

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

HOST INFORMATION:

IP address: 192.168.1.43
Host name: Workshopper-PC
MAC address: 18:03:73:67:fb:8c (Dell_67:fb:8c)

MALWARE:

C:\Users\granny.hightower\Downloads\Boleto_Bancariold3005201612.exe

SOURCE:

Malspam at 2016-06-01 at 1748 UTC (email: 2016-06-01-1748-UTC.eml) with a Google Drive link.

MALWARE:

C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytgcy\lytg.dll
C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytgcy\lytgc.exe
C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytgcy\lytgc32.dll

SOURCE:

Delivered by Rig exploit kit (EK) on 46.30.47.17 (domain: ef.crazyballoon.org) triggered after viewing a compromised website at
http://www.curetoothdecay.com/Tooth_Decay/foods_promote_decay.htm

DETAILS

NOTE: I always recommend chaning the default column display in Wireshark before you review the exercise pcaps. More information at:

<http://malware-traffic-analysis.net/tutorials/index.html>

Host information can be found from viewing the DHCP traffic or the NBNS traffic.

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

Filter: udp.port eq 67						Expression...	Clear	Apply	Save
Time	Src	port	Dst	port	Info				
2016-06-03 21:41:05	192.168.1.1	67	192.168.1.43	68	DHCP ACK - Transaction ID 0x90e20722				
2016-06-03 21:41:09	192.168.1.43	68	255.255.255.255	67	DHCP Inform - Transaction ID 0x580ad57f				
2016-06-03 21:41:09	192.168.1.1	67	192.168.1.43	68	DHCP ACK - Transaction ID 0x580ad57f				
2016-06-03 21:42:27	192.168.1.43	68	255.255.255.255	67	DHCP Inform - Transaction ID 0x862f49a3				

Seconds elapsed: 0

- ▶ Bootp flags: 0x0000 (Unicast)
- Client IP address: 192.168.1.43 (192.168.1.43)
 - Your (client) IP address: 0.0.0.0 (0.0.0.0)
 - Next server IP address: 0.0.0.0 (0.0.0.0)
 - Relay agent IP address: 0.0.0.0 (0.0.0.0)
 - Client MAC address: Dell_67:fb:8c (18:03:73:67:fb:8c)
 - Client hardware address padding: 00000000000000000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: DHCP
- ▶ Option: (53) DHCP Message Type (Inform)
- ▼ Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: Dell_67:fb:8c (18:03:73:67:fb:8c)
- ▼ Option: (12) Host Name
 - Length: 14
 - Host Name: Workshopper-PC
- ▶ Option: (60) Vendor class identifier
 - Option: (55) Parameter Request List

Shown above: DHCP traffic with the appropriate information highlighted.

Time	Src	port	Dst	port	Info				
2016-06-03 21:41:05	192.168.1.1	67	192.168.1.43	68	DHCP ACK - Transaction ID 0x90e20722				
2016-06-03 21:41:05	192.168.1.43	63186	224.0.0.252	5355	Standard query 0x6903 ANY Workshopper-PC				
2016-06-03 21:41:06	192.168.1.43	137	192.168.1.255	137	Registration NB WORKSHOPPER-PC<00>				
2016-06-03 21:41:06	192.168.1.43	137	192.168.1.255	137	Registration NR WORKGROUP<00>				

Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

- ▶ Ethernet II, Src: Dell_67:fb:8c (18:03:73:67:fb:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- ▶ Internet Protocol Version 4, Src: 192.168.1.43 (192.168.1.43), Dst: 192.168.1.255 (192.168.1.255)
- ▶ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
- ▼ NetBIOS Name Service
 - Transaction ID: 0x84b2
 - ▶ Flags: 0x2910 (Registration)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
 - ▶ Queries
 - ▼ Additional records
 - ▶ WORKSHOPPER-PC<00>; type NB, class IN
 - Name: WORKSHOPPER-PC<00> (Workstation/Redirector)
 - Type: NB
 - Class: IN
 - Time to live: 3 days, 11 hours, 20 minutes
 - Data length: 6
 - ▶ Name flags: 0x0000(B-node, unique)
 - Addr: 192.168.1.43

Shown above: NBNS frame with the appropriate information highlighted.

