2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

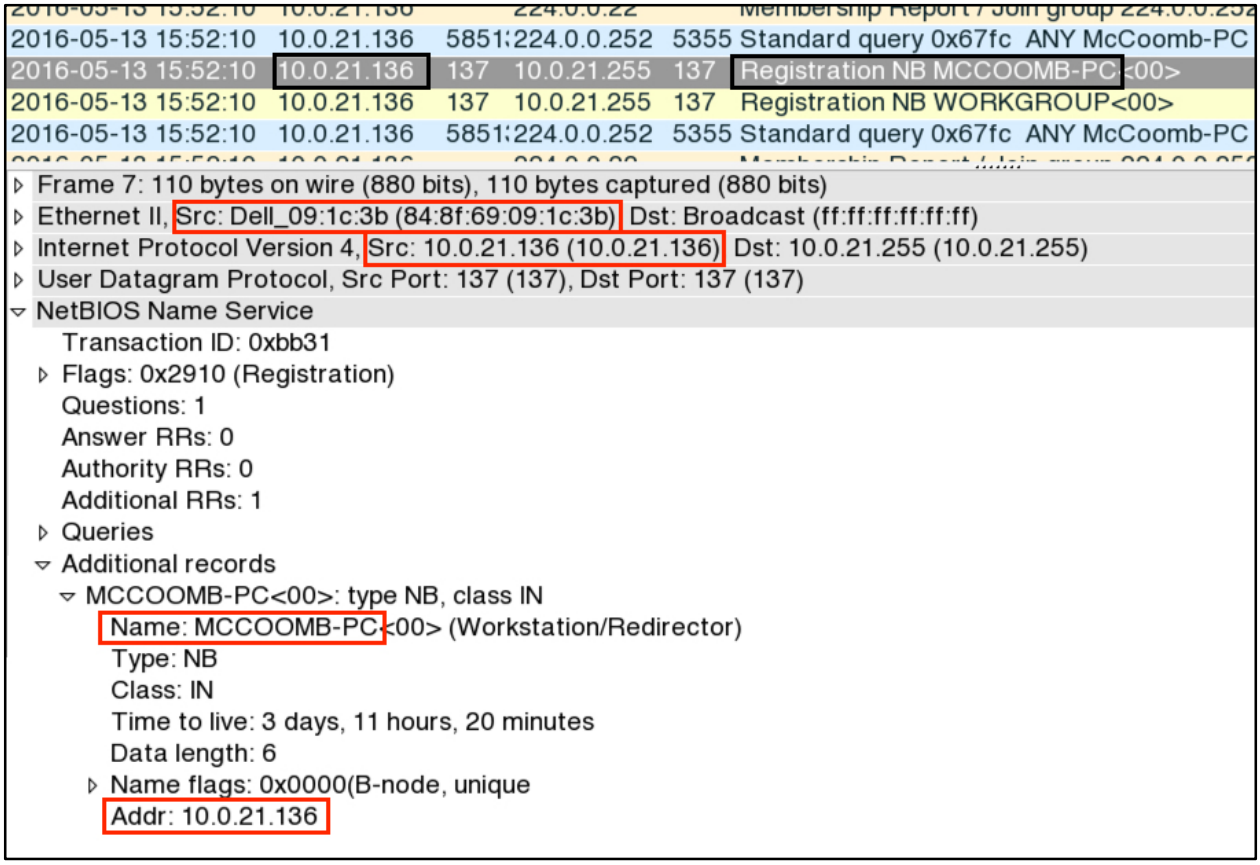
ANSWERS:

- User's first and last name: *probably* ***Donald McCoomb***
- Host name of the user's Windows computer: ***McCoomb-PC***
- IP address of the user's Windows computer: ***10.0.21.136***
- MAC address of the user's computer: ***84:8f:69:09:1c:3b*** *(Dell_09:1c:3b)*
- Item(s) of malware the user's computer is infected with and how it got infected:

    - First infection: Locky ransomware from malspam
    - Second infection: Something (unknown) from Angler EK
    - Third infection: CryptXXX from Angler EK

DETAILS:

IP ADDRESS / HOST NAME / MAC ADDRESS:

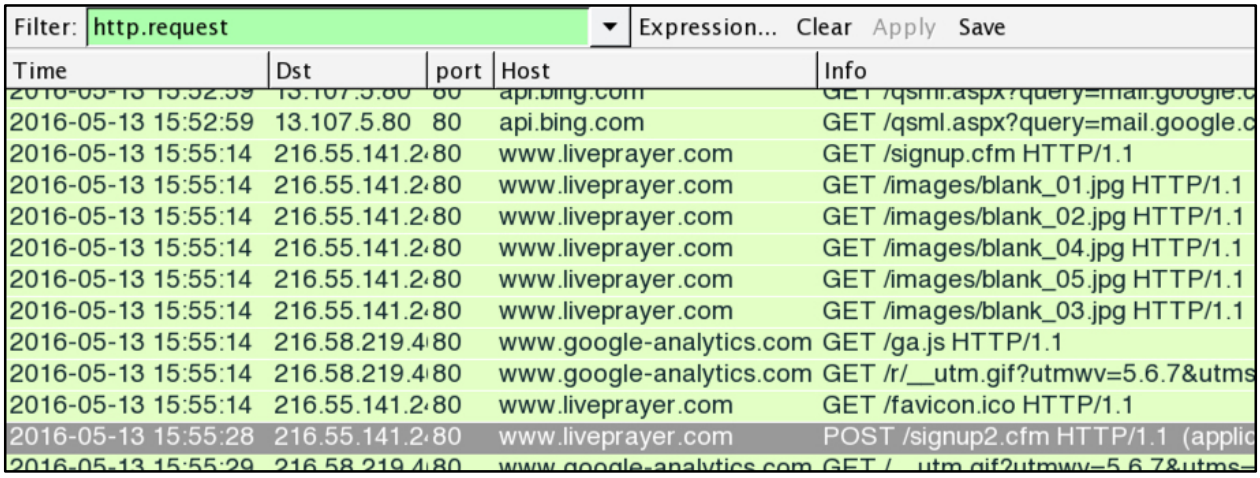


Shown above: NBNS traffic showing the user's host name, IP address, and MAC address.

2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

USER'S FIRST AND LAST NAME:

Although the host name is easy enough to figure out, you usually won't find the user's first and last name. Fortunately, the user registered for something on ***www.liveprayer.com*** with his email address.



Filter: http.request — Expression... Clear Apply Save

Time	Dst	port	Host	Info
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.google.c
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /signup.cfm HTTP/1.1
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /images/blank_01.jpg HTTP/1.1
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /images/blank_02.jpg HTTP/1.1
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /images/blank_04.jpg HTTP/1.1
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /images/blank_05.jpg HTTP/1.1
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /images/blank_03.jpg HTTP/1.1
2016-05-13 15:55:14	216.58.219.4	80	www.google-analytics.com	GET /ga.js HTTP/1.1
2016-05-13 15:55:14	216.58.219.4	80	www.google-analytics.com	GET /r/__utm.gif?utmwv=5.6.7&utms
2016-05-13 15:55:14	216.55.141.2	80	www.liveprayer.com	GET /favicon.ico HTTP/1.1
2016-05-13 15:55:28	216.55.141.2	80	www.liveprayer.com	POST /signup2.cfm HTTP/1.1 (applic

Shown above: The HTTP POST request (highlighted in grey).

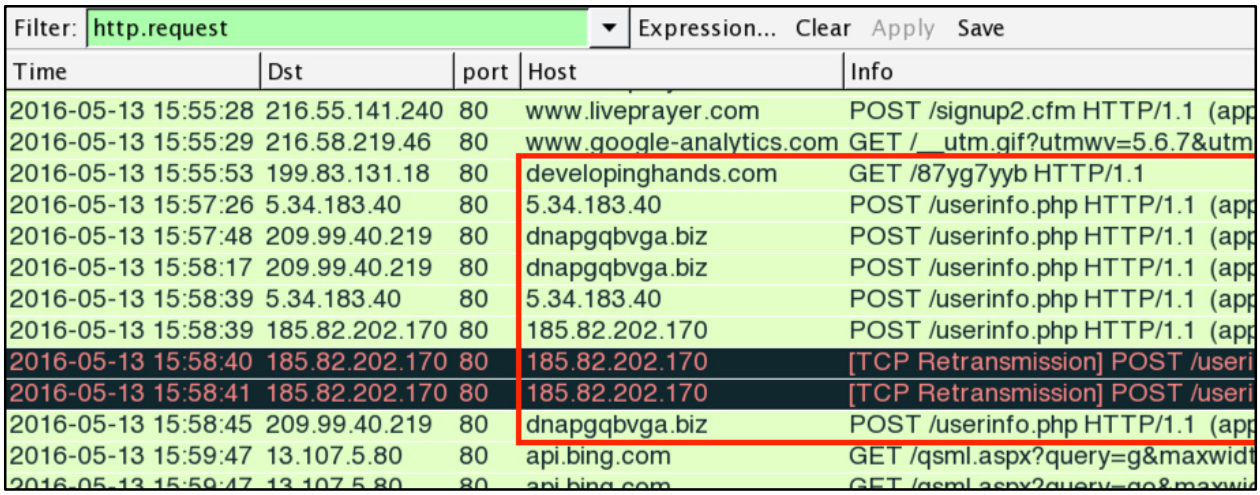
```
POST /signup2.cfm HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.liveprayer.com/signup.cfm
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.liveprayer.com
Content-Length: 47
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: CFID=613826; CFTOKEN=68942474; CFCLIENT_LIVEPRAYER=affid%
3D0%23; CFGLOBALS=urltoken%3DCFID%23%3D613826%26CFTOKEN%23%
3D68942474%23lastvisit%3D%7Bts%20%272016%2D05%2D13%2011%3A55%
3A14%27%7D%23timecreated%3D%7Bts%20%272016%2D05%2D13%2011%
3A55%3A14%27%7D%23hitcount%3D2%23cftoken%3D68942474%23cfid%
3D613826%23;
__utma=236335900.162862547.1463154920.1463154920.1463154920.1;
__utmb=236335900.1.10.1463154920; __utmc=236335900;
__utmz=236335900.1463154920.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=
(none); __utmt=1

email=donald.mccoomb@gmail.com&submit=SubscribeHTTP/1.1 200 OK
Date: Fri, 13 May 2016 15:55:28 GMT
```

Shown above: Email address with first & last name in the HTTP POST request.

