

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Start date and time of the traffic: **Saturday 2016-12-17 at approximately 02:30 UTC**

MAC address of infected Windows computer: **00:1c:23:9b:70:5e (Dell_9b:70:5e)**

IP address of the infected Windows computer: **172.16.2.96**

Host name of the infected Windows computer: **Froggy-PC**

Person's name (account name) using the infected Windows host: **Matthew.Frogman**

Public IP address of the infected Windows computer: **201.16.144.112**

Country or general location of the infected Windows computer: **Brazil**

A description of what happened:

The user (Matthew.Frogman) was infected through a link from an Boleto-themed malicious spam (malspam) in an ongoing campaign I previously documented earlier this year on a few occasions:

- <http://www.malware-traffic-analysis.net/2016/07/25/index4.html>
- <http://www.malware-traffic-analysis.net/2016/08/13/index.html>
- <http://www.malware-traffic-analysis.net/2016/08/16/index2.html>
- <http://www.malware-traffic-analysis.net/2016/08/17/index2.html>
- <http://www.malware-traffic-analysis.net/2016/08/18/index4.html>
- <http://www.malware-traffic-analysis.net/2016/08/22/index.html>
- <http://www.malware-traffic-analysis.net/2016/08/23/index.html>
- <http://www.malware-traffic-analysis.net/2016/08/25/index.html>
- <http://www.malware-traffic-analysis.net/2016/09/21/index3.html>

The indicators of compromise (IOCs) have changed a little since the last time they were documented on the blog in September 2016, but it's recognizably the same type of traffic.

IOCs for this infection:

Link from the email:

- 65.181.125.20 port 80 - **wme0hsxg.e6to8jdmiysycbmeepm29nfprvigdwev.top** - GET /1dkfJu.php?1dkfJu=wME0HsXGMATTHEW

Redirect to .js file hosted on 4shared.com:

- 74.117.178.179 port 80 - **dc621.4shared.com** - GET /download/j2PZxBQ-ba/16122016xoGul9iOhm1WwDLLwlkxwX.vbe?*[long string]*

Post-infection HTTP traffic:

- 65.181.112.240 port 80 - **65.181.112.240** - GET /bibi/w7.txt
- 65.181.112.240 port 80 - **65.181.112.240** - GET /bibi/aw7.tiff
- 65.181.112.240 port 80 - **65.181.112.240** - GET /bibi/W7.zip
- 65.181.112.240 port 80 - **65.181.112.240** - GET /bibi/dll.dll

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

- 65.181.112.240 port 80 - **65.181.112.240** - GET /bibi/dll.dll.exe
- 65.181.112.240 port 80 - **www.devyatinskiy.ru** - GET /bsb/infected/index.php?[long string]
- 65.181.112.240 port 80 - **www.devyatinskiy.ru** - GET /bsb/debugnosso/index.php?[long string]
- 158.69.99.213 port 80 - **log.houselannister.top** - POST /mestre/admin/x.php