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

FIRST MALWARE:

C:\Users\granny.hightower\Downloads\Boleto_Bancariold3005201612.exe

This one's fairly easy to find in the pcap. Filter on **http.request** and scroll down until 21:44 UTC.

Dst	port	Host	Info
199.96.57.6	80	platform.twitter.com	GET /widgets/tweet_button.c5094533286f08172435cb9c1efe2915
64.13.192.122	80	drperrone.com	GET /favicon.ico HTTP/1.1
174.129.12.168	80	cl.ly	GET /1G2T1N2J2p3i/download/Boleto_Bancariold3005201612.exe
54.235.164.34	80	api.cld.me	GET /1G2T1N2J2p3i/download/Boleto_Bancariold3005201612.exe
204.79.197.200	80	www.bing.com	GET /favicon.ico HTTP/1.1
216.58.194.132	80	www.google.com	GET /HTTP/1.1
216.58.194.132	80	www.google.com	GET /url?sa=t&rct=i&a=8&src=s&source=web&cd=1&ved=0ahUIKE

This came from malspam. Unfortunately, those URLs don't exist in any of the emails for this exercise. There's no referrer in the traffic, so where did it come from? It likely came from the email **2016-06-01-1748-UTC.eml**.

From: Sedex 3ª Tentativa de Entrega 820767 <handersonleao@gmail.com>
Date: Wednesday, June 1, 2016 at 17:48 UTC
To: Granny Hightower <granny.hightower@bobsdonutshack.com>
Subject: Entrega Devolvida Correios!

<https://googledrive.com/host/0B05TIULfbhM6aFdZT2ZTa0VGems/?=3.Tentativa.SEDEX>

 CORREIOS - Rastreamento de objetos

Informações de sua encomenda: [Objeto \(AA100833276BR\)](#) - [Visualizar Relatório](#)
Protocolo: 1787886150558

Data	Local	Situação
20/05/2016 - 11:35	CDD Central de Distribuição	Conferido
20/05/2016 - 13:40	CT Em trânsito para CTR399181	Encaminhado
24/05/2016 - 14:02	CT Agência 39110	Saiu para entrega
24/05/2016 - 15:45	Será realizada uma nova tentativa...	Destinatário ausente
27/05/2016 - 09:20	CT Agência 39110	Saiu para entrega
27/05/2016 - 10:45	CT Agência 39110	Destinatário ausente
31/05/2016 - 13:28	BRASIL - BRASIL R390002/XX	Aguardando retirada
31/05/2016 - 15:02	CT BR - Agência Liberado	Aguardando retirada

*O horário não indica quando a situação ocorreu, mas sim quando os dados foram recebidos pelo sistema.

Tentativa de entrega sem sucesso, segue comunicado de postagem aguardando retirada no local.

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

The **cl.ly** and **api.cld.me** URLs follow the same patterns from another malspam example I did a blog post on at <http://malware-traffic-analysis.net/2016/06/09/index.html> (the second example). Also, you can filter **on http.request or ip contains googledrive** and find some Google Drive traffic right before the HTTP GET requests for the Boleto malware.

