

# 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:

2016-05-13 15:52:10	10.0.21.136	224.0.0.22	Membership Report / Join group 224.0.0.22		
2016-05-13 15:52:10	10.0.21.136	5851:224.0.0.252	5355	Standard query 0x67fc	ANY McCoomb-PC
2016-05-13 15:52:10	10.0.21.136	137	10.0.21.255	137	Registration NB MCCOOMB-PC<00>
2016-05-13 15:52:10	10.0.21.136	137	10.0.21.255	137	Registration NB WORKGROUP<00>
2016-05-13 15:52:10	10.0.21.136	5851:224.0.0.252	5355	Standard query 0x67fc	ANY McCoomb-PC
2016-05-13 15:52:10	10.0.21.136	137	10.0.21.255	137	Membership Report / Join group 224.0.0.22
► Frame 7: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)					
► Ethernet II, Src: Dell_09:1c:3b (84:8f:69:09:1c:3b) Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
► Internet Protocol Version 4, Src: 10.0.21.136 (10.0.21.136) Dst: 10.0.21.255 (10.0.21.255)					
► User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)					
▼ NetBIOS Name Service					
Transaction ID: 0xbb31					
► Flags: 0x2910 (Registration)					
Questions: 1					
Answer RRs: 0					
Authority RRs: 0					
Additional RRs: 1					
► Queries					
▼ Additional records					
► MCCOOMB-PC<00>: type NB, class IN					
Name: MCCOOMB-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: 10.0.21.136					

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](http://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.o	
2016-05-13 15:52:59	13.107.5.80	80	api.bing.com	GET /qsml.aspx?query=mail.google.o	
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 (application/x-www-form-urlencoded)	
2016-05-13 15:55:29	216.58.219.4.80		www.google-analytics.com	GET /r/_utm.gif?utmwv=5.6.7&utms	

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

The screenshot shows a Google search results page for the URL [developinghands.com/87yg7yyb](http://developinghands.com/87yg7yyb). The search bar at the top has the query "developinghands.com/87yg7yyb". Below the search bar, there are navigation links for All, Maps, Videos, News, Shopping, More, and Search tools. A message indicates "About 203 results (0.58 seconds)".

The first result is a link to a VirusTotal scan report for the URL. The report title is "Scan report for http://developinghands.com/87yg7yyb at ... - VirusTotal". It includes a link to the analysis page (<https://www.virustotal.com/en/url/.../analysis/>) and the date of the analysis (May 11, 2016). The report notes a detection ratio of 5 / 67.

The second result is another VirusTotal scan report for the same URL, titled "Scan report for http://developinghands.com/87yg7yyb at ... - VirusTotal". It also includes a link to the analysis page and the date (May 11, 2016). It states that 5 out of 67 scanners detected the site as malicious.

A third result is a blog post from "Dynamoo's Blog" titled "Malware spam: Emailing: Photo 05-11-2016, 03 26 04". The link is [blog.dynamoo.com/2016/05/malware-spam-emailing-photo-05-11-2016.html](http://blog.dynamoo.com/2016/05/malware-spam-emailing-photo-05-11-2016.html). The post discusses malware spam and includes a screenshot of the blog post content.

Below these results, there are two more entries from urlquery.net:

- "Last 2 reports on domain: developinghands.com - urlquery.net - Free ..." with a link to <https://urlquery.net/report.php?id=1463014509112>. It provides details about the URL, IP address (199.83.129.18), ASN (AS19551), and location (United States).
- "Last 1 reports on domain: developinghands.com - urlquery.net - Free ..." with a link to <https://urlquery.net/report.php?id=1462962185929>. It also provides similar details about the URL and its characteristics.

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.

## 2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

### SECOND INFECTION: SOMETHING (UNKNOWN) FROM ANGLER EK

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

Time	Dst	port	Host	Info
2016-05-13 10:05:59	149.50.5.44	80	www.mobilesguide.org	GET /wp-content/uploads/2015/10/2
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/2015/07/1
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_Swvz&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.emidioelite.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=&
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.com	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.emidioelite.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">
</head><body>
```

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

## 2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

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>

```
GET /?k=KuNQYN&f=KTuWF&o=&d=vDe-
IOLYkHbE6emqH1GPKbCO3II6UV9BNdpEo HTTP/1.1
Connection: Keep-Alive
Accept: /*
Accept-Encoding: gzip, deflate
Accept-Language: en-US
Referer: http://www.emidioleite.com.br/2014/09/26/solucionando-erro-429-activex-ao-
enviar-re-sefip-cns/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; rv:11.0)
like Gecko
Host: e7qx9y.he6gnm.top

