn1pw0K2dP

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

Open Recent	,		441		
Merge	f	Source	Destination	Protocol	Length Info
Import from Hex Dump		192.168.2.7	172.16.83.101	DNS	74 Standard query 0xd593 TXT QEZyM1N6AAAACw
Close	Ctrl+W	192.168.2.7	172.16.83.101	DNS	235 Standard guery 0xe5c7 TXT QENQ.AAAAAA.N3g8ryccAAT2/wg
Same	2 1 1 47	192.168.2.7	172.16.83.101	DNS	235 Standard guery 0xd08b TXT QENQ.AAAAAQ.AfF3hYA2YSuzeIu
Court As	CLI CLID C	192.168.2.7	172.16.83.101	DNS	235 Standard guery 0x258c TXT QENQ.AAAAAg.RRMixKQL9UCNQBN
Save As Ctri+Shift+S		192.168.2.7	172.16.83.101	DNS	235 Standard guery 0x7a1b TXT QENQ.AAAAAAw.CljQ22i422paZr3
File Set		192.168.2.7	172.16.83.101	DNS	235 Standard guery 0xc272 TXT QENO.AAAABA.kSDVb8eb4bsNEGi
		192.168.2.7	172.16.83.101	DNS	235 Standard guery 0x5eb1 TXT QENQ.AAAABQ.AaKeKJIK7a1hCYs
Export Specified Packets		**** *** * *	172.16.83.101	DNS	235 Standard guery 0x73eb TXT QENO.AAAABg.pA9juU2URN9NfKa
Export Packet Dissections	*	As Plain Text	172.16.83.101	DNS	235 Standard guery 0x27a2 TXT QENO.AAAAABw.7LEgJpb/y80Ua1J
Export Packet Bytes	Ctrl+Shift+X	As CSV	172.16.83.101	DNS	235 Standard guery 0x9123 TXT OENO.AAAACA.UAvSd5xWgIweRef
Export PDUs to File		As "C" Arrays	172.16.83.101	DNS	235 Standard guery 0xfa56 TXT OENO.AAAACO.kU301x1fWOFczD9
Export TLS Session Keys			172,16,83,101	DNS	107 Standard guery 0xdc42 TXT OENO, AAAACg, bAAAABOKAOC8f/F
Event Objects		As PSML XML			
Export objects		As PDML XML			

### Open the exported file and investigate.

Ede Edit Search View Encoding Language Settings Tools Macro Run Plugins Window 2		x
exported cav [3]		
1 nation", "Protocol", "Length", "Info" 2 2.7", "172.16.83.101", "DNS", "74", "Standard query 0xd593 TXT QEZyM1N6AAAAACw" 3.2", "172.16.83.101", "DNS", "235", "Standard query 0xe5c7 TXT OENO.AAAAAA.M308ryccAA	wodMAOAAAAAAAAB6AAAAAAAAAI79.WB/Xnko	CZMuksJ28D01kEhmnea6/WIJcGokSMIaL2.apLB98ula
4 2.7", '172.16.83.101", 'DNS", '235", 'Standard query 0xd08b TXT QENQ.AAAAAQ.AfF3hYA2YS 5 2.7", '172.16.83.101', 'DNS', '235', 'Standard query 0x258c TXT QENQ.AAAAAQ.RMWxkQQU0 6 2.7", '172.16.83.101', 'DNS', '235', 'Standard query 0x7ab TXT QENQ.AAAAAA.Clj022t422	IuGvuMZHSpqL9fBHYZz8inMpbSj.cSbs9ra BNpIhf6Wpjtvy1omeqsJlIIC4vN.1RjJ8u r3l28zlZnP3NoPXNmhX9rDyXFUG.NS6QDGa	awqdPQbYHXhlmdUgSC8HwMbVfihCphanKf.CqFMGJsMB S+xCgp0XLAl2a68t+UU3MFDKpxqrb9qi/a.of880HL4I a0qa2k+7vi7YEufMesUJo1Iw8Lcuy9Tbc8.7v6aJdW0f
7 2.7", "172.16.83.101", "DNS", "235", "Standard query 0xc272 TXT QENQ.AAAABQ.ksK0Vb8cb40 8 2.7", "172.16.83.101", "DNS", "235", "Standard query 0x5eb1 TXT QENQ.AAAABQ.AaKeK3IX73 9 2.7", "172.16.83.101", "DNS", "235", "Standard query 0x73eb TXT QENQ.AAAABQ.AaKeK3IX73	GiDgD88aMNykKWqgJIraW7oyyRV.Tzuzryc Ys9qkbvwMCqztlg4/lw09ljygYi.ZC8w291 Ka1oWg8N3RnKj3gPVubVHrFl1WW.A/IVBe	oujyB6IwF8t+TWsixF/yzb67nYVEÍxOwEn.tw0pA6ODP f/XiLUEGNqIm9Gk/9Hkw404KFAIov4Phdh.+2tRabwgn 3rrSmRxD2EpzaNTgjmE0vDZ51MPyU+nBkI.S+3KjEEpN
10 2.7", '172.16.83.101', 'DNS', '235', 'Standard query 0x27a2 TXT QENQ.AAAABX_ILEqJpb/y8 11 2.7", '172.16.83.101', 'DNS', '235', 'Standard query 0x9123 TXT QENQ.AAAACA.UAv5dSxHgT 2.7", '172.16.83.101', 'DNS', '235', 'Standard query 0xfa56 TXT QENQ.AAAACQ.kU301x1FNQ	1JuSj6T8gTQfKFJ8SVnGerDLb2F.vGZ78C efxkD6xXjEm8ZVjdbcF24urtk6C.ps8Krd1 D9GNgb5Mxg9S1nyp/3+AQQGAAEJ.hDAABw	jEH3aGJMaTxWNanYCPgUFgPOm/BdgJS3bq.f6v2ByF31 f3piYdLdnipwOK2dPLAHBM+mFaTFIizQdi.wVZ46A82+ sBAAIkBvEHAQpTB3DW9MZDBKkeISEBAAEA.DIQmjPYAC
13 2.7","172.16.83.101","DNS","107","Standard query 0xdc42 TXT QENQ.AAAACg.bAAAABQKAQ	/FFNhHVARUGAQAgAAAAAAA"	
د Normal text file	th:2,966 lines:14 Ln:14 Col:1 Sel:0	Windows (CR LF) UTF-8 IN