Filter: http.request or ip contains googledrive				▼ Expression... Clear Apply Save
Time	Dst	port	Host	Info
2016-06-03 21:43:29	199.96.57.6	80	platform.twitter.com	GET /widgets/tweet_button.c509453286f08172435cb9c1efe2915
2016-06-03 21:43:30	64.13.192.122	80	drperrone.com	GET /favicon.ico HTTP/1.1
2016-06-03 21:44:02	192.168.1.1	53		Standard query 0xe57f A googledrive.com
2016-06-03 21:44:02	192.168.1.43	6533		Standard query response 0xe57f A 216.58.194.65
2016-06-03 21:44:02	216.58.194.65	443		Client Hello
2016-06-03 21:44:02	216.58.194.65	443		Client Hello
2016-06-03 21:44:02	192.168.1.43	4925		Server Hello
2016-06-03 21:44:02	192.168.1.43	4925		Server Hello
2016-06-03 21:44:02	192.168.1.1	53		Standard query 0xc6c1 A 7c416cff040b7449328d095b3e98e12d5f
2016-06-03 21:44:02	192.168.1.43	5794		Standard query response 0xc6c1 CNAME googlehosted.l.googleusercontent.com
2016-06-03 21:44:02	216.58.194.65	443		Client Hello
2016-06-03 21:44:02	216.58.194.65	443		Client Hello
2016-06-03 21:44:02	192.168.1.43	4925		Server Hello
2016-06-03 21:44:02	192.168.1.43	4925		Server Hello
2016-06-03 21:44:03	174.129.12.168	80	cl.ly	GET /1G2T1N2J2p3i/download/Boleto_Bancariold3005201612.exe
2016-06-03 21:44:03	54.235.164.34	80	api.cld.me	GET /1G2T1N2J2p3i/download/Boleto_Bancariold3005201612.exe
2016-06-03 21:49:22	204.79.197.200	80	www.bing.com	GET /favicon.ico HTTP/1.1

SECOND MALWARE:

C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytcy\lytg.dll
C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytcy\lytgc.exe
C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytcy\lytgc32.dll

These are artifacts after an infection from Rig EK on 46.30.47.17 (domain: **ef.crazyballoon.org**) triggered after viewing a compromised website at http://www.curetoothdecay.com/Tooth_Decay/

The pcap has already been submitted to VirusTotal, and you'll find alerts for Rig EK listed for that pcap.

<https://virustotal.com/en/file/1f1cd5d1ada62a99dafcbb5bcfcefac5010c05b0591f9488bac4e5a4afe28f7/analysis/>

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

▲ Suricata alerts	Emerging Threats ETPro ruleset
ET CURRENT_EVENTS RIG Landing URI Struct March 20 2015 (A Network Trojan was Detected) [2020722]	
ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015 (A Network Trojan was Detected) [2020720]	
ET CURRENT_EVENTS RIG Exploit URI Struct March 20 2015 (A Network Trojan was Detected) [2020721]	
ETPRO CURRENT_EVENTS RIG EK Landing Jan 29 M2 (A Network Trojan was Detected) [2816024]	
ET POLICY exe download via HTTP - Informational (Potential Corporate Privacy Violation) [2003595]	
ET POLICY Reserved Internal IP Traffic (Potentially Bad Traffic) [2002752]	
ETPRO CURRENT_EVENTS Possible Evil Redirector Leading to EK Dec 03 2015 M3 (A Network Trojan was Detected) [2815199]	
ET CURRENT_EVENTS RIG encrypted payload Feb 02 (1) (A Network Trojan was Detected) [2022484]	
ETPRO WEB_CLIENT Mozilla Firefox IFRAME Cross Site Scripting (Attempted User Privilege Gain) [2800052]	
ET DNS Standard query response, Name Error (Not Suspicious Traffic) [2001117]	
ET WEB_CLIENT Possible Malicious String.fromCharCode with charCodeAt String (Misc activity) [2012205]	
GPL WEB_CLIENT web bug 0x0 gif attempt (Misc activity) [2102925]	
ETPRO CURRENT_EVENTS RIG EK Flash Exploit Mar 29 2016 (A Network Trojan was Detected) [2816808]	
ET WEB_CLIENT Possible String.fromCharCode Javascript Obfuscation Attempt (Potentially Bad Traffic) [2011347]	
Contract	

Shown above: Suricata alerts from the VirusTotal entry on that pcap.

