сайт команды "err0r-451" / "err0r-451" team website

Nuit du Hack 2016 — Forensics — Trololo [100 PTS]

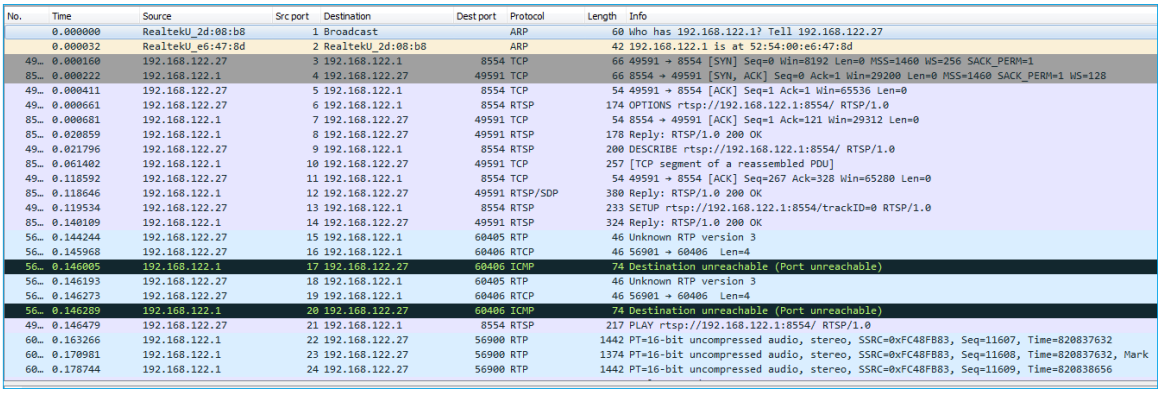
by lostpassword

Task: A computer belonging to a new company has been infected by a malware. This is a known version of a cryptolocker software, that uses a irc server to received commands. Let's try to grab its password…
File: trololo.pcap

English

TL;DR: Wireshark filters + a tiny bit of cryptanalysis.

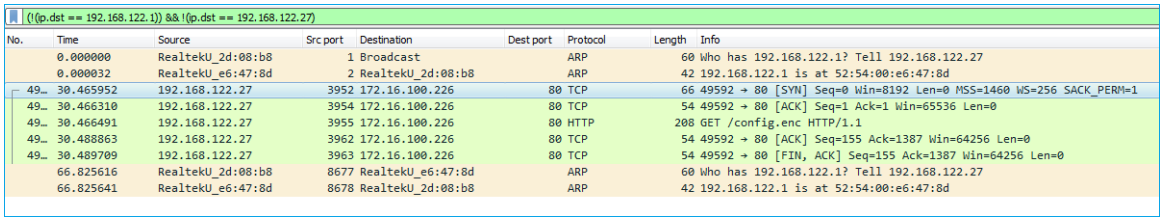
The first step is quite obvious: just open a PCAP file with Wireshark.



No.	Time	Source	Src port	Destination	Dest port	Protocol	Length	Info
	0.000000	RealtekU_2d:08:b8	1	Broadcast		ARP	60	Who has 192.168.122.1? Tell 192.168.122.27
	0.000032	RealtekU_e6:47:8d	2	RealtekU_2d:08:b8		ARP	42	192.168.122.1 is at 52:54:00:e6:47:8d
49…	0.000160	192.168.122.27	3	192.168.122.1	8554	TCP	66	49591 → 8554 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
85…	0.000222	192.168.122.1	4	192.168.122.27	49591	TCP	66	8554 → 49591 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
49…	0.000411	192.168.122.27	5	192.168.122.1	8554	TCP	54	49591 → 8554 [ACK] Seq=1 Ack=1 Win=65536 Len=0
49…	0.000661	192.168.122.27	6	192.168.122.1	8554	RTSP	174	OPTIONS rtsp://192.168.122.1:8554/ RTSP/1.0
85…	0.000681	192.168.122.1	7	192.168.122.27	49591	TCP	54	8554 → 49591 [ACK] Seq=1 Ack=121 Win=29312 Len=0
85…	0.020859	192.168.122.1	8	192.168.122.27	49591	RTSP	178	Reply: RTSP/1.0 200 OK
49…	0.021796	192.168.122.27	9	192.168.122.1	8554	RTSP	200	DESCRIBE rtsp://192.168.122.1:8554/ RTSP/1.0
85…	0.061402	192.168.122.1	10	192.168.122.27	49591	TCP	257	[TCP segment of a reassembled PDU]
49…	0.118592	192.168.122.27	11	192.168.122.1	8554	TCP	54	49591 → 8554 [ACK] Seq=267 Ack=328 Win=65280 Len=0
85…	0.118646	192.168.122.1	12	192.168.122.27	49591	RTSP/SDP	380	Reply: RTSP/1.0 200 OK
49…	0.119534	192.168.122.27	13	192.168.122.1	8554	RTSP	233	SETUP rtsp://192.168.122.1:8554/trackID=0 RTSP/1.0
85…	0.140109	192.168.122.1	14	192.168.122.27	49591	RTSP	324	Reply: RTSP/1.0 200 OK
56…	0.144244	192.168.122.27	15	192.168.122.1	60405	RTP	46	Unknown RTP version 3
56…	0.145968	192.168.122.27	16	192.168.122.1	60406	RTCP	46	56901 → 60406 Len=4
56…	0.146005	192.168.122.1	17	192.168.122.27	60406	ICMP	74	Destination unreachable (Port unreachable)
56…	0.146193	192.168.122.27	18	192.168.122.1	60405	RTP	46	Unknown RTP version 3
56…	0.146273	192.168.122.27	19	192.168.122.1	60406	RTCP	46	56901 → 60406 Len=4
56…	0.146289	192.168.122.1	20	192.168.122.27	60406	ICMP	74	Destination unreachable (Port unreachable)
49…	0.146479	192.168.122.27	21	192.168.122.1	8554	RTSP	217	PLAY rtsp://192.168.122.1:8554/ RTSP/1.0
60…	0.163266	192.168.122.1	22	192.168.122.27	56900	RTP	1442	PT=16-bit uncompressed audio, stereo, SSRC=0xFC48FB83, Seq=11607, Time=820837632
60…	0.170981	192.168.122.1	23	192.168.122.27	56900	RTP	1374	PT=16-bit uncompressed audio, stereo, SSRC=0xFC48FB83, Seq=11608, Time=820837632, Mark
60…	0.178744	192.168.122.1	24	192.168.122.27	56900	RTP	1442	PT=16-bit uncompressed audio, stereo, SSRC=0xFC48FB83, Seq=11609, Time=820838656

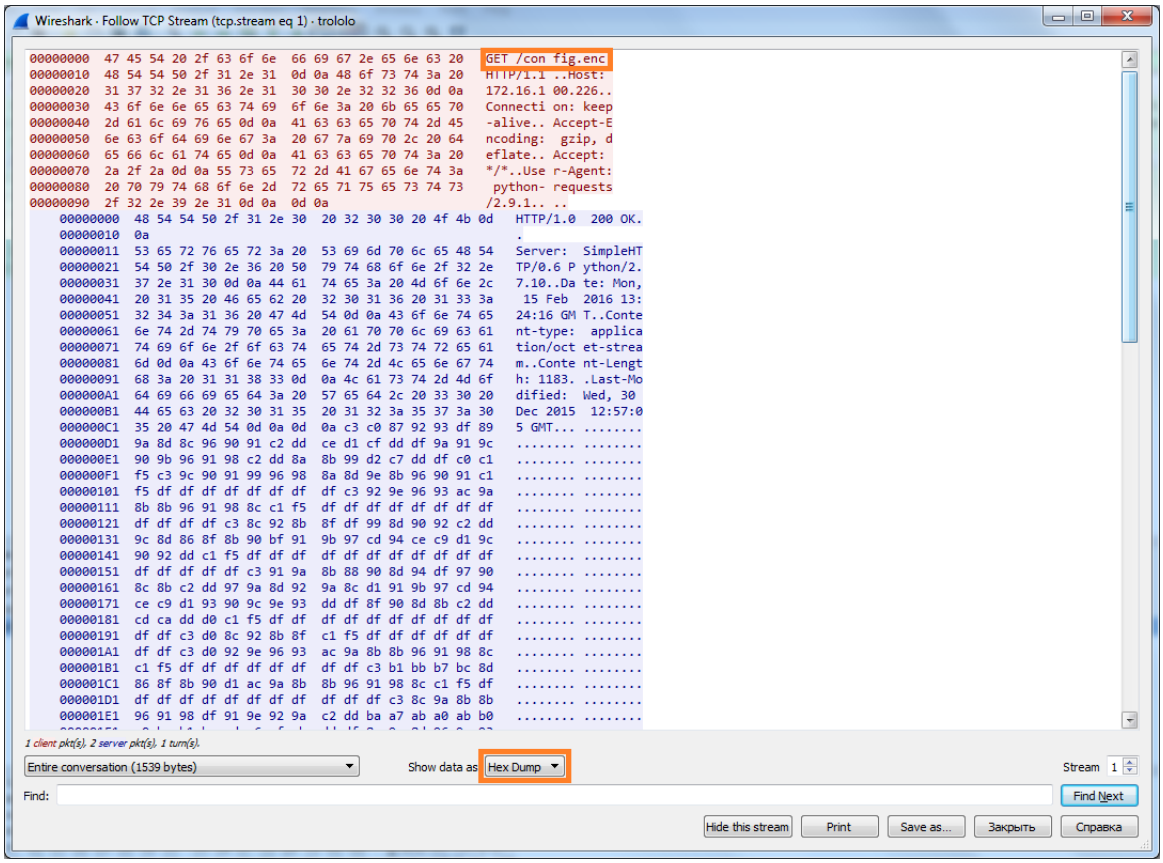
As we can see, many packets are circulating between 192.168.122.1 and 192.168.122.27. Since these addresses are internal (non-routable in the Internet), this traffic is probably not our goal. The situation when malware C&C server is operating right within the internal network is quite uncommon. □

So we can filter these packets out:



Most of the packets were filtered out. And now we can spot easily the interesting TCP session between 192.168.122.27 and 172.16.100.226.

The next step is to view the conversation between these hosts. Right-click on the session and select «Follow» -> «TCP Stream». After that we may select the «Hex Dump» mode in the window opened:



As we can see, there's a HTTP request from 192.168.122.27 to 172.16.100.226, in which a «config.enc» file is requested from the server. Looks like that's the malware configuration file we're looking for!