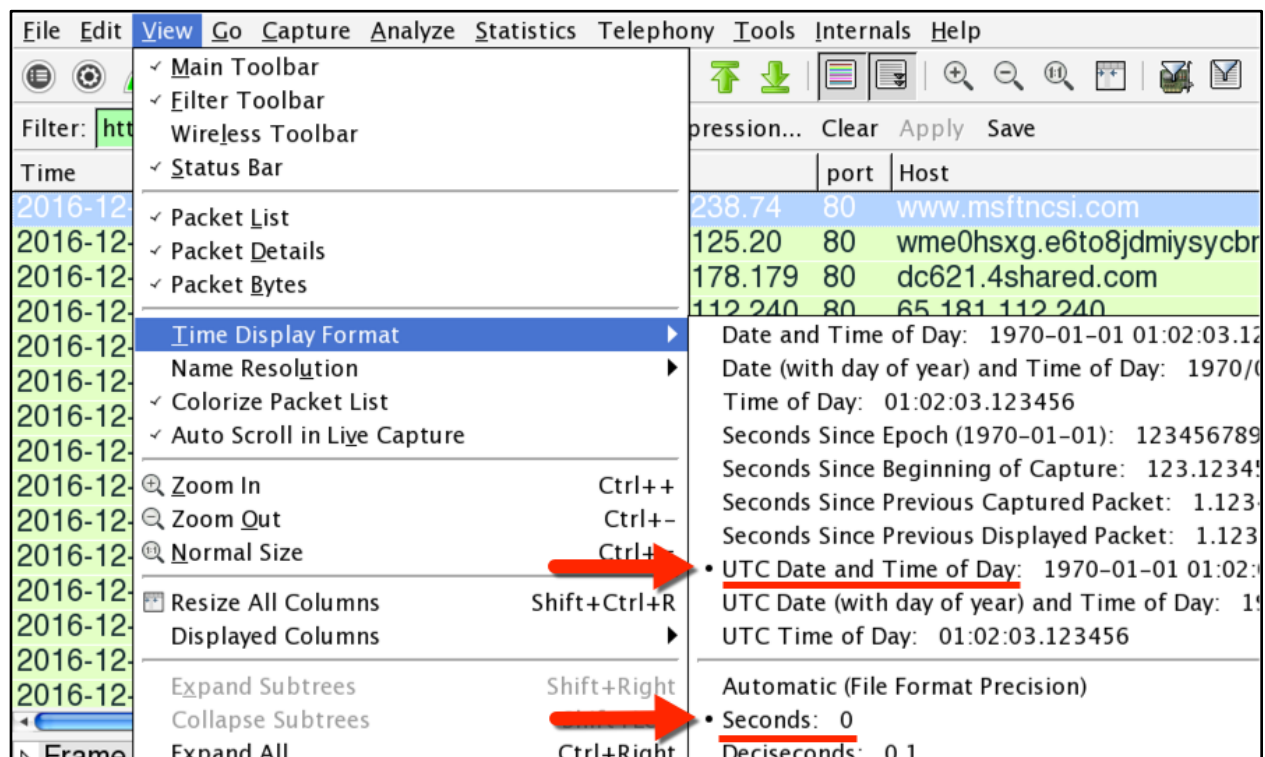
Post-infection IRC traffic:

- 65.181.113.204 port 443 - **ssl.houselannister.top** - IRC traffic (botnet command and control, not encrypted)

DETAILS

Let's get the basics out of the way. The pcap is drawn from a single IP address, 172.16.2.96, so that's the IP address of the infected host. If you filter on **!(ip.addr eq 172.16.2.96)** in Wireshark, there isn't anything left in the pcap.

The start time of the pcap is 2016-12-17 at 02:30 UTC. It's important to note the time zone when you're reporting on an incident. I always use UTC (same as GMT) because that's universal. In Wireshark, you need to ensure you're using the correct display format.



Shown above: Ensuring your time is displaying correctly in Wireshark.

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Note that you'll also want to make sure it shows as UTC for the display columns under the Wireshark .

The MAC address can be found by correlating it with the IP address. You can also correlate the MAC address, IP address, and host name by looking at the DHCP traffic. Use the Wireshark filter **udp.port eq 67** and look at the packet and frame details as seen in the image below.