▲ Snort alerts	Sourcefire VRT ruleset
POLICY-OTHER file URI scheme attempt (Potential Corporate Privacy Violation) [16642]	
DELETED INFO web bug 1x1 gif attempt (Misc activity) [2925]	
PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt (Attempted User Privilege Gain) [19187]	
INDICATOR-OBFUSCATION Multiple Products IFRAME src javascript code execution (Attempted User Privilege Gain) [3679]	
PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority (Potentially Bad Traffic) [254]	
EXPLOIT-KIT Multiple exploit kit flash file download (A Network Trojan was detected) [31902]	
(spp_sdf) SDF Combination Alert (Sensitive Data) [1]	
(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE (Unknown Traffic) [3]	
SENSITIVE-DATA U.S. Social Security Numbers (w/out dashes) (Sensitive Data) [4]	
(http_inspect) HTTP RESPONSE GZIP DECOMPRESSION FAILED (Unknown Traffic) [6]	
DELETED EXPLOIT-KIT Multiple exploit kit flash exploit download (A Network Trojan was detected) [28964]	
DELETED SERVER-OTHER HP LoadRunner stack buffer overflow attempt (Attempted Administrator Privilege Gain) [32996]	
POLICY-OTHER Remote non-JavaScript file found in script tag src attribute (Potential Corporate Privacy Violation) [32481]	
DELETED EXPLOIT-KIT Fiesta exploit kit landing page (A Network Trojan was detected) [30313]	
EXPLOIT-KIT Rig exploit kit outbound communication (A Network Trojan was detected) [33906]	
EXPLOIT-KIT Rig exploit kit outbound communication (A Network Trojan was detected) [33905]	
DELETED BAD TRAFFIC Non-Standard IP protocol (Detection of a non-standard protocol or event) [1620]	
DELETED POLICY inbound potentially malicious file download attempt (A suspicious filename was detected) [12500]	

Shown above: Snort alerts from the VirusTotal entry on that pcap.

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

I used **tcpreplay** on the exercise pcap in Security Onion to get an idea of the IP address and domain for the Rig EK.

Src IP	SPort	Dst IP	DPort	Pr	Event Message
23.235.40.133	80	192.168.1.43	49224	6	FILE tracking PNG (1x1 pixel) (1)
174.136.46.174	80	192.168.1.43	49288	6	snort general alert
192.168.1.43	49298	67.215.187.94	80	6	ETPRO CURRENT_EVENTS Possible Evil Redirector Leading to EK Dec 0...
192.168.1.43	49300	46.30.47.17	80	6	ET CURRENT_EVENTS RIG Landing URI Struct March 20 2015
46.30.47.17	80	192.168.1.43	49300	6	ETPRO CURRENT_EVENTS Sundown/Xer EK Landing May 05 2016 (b641)
46.30.47.17	80	192.168.1.43	49300	6	ETPRO CURRENT_EVENTS RIG EK Landing Jan 29 M2
192.168.1.43	49300	46.30.47.17	80	6	ET CURRENT_EVENTS RIG Exploit URI Struct March 20 2015
46.30.47.17	80	192.168.1.43	49300	6	ETPRO CURRENT_EVENTS SunDown EK Flash June 23 2015 M1
46.30.47.17	80	192.168.1.43	49300	6	ETPRO CURRENT_EVENTS RIG EK Flash Exploit Mar 29 2016
192.168.1.43	49301	46.30.47.17	80	6	ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015
46.30.47.17	80	192.168.1.43	49301	6	ET CURRENT_EVENTS RIG encrypted payload Feb 02 (1)
172.217.0.238	80	192.168.1.43	49293	6	FILE tracking GIF (1x1 pixel)
172.217.0.238	80	192.168.1.43	49293	6	GPL WEB_CLIENT web bug 0x0 gif attempt

Then filtering on **http.request** in Wireshark, I found the associated gate and EK traffic:

Time	Dst	port	Host	Info
2016-06-03 21:49:56	174.136.46.174	80	www.curetoothdecay.com	GET /Cure_Tooth_Decay_img/backg...
2016-06-03 21:49:56	174.136.46.174	80	www.curetoothdecay.com	GET /Cure_Tooth_Decay_img/ebook...
2016-06-03 21:49:56	174.136.46.174	80	www.curetoothdecay.com	GET /Cure_Tooth_Decay_img/ebook...
2016-06-03 21:49:56	174.136.46.174	80	www.curetoothdecay.com	GET /Cure_Tooth_Decay_img/divide...
2016-06-03 21:49:56	172.217.0.238	80	www.google-analytics.com	GET /ga.js HTTP/1.1
2016-06-03 21:49:56	67.215.187.94	80	a.topgunn.photography	GET /nvfviewforumag.php HTTP/1.1
2016-06-03 21:49:56	172.217.0.238	80	www.google-analytics.com	GET /r/_utm.gif?utmwv=5.6.7&utm...
2016-06-03 21:49:58	46.30.47.17	80	ef.crazyballoon.org	GET /?zniKfrGfKxvPCYU=l3SKfPrfJ
2016-06-03 21:49:58	46.30.47.17	80	ef.crazyballoon.org	GET /index.php?zniKfrGfKxvPCYU=l
2016-06-03 21:49:59	46.30.47.17	80	ef.crazyballoon.org	GET /index.php?zniKfrGfKxvPCYU=l
2016-06-03 21:49:59	174.136.46.174	80	www.curetoothdecay.com	GET /favicon.ico HTTP/1.1
2016-06-03 21:50:00	46.30.47.17	80	ef.crazyballoon.org	GET /index.php?zniKfrGfKxvPCYU=l
2016-06-03 21:50:01	23.73.181.48	80	fptdownload2.macromedia.cor	GET /get/flashplayer/update/current
2016-06-03 21:50:01	174.136.46.174	80	www.curetoothdecay.com	GET /Cure_Tooth_Decay_img/subsc...
2016-06-03 21:50:01	23.235.44.143	80	forms.aweber.com	GET /images/closebox.png HTTP/1.1

This is the same campaign I've described in a couple of ISC diaries:

<https://isc.sans.edu/forums/diary/Actor+using+Rig+EK+to+deliver+Qbot/20513/>
<https://isc.sans.edu/forums/diary/Actor+using+Rig+EK+to+deliver+Qbot+update/20551/>

This traffic is also similar to some blog posts I did about Rig EK triggered by a different compromised website.

<http://malware-traffic-analysis.net/2016/06/02/index.html>
<http://malware-traffic-analysis.net/2016/06/06/index.html>

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

Checking the traffic reveals the original referer (the compromised website that kicked off the infection chain and led to Rig EK):

```
GET /?zniKfrGfKxzPCYU=I3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cm
Q9laHYghP7caVR7M60AugzrUXIZgnwh_U6mFQz-8aUw9GswIUnajNBKqE
HTTP/1.1
Accept: text/html, application/xhtml+xml, /*
Referer: http://www.curetoothdecay.com/Tooth_Decay/foods_promote_decay.htm
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: ef.crazyballoon.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 03 Jun 2016 21:49:58 GMT
Content-Type: text/html
Content-Length: 2257
```

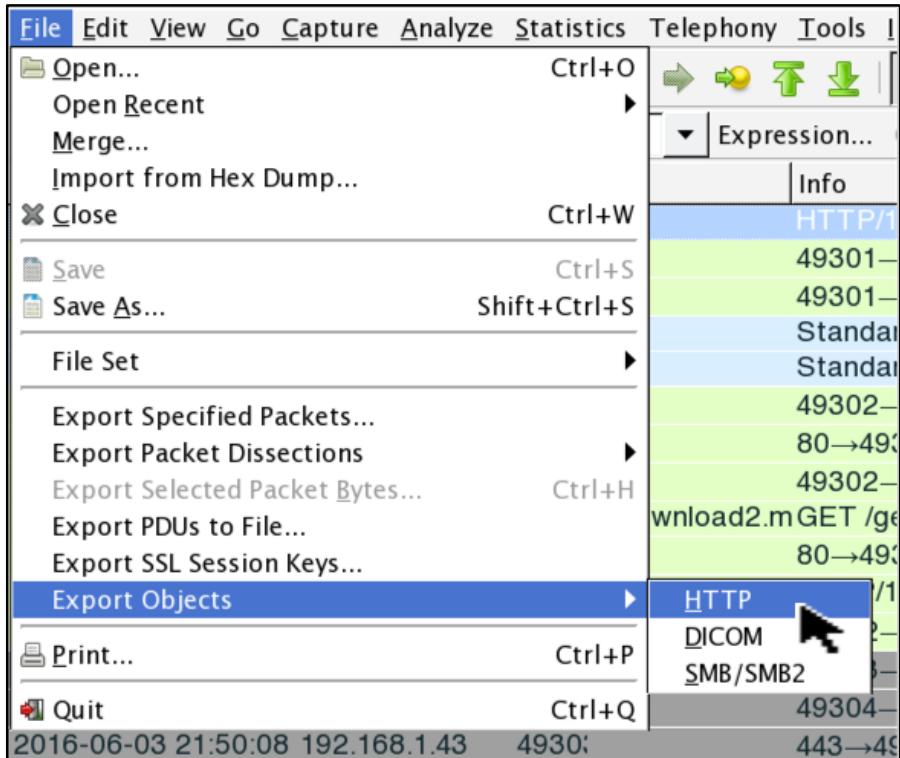
Use ***tcp.stream eq 140*** in the Wireshark filter and follow the TCP stream. This shows the Rig EK malware payload being sent. It's XOR-ed with the ASCII string ***vwMKCwwA***.

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

Shown above: Rig EK sends the malware payload from TCP stream 140 in the pcap.

You can extract the payload from the pcap by exporting HTTP objects.

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS



Packet num	Hostname	Content Type	Size	Filename
9815	www.curetoothdecay.com	image/png	654 bytes	ebook-name.p
9817	www.curetoothdecay.com	image/png	940 bytes	ebook-input.p
9819	www.curetoothdecay.com	image/png	1031 bytes	divider.png
9857	www.google-analytics.com	text/javascript	43 kB	ga.js
9907	www.google-analytics.com	image/gif	35 bytes	_utm.gif?utmv
9917	a.topgunn.photography	text/javascript	954 bytes	nfvviewforumad
9930	ef.crazyballoon.org	text/html	4908 bytes	?zniKfrGfKxvPC
9985	ef.crazyballoon.org	application/x-shockwave-flash	37 kB	index.php?zniK
9997	www.curetoothdecay.com	image/x-icon	3638 bytes	favicon.ico
10479	ef.crazyballoon.org	application/x-msdownload	348 kB	index.php?zniK
10489	fpdownload2.macromedia.com	text/html	349 bytes	version.xml17.0
10589	www.curetoothdecay.com	image/png	3119 bytes	subscribe.png
10600	forms.aweber.com	image/png	1910 bytes	closebox.png

2016-06-03 TRAFFIC ANALYSIS EXERCISE ANSWERS

Then use something like the following Python script to decode it:

```
#!/usr/bin/env python

b = bytearray(open('extracted-file.bin', 'rb').read())
k = bytearray('vwMKCwwA')
for i in range(len(b)):
    b[i]^=k[i%len(k)]
open('decoded-binary.exe', 'wb').write(b)
```

Decrypting the Rig EK payload should give you a file with the same hash as
C:\Users\granny.hightower\AppData\Roaming\Microsoft\Lytgcy\lytgc.exe