Now we must obtain this file from Wireshark. When I was solving this challenge, I selected the «Raw» mode, then copied hex data to the text document and decoded it with Python. While writing this writeup, however, I realized that there is another, much convinient way to do it. We can just use the «File» -> «Export Objects…» -> «HTTP» menu item in Wireshark.

Anyway, here is the data:

C3 C0 87 92 93 DF 89 9A 8D 8C 96 90 91 C2 DD CE D1 CF DD DF 9A 91 9C 90 9B 96 91 98 C2 DD 8A 8B 99 D2 C7 DD DF C0 C1 F5 C3 9C 90 91 99 96 98 8A 8D 9E 8B 96 90 91 C1 F5

DF DF DF DF DF DF DF DF C3 92 9E 96 93 AC 9A 8B 8B 96 91 98 8C C1 F5 DF DF DF DF
DF DF DF DF DF DF DF DF C3 8C 92 8B 8F DF 99 8D 90 92 C2 DD 9C 8D 86 8F 8B 90 BF
91 9B 97 CD 94 CE C9 D1 9C 90 92 DD C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF
DF DF DF DF C3 91 9A 8B 88 90 8D 94 DF 97 90 8C 8B C2 DD 97 9A 8D 92 9A 8C D1 91 9B
97 CD 94 CE C9 D1 93 90 9C 9E 93 DD DF 8F 90 8D 8B C2 DD CD CA DD D0 C1 F5 DF DF
DF DF DF DF DF DF DF DF DF DF C3 D0 8C 92 8B 8F C1 F5 DF DF DF DF DF DF DF DF DF
C3 D0 92 9E 96 93 AC 9A 8B 8B 96 91 98 8C C1 F5 DF DF DF DF DF DF DF DF C3 B1 BB
B7 BC 8D 86 8F 8B 90 D1 AC 9A 8B 8B 96 91 98 8C C1 F5 DF DF DF DF DF DF DF DF DF
DF DF DF C3 8C 9A 8B 8B 96 91 98 DF 91 9E 92 9A C2 DD BA A7 AB A0 AB B0 A0 BA B1
BC AD A6 AF AB DD DF 8C 9A 8D 96 9E 93 96 85 9A BE 8C C2 DD AC 8B 8D 96 91 98 DD
C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF DF DF DF DF C3 89 9E 93 8A 9A C1 9B
90 9C 87 C5 9B 90 9C C5 87 93 8C C5 87 93 8C 87 C5 8F 9B 99 C5 95 8F 98 C5 90 9B 8B C5
90 9B 8C C5 8F 91 98 C5 9D 92 8F C5 9E 89 96 C5 92 8F CB C3 D0 89 9E 93 8A 9A C1 F5
DF DF DF DF DF DF DF DF DF DF DF DF C3 D0 8C 9A 8B 8B 96 91 98 C1 F5 DF DF DF
DF DF DF DF DF DF DF DF DF DF DF C3 8C 9A 8B 8B 96 91 98 DF 91 9E 92 9A C2 DD B4 BA A6
DD DF 8C 9A 8D 96 9E 93 96 85 9A BE 8C C2 DD AC 8B 8D 96 91 98 DD C1 F5 DF DF DF
DF DF DF DF DF DF DF DF DF DF DF DF DF C3 89 9E 93 8A 9A C1 BE BB C8 C7 CB BB
BE C9 CD BB CE BB BB BD BD CE C6 BD C8 B9 CF CA CF CF BE CA CD BB BB CE CA
BC CF BD BB C8 CF B9 C6 CD CB BE CA BA B9 C8 BC CC BC BA BE CE CC CB BC CB
CD C7 C8 CB C8 BE B9 BD C3 D0 89 9E 93 8A 9A C1 F5 DF DF DF DF DF DF DF DF DF
DF DF DF C3 D0 8C 9A 8B 8B 96 91 98 C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF
C3 8C 9A 8B 8B 96 91 98 DF 91 9E 92 9A C2 DD AC AA BD B5 BA BC AB DD DF 8C 9A 8D
96 9E 93 96 85 9A BE 8C C2 DD AC 8B 8D 96 91 98 DD C1 F5 DF DF DF DF DF DF DF DF
DF DF DF DF DF DF DF DF C3 89 9E 93 8A 9A C1 B1 9A 88 DF 96 91 99 9A 9C 8B 9A 9B
C3 D0 89 9E 93 8A 9A C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF C3 D0 8C 9A 8B 8B
96 91 98 C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF C3 8C 9A 8B 8B 96 91 98 DF 91
9E 92 9A C2 DD B6 AD BC A0 AC AD A9 DD DF 8C 9A 8D 96 9E 93 96 85 9A BE 8C C2 DD
AC 8B 8D 96 91 98 DD C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF DF DF DF DF C3
89 9E 93 8A 9A C1 96 8D 9C C5 D0 D0 96 8D 9C D1 91 9B 97 CD 94 CE C9 D1 9C 90 92 C5
C9 C9 C9 C8 C3 D0 89 9E 93 8A 9A C1 DF F5 DF DF DF DF DF DF DF DF DF DF DF DF DF
C3 D0 8C 9A 8B 8B 96 91 98 C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF C3 8C 9A 8B
8B 96 91 98 DF 91 9E 92 9A C2 DD B6 AD BC A0 BC B7 BE B1 DD DF 8C 9A 8D 96 9E 93
96 85 9A BE 8C C2 DD AC 8B 8D 96 91 98 DD C1 F5 DF DF DF DF DF DF DF DF DF DF
DF DF DF DF DF DF C3 89 9E 93 8A 9B 9A C1 DC BC 8D 86 8F 8B CF B1 BB B7 CD B4 CE
C9 C3 D0 89 9E 93 8A 9A C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF C3 D0 8C 9A 8B
8B 96 91 98 C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF C3 8C 9A 8B 8B 96 91 98 DF
91 9E 92 9A C2 DD B6 AD BC A0 BC B7 BE B1 AF BE AC AC DD DF 8C 9A 8D 96 9E 93 96
85 9A BE 8C C2 DD AC 8B 8D 96 91 98 DD C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF
DF DF DF DF DF C3 89 9E 93 8A 9A C1 90 8D 8A 9B 9A 8A 95 96 9A 97 C9 90 90 91 98 9A
CB AC 97 9A C3 D0 89 9E 93 8A 9A C1 F5 DF DF DF DF DF DF DF DF DF DF DF DF DF C3 D0
8C 9A 8B 8B 96 91 98 C1 F5 DF DF DF DF DF DF DF DF C3 D0 B1 BB B7 BC 8D 86 8F 8B
90 D1 AC 9A 8B 8B 96 91 98 8C C1 F5 C3 D0 9C 90 91 99 96 98 8A 8D 9E 8B 96 90 91 C1 F5

No meaningful ASCII symbols, no nothing. I had no idea what am I supposed do with all that stuff.

Maybe a bit of Google search can help?

https://www.google.ru/search?q=%22config.enc%22
https://www.google.ru/search?q=%22config.enc%22&start=10
https://www.google.ru/search?q=%22config.enc%22+
https://www.google.ru/search?q=%22config.enc%22+cryptolocker+
https://www.google.ru/search?q=%22config.enc%22+malware
https://www.google.ru/search?q=%22config.enc%22+virus
https://www.google.ru/search?q=184.25.56.98+%22config.enc%22
https://www.google.ru/search?q=184.25.56.98+config.enc
https://www.google.ru/search?q=GET+%2Fconfig.enc

And I found something indeed! Here is a blog of an «Aspiring Cyber Security Specialist» with a very interesting article regarding the «Insomnia» trojan. That malware was written with .NET, so the blog author decompiled it with DotPeek, regained the source code, analyzed it — and even managed to write a small program with C# to decrypt the config file! Great job, I mean it!

Perfect work! But completely useless in this challenge. What a pity…

Another interesting link is a Malwr.com sample analysys. A file named «config.enc» has been analyzed on the April, 1st. No use in our task, however.

You know, I'm not very fond of thinking — I'd rather prefer to google. But that time I had no options left, soooo…

I was completely stuck. I had no idea what to do. But at it often happens, help came from an unexpected quarter.

A few days ago I've decided to take a Cryptography course at Coursera. Professor Dan Boneh is a great tutor, I'm looking forward to the upcoming lectures. In the last part of the first module there was a task to decrypt the encoded message. I've remembered that task and decided to use the same approach here.

