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/16122016xoGuI9iOhm1WwDLLwlkxwX.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

- 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/infects/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

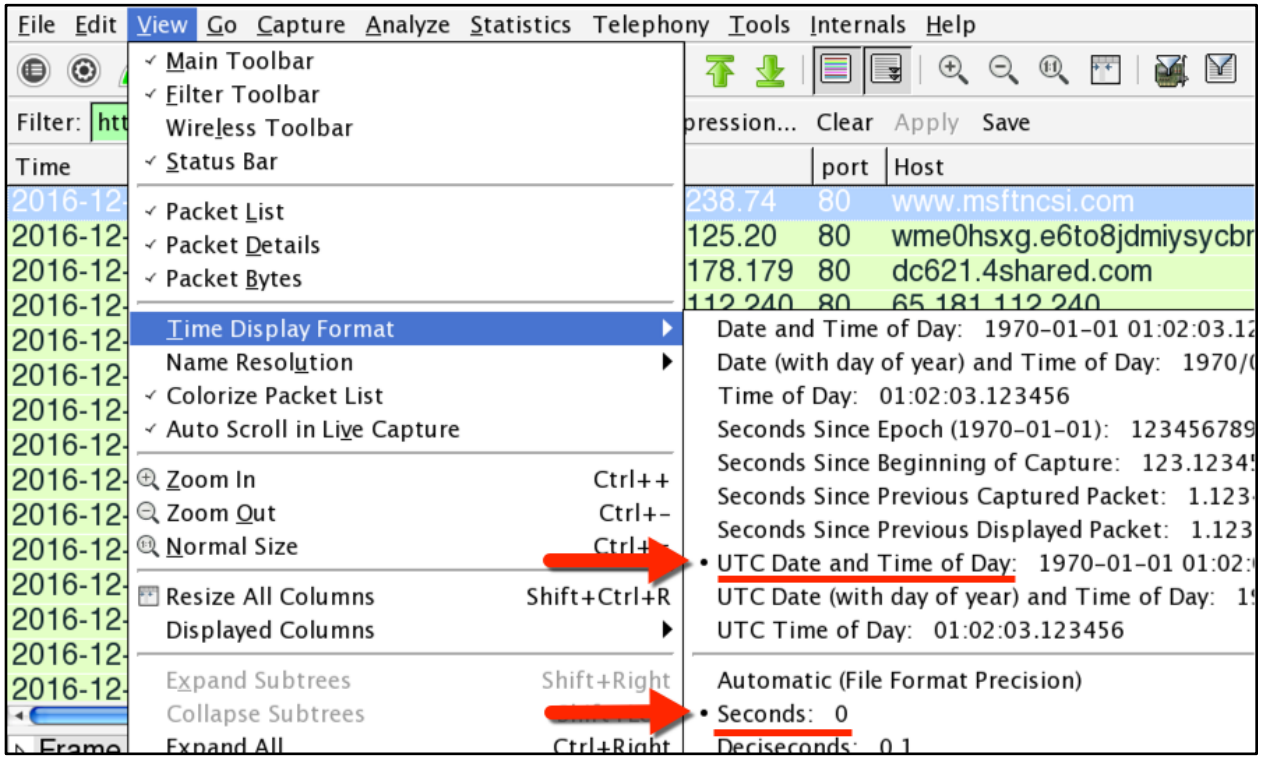
Post-infection IRC traffic:

- 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.

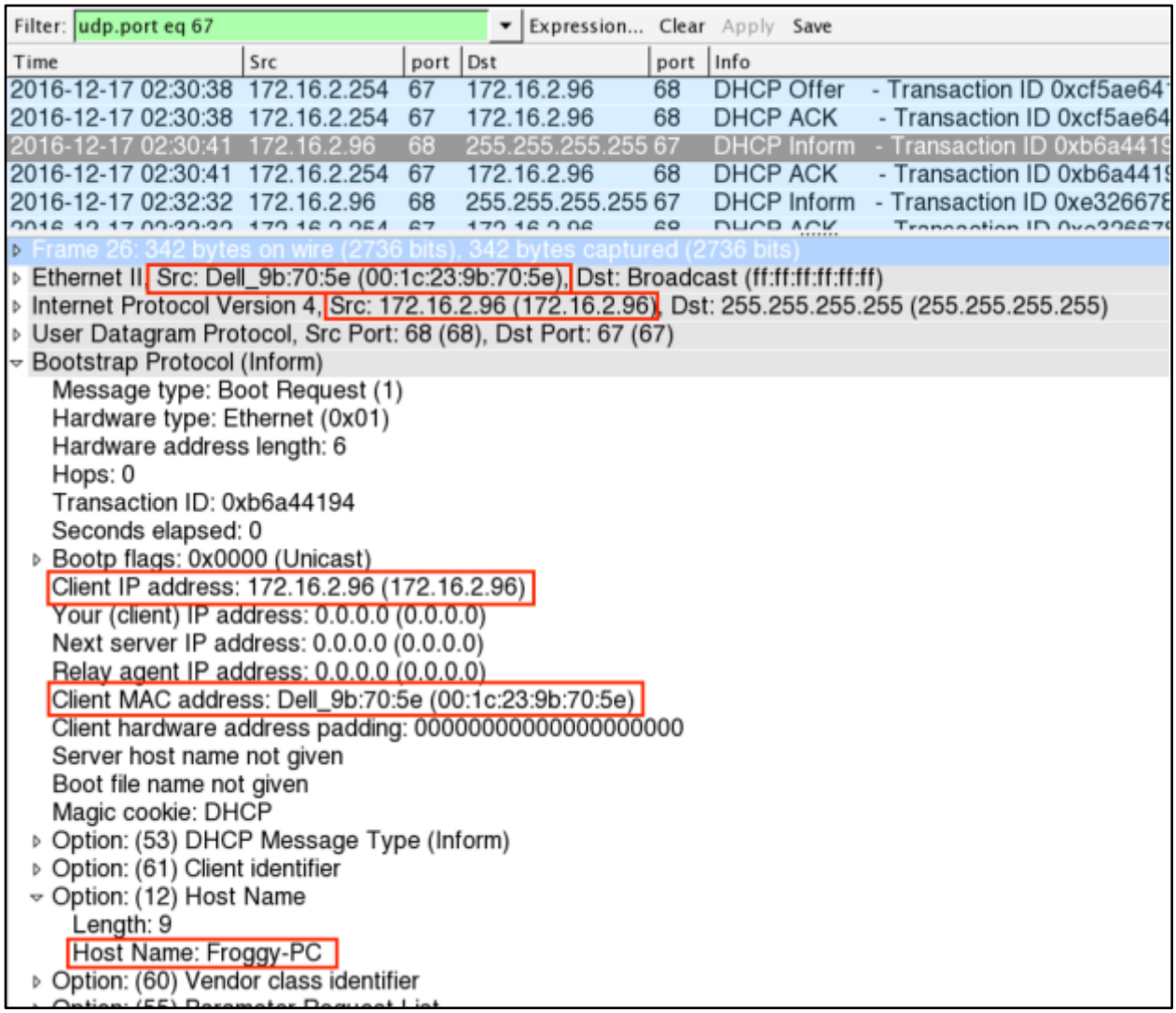


Shown above: Ensuring your time is displaying correctly in Wireshark.

2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

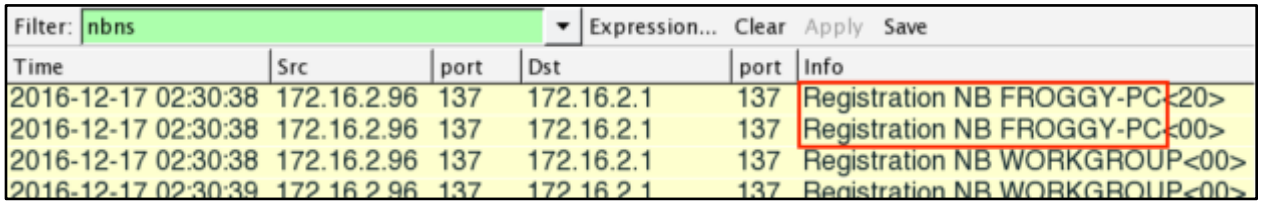
Note that you'll also want to make sure it shows as UTC for the display columns under the Wirshark .

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.k Use the Wireshark filter **udp.port eq 67** and look at the packet and frame details as seen in the image below.



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

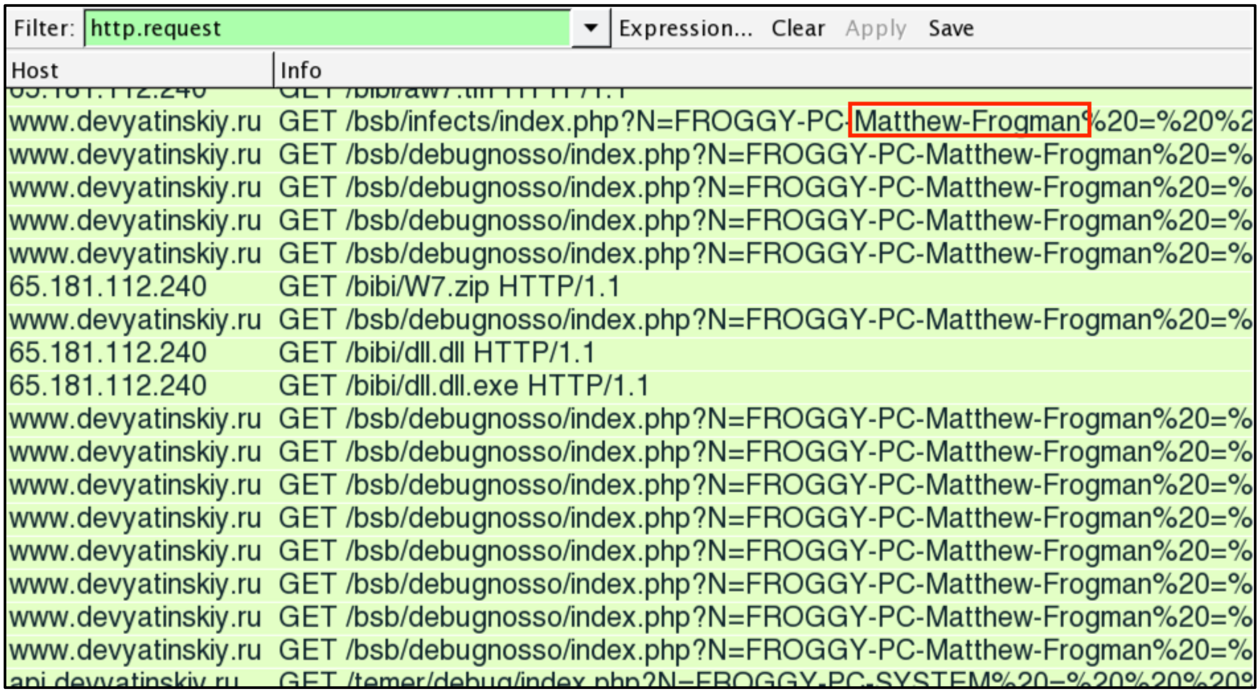
Since this is a Windows host, you can also get the host name from the NBNS traffic.



Shown above: Host name in NBNS traffic.

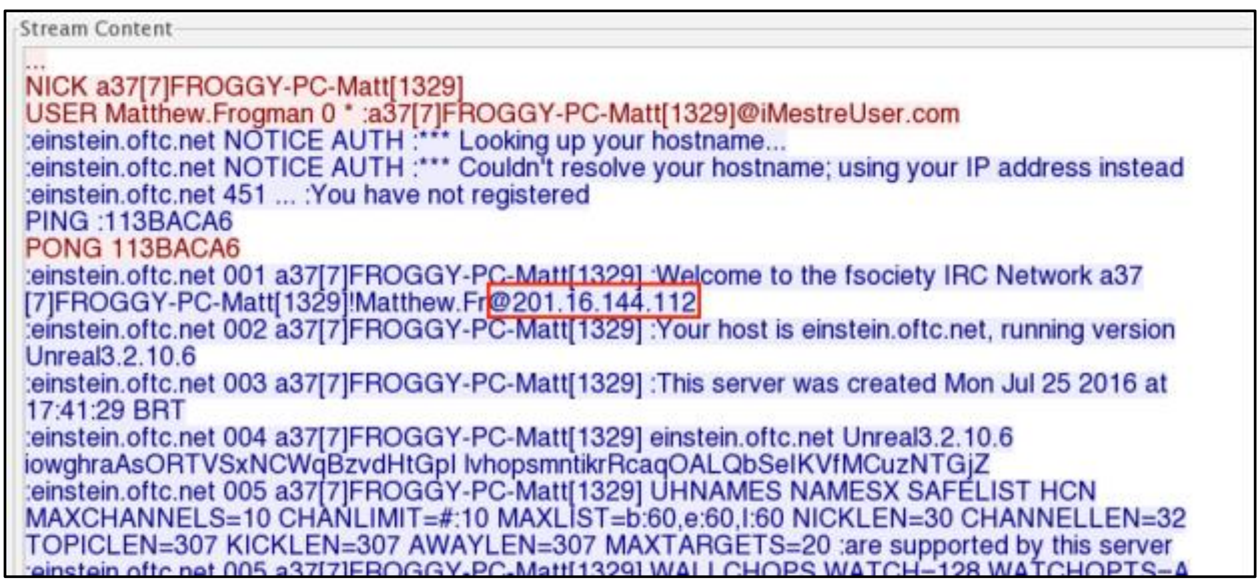
2016-12-17 TRAFFIC ANALYSIS EXERCISE - ANSWERS

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.



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.

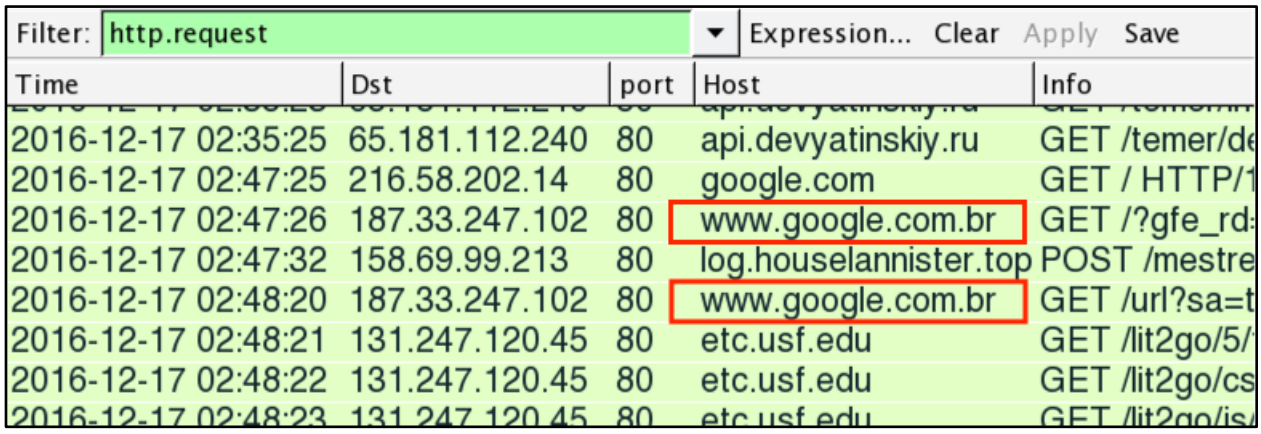


Shown above: IRC traffic on TCP port 443 showing the user's IP address.

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

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.



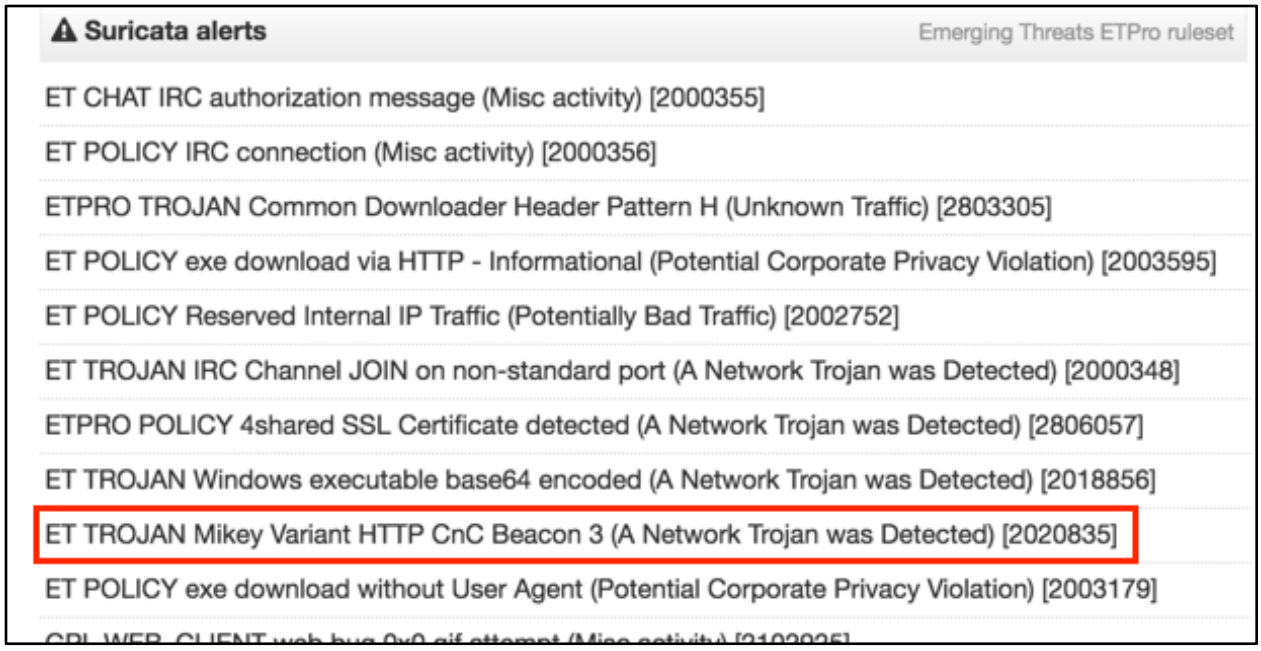
Shown above: ***google.com.br*** *domain indicates this traffic if from Brazil-based IP.*

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

INVESTIGATION

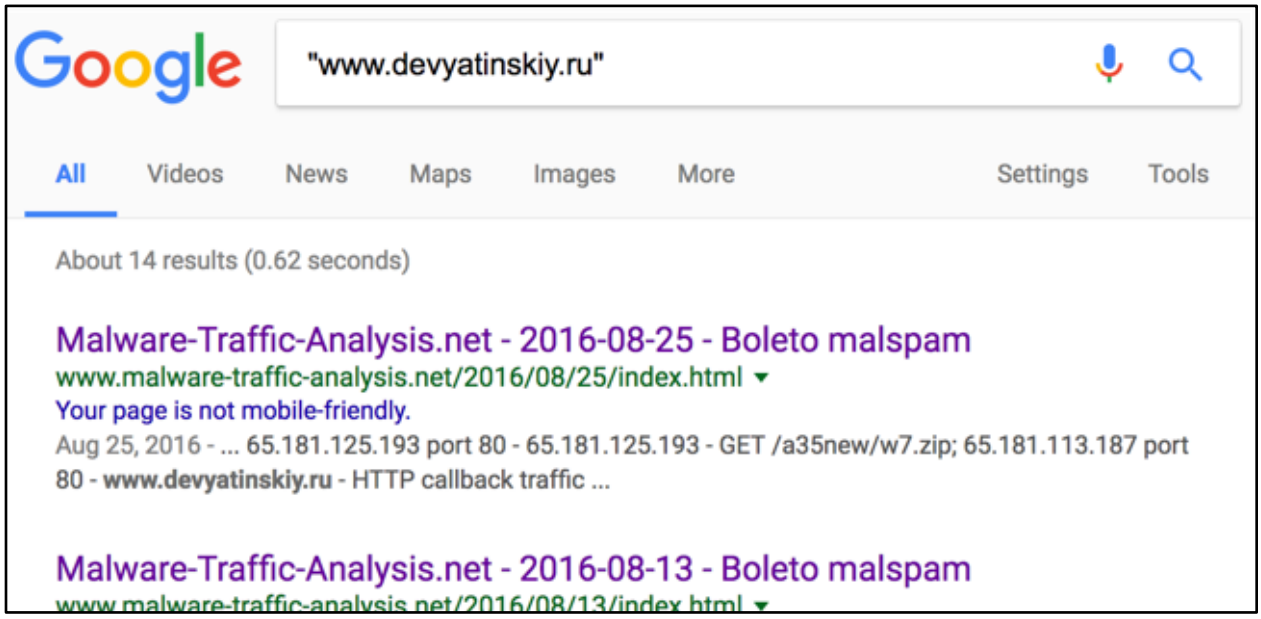
The Snort and Suricata alerts won't tell you much about what happened. The pcap has already been submitted to Virus Total, and you can review the IDS alerts on the traffic.

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



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.