2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

FIRST INFECTION: LOCKY FROM MALSPAM.

Shortly after Donald registered at ***www.liveprayer.com***, we see some suspicious HTTP GET and POST requests. They are associated with Locky ransomware.

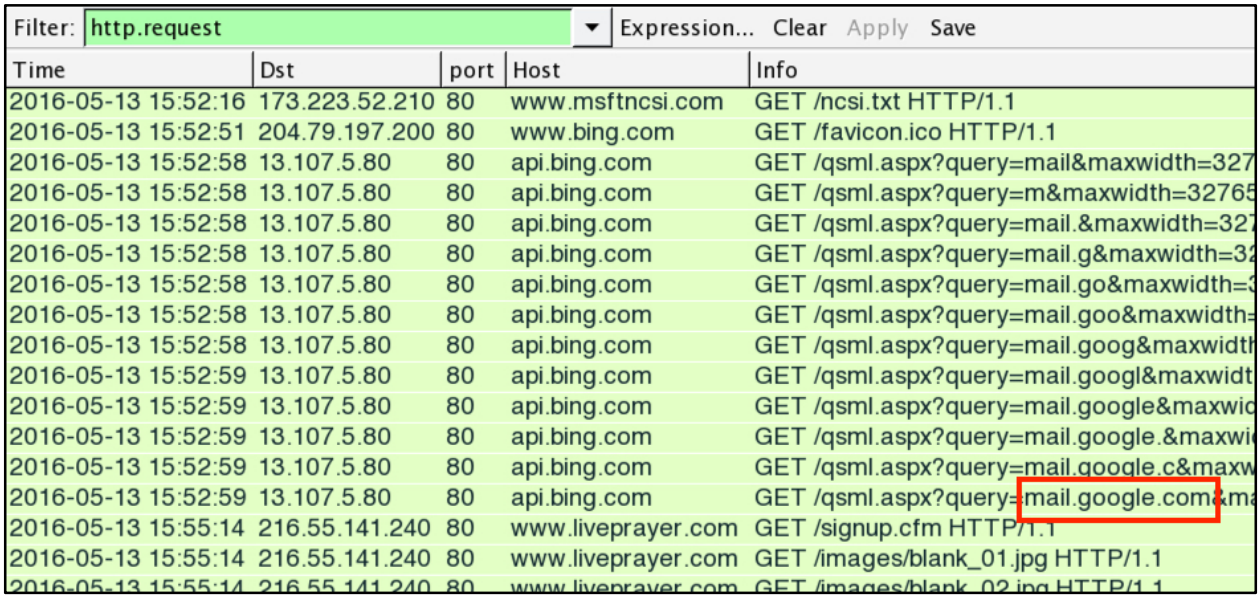


Filter: http.request — Expression... Clear Apply Save

Time	Dst	port	Host	Info
2016-05-13 15:55:28	216.55.141.240	80	www.liveprayer.com	POST /signup2.cfm HTTP/1.1 (app
2016-05-13 15:55:29	216.58.219.46	80	www.google-analytics.com	GET /__utm.gif?utmwv=5.6.7&utm
2016-05-13 15:55:53	199.83.131.18	80	developinghands.com	GET /87yg7yyb HTTP/1.1
2016-05-13 15:57:26	5.34.183.40	80	5.34.183.40	POST /userinfo.php HTTP/1.1 (app
2016-05-13 15:57:48	209.99.40.219	80	dnapgqbvga.biz	POST /userinfo.php HTTP/1.1 (app
2016-05-13 15:58:17	209.99.40.219	80	dnapgqbvga.biz	POST /userinfo.php HTTP/1.1 (app
2016-05-13 15:58:39	5.34.183.40	80	5.34.183.40	POST /userinfo.php HTTP/1.1 (app
2016-05-13 15:58:39	185.82.202.170	80	185.82.202.170	POST /userinfo.php HTTP/1.1 (app
2016-05-13 15:58:40	185.82.202.170	80	185.82.202.170	[TCP Retransmission] POST /useri
2016-05-13 15:58:41	185.82.202.170	80	185.82.202.170	[TCP Retransmission] POST /useri
2016-05-13 15:58:45	209.99.40.219	80	dnapgqbvga.biz	POST /userinfo.php HTTP/1.1 (app
2016-05-13 15:59:47	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=g&maxwidt

Shown above: HTTP requests associated with Lock ransomware.

This happened right after the ***liveprayer.com*** activity, and we can see the user signed into their Gmail shortly before that.