As we can surely notice, the ciphertext contains a bunch of «DF» bytes, and these bytes are often grouped together. I assumed that the initial message was encoded byte by byte using a simple XOR with some key byte. If that is true, these «DF» bytes might correspond to some non-letter symbol in plaintext, e. g. a space. So everything I've needed to do is to test all possible combination of the key byte. It's just 256 combinations here (well, it's actually 255, but who cares?):

```
1. esb = [195, 192, 135, 146, 147, 223, 137, 154, 141, 140, 150, 144, 145,
   194, 221, 206, 209, 207, 221, 223, 154, 145, 156, 144, 155, 150, 145,
   152, 194, 221, 138, 139, 153, 210, 199, 221, 223, 192, 193, 245, 195,
   156, 144, 145, 153, 150, 152, 138, 141, 158, 139, 150, 144, 145, 193,
   245, 223, 223, 223, 223, 223, 223, 223, 223, 195, 146, 158, 150, 147,
   172, 154, 139, 139, 150, 145, 152, 140, 193, 245, 223, 223, 223, 223,
   223, 223, 223, 223, 223, 223, 223, 223, 195, 140, 146, 139, 143, 223,
   153, 141, 144, 146, 194, 221, 156, 141, 134, 143, 139, 144, 191, 145,
   155, 151, 205, 148, 206, 201, 209, 156, 144, 146, 221, 193, 245, 223,
   223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
```

```
223, 195, 145, 154, 139, 136, 144, 141, 148, 223, 151, 144, 140, 139,
194, 221, 151, 154, 141, 146, 154, 140, 209, 145, 155, 151, 205, 148,
206, 201, 209, 147, 144, 156, 158, 147, 221, 223, 143, 144, 141, 139,
194, 221, 205, 202, 221, 208, 193, 245, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 208, 140, 146, 139, 143, 193, 245,
223, 223, 223, 223, 223, 223, 223, 223, 195, 208, 146, 158, 150, 147,
172, 154, 139, 139, 150, 145, 152, 140, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 195, 177, 187, 183, 188, 141, 134, 143, 139, 144,
209, 172, 154, 139, 139, 150, 145, 152, 140, 193, 245, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 223, 195, 140, 154, 139, 139,
150, 145, 152, 223, 145, 158, 146, 154, 194, 221, 186, 167, 171, 160,
171, 176, 160, 186, 177, 188, 173, 166, 175, 171, 221, 223, 140, 154,
141, 150, 158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141,
150, 145, 152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 154,
193, 155, 144, 156, 135, 197, 155, 144, 156, 197, 135, 147, 140, 197,
135, 147, 140, 135, 197, 143, 155, 153, 197, 149, 143, 152, 197, 144,
155, 139, 197, 144, 155, 140, 197, 143, 145, 152, 197, 157, 146, 143,
197, 158, 137, 150, 197, 146, 143, 203, 195, 208, 137, 158, 147, 138,
154, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 195, 208, 140, 154, 139, 139, 150, 145, 152, 193, 245, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 140, 154, 139,
139, 150, 145, 152, 223, 145, 158, 146, 154, 194, 221, 180, 186, 166,
221, 223, 140, 154, 141, 150, 158, 147, 150, 133, 154, 190, 140, 194,
221, 172, 139, 141, 150, 145, 152, 221, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 195, 137,
158, 147, 138, 154, 193, 190, 187, 200, 199, 203, 187, 190, 201, 205,
187, 206, 187, 187, 189, 189, 206, 198, 189, 200, 185, 207, 202, 207,
207, 190, 202, 205, 187, 187, 206, 202, 188, 207, 189, 187, 200, 207,
185, 198, 205, 203, 190, 202, 186, 185, 200, 188, 204, 188, 186, 190,
206, 204, 203, 188, 203, 205, 199, 200, 203, 200, 190, 185, 189, 195,
208, 137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145,
152, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158, 146, 154,
194, 221, 172, 170, 189, 181, 186, 188, 171, 221, 223, 140, 154, 141,
150, 158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141, 150,
145, 152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 154, 193,
177, 154, 136, 223, 150, 145, 153, 154, 156, 139, 154, 155, 195, 208,
137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145, 152,
193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158, 146, 154, 194,
221, 182, 173, 188, 160, 172, 173, 169, 221, 223, 140, 154, 141, 150,
158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141, 150, 145,
152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 154, 193, 150,
141, 156, 197, 208, 208, 150, 141, 156, 209, 145, 155, 151, 205, 148,
206, 201, 209, 156, 144, 146, 197, 201, 201, 201, 200, 195, 208, 137,
158, 147, 138, 154, 193, 223, 245, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145, 152,
193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158, 146, 154, 194,
221, 182, 173, 188, 160, 188, 183, 190, 177, 221, 223, 140, 154, 141,
150, 158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141, 150,
145, 152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 155, 154,
193, 220, 188, 141, 134, 143, 139, 207, 177, 187, 183, 205, 180, 206,
201, 195, 208, 137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139,
150, 145, 152, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158,
146, 154, 194, 221, 182, 173, 188, 160, 188, 183, 190, 177, 175, 190,
172, 172, 221, 223, 140, 154, 141, 150, 158, 147, 150, 133, 154, 190,
```

```
    140, 194, 221, 172, 139, 141, 150, 145, 152, 221, 193, 245, 223, 223,
    223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
    195, 137, 158, 147, 138, 154, 193, 144, 141, 138, 155, 154, 138, 149,
    150, 154, 151, 201, 144, 144, 145, 152, 154, 203, 172, 151, 154, 195,
    208, 137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223, 223, 223,
    223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145,
    152, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 195, 208, 177,
    187, 183, 188, 141, 134, 143, 139, 144, 209, 172, 154, 139, 139, 150,
    145, 152, 140, 193, 245, 195, 208, 156, 144, 145, 153, 150, 152, 138,
    141, 158, 139, 150, 144, 145, 193, 245]

outfile = open("result.lol", "wb")
for i in range(0, 256):
outfile.write(b"\n\n----------------\n")
outfile.write(str(i).encode("ascii"))
outfile.write(b"\n\n")
ba = bytearray()
for b in esb:
ba.append(b ^ i)
outfile.write(ba)
outfile.close()
```

The code is not very clean — I should have read the data from the file, not from array — but that was OK for me.

Here's the output:

```
----------------
0

ÃÀ‡’"ß‰šŒ–‘ÂÝÎÑÏÝßš‘œ›–‘ÂÝŠ‹™ÒÇÝßÀÁõÃœ‘™–
Šž‹–‘ÁõßßßßßßßßÃ’ž–"¬š‹‹–‘ŒÁõßßßßßßßßßßßÃŒ’‹ß™’ÂÝœ†‹¿‘›–
Í"ÎÉÑœ’ÝÁõßßßßßßßßßßßßßßßßÃ‘š‹^"ß—Œ‹ÂÝ—š’šŒÑ‘›–
Í"ÎÉÑ"œž"Ýß‹ÂÝÍÊÝÐÁõßßßßßßßßßßßßßÃÐŒ’‹ÁõßßßßßßßßßÃÐ’ž–"¬š‹‹–‘ŒÁõßßßßßßßßßÃ
±»·¼†‹Ñ¬š‹‹–‘ŒÁõßßßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ°§«  «°  °±¼¦¯«ÝßŒš–ž"–…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßßÃ‰ž"ŠšÁ›œ‡Å›œÅ‡"ŒÅ‡"Œ‡Å›™Å•Å›‹Å›ŒÅ‘Å’Åž‰–
Å’ËÃÐ‰ž"ŠšÁõßßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ´°¦ÝßŒš–ž"–
…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßßÃ‰ž"ŠšÁ¾»ÈÇË»¾ÉÍ»Î»»½½ÎÆ½È¹ÏÊÏÏ¾ÊÍ»»ÎÊ¼Ï½»È
Ï¹ÆÍË¾Ê°¹È¼Ì¼°¾Î¹ÌË¼ËÍÇÈËÈ¾¹½ÃÐ‰ž"ŠšÁõßßßßßßßßßßßßßÃÐŒš‹‹–‘Áõßßßßßßßßßßßß
ÃŒš‹‹–‘ß‘ž’šÂÝ¬ª½µ°¼«ÝßŒš–ž"–…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßßÃ‰ž"ŠšÁ±šˆß–‘™šœ‹š›ÃÐ‰ž"ŠšÁõßßßßßßßßßßßßßÃÐŒ
š‹‹–‘ÁõßßßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ¶¼ ¬©ÝßŒš–ž"–…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßßÃ‰ž"ŠšÁ–œÅÐÐ–œÑ‘›–
Í"ÎÉÑœ’ÅÉÉÉÈÃÐ‰ž"ŠšÁßõßßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ
¶¼ ¼·¾±ÝßŒš–ž"–…š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßßÃ‰ž"Š›šÁÜ¼†‹Ï±»·Í
´ÎÉÃÐ‰ž"ŠšÁõßßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ¶¼
¼·¾±¯¾¬¬ÝßŒš–ž"–…š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßßÃ‰ž"ŠšÁŠ›šŠ•–š—É‘šË¬—
šÃÐ‰ž"ŠšÁõßßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßÃÐ±»·¼†‹Ñ¬š‹‹–‘ŒÁõÃÐœ™–Šž‹–‘Áõ

----------------
1

ÂÁ†"’Þˆ›Œ–‘ÃÜÏÐÎÜÞ›‘š—™ÃÜ‹ŠÓÆÜÞÁÀôÂ‘˝™‹ŒŸŠ—‘ÀôÞÞÞÞÞÞÂ"Ÿ–’›ŠŠ—
™ÀôÞÞÞÞÞÞÞÞÞÞÂ"ŠŽÞŒ‘"ÃÜŒ‡ŽŠ‘¾š–
Ì•ÏËÐ‘"ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÂ›Š‰‘Œ•Þ–‘ŠÃÜ–›Œ"›Ðš–
Ì•ÏËÐ’‘Ÿ’ÜÞŽ‘ŒŠÃÜÏËÜÑÀôÞÞÞÞÞÞÞÞÞÞÂÑ"ŠŽÀôÞÞÞÞÞÞÞÂÑ"Ÿ–’›ŠŠ—
™ÀôÞÞÞÞÞÞÞÂ°°¶½Œ‡ŽŠ‘Ð›ŠŠ—™ÀôÞÞÞÞÞÞÞÞÞÂ›ŠŠ—™ÞŸ"›ÃÜ»¦ª¡ª±¡»°½¬§®ªÜÞ›Œ
—Ÿ’—„›¿ÃÜŠŒ—
```

™ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÞÞÂˆŸ’‹ ›ÀŠ ‘†ÄŠ ‘Ä†’Ä†’†ÄŽŠÄ”Ž™Ä ‘ŠŠÄ ‘ŠÄŽ™Äœ“ŽÄŸˆ—
Ä“ŽÊÂÑˆŸ’‹ ›ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂÑ ›ŠŠ—™ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂ ›ŠŠ—™ÞŸ“ ›ÃÜµ»§ÜÞ ›Œ—Ÿ’—
„ ›¿ÃÜŠŒ—
™ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÞÞÂˆŸ’‹ ›À¿°ÉÆÊ°¿ÈÌ°Ï°°¹¼¼ÏÇ¼É¸ÎËÎÎ¿ËÌ°°ÏË½Î¼°ÉÎ¸ÇÌÊ¿Ë»
¸É½Í½»¿ÏÍÊ½ÊÌÆÉÊÉ¿¸¼ÃÑˆŸ’‹ ›ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂÑ ›ŠŠ—™ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂ ›ŠŠ—
™ÞŸ“ ›ÃÜ«¼´»½ª ÜÞ ›Œ—Ÿ’—„ ›¿ÃÜŠŒ—™ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÞÞÂˆŸ’‹ ›À° ›‰Þ—
ʒŠ ›šÂÑˆŸ’‹ ›ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂÑ ›ŠŠ—™ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂ ›ŠŠ—™ÞŸ“ ›ÃÜ ·¬½¡¬¨ÜÞ ›Œ—
Ÿ’—„ ›¿ÃÜŠŒ—™ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÞÞÂˆŸ’‹ ›À—ŒÄÑÑ—ŒÐš–
Ì•ÏÈÐ‘“ÄÈÈÈÉÂÑˆŸ’‹ ›ÀÞôÞÞÞÞÞÞÞÞÞÞÞÞÂÑ ›ŠŠ—™ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂ ›ŠŠ—
™ÞŸ“ ›ÃÜ ·¬½¡½¶¿°ÜÞ ›Œ—Ÿ’—„ ›¿ÃÜŠŒ—
™ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÞÞÂˆŸ’‹ š ›ÀÝ½Œ‡ŽŠÎ°°¶ÌµÏÈÂÑˆŸ’‹ ›ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂÑ ›ŠŠ—
™ÀôÞÞÞÞÞÞÞÞÞÞÞÞÂ ›ŠŠ—™ÞŸ“ ›ÃÜ ·¬½¡½¶¿°®¿ÜÞ ›Œ—Ÿ’—„ ›¿ÃÜŠŒ—
™ÜÀôÞÞÞÞÞÞÞÞÞÞÞÞÞÞÂˆŸ’‹ ›À‘Œ‹ š ›‹ ”—›–
È‘‘™ ›Ê– ›ÂÑˆŸ’‹ ›ÀôÞÞÞÞÞÞÞÞÞÞÞÂÑ ›ŠŠ—™ÀôÞÞÞÞÞÞÞÂÑ°°¶½Œ‡ŽŠ‘Ð ›ŠŠ—™ÀôÂÑ‘“
™‹ŒŸŠ—‘Àô