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:

Elie Edit Sauch View Encoding Lunguage Settings Tools Micro Bun Bugins Window 2	MIJCGokSMIaL2qpLB998ulaXHMr2l+kIpBg MUDYGhCgPHGJsMBpfNP/G7bupJ HFDKparb9q/aofB80HL414075nn9NTpwf J1WBLcuyPE37Vs6J3MBfYGYssffCH00- b04KFA104Phdh-2tRabwghUTBJ94cKnvuk uD25IPMyUnBkIS-3XJEEpNeL-BxtV08z66 FgP0n/BdgJS3bqf6v2ByF31FV7Jwq4Fntf6 JHnr6aTFI:tqdtwlZ46A82+b2x807NtJ2cc DDBKkeISEBAAEADIQmjPYACAoBRuZotgAAE	/UBtQ6x1y99N6/J59zYZjCrKS6rD JiqjIZXMzj+INFEN+/xu+v2ZxMr FPGshops9+tw0s1RTEr8Fb6N3npc (uf+j26IXzCBpB1ptschCn2xhBL0 (uf+j26IXzCBpB1ptschCn2xhBL0 yrpfi63Uu63dw3LYfSLRvZyg9h N1150cuICaJ7uvmHnbzUGrVthC09 scXAM0IPnk/aVe262-JYGVMrZQIF Alij912CLFFbhuMxhNAF/JBFKD3+ QGEZBgAAAAAAABELAHAAYQ80AGkA	mNwqBm/eM61+DsIR2 CxGSY0+8axzLypALL 11qoBEVMOwzED7M87 23asFiPiCrY3jGC2d 2NmKK2ZLg7UmK/eI 20etqbL4-JxXR2SyvM ijFSq212C7I52D9Xx 4/t60Y016cXJcHd61 ZQBUAHQAcw8fADIAH	8beDBoo60KtjBPlq "mrzW20GoR3tz9cD XRjWsitNPLA/dxM (091dpjH=KR5SCO .79gX1+0CSTVNavJ InBrZw81V0px+swB I7DeXvtjqY9/K4BF (r+CQ708ZRju9gy7 J.7QwSxu+o/Vv55z LAAxADkALgBzAHEA
¢				

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

Eile Edit	Search View Encoding Language Settings Tools Macro Run Plugins Window 2
extracte	
1 7:	z% <sup>- \</sup> ESNULEOTöÿ
2 0	EOTNULNULNULNULNULNULNULNULNULNULNULNULNULN
3 ;1	LCAN>FFACK—Í?ñ»nêuþX°@†W38þ ND7ïñ»ëögNAK«VNDCAÌ′cO%kFSËÉVN-jó[c†;GS\Ï×ÉTXEDCSSYNĤVNō@@DCB\"FTBúZ~í
4 X	ŊŨħ,ŨjZf%åÛÌåfs÷6f×6ħWö°ò\UÆK5.☶f´@·¤û»âí. ǬPš5#\$コ\Mrrì%M·<îþš%Õ´~¦,²·ÜXú/^ámž¥_1,¤GSi¶Ç;\$UBm°,,DG
5 D	I∰f€? <hār¥ª€'+inèë\$u0;³⁻*. td="" z#soh ·äö²,eÿ,ûë¹øtb1;soh'·<=""></hār¥ª€'+inèë\$u0;³⁻*.>
6)	■IX4£f>ဩIX°>,-ʇ[≦SCaÎp_H;lwÈ%â%øÚ⊟N0`aÁ°⊑SÜùŠ+fKf,⊚šOÞ-³à´\$Ö5«ÉSO1¢ž('
7 i	_a <=°FïÀÀ°ÎÙ`āùpÓÙcÊÆKK"d/0Û×ÿ^"ÔDEcj"oF"ÿG <b>"SOSO</b> à;@"<ø>ITBaûkQi% b 2ŽIS[IS8,_) %•Q@9wÌ7+‡Ò,ÆUÞSTa.
8 3	
0 0	

Change the file extension to 7z' and open it:

<u>File Edit View Favori</u>	ites <u>T</u> ools <u>H</u> elp				
Add Extract Test	Copy Move D	× 1 elete Info			
C:\Users\Dániel	Göttler\Docume	ents\ITU2019\walk-through\extracted.7z\			
Name	Size	Packed Size Modified	Attributes	CRC	Encrypted Method
patients_2019.sql	3 318	1 072 2019-05-23 09:08	А	B668E646	+ LZMA2:12 7zAES:19
0 / 1 object(s) selecte					

'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

dyGorxCJIEnq2aGSqaLF8nZh5lko7vmn

gjaPUrWk1Na6InDonnqCHFI0gzL1ozAk

The third one helps:



Here is the proof of the data breach.