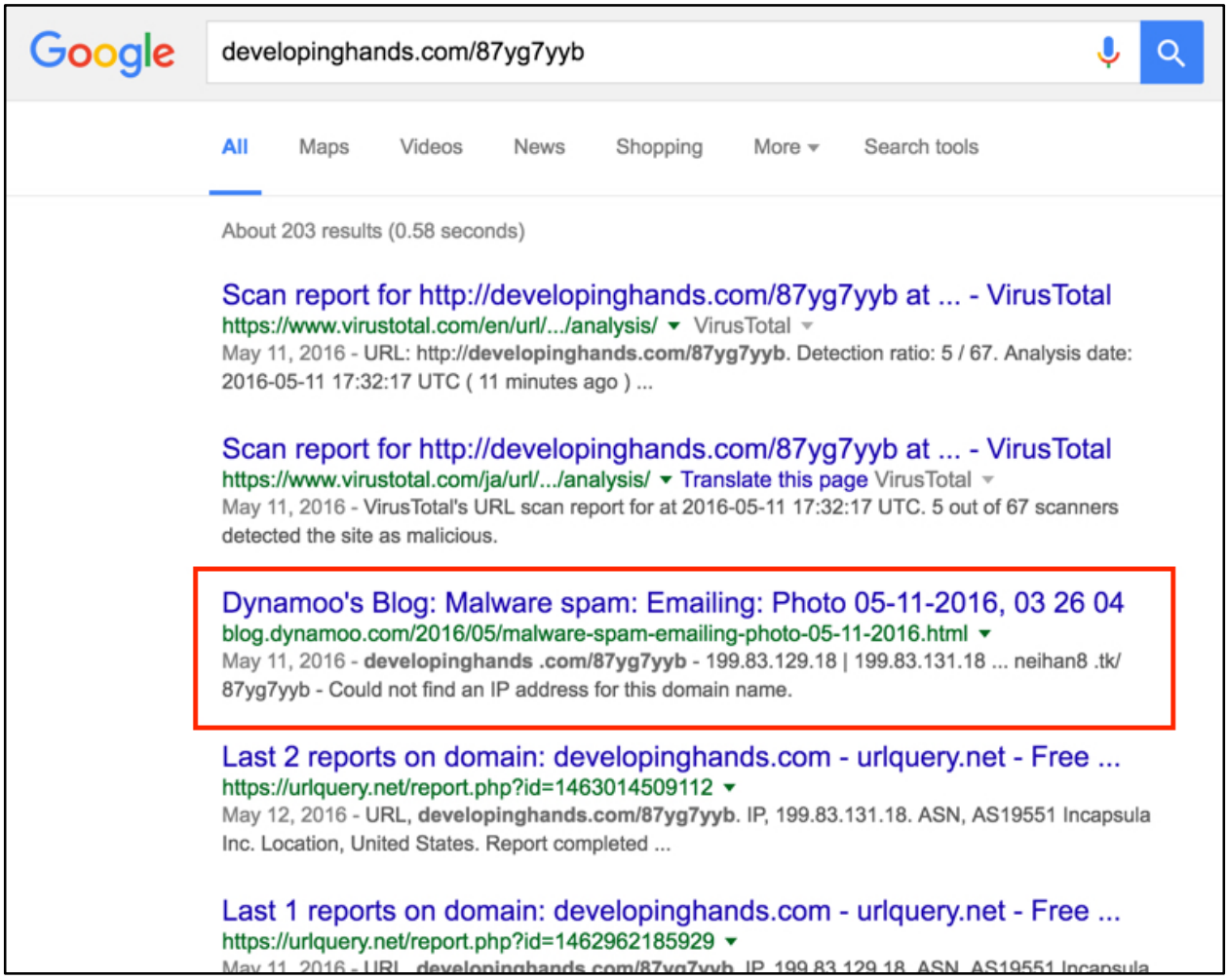


Filter: http.request — Expression... Clear Apply Save

Time	Dst	port	Host	Info
2016-05-13 15:52:16	173.223.52.210	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2016-05-13 15:52:51	204.79.197.200	80	www.bing.com	GET /favicon.ico HTTP/1.1
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail&maxwidth=327
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=m&maxwidth=32765
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.&maxwidth=32
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.g&maxwidth=3
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.go&maxwidth=
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.goo&maxwidth=
2016-05-13 15:52:58	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.goog&maxwidth
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.googl&maxwidt
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.google&maxwi
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.google.&maxwi
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.google.c&maxw
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.google.com&ma
2016-05-13 15:55:14	216.55.141.240	80	www.liveprayer.com	GET /signup.cfm HTTP/1.1
2016-05-13 15:55:14	216.55.141.240	80	www.liveprayer.com	GET /images/blank_01.jpg HTTP/1.1

*Shown above: The user typing **mail.google.com** in the browser address bar.*

In the Locky activity, the first thing we see is an HTTP request for: ***developinghands.com - GET /87yg7yyb***. Search google for more info...



Shown above: Search results for the URL showing a blog post about malspam.

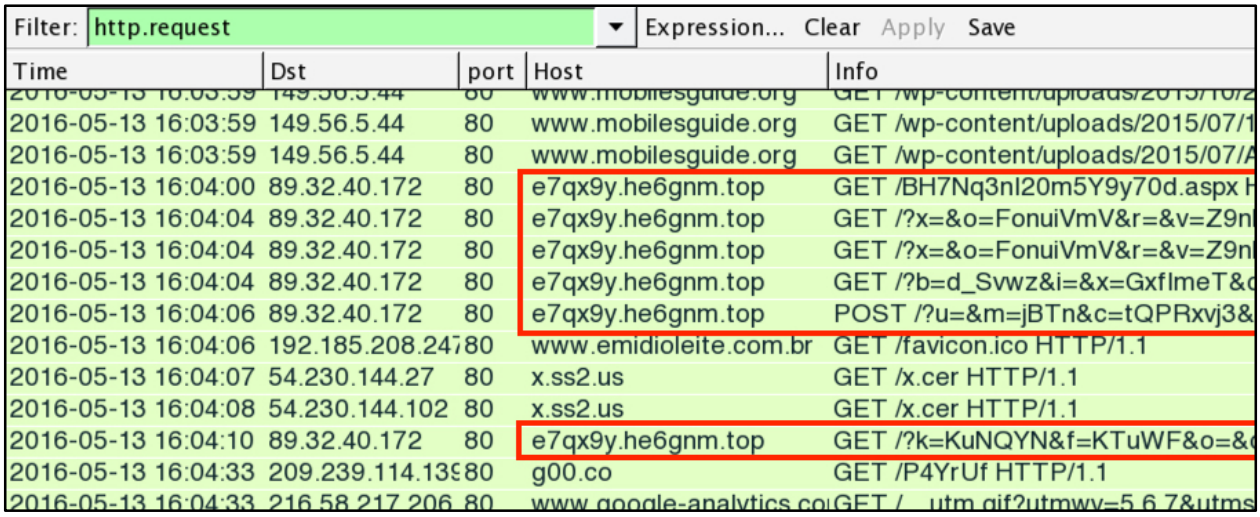
In the search results, you'll see Dynamoo's Blog with a post about malspam with zipped .js attachments that grab Locky. He says the grabbed malware is likely Locky, and when you view the VirusTotal URL from that post, you'll find several comments stating the downloaded .exe is, in fact, Locky.

Both the Snort and Suricata alerts identify the infection traffic (all those HTTP POST requests) as malware. Those POST requests match patterns for other malware, which is why you see other alerts on the same activity, but this is Locky.

The POST requests occur throughout the pcap while the user browses the web after getting infected.

SECOND INFECTION: SOMETHING (UNKOWN) FROM ANGLER EK

Next, we see some HTTP requests matching Angler EK at 16:04 UTC.