2

ÁÂ…‘Ý‹Ž”’“ÀßÌÓÍßÝ“ž’™”“šÀß^‰ ›ÐÅßÝÂÃ÷Áž’“ ›”š^œ‰”’“Ã÷ÝÝÝÝÝÝÝÝÁœ”‘®‰
‰”“šŽÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁŽ‰Ý ›’Àßž„‰’½“™•Ï–ÌËÓž’ßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ“‰Š’–
Ý•’Ž‰Àß•ŽÓ“™•Ï–ÌËÓ‘’žœ‘ßÝ’‰ÀßÏÈßÒÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰Ã÷ÝÝÝÝÝÝÝÝÁÒœ”‘®‰
‰”“šŽÃ÷ÝÝÝÝÝÝÝÝÁ³¹µ¾„‰’Ó®‰‰”“šŽÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁž‰‰”“šÝ“œÀß¸¥©¢©²¢¸³¾¯¤–
©ßÝŽ”œ‘”‡¾ŽÀß®‰”“šßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ‹œ‘ˆÃ™’ž…Ç™’žÇ…‘ŽÇ…‘Ž…Ç™ ›Ç—
šÇ’™‰Ç’™ŽÇ“šÇŸÇœ‹ ”ÇÉÁÒ‹œ‘ˆÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰‰”“šÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁŽ‰
‰”“šÝ“œÀß¶¸¤ßÝŽ”œ‘”‡¾ŽÀß®‰”“šßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ‹œ‘ˆÃ¼¹ÊÅÉ¹¼ËÏ¹Ì¹¹¿¿ÌÄ
¿Ê»ÍÈÍÍ¼ÈÏ¹¹ÌÈ¾Í¿¹ÊÍ»ÄÏÉ¼È¸»Ê¾Î¾¸¼ÌÎÉ¾É¼ÏÅÊÉÊ¼»¿ÁÒ‹œ‘ˆÃ÷ÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰
‰”“šÃ÷ÝÝÝÝÝÝÝÝÝÝÝÁŽ‰
‰”“šÝ“œÀß®¨¿¸¸¾©ßÝŽ”œ‘”‡¾ŽÀß®‰”“šßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ‹œ‘ˆÃ³ŠÝ”“ ›ž‰™ÁÒ‹œ
‘ˆÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰‰”“šÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁŽ‰‰”“šÝ“œÀß
´¯¾¢®¯«ßÝŽ”œ‘”‡¾ŽÀß®‰”“šßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ‹œ‘ˆÃ”ŽÇÒÒ”žÓ“™•Ï–
ÌËÓž’ÇËËËÊÁÒ‹œ‘ˆÃÝ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰‰”“šÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁŽ‰‰”“šÝ“œÀß
´¯¾¢³¾µ¼³ßÝŽ”œ‘”‡¾ŽÀß®‰”“šßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ‹œ‘ˆ™ÃÞ³„‰Í³¹µÏ¶ÌËÁÒ‹œ‘ˆÃ÷
ÝÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰‰”“šÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÁŽ‰‰”“šÝ“œÀß´¯¾¢³¾µ¼³–
¼®®ßÝŽ”œ‘”‡¾ŽÀß®‰”“šßÃ÷ÝÝÝÝÝÝÝÝÝÝÝÝÝÝÁ‹œ‘ˆÃ’ˆ™ˆ
—”•Ë’’“šÉ®•ÁÒ‹œ‘ˆÃ÷ÝÝÝÝÝÝÝÝÝÝÝÁÒŽ‰‰”“šÃ÷ÝÝÝÝÝÝÝÁÒ³¹µ¾„‰’Ó®‰
‰”“šŽÃ÷ÁÒž’“ ›”š^œ‰”’“Ã÷

3

ÀÃ„‘ÜŠ™Ž•“’ÁÞÍÒÌÞÜ™’Ÿ“•’ ›ÁÞ‰^šÑÄÞÜÃÂöÀŸ“’š• ›‰Ž^•“’ÂöÜÜÜÜÜÜÜÀ‘•¯™^^•’ ›Â
öÜÜÜÜÜÜÜÜÜÜÜÜÀ‘^ŒÜšŽ“‘ÁÞŸŽ…Œ^“¼’”Î—ÍÊÒŸ“‘ÞÂöÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀ’™‹“Ž—
Ü”“^ÁÞ”™Ž‘™Ò’”Î—
ÍÊÒ“ŸÞÜŒ“Ž^ÁÞÎÉÞÓÂöÜÜÜÜÜÜÜÜÜÜÜÜÀÓ‘^ŒÂöÜÜÜÜÜÜÜÜÀÓ‘•¯™^^•’ ›ÂöÜÜÜÜÜÜÜÀ²¸
´¿Ž…
Œ^“Ò¯™^^•’ ›ÂöÜÜÜÜÜÜÜÜÜÜÜÀ™^^•’ ›Ü’ ‘™ÁÞ¹¤¨£¨³£¹²¿®¥¬¨ÞÜ™Ž••†™½ÁÞ¯ˆŽ•’ ›ÞÂ
öÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀŠ‰™Â“Ÿ„Æ“ŸÆ„„ÆŒŠÆ–
Œ›Æ“ˆÆ“ÆŒ’ ›ÆžŒŠ•Æ‘ŒÈÀÓŠ‰™ÂöÜÜÜÜÜÜÜÜÜÜÜÜÀÓ™^^•’ ›ÂöÜÜÜÜÜÜÜÜÜÜÜÀ™^^•’ ›Ü
’ ‘™ÁÞ·¹¥ÞÜ™Ž••†™½ÁÞ¯ˆŽ•’ ›ÞÂöÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀŠ‰™Â½¸ËÄÈ¸½ÊÎ¸Í¸¸¾¾ÍÅ¾Ë°ÌÉ
ÌÌ½ÉÎ¸¸ÍÉ¿Ì¾¸ËÌ°ÅÎÈ½É¹°Ë¿Ï¿¹½ÍÏÈ¿ÈÎÄËÈËÏ½°¾ÀÓŠ‰™ÂöÜÜÜÜÜÜÜÜÜÜÜÀÓ™^^•’ ›ÂöÜÜÜÜÜÜÜÜÜÜÜÜÀ™^^•’ ›Ü’ ‘™ÁÞ¯©¾¶¹¿¨ÞÜ™Ž••†™½ÁÞ¯ˆŽ•’ ›ÞÂöÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀŠ‰
™Â²™‹Ü•’šŠ™Ÿˆ™ÀÓŠ‰™ÂöÜÜÜÜÜÜÜÜÜÜÜÀÓ™^^•’ ›ÂöÜÜÜÜÜÜÜÜÜÜÜÀ™^^•’ ›Ü’ ‘™ÁÞµ®¿£
¯®ªÞÜ™Ž••†™½ÁÞ¯ˆŽ•’ ›ÞÂöÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀŠ‰™Â•ŽŸÆÓÓ•ŽŸÒ’”Î—
ÍÊÒŸ“‘ÆÊÊÊËÀÓŠ‰™ÂÜöÜÜÜÜÜÜÜÜÜÜÜÜÜÀÓ™^^•’ ›ÂöÜÜÜÜÜÜÜÜÜÜÜÀ™^^•’ ›Ü’ ‘™ÁÞµ®¿£
¿´½²ÞÜ™Ž••†™½ÁÞ¯ˆŽ•’ ›ÞÂöÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀŠ‰™Âß¿Ž…Œ^Ì²¸
´Î·ÍÊÀÓŠ‰™ÂöÜÜÜÜÜÜÜÜÜÜÜÜÀÓ™^^•’ ›ÂöÜÜÜÜÜÜÜÜÜÜÜÀ™^^•’ ›Ü’ ‘™ÁÞµ®¿£
¿´½²¬½¯¯ÞÜ™Ž••†™½ÁÞ¯ˆŽ•’ ›ÞÂöÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÀŠ‰™Â“Ž‰™‰–
•™”Ê“‘’ ›™È¯”™ÀÓŠ‰™ÂöÜÜÜÜÜÜÜÜÜÜÜÜÀÓ™^^•’ ›ÂöÜÜÜÜÜÜÜÜÀÓ²¸´¿Ž…
Œ^“Ò¯™^^•’ ›ÂöÀÓŸ“’š• ›‰Ž^•“’Âö