Filter:	udp.port eq 67	Expression...	Clear	Apply	Save
Time	Src	port	Dst	port	Info
2016-12-17 02:30:38	172.16.2.254	67	172.16.2.96	68	DHCP Offer - Transaction ID 0xcf5ae64
2016-12-17 02:30:38	172.16.2.254	67	172.16.2.96	68	DHCP ACK - Transaction ID 0xcf5ae64
2016-12-17 02:30:41	172.16.2.96	68	255.255.255.255	67	DHCP Inform - Transaction ID 0xb6a4419
2016-12-17 02:30:41	172.16.2.254	67	172.16.2.96	68	DHCP ACK - Transaction ID 0xb6a4419
2016-12-17 02:32:32	172.16.2.96	68	255.255.255.255	67	DHCP Inform - Transaction ID 0xe326678
2016-12-17 02:32:32	172.16.2.254	67	172.16.2.96	68	DHCP ACK - Transaction ID 0xe326678
▶ Frame 26: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)					
▶ Ethernet II, Src: Dell_9b:70:5e (00:1c:23:9b:70:5e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
▶ Internet Protocol Version 4, Src: 172.16.2.96 (172.16.2.96), Dst: 255.255.255.255 (255.255.255.255)					
▶ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)					
▼ Bootstrap Protocol (Inform)					
Message type: Boot Request (1)					
Hardware type: Ethernet (0x01)					
Hardware address length: 6					
Hops: 0					
Transaction ID: 0xb6a44194					
Seconds elapsed: 0					
▶ Bootp flags: 0x0000 (Unicast)					
Client IP address: 172.16.2.96 (172.16.2.96)					
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_9b:70:5e (00:1c:23:9b:70:5e)					
Client hardware address padding: 00000000000000000000					
Server host name not given					
Boot file name not given					
Magic cookie: DHCP					
▶ Option: (53) DHCP Message Type (Inform)					
▶ Option: (61) Client identifier					
▼ Option: (12) Host Name					
Length: 9					
Host Name: Froggy-PC					
▶ Option: (60) Vendor class identifier					
▶ Option: (55) Parameter Request List					

Shown above: DHCP traffic showing the host name, IP address, and MAC address.

Since this is a Windows host, you can also get the host name from the NBNS traffic.

Filter:	nbns	Expression...	Clear	Apply	Save
Time	Src	port	Dst	port	Info
2016-12-17 02:30:38	172.16.2.96	137	172.16.2.1	137	Registration NB FROGGY-PC<20>
2016-12-17 02:30:38	172.16.2.96	137	172.16.2.1	137	Registration NB FROGGY-PC<00>
2016-12-17 02:30:38	172.16.2.96	137	172.16.2.1	137	Registration NB WORKGROUP<00>
2016-12-17 02:30:39	172.16.2.96	137	172.16.2.1	137	Registration NB WORKGROUP<00>

Shown above: Host name in NBNS traffic.

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

The user;s name shows up in the post-infection traffic to **www.devyatinskiy.ru**. You can correlate the user name with Froggy-PC as seen in the image below.

Filter:	http.request	Expression...	Clear	Apply	Save
Host	Info				
65.181.112.240	GET /bibi/aw7.dll HTTP/1.1				
www.devyatinskiy.ru	GET /bsb/infecteds/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
65.181.112.240	GET /bibi/W7.zip HTTP/1.1				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
65.181.112.240	GET /bibi/dll.dll HTTP/1.1				
65.181.112.240	GET /bibi/dll.dll.exe HTTP/1.1				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
www.devyatinskiy.ru	GET /bsb/debugnosso/index.php?N=FROGGY-PC-Matthew-Frogman%20=%20%20%				
api.devyatinskiy.ru	GET /temer/debug/index.php?N=FROGGY-PC-SYSTEM%20=%20%20%20%				

Shown above: User's name from the post-infeciton traffic.