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 13 May 2016 16:03:56 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 443942
Connection: keep-alive
Set-Cookie: session_id=E365E099-C496-47D1-81B9-A1B8A5459EC8; expires=Sat,
14-May-2016 16:04:10 GMT; path=/

CWS
....x.$.GC:..e.....+[.r.m.+..Sxl."....>bg.....).pk.j.#r.....#.UF{}*.....{h.....N.
+~#z..FS..F..R.n..SI.ii.....m.....D:2SRMk4Ab#.
.....J ..R.)..0..Os=M.~....$.p:..u.Y..%.tD..
.....1.....
.....t....u....Q}...~1$.q..
```

443K payload sent by  
Angler EK. It's encrypted  
and masquerading as a  
Flash file

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](http://www.emidioleite.com.br)) and Angler EK ([e7qx9y.he6gnm.top](http://e7qx9y.he6gnm.top)). You'll find the EITest gate IP address at **85.93.0.68**, and the domain was **mohecy.tk**.

## 2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

### THIRD INFECTION: ANGLER EK SENDS CRYPTXXX RANSOMWARE

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

Time	Dst	port	Host	Info
2016-05-13 16:25:15	192.186.197.133	80	www.tenmagroup.org	GET /ckeawp-content
2016-05-13 16:25:15	192.186.197.133	80	www.tenmagroup.org	GET /ckeawp-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 HTTP/1.1
2016-05-13 16:25:20	192.186.197.133	80	www.tenmagroup.org	GET /favicon.ico HTTP/1.1
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 HTTP/1.1
2016-05-13 16:28:02	209.99.40.210	80	dnanrahywaz.biz	POST /userinfo.php HTTP/1.1

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/ckeawp-content/
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 quest, that pressed them very earnestly to

```

Shown above: TCP stream 413 from the pcap.

## 2016-05-13 TRAFFIC ANALYSIS EXERCISE - ANSWERS

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.

Filter: http.request or (tcp.port eq 443 and tcp.flags eq 0x0002)				Expression... Clear Apply Save
Time	Dst	port	Host	Info
2016-05-13 16:25:18	85.25.79.151	80	ululataque-forstbea.bondcroftatvs.co.uk	GET /?k=6myQL5U3
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=Pks70
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 16:25:29	144.76.82.19	443		49798→443 [SYN] S
2016-05-13 16:25:29	144.76.82.19	443		49799→443 [SYN] S
2016-05-13 16:25:32	5.34.183.40	80	5.34.183.40	POST /userinfo.php H
2016-05-13 16:25:33	144.76.82.19	443		49802→443 [SYN] S
2016-05-13 16:28:02	209.99.40.219	80	dnapqqbvga.biz	POST /userinfo.php H
2016-05-13 16:29:46	5.34.183.40	80	5.34.183.40	POST /userinfo.php H

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

```
2016-05-13-traffic-...-snort-events.txt x
***A**** Seq: 0x21A49131 Ack: 0x791CE886 Win: 0x3DF8 TcpLen: 20

[**] [1:38784:2] MALWARE-CNC CryptXXX initial outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
05/13-16:25:33.834610 10.0.21.136:49802 -> 144.76.82.19:443
TCP TTL:128 TOS:0x0 ID:18400 IpLen:20 DgmLen:92 DF
***AP*** Seq: 0x51A4BDB6 Ack: 0x41190C7E Win: 0x100 TcpLen: 20
[Xref => http://virustotal.com/en/file/0b12584302a5a72f467a08046814593ea505fa397785f1012ab
973dd961a6c0e/analysis/]

[**] [1:25050:7] MALWARE-CNC Win.Trojan.Zeus variant outbound connection [**]
```

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

```
2016-05-13-traffic-...-suricata-events.txt x
-----
Count:1 Event#3.15817 2016-05-13 ???:???
ETPRO TROJAN CryptXXX 2.06 Checkin
10.0.21.136 -> 144.76.82.19
IPVer=4 hlen=5 toss=0 dlen=92 ID=18270 flags=2 offset=0 ttl=128 chksum=45398
Protocol: 6 sport=49799 -> dport=443

Seq=1925281218 Ack=3439782494 Off=5 Res=0 Flags=***AP*** Win=256 urp=25367 chksum=0
-----
Count:1 Event#3.15818 2016-05-13 ???:???
ET TROJAN Generic - POST To .php w/Extended ASCII Characters
```

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](#).