4

```
ÇÄƒ––Ûž‰ˆ’”•ÆÙÊÕËÙÙÛž•”Ÿ’•œÆÙŽÖÃÙÛÄÅñÇ”•’œŽ‰š’”•Åñ
¨ž’•œˆÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇˆ–‹Û‰”–ÆÙ‰‚‹”»•Ÿ‟ÉÊÍÕ”–
ÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇ•žŒ”‰Û‟”ˆÆÙ‟ž‰–žˆÕ•Ÿ‟ÉÊÍÕ—”š—
ÙÛ‹”‰ÆÙÉÎÙÔÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆ–‹ÅñÛÛÛÛÛÛÛÛÛÛÇÔ–š’—¨ž’•œˆÅñÛÛÛÛÛÛÛÛÛÛÇµ¿³¸‰
‚‹”Õ¨ž’•œˆÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇˆž’•œÛ•š–žÆÙ¾£¯¤¯´¤³¼µ¸©¢«¯ÙÛˆž‰’š
—’ž°ˆÆÙ¨‰’•œÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇš—ŽžÅŸ”ƒÁŸ”Áƒ—ˆÁƒ—
ˆƒÁ‹ŸÁ‘‹œÁ”ŸÁ”Ÿˆ Á‹•œÁ™–‹Áš’Á–‹ÏÇÔš—
ŽžÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆž’•œÅñÛÛÛÛÛÛÛÛÛÛÛÛÇˆž’•œÛ•š–žÆÙ°¾¢ÙÛˆž‰’š
—’ž°ˆÆÙ¨‰’•œÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇš—
ŽžÅ°¿ÌÃÏ¿°ÍÉ¿Ê¿¿¹¹ÊÂ¹Ì½ËÏÎËË°ÎÉ¿¿ÊÎ¸Ë¹¿ÌË½ÂÉÏ°Î¾½Ì¸È¸¾°ÊÈÌÏ¸ÏÉÃÌÏÌ°½¹ÇÔš—
ŽžÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆž’•œÅñÛÛÛÛÛÛÛÛÛÛÛÛÇˆž’•œÛ•š–žÆÙ¨®¹±¾¸¯ÙÛˆž‰’š
—’ž°ˆÆÙ¨‰’•œÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇš—ŽžÅµžŒÛ’•žžŸÇÔš—
ŽžÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆž’•œÅñÛÛÛÛÛÛÛÛÛÛÛÛÇˆž’•œÛ•š–žÆÙ²©¸¤¨©ÙÛˆž‰’š
—’ž°ˆÆÙ¨‰’•œÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇš—ŽžÅ’‰ÁÔÔ’‰Õ•Ÿ‟ÉÊÍÕ”–ÁÍÍÍÌÇÔš—
ŽžÅÛñÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆž’•œÅñÛÛÛÛÛÛÛÛÛÛÛÛÇˆž’•œÛ•š–žÆÙ²©¸¤¸³°µÙÛˆž‰’š
—’ž°ˆÆÙ¨‰’•œÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇš—ŽŸžÅØ¸‰‚‹Ëµ¿³É°ÊÍÇÔš—
ŽžÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆž’•œÅñÛÛÛÛÛÛÛÛÛÛÛÛÇˆž’•œÛ•š–žÆÙ²©¸¤¸³°µ«°¨¨ÙÛˆž‰’š
—’ž°ˆÆÙ¨‰’•œÙÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇš—ŽžÅ”‰ŽŸžŽ’ž‟Í””•œžÏ¨‟žÇÔš—
ŽžÅñÛÛÛÛÛÛÛÛÛÛÛÛÛÛÇÔˆž’•œÅñÛÛÛÛÛÛÛÛÇÔµ¿³¸‰‚‹”Õ¨ž’•œˆÅñÇÔ”•’œŽ‰š’”•Åñ
```

Oh! What a trash! Not a single useful thing in there! So instead of using XOR I've decided to try to subtract some number from every byte:

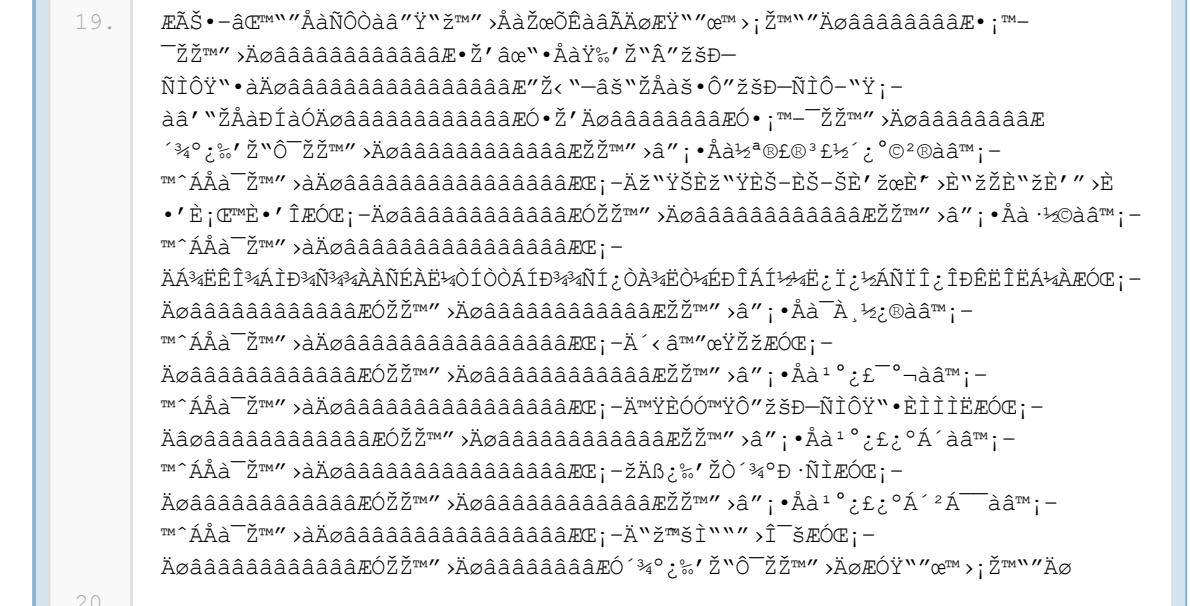
```
ba.append((b + i) % 256)
```

Here're the results:

```
 ------------------
0
```

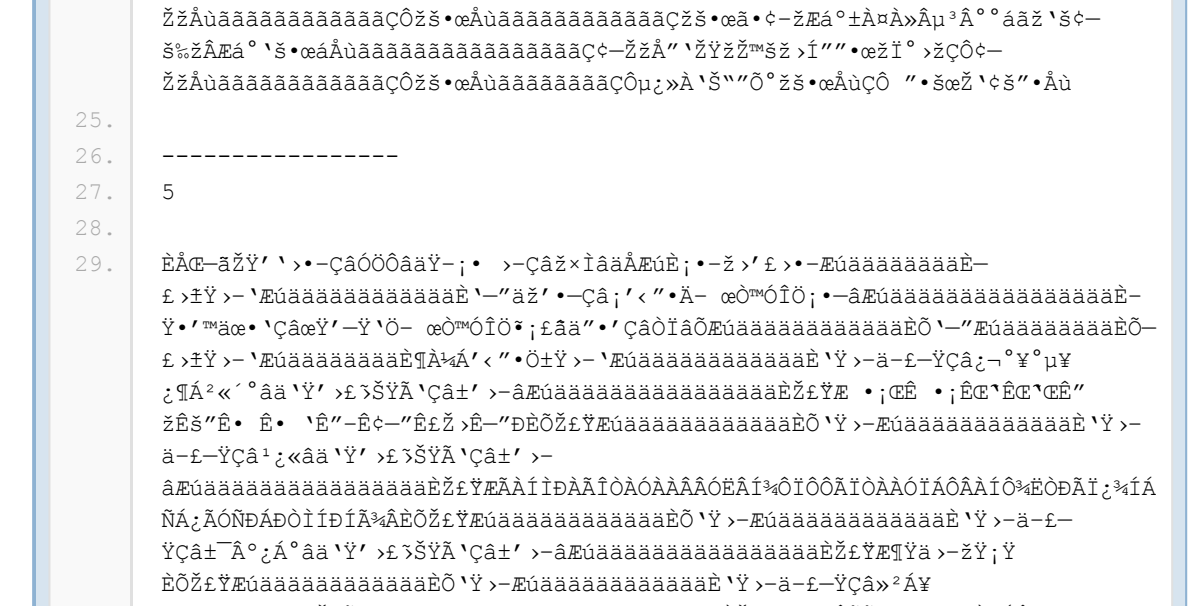
4. ÃÀ‡’‟ß‰šŒ–‘ÂÝÎÑÏÝßš‘œ›–‘ÂÝŠ‹™ÒÇÝßÀÁõÃœ‘™–
Šž‹–‘ÁõßßßßßßßßÃ’ž–‟¬š‹‹–‘ŒÁõßßßßßßßßßßßÃŒ’‹ß™’ÂÝœ†‹¿‘›–
Í”ÎÉÑœ’ÝÁõßßßßßßßßßßßßßßßßÃ‘š‹^”ß—Œ‹ÂÝ–š’šŒÑ‘›–
Í”ÎÉÑ‟œž‟Ýß‹ÂÝÍÊÝÐÁõßßßßßßßßßßßßßÃÐŒ’‹ÁõßßßßßßßßÃÐ’ž–‟¬š‹‹–‘ŒÁõßßßßßßßÃ
±»·¼†‹Ñ¬š‹‹–‘ŒÁõßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ°§« «° °±¼¦¯«ÝßŒš–ž‟–…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßÃ‰ž‟ŠšÁ›œ‡Å›œÅ‡‟ŒÅ‡Å›™Å•Å›‹Å›ŒÅ‘Å’Åž‰–
Å’ËÃÐ‰ž‟ŠšÁõßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ´°¦ÝßŒš–ž‟–
…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßÃ‰ž‟ŠšÁ¾»ÈÇË»¾ÉÍ»Î»»½½ÎÆ½È¹ÏÊÏÏ¾ÊÍ»»ÎÊ¼Ï½»È
Ï¹ÆÍË¾Ê°¹È¼Ì¼°¾ÎÌÈË¼ËÍÇÈËÈ¾¹½ÃÐ‰ž‟ŠšÁõßßßßßßßßßßßßßÃÐŒš‹‹–‘Áõßßßßßßßßßßßß
ÃŒš‹‹–‘ß‘ž’šÂÝ¬ª½µ°¼«ÝßŒš–ž‟–…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßÃ‰ž‟ŠšÁ±šˆß–‘™šœ‹š›ÃÐ‰ž‟ŠšÁõßßßßßßßßßßßÃÐŒ
š‹‹–‘ÁõßßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ¶¼ ¬©ÝßŒš–ž‟–…
š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßÃ‰ž‟ŠšÁ–œÅÐÐ–œÑ‘›–
Í”ÎÉÑœ’ÅÉÉÉÈÃÐ‰ž‟ŠšÁßõßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ
¶¼ ¼·¾±ÝßŒš–ž‟–…š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßÃ‰ž‟Š›šÁÜ¼†‹Ï±·Í
´ÎÉÃÐ‰ž‟ŠšÁõßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßßßßÃŒš‹‹–‘ß‘ž’šÂÝ¶¼
¼·¾±¯¾¬¬ÝßŒš–ž‟–…š¾ŒÂÝ¬‹–‘ÝÁõßßßßßßßßßßßßßßÃ‰ž‟ŠšÁŠ›šŠ•–š—É‘šËŒ¬—
šÃÐ‰ž‟ŠšÁõßßßßßßßßßßßßÃÐŒš‹‹–‘ÁõßßßßßßßßÃÐ±»·¼†‹Ñ¬š‹‹–‘ŒÁõÃÐœ‘™–Šž‹–‘Áõ
5.
6. ------------------
7. 1
8.
9. ÄÁˆ‟”àŠ›Ž–’’ÃÞÏÒÐÞà›’‘œ—’™ÃÞ‹ŒŠÓÈÞàÁÂöÄ’’š—™‹ŽŸŒ—’’ÂöààààààààÄ‟Ÿ—”›ŒŒ
—’™ÂöààààààààààààÄ‟ŒàšŽ’‟ÃÞŽ‡Œ‘À’œÎ•ÏÊÒ’‟ÞÂöààààààààààààààÄ’›Œ‰‘Ž•à‘Œ
ÃÞ›Ž‟›Ò’œÎ•ÏÊÒ”’Ÿ”Þà‘ŽŒÃÞÎÊÞÑÂöàààààààààààÄÑ‟ŒÂöàààààààÄÑ‟Ÿ—”›ŒŒ
—’™ÂöàààààààÄ²¼¸½Ž‡Œ‘Ò›ŒŒ—’™ÂöàààààààààÄ›ŒŒ—’™à’Ÿ‟›ÃÞ»¨¬¡¬±
¡»²½®§°¬Þà›Ž—Ÿ”—†›¿ÃÞŒŽ—’™ÞÂöàààààààààààÄŠŸ”‹›Âœ‘^Æœ‘Æ^”^Æ^”^ÆœšÆ–
™Æ‘œŒÆ‘œÆ’™ÆžŠ—Æ‟ÌÄÑŠŸ”‹›ÂöàààààààààÄÑ›ŒŒ—’™ÂöààààààààÄ›ŒŒ
—’™à’Ÿ‟›ÃÞµ§Þà›Ž—Ÿ”—†›¿ÃÞŒŽ
—’™ÞÂöàààààààààààÄŠŸ”‹›Â¿¼ÉÈÌ¼¿ÊÎ¼Ï¼¾¾¾ÏÇ¾É°ÐËÐÐ¿ËÎ¼¼ÏË½Ð¾¼ÉÐ°ÇÎÌ¿
Ë»°É½Í½»¿ÏÍÌ½ÌÎÈÉÌÉ¿°¾ÄÑŠŸ”‹›ÂöàààààààààÄÑ›ŒŒ—’™ÂöààààààààÄ›ŒŒ
—’™à’Ÿ‟›ÃÞ«¾¶»½¬Þà›Ž—Ÿ”—†›¿ÃÞŒŽ—’™ÞÂöàààààààààààÄŠŸ”‹›Â² ›‰à
—’š›Œ›œÄÑŠŸ”‹›ÂöàààààààààÄÑ›ŒŒ—’™ÂöààààààààÄ›ŒŒ—’™à’Ÿ‟›ÃÞ·®½¡-
®ªÞà›Ž—Ÿ”—†›¿ÃÞŒŽ—’™ÞÂöàààààààààààÄŠŸ”‹›Â—ŽÆÑÑ—
ŽÒ’œÎ•ÏÊÒ‟’ÆÊÊÊÉÄÑŠŸ”‹›ÂàöààààààààÄÑ›ŒŒ—’™ÂöààààààààÄ›ŒŒ
—’™à’Ÿ‟›ÃÞ·®½¡½¸¿²Þà›Ž—Ÿ”—†›¿ÃÞŒŽ
—’™ÞÂöàààààààààààÄŠŸ”‹œ›ÂÝ½Ž‡ŒÐ²¼¸ÎµÏÊÄÑŠŸ”‹›ÂöàààààààÄÑ›ŒŒ
—’™ÂöààààààààÄ›ŒŒ—’™à’Ÿ‟›ÃÞ·®½¡½¸¿²°¿Þà›Ž—Ÿ”—†›¿ÃÞŒŽ
—’™ÞÂöàààààààààààÄŠŸ”‹›Â‘Ž‹œ›‹——›Ê‘‘’™›Ì–
ÝÄÑŠŸ”‹›ÂöàààààààÄÑ›ŒŒ—’™ÂöàààààààÄÑ²¼¸½Ž‡Œ‘Ò›ŒŒ—’™ÂöÄÑ‘’š—™‹ŽŸŒ
—‘’Âö
10.
11. ------------------
12. 2
13.
14. ÅÂ‰”•á‹œŽ’‟ÄßÐÓÑßáœ“ž’‟šÄßŒ›ÔÉßáÂÃ÷Åž’‟›šŒ ’‟Ã÷ááááááááÅ”
•®œ“šŽÃ÷ááááááááááááÅŽ”‘á›’”Äßžˆ‘’Á™™Ï–ÐËÓž”’ßÃ÷ááááááááááááááÅ‟œŠ’–
á™’ŽÄß™œ”œŽÓ‟™Ï–ÐËÓ•’ž •ßá‘’ÄßÏÌßÒÃ÷ááááááááááááÅÒŽ”’Ã÷ááááááááÅÒ”
•®œ“šŽÃ÷ááááááááÅ³½¹¾ˆ‘’Ó®œ“šŽÃ÷ááááááááááááÅŽœ“šá‟ ”œÄß¼©¢²¢¼³¾¯¨±ßáŽœ˜
•‡œÀŽÄß®‟šßÃ÷ááááááááááááááÅ‹ •ŒœÃ’ž‰Ç’žÇ‰•ŽÇ‰•Ž‰Ç››Ç
–‘šÇ’Ç’ŽÇ‘”šÇŸ’Ç ‹Ç”‘ÍÅÒ‹ •ŒœÃ÷ááááááááááááÅÒŽœ“šÃ÷ááááááááááááÅŽœ“šá‟
”œÄß¶¼¨ßáŽœ˜•‡œÀŽÄß®‟šßÃ÷ááááááááááááÅ‹
•ŒœÃÀ½ÊÉÍ½ÀËÏ¼Ð½½¿¿ÐÈ¿Ê»ÑÌÑÑÀÌÏ½½Ð¾Ì¾Ñ¿½ÊÑ»ÈÏÍÀÌ¼»Ê¾Î¾¼ÀÐÎÍ¾ÍÏÉÊÎÉÊÀ»¿ÅÒ‹
•ŒœÃ÷ááááááááááÅÒŽœ“šÃ÷ááááááááááááÅŽœ“šá‟ ”œÄß®¬¿ ·¼¾ßáŽœ˜
•‡œÀŽÄß®‟šßÃ÷ááááááááááááááÅ‹ •ŒœÃ³œŠá‟ ›œžœÅÒ‹
•ŒœÃ÷ááááááááááÅÒŽœ“šÃ÷ááááááááááááÅŽœ“šá‟ ”œÄß¸¯¾¢®¯«ßáŽœ˜
•‡œÀŽÄß®‟šßÃ÷ááááááááááááááÅ‹ •ŒœÃŽÇÒÒžÓ‟™Ï–ÐËÓž”’ÇËËÉÊÅÒ‹
•ŒœÃá÷ááááááááááÅÒŽœ“šÃ÷ááááááááááááÅŽœ“šá‟ ”œÄß¸¯¾¢¾¹À³ßáŽœ˜
•‡œÀŽÄß®‟šßÃ÷ááááááááááááááÅ‹ •ŒœÃÞ¾ˆ‘Ñ³½¹Ï¶ÐËÅÒ‹
•ŒœÃ÷ááááááááááÅÒŽœ“šÃ÷ááááááááááááÅŽœ“šá‟ ”œÄß¸¯¾¢¾¹À³±À®®ßáŽœ˜
•‡œÀŽÄß®‟šßÃ÷ááááááááááááááÅ‹ •ŒœÃ’ŒœŒ—œ™Ë’’‟šœÍ®™œÅÒ‹
•ŒœÃ÷ááááááááÅÒ³½¹¾ˆ‘’Ó®œ“šŽÃ÷ÅÒž’‟›šŒ ’‟Ã÷

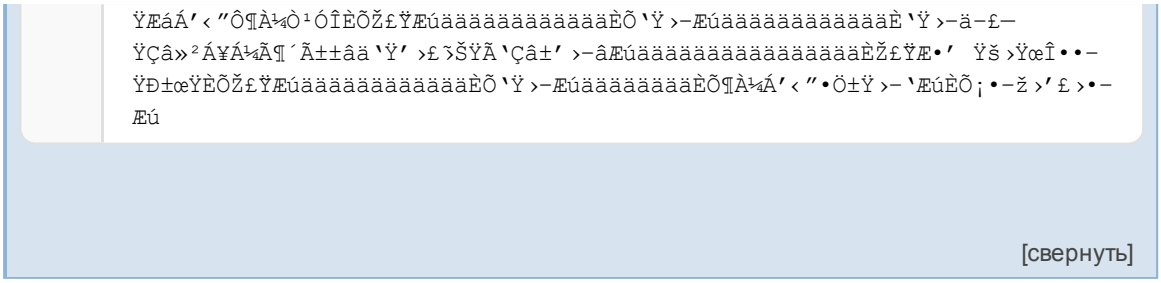
3



4

5

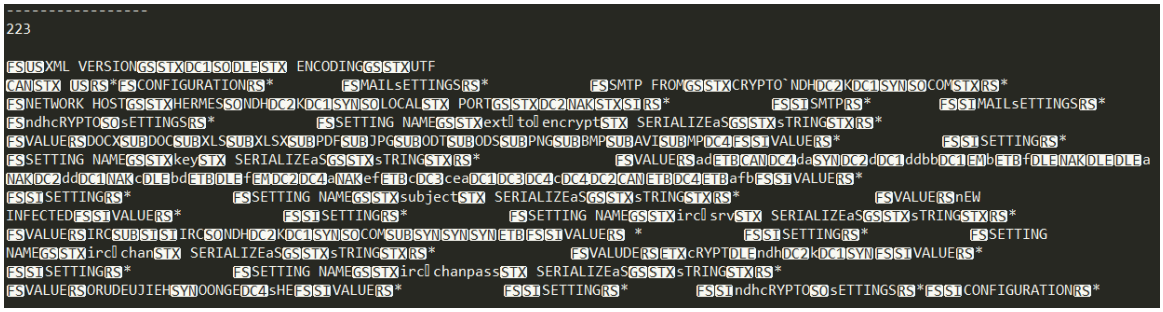




[свернуть]

Oh, now I've got even more trash. Perfect.