The infected host's IP address shows up in IRC traffic on TCP port 443 to **ssl.houselannister.top** on 65.181.113.204. First, filter on **ip.addr eq 65.181.113.204** to get that traffic. Then follow the TCP stream from the first frame.

```
Stream Content
...
NICK a37[7]FROGGY-PC-Matt[1329]
USER Matthew.Frogman 0 * :a37[7]FROGGY-PC-Matt[1329]@iMestreUser.com
:einstein.oftc.net NOTICE AUTH :*** Looking up your hostname...
:einstein.oftc.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:einstein.oftc.net 451 ... :You have not registered
PING :113BACA6
PONG 113BACA6
:einstein.oftc.net 001 a37[7]FROGGY-PC-Matt[1329] :Welcome to the fsociety IRC Network a37
[7]FROGGY-PC-Matt[1329]!Matthew.Fr@201.16.144.112
:einstein.oftc.net 002 a37[7]FROGGY-PC-Matt[1329] :Your host is einstein.oftc.net, running version
Unreal3.2.10.6
:einstein.oftc.net 003 a37[7]FROGGY-PC-Matt[1329] :This server was created Mon Jul 25 2016 at
17:41:29 BRT
:einstein.oftc.net 004 a37[7]FROGGY-PC-Matt[1329] einstein.oftc.net Unreal3.2.10.6
iowghraAsORTVSxNCWqBzvdHtGpl lvhopsmntikRcaqOALQbSelKVfMCuzNTGjZ
:einstein.oftc.net 005 a37[7]FROGGY-PC-Matt[1329] UHNAMES NAMESX SAFELIST HCN
MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,l:60 NICKLEN=30 CHANNELLEN=32
TOPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported by this server
:einstein.oftc.net 006 a37[7]FROGGY-PC-Matt[1329] WALL CHOPS WATCH_128 WATCHOPS_A
```

Shown above: IRC traffic on TCP port 443 showing the user's IP address.

NOTE: I've edited the pcap, so it doesn't show the actual IP address the infected host was actually using.

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

You can look up that IP address and see it's a Brazil-based IP. You can also check one of the google search URLs from the pcap, and you'll see **www.google.com.br** as the domain, which is Google for Brazil.

If you're on an IP in Brazil, if you type google.com in the address bar, your browser will go to **www.google.com.br**. It's the same for IP addresses based in other countries.

Filter:	http.request	▼	Expression...	Clear	Apply	Save
Time	Dst	port	Host	Info		
2016-12-17 02:35:25	65.181.112.240	80	api.devyatinskiy.ru	GET /temer/de		
2016-12-17 02:47:25	216.58.202.14	80	google.com	GET / HTTP/1		
2016-12-17 02:47:26	187.33.247.102	80	www.google.com.br	GET /?gfe_rd=		
2016-12-17 02:47:32	158.69.99.213	80	log.houselannister.top	POST /mestre		
2016-12-17 02:48:20	187.33.247.102	80	www.google.com.br	GET /url?sa=t		
2016-12-17 02:48:21	131.247.120.45	80	etc.usf.edu	GET /lit2go/5/		
2016-12-17 02:48:22	131.247.120.45	80	etc.usf.edu	GET /lit2go/cs		
2016-12-17 02:48:23	131.247.120.45	80	etc.usf.edu	GET /lit2go/is		

Shown above: **google.com.br** domain indicates this traffic is from Brazil-based IP.

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
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
Connection: Keep-Alive
Host: google.com
Cookie: NID=92=r1MLTCDqC0ikrEwqVorRx0PbDmD69Tu4Zth3SXhe1HTJQAz_Va5n8-
pSCpgriDU7Ee3KM_StOusfUmi3Etr8GEh5dTv1ui8WCxRT_xqM9V24ccdLoAT9jSwNQ1D6oie0;
OGPC=883864576-2:

HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Location: http://www.google.com.br/?gfe_rd=cr&ei=PadUWP-ZI8jK8ge7pZ-ABg
Content-Length: 262
Date: Sat, 17 Dec 2016 02:47:25 GMT

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
```

Shown above: **google.com** redirecting to **www.google.com.br**.

INVESTIGATION

The Snort and Suricata alerts won't tell you much about what happened. The pcap has already been submitted to Virus Total, and you can review the IDS alerts on the traffic.

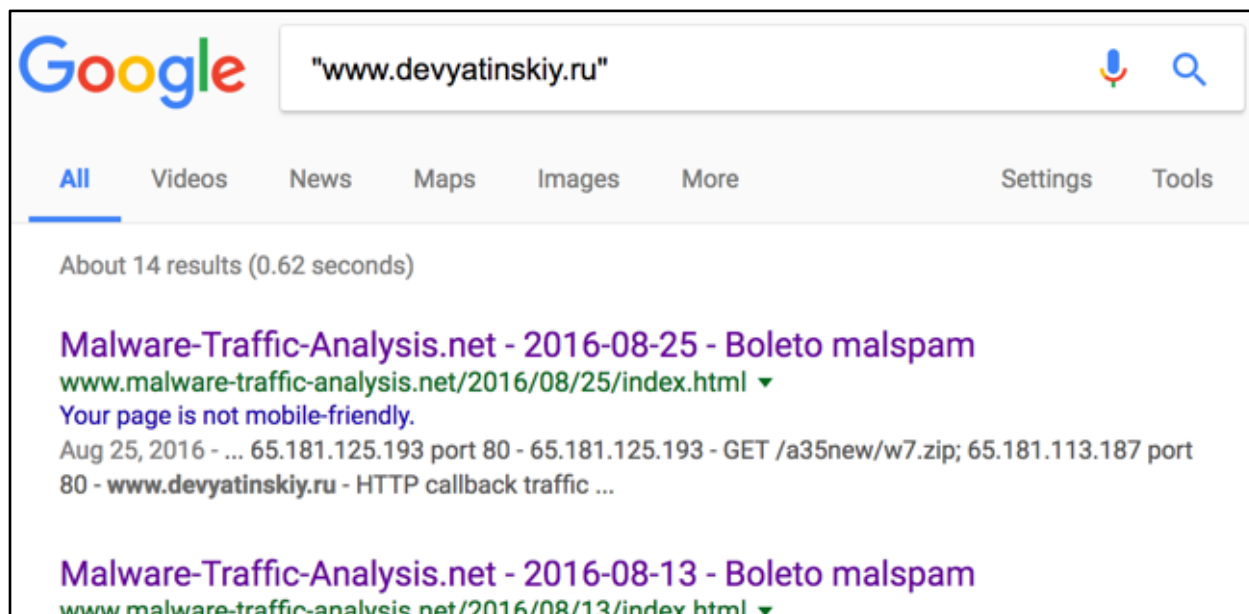
- <https://www.virustotal.com/en/file/cf9ab6a3e40a1c73d14fe28b572aefefe4bc21333f7712a3f2aca52c847c525f/analysis/>

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

Suricata alerts	Emerging Threats ETPro ruleset
ET CHAT IRC authorization message (Misc activity) [2000355]	
ET POLICY IRC connection (Misc activity) [2000356]	
ETPRO TROJAN Common Downloader Header Pattern H (Unknown Traffic) [2803305]	
ET POLICY exe download via HTTP - Informational (Potential Corporate Privacy Violation) [2003595]	
ET POLICY Reserved Internal IP Traffic (Potentially Bad Traffic) [2002752]	
ET TROJAN IRC Channel JOIN on non-standard port (A Network Trojan was Detected) [2000348]	
ETPRO POLICY 4shared SSL Certificate detected (A Network Trojan was Detected) [2806057]	
ET TROJAN Windows executable base64 encoded (A Network Trojan was Detected) [2018856]	
ET TROJAN Mikey Variant HTTP CnC Beacon 3 (A Network Trojan was Detected) [2020835]	
ET POLICY exe download without User Agent (Potential Corporate Privacy Violation) [2003179]	
CPL WEB_CLIENT web bug 0x0.gif attempt (Misc activity) [2010005]	

Shown above: Suricata events from the exercise pcap on Virus Total

I'm not sure what a Mikey variant is. But try a Google search on some of the domains in the pcap, and you'll run eventually run across some of my blog posts.



Shown above: Google searching is your friend.

You can read through my previous blog posts on this infection traffic to get a better idea what is happening. I haven't identified it as part of any specific malspam campaign yet. But it's not normal. This is the type of traffic where someone has infected a Windows host with command and control channel established through IRC.