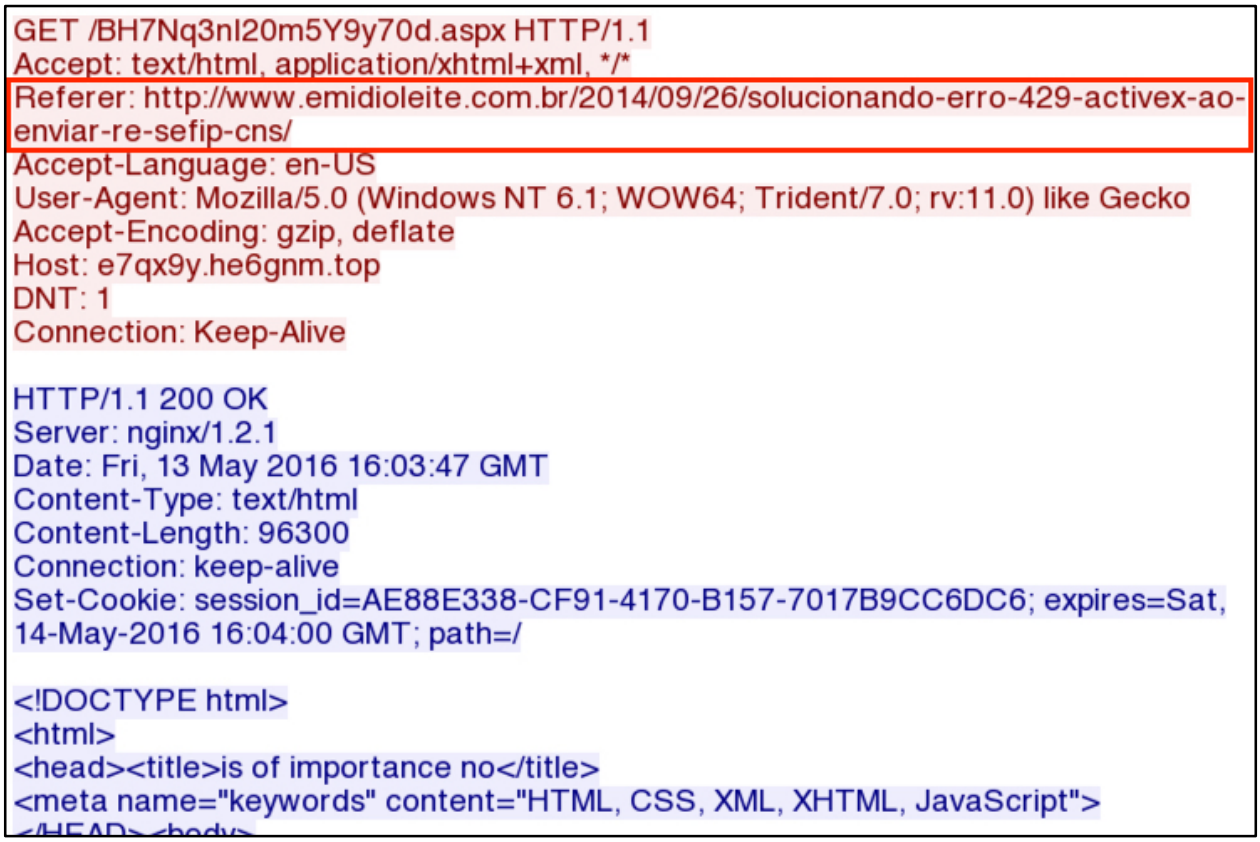


Filter: http.request — Expression... Clear Apply Save

Time	Dst	port	Host	Info
2016-05-13 16:03:59	149.56.5.44	80	www.mobilesguide.org	GET /wp-content/uploads/2015/07/1
2016-05-13 16:03:59	149.56.5.44	80	www.mobilesguide.org	GET /wp-content/uploads/2015/07/A
2016-05-13 16:04:00	89.32.40.172	80	e7qx9y.he6gnm.top	GET /BH7Nq3nl20m5Y9y70d.aspx H
2016-05-13 16:04:04	89.32.40.172	80	e7qx9y.he6gnm.top	GET /?x=&o=FonuiVmV&r=&v=Z9n
2016-05-13 16:04:04	89.32.40.172	80	e7qx9y.he6gnm.top	GET /?x=&o=FonuiVmV&r=&v=Z9n
2016-05-13 16:04:04	89.32.40.172	80	e7qx9y.he6gnm.top	GET /?b=d_Svwz&i=&x=GxfImeT&c
2016-05-13 16:04:06	89.32.40.172	80	e7qx9y.he6gnm.top	POST /?u=&m=jBTn&c=tQPRxvj3&
2016-05-13 16:04:06	192.185.208.247	80	www.emidioleite.com.br	GET /favicon.ico HTTP/1.1
2016-05-13 16:04:07	54.230.144.27	80	x.ss2.us	GET /x.cer HTTP/1.1
2016-05-13 16:04:08	54.230.144.102	80	x.ss2.us	GET /x.cer HTTP/1.1
2016-05-13 16:04:10	89.32.40.172	80	e7qx9y.he6gnm.top	GET /?k=KuNQYN&f=KTuWF&o=&c
2016-05-13 16:04:33	209.239.114.139	80	g00.co	GET /P4YrUf HTTP/1.1
2016-05-13 16:04:33	216.58.217.206	80	www.google-analytics.co	GET /__utm.gif?utmwv=5.6.7&utms

Shown above: Angler EK traffic at 16:04 UTC.

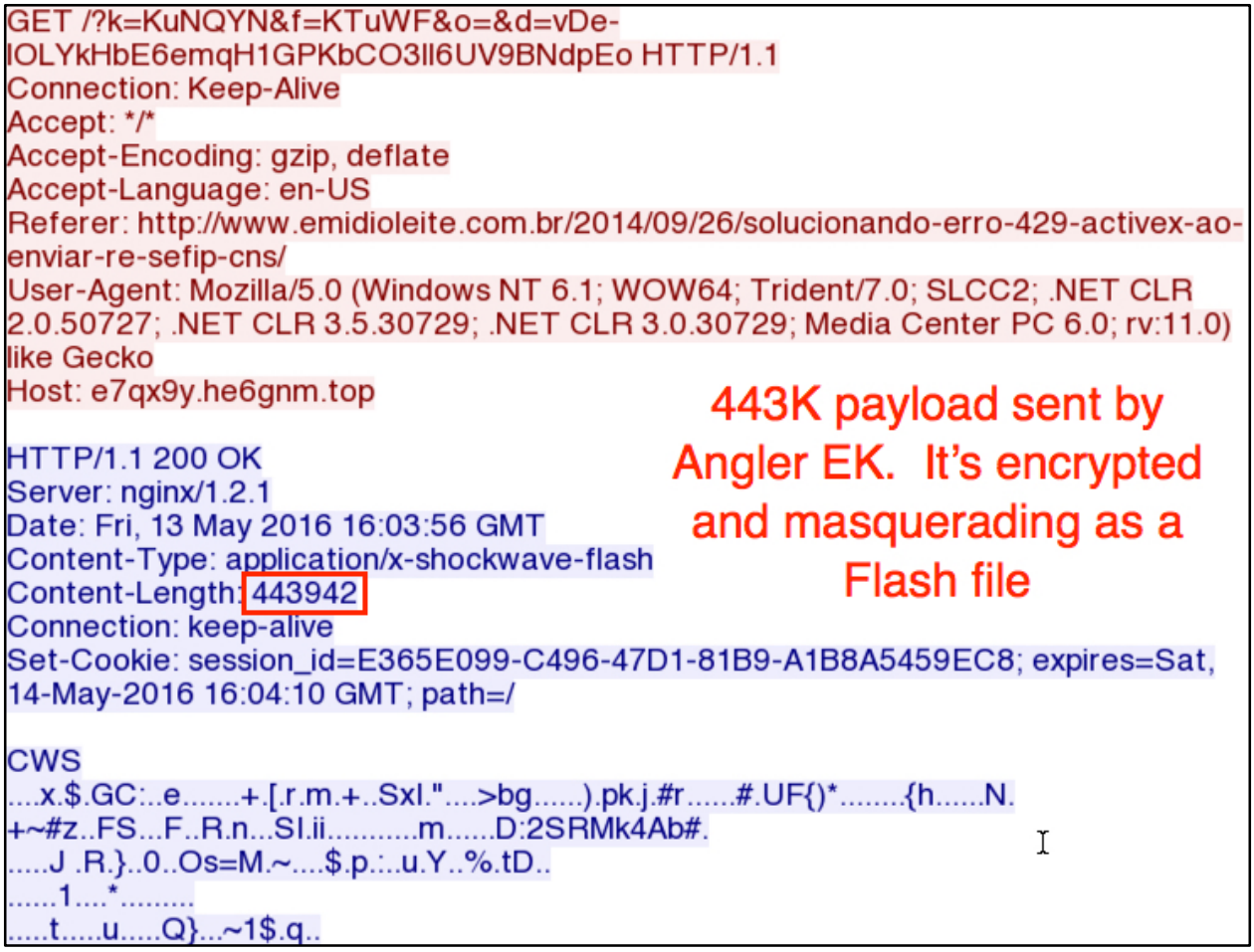
Check the landing page (the first HTTP GET request to the Angler EK domain), and you'll find the compromised website that led to it.



```
GET /BH7Nq3nl20m5Y9y70d.aspx HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.emidioleite.com.br/2014/09/26/solucionando-erro-429-activex-ao-
enviar-re-sefip-cns/
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: e7qx9y.he6gnm.top
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 13 May 2016 16:03:47 GMT
Content-Type: text/html
Content-Length: 96300
Connection: keep-alive
Set-Cookie: session_id=AE88E338-CF91-4170-B157-7017B9CC6DC6; expires=Sat,
14-May-2016 16:04:00 GMT; path=/

<!DOCTYPE html>
<html>
<head><title>is of importance no</title>
<meta name="keywords" content="HTML, CSS, XML, XHTML, JavaScript">
```

Shown above: The Angler EK landing page showing the referer.

Angler EK delivered a 443K payload. Earlier this year, Angler EK started masquerading their payloads as Flash files. They aren't actually Flash files, though. They are encrypted binaries that have a few bytes at the beginning that make them look like Flash files, and the HTTP headers identify them as Flash files. However, they are not Flash, and the encrypted binaries are decoded on the user's computer and used by Angler EK to infect the host. Security researcher Kafeine first spotted this in April 2016 - https://twitter.com/kafeine/status/718449401396654080



Shown above: TCP stream 246 from the pcap.

The malware payload was sent, but there's no post-infection traffic in the pcap. All we see are the same HTTP POST requests caused by Locky.

Angler EK for this second infection came from the EITest campaign (more on that here). This campaign uses a gate between the compromised website (www.emidioleite.com.br) and Angler EK (e7qx9y.he6gnm.top). You'll find the EITest gate IP address at ***85.93.0.68***, and the domain was ***mohecy.tk***.

THIRD INFECTION: ANGLER EK SENDS CRYPTXXX RANSOMWARE

Later in the pcap at 16:25 UTC, you'll see another instance of Angler EK.

Filter: http.request — Expression... Clear Apply Save

Time	Dst	port	Host	Info
2016-05-13 16:25:15	192.186.197.133	80	www.tenmagroup.org	GET /ckea/wp-content
2016-05-13 16:25:15	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	GET /FcMKswvCy_ba_
2016-05-13 16:25:18	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	GET /?k=6myQL5U3s
2016-05-13 16:25:18	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	GET /?k=6myQL5U3s
2016-05-13 16:25:18	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	GET /?x=&m=Y6cj&t=
2016-05-13 16:25:20	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	POST /?l=&o=PkS7Q
2016-05-13 16:25:20	192.186.197.133	80	www.tenmagroup.org	GET /favicon.ico HTT
2016-05-13 16:25:20	192.186.197.133	80	www.tenmagroup.org	GET /favicon.ico HTT
2016-05-13 16:25:26	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	GET /?e=1vgr&o=&g=
2016-05-13 16:25:32	5.34.183.40	80	5.34.183.40	POST /userinfo.php H

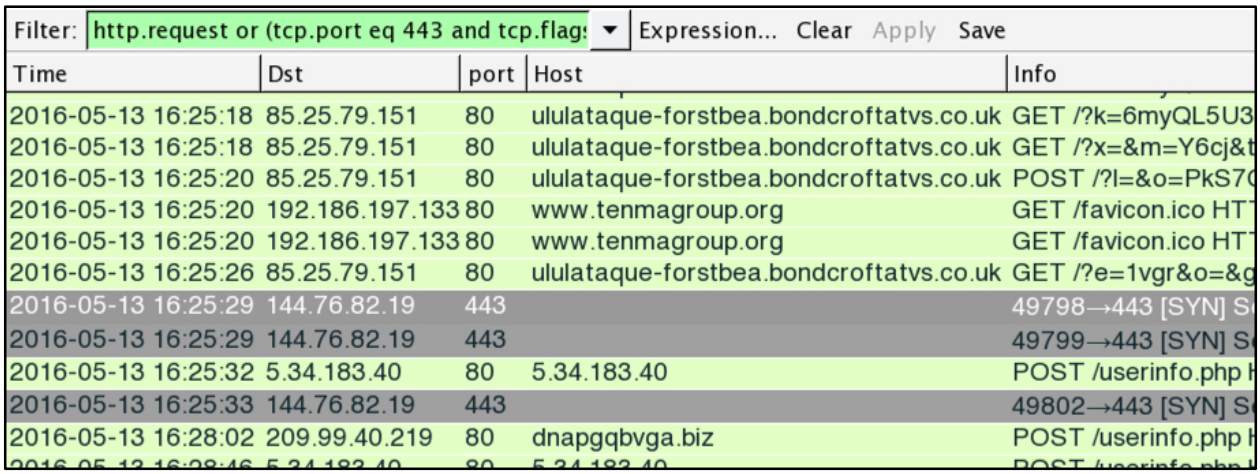
Shown above: More Angler EK at 16:25 UTC.

Follow the TCP stream to find the compromised website that led to this EK.

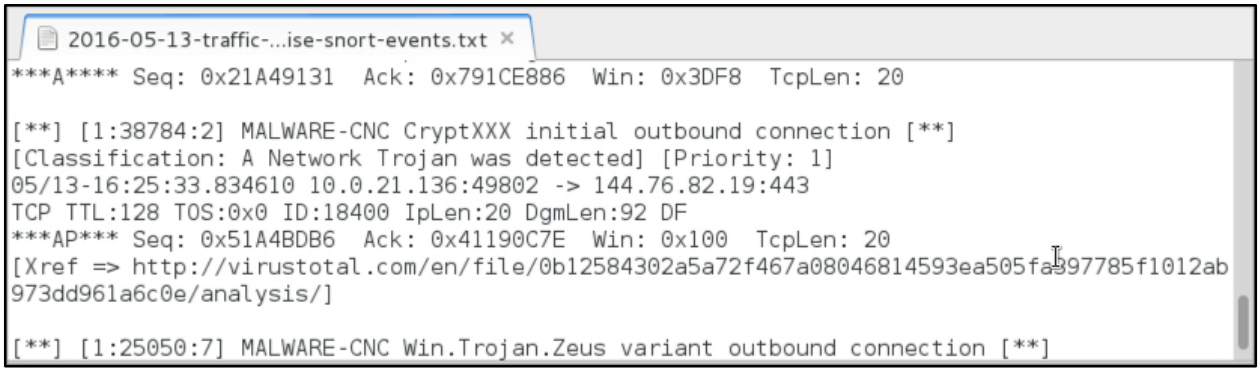
```
GET /FcMKswvCy_ba_IXEFyV.html HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.tenmagroup.org/ckea/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: ululataque-forstbea.bondcroftatvs.co.uk
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 May 2016 16:25:15 GMT
Content-Type: text/html
Content-Length: 96324
Connection: keep-alive
Set-Cookie: session_id=9DEC608D-CE81-45C8-944F-40905C5AD61A; expires=Sat,
14-May-2016 16:25:16 GMT; Max-Age=86400; path=/

<!DOCTYPE html>
<html>
<head><title>is of importance no</title>
<meta name="keywords" content="HTML, CSS, XML, XHTML, JavaScript">
</HEAD><body>
<sup>
 "Are you certain that was weary of guest, that pressed them very earnestly to
```

Shown above: TCP stream 413 from the pcap.

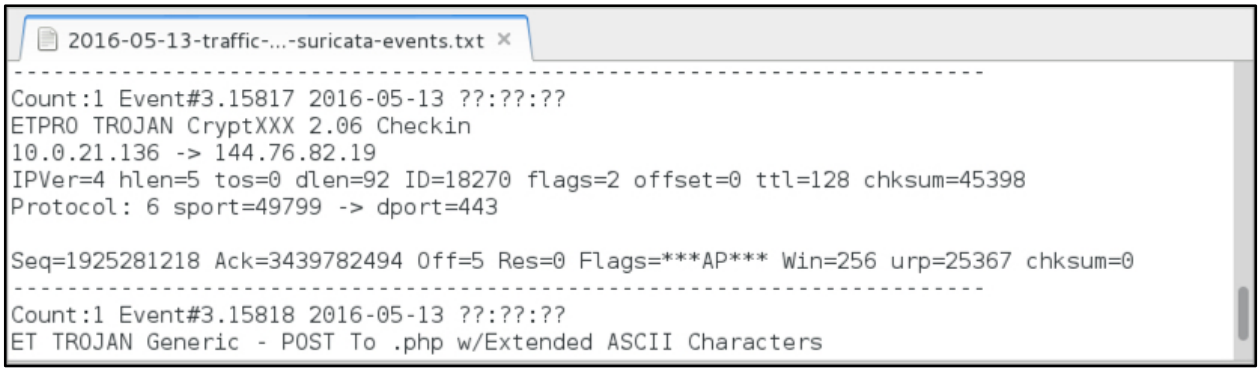
Immediately after this Angler EK, you'll notice traffic over port 443 to 144.76.82.19, which is post-infection traffic caused by CryptXXX. Use the Wireshark filter ***http.request or (tcp.port eq 443 and tcp.flags eq 0x0002)*** to get an idea of the traffic.



Shown above: CryptXXX traffic over TCP port 443 (the gray lines).



Shown above: One of the Snort events identifying this as CryptXXX traffic.



Shown above: One of the Suricata events identifying this as CryptXXX traffic.

This is part of the pseudo-Darkleech campaign, which you can read more about here.