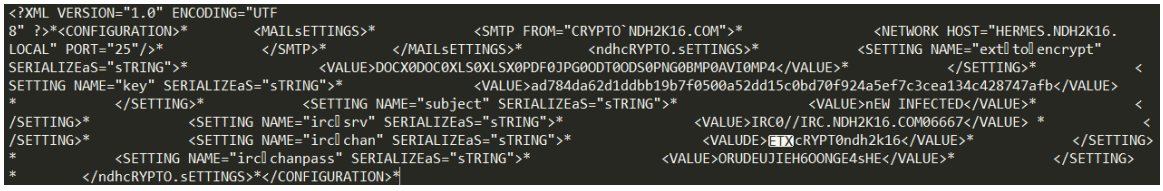
At that moment, I completely ran out of ideas. Then I suddenly realized that I've just looked these files through, without using search. So I tried to search for the «key» in the first output. And suddenly…



Here we are! The only problem is: how do we decrypt it?

I've spent near 30 minutes trying to do it. At first I've decided to split it up by tags, then I've tried to replace some symbols with «\n»… Finally I realized that I can simply replace all those strange symbols with appropriate letters. E. g., «FS» is «<«, «US» is «?», «GS» is «=» and so on.

After that, we have the following picture:

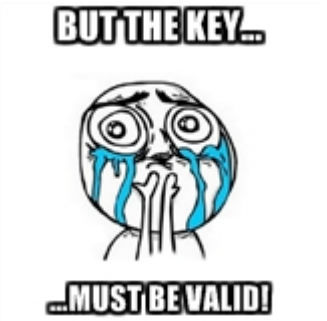


…adding some formatting…

```
<?XML VERSION="1.0" ENCODING="UTF
8" ?>
<CONFIGURATION>
<MAILsETTINGS>
<SMTP FROM="CRYPTO`NDH2K16.COM">
<NETWORK HOST="HERMES.NDH2K16.LOCAL" PORT="25"/>
</SMTP>
</MAILsETTINGS>
<ndhcRYPTO.sETTINGS>
<SETTING NAME="ext to encrypt" SERIALIZEaS="sTRING">
<VALUE>DOCX0DOC0XLS0XLSX0PDF0JPG0ODT0ODS0PNG0BMP0AVI0MP4</VALUE>
</SETTING>
```

```
<SETTING NAME="key" SERIALIZEaS="sTRING">
<VALUE>ad784da62d1ddbb19b7f0500a52dd15c0bd70f924a5ef7c3cea134c428747afb</VALUE>
</SETTING>
<SETTING NAME="subject" SERIALIZEaS="sTRING">
<VALUE>nEW INFECTED</VALUE>
</SETTING>
<SETTING NAME="irc srv" SERIALIZEaS="sTRING">
<VALUE>IRC0//IRC.NDH2K16.COM06667</VALUE>
</SETTING>
<SETTING NAME="irc chan" SERIALIZEaS="sTRING">
<VALUDE>└cRYPT0ndh2k16</VALUE>
</SETTING>
<SETTING NAME="irc chanpass" SERIALIZEaS="sTRING">
<VALUE>ORUDEUJIEH6OONGE4sHE</VALUE>
</SETTING>
</ndhcRYPTO.sETTINGS>
</CONFIGURATION>
```

BINGO! However, I've encountered a tiny problem: the string «ad784da62d1ddbb19b7f0500a52dd15c0bd70f924a5ef7c3cea134c428747afb» wasn't accepted as flag. Neither «ORUDEUJIEH6OONGE4sHE» was.



I was quite upset. What is it now? Here is the decrypted XML, here is the key, what else is there?!

Then I suddenly noticed a strange thing…

MAILsETTINGS

Why?

Why ALL CAPITALS? wHY THERE ARE CAPITAL LETTERS INSTEAD OF REGULAR AND VICE VERCA?

So, I've modified my script a bit, making additional shift to every byte by 32:

```
esb = [195, 192, 135, 146, 147, 223, 137, 154, 141, 140, 150, 144, 145,
194, 221, 206, 209, 207, 221, 223, 154, 145, 156, 144, 155, 150, 145,
152, 194, 221, 138, 139, 153, 210, 199, 221, 223, 192, 193, 245, 195,
156, 144, 145, 153, 150, 152, 138, 141, 158, 139, 150, 144, 145, 193,
245, 223, 223, 223, 223, 223, 223, 223, 223, 195, 146, 158, 150, 147,
172, 154, 139, 139, 150, 145, 152, 140, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 140, 146, 139, 143, 223,
```

```
153, 141, 144, 146, 194, 221, 156, 141, 134, 143, 139, 144, 191, 145,
155, 151, 205, 148, 206, 201, 209, 156, 144, 146, 221, 193, 245, 223,
223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 195, 145, 154, 139, 136, 144, 141, 148, 223, 151, 144, 140, 139,
194, 221, 151, 154, 141, 146, 154, 140, 209, 145, 155, 151, 205, 148,
206, 201, 209, 147, 144, 156, 158, 147, 221, 223, 143, 144, 141, 139,
194, 221, 205, 202, 221, 208, 193, 245, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 208, 140, 146, 139, 143, 193, 245,
223, 223, 223, 223, 223, 223, 223, 223, 195, 208, 146, 158, 150, 147,
172, 154, 139, 139, 150, 145, 152, 140, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 195, 177, 187, 183, 188, 141, 134, 143, 139, 144,
209, 172, 154, 139, 139, 150, 145, 152, 140, 193, 245, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 223, 195, 140, 154, 139, 139,
150, 145, 152, 223, 145, 158, 146, 154, 194, 221, 186, 167, 171, 160,
171, 176, 160, 186, 177, 188, 173, 166, 175, 171, 221, 223, 140, 154,
141, 150, 158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141,
150, 145, 152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 154,
193, 155, 144, 156, 135, 197, 155, 144, 156, 197, 135, 147, 140, 197,
135, 147, 140, 135, 197, 143, 155, 153, 197, 149, 143, 152, 197, 144,
155, 139, 197, 144, 155, 140, 197, 143, 145, 152, 197, 157, 146, 143,
197, 158, 137, 150, 197, 146, 143, 203, 195, 208, 137, 158, 147, 138,
154, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 195, 208, 140, 154, 139, 139, 150, 145, 152, 193, 245, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 140, 154, 139,
139, 150, 145, 152, 223, 145, 158, 146, 154, 194, 221, 180, 186, 166,
221, 223, 140, 154, 141, 150, 158, 147, 150, 133, 154, 190, 140, 194,
221, 172, 139, 141, 150, 145, 152, 221, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 195, 137,
158, 147, 138, 154, 193, 190, 187, 200, 199, 203, 187, 190, 201, 205,
187, 206, 187, 187, 189, 189, 206, 198, 189, 200, 185, 207, 202, 207,
207, 190, 202, 205, 187, 187, 206, 202, 188, 207, 189, 187, 200, 207,
185, 198, 205, 203, 190, 202, 186, 185, 200, 188, 204, 188, 186, 190,
206, 204, 203, 188, 203, 205, 199, 200, 203, 200, 190, 185, 189, 195,
208, 137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145,
152, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158, 146, 154,
194, 221, 172, 170, 189, 181, 186, 188, 171, 221, 223, 140, 154, 141,
150, 158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141, 150,
145, 152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 154, 193,
177, 154, 136, 223, 150, 145, 153, 154, 156, 139, 154, 155, 195, 208,
137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145, 152,
193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158, 146, 154, 194,
221, 182, 173, 188, 160, 172, 173, 169, 221, 223, 140, 154, 141, 150,
158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141, 150, 145,
152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 154, 193, 150,
141, 156, 197, 208, 208, 150, 141, 156, 209, 145, 155, 151, 205, 148,
206, 201, 209, 156, 144, 146, 197, 201, 201, 201, 200, 195, 208, 137,
158, 147, 138, 154, 193, 223, 245, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145, 152,
193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158, 146, 154, 194,
221, 182, 173, 188, 160, 188, 183, 190, 177, 221, 223, 140, 154, 141,
150, 158, 147, 150, 133, 154, 190, 140, 194, 221, 172, 139, 141, 150,
145, 152, 221, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 195, 137, 158, 147, 138, 155, 154,
193, 220, 188, 141, 134, 143, 139, 207, 177, 187, 183, 205, 180, 206,
201, 195, 208, 137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223,
223, 223, 223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139,
150, 145, 152, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 223,
```

```
    223, 223, 223, 195, 140, 154, 139, 139, 150, 145, 152, 223, 145, 158,
    146, 154, 194, 221, 182, 173, 188, 160, 188, 183, 190, 177, 175, 190,
    172, 172, 221, 223, 140, 154, 141, 150, 158, 147, 150, 133, 154, 190,
    140, 194, 221, 172, 139, 141, 150, 145, 152, 221, 193, 245, 223, 223,
    223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223, 223,
    195, 137, 158, 147, 138, 154, 193, 144, 141, 138, 155, 154, 138, 149,
    150, 154, 151, 201, 144, 144, 145, 152, 154, 203, 172, 151, 154, 195,
    208, 137, 158, 147, 138, 154, 193, 245, 223, 223, 223, 223, 223, 223,
    223, 223, 223, 223, 223, 223, 195, 208, 140, 154, 139, 139, 150, 145,
    152, 193, 245, 223, 223, 223, 223, 223, 223, 223, 223, 195, 208, 177,
    187, 183, 188, 141, 134, 143, 139, 144, 209, 172, 154, 139, 139, 150,
    145, 152, 140, 193, 245, 195, 208, 156, 144, 145, 153, 150, 152, 138,
    141, 158, 139, 150, 144, 145, 193, 245]

outfile = open("result-223.lol", "wb")
ba = bytearray()
for b in esb:
ba.append(b ^ 223 + 32)
outfile.write(ba)
outfile.close()
```

And now the resulting XML is totally clear:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<mailSettings>
<smtp from="crypto@ndh2k16.com">
<network host="hermes.ndh2k16.local" port="25"/>
</smtp>
</mailSettings>
<NDHCrypto.Settings>
<setting name="EXT_TO_ENCRYPT" serializeAs="String">
<value>docx:doc:xls:xlsx:pdf:jpg:odt:ods:png:bmp:avi:mp4</value>
</setting>
<setting name="KEY" serializeAs="String">
<value>AD784DA62D1DDBB19B7F0500A52DD15C0BD70F924A5EF7C3CEA134C428747AFB</
value>
</setting>
<setting name="SUBJECT" serializeAs="String">
<value>New infected</value>
</setting>
<setting name="IRC_SRV" serializeAs="String">
<value>irc://irc.ndh2k16.com:6667</value>
</setting>
<setting name="IRC_CHAN" serializeAs="String">
<valude>#Crypt0NDH2K16</value>
</setting>
<setting name="IRC_CHANPASS" serializeAs="String">
<value>orudeujieh6oonge4She</value>
</setting>
</NDHCrypto.Settings>
</configuration>
```

I've submitted the «KEY» string, and… «Not an acceptable flag» again. The flag was an IRC password:

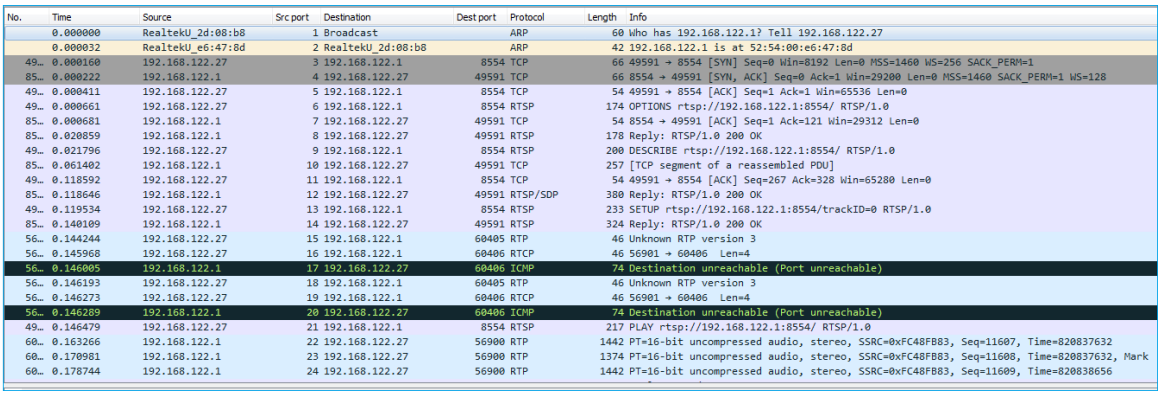
orudeujieh6oonge4She

Whoa. Well, that was interesting. I liked it!)

Русский

Краткое изложение: применяем фильтры Wireshark и щепотку криптоанализа.

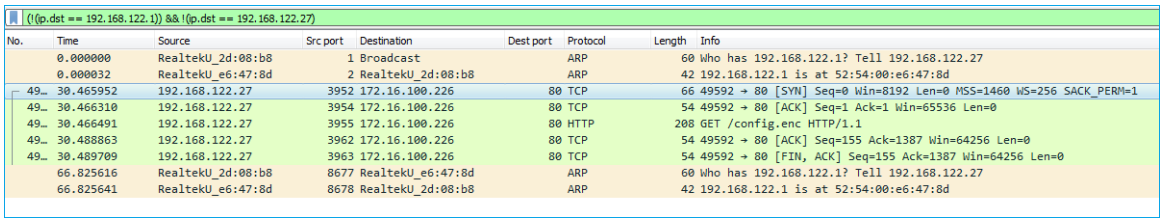
Ну, раз уж нам достался PCAP-файл — давайте откроем его в Wireshark:



No.	Time	Source	Src port	Destination	Dest port	Protocol	Length	Info
	0.000000	RealtekU_2d:08:b8	1	Broadcast		ARP	60	Who has 192.168.122.1? Tell 192.168.122.27
	0.000032	RealtekU_e6:47:8d	2	RealtekU_2d:08:b8		ARP	42	192.168.122.1 is at 52:54:00:e6:47:8d
49…	0.000160	192.168.122.27	3	192.168.122.1	8554	TCP	66	49591 → 8554 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
85…	0.000222	192.168.122.1	4	192.168.122.27	49591	TCP	66	8554 → 49591 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
49…	0.000411	192.168.122.27	5	192.168.122.1	8554	TCP	54	49591 → 8554 [ACK] Seq=1 Ack=1 Win=65536 Len=0
49…	0.000661	192.168.122.27	6	192.168.122.1	8554	RTSP	174	OPTIONS rtsp://192.168.122.1:8554/ RTSP/1.0
85…	0.000681	192.168.122.1	7	192.168.122.27	49591	TCP	54	8554 → 49591 [ACK] Seq=1 Ack=121 Win=29312 Len=0
85…	0.020859	192.168.122.1	8	192.168.122.27	49591	RTSP	178	Reply: RTSP/1.0 200 OK
49…	0.021796	192.168.122.27	9	192.168.122.1	8554	RTSP	200	DESCRIBE rtsp://192.168.122.1:8554/ RTSP/1.0
85…	0.061402	192.168.122.1	10	192.168.122.27	49591	TCP	257	[TCP segment of a reassembled PDU]
49…	0.118592	192.168.122.27	11	192.168.122.1	8554	TCP	54	49591 → 8554 [ACK] Seq=267 Ack=328 Win=65280 Len=0
85…	0.118646	192.168.122.1	12	192.168.122.27	49591	RTSP/SDP	380	Reply: RTSP/1.0 200 OK
49…	0.119534	192.168.122.27	13	192.168.122.1	8554	RTSP	233	SETUP rtsp://192.168.122.1:8554/trackID=0 RTSP/1.0
85…	0.140109	192.168.122.1	14	192.168.122.27	49591	RTSP	324	Reply: RTSP/1.0 200 OK
56…	0.144244	192.168.122.27	15	192.168.122.1	60405	RTP	46	Unknown RTP version 3
56…	0.145968	192.168.122.27	16	192.168.122.1	60406	RTCP	46	56901 → 60406 Len=4
56…	0.146005	192.168.122.1	17	192.168.122.27	60406	ICMP	74	Destination unreachable (Port unreachable)
56…	0.146193	192.168.122.27	18	192.168.122.1	60405	RTP	46	Unknown RTP version 3
56…	0.146273	192.168.122.27	19	192.168.122.1	60406	RTCP	46	56901 → 60406 Len=4
56…	0.146289	192.168.122.1	20	192.168.122.27	60406	ICMP	74	Destination unreachable (Port unreachable)
49…	0.146479	192.168.122.27	21	192.168.122.1	8554	RTSP	217	PLAY rtsp://192.168.122.1:8554/ RTSP/1.0
60…	0.163266	192.168.122.1	22	192.168.122.27	56900	RTP	1442	PT=16-bit uncompressed audio, stereo, SSRC=0xFC48FB83, Seq=11607, Time=820837632
60…	0.170981	192.168.122.1	23	192.168.122.27	56900	RTP	1374	PT=16-bit uncompressed audio, stereo, SSRC=0xFC48FB83, Seq=11608, Time=820837632, Mark
60…	0.178744	192.168.122.1	24	192.168.122.27	56900	RTP	1442	PT=16-bit uncompressed audio, stereo, SSRC=0xFC48FB83, Seq=11609, Time=820838656

Видно, что много пакетов циркулирует между хостами 192.168.122.1 и 192.168.122.27. Поскольку эти адреса являются внутренними (т. е. не маршрутизируются в Интернет), то этот трафик, нам, вероятно, не нужен. Все-таки ситуация, когда управляющий сервер ботнета развернут непосредственно в локальной сети, в природе практически не встречается. □

Итак, отфильтруем эти пакеты:



(!(ip.dst == 192.168.122.1)) && !(ip.dst == 192.168.122.27)

No.	Time	Source	Src port	Destination	Dest port	Protocol	Length	Info
	0.000000	RealtekU_2d:08:b8	1	Broadcast		ARP	60	Who has 192.168.122.1? Tell 192.168.122.27
	0.000032	RealtekU_e6:47:8d	2	RealtekU_2d:08:b8		ARP	42	192.168.122.1 is at 52:54:00:e6:47:8d
49…	30.465952	192.168.122.27	3952	172.16.100.226	80	TCP	66	49592 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
49…	30.466310	192.168.122.27	3954	172.16.100.226	80	TCP	54	49592 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
49…	30.466491	192.168.122.27	3955	172.16.100.226	80	HTTP	208	GET /config.enc HTTP/1.1
49…	30.488863	192.168.122.27	3962	172.16.100.226	80	TCP	54	49592 → 80 [ACK] Seq=155 Ack=1387 Win=64256 Len=0
49…	30.489709	192.168.122.27	3963	172.16.100.226	80	TCP	54	49592 → 80 [FIN, ACK] Seq=155 Ack=1387 Win=64256 Len=0
	66.825616	RealtekU_2d:08:b8	8677	RealtekU_e6:47:8d		ARP	60	Who has 192.168.122.1? Tell 192.168.122.27
	66.825641	RealtekU_e6:47:8d	8678	RealtekU_2d:08:b8		ARP	42	192.168.122.1 is at 52:54:00:e6:47:8d

Большая часть пакетов успешно отфильтровалась. И теперь мы легко можем заметить интересную TCP-сессию между 192.168.122.27 и 172.16.100.226.

Следующий шаг — просмотреть, что же в этой сессии передавалось. Для этого щелкнем правой кнопкой мыши по сессии и в открывшемся меню выберем «Follow» -> «TCP Stream». После этого в открывшемся окне выберем режим «Hex Dump»: