



University  
of Victoria

**ECE 570**  
**Project III: Network Forensics Investigation**



**Somayeh Roshandel V00942553**

**Behnaz Saropourian V00857804**

**August 2020**



<b>1. Identify the following characteristics for the infected host :</b>	<b>3</b>
<b>2. What is the IP address and URL of the compromised website the user looked at that triggered the malware traffic (i.e. before the malware traffic happened)?</b>	<b>8</b>
<b>3. What is the IP address and domain name that delivered the malware?</b>	<b>47</b>
<b>4. Identify the type of malware involved and check the payload by running the associated file (or files) against an online virus checker (i.e. VirusTotal).</b>	<b>102</b>
<b>5. Identify other malicious hosts or sites with which the compromised host interacted. Only malicious hosts should be included in this list. Provide your response in a table listing the following.</b>	<b>129</b>
<b>6. Give an outline of the attack scenario by describing it in a few paragraphs and by providing a graphical sketch. The attack scenario must include both the infection and post-infection steps</b>	<b>139</b>
<b>7. Discuss remediation and mitigation solutions for such threats.</b>	<b>141</b>





1. Identify the following characteristics for the infected host :

- a. IP address of computer
  - b. Hostname of computer
  - c. MAC address of computer
  - d. Operating System (OS)

In this scenario we did not have any DHCP packets. Fortunately, we can use NBNS traffic to identify hostnames for computers running Microsoft Windows or Apple hosts running MacOS.

This pcap is from a Windows host using an IP address at 192.168.122.62. Open the pcap in Wireshark and filter on ***nbns***. This should reveal the NBNS traffic. Select the first frame, as shown

The host name is found here:



```
* Flags: 0x0000, Opcode: Name query
  0... .... .... = Response: Message is a query
  .000 0... .... = Opcode: Name query (0)
  .... .0 .... .... = Truncated: Message is not truncated
  .... ..0 .... .... = Recursion desired: Don't do query recursively
  .... ...0 .... .... = Broadcast: Not a broadcast packet
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
* Queries
  * <00><00><00><00><00><00><00><00><00><00><00><00><00><00>: type NBSTAT, class IN
    Name: *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00> (Workstation/Redirector)
    Type: NBSTAT (33)
    Class: IN (1)
```

IP address is 192.168.122.62 for host machine found here:

ip.dst == 78.129.168.237						
Title: Info		Type: Information	Fields: Enter a field ...			Occurrence:
No.	Time	Source	Destination	Protocol	Length	Info
-	1314 266.790028	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><.. 137
	1315 268.289454	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><.. 137
	1316 269.8803017	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><.. 137

.... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 78  
 Identification: 0x0267 (615)  
 Flags: 0x0000  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: UDP (17)  
 Header checksum: 0x05e3 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.122.62  
 Destination: 78.129.168.237  
 User Datagram Protocol, Src Port: 137, Dst Port: 137  
 Source Port: 137  
 Destination Port: 137  
 Length: 58

0010 00 4c 02 67 00 00 80 11 05 e3 c0 a8 7a 3e 8e 81 - N.g... .z>N.  
 WARNING: is the highest extent information layout

As can be seen that Mac-address is not valid and all octet detected by 0.

This is Mac spoofing or DNS hijacking.

A MAC spoofing attack is where the intruder sniffs the network for valid MAC addresses and attempts to act as one of the valid MAC addresses. The intruder then presents itself as the default gateway and copies all of the data forwarded to the default gateway without being detected. This provides the intruder valuable details about applications in use and destination host IP addresses.

In layer II, we can find MAC addresses. But here all data are changed to zero.

```
[Coloring Rule String: smb || nbss || nbns || netbios]
▼ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
  ▼ Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      .... ..0. .... ..... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... ..... .... = IG bit: Individual address (unicast)
  ▼ Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      .... ..0. .... ..... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... ..... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Based on Networkminer report on details of 216.58.210.68, on Host details, we found two Web Server Banner.

8 216.58.210.67 [www.google.co.uk] [ssl.gstatic.com] [clients-cctld.google.com] [clients1.google.co.uk]

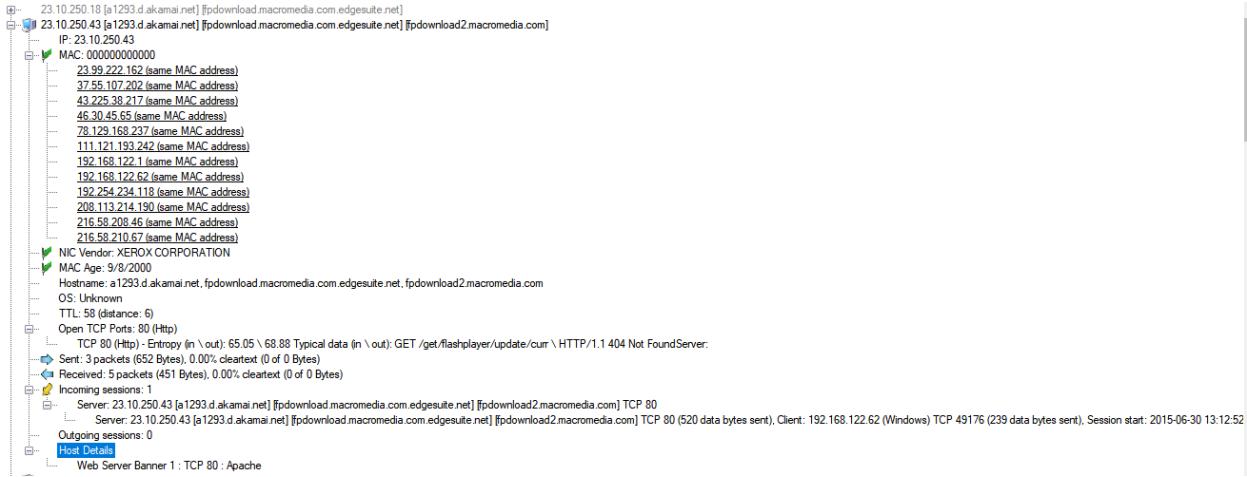
- IP: 216.58.210.67
- + MAC: 000000000000
- + NIC Vendor: XEROX CORPORATION
- + MAC Age: 9/8/2000
- Hostname: www.google.co.uk, ssl.gstatic.com, clients-cctld.google.com, clients1.google.co.uk
- OS: Unknown
- TTL: 56 (distance: 8)
- + Open TCP Ports: 80 (Http) 443 (Ssl)
- + Sent: 282 packets (303,765 Bytes), 0.00% cleartext (0 of 0 Bytes)
- + Received: 230 packets (42,008 Bytes), 0.00% cleartext (0 of 0 Bytes)
- + Incoming sessions: 12
- Outgoing sessions: 0
- + Host Details
  - favicon : C:\Users\behna\AppData\Local\Temp\Rar\$EXa5200.38723\NetworkMiner\_2-5\AssembledFiles\216.58.210.67\TCP-80\favicon.ico
  - Domain Name 1 : google.com
  - Web Server Banner 1 : TCP 80 : gws
  - Web Server Banner 2 : TCP 80 : sfge
  - X.509 Certificate Subject Alternative Name 1 : DNS Name=www.google.co.uk
  - X.509 Certificate Subject Alternative Name 10 : DNS Name=\*.google.co.jp
  - X.509 Certificate Subject Alternative Name 11 : DNS Name=\*.google.co.uk
  - X.509 Certificate Subject Alternative Name 12 : DNS Name=\*.google.com.ar
  - X.509 Certificate Subject Alternative Name 13 : DNS Name=\*.google.com.au
  - X.509 Certificate Subject Alternative Name 14 : DNS Name=\*.google.com.br
  - X.509 Certificate Subject Alternative Name 15 : DNS Name=\*.google.com.co
  - X.509 Certificate Subject Alternative Name 16 : DNS Name=\*.google.com.mx
  - X.509 Certificate Subject Alternative Name 17 : DNS Name=\*.google.com.tr
  - X.509 Certificate Subject Alternative Name 18 : DNS Name=\*.google.com.vn
  - X.509 Certificate Subject Alternative Name 19 : DNS Name=\*.google.de
  - X.509 Certificate Subject Alternative Name 2 : DNS Name=\*.google.com
  - X.509 Certificate Subject Alternative Name 20 : DNS Name=\*.google.es
  - X.509 Certificate Subject Alternative Name 21 : DNS Name=\*.google.fr

A **server banner** is a particular greeting message sent by a **server** running on a host. It is very important to hide this information as it may contain important strings that can



help an attacker to find breaks on your system. This tool shows you the banners sent by popular services over the internet. **Server banner** check.

And also we can found that in Network miner Web server banner use here, in screen shot is shown:



The attacker uses 23.10.250.43 and the server IP address is 23.10.250.18. The name is a.1293.d.akamai.net on TCP port 80 use Web Server Banner 1 to DNS hijacking and Mac spoofing.



In wireshark if right click on the IP address that is hosted and go to Follow/TCP stream . In this page we found Operating System information. The screenshot of operating system of host found based on wireshark capture is as follows:

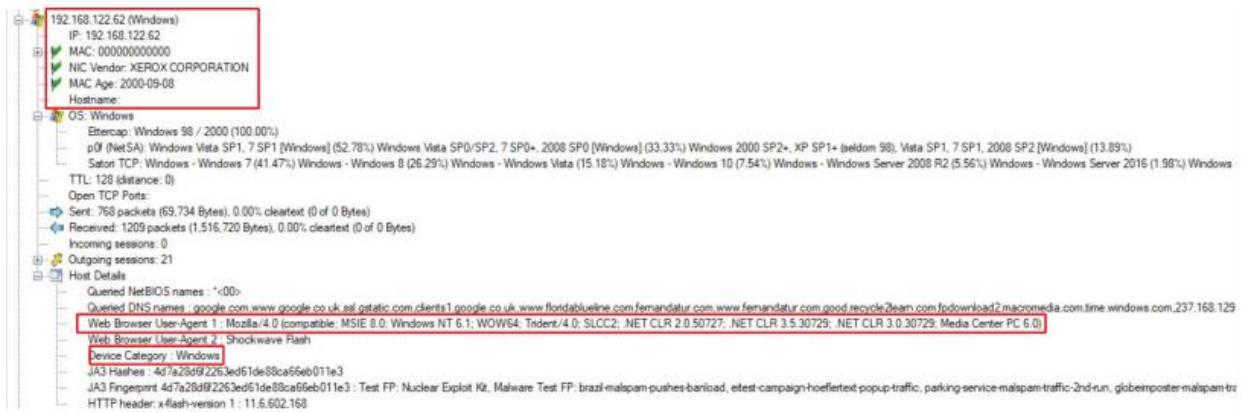


```
Wireshark - Follow TCP Stream (tcp.stream eq 0) · ECE570-2020-project3.pcap
```

```
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, /*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: google.com
Connection: Keep-Alive
```

Windows NT 6.1 represents windows 7. So, the operating system of host with ip address 192.168.122.62 is Windows 7.

Also according to network miner report, we found information about the infected host such as operating system, IP address, web browser as following picture:



192.168.122.62 (Windows)

- IP: 192.168.122.62
- MAC: 000000000000
- NIC Vendor: XEROX CORPORATION
- MAC Age: 2000-09-08
- Hostname:

OS: Windows

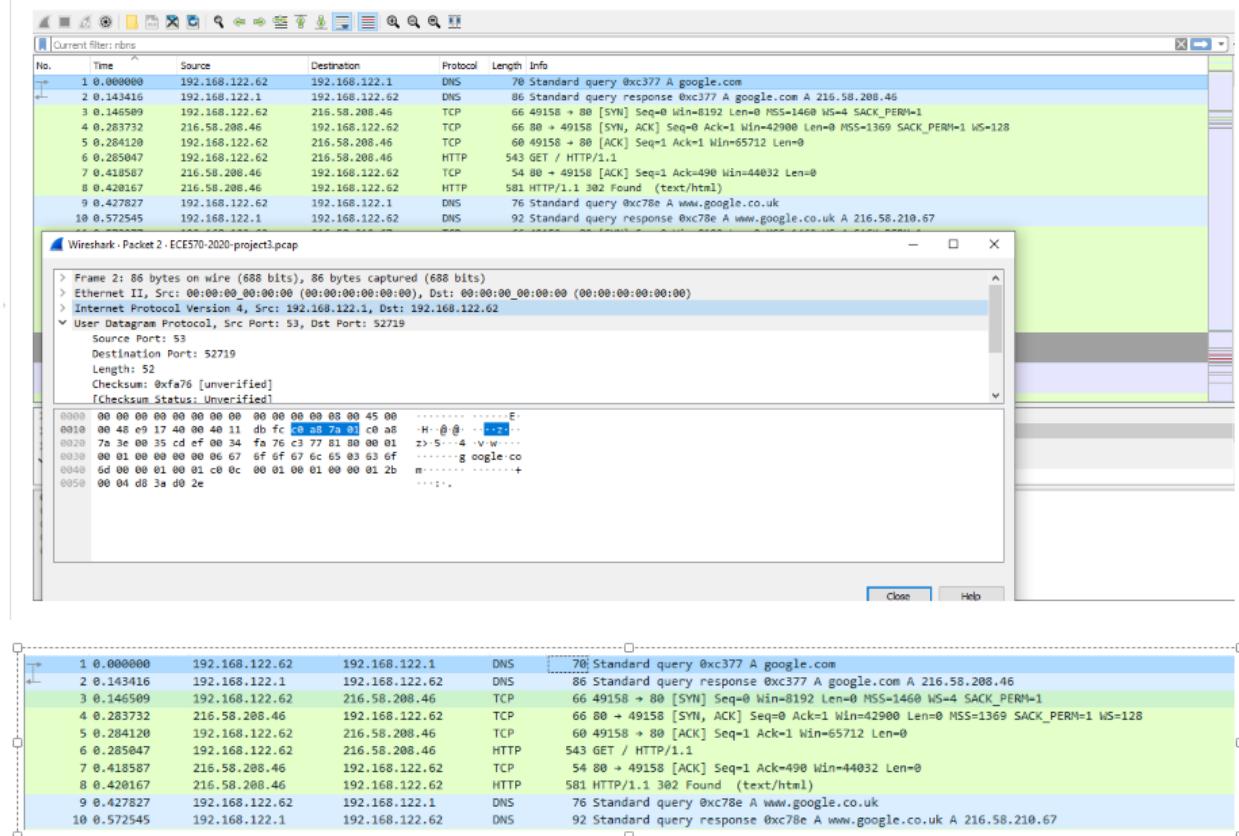
- Ethercap: Windows 98 / 2000 (100.00%)
- p0f (NetSA): Windows Vista SP1, 7 SP1 [Windows] (52.78%) Windows Vista SP0/SP2, 7 SP0+ [Windows] (33.33%) Windows 2000 SP2+, XP SP1+ (seldom 98), Vista SP1, 7 SP1, 2008 SP2 [Windows] (13.89%)
- Satos: TCP: Windows - Windows 7 (41.47%) Windows - Windows 8 (26.29%) Windows - Windows Vista (15.18%) Windows - Windows 10 (7.54%) Windows - Windows Server 2008 R2 (5.56%) Windows - Windows Server 2016 (1.98%) Windows
- TTL: 128 (distance: 0)
- Open TCP Ports:
- Sent: 768 packets (69,734 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Received: 1209 packets (1,516,720 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Incoming sessions: 0
- Outgoing sessions: 21

Host Details

- Queried NetBIOS names: -<00>
- Queried DNS names: google.com, www.google.co.uk, www.gatatic.com, clients1.google.co.uk, www.floridablueline.com, www.femandatur.com, www.femandatur.com, good.recycleteam.com, fodownload2.macromedia.com, time.windows.com, 237.168.129
- Web Browser User-Agent 1: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
- Web Browser User-Agent 2: Shockwave Flash
- Device Category: Windows
- JAH Hashes: 4d7a2bd92263ed61de88ca66eb011e3
- JAH Fingerprint: 4d7a2bd92263ed61de88ca66eb011e3 : Test FP: Nuclear Exploit Kit, Malware Test FP: brazil-malspam-pushes-barload, e-test-campaign-hoefle-text-popup-traffic, parking-service-malspam-traffic-2nd-run, globeimposter-malspam-tr
- HTTP header: x-flash-version 1; 11.6.602.168

2. What is the IP address and URL of the compromised website the user looked at that triggered the malware traffic (i.e. before the malware traffic happened)?

The scenario starts from first frame in wireshark capture



Wireshark - Packet 2 - ECE570-2020-project3.pcap

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)  
 Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)  
 Internet Protocol Version 4, Src: 192.168.122.1, Dst: 192.168.122.62  
 User Datagram Protocol, Src Port: 53, Dst Port: 52719  
 Source Port: 53  
 Destination Port: 52719  
 Length: 52  
 Checksum: 0xfa76 [unverified]  
 [Checksum Status: Unverified]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.122.62	192.168.122.1	DNS	76	Standard query 0xc377 A google.com
2	0.143416	192.168.122.1	192.168.122.62	DNS	86	Standard query response 0xc377 A google.com A 216.58.208.46
3	0.146509	192.168.122.62	216.58.208.46	TCP	66	49158 + 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.283732	216.58.208.46	192.168.122.62	TCP	66	80 + 49158 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1369 SACK_PERM=1 WS=128
5	0.284120	192.168.122.62	216.58.208.46	TCP	66	49158 + 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
6	0.285047	192.168.122.62	216.58.208.46	HTTP	543	GET / HTTP/1.1
7	0.418587	216.58.208.46	192.168.122.62	TCP	54	80 + 49158 [ACK] Seq=1 Ack=490 Win=44032 Len=0
8	0.420167	216.58.208.46	192.168.122.62	HTTP	581	HTTP/1.1 302 Found (text/html)
9	0.427827	192.168.122.62	192.168.122.1	DNS	76	Standard query 0xc78e A www.google.co.uk
10	0.572545	192.168.122.1	192.168.122.62	DNS	92	Standard query response 0xc78e A www.google.co.uk A 216.58.210.67

Here 192.168.122.62 target of suspected malware attack sent an packet to 192.168.122.1 as a DNS server for open google.com  
 A milli seconds later 192.168.122.1 replay to host request. And three TCP handshaking between host and google website done. Then in frame 6 the GET is a Hypertext Transfer Protocol command to ask for data from an HTTP Server.  
 In frame 8, the response of frame 6 indicates the HyperText Transfer Protocol (HTTP) **302 Found**. It means that redirect status response code indicates that the resource requested has been temporarily moved to the URL given by the Location header.



So another google website ip address for google.co.uk sent to the host.  
Here prove that the host is from the UK.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.122.62	192.168.122.1	DNS	78	Standard query 0xc377 A google.com
2	0.143416	192.168.122.1	192.168.122.62	DNS	86	Standard query response 0xc377 A google.com A 216.58.208.46
3	0.146589	192.168.122.62	216.58.208.46	TCP	66	49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.283732	216.58.208.46	192.168.122.62	TCP	66	80 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1369 SACK_PERM=1 WS=128
5	0.284120	192.168.122.62	216.58.208.46	TCP	60	49158 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
6	0.285047	192.168.122.62	216.58.208.46	HTTP	543	GET / HTTP/1.1
7	0.418587	216.58.208.46	192.168.122.62	TCP	54	80 → 49158 [ACK] Seq=1 Ack=499 Win=44032 Len=0
8	0.420167	216.58.208.46	192.168.122.62	HTTP	581	HTTP/1.1 302 Found (text/html)
9	0.427827	192.168.122.62	192.168.122.1	DNS	78	Standard query 0xc78e A www.google.co.uk
10	0.572545	192.168.122.1	192.168.122.62	DNS	92	Standard query response 0xc78e A www.google.co.uk A 216.58.210.67
11	0.573977	192.168.122.62	216.58.210.67	TCP	66	49159 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
12	0.628749	192.168.122.62	216.58.208.46	TCP	66	49158 → 80 [ACK] Seq=490 Ack=528 Win=65184 Len=0
13	0.703413	216.58.210.67	192.168.122.62	TCP	66	80 → 49159 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1369 SACK_PERM=1 WS=128
14	0.703768	192.168.122.62	216.58.210.67	TCP	60	49159 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
15	0.704222	192.168.122.62	216.58.210.67	HTTP	585	GET /?gfe_rd=cr&ei=15WSVaXXFrPj8wfRnYHACw HTTP/1.1
16	0.834170	216.58.210.67	192.168.122.62	TCP	54	80 → 49159 [ACK] Seq=532 Ack=532 Win=44032 Len=0
17	0.849882	216.58.210.67	192.168.122.62	HTTP	1187	HTTP/1.1 302 Found (text/html)

According to information from NetworkMiner and packet total and also wireshark capture report, all communication via TCP, TLSv1.2 are normal till frame 512 that host request for floridablueline.com

In this screenshot information about SSL Certificates are indicates the time between 13:11:52 to 13:11:57 is during access to google.co.uk

Malicious Activity   Suspicious Activity   Connections   DNS   HTTP   **SSL Certificates**   PKI (X.509)   Transferred Files   Strange Activity   Community Tags

Similar Packet Captures

Q Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Version	Cipher	Curve
2015-08-30 13:11:52 Z	CliqRc3Kwi3x2Qr2AT3	192.168.122.62	49160	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-08-30 13:11:52 Z	CKRq1rfuifofuuu79	192.168.122.62	49161	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-08-30 13:11:53 Z	CHF3ut1O2Bfav6Dg6i	192.168.122.62	49162	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-08-30 13:11:53 Z	CAJS742AnYq0RYa281	192.168.122.62	49164	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-08-30 13:11:53 Z	CbkHf3lny13n7mo6	192.168.122.62	49163	216.58.210.67	443	TLSv12	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	secp256r1
2015-08-30 13:11:54 Z	CS0cRC2zWbi1T0kdh	192.168.122.62	49165	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-08-30 13:11:57 Z	CB1rXq4rFuMENusE9	192.168.122.62	49166	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-08-30 13:11:57 Z	CoBZSm1VZZeAr1hQJ4	192.168.122.62	49167	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-08-30 13:11:57 Z	CpVrsfMUC2HX1Mlc	192.168.122.62	49168	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1
2015-08-30 13:11:57 Z	CimG1k34bfUfsxyVMd	192.168.122.62	49169	216.58.210.67	443	TLSv12	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256r1

And in search engine of this site ([www.google.co.uk](http://www.google.co.uk)) host write down and was going to open (access) to floridablueline.com

Frame	Source IP	Destination IP	Protocol	Content
512 53.0.35632	192.168.122.62	216.58.210.67	HTTP	932 GET /url?url=http://www.floridablueline.com/&ct=j&frm=1&q=&src=s&sa=U&ei=q5w5VeODFNPtyg0-goCgBQ&ved=0CBQQ..
513 53.174647	216.58.210.67	192.168.122.62	TCP	54 88 → 49170 [ACK] Seq=1 Ack=879 Win=44672 Len=0
514 53.207113	216.58.210.67	192.168.122.62	HTTP	856 HTTP/1.1 200 OK (text/html)
515 53.233025	192.168.122.62	216.58.210.67	HTTP	586 GET /favicon.ico HTTP/1.1
516 53.288100	192.168.122.62	192.168.122.1	DNS	83 Standard query 0xf29b A www.floridablueline.com
517 53.368358	216.58.210.67	192.168.122.62	TCP	1423 88 → 49170 [ACK] Seq=803 Ack=1411 Win=46464 Len=1369 [TCP segment of a reassembled PDU]
518 53.368405	216.58.210.67	192.168.122.62	HTTP	78 HTTP/1.1 200 OK (image/x-icon)
519 53.368961	192.168.122.62	216.58.210.67	TCP	68 49170 → 88 [ACK] Seq=1411 Ack=2188 Win=65712 Len=0
520 53.569309	192.168.122.1	192.168.122.62	DNS	113 Standard query response 0xf29b A www.floridablueline.com CNAME floridablueline.com A 192.254.234.118
521 53.570661	192.168.122.62	192.254.234.118	TCP	66 49171 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1468 WS=4 SACK_PERM=1
522 53.826907	192.254.234.118	192.168.122.62	TCP	66 88 → 49171 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1369 SACK_PERM=1 WS=128
523 53.827291	192.168.122.62	192.254.234.118	TCP	60 49171 → 88 [ACK] Seq=1 Ack=1 Win=65712 Len=0
524 53.827825	192.168.122.62	192.254.234.118	HTTP	736 GET / HTTP/1.1
525 54.086462	192.254.234.118	192.168.122.62	TCP	54 88 → 49171 [ACK] Seq=1 Ack=683 Win=30592 Len=0
526 54.217787	192.254.234.118	192.168.122.62	TCP	776 88 → 49171 [PSH, ACK] Seq=1 Ack=683 Win=30592 Len=722 [TCP segment of a reassembled PDU]
527 54.217844	192.254.234.118	192.168.122.62	HTTP	74 HTTP/1.1 200 OK (text/html)
528 54.218472	192.168.122.62	192.254.234.118	TCP	60 49171 → 88 [ACK] Seq=683 Ack=743 Win=64966 Len=0
529 54.225439	192.168.122.62	192.254.234.118	HTTP	435 GET /floridabluelineheader.jpg HTTP/1.1
530 54.236543	192.168.122.62	192.168.122.1	DNS	75 Standard query 0x8120 A fernandatur.com
531 54.467429	192.168.122.1	192.168.122.62	DNS	91 Standard query response 0x9120 A fernandatur.com A 208.113.214.190

According to the wireshark and network miner report, after clicking or accessing an image via floridablueline.com.

In frame number 512 in Wireshark, the host machine asks for data from HTTP server.  
In frame 515, host request for favicon.ico from HTTP server with GET HTTP1.1 .

### Note **HTTP1.1:**

The HyperText Transport Protocol is a text-based request-response client-server protocol. A HTTP client (e.g. a web browser such as Mozilla) performs a HTTP request to a HTTP server (e.g. the Apache HTTP server), which in return will issue a HTTP response. The HTTP protocol header is text-based, where headers are written in text lines.

HTTP/1.1 allows for client-server connections to be pipelined, whereby multiple requests can be sent (often in the same packet), without waiting for a response from the server. The only restriction is the server MUST return the responses in the same order as they were received. This enables greater efficiency, especially on revalidation.

The below screenshots indicate that the floridablueline.com host machine requested two pictures, one of them icon (favicon.co) and the other one is header of site (floridabluelineheader.jpg).





512	2015-06-30	13:12:44:	085352	192.168.122.62	216.58.210.67	HTTP	932	GET /url?url=http://www.floridablueline.com/?rct=j&frm=1&q=esrc=s+sa+U+ei=q5WSvEODFMPYg0+goCgBQ&ved=0
513	2015-06-30	13:12:44:	224367	216.58.210.67	192.168.122.62	TCP	54	80 → 49170 [ACK] Seq=1 Ack=879 Win=44672 Len=0
514	2015-06-30	13:12:44:	256833	216.58.210.67	192.168.122.62	HTTP	859	HTTP/1.1 200 OK (text/html)
515	2015-06-30	13:12:44:	282745	192.168.122.62	216.58.210.67	HTTP	585	GET /favicon.ico HTTP/1.1
516	2015-06-30	13:12:44:	329820	192.168.122.62	192.168.122.1	DNS	83	Standard query 0x29b A www.floridablueline.com
517	2015-06-30	13:12:44:	418876	216.58.210.67	192.168.122.62	TCP	1423	80 → 49170 [ACK] Seq=803 Ack=1411 Win=46464 Len=1369 [TCP segment of a reassembled PDU]
518	2015-06-30	13:12:44:	418123	216.58.210.67	192.168.122.62	TCP	79	HTTP/1.1.200 OK (image/x-icon)
519	2015-06-30	13:12:44:	418681	192.168.122.62	216.58.210.67	TCP	60	49170 → 80 [ACK] Seq=1411 Ack=2188 Win=65712 Len=0
520	2015-06-30	13:12:44:	619892	192.168.122.11	192.168.122.62	DNS	113	Standard query response 0x29b A www.floridablueline.com CNAME floridablueline.com A 192.254.234.118
521	2015-06-30	13:12:44:	620381	192.168.122.62	192.254.234.118	TCP	60	49171 → 80 [SYN] Seq=Win=81922 Ack=14604 WS=4 SACK_PERM=1
522	2015-06-30	13:12:44:	876627	192.254.234.118	192.168.122.62	TCP	60	80 → 49171 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1369 SACK_PERM=1 WS=128
523	2015-06-30	13:12:44:	877011	192.168.122.62	192.254.234.118	TCP	60	49171 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
524	2015-06-30	13:12:44:	877545	192.168.122.62	192.254.234.118	HTTP	736	GET / HTTP/1.1
525	2015-06-30	13:12:45:	136182	192.254.234.118	192.168.122.62	TCP	54	80 → 49171 [ACK] Seq=1 Ack=683 Win=30592 Len=0
526	2015-06-30	13:12:45:	267597	192.254.234.118	192.168.122.62	TCP	776	80 → 49171 [PSH, ACK] Seq=1 Ack=683 Win=30592 Len=722 [TCP segment of a reassembled PDU]
527	2015-06-30	13:12:45:	267564	192.254.234.118	192.168.122.62	HTTP	74	HTTP/1.1.200 OK (text/html)
528	2015-06-30	13:12:45:	268192	192.168.122.62	192.254.234.118	TCP	60	49171 → 80 [ACK] Seq=683 Ack=743 Win=44968 Len=0

Both pictures are shown in Networkminer report.

And also, we check both pictures linked on virustotal.com which are clean. Screen shots of virustotal and wireshark about those pictures as a following pictures:

This site is clean and safe <http://www.google.co.uk/favicon.ico>

The Wireshark interface displays a list of network packets. The first five packets are highlighted in green, indicating they are part of the same session. The selected packet is number 515, which is a GET request for the favicon.ico file from the website www.google.co.uk. The packet details pane shows the HTTP headers and the truncated cookie value.

No.	Time	Source	Destination	Protocol	Length	Info
512	2015-06-30 13:12:44.085352	192.168.122.62	216.58.210.67	HTTP	932	GET /ur1?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5iSVeODFMPYtg0-goCgBQ&ved...
513	2015-06-30 13:12:44.224367	216.58.210.67	192.168.122.62	TCP	54	80 → 49170 [ACK] Seq=1 Ack=879 Win=44672 Len=0
514	2015-06-30 13:12:44.256833	216.58.210.67	192.168.122.62	HTTP	856	HTTP/1.1 200 OK (text/html)
515	2015-06-30 13:12:44.282745	192.168.122.62	216.58.210.67	HTTP	586	GET /favicon.ico HTTP/1.1

Wireshark - Packet 515 - ECE570-2020-project3.pcap

Accept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6. Host: www.google.co.uk\r\nConnection: Keep-Alive\r\n> [truncated]Cookie: PREF=ID=1111111111111111:FF=0:TM=1435669911:LM=1435669911:V=1:S=irGPM4gmcurKWhpe; NID=68=jXeeyRBMr1lR6NOHTIsioGVRdfQLZu9BKUlw5vSeguUxX4E-\_M\_v2srei\r\n\r\n[Full request URI: http://www.google.co.uk/favicon.ico]  
[HTTP request 2/2]  
[Prev request in frame: 512]  
[Response in frame: 518]

https://www.google.co.uk/favicon.ico

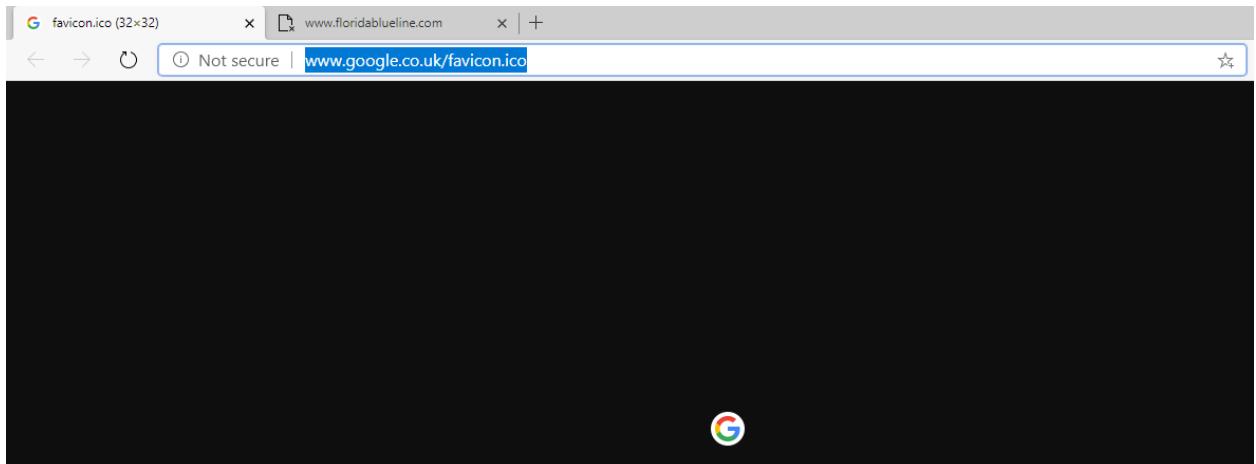
No engines detected this URL

https://www.google.co.uk/favicon.ico  
www.google.co.uk

200 Status | image/x-icon Content Type | 2020-07-24 12:38:40 UTC  
7 days ago

Community Score

DETECTION	DETAILS	COMMUNITY
ADMINUSLabs	<span>✓ Clean</span>	AegisLab WebGuard <span>✓ Clean</span>
AlienVault	<span>✓ Clean</span>	Anty-AVL <span>✓ Clean</span>
Artists Against 419	<span>✓ Clean</span>	Avira (no cloud) <span>✓ Clean</span>
BADWARE.INFO	<span>✓ Clean</span>	Baidu-International <span>✓ Clean</span>
BitDefender	<span>✓ Clean</span>	BlockList <span>✓ Clean</span>
Blueliv	<span>✓ Clean</span>	Botvrij.eu <span>✓ Clean</span>
Certego	<span>✓ Clean</span>	CINS Army <span>✓ Clean</span>





ECE570-2020-project3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
527	2015-06-30 13:12:45.267564	192.254.234.118	192.168.122.62	HTTP	74	HTTP/1.1 200 OK (text/html)
528	2015-06-30 13:12:45.268192	192.168.122.62	192.254.234.118	TCP	60	49171 → 80 [ACK] Seq=683 Ack=743 Win=64968 Len=0
529	2015-06-30 13:12:45.275159	192.168.122.62	192.254.234.118	HTTP	435	GET /floridablueheader.jpg HTTP/1.1

Wireshark - Packet 529 - ECE570-2020-project3.pcap

```
Accept-Language: en-US\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC-)\r\nAccept-Encoding: gzip, deflate\r\nHost: www.floridablue.com\r\nConnection: Keep-Alive\r\n\r\n[Full request URI: http://www.floridablue.com/floridablueheader.jpg]\r\n[HTTP request 2/3]\r\n[Prev request in frame: 524]\r\n[Response in frame: 755]\r\n[Next request in frame: 1247]
```

Σ http://www.floridablue.com/floridablueheader.jpg

0 / 68

No engines detected this URL

http://www.floridablue.com/floridablueheader.jpg

404 Status

text/html, charset=UTF-8 Content Type

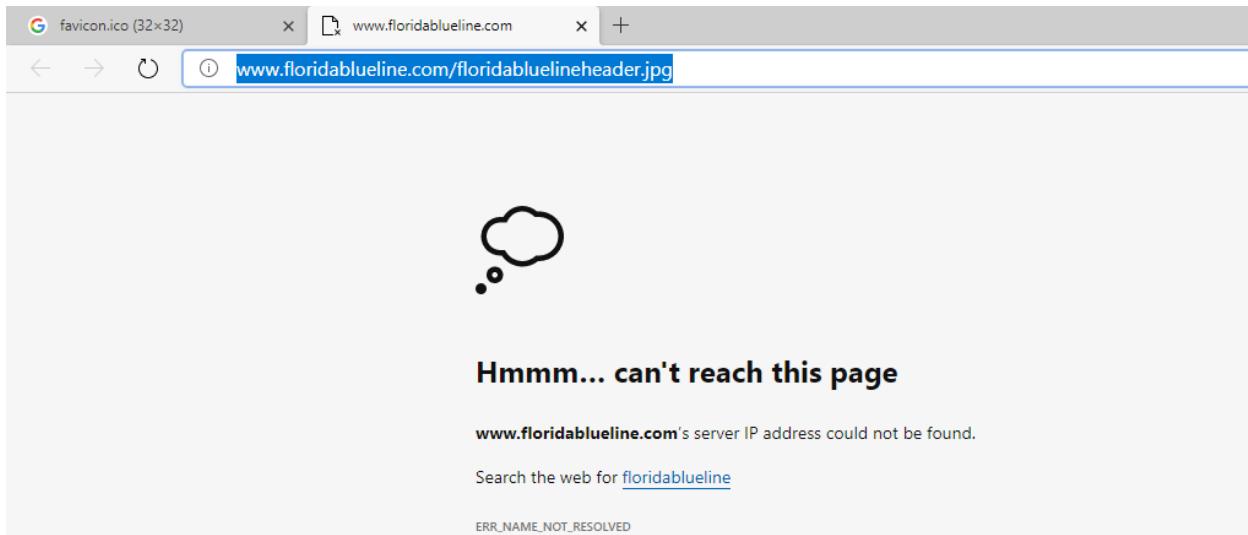
2018-08-04 00:35:17 U

Community Score

Detection Details Relations Community

Detection	Details	Relations	Community
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Anti-AVL	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	BitDefender	Clean
Bluelv	Clean	Certly	Clean
CLEAN MX	Clean	Comodo Site Inspector	Clean
CyberCrime	Clean	CyRadar	Clean

But this site has a **404 error** that indicates the server itself was found, but that the server was not able to retrieve the requested page.

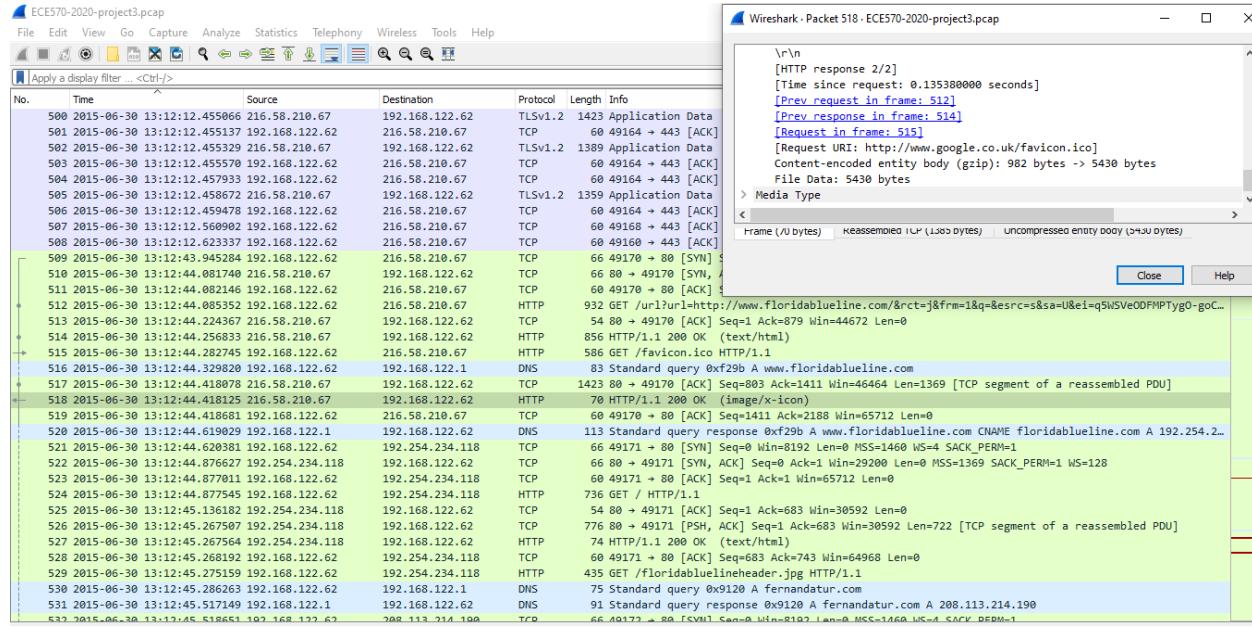


In frame 530, the host requested another website. The name of the website is **fernandatur.com** screen shots of request/response frames (530/531 in wireshark) are shows as a follows:

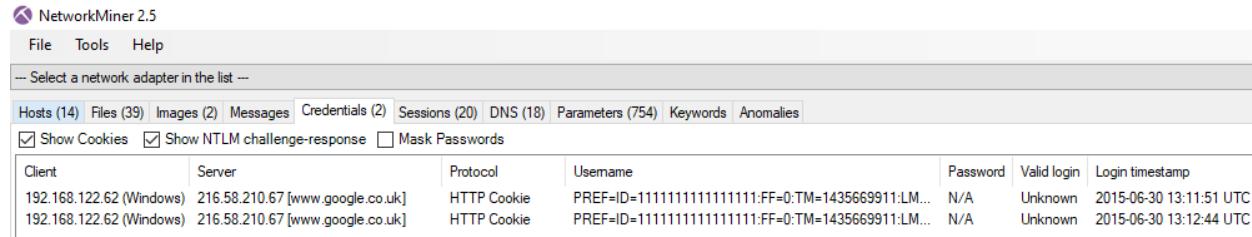
The figure displays two Wireshark windows. The left window, titled 'Wireshark - Packet 530 - ECE570-2020-project3.pcap', shows a DNS query from port 530 to 53. The right window, titled 'Wireshark - Packet 531 - ECE570-2020-project3.pcap', shows the DNS response from port 53 to 530. Both windows show the raw hex and ASCII data for each packet.

Note: when host access to floridablueline.com cookies created in 13:12:44

And later than in 13.11.51 another cookies created for google.co.uk  
 Both sites server is google.co.uk



based on network miner/credentials report, at the same time 13:12:44 HTTP (same time based on wireshark screenshots in above) cookies are created.



NetworkMiner 2.5

File Tools Help

-- Select a network adapter in the list --

Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Show Cookies  Show NTLM challenge-response  Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.122.62 (Windows)	216.58.210.67 [www.google.co.uk]	HTTP Cookie	PREF=ID=1111111111111111:FF=0:TM=1435669911:LM...	N/A	Unknown	2015-06-30 13:11:51 UTC
192.168.122.62 (Windows)	216.58.210.67 [www.google.co.uk]	HTTP Cookie	PREF=ID=1111111111111111:FF=0:TM=1435669911:LM...	N/A	Unknown	2015-06-30 13:12:44 UTC

Based on the packet total report, in Transferred Files. We have two files transferred in that transfer between google.co.uk website (216.58.218.67) and host machine(192.168.122.67) in the time 13:12:44 and date 2015-06-30, text/plain and image/x-icon . Both of them are virustotal safe. Screenshots are as follows:

 2015-05-30 13:12:44 Z CIFU4P2TqMGvSgfc62 FVBL1HGFV5ERAST... 	 1332bd535c81fd41228b3e6c6f5e1723 	 da951504bb632202941bf62870ccdede3c35aeff 	 216.58.210.67 	192.168.122.62	HTTP	0
Mime Type text/plain						
File Name null						
Total Bytes null						

 2015-05-30 13:12:44 Z CIFU4P2TqMGvSgfc62 F9ZM13KOMATOWH... 	 a300691728f5cad531a6886d9b8f38c2 	 e2820bf4f2b65f62434c62ea967973140b3380df 	 216.58.210.67 	192.168.122.62	HTTP	0
Mime Type image/x-icon						
File Name null						
Total Bytes null						

Two screenshots that prove no detection based on virustotal.com report:

 165e12d13971f01b4c668d177d9bec4336856a1cf9ac946eb5953b93bef37cfb
 


  
/ 58

 No engines detected this file

165e12d13971f01b4c668d177d9bec4336856a1cf9ac946eb5953b93bef37cfb  
&rct=j&frm=1&q=&esc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUmlRimDVTKWno90XOpmcDu8zA  
text

1.04 KB      2018-08-04 04:16:15 UTC  
Size      2 years ago

DETECTION	DETAILS	COMMUNITY
Ad-Aware	 Undetected	AegisLab  Undetected
AhnLab-V3	 Undetected	ALYac  Undetected
Antiy-AVL	 Undetected	Arcabit  Undetected
Avast	 Undetected	Avast-Mobile  Undetected
AVG	 Undetected	Avira (no cloud)  Undetected
AVWare	 Undetected	Babable  Undetected

aab089af3b8390a350352b5b7900f5747ba57ef1caf4120cced745518e8b5477 | 🔍 ⏷



No engines detected this file

aab089af3b8390a350352b5b7900f5747ba57ef1caf4120cced745518e8b5477  
favicon.ico

attachment ico via-tor

Community Score

5.30 KB | 2020-05-26 11:23:28 UTC | 2 months ago

DETECTION	DETAILS	RELATIONS	COMMUNITY
Ad-Aware	Undetected		AegisLab Undetected
AhnLab-V3	Undetected		ALYac Undetected
Antiy-AVL	Undetected		Arcabit Undetected
Avast	Undetected		Avast-Mobile Undetected
AVG	Undetected		Avira (no cloud) Undetected
Baidu	Undetected		BitDefender Undetected

According to investigation all transferred Files in packet total From 13:11:51 that the capture started, to 13:12:44. We found that in these periods of time files, text, images, packets transferred were safe.

The graph shows in the following pictures:

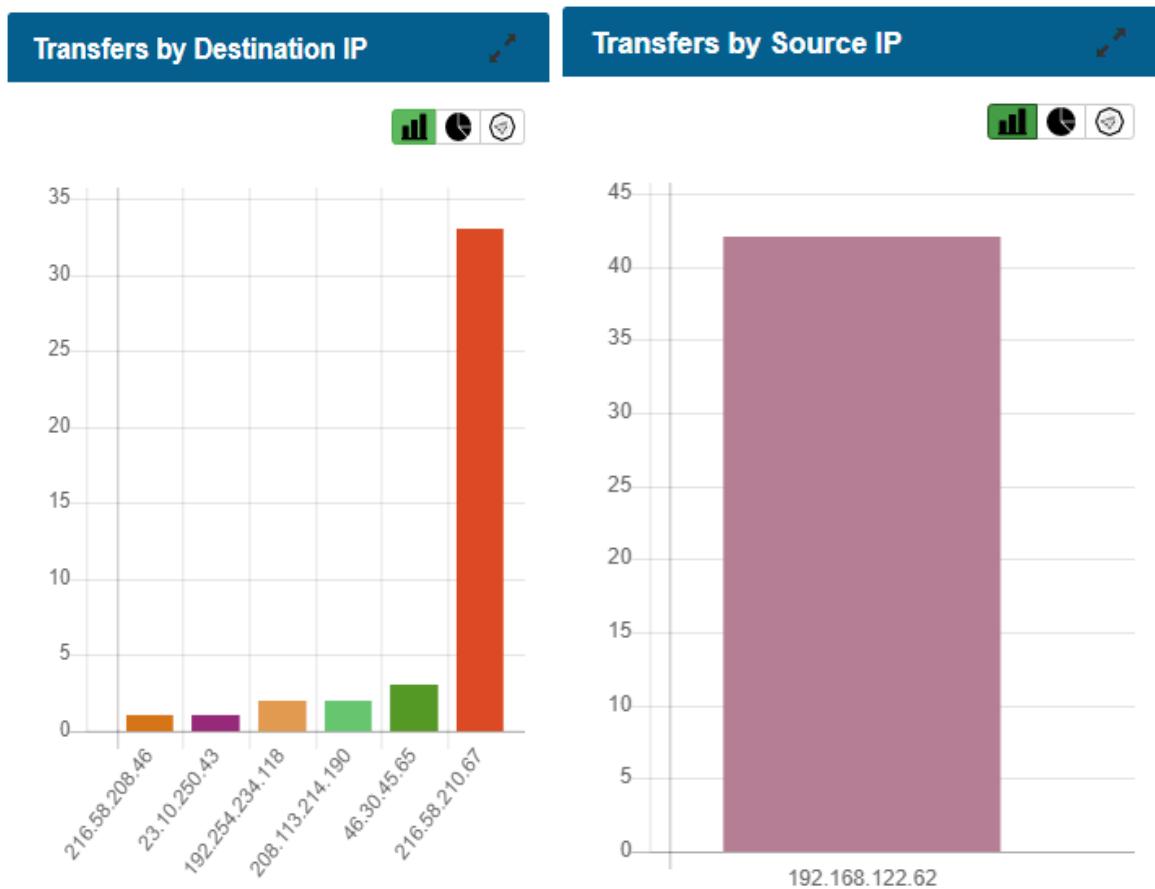




In this picture transfer data starts from the time 13:11:51 in the first frame of wireshark capture. After 14:00:41 duration transferred data received to time 13:12:44. So the time that our diagram is zero is between 13:11:57 and 13:12:44.

And also transferred files by source ip and destination ip during this time shown as following pictures in Bar chart:





34 files transferred between host and three different destination to those destination and host including: google.com, google.co.uk, and floridablueline.com that all of them checked on virustotal.com from Transferred Files Tab in packet total and they are clean and no detected report.

But at 13:12:45 the malicious traffic started.

According to the packettotal report, three Malicious activity from source IP address 192.265.234.118 related to floridablueline.com website to host machine (192.168.122.62) on TCP protocol done.



**Similar Packet Captures**

Similar Packet Captures									
Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 08	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com

Attention to alerts signature of those three malicious activities and description show that **A Network Trojan was detected.**

We check all three alerts one by one and screenshots are in the following pictures. All three alerts contain one HTTP referred that checked on virus total. And also, all alerts description.

First alert alert signature mentions the ET CURRENT\_EVENTS Malicious Redirect 8x8 script tag. The picture show that a malicious script appended from the infected website:

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
<hr/>									
HTTP URI /									
HTTP Content-Type text/html									
HTTP Method GET									
HTTP User Agent ...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) v									
HTTP Referrer <a href="http://www.google.co.uk/url?url=http://www.floridablueline.com/&amp;rct=j&amp;frm=1&amp;q=&amp;esrc=s&amp;sa=U&amp;ei=q5WSVeODFMPtygO-goCgBQ&amp;ved=0CBQQFjAA&amp;usg=AFOjCNEUmRimmDVTKWno9XOpncDu8zA">http://www.google.co.uk/url?url=http://www.floridablueline.com/&amp;rct=j&amp;frm=1&amp;q=&amp;esrc=s&amp;sa=U&amp;ei=q5WSVeODFMPtygO-goCgBQ&amp;ved=0CBQQFjAA&amp;usg=AFOjCNEUmRimmDVTKWno9XOpncDu8zA</a>									
HTTP Protocol HTTP/1.1									
HTTP Length 516									
HTTP Status Code 200									

When checked HTTP referred on virustotal.com we found this URL is clean:



http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg: Q ↻ ⚙



✓ No engines detected this URL

http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnRimmDVTKWno90XOpncDu8zA

200  
Status

text/html, charset=UTF-8  
Content Type

2018-03-16 10:27:06 UTC  
2 years ago

DETECTION	DETAILS	RELATIONS	COMMUNITY
ADMINUSLabs	✓ Clean		AegisLab WebGuard ✓ Clean
AlienVault	✓ Clean		Antiy-AVL ✓ Clean
Avira (no cloud)	✓ Clean		Baidu-International ✓ Clean
BitDefender	✓ Clean		Blueliv ✓ Clean
Certy	✓ Clean		CLEAN MX ✓ Clean
Comodo Site Inspector	✓ Clean		CyberCrime ✓ Clean

The second alert signature is ET CURRENT\_EVENTS Evil Redirector Leading to EK Dec 09. This alert is show:

2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09	1	192.234.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
<hr/>									
HTTP URI /									
HTTP Content-Type text/html									
HTTP Method GET									
HTTP User Agent Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)									
HTTP Referrer http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPTygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnRimmDVTKWno90XOpncDu8zA									
HTTP Protocol HTTP/1.1									
HTTP Length 516									
HTTP Status Code 200									

When checked HTTP referred on virustotal.com we found this URL is clean:



http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPtygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnRimmDVTKWno90XOpmeDu8zA

No engines detected this URL

0 / 67

Community Score

http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPtygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnRimmDVTKWno90XOpmeDu8zA

200 Status | text/html; charset=UTF-8 Content Type | 2018-03-16 10:27:06 UTC | 2 years ago

www.google.co.uk

DETECTION	DETAILS	RELATIONS	COMMUNITY
ADMINUSLabs	<span>✓</span> Clean		AegisLab WebGuard <span>✓</span> Clean
AlienVault	<span>✓</span> Clean		Antly-AVL <span>✓</span> Clean
Avira (no cloud)	<span>✓</span> Clean		Baidu-International <span>✓</span> Clean
BitDefender	<span>✓</span> Clean		Blueliv <span>✓</span> Clean
Certify	<span>✓</span> Clean		CLEAN MX <span>✓</span> Clean
Comodo Site Inspector	<span>✓</span> Clean		CyberCrime <span>✓</span> Clean

### The third alert is ET CURRENT\_EVENTS Evil Redirector:

2015-09-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com
<hr/>									
HTTP URI /									
HTTP Content-Type text/html									
HTTP Method GET									
HTTP User Agent Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)									
HTTP Referrer http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPtygO-goCgBQ&ved=0CBQQFjAA&usg=AFQjCNEUrnRimmDVTKWno90XOpmeDu8zA									
HTTP Protocol HTTP/1.1									
HTTP Length 516									
HTTP Status Code 200									

When checked HTTP referred on virustotal.com we found this URL is clean:



	http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPtygO-goCgBQ&ved=0CBQQFjAA&usg:			
---	---	---	---	---



No engines detected this URL

http://www.google.co.uk/url?url=http://www.floridablueline.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=q5WSVeODFMPtygO-goCgBQ&ved=0CBQQFjAA&usg:TKWno90XOpmeDu8zA

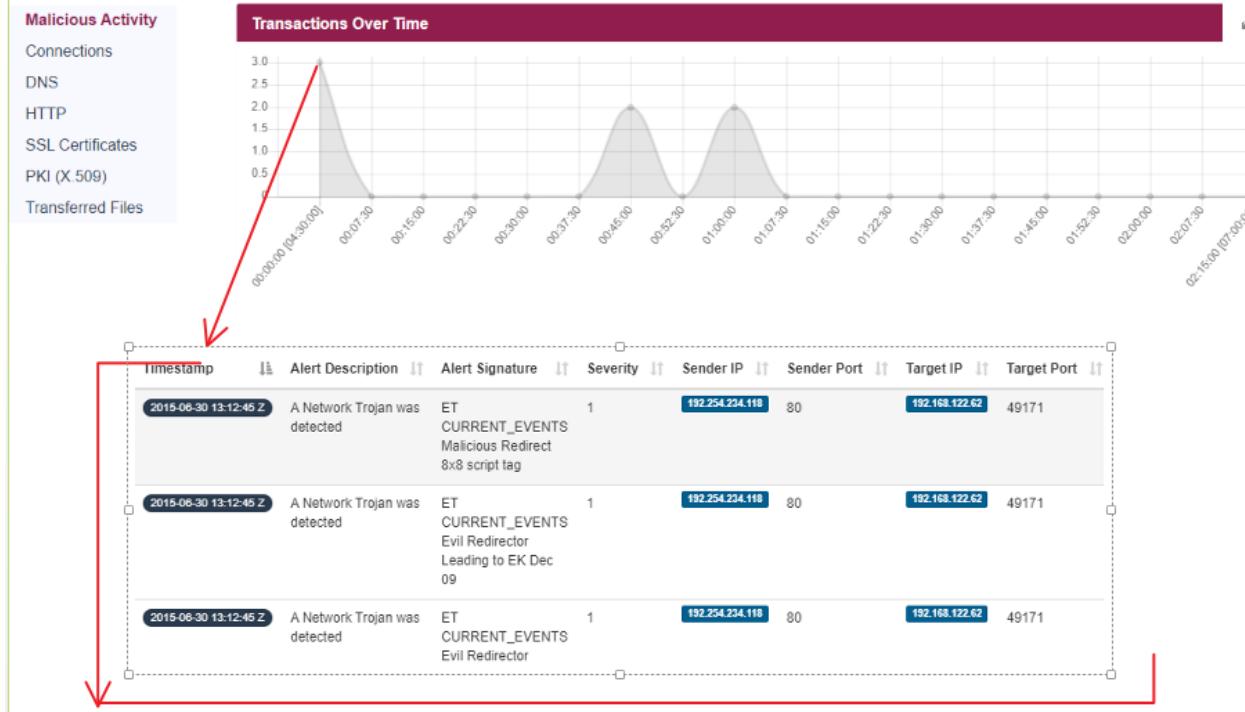
www.google.co.uk

Community Score

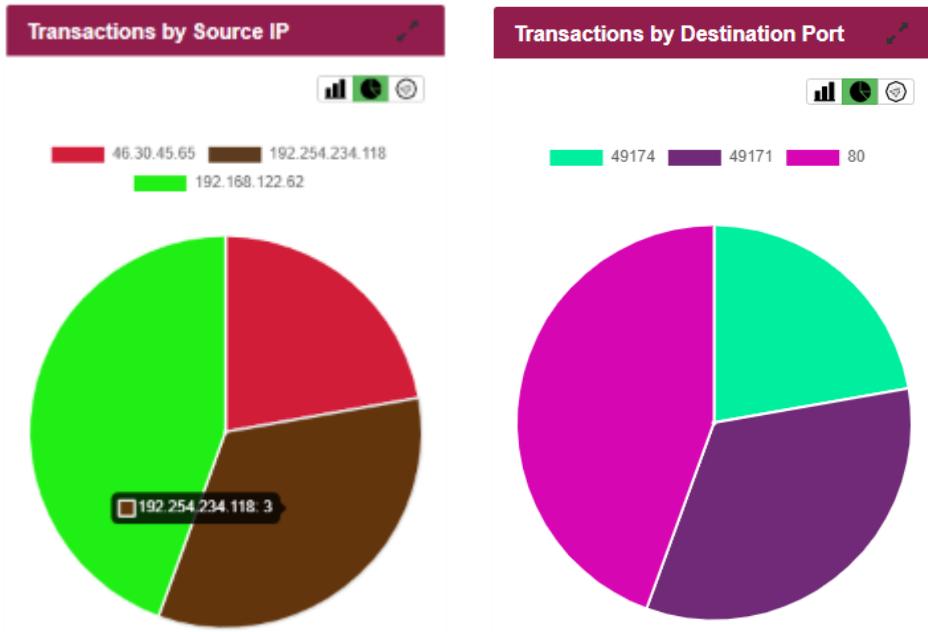
200 Status | text/html; charset=UTF-8 Content Type | 2018-03-16 10:27:06 UTC | 2 years ago

DETECTION	DETAILS	RELATIONS	COMMUNITY
ADMINUSLabs	 Clean		AegisLab WebGuard  Clean
AlienVault	 Clean		Antiy-AVL  Clean
Avira (no cloud)	 Clean		Baidu-International  Clean
BitDefender	 Clean		Blueliv  Clean
Certy	 Clean		CLEAN MX  Clean
Comodo Site Inspector	 Clean		CyberCrime  Clean

The graph of show as follows, those three transactions are highlights by red line on the graph.



The pie chart illustrates three transaction occurs by source ip (192.254.234.118)  
And also three transaction Destination ports are 49171 on TCP protocol.



And also in this time 13.12.45 we checked Transferred Files in packet total and we found that three files transferred in that time, the screenshots are shown as following picture:



Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	<a href="#">F1A40012BQh6PYX...</a>	4531aa227a2652f5603b034fe52ff9fea	4627dab7eaef5154bd8197aa7e9307f8473f34570	192.254.234.118	192.168.122.62	HTTP	0
Mime Type	text/html							
File Name	null							
Total Bytes	null							
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	<a href="#">F1C21D2E9NTQhZ7U...</a>	cb5d1a0b11ef7b2204f3c8ef066d4918	#fbec3e65d9cefaad31bde45c80cah2b95cdbe35	192.254.234.118	192.168.122.62	HTTP	0
Mime Type	image/jpeg							
File Name	null							
Total Bytes	183799							
2015-06-30 13:12:45 Z	CMvAQV20wIXQnWdhX2	<a href="#">17RQYF222196BDT...</a>	1473befb11864f12ed74b6d4fe7e21c	f162bf38954f6e949ebcf0319b27b24ab23ae8580	206.213.234.106	192.168.122.62	HTTP	0
Mime Type	text/html							
File Name	null							
Total Bytes	null							

The check of all those three files on virustotal shows that the first files include text/html detected by 27 engines in virustotal.com and Trojan this is trojan scripts.

The other two files are checked in virus total and clean.

This file transferred from 192.254.234.118 that we know is the ip address of floridablueline.com to our host machine with the IP address of 192.168.122.62 on HTTP protocol. The virustotal report is shows as follows:



31a8f5172fb0787327616f0cd10eeb2cf5614f02db60186a1f3d029be237041a



Sign in

27
/ 60
Community Score

ⓘ 27 engines detected this file

31a8f5172fb0787327616f0cd10eeb2cf5614f02db60186a1f3d029be237041a	index.html	829.00 B	2020-05-24 03:39:41 UTC	2 months ago	
DETECTION	DETAILS	COMMUNITY			
Ad-Aware	ⓘ Trojan.GenericKD.31150873	AegisLab	ⓘ Trojan.Script.Generic.4!c		
AhnLab-V3	ⓘ HTML/Redirect	ALYac	ⓘ Trojan.GenericKD.31150873		
Anti-AVL	ⓘ Trojan/JS.Redirector.nt	Arcabit	ⓘ Trojan.Generic.D1DB5319		
Avast	ⓘ HTML.Includer-BR [Trj]	AVG	ⓘ HTML.Includer-BR [Trj]		
Avira (no cloud)	ⓘ HTML/Rce.Gen2	BitDefender	ⓘ Trojan.GenericKD.31150873		
CAT-QuickHeal	ⓘ JS.Redirector.AN	Emsisoft	ⓘ Trojan.GenericKD.31150873 (B)		
eScan	ⓘ Trojan.GenericKD.31150873	F-Secure	ⓘ Malware.HTML/Rce.Gen2		
FireEye	ⓘ Trojan.GenericKD.31150873	Fortinet	ⓘ HTML/InjectedPhp.NZltr		
GData	ⓘ Script.Packed.IFrame.K@gen	Ikarus	ⓘ Trojan.Script		
Kaspersky	ⓘ HEUR.Trojan.Script.Generic	MAX	ⓘ Malware (ai Score=99)		
Microsoft	ⓘ Trojan.HTML/Redirector.EP	NANO-Antivirus	ⓘ Trojan.Html.Iframe.dcipov		
Qihoo-360	ⓘ Generic/Trojan.Script.ed4	Sophos AV	ⓘ TrojJSRedir-NZ		
Symantec	ⓘ Trojan.Gen.2	VIPRE	ⓘ LooksLike JS.Redirector.nt (v)		
ZoneAlarm by Check Point	ⓘ HEUR:Trojan.Script.Generic	Avast-Mobile	ⓘ Undetected		
Baidu	ⓘ Undetected	BitDefenderTheta	ⓘ Undetected		
Bkav	ⓘ Undetected	ClamAV	ⓘ Undetected		
CMC	ⓘ Undetected	Comodo	ⓘ Undetected		
Cyren	ⓘ Undetected	DrWeb	ⓘ Undetected		
ESET-NOD32	ⓘ Undetected	F-Prot	ⓘ Undetected		

The Network Miner report in parameters shows that this file is on frame 526.



NetworkMiner 2.5

File Tools Help

Select a network adapter in the list --

Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Filter keyword: **text/html**  Case sensitive  ExactPhrase  Any column  Clear  Apply

Parameter name	Parameter value	Frame num...	Source host	Source port	Destination host	Destination port	Timestamp	Details
Content-Type	text/html; charset=UTF-8	8	216.58.208.46 [google.com]	TCP 80	192.168.122.62 (Windows)	TCP 49158	2015-06-30 13:11:51 UTC	HTTP Header
Content-Type	text/html; charset=UTF-8	17	216.58.210.67 [www.google.co.uk]	TCP 80	192.168.122.62 (Windows)	TCP 49159	2015-06-30 13:11:51 UTC	HTTP Header
Content-Type	text/html; charset=UTF-8	514	216.58.210.67 [www.google.co.uk]	TCP 80	192.168.122.62 (Windows)	TCP 49170	2015-06-30 13:12:44 UTC	HTTP Header
Content-Type	text/html	526	192.254.234.118 [floridablue.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Type	text/html; charset=iso-8859-1	575	208.113.214.190 [emandatur.com]	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Type	text/html	757	208.113.214.190 [emandatur.com]	TCP 80	192.168.122.62 (Windows)	TCP 49173	2015-06-30 13:12:47 UTC	HTTP Header
Content-Type	text/html	768	46.30.45.65 [goodrecycleteam.com]	TCP 80	192.168.122.62 (Windows)	TCP 49174	2015-06-30 13:12:48 UTC	HTTP Header
Content-Type	text/html; charset=iso-8859-1	843	23.10.250.43 [a1293.akamai.net]	TCP 80	192.168.122.62 (Windows)	TCP 49176	2015-06-30 13:12:52 UTC	HTTP Header

The wireshark information on frame 526 show that this frame reassembled PDU in frame 527. The screen shot is shown in following picture:

ECE570-2020-project3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 13

No.	Time	Source	Destination	Protocol	Length	Info
524	2015-06-30 13:12:44.877545	192.168.122.62	192.254.234.118	HTTP	736	GET / HTTP/1.1
525	2015-06-30 13:12:45.136182	192.254.234.118	192.168.122.62	TCP	54	80 → 49171 [ACK] Seq=1 Ack=683 Win=30592 Len=0
526	2015-06-30 13:12:45.267507	192.254.234.118	192.168.122.62	TCP	776	80 → 49171 [PSH, ACK] Seq=1 Ack=683 Win=30592 Len=722 [TCP segment of a reassembled PDU]
527	2015-06-30 13:12:45.267564	192.254.234.118	192.168.122.62	HTTP	74	HTTP/1.1 200 OK (text/html)

Wireshark - Packet 526 - ECE570-2020-project3.pcap

0x0101 .... = Header Length: 20 bytes (5)  
 ↴ Flags: 0x018 (PSH, ACK)  
 000. .... .... = Reserved: Not set  
 ...0 .... .... = Nonce: Not set  
 ....0.... .... = Congestion Window Reduced (CWR): Not set  
 ....0.... .... = ECN-Echo: Not set  
 ....0.... .... = Urgent: Not set  
 ....0....1.... = Acknowledgment: Set  
 ....0....1.... = Push: Set  
 ....0....0... = Reset: Not set  
 ....0....0... = Syn: Not set  
 ....0....0... = Fin: Not set  
 [TCP Flags: .....AP...]  
 Window size value: 239  
 [Calculated window size: 30592]  
 [Window size scaling factor: 128]  
 Checksum: 0xfed4 [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 ↴ [SEQ/ACK analysis]  
 [iRTT: 0.256630000 seconds]  
 [Bytes in flight: 722]  
 [Bytes sent since last PSH flag: 722]  
 ↴ [Timestamps]  
 [Time since first frame in this TCP stream: 0.647126000 seconds]  
 [Time since previous frame in this TCP stream: 0.131325000 seconds]  
 TCP payload (722 bytes)  
 [Reassembled PDU in frame: 527]  
 TCP segment data (722 bytes)

In this frame, frame 526, we have PSH,ACK.

The **ACK** indicates that a host is acknowledging having received some data, and the **PSH,ACK** indicates the host is acknowledging receipt of some previous data and also transmitting some more data.

So, here based on all information above **floridablue.com** with the ip address of 192.254.234.118 is the compromised website.





The two other two screen shots for virustotal.com of two timestamps of File transferred are shown in following pictures:

Tow files are clean in virustotal scan.

Two screenshots from virustotal.com showing file analysis results for two different timestamps. Both files were found to be clean (0 detections).

**File 1 (2015-06-30 13:12:45 Z):**

- Mime Type: image/jpeg
- File Name: null
- Total Bytes: 183799

**File 2 (2015-06-30 13:12:45 Z):**

- Mime Type: text/html
- File Name: null
- Total Bytes: null

**File Analysis Summary:**

0 / 59 engines detected this file

f2ff22822d59da5361d7aee4f4f356a278e6f47976013aedec26790c45db5537  
floridabluelineheader.jpg  
jpeg

Community Score: 0

179.49 KB | 2018-08-04 04:16:42 UTC | 2 years ago

DETECTION	DETAILS	COMMUNITY	
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
AVware	Undetected	Babable	Undetected



fee02bb3cc6581fa226c60ea23b3c2e1a069e34a35ecb9025f5898488904162

No engines detected this file

0 / 58

Community Score

fee02bb3cc6581fa226c60ea23b3c2e1a069e34a35ecb9025f5898488904162  
hqnybx2w.php?id=960135

265.00 B | 2018-08-04 04:17:22 UTC | Size | 2 years ago

html

DETECTION	DETAILS	COMMUNITY	
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
AVWare	Undetected	Babable	Undetected

And also in frame 530, host request to DNS for fernandature.com The website ip address is sent to host by DNS, 208.113.214.190 . The screenshot shows as a follows:

The screenshot shows the Wireshark interface with the following details:

- Panels:** No, Time, Source, Destination, Protocol, Length, Info.
- Selected Packet:** 530 2015-06-30 13:12:45.286263 192.168.122.62 DNS 75 Standard query 0x9120 A fernandatur.com
- Details View:** Shows the transaction ID 0x9120, flags (0x0100 Standard query), questions (1), answer RRs (0), authority RRs (0), additional RRs (0), and a query for fernandatur.com type A, class IN.
- Bytes View:** Displays the raw hex and ASCII data for the selected DNS response.
- Right Panel:** Shows the reassembled PDU for the response, which includes the domain name "fernandatur.com".
- Status Bar:** Len=0, Len=0, RM=1 WS=128.

Host sent an SYN to this site from frame 532. In frame 551 ferandature.com sent an SYN.ACK to the host. Host sent back the ACK to this site in frame number 662. The picture as a following show this handshaking:

No.	Time	Source	Destination	Protocol	Length	Info
529	2015-06-30 13:12:45.275159	192.168.122.62	192.254.234.118	HTTP	435	GET /floridebluelinemheader.jpg HTTP/1.1
530	2015-06-30 13:12:45.286629	192.168.122.62	192.168.122.1	DNS	75	Standard query 0x9120 A fernandatur.com
531	2015-06-30 13:12:45.517149	192.168.122.1	192.168.122.62	DNS	93	Standard query response 0x9120 A fernandatur.com A 200.113.214.190
532	2015-06-30 13:12:45.518861	192.168.122.62	298.113.234.198	TCP	66	49172 + 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1468 WS=4 SACK_PERM=1
533	2015-06-30 13:12:45.536080	192.168.122.62	192.254.234.118	TCP	54	49171 + 80 [ACK] Seq=743 Ack=1864 Win=32000 Len=0
534	2015-06-30 13:12:45.601811	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=743 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
535	2015-06-30 13:12:45.602182	192.168.122.62	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=2112 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
536	2015-06-30 13:12:45.602300	192.168.122.62	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=3401 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
537	2015-06-30 13:12:45.602432	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=3401 Ack=1864 Win=65712 Len=0
538	2015-06-30 13:12:45.602580	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=48597 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
539	2015-06-30 13:12:45.602597	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=6219 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
540	2015-06-30 13:12:45.602805	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=7588 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
541	2015-06-30 13:12:45.602818	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=1864 Ack=6219 Win=65712 Len=0
542	2015-06-30 13:12:45.603097	192.168.122.62	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=8937 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
543	2015-06-30 13:12:45.603099	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=18326 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
544	2015-06-30 13:12:45.603124	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=11695 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
545	2015-06-30 13:12:45.603201	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=1864 Ack=8957 Win=65712 Len=0
546	2015-06-30 13:12:45.603339	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=13064 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
547	2015-06-30 13:12:45.603349	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=1864 Ack=11095 Win=62972 Len=0
548	2015-06-30 13:12:45.603849	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=1864 Ack=14433 Win=60236 Len=0
549	2015-06-30 13:12:45.604083	192.168.122.62	192.254.234.118	TCP	66	[TCP Window Update] 49171 + 80 [ACK] Seq=1864 Ack=14433 Win=63708 Len=0
550	2015-06-30 13:12:45.605186	192.168.122.62	192.254.234.118	TCP	66	[TCP Window Update] 49171 + 80 [ACK] Seq=1864 Ack=14433 Win=65712 Len=0
551	2015-06-30 13:12:45.720671	208.113.214.198	192.168.122.62	HTTP	66	49172 + 80 [SYN, ACK] Seq=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=128
552	2015-06-30 13:12:45.721084	192.168.122.62	208.113.214.198	TCP	66	49172 + 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
553	2015-06-30 13:12:45.721765	192.168.122.62	298.113.234.198	TCP	412	GET /Xcripts/hpnyvbx2u.php?id=980115 HTTP/1.1
554	2015-06-30 13:12:45.858371	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=14433 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
555	2015-06-30 13:12:45.858600	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=15882 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
556	2015-06-30 13:12:45.858707	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=1864 Ack=17171 Win=65712 Len=0
557	2015-06-30 13:12:45.858049	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=17171 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
558	2015-06-30 13:12:45.859896	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [PSH, ACK] Seq=18549 Ack=30606 Win=52000 Len=1369 [TCP segment of a reassembled PDU]
559	2015-06-30 13:12:45.850223	192.168.122.62	192.254.234.118	TCP	66	49171 + 80 [ACK] Seq=1864 Ack=19989 Win=65712 Len=0
560	2015-06-30 13:12:45.859352	192.168.122.62	192.254.234.118	TCP	1423	88 + 49171 [ACK] Seq=19989 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]

And also in the above picture that is highlighted by a red pen. The time of frame 553 is 13:12:45.

We found two GET HTTP protocols in packettotal/HTTP . According to packet total report, we checked two files are HTTP on time 13:12:45 on virustotal com

**Similar Packet Captures**

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:11:51 Z	Cs8Y2Q2yukRvbFS6	192.168.122.62	49158	216.58.208.46	80	1	GET	google.com
2015-06-30 13:11:51 Z	CMuHRQ3JifFRKK1Qc	192.168.122.62	49159	216.58.218.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgf62	192.168.122.62	49170	216.58.218.67	80	1	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgf62	192.168.122.62	49170	216.58.218.67	80	2	GET	www.google.co.uk
2015-06-30 13:12:44 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.com
2015-06-30 13:12:49 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
2015-06-30 13:12:45 Z	CMvAQV2OwRXQmWdhX2	192.168.122.62	49172	268.113.224.198	80	1	GET	fernandular.com
2015-06-30 13:12:46 Z	CMHrzK1MVhV1X1U2j	192.168.122.62	49173	268.113.224.198	80	1	GET	www.fernandular.com
2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.186.41.40	80	1	GET	good.recycle2learn.com
2015-06-30 13:12:48 Z	CTG1822yRPVILob	192.168.122.62	49175	46.186.41.40	80	1	GET	good.recycle2learn.com

The first is related to [www.floridablueline.com](http://www.floridablueline.com) that source IP is Host (192.168.122.62) to the IP address of this site as a destination. We checked this file on virustotal and result is shown as a follows:

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
<b>URI</b> /floridabluelineheader.jpg								
<b>Referrer</b> http://www.floridablueline.com/								
<b>User Agent</b> ...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) v								
<b>Request Body Length</b> 0								
<b>Response Body Length</b> 183799								
<b>Status Code</b> 200								
<b>Status Message</b> OK								
<b>Info Code</b> null								
<b>Info Message</b> null								
<b>File</b> null								
<b>Username</b> null								
<b>Password</b> null								
<b>Proxied</b> null								
<b>Sender File IDs</b> null								
<b>Sender Mime Types</b> null								
<b>Recipient File IDs</b> FZIC2ID2ENIQ6Z2U... 								
<b>Recipient Mime Types</b> image/jpeg								
<b>Client Headers</b> ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,HOST,CONNECTION								
<b>Server Headers</b> null								
<b>Cookie Variables</b> null								
<b>URI Variables</b> /floridabluelineheader.jpg								

Virustotal scan result is this file that transfer via HTTP protocol is clean.



f2ff22822d59da5361d7aee4f4f356a278e6f47976013aedec26790c45db5537

No engines detected this file

0 / 59

f2ff22822d59da5361d7aee4f4f356a278e6f47976013aedec26790c45db5537  
floridabluelineheader.jpg  
jpeg

Community Score

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Undetected	AegisLab
AhnLab-V3	Undetected	ALYac
Antiy-AVL	Undetected	Arcabit
Avast	Undetected	Avast-Mobile
AVG	Undetected	Avira (no cloud)
AVware	Undetected	Babable

The second is related to fernandature.com that source IP is Host (192.168.122.62) to this site as a destination. We checked this file on virustotal and result is shown as follows:



-	2015-09-30 13:12:49 Z	CMvAQV2OvrXQnWdhX2	192.168.122.52	49172	268.113.214.198	80	1	GET	fernandatur.com
URI	/Scripts/hqnybx2w.php?id=960135								
Referrer	http://www.floridablueline.com/								
User Agent	... .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) ^								
Request Body Length	0								
Response Body Length	265								
Status Code	301								
Status Message	Moved Permanently								
Info Code	null								
Info Message	null								
File	null								
Username	null								
Password	null								
Proxied	null								
Sender File IDs	null								
Sender Mime Types	null								
Recipient File IDs	13PQYF223166807...	...							
Recipient Mime Types	text/html								
Server Headers	null								
Cookie Variables	null								
URI Variables	/Scripts/hqnybx2w.php?id								

Virustotal scan result is this file that transfer visa HTTP protocol is clean.



Σ feec02bb3cc6581fa226c60ea23b3c2e1a069e34a35ecb9025f5898488904162

No engines detected this file

0 / 58

Community Score

feec02bb3cc6581fa226c60ea23b3c2e1a069e34a35ecb9025f5898488904162  
hqnybx2w.php?id=960135  
html

265.00 B | 2018-08-04 04:17:22 UTC | 2 years ago

DETECTION	DETAILS	COMMUNITY	
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
AVware	Undetected	Babable	Undetected

In wireshark capture data, in frame 553 that we highlighted in above last wireshark screenshot. We found GET scripts via fernandature.com

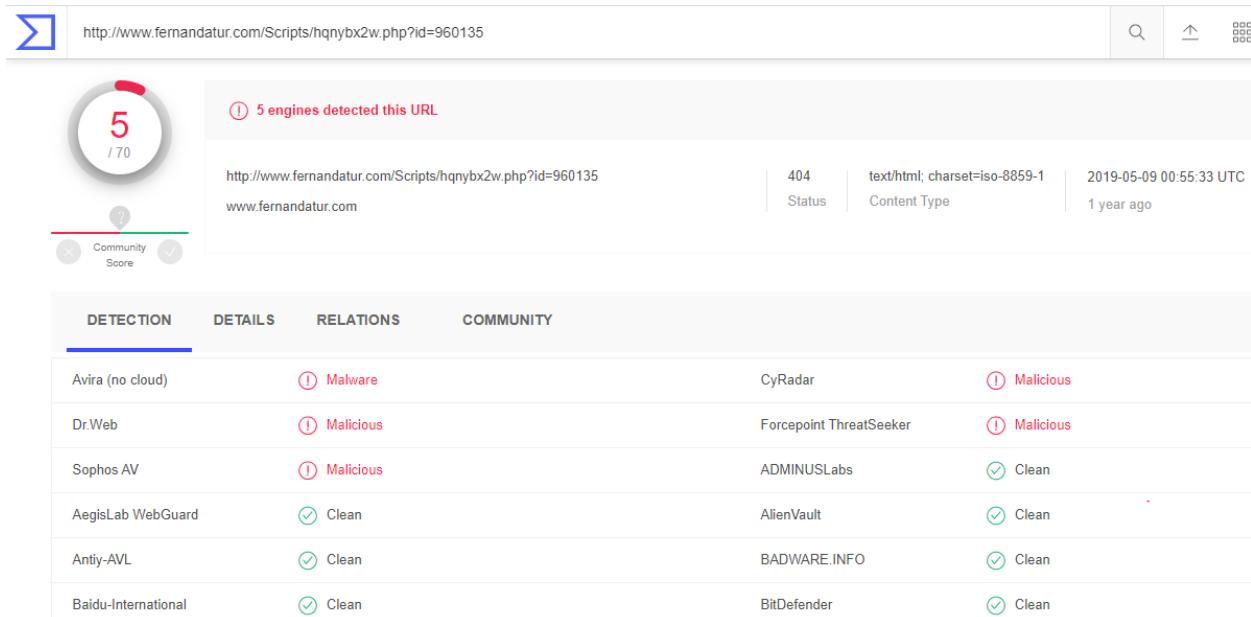


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
553	2015-06-30 13:12:45.721765	192.168.122.62	208.113.214.190	HTTP	432	GET /Scripts/hqnybx2w.php?id=960135 HTTP/1.1
554	2015-06-30 13:12:45.721765	EC5E70-2020-project3.pcap				TCP segment of a reassembled PDU
555	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
556	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
557	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
558	2015-06-30 13:12:45.721765					369 [TCP segment of a reassembled PDU]
559	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
560	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
561	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
562	2015-06-30 13:12:45.721765					User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 1.1.432.0; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 3.5.1.4075)
563	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
564	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
565	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
566	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
567	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
568	2015-06-30 13:12:45.721765					[HTTP request 1/1]
569	2015-06-30 13:12:45.721765					[Response in frame: 573]
570	2015-06-30 13:12:45.721765					< ... >
571	2015-06-30 13:12:45.721765					571 201
572	2015-06-30 13:12:45.721765					0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E:
573	2015-06-30 13:12:45.721765					01 a2 01 40 40 00 00 00 00 00 00 00 00 00 00 00 @@...> q
574	2015-06-30 13:12:45.721765					d6 be c0 14 00 50 62 c0 58 41 6c d7 89 05 18 Pb XA!..P
575	2015-06-30 13:12:45.721765					0030 40 2c e5 e3 00 00 47 45 54 20 2f 53 63 72 69 70 @,... GE T /Script
576	2015-06-30 13:12:45.721765					0040 74 73 2f 68 71 6e 79 62 78 32 77 2e 70 68 70 3f ts/hqnybx2w.php?
577	2015-06-30 13:12:45.721765					0050 69 64 3d 39 36 30 31 33 35 20 48 54 54 50 2f 31 id=960135 HTTP/1
578	2015-06-30 13:12:45.721765					0060 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d .1...Acce pt: /*.*
579	2015-06-30 13:12:45.721765					
580	2015-06-30 13:12:45.721765					
581	2015-06-30 13:12:45.721765					
582	2015-06-30 13:12:46.118388	192.254.234.118	192.168.122.62	TCP	1423 80 → 49171 [ACK] Seq=37706 Ack=1064 Win=32000 Len=1369	[TCP segment of a reassembled PDU]
583	2015-06-30 13:12:46.118409	192.254.234.118	192.168.122.62	TCP	60 49171 → 80 [ACK] Seq=1064 Ack=37706 Win=65712 Len=0	[TCP segment of a reassembled PDU]
584	2015-06-30 13:12:46.118640	192.254.234.118	192.168.122.62	TCP	1423 80 → 49171 [ACK] Seq=39875 Ack=1064 Win=32000 Len=1369	[TCP segment of a reassembled PDU]
585	2015-06-30 13:12:46.118806	192.254.234.118	192.168.122.62	TCP	1423 80 → 49171 [ACK] Seq=40444 Ack=1064 Win=32000 Len=1360	[TCP segment of a reassembled PDU]

When we checked this URL that shows with blue color on virustotal.com, we found that this URL is malicious and Malware. The screenshots are as following picture:



① 5 engines detected this URL

<http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135>

Community Score: 5 / 70

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware	CyRadar	① Malicious
Dr.Web	① Malicious	Forcepoint ThreatSeeker	① Malicious
Sophos AV	① Malicious	ADMINUSLabs	✓ Clean
AegisLab WebGuard	✓ Clean	AlienVault	✓ Clean
Anti-AVL	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean

According to Networkminer report, frame 553 is a file that name is hqnybx2w.php.html

NetworkMiner 2.5

File Tools Help

Select a network adapter in the list --

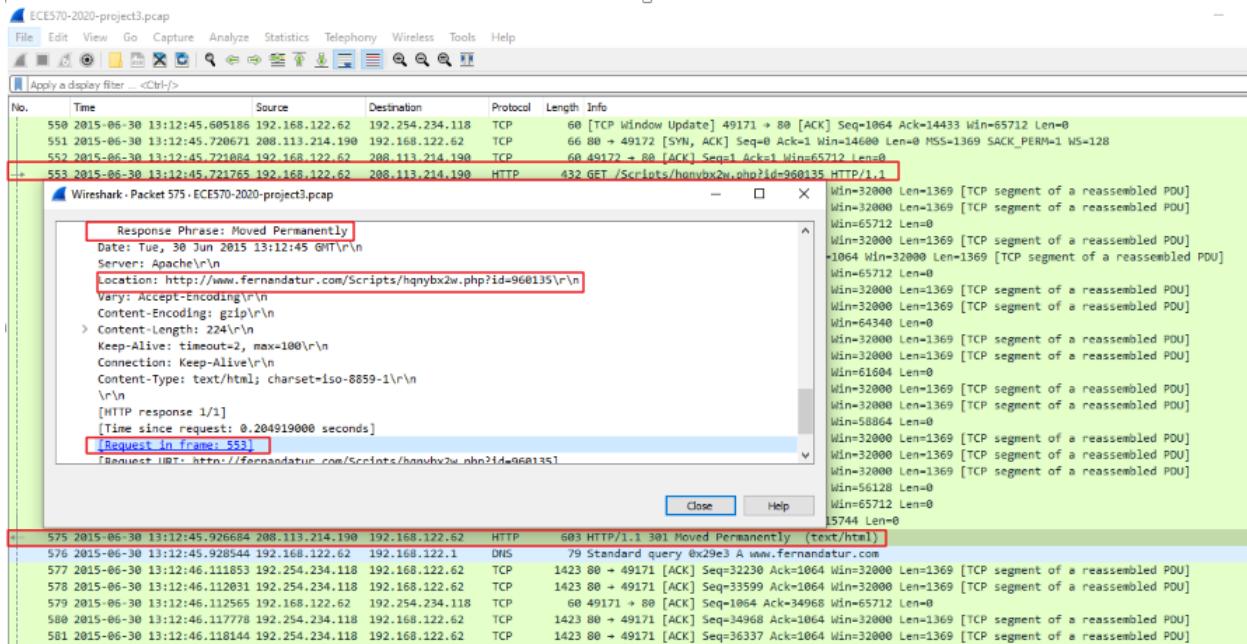
Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Filter keyword:  Case sensitive ExactPhrase Any column Clear App

Fram...	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed...	Details
96	www.google.co.uk[2].cer	cer	1150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=GeoTrust Global CA[2].cer
96	Google Internet Authority G2[2].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoTrust Global CA[2].cer
96	GeoTrust Global CA[2].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
105	google.com.cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
105	Google Internet Authority G2[3].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
109	www.google.co.uk[3].cer	cer	1150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=Geo
109	Google Internet Authority G2[4].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
317	google.com[1].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
317	Google Internet Authority G2[5].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
317	GeoTrust Global CA[5].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
354	google.com[2].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49167	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
354	Google Internet Authority G2[6].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
365	google.com[3].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
365	Google Internet Authority G2[7].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
365	GeoTrust Global CA[7].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
377	google.com[4].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
377	Google Internet Authority G2[8].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
512	url.888C5CB3.html	html	1070 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...)	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/?url=http://www.floridablueline.com
515	favicon.ico	ico	5430 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...)	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/favicon.ico
524	index.html	html	829 B	192.254.234.118 [floridablueline.co...]	TCP 80	192.168.122.62 (Win...)	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 ...	C:\Users\beh...	www.floridablueline.com/
553	hnybx2w.php.html	html	265 B	208.113.214.190 [fernandatur...	TCP 80	192.168.122.62 (Win...)	TCP 49172	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	fernandatur.com/Scripts/hnybx2w.php?id=960135
529	floridabluelineheader.jpg	jpg	183.79 B	192.254.234.118 [floridablueline.co...]	TCP 80	192.168.122.62 (Win...)	TCP 49172	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	www.floridablueline.com/floridabluelineheader.jpg
659	hnybx2w.php[1].html	html	323 B	208.113.214.190 [fernandatur...	TCP 80	192.168.122.62 (Win...)	TCP 49173	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	www.fernandatur.com/Scripts/hnybx2w.php?id=960135
764	index.6558F0B7.html	html	142.97 B	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (Win...)	TCP 49174	HttpGetNormal	2015-06-30 13:12:47 ...	C:\Users\beh...	good.recycle2team.com/?nKfrelLbVKDlU=3SKfPjx2f
811	index.php.swf	swf	15.763 B	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (Win...)	TCP 49175	HttpGetNormal	2015-06-30 13:12:49 ...	C:\Users\beh...	good.recycle2team.com/index.php?nKfrelLbVKDlU=3
841	version.xml11.6.602.html	html	351 B	23.10.250.43 [a1293.d.akamai.net] ...	TCP 80	192.168.122.62 (Win...)	TCP 49176	HttpGetNormal	2015-06-30 13:12:52 ...	C:\Users\beh...	fptdownload2.macromedia.com/get.flashplayer/update/ci
833	index.php.x-msdownload	x...	352.25 B	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (Win...)	TCP 49174	HttpGetNormal	2015-06-30 13:12:51 ...	C:\Users\beh...	good.recycle2team.com/index.php?nKfrelLbVKDlU=43

In frame 575, in wireshark capture, we found that fernandature.com with IP address 208.113.214.190 sent HTTP1.1 moved permanently to the host machine(192.168.122.62) . Moreover, this frame is the response frame of 553. The wireshark screenshot is shown as a following picture:





Here, we found that A TCP handshake does not contain any redirect information. So TCP handshaking is fine. However, we check the application layer, we found that:

< HTTP/1.1 301 Moved Permanently ...

< Location: <http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135>

Since this is a 301 **permanent** redirect the client does not even need to visit the original site again but will instead use the new location on repeated tries. Only on the first try it will visit the original site to receive the redirect.

In Networkminer is again this redirection shows:

NetworkMiner 2.5

File Tools Help

– Select a network adapter in the list –

Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Filter keyword: **HTTP**  Case sensitive  ExactPhrase  Any column  Clear

Parameter name	Parameter value	Frame num...	Source host	Source port	Destination host	Destination port	Timestamp	Details
Transfer-Encoding	chunked	526	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Connection	keep-alive	526	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Last-Modified	Thu, 04 Jun 2015 13:47:01 GMT	526	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Encoding	gzip	526	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
GET	/fondabluelineheader.jpg	529	192.160.122.62 (Windows)	TCP 49171	192.254.234.118 [fondablueli...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Request to www.fondablueline.com
Referrer	http://www.fondablueline.com/	529	192.160.122.62 (Windows)	TCP 49171	192.254.234.118 [fondablueli...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; ...	529	192.160.122.62 (Windows)	TCP 49171	192.254.234.118 [fondablueline.com]	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
Host	www.fondablueline.com	529	192.160.122.62 (Windows)	TCP 49171	192.254.234.118 [fondablueli...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
HTTP Response...	200 OK	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Response
Server	nginx/1.8.0	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Date	Tue, 30 Jun 2015 13:12:45 GMT	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Type	image/jpeg	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Length	183799	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Connection	keep-alive	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Last-Modified	Mon, 22 Dec 2014 20:25:51 GMT	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Accept-Ranges	bytes	534	192.254.234.118 [fondablueline.com]...	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
GET	/Scripts/happybox2x.php?Id=960135	553	192.160.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Request to fernandatur.com
Referrer	http://www.fondablueline.com/	553	192.160.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; ...	553	192.160.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
Host	fernandatur.com	553	192.160.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
id	960135	553	192.160.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP QueryString to fernandatur.com
HTTP Response...	301 Moved Permanently	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Response
Date	Tue, 30 Jun 2015 13:12:45 GMT	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Server	Apache	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Location	http://www.fernandatur.com/Scripts/...	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Vary	Accept-Encoding	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Encoding	gzip	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Length	224	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Keep-Alive	timeout=2, max=100	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Connection	Keep-Alive	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Type	text/html; charset=UTF-8	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
GET	/Scripts/happybox2x.php?Id=960135	659	192.160.122.62 (Windows)	TCP 49173	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:46 UTC	HTTP Request to www.fernandatur.com

Finally, as a report of packettotal in DNS Tab we can see that this site is redirected.

Malicious Activity Suspicious Activity Connections DNS HTTP SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

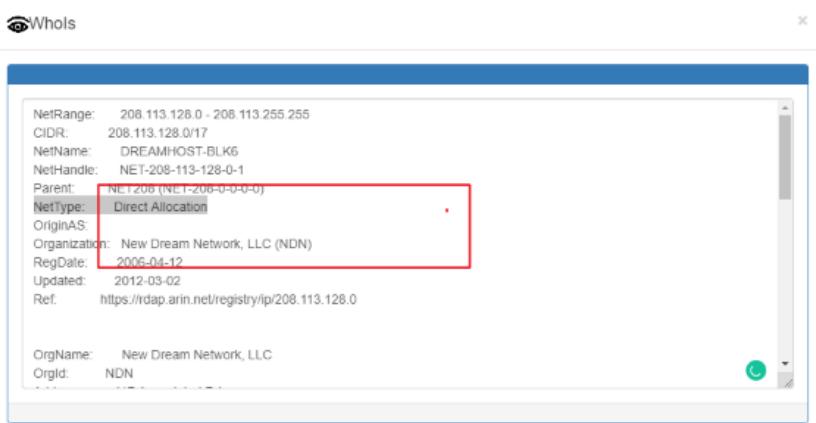
Similar Packet Captures

Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:11:51 Z	CFOesJ21Bmd4FhoX02	192.168.122.62	52719	192.168.122.1	53	udp	50039	google.com
2015-06-30 13:11:51 Z	C9UDXW1tbC8Kb0UdZ	192.168.122.62	52063	192.168.122.1	53	udp	51086	www.google.co.uk
2015-06-30 13:11:52 Z	CKxDXMy4bchmaV2uPk	192.168.122.62	56599	192.168.122.1	53	udp	48084	val.gafatic.com
2015-06-30 13:11:53 Z	C2Qm21H8X3mlDwuBf	192.168.122.62	55533	192.168.122.1	53	udp	31829	elientst.google.co.uk
2015-06-30 13:12:44 Z	CVWlzdG0quCNia8	192.168.122.62	57473	192.168.122.1	53	udp	62107	www.fondablueline.com
2015-06-30 13:12:45 Z	CVZj034HeWhYEPJygd	192.168.122.62	50955	192.168.122.1	53	udp	37152	fernandatur.com
2015-06-30 13:12:45 Z	CR9x8sdRdQ0MDUCGB	192.168.122.62	54137	192.168.122.1	53	udp	10723	www.fernandatur.com
2015-06-30 13:12:47 Z	CF90e4APfPYX0dSMU	192.168.122.62	59978	192.168.122.1	53	udp	48790	good.recycle2learn.com
2015-06-30 13:12:52 Z	CKdhc21h1h9koH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	23089	fpdownload2.msnmedia.com
2015-06-30 13:16:12 Z	ChJHC4Jp9Oh2MaJSa	192.168.122.62	65237	192.168.122.1	53	udp	52964	time.windows.com

When we click on whois Lookup we can see that those sites (fernandatur.com and www.fernandatur.com ) are Direct Allocation.All screenshots are shown as a following pictures:



Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:12:45 Z	CVZlp34HeWhYEPJygd	192.168.122.62	50855	192.168.122.1	53	udp	37152	<a href="#">fermandatur.com</a>
Query Class Desc C_INTERNET Query Type 1 Query Type Desc A Response Code 0 Response Code Desc NOERROR Authoritative Answer? F Truncated? F Recursion Desired? T Recursion Available? T <b>Answers</b> <a href="#">208.113.254.198</a> <b>TTLs</b> 14389.00 Authoritative Response null Additional Response(s) null								
 <p>Whois</p> <p>NetRange: 208.113.128.0 - 208.113.255.255    CIDR: 208.113.128.0/17    NetName: DREAMHOST-BLK6    NetHandle: NET-208-113-128-0-1    Parent: NET-200 (NET-200-0-0-0-0)  <b>NetType:</b> Direct Allocation    OriginAS:    Organization: New Dream Network, LLC (NDN)    RegDate: 2006-04-12    Updated: 2012-03-02    Ref: <a href="https://rdap.arin.net/registry/ip/208.113.128.0">https://rdap.arin.net/registry/ip/208.113.128.0</a></p> <p>OrgName: New Dream Network, LLC    Orgid: NDN</p>								
2015-06-30 13:12:40 Z	CR9xfid	Query Class Desc C_INTERNET Query Type 1						





2015-09-30 13:12:45 2 CR9x6sdRdQ0MDUCG8 192.168.122.62 54137 192.168.122.1 53 udp 10723 www.fernandature.com

Query Class Desc C\_INTERNET  
Query Type 1  
Query Type Desc A  
Response Code 0  
Response Code Desc NOERROR  
Authoritative Answer? F  
Truncated? F  
Recursion Desired? T  
Recursion Available? T

Answers 208.113.214.190  
TTLs 14399.00  
Authoritative Response null  
Additional Response(s) null

Timestamp Connect  
2015-09-30 13:11:51 CFQuesJZ  
2015-09-30 13:11:51 CKUDX4  
2015-09-30 13:11:52 CZQM21  
2015-09-30 13:11:53 CXWUzD  
2015-09-30 13:12:44 CV2Ip34  
2015-09-30 13:12:45 CR9x6sdRdQ0MDUCG8  
2015-09-30 13:12:45 CR9x6sdRdQ0MDUCG8

Whols

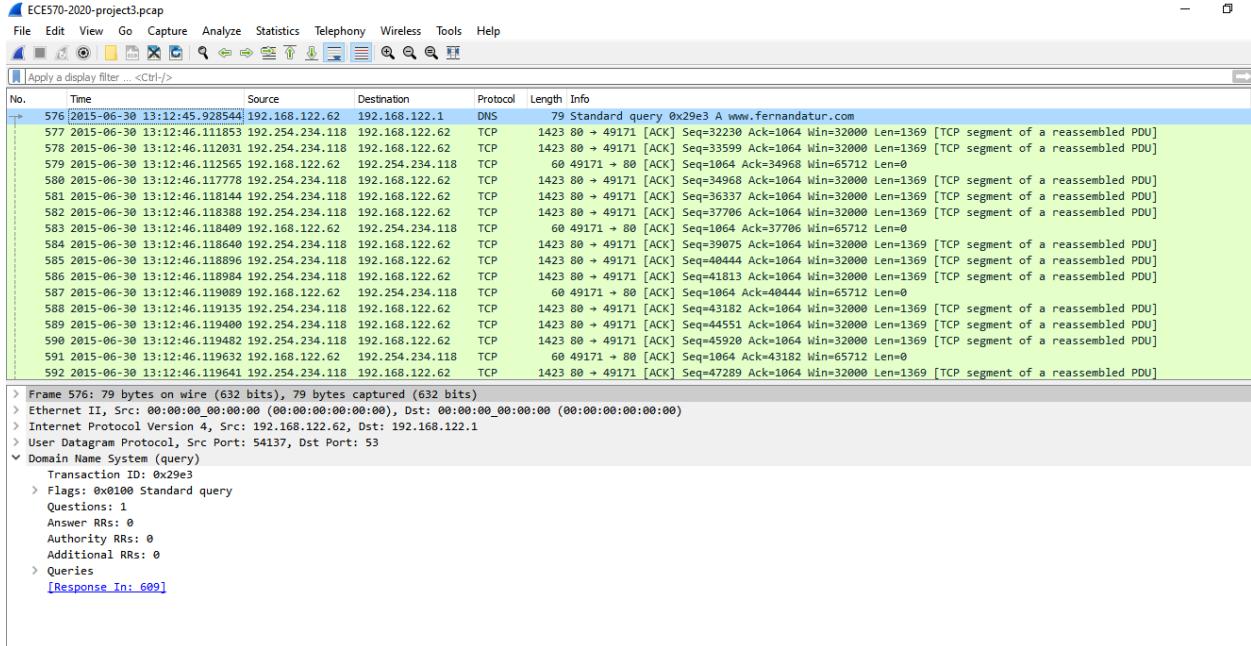
NetRange: 208.113.128.0 - 208.113.255.255  
CIDR: 208.113.128.0/17  
NetName: DREAMHOST-BLK6  
NetHandle: NET-208-113-128-0-1  
Parent: NET206 (NET-206-0-0-0-0)  
NetType: Direct Allocation  
OriginAS:  
Organization: New Dream Network, LLC (NDN)  
RegDate: 2006-04-12  
Updated: 2012-03-02  
Ref: https://rdap.arin.net/registry/ip/208.113.128.0

OrgName: New Dream Network, LLC  
OrgId: NDN

Note: We have a lot of TCP ACK between floridablueline.com and host from frame 533 after host open fernandature.com

At the end of seconds of 13:12:45, in frame 576 the host sent a request to DNS for open www.fernandature.com. In frame 609, DNS responded to the host and sent the IP address of this site. The IP address is 208.113.214.190.





In frame 610 host request to start TCP handshaking to IP address is 208.113.214.190.

In frame 610 send SYN, IP address 208.113.214.190 response SYN,ACK on frame 657. And immediately on frame 658 the host sent ACK to this IP address that is the website: [www.fernandature.com](http://www.fernandature.com).

In frame 659, the host machine sent one HTTP request to 208.113.214.190. This request was sent via HTTP protocol at 13:12:46. The wireshark screenshot is as follows:



ECE570-2020-project3.pcap

tcp.stream eq 15

No.	Time	Source	Destination	Protocol	Length	Info
61	2015-06-30 13:12:46.240613	192.168.122.62	208.113.214.198	TCP	66	49173 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1468 WS=4 SACK_PERM=1
657	2015-06-30 13:12:46.455244	208.113.214.198	192.168.122.62	TCP	66	80 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=128
658	2015-06-30 13:12:46.455635	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
659	2015-06-30 13:12:46.457724	192.168.122.62	208.113.214.198	HTTP	436	GET /Scripts/hqnybxzw.php?id=960135 HTTP/1.1
728	2015-06-30 13:12:46.660357	208.113.214.198	192.168.122.62	TCP	54	80 → 49173 [ACK] Seq=1 Ack=383 Win=15744 Len=0
757	2015-06-30 13:12:47.050032	208.113.214.198	192.168.122.62	HTTP	572	HTTP/1.1 200 OK (text/html)
761	2015-06-30 13:12:47.252248	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [ACK] Seq=383 Ack=519 Win=65192 Len=0
812	2015-06-30 13:12:49.052138	208.113.214.198	192.168.122.62	TCP	54	80 → 49173 [FIN, ACK] Seq=519 Ack=383 Win=15744 Len=0
813	2015-06-30 13:12:49.052332	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [ACK] Seq=383 Ack=520 Win=65192 Len=0
844	2015-06-30 13:12:52.787135	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [RST, ACK] Seq=383 Ack=520 Win=0 Len=0

Wireshark - Follow TCP Stream (tcp.stream eq 15) · ECE570-2020-project3.pcap

3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0  
Accept-Encoding: gzip, deflate  
Connection: Keep-Alive  
Host: www.fernandatur.com

HTTP/1.1 200 OK  
Date: Tue, 30 Jun 2015 13:12:46 GMT  
Server: Apache  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 297  
Keep-Alive: timeout=2, max=100  
Connection: Keep-Alive  
Content-Type: text/html

.....=....0@...|a...A..D...".!#qc...L.X.T.....,M.J.o)b..7C9M  
.45D.X5...Y...b.b...B.%rs  
....{4wng..0..J...34.....(..K..#.Op091,...Q.....+..;^`h&.a.b.1.Q.k.....@\$>]....N..L..5.?...F.z....o  
...9Z.....=180..r6..\$.H..\*..3R.wfj..).Br.....n..E.E....\*(@.n..1..M.....2...c...

I client ptk, I server ptk, I am.

Entire conversation (900 bytes) Show and save data as: ASCII Stream 15

The host machine was infected by a file transferred on frame 526 from floridablueline.com and after that the host led to infection of other sites.

During that time again floridablueline.com sent an ACK to the host and after some ACK from this site the host sent a response.

According to packet total information, in HTTP Tab we found one data related to 13:12:46. After, download that file and check on virustotal. We found that this script is trojan. Infact, this script is the same as the script of frame 553. This file transferred to host in frame 526 from floridablueline.com .





Malicious Activity Suspicious Activity Connections DNS HTTP SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

Similar Packet Captures

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
[+] 2015-06-30 13:11:51 Z	Cs8Y2Q2yukRvbFS6	192.168.122.62	49158	216.58.208.46	80	1	GET	google.com
[+] 2015-06-30 13:11:51 Z	CMuHRQ3Jfj0FRkK1Qc	192.168.122.62	49159	216.58.218.47	80	1	GET	www.google.co.uk
[+] 2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgf62	192.168.122.62	49170	216.58.218.47	80	1	GET	www.google.co.uk
[+] 2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgf62	192.168.122.62	49170	216.58.218.47	80	2	GET	www.google.co.uk
[+] 2015-06-30 13:12:44 Z	CaLygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.com
[+] 2015-06-30 13:12:45 Z	CaLygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
[+] 2015-06-30 13:12:45 Z	CMVAQV2OwIXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	1	GET	fernandatur.com
[+] 2015-06-30 13:12:46 Z	CMHzK1MViHV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com
[+] 2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.38.45.65	80	1	GET	good.recycle2learn.com
[+] 2015-06-30 13:12:48 Z	CtG8I22yrRPViLob	192.168.122.62	49175	46.38.45.65	80	1	GET	good.recycle2learn.com

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
- 2015-06-30 13:12:40 Z	CMHzK1MViHV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com

URI /Scripts/hqnybx2w.php?id=960135

Referrer http://www.floridablueline.com/

User Agent ...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Request Body Length 0

Response Body Length 323

Status Code 200

Status Message OK

Info Code null

Info Message null

File null

Username null

Password null

Proxied null

Sender File IDs null

Sender Mime Types null

Recipient File IDs f43ayX1v5tBLTT...

Recipient Mime Types application/javascript

Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,CONNECTION,HOST

Server Headers null

Cookie Variables null

URI Variables /Scripts/hqnybx2w.php?id





SUMMARY		DETECTION	DETAILS	COMMUNITY
AegisLab			!	Script.Troj.Genlc
Avast			!	JS:Iframe-EOD [Trj]
AVG			!	JS:Iframe-EOD [Trj]
Bkav			!	JS:elframeDwNMe.FE8B
GData			!	Script.Trojan.Redirector.AZ
Ikarus			!	HTML.Framer
Qihoo-360			!	Virus.js.qexvmc.1
TrendMicro-HouseCall			!	Suspicious_GEN.F47V0731
Ad-Aware			✓	Undetected
AhnLab-V3			✓	Undetected
ALYac			✓	Undetected
Antiy-AVL			✓	Undetected
Arcabit			✓	Undetected

Again the URL of this site is in virus total indicates trojan. Same as frame 553.

http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135

5 engines detected this URL

http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135 | 404 Status | text/html; charset=iso-8859-1 Content Type | 2019-05-09 00:55:33 UTC | 1 year ago

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware	CyRadar	① Malicious
DrWeb	① Malicious	Forcepoint ThreatSeeker	① Malicious
Sophos AV	① Malicious	ADMINUSLabs	✓ Clean
AegisLab WebGuard	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean

In the connection Tab of the packet total we found that in time 13:12:46 the connection duration between host and 208.113.214.190 is 6:55 seconds.

Malicious Activity Suspicious Activity | Connections | DNS HTTP SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

Similar Packet Captures

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent
+ 2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	tcp	http	2.95	378	630
+ 2015-06-30 13:12:45 Z	CR9x6sdRdQ0MDUCG8	192.168.122.62	54137	192.168.122.1	53	udp	dns	0.51	37	65
- 2015-06-30 13:12:46 Z	CMHzK1MVlhV1X1Uj	192.168.122.62	49173	208.113.214.190	80	tcp	http	6.55	382	634

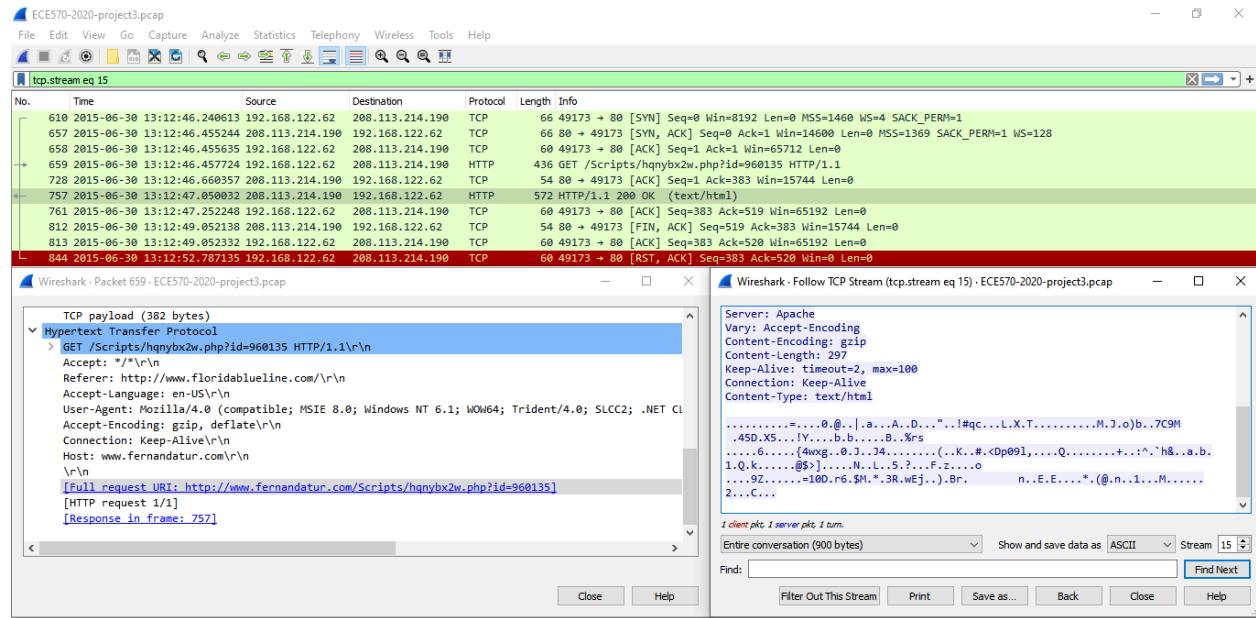
Payload Bytes Received 518  
 Total Bytes Received 690  
 Missed Bytes 0  
 Packets Sent 6  
 Packets Received 4  
 Originated Locally? null  
 Tunnel Parent Connection ID (empty)

History ShADadfR

After HTTP request of host to 208.113.214.190 in frame 659 to GET malicious scripts.  
 In frame 757, the target with 208.113.214.190 as an IP address sent HTTP 1.1 200 OK



to the host. The host IP address is 192.168.122.62. The wireshark screenshot and TCP stream is as follows:



The Wireshark interface displays a list of network packets and a detailed TCP stream analysis.

**tcp.stream eq 15** (Selected Stream):

No.	Time	Source	Destination	Protocol	Length	Info
610	2015-06-30 13:12:46.240613	192.168.122.62	208.113.214.190	TCP	66	49173 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
657	2015-06-30 13:12:46.455244	208.113.214.190	192.168.122.62	TCP	66	80 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=128
658	2015-06-30 13:12:46.455635	192.168.122.62	208.113.214.190	TCP	66	49173 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
659	2015-06-30 13:12:46.457724	192.168.122.62	208.113.214.190	HTTP	436	GET /Scripts/hqnybx2w.php?id=960135 HTTP/1.1
728	2015-06-30 13:12:46.660357	208.113.214.190	192.168.122.62	TCP	54	80 → 49173 [ACK] Seq=1 Ack=383 Win=15744 Len=0
757	2015-06-30 13:12:47.050032	208.113.214.190	192.168.122.62	HTTP	572	HTTP/1.1 200 OK (text/html)
761	2015-06-30 13:12:47.252248	192.168.122.62	208.113.214.190	TCP	60	49173 → 80 [ACK] Seq=383 Ack=519 Win=65192 Len=0
812	2015-06-30 13:12:49.052138	208.113.214.190	192.168.122.62	TCP	54	80 → 49173 [FIN, ACK] Seq=519 Ack=383 Win=15744 Len=0
813	2015-06-30 13:12:49.052332	192.168.122.62	208.113.214.190	TCP	66	49173 → 80 [ACK] Seq=383 Ack=520 Win=65192 Len=0
844	2015-06-30 13:12:52.787135	192.168.122.62	208.113.214.190	TCP	60	49173 → 80 [RST, ACK] Seq=383 Ack=520 Win=0 Len=0

**TCP payload (382 bytes):**

```

> GET /Scripts/hqnybx2w.php?id=960135 HTTP/1.1\r\n
  Accept: */*\r\n
  Referer: http://www.floridablueline.com/\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 3.5.2; .NET CLR 3.0.30729; .NET CLR 2.0.50727; .NET4.0E)\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: Keep-Alive\r\n
  Host: www.fernandatur.com\r\n
  \r\n
[Full request URI: http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135]
[HTTP request 1/1]
[Response in frame: 757]

```

**Follow TCP Stream (tcp.stream eq 15) - ECE570-2020-project3.pcap:**

Server: Apache  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 297  
Keep-Alive: timeout=2, max=100  
Connection: Keep-Alive  
Content-Type: text/html

.....=....@...[a...A..D...".!#qc...L.X.T.....M.J.o)b...7C9M  
.45D.XS...!Y...b.b....B.%rs  
.....6....{4wg...@...J..34.....(..K.#.<Dp@91,...Q.....+...^.%h&.a.b.  
1.Q.k....@\$...)....N.L.S?...F.z...o  
.....92.....=100.r6.\$M.\*.3R.wEj..)Br...n..E.E....\*(@.n..1...M.....  
2...C...

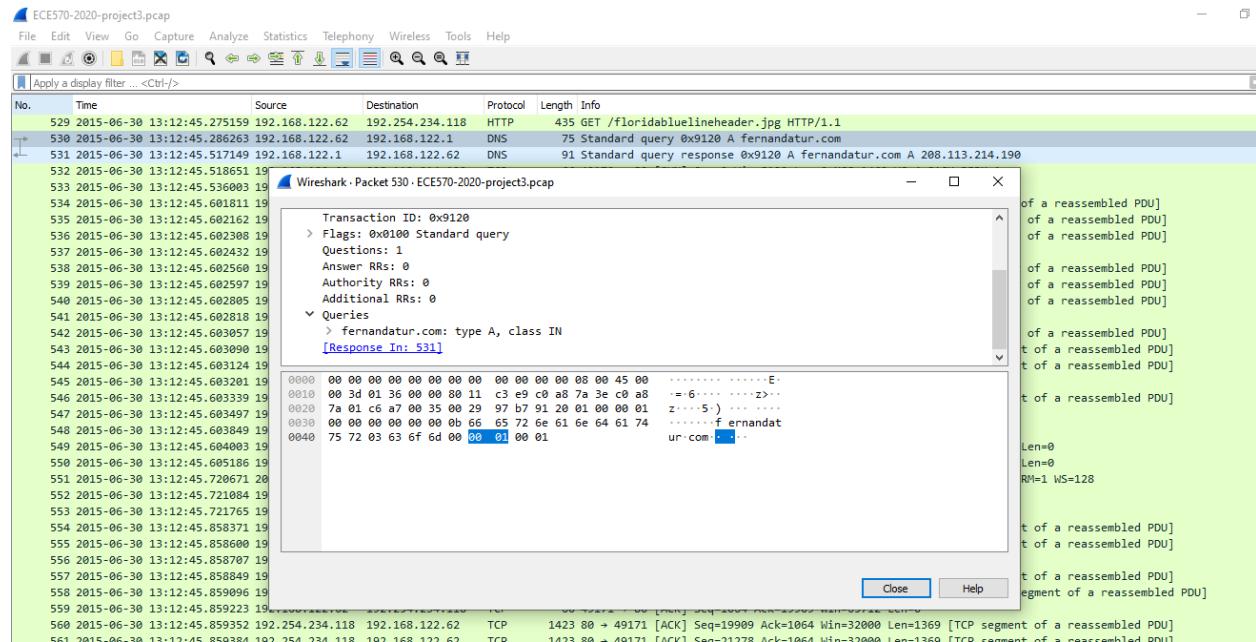
Note: The **HTTP 200 OK** success status response code indicates that the request has succeeded.

### 3. What is the IP address and domain name that delivered the malware?

This scenario that host machine infected some websites or IP address is start from frame 530 that host request to access to site fernandature.com

So,

in frame 530, host request to DNS for fernandature.com The website ip address is sent to host by DNS, 208.113.214.190 . The screenshot shows as a follows:



Host sent an SYN to this site from frame 532. In frame 551 ferandature.com sent an SYN.ACK to the host. Host sent back the ACK to this site in frame number 662. The picture as a following show this handshaking:



No.	Time	Source	Destination	Protocol	Length	Info
529	2015-06-30 13:12:45.275159	192.168.122.62	192.254.234.118	HTTP	435	GET /floridabluellineheader.jpg HTTP/1.1
530	2015-06-30 13:12:45.286269	192.168.122.62	192.168.122.1	DNS	75	Standard query response 0x912B A fernandatur.com A 200.113.214.190
531	2015-06-30 13:12:45.517149	192.168.122.1	192.168.122.62	DNS	91	Standard query response 0x912B A fernandatur.com A 200.113.214.190
532	2015-06-30 13:12:45.518851	192.168.122.62	200.113.214.198	TCP	66	49172 + 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1468 WS=4 SACK_PERM=1
533	2015-06-30 13:12:45.536083	192.254.234.118	192.168.122.62	TCP	54	88 + 49171 [ACK] Seq=43 Ack=1864 Win=32000 Len=8
534	2015-06-30 13:12:45.601811	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=743 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
535	2015-06-30 13:12:45.602162	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=2112 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
536	2015-06-30 13:12:45.602280	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=3481 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
537	2015-06-30 13:12:45.602432	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=3481 Win=65712 Len=8
538	2015-06-30 13:12:45.602568	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=4859 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
539	2015-06-30 13:12:45.602597	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=6219 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
540	2015-06-30 13:12:45.602895	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=7558 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
541	2015-06-30 13:12:45.602918	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=6219 Win=65712 Len=8
542	2015-06-30 13:12:45.603957	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=8957 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
543	2015-06-30 13:12:45.603989	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=1036 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
544	2015-06-30 13:12:45.603124	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=11695 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
545	2015-06-30 13:12:45.603201	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=11695 Win=65712 Len=8
546	2015-06-30 13:12:45.603339	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=13064 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
547	2015-06-30 13:12:45.603597	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=8957 Win=62972 Len=8
548	2015-06-30 13:12:45.603849	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=14433 Win=60236 Len=8
549	2015-06-30 13:12:45.604083	192.168.122.62	192.254.234.118	TCP	68	[TCP Window Update] 49171 + 80 [ACK] Seq=1054 Ack=14433 Win=63708 Len=8
550	2015-06-30 13:12:45.605186	192.168.122.62	192.254.234.118	TCP	68	[TCP Window Update] 49171 + 80 [ACK] Seq=1054 Ack=14433 Win=65712 Len=8
551	2015-06-30 13:12:45.720671	200.113.214.198	192.168.122.62	TCP	66	88 + 49172 [SYN] Seq=0 Win=14600 Len=8 MSS=1369 SACK_PERM=1 WS=128
552	2015-06-30 13:12:45.721084	192.168.122.62	200.113.214.198	TCP	68	49172 + 80 [ACK] Seq=1 Win=65712 Len=8
553	2015-06-30 13:12:45.721765	192.168.122.62	200.113.214.198	HTTP	412	GET /Xcripts/hpnyvrx2a.php?1#98015 HTTP/1.1
554	2015-06-30 13:12:45.858371	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=14433 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
555	2015-06-30 13:12:45.858608	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=15882 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
556	2015-06-30 13:12:45.858707	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=17171 Win=65712 Len=8
557	2015-06-30 13:12:45.858849	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=17171 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
558	2015-06-30 13:12:45.859096	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [PSH, ACK] Seq=18549 Ack=1864 Win=52088 Len=1369 [TCP segment of a reassembled PDU]
559	2015-06-30 13:12:45.859223	192.168.122.62	192.254.234.118	TCP	68	49171 + 80 [ACK] Seq=1864 Ack=19989 Win=65712 Len=8
560	2015-06-30 13:12:45.859352	192.254.234.118	192.168.122.62	TCP	1423	88 + 49171 [ACK] Seq=19989 Ack=1864 Win=32000 Len=1369 [TCP segment of a reassembled PDU]

And also in the above picture that is highlighted by a red pen. The time of frame 553 is 13:12:45.

We found two GET HTTP protocols in packettotal/HTTP . According to packet total report, we checked two files are HTTP on time 13:12:45 on virustotal.com

Malicious Activity	Suspicious Activity	Connections	DNS	HTTP	SSL Certificates	PKI (X.509)	Transferred Files	Strange Activity	Community Tags
<b>Similar Packet Captures</b>									
Search in results									
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host	
+ 2015-06-30 13:11:51 Z	C8y8Y2Q2yukRvbFS6	192.168.122.62	49158	216.88.200.46	80	1	GET	google.com	
+ 2015-06-30 13:11:51 Z	CMUHRQ3Jfj0FRKK1Qc	192.168.122.62	49159	216.88.200.47	80	1	GET	www.google.co.uk	
+ 2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.88.218.47	80	1	GET	www.google.co.uk	
+ 2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgfc62	192.168.122.62	49170	216.88.218.47	80	2	GET	www.google.co.uk	
+ 2015-06-30 13:12:44 Z	CALygR1JnJxOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.fondahusine.com	
+ 2015-06-30 13:12:45 Z	CALygR1JnJxOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.fondahusine.com	
+ 2015-06-30 13:12:45 Z	CMvAQV2OwfxQnVdhX2	192.168.122.62	49172	200.113.214.198	80	1	GET	fernandatur.com	
+ 2015-06-30 13:12:46 Z	CMHhzK1MViV1X1U2j	192.168.122.62	49173	200.113.214.198	80	1	GET	www.fondahusine.com	
+ 2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.38.45.45	80	1	GET	good.recycle2learn.com	
+ 2015-06-30 13:12:48 Z	CtG18l22yRPVIIlob	192.168.122.62	49175	46.38.45.45	80	1	GET	good.recycle2learn.com	



The first is related to [www.floridablueline.com](http://www.floridablueline.com) that source IP is Host (192.168.122.62) to the IP address of this site as a destination. We checked this file on virustotal and result is shown as a follows:

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:45 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	<a href="http://www.floridablueline.com">www.floridablueline.com</a>
URI	/floridabluelineheader.jpg							
Referrer	http://www.floridablueline.com/							
User Agent	...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) +							
Request Body Length	0							
Response Body Length	183799							
Status Code	200							
Status Message	OK							
Info Code	null							
Info Message	null							
File	null							
Username	null							
Password	null							
Proxied	null							
Sender File IDs	null							
Sender Mime Types	null							
Recipient File IDs	<a href="#">F3C1D2ENQEZU...</a>							
Recipient Mime Types	image/jpeg							
Client Headers	ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,HOST,CONNECTION							
Server Headers	null							
Cookie Variables	null							
URI Variables	/floridabluelineheader.jpg							

Virustotal scan result is this file that transfer visa HTTP protocol is clean.

f2ff22822d59da5361d7aee4f4f356a278e6f47976013aedec26790c45db5537

No engines detected this file

0 / 59

f2ff22822d59da5361d7aee4f4f356a278e6f47976013aedec26790c45db5537  
floridabluelineheader.jpg  
jpeg

Community Score: ?

DETECTION	DETAILS	COMMUNITY	
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
AVware	Undetected	Babable	Undetected

The second is related to fernandature.com that source IP is Host (192.168.122.62) to this site as a destination. We checked this file on virustotal and result is shown as follows:



-	2015-09-30 13:12:49 Z	CMvAQV2OvrXQnWdhX2	192.168.122.52	49172	268.113.214.198	80	1	GET	fernandatur.com
URI	/Scripts/hqnybx2w.php?id=960135								
Referrer	http://www.floridablueline.com/								
User Agent	... .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) ^								
Request Body Length	0								
Response Body Length	265								
Status Code	301								
Status Message	Moved Permanently								
Info Code	null								
Info Message	null								
File	null								
Username	null								
Password	null								
Proxied	null								
Sender File IDs	null								
Sender Mime Types	null								
Recipient File IDs	13PQYF223166807...	...							
Recipient Mime Types	text/html								
Server Headers	null								
Cookie Variables	null								
URI Variables	/Scripts/hqnybx2w.php?id								

Virustotal scan result is this file that transfer visa HTTP protocol is clean.



Σ feec02bb3cc6581fa226c60ea23b3c2e1a069e34a35ecb9025f5898488904162

No engines detected this file

0 / 58

Community Score

feec02bb3cc6581fa226c60ea23b3c2e1a069e34a35ecb9025f5898488904162  
hqnybx2w.php?id=960135

265.00 B | 2018-08-04 04:17:22 UTC | 2 years ago

html

DETECTION	DETAILS	COMMUNITY	
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
AVware	Undetected	Babable	Undetected

In wireshark capture data, in frame 553 that we highlighted in above last wireshark screenshot. We found GET scripts via fernandature.com

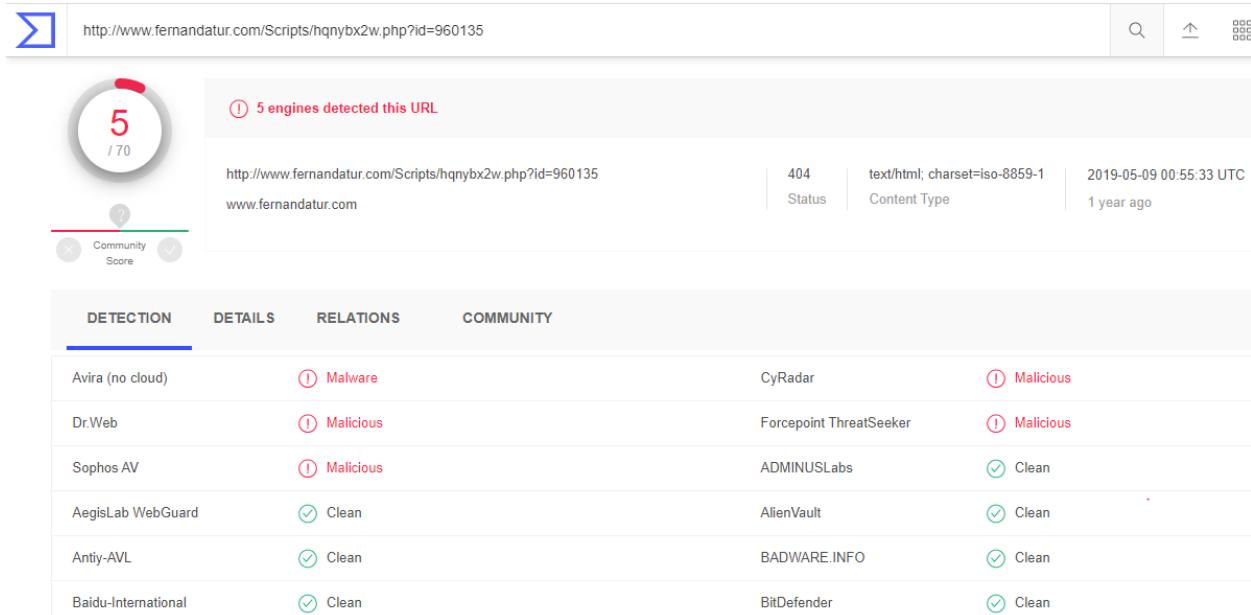


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
553	2015-06-30 13:12:45.721765	192.168.122.62	208.113.214.190	HTTP	432	GET /Scripts/hqnybx2w.php?id=960135 HTTP/1.1
554	2015-06-30 13:12:45.721765	EC5E70-2020-project3.pcap				TCP segment of a reassembled PDU
555	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
556	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
557	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
558	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
559	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
560	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
561	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
562	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
563	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
564	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
565	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
566	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
567	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
568	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
569	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
570	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
571	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
572	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
573	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
574	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
575	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
576	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
577	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
578	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
579	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
580	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
581	2015-06-30 13:12:45.721765					TCP segment of a reassembled PDU
582	2015-06-30 13:12:46.118388	192.254.234.118	192.168.122.62	TCP	1423	80 → 49171 [ACK] Seq=37706 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
583	2015-06-30 13:12:46.118409	192.254.234.118	192.168.122.62	TCP	60	49171 → 80 [ACK] Seq=1064 Ack=37706 Win=65712 Len=0 [TCP segment of a reassembled PDU]
584	2015-06-30 13:12:46.118640	192.254.234.118	192.168.122.62	TCP	1423	80 → 49171 [ACK] Seq=39875 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
585	2015-06-30 13:12:46.118806	192.254.234.118	192.168.122.62	TCP	1423	80 → 49171 [ACK] Seq=40444 Ack=1064 Win=32000 Len=1360 [TCP segment of a reassembled PDU]

When we checked this URL that shows with blue color on virustotal.com, we found that this URL is malicious and Malware. The screenshots are as following picture:



① 5 engines detected this URL

<http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135>

Community Score: 5 / 70

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware	CyRadar	① Malicious
Dr.Web	① Malicious	Forcepoint ThreatSeeker	① Malicious
Sophos AV	① Malicious	ADMINUSLabs	✓ Clean
AegisLab WebGuard	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean

According to Networkminer report, frame 553 is a file that name is hqnybx2w.php.html

NetworkMiner 2.5

File Tools Help

Select a network adapter in the list --

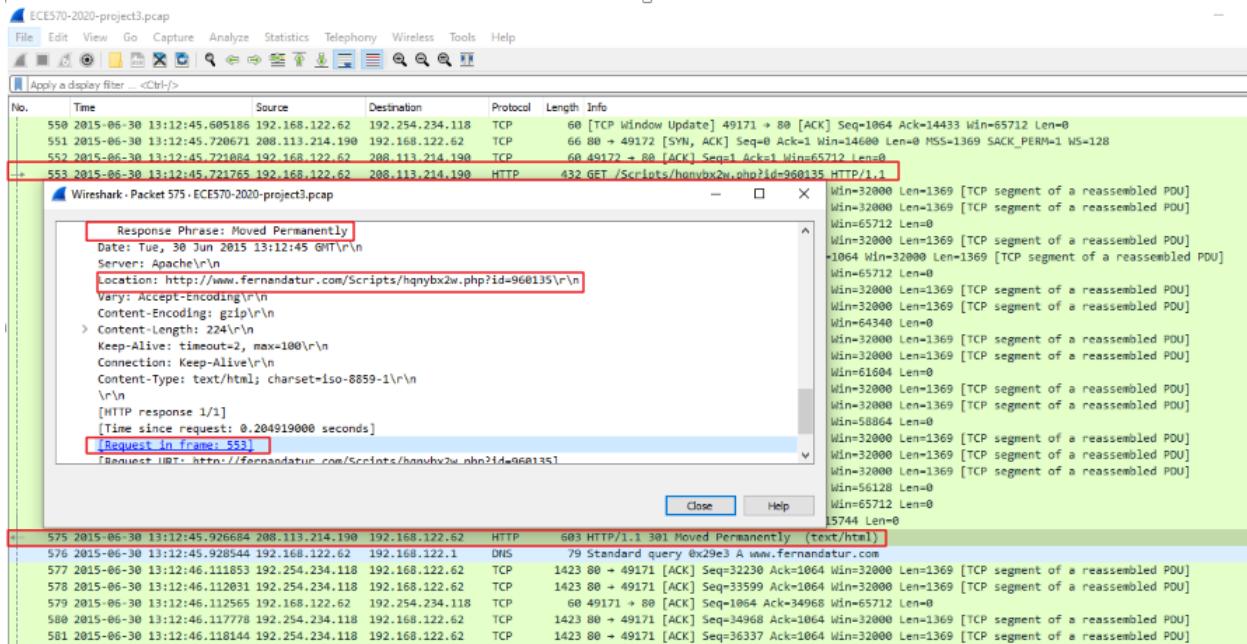
Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Filter keyword:  Case sensitive ExactPhrase Any column Clear App

Fram...	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed...	Details
96	www.google.co.uk[2].cer	cer	1150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=GeoTrust Global CA[2].cer
96	Google Internet Authority G2[2].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoTrust Global CA[2].cer
96	GeoTrust Global CA[2].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
105	google.com.cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
105	Google Internet Authority G2[3].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
109	www.google.co.uk[3].cer	cer	1150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=Geo
109	Google Internet Authority G2[4].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
317	google.com[1].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
317	Google Internet Authority G2[5].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
317	GeoTrust Global CA[5].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
354	google.com[2].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49167	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
354	Google Internet Authority G2[6].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
365	google.com[3].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
365	Google Internet Authority G2[7].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
365	GeoTrust Global CA[7].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
377	google.com[4].cer	cer	11737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Mou
377	Google Internet Authority G2[8].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Geo
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (Win...)	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc
512	url.888C5CB3.html	html	1070 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...)	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/?url=http://www.floridablueline.com
515	favicon.ico	ico	5430 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (Win...)	TCP 49170	HttpGetNormal	2015-06-30 13:12:44 ...	C:\Users\beh...	www.google.co.uk/favicon.ico
524	index.html	html	829 B	192.254.234.118 [floridablueline.co...]	TCP 80	192.168.122.62 (Win...)	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 ...	C:\Users\beh...	www.floridablueline.com/
553	hnybx2w.php.html	html	265 B	208.113.214.190 [fernandatur...	TCP 80	192.168.122.62 (Win...)	TCP 49172	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	fernandatur.com/Scripts/hnybx2w.php?id=960135
529	floridabluelineheader.jpg	jpg	183.79	192.254.234.118 [floridablueline.co...]	TCP 80	192.168.122.62 (Win...)	TCP 49172	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	www.floridablueline.com/floridabluelineheader.jpg
659	hnybx2w.php[1].html	html	323 B	208.113.214.190 [fernandatur...	TCP 80	192.168.122.62 (Win...)	TCP 49173	HttpGetNormal	2015-06-30 13:12:45 ...	C:\Users\beh...	www.fernandatur.com/Scripts/hnybx2w.php?id=960135
764	index.6558F0B7.html	html	142.97 ...	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (Win...)	TCP 49174	HttpGetNormal	2015-06-30 13:12:47 ...	C:\Users\beh...	good.recycle2team.com/?nKfrelLbVKDlU=3SKfPjx2f
811	index.php.swf	swf	15.763 B	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (Win...)	TCP 49175	HttpGetNormal	2015-06-30 13:12:49 ...	C:\Users\beh...	good.recycle2team.com/index.php?nKfrelLbVKDlU=3
841	version.xml11.6.602.html	html	351 B	23.10.250.43 [a1293.d.akamai.net] ...	TCP 80	192.168.122.62 (Win...)	TCP 49176	HttpGetNormal	2015-06-30 13:12:52 ...	C:\Users\beh...	fptdownload2.macromedia.com/get.flashplayer/update/ci
833	index.php.x-msdownload	x...	352.25 ...	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (Win...)	TCP 49174	HttpGetNormal	2015-06-30 13:12:51 ...	C:\Users\beh...	good.recycle2team.com/index.php?nKfrelLbVKDlU=43

In frame 575, in wireshark capture, we found that fernandature.com with IP address 208.113.214.190 sent HTTP1.1 moved permanently to the host machine(192.168.122.62) . Moreover, this frame is the response frame of 553. The wireshark screenshot is shown as a following picture:





Here, we found that A TCP handshake does not contain any redirect information. So TCP handshaking is fine. However, we check the application layer, we found that:

< HTTP/1.1 301 Moved Permanently ...

< Location: <http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135>

Since this is a 301 **permanent** redirect the client does not even need to visit the original site again but will instead use the new location on repeated tries. Only on the first try it will visit the original site to receive the redirect.

In Networkminer is again this redirection shows:

NetworkMiner 2.5

File Tools Help

— Select a network adapter in the list —

Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Filter keyword: **HTTP** Case sensitive ExactPhrase Any column Clear All

Parameter name	Parameter value	Frame num...	Source host	Source port	Destination host	Destination port	Timestamp	Details
Transfer-Encoding	chunked	526	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Connection	keep-alive	526	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Last-Modified	Thu, 04 Jun 2015 13:47:01 GMT	526	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Encoding	gzip	526	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
GET	/fondbluelineheader.jpg	529	192.168.122.62 (Windows)	TCP 49171	192.168.234.118 [fondblueline.com]	TCP 80	2015-06-30 13:12:45 UTC	HTTP Request to www.fondblueline.com
Referrer	http://www.fondblueline.com/	529	192.168.122.62 (Windows)	TCP 49171	192.168.234.118 [fondblueline.com]	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; ...)	529	192.168.122.62 (Windows)	TCP 49171	192.168.234.118 [fondblueline.com]	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
Host	www.fondblueline.com	529	192.168.122.62 (Windows)	TCP 49171	192.168.234.118 [fondblueline.com]	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
HTTP Response	200 OK	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Response
Server	nginx/1.8.0	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Date	Tue, 30 Jun 2015 13:12:45 GMT	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Type	image/jpeg	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Content-Length	183799	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Connection	keep-alive	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Last-Modified	Mon, 22 Dec 2014 20:25:51 GMT	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
Accept-Ranges	bytes	534	192.168.234.118 [fondblueline.com]	TCP 80	192.168.122.62 (Windows)	TCP 49171	2015-06-30 13:12:45 UTC	HTTP Header
GET	/Scripts/happybox2w.php?id=960135	553	192.168.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Request to fernandatur.com
Referrer	http://www.fondblueline.com/	553	192.168.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; ...)	553	192.168.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
Host	fernandatur.com	553	192.168.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
id	960135	553	192.168.122.62 (Windows)	TCP 49172	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:45 UTC	HTTP Header
HTTP Response	301 Moved Permanently	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Response
Date	Tue, 30 Jun 2015 13:12:45 GMT	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Server	Apache	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Location	http://www.fernandatur.com/Scripts/happybox2w.php?id=960135	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Vary	Accept-Encoding	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Encoding	gzip	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Length	224	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Keep-Alive	timeout=2, max=100	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Connection	Keep-Alive	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
Content-Type	text/html; charset=UTF-8	575	208.113.214.190 [fernandatur.com] [w...	TCP 80	192.168.122.62 (Windows)	TCP 49172	2015-06-30 13:12:45 UTC	HTTP Header
GET	/Scripts/happybox2w.php?id=960135	593	192.168.122.62 (Windows)	TCP 49173	208.113.214.190 [fernandatur...	TCP 80	2015-06-30 13:12:46 UTC	HTTP Request to www.fernandatur.com

Finally, as a report of packettotal in DNS Tab we can see that this site is redirected.

Malicious Activity Suspicious Activity Connections DNS HTTP SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

Similar Packet Captures

Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:11:51 Z	CFQesJ21Bmd4FhoX02	192.168.122.62	52719	192.168.122.1	53	udp	50039	google.com ↗
2015-06-30 13:11:51 Z	CRUDxWt1bC8Kb8Ud2	192.168.122.62	52063	192.168.122.1	53	udp	51086	www.google.co.uk ↗
2015-06-30 13:11:52 Z	CKxDXf4YbchmaV2uPk	192.168.122.62	56599	192.168.122.1	53	udp	40084	val.galactic.com ↗
2015-06-30 13:11:53 Z	Cz2QM11H8XmIDwuBl	192.168.122.62	55533	192.168.122.1	53	udp	31829	clients1.google.co.uk ↗
2015-06-30 13:12:44 Z	CXWf1zDG0quCNIAa8	192.168.122.62	57473	192.168.122.1	53	udp	62107	www.fernandatur.com ↗
2015-06-30 13:12:45 Z	CVZj034HeWhYEPJygd	192.168.122.62	50855	192.168.122.1	53	udp	37152	fernandatur.com ↗
2015-06-30 13:12:45 Z	CR9x8sdRd0MDUCG8	192.168.122.62	54137	192.168.122.1	53	udp	10723	www.fernandatur.com ↗
2015-06-30 13:12:47 Z	Cf090e4APdPX0d9MLI	192.168.122.62	59978	192.168.122.1	53	udp	48790	good.recycle2learn.com
2015-06-30 13:12:52 Z	CKdhc21h1h9uolHsm2g	192.168.122.62	54128	192.168.122.1	53	udp	23089	fpdownload.macromedia.com ↗
2015-06-30 13:16:12 Z	ChjHIC4Jp9Oh2MajSa	192.168.122.62	65237	192.168.122.1	53	udp	52954	time.windows.com ↗

When we click on whois Lookup we can see that those sites (fernandatur.com and www.fernandatur.com ) are Direct Allocation.All screenshots are shown as a following pictures:



2015-06-30 13:12:45 Z CVZlp34HeWhYEPJygd 192.168.122.62 50855 192.168.122.1 53 udp 37152 fernandatur.com

Query Class Desc C\_INTERNET  
 Query Type 1  
 Query Type Desc A  
 Response Code 0  
 Response Code Desc NOERROR  
 Authoritative Answer? F  
 Truncated? F  
 Recursion Desired? T  
 Recursion Available? T

Answers 208.113.254.198  
 TTLs 14389.00

Authoritative Response null  
 Additional Response(s) null

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:12:45 Z	CVZlp34HeWhYEPJygd							Whois
Whois <div style="border: 1px solid red; padding: 5px;"> <b>NetRange:</b> 208.113.128.0 - 208.113.255.255  <b>CIDR:</b> 208.113.128.0/17  <b>NetName:</b> DREAMHOST-BLK6  <b>NetHandle:</b> NET-208-113-128-0-1  <b>Parent:</b> NET-200 (NET-200-0-0-0-0)  <b>NetType:</b> Direct Allocation  <b>OriginAS:</b>  <b>Organization:</b> New Dream Network, LLC (NDN)  <b>RegDate:</b> 2006-04-12  <b>Updated:</b> 2012-03-02  <b>Ref:</b> https://rdap.arin.net/registry/ip/208.113.128.0                     </div> <b>OrgName:</b> New Dream Network, LLC <b>Orgid:</b> NDN								
2015-06-30 13:12:45 Z	CR9xfid							Query Class Desc C_INTERNET Query Type 1





2015-09-30 13:12:45 2 CR9x6sdRdQ0MDUCG8 192.168.122.62 54137 192.168.122.1 53 udp 10723 www.fernandature.com

Query Class Desc C\_INTERNET  
Query Type 1  
Query Type Desc A  
Response Code 0  
Response Code Desc NOERROR  
Authoritative Answer? F  
Truncated? F  
Recursion Desired? T  
Recursion Available? T

Answers 208.113.214.190  
TTLs 14399.00  
Authoritative Response null  
Additional Response(s) null

Timestamp Connect ID  
+ 2015-09-30 13:11:51 CFQuesJZ  
+ 2015-09-30 13:11:51 CKDXT4  
+ 2015-09-30 13:11:53 CZQM21  
+ 2015-09-30 13:12:44 CXWlizD  
+ 2015-09-30 13:12:45 CV2lp34  
- 2015-09-30 13:12:45 CR9x6sd

Whols

NetRange: 208.113.128.0 - 208.113.255.255  
CIDR: 208.113.128.0/17  
NetName: DREAMHOST-BLK6  
NetHandle: NET-208-113-128-0-1  
Parent: NET206 (NET-206-0-0-0-0)  
NetType: Direct Allocation  
OriginAS:  
Organization: New Dream Network, LLC (NDN)  
RegDate: 2006-04-12  
Updated: 2012-03-02  
Ref: https://rdap.arin.net/registry/ip/208.113.128.0

OrgName: New Dream Network, LLC  
OrgId: NDN

Note: We have a lot of TCP ACK between floridablueline.com and host from frame 533 after host open fernandature.com

At the end of seconds of 13:12:45, in frame 576 the host sent a request to DNS for open www.fernandature.com. In frame 609, DNS responded to the host and sent the IP address of this site. The IP address is 208.113.214.190.





The screenshot shows a Wireshark capture of network traffic. The packet list pane displays 592 DNS requests from 192.168.122.1 to 192.168.122.62. The first few packets are as follows:

- Pkt 576: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)  
Internet Protocol Version 4, Src: 192.168.122.62, Dst: 192.168.122.1  
User Datagram Protocol, Src Port: 54137, Dst Port: 53
- Pkt 577: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
DNS Standard query 0x29e3 A www.fernandatur.com
- Pkt 578: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=32230 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 579: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=33599 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 580: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=34968 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 581: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=36337 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 582: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=37708 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 583: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=39075 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 584: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=40444 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 585: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=41813 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 586: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=43182 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 587: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=44551 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 588: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=45920 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 589: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=47289 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 590: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=48658 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]
- Pkt 591: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=49171 + 80 [ACK] Seq=1064 Ack=43182 Win=65712 Len=0
- Pkt 592: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)  
TCP 192.168.122.62 > 192.168.122.1 [ACK] Seq=47289 Ack=1064 Win=32000 Len=1369 [TCP segment of a reassembled PDU]

In frame 610 host request to start TCP handshaking to IP address is 208.113.214.190.

In frame 610 send SYN, IP address 208.113.214.190 response SYN,ACK on frame 657. And immediately on frame 658 the host sent ACK to this IP address that is the website: [www.fernandature.com](http://www.fernandature.com).

In frame 659, the host machine sent one HTTP request to 208.113.214.190. This request was sent via HTTP protocol at 13:12:46. The wireshark screenshot is as follows:



ECE570-2020-project3.pcap

tcp.stream eq 15

No.	Time	Source	Destination	Protocol	Length	Info
61	2015-06-30 13:12:46.240613	192.168.122.62	208.113.214.198	TCP	66	49173 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1468 WS=4 SACK_PERM=1
657	2015-06-30 13:12:46.455244	208.113.214.198	192.168.122.62	TCP	60	80 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=128
658	2015-06-30 13:12:46.455635	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
659	2015-06-30 13:12:46.457724	192.168.122.62	208.113.214.198	HTTP	436	GET /Scripts/hqnybxzw.php?id=960135 HTTP/1.1
728	2015-06-30 13:12:46.660357	208.113.214.198	192.168.122.62	TCP	54	80 → 49173 [ACK] Seq=1 Ack=383 Win=15744 Len=0
757	2015-06-30 13:12:47.050032	208.113.214.198	192.168.122.62	HTTP	572	HTTP/1.1 200 OK (text/html)
761	2015-06-30 13:12:47.252248	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [ACK] Seq=383 Ack=519 Win=65192 Len=0
812	2015-06-30 13:12:49.052138	208.113.214.198	192.168.122.62	TCP	54	80 → 49173 [FIN, ACK] Seq=519 Ack=383 Win=15744 Len=0
813	2015-06-30 13:12:49.052332	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [ACK] Seq=383 Ack=520 Win=65192 Len=0
844	2015-06-30 13:12:52.787135	192.168.122.62	208.113.214.198	TCP	60	49173 → 80 [RST, ACK] Seq=383 Ack=520 Win=0 Len=0

Wireshark - Follow TCP Stream (tcp.stream eq 15) · ECE570-2020-project3.pcap

3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0  
Accept-Encoding: gzip, deflate  
Connection: Keep-Alive  
Host: www.fernandatur.com

HTTP/1.1 200 OK  
Date: Tue, 30 Jun 2015 13:12:46 GMT  
Server: Apache  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 297  
Keep-Alive: timeout=2, max=100  
Connection: Keep-Alive  
Content-Type: text/html

.....=....0@...|a...A..D...".!#qc...L.X.T.....,M.J.o)b..7C9M  
.45D.X5...Y...b.b...B.%rs  
....{4wng..0..J...34.....(..K..#.Op091,...Q.....+..;^h&.a.b.1.Q.k.....@\$>]....N..L..5.?...F.z....o  
...9Z.....=180..r6..\$.H..\*..3R.wfj..).Br.....n..E.E....\*(@.n..1..M.....2...C...

I client pkt, I server pkt, I cur.  
Entire conversation (900 bytes) Show and save data as: ASCII Stream 15

The host machine was infected by a file transferred on frame 526 from floridablueline.com and after that the host led to infection of other sites.

During that time again floridablueline.com sent an ACK to the host and after some ACK from this site the host sent a response.

According to packet total information, in HTTP Tab we found one data related to 13:12:46. After, download that file and check on virustotal. We found that this script is trojan. Infact, this script is the same as the script of frame 553. This file transferred to host in frame 526 from floridablueline.com .



Malicious Activity Suspicious Activity Connections DNS HTTP SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

Similar Packet Captures

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
[+] 2015-06-30 13:11:51 Z	Cs8Y2Q2yukRvbFS6	192.168.122.62	49158	216.58.208.46	80	1	GET	google.com
[+] 2015-06-30 13:11:51 Z	CMuHRQ3Jfj0FRkK1Qc	192.168.122.62	49159	216.58.218.47	80	1	GET	www.google.co.uk
[+] 2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgf62	192.168.122.62	49170	216.58.218.47	80	1	GET	www.google.co.uk
[+] 2015-06-30 13:12:44 Z	CIFU4P2TqMGvSgf62	192.168.122.62	49170	216.58.218.47	80	2	GET	www.google.co.uk
[+] 2015-06-30 13:12:44 Z	CaLygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	1	GET	www.floridablueline.com
[+] 2015-06-30 13:12:45 Z	CaLygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	2	GET	www.floridablueline.com
[+] 2015-06-30 13:12:45 Z	CMVAQV2OwIXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	1	GET	fernandatur.com
[+] 2015-06-30 13:12:46 Z	CMHzK1MViHV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com
[+] 2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.38.45.65	80	1	GET	good.recycle2learn.com
[+] 2015-06-30 13:12:48 Z	CtG8i22yrRPViLob	192.168.122.62	49175	46.38.45.65	80	1	GET	good.recycle2learn.com

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
- 2015-06-30 13:12:40 Z	CMHzK1MViHV1X1U2j	192.168.122.62	49173	208.113.214.190	80	1	GET	www.fernandatur.com

URI /Scripts/hqnybx2w.php?id=960135

Referrer http://www.floridablueline.com/

User Agent ...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Request Body Length 0

Response Body Length 323

Status Code 200

Status Message OK

Info Code null

Info Message null

File null

Username null

Password null

Proxied null

Sender File IDs null

Sender Mime Types null

Recipient File IDs f43ayX1v5tBLTT...

Recipient Mime Types application/javascript

Client Headers ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,CONNECTION,HOST

Server Headers null

Cookie Variables null

URI Variables /Scripts/hqnybx2w.php?id





SUMMARY		DETECTION	DETAILS	COMMUNITY
AegisLab			!	Script.Troj.Genlc
Avast			!	JS:Iframe-EOD [Trj]
AVG			!	JS:Iframe-EOD [Trj]
Bkav			!	JS:elframeDwNMe.FE8B
GData			!	Script.Trojan.Redirector.AZ
Ikarus			!	HTML.Framer
Qihoo-360			!	Virus.js.qexvmc.1
TrendMicro-HouseCall			!	Suspicious_GEN.F47V0731
Ad-Aware			✓	Undetected
AhnLab-V3			✓	Undetected
ALYac			✓	Undetected
Antiy-AVL			✓	Undetected
Arcabit			✓	Undetected

Again the URL of this site is in virus total indicates trojan. Same as frame 553.

http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135

5 engines detected this URL

http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135 | 404 Status | text/html; charset=iso-8859-1 Content Type | 2019-05-09 00:55:33 UTC | 1 year ago

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware	CyRadar	① Malicious
DrWeb	① Malicious	Forcepoint ThreatSeeker	① Malicious
Sophos AV	① Malicious	ADMINUSLabs	✓ Clean
AegisLab WebGuard	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean

In the connection Tab of the packet total we found that in time 13:12:46 the connection duration between host and 208.113.214.190 is 6:55 seconds.

Malicious Activity Suspicious Activity | Connections | DNS HTTP SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

Similar Packet Captures

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent
+ 2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	192.168.122.62	49172	208.113.214.190	80	tcp	http	2.95	378	630
+ 2015-06-30 13:12:45 Z	CR9x6sdRdQ0MDUCG8	192.168.122.62	54137	192.168.122.1	53	udp	dns	0.51	37	65
- 2015-06-30 13:12:46 Z	CMHzK1MVlhV1X1Uj	192.168.122.62	49173	208.113.214.190	80	tcp	http	6.55	382	634

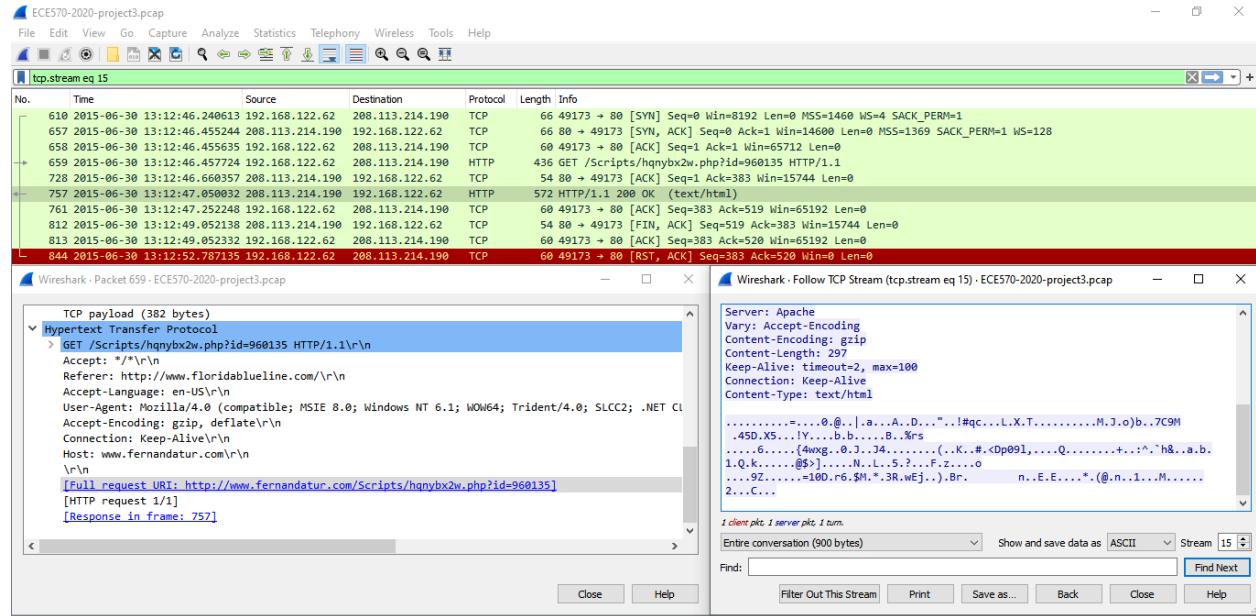
Payload Bytes Received 518  
 Total Bytes Received 690  
 Missed Bytes 0  
 Packets Sent 6  
 Packets Received 4  
 Originated Locally? null  
 Tunnel Parent Connection ID (empty)

History ShADadfR

After HTTP request of host to 208.113.214.190 in frame 659 to GET malicious scripts.  
 In frame 757, the target with 208.113.214.190 as an IP address sent HTTP 1.1 200 OK



to the host. The host IP address is 192.168.122.62. The wireshark screenshot and TCP stream is as a follows:



The Wireshark interface displays a list of network frames and a detailed TCP stream analysis.

**tcp.stream eq 15** (Selected Stream):

No.	Time	Source	Destination	Protocol	Length	Info
610	2015-06-30 13:12:46.240613	192.168.122.62	208.113.214.190	TCP	66	49173 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
657	2015-06-30 13:12:46.455244	208.113.214.190	192.168.122.62	TCP	64	80 → 49173 [SYN, ACK] Seq=1 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=128
658	2015-06-30 13:12:46.455635	192.168.122.62	208.113.214.190	TCP	68	49173 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
659	2015-06-30 13:12:46.457724	192.168.122.62	208.113.214.190	HTTP	436	GET /Scripts/hqnybx2w.php?id=960135 HTTP/1.1
728	2015-06-30 13:12:46.660357	208.113.214.190	192.168.122.62	TCP	54	80 → 49173 [ACK] Seq=1 Ack=383 Win=15744 Len=0
757	2015-06-30 13:12:47.050032	208.113.214.190	192.168.122.62	HTTP	572	HTTP/1.1 200 OK (text/html)
761	2015-06-30 13:12:47.252248	192.168.122.62	208.113.214.190	TCP	60	49173 → 80 [ACK] Seq=383 Ack=519 Win=65192 Len=0
812	2015-06-30 13:12:49.052138	208.113.214.190	192.168.122.62	TCP	54	80 → 49173 [FIN, ACK] Seq=519 Ack=383 Win=15744 Len=0
813	2015-06-30 13:12:49.052332	192.168.122.62	208.113.214.190	TCP	68	49173 → 80 [ACK] Seq=383 Ack=520 Win=65192 Len=0
844	2015-06-30 13:12:52.787135	192.168.122.62	208.113.214.190	TCP	60	49173 → 80 [RST, ACK] Seq=383 Ack=520 Win=0 Len=0

**TCP payload (382 bytes):**

```

> GET /Scripts/hqnybx2w.php?id=960135 HTTP/1.1\r\n
  Accept: */*\r\n
  Referer: http://www.floridablueline.com/\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; .NET 4.0.30319)\r\n
  Accept-Encoding: gzip,deflate\r\n
  Connection: Keep-Alive\r\n
  Host: www.fernandatur.com\r\n
  \r\n
[Full request URI: http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135]
[HTTP request 1/1]
[Response in frame: 757]
  
```

**Follow TCP Stream (tcp.stream eq 15) - ECE570-2020-project3.pcap:**

Server: Apache  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 297  
Keep-Alive: timeout=2, max=100  
Connection: Keep-Alive  
Content-Type: text/html

.....=.0@...|.a..A..D...".!#qc...L.X.T.....M.J.o)b..7C9M  
.45D.XS...!Y...B.B...B.%rs  
.....{4wg...0.J..34.....(.K..#.=<Op091,...Q.....+...^.'h&.a.b.  
1.Q.k.....@\$>)...N.L.S?...F.z...o  
.....92.....=100.r6.\$M.\*.3R.wEj..)Br....n..E.E....\*(@.n..1...M.....  
2.C...

Note: The **HTTP 200 OK** success status response code indicates that the request has succeeded.

In frame 758, new requests start. Host sent a request to the DNS server to access the site good.recycle2learn.com at 13:12:47. And in the next frame, DNS responded to the host and sent the IP address of this site. The ip address is 46.30.45.65. The wireshark screenshot is as a follow:



No.	Time	Source	Destination	Protocol	Length	Info
756	2015-06-30 13:12:46.987669	192.168.122.62	192.168.234.118	TCP	68	49171 → 88 [ACK] Seq=1064 Ack=184761 Win=65712 Len=0
757	2015-06-30 13:12:47.058032	288.113.214.198	192.168.122.62	HTTP	572	HTTP/1.1 200 OK (text/html)
758	2015-06-30 13:12:47.058553	192.168.122.62	192.168.122.62	DNS	82	[Standard query 0xbef96 A good.recycle2learn.com]
759	2015-06-30 13:12:47.298099	192.168.122.1	192.168.122.62	DNS	98	[Standard query response 0xbef96 A good.recycle2learn.com A 46.30.45.65]
760	2015-06-30 13:12:47.408610	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=14686 Win=4 SHCK_PERN=1
761	2015-06-30 13:12:47.252248	192.168.122.62	288.113.214.198	TCP	68	49173 → 88 [ACK] Seq=383 Ack=519 Win=65192 Len=0
762	2015-06-30 13:12:47.337263	46.30.45.65	192.168.122.62	TCP	58	88 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=14689 Len=0 MSS=1369
763	2015-06-30 13:12:47.472695	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=1 Win=64343 Len=0
764	2015-06-30 13:12:47.338158	192.168.122.62	46.30.45.65	HTTP	768	GET /?xn1KfreflBvKDfU-135KfPPrfTxzFGMSub-nDaa9GpkKCRLPh4SGhKrKCJ-ofSih170IPxzsmTu2KV_OpxqxeN85ZFT_zR3...
765	2015-06-30 13:12:47.462836	46.30.45.65	192.168.122.62	TCP	54	88 → 49174 [ACK] Seq=715 Win=15708 Len=0
766	2015-06-30 13:12:47.928739	288.113.214.198	192.168.122.62	TCP	58	88 → 49172 [IN, ACK] Seq=598 Ack=379 Win=15744 Len=0
767	2015-06-30 13:12:47.929308	192.168.122.62	288.113.214.198	TCP	68	49172 → 88 [ACK] Seq=379 Ack=551 Win=65168 Len=0
768	2015-06-30 13:12:48.462306	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=1 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
769	2015-06-30 13:12:48.462594	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=1378 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
770	2015-06-30 13:12:48.462636	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=2739 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
771	2015-06-30 13:12:48.463098	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=4188 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
772	2015-06-30 13:12:48.463184	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=4188 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
773	2015-06-30 13:12:48.463221	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=711 Ack=2739 Win=64343 Len=0
774	2015-06-30 13:12:48.465340	46.30.45.65	192.168.122.62	TCP	1406	88 → 49174 [PSH, ACK] Seq=6846 Ack=715 Win=15708 Len=1352 [TCP segment of a reassembled PDU]
775	2015-06-30 13:12:48.465351	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=6198 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
776	2015-06-30 13:12:48.465615	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=9567 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
777	2015-06-30 13:12:48.465976	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=5477 Win=64343 Len=0
778	2015-06-30 13:12:48.466420	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=6198 Win=64343 Len=0
779	2015-06-30 13:12:48.466471	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=10936 Win=61605 Len=0
780	2015-06-30 13:12:48.465351	192.168.122.62	288.113.214.198	TCP	68	49172 → 88 [RST, ACK] Seq=551 Win=0 Len=0
781	2015-06-30 13:12:48.465857	192.168.122.62	46.30.45.65	TCP	68	[TCP Window Update] 49174 → 88 [ACK] Seq=715 Ack=10936 Win=64343 Len=0
782	2015-06-30 13:12:48.485338	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=10936 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
783	2015-06-30 13:12:48.485338	192.168.122.62	46.30.45.65	TCP	1423	88 → 49174 [ACK] Seq=12387 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
784	2015-06-30 13:12:48.485786	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=13674 Win=64343 Len=0
785	2015-06-30 13:12:48.603284	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=13674 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
786	2015-06-30 13:12:48.603520	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=15043 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
787	2015-06-30 13:12:48.603711	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=16412 Win=64343 Len=0

After TCP handshaking in packet 760-761-762, the host sent ACK to 46.30.45.65. In frame number 764, the host sent an HTTP GET request to 46.30.45.65 at 13:12:47.

No.	Time	Source	Destination	Protocol	Length	Info
768	2015-06-30 13:12:47.200861	192.168.122.62	46.30.45.65	TCP	68	49176 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=14686 Win=4 SHCK_PERN=1
769	2015-06-30 13:12:47.252236	192.168.122.62	288.113.214.198	TCP	68	49176 → 88 [ACK] Seq=1811 Ack=519 Win=65192 Len=0
770	2015-06-30 13:12:47.887281	46.30.45.65	192.168.122.62	TCP	58	88 → 49174 [SYN, ACK] Seq=1811 Ack=519 Win=65192 Len=0
771	2015-06-30 13:12:47.887281	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Win=15708 Len=0
772	2015-06-30 13:12:47.887281	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=12387 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
773	2015-06-30 13:12:47.887281	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=16412 Win=64343 Len=0
774	2015-06-30 13:12:47.887281	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=12387 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
775	2015-06-30 13:12:47.887281	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=16412 Win=64343 Len=0
776	2015-06-30 13:12:47.887281	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=715 Ack=16412 Win=64343 Len=0
777	2015-06-30 13:12:47.887281	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=16412 Win=64343 Len=0
778	2015-06-30 13:12:47.887281	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=715 Ack=16412 Win=64343 Len=0
779	2015-06-30 13:12:47.887281	192.168.122.62	46.30.45.65	TCP	68	49174 → 88 [ACK] Seq=715 Ack=16412 Win=64343 Len=0
780	2015-06-30 13:12:47.887281	46.30.45.65	192.168.122.62	TCP	68	49172 → 88 [RST, ACK] Seq=551 Win=0 Len=0
781	2015-06-30 13:12:48.465857	192.168.122.62	46.30.45.65	TCP	68	[TCP Window Update] 49174 → 88 [ACK] Seq=715 Ack=10936 Win=64343 Len=0
782	2015-06-30 13:12:48.485338	46.30.45.65	192.168.122.62	TCP	1423	88 → 49174 [ACK] Seq=10936 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
783	2015-06-30 13:12:48.485338	192.168.122.62	46.30.45.65	TCP	1423	88 → 49174 [ACK] Seq=12387 Ack=715 Win=15708 Len=1369 [TCP segment of a reassembled PDU]
784	2015-06-30 13:12:48.485786	192.168.122.62	46.30.45.65	TCP	68	49172 → 88 [RST, ACK] Seq=551 Win=0 Len=0
785	2015-06-30 13:12:48.471666	46.30.45.65	192.168.122.62	TCP	54	88 → 49174 [ACK] Seq=1 Ack=715 Win=15708 Len=0
786	2015-06-30 13:12:47.928759	206.113.214.198	192.168.122.62	TCP	54	88 → 49172 [FIN, ACK] Seq=550 Ack=379 Win=15744 Len=0

```
> [SEQ/ACK analysis]
< [Timestamp]
[Time since first frame in this TCP stream: 0.137540000 seconds]
[Time since previous frame in this TCP stream: 0.000499000 seconds]
[TCP payload (714 bytes)]
> [Data transfer protocol]
GET /?xn1KfreflBvKDfU-135KfPPrfTxzFGMSub-nDaa9GpkKCRLPh4SGhKrKCJ-ofSih170IPxzsmTu2KV_OpxqxeN85ZFT_zR3...
Accept: application/x-ms-application, image/jpeg, application/x-ms-application/+xml, application/xaml+xml, image/gif, application/x-javascript, application/x-ms-xbap, application/x-ms-wmlc, application/vnd.ms-powerpoint, application/x-ms-tnef
Referer: http://www.floridablueinsure.com/v/v/
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; rv:11.0)
Accept-Encoding: gzip, deflate
Host: good.recycle2learn.com/v/v
Connection: Keep-Alive
VIA: 
[full request URL: http://good.recycle2learn.com/v/v/xn1KfreflBvKDfU-135KfPPrfTxzFGMSub-nDaa9GpkKCRLPh4SGhKrKCJ-ofSih170IPxzsmTu2KV_OpxqxeN85ZFT_zR3...]
[Response in frame: 885]
[Next request in frame: 833]
```



At 13:12:47 in File Transferred on packet total we found information that the host machine infected 46.30.45.65 with file as a script like the last two IP addresses which related to fernandature.com and www.fernandature.com . Screenshot is shown as a follows:

The screenshot shows a network traffic analysis interface. At the top, there are several tabs with file names and their corresponding MD5 hashes: CMHzK1MVlhV1X1U2j (F43AYX1VSTBLTT5...), b69afae73df2f68c5b3ddff91ab61e410 (713824ab6f35a5e4457a642e6d09b0054b5d4098), and 209.113.214.190 (192.168.122.62). Below the tabs, detailed file information is provided:

Mime Type	application/javascript
File Name	null
Total Bytes	null

The virustotal check result of this scripts shown as a follows:

The screenshot shows the VirusTotal analysis page for the file 5fbe87afde3c846dd0f6688abfb6af35ed0c96aeeb476bae7244add3c6ecb2. The page indicates that 8 engines detected the file. The file was uploaded on 2018-08-04 at 04:17:07 UTC (2 years ago).

DETECTION	DETAILS	COMMUNITY
AegisLab	Script.Troj.Genlc	Avast
AVG	JS:Iframe-EOD [Tr]	Bkav
GData	Script.Trojan.Redirector.AZ	Ikarus
Qihoo-360	Virus.js.qexvmc.1	TrendMicro-HouseCall
Ad-Aware	Undetected	AhnLab-V3
ALYac	Undetected	Anti-AVL

Network miner report on part Files prove that this scripts and file transferred to good.recycle2learn.com with IP address 46.30.45.65 from host (192.168.122.62).The screenshot shown as a follows:





NetworkMiner 2.5													
-- Select a network adapter in the list --													
Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies													
Filter keyword: <input type="text"/> <input checked="" type="checkbox"/> Case sensitive <input type="checkbox"/> ExactPhrase <input type="checkbox"/> Any column <input type="button" value="Clear"/> <input type="button" value="Apply"/>													
Fram...	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed...	Details	...	...
96	www.google.co.uk[2].cer	cer	1 150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=		
96	Google Internet Authority G2[2].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoTrust Inc.		
96	GeoTrust Global CA[2].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
105	google.com.cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=google.com, O=Google Inc, L=Mouri		
105	Google Internet Authority G2[3].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoG		
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
109	www.google.co.uk[3].cer	cer	1 150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=		
109	Google Internet Authority G2[4].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoG		
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
317	google.com[1].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:54 U...	C:\Users\beh...	TLS Certificate: CN=google.com, O=Google Inc, L=Mouri		
317	Google Internet Authority G2[5].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoG		
317	GeoTrust Global CA[5].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
354	google.com[2].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=google.com, O=Google Inc, L=Mouri		
354	Google Internet Authority G2[6].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoG		
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
365	google.com[3].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=google.com, O=Google Inc, L=Mouri		
365	Google Internet Authority G2[7].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoG		
365	GeoTrust Global CA[7].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
377	google.com[4].cer	cer	1 737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=google.com, O=Google Inc, L=Mouri		
377	Google Internet Authority G2[8].cer	cer	1 012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=GeoG		
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.		
512	url.868C5CB3.html	html	1 070 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (W...	TCP 49170	HttpGetNor...	2015-06-30 13:12:44 U...	C:\Users\beh...	www.google.co.uk/ur?url=http://www.floridablueline.com/		
515	favicon.ico	ico	5 430 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (W...	TCP 49170	HttpGetNor...	2015-06-30 13:12:44 U...	C:\Users\beh...	www.google.co.uk/favicon.ico		
524	index.html	html	829 B	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (W...	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 U...	C:\Users\beh...	www.floridablueline.com/		
553	hqnybx2w.php.html	html	265 B	208.113.214.190 [femandatur.com] ...	TCP 80	192.168.122.62 (W...	TCP 49172	HttpGetNor...	2015-06-30 13:12:45 U...	C:\Users\beh...	femandatur.com/Scripts/hqnybx2w.php?id=960135		
529	floridabluelineheader.jpg	jpg	183 79...	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (W...	TCP 49171	HttpGetNor...	2015-06-30 13:12:45 U...	C:\Users\beh...	www.floridablueline.com/floridabluelineheader.jpg		
659	hqnybx2w.php[1].html	html	323 B	208.113.214.190 [femandatur.com] ...	TCP 80	192.168.122.62 (W...	TCP 49173	HttpGetNor...	2015-06-30 13:12:46 U...	C:\Users\beh...	www.femandatur.com/Scripts/hqnybx2w.php?id=960135		
764	index.6558F0B7.html	html	142 97...	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (W...	TCP 49174	HttpGetNor...	2015-06-30 13:12:47 U...	C:\Users\beh...	good.recycle2team.com/?nilFredLBvKDIU43SKRfJxR		
811	index.php.swf	swf	15 763 B	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (W...	TCP 49175	HttpGetNor...	2015-06-30 13:12:48 U...	C:\Users\beh...	good.recycle2team.com/index.php?nilFredLBvKDIU43S...		
841	version.xml11.6.602.html	html	351 B	23.10.250.43 [a1293.akamaie.net] ...	TCP 80	192.168.122.62 (W...	TCP 49176	HttpGetNor...	2015-06-30 13:12:52 U...	C:\Users\beh...	fpdownload2.macromedia.com/get/flashplayer/update/cu...		
853	index.php.xmsdownload	x...	352 25...	46.30.45.65 [good.recycle2team.com]	TCP 80	192.168.122.62 (W...	TCP 49174	HttpGetNor...	2015-06-30 13:12:51 U...	C:\Users\beh...	good.recycle2team.com/index.php?nilFredLBvKDIU43S...		

In packettotal report, in HTTP Tab, we found one HTTP Transaction between Sender IP: 192.168.122.62 and target IP: 46.30.45.65 . The screenshot shown as a follows:

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:47 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.38.45.65	80	1	GET	good.recycle2learn.com
URI	/?xnIKfredLBvKDIU=3SKIPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0S2FT_zR3AaQ4llotXQB5MrPzwnEq\WvxWeioXW_RGNJ1hM-5DAFrE92lyjx-cUtsN2wR7QumAGzO0ZUEgbmA							
Referrer	http://www.floridablueline.com/							
User Agent	....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) ~							
Request Body Length	0							
Response Body Length	142971							
Status Code	200							
Status Message	OK							
Info Code	null							
Info Message	null							
File	null							
Username	null							
Password	null							
Proxied	null							
Sender File IDs	null							
Sender Mime Types	null							
Recipient File IDs	HEADERSMAP/XD93CT...▲							
Recipient Mime Types	text/html							
Client Headers	ACCEPT,REFERER,ACCEPT-LANGUAGE,USER-AGENT,ACCEPT-ENCODING,HOST,CONNECTION							
Server Headers	null							
Cookie Variables	null							
URI Variables	/?xnIKfredLBvKDIU							

The virustotal check of the file in this part illustrates that this script is trojan scripts. Again like other URLs , fernandature.com, www.fernandature.com this site good.recycled2learn.com and this scriptis is Trojan scripts and Malware. The screen shot of virustotal report is as follows:



Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

## VIRUSTOTAL

- SUMMARY
- DETECTION**
- DETAILS
- COMMUNITY

AegisLab	!	Trojan.HTML.Generic.4!c
ESET-NOD32	!	JS/Kryptik.AVE
Ikarus	!	JS.Exploit
Kaspersky	!	HEUR:Exploit.Script.Generic
McAfee-GW-Edition	!	BehavesLike.HTML.ExploitBlacole.cr
Microsoft	!	Trojan:Script/Wacatac.C!ml
Qihoo-360	!	Generic/Trojan.Exploit.b4f
Rising	!	Trojan.Kryptik!8.8 (TOPIS:E0:0xbvllh1xeV)
Sangfor Engine Zero	!	Malware
Sophos AV	!	Troj/ExpJS-KX
Symantec	!	Trojan.Gen.7
ZoneAlarm by Check Point	!	HEUR:Exploit.Script.Generic
Ad-Aware	✓	Undetected

The DNS Tab in the packet total gives information about sender IP is 192.168.122.62 and target IP is DNS server with IP address 192.168.122.1. Sender port is 59978 and target port is 53 on UDP transport protocol at 13:12:47. The screenshot is as follows:

Note:

**Port: 59978/TCP**

59978/TCP - Known port assignments (2 records found)		
Service	Details	Source
	Dynamic and/or Private Ports	IANA
	Xsan. Xsan Filesystem Access	Apple

**Port: 59978/UDP**

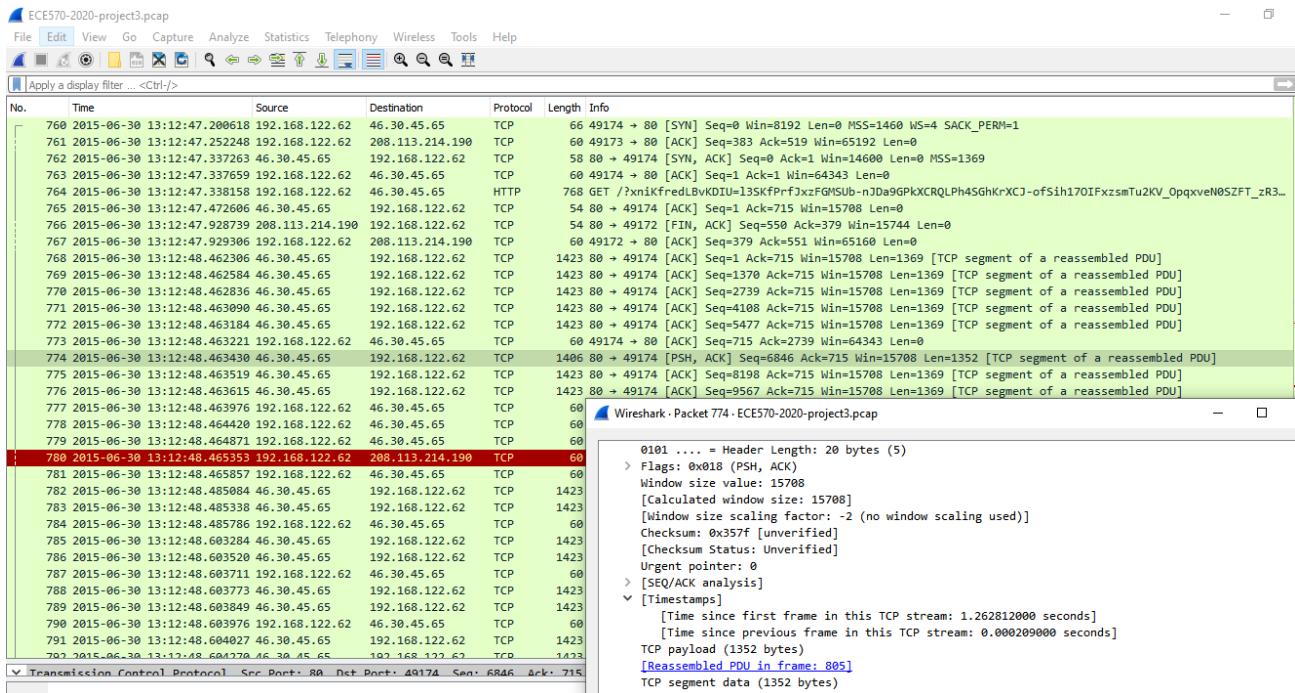
59978/UDP - Known port assignments (1 record found)		
Service	Details	Source
	Dynamic and/or Private Ports	IANA

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query
2015-06-30 13:12:47.2	Cf090e4APdPX0dSMLI	192.168.122.62	59978	192.168.122.1	53	udp	48790	good.recycle2learn.com
Query Class Desc C_INTERNET								
Query Type 1								
Query Type Desc A								
Response Code 0								
Response Code Desc NOERROR								
Authoritative Answer? F								
Truncated? F								
Recursion Desired? T								
Recursion Available? T								
Answers		46.30.45.65						
TTLs		3321.00						
Authoritative Response null								
Additional Response(s) null								

In frame 768, good.recycle2learn.com with IP address 46.30.45.65 sent some ACK to the host. After 5 frames, the host sent ACK to respond in time :13:12:48.

In frame 774, good.recycle2learn.com with IP address 46.30.45.65 sent some PSH,ACK to the host. PSH,ACK indicates the host is acknowledging receipt of some previous data and also transmitting some more data.





According to information on packettotal in the Connections part, we found a packet information between host and good,recycle2learn.com on TCP transport protocol and http services.

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent
2015-06-30 13:12:48.2	CtG18I22yRPVILob	192.168.122.62	49175	46.30.45.65	80	tcp	http	67.17	724	1216
Payload Bytes Received 15932										
Total Bytes Received 16536										
Missed Bytes 0										
Packets Sent 12										
Packets Received 15										
Originated Locally? null										
Tunnel Parent Connection ID (empty)										
History ShADadIR										

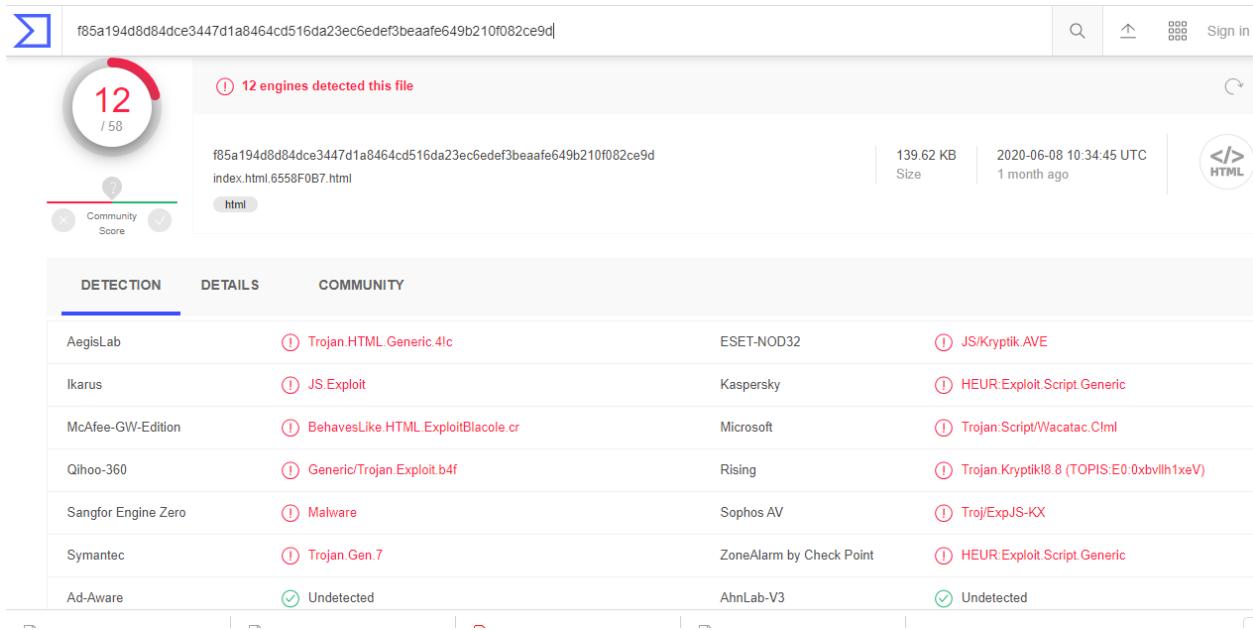
Data from Files Transferred in packet total illustrates that the data transferred between 46.30.45.65 and 192.168.122.62 are malware and virustotal indicates that this is a



Trojan script. 12 engines prove this, and text/html file is detected by 12 engines. The screenshots are as a follows:

Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth
+ 2015-06-30 13:12:47 Z	CMHzK1MViV1X1U2j	F43ATXVSTBLTT... ↗	b6d9efae73df2f6dc5b3ddff51ab0b1e418 ↗ vb % Q	713824a0#f5a5e4457ad42e6d0be054b5dd4fb9 ↗ vb % Q	208.113.214.198 ↗ vb % Q	192.168.122.62 ↗	HTTP	0
- 2015-06-30 13:12:48 Z	CocBdE3VP4U7EE8PX5	FEEAQMAPX0NSCT... ↗	4634a951740f14922d030e8d2add97a18 ↗ vb % Q	bd7777893cd315f781545e4263500e9f483c1e ↗ vb % Q	46.38.45.65 ↗	192.168.122.62 ↗	HTTP	0

Mime Type: text/html  
File Name: null  
Total Bytes: null



The screenshot shows a file entry for f85a194d8d84dce3447d1a8464cd516da23ec6edef3beaafe649b210f082ce9d. A circular progress bar indicates 12 detections out of 58. The file is identified as index.html.6558F0B7.html and is categorized as html. The detection details table lists 12 engines that detected the file, including AegisLab, Ikarus, McAfee-GW-Edition, Qihoo-360, Sangfor Engine Zero, Symantec, and Ad-Aware, among others.

DETECTION	DETAILS	COMMUNITY	
AegisLab	① Trojan.HTML.Generic.4lc	ESET-NOD32	① JS/Kryptik.AVE
Ikarus	① JS Exploit	Kaspersky	① HEUR.Exploit.Script.Generic
McAfee-GW-Edition	① BehavesLike HTML ExploitBlacole.cr	Microsoft	① Trojan.Script/Wacatac.Clml
Qihoo-360	① Generic/Trojan.Exploit.b4f	Rising	① Trojan.Kryptik!8.8 (TOPIS:E0.0xbvllh1xeV)
Sangfor Engine Zero	① Malware	Sophos AV	① Troj/ExpJS-KX
Symantec	① Trojan.Gen.7	ZoneAlarm by Check Point	① HEUR.Exploit.Script.Generic
Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected

Packettotal malicious activity illustrates that at 13:12:48, we found two alert descriptions. The screenshot is shown as a follows:



**Similar Packet Captures**

Search in results											
Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname		
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag	1	192.254.234.118	80	192.168.122.62	49171	TCP	<a href="#">www.floridablueline.com</a>		
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09	1	192.254.234.118	80	192.168.122.62	49171	TCP	<a href="#">www.floridablueline.com</a>		
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 08	1	192.254.234.118	80	192.168.122.62	49171	TCP	<a href="#">www.floridablueline.com</a>		
2015-06-30 13:12:48 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Landing URI Struct March 20 2015	1	192.168.122.62	49174	46.39.45.65	80	TCP	good.recycle2learn.com		
2015-06-30 13:12:48 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG EK Landing March 20 2015 M2	1	46.39.45.65	80	192.168.122.62	49174	TCP	good.recycle2learn.com		
2015-06-30 13:12:49 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Windows Flash Version IE	1	192.168.122.62	49175	46.39.45.65	80	TCP	good.recycle2learn.com		
2015-06-30 13:12:49 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Exploit URI Struct	1	192.168.122.62	49175	46.39.45.65	80	TCP	good.recycle2learn.com		

In this time, we check both alerts at time 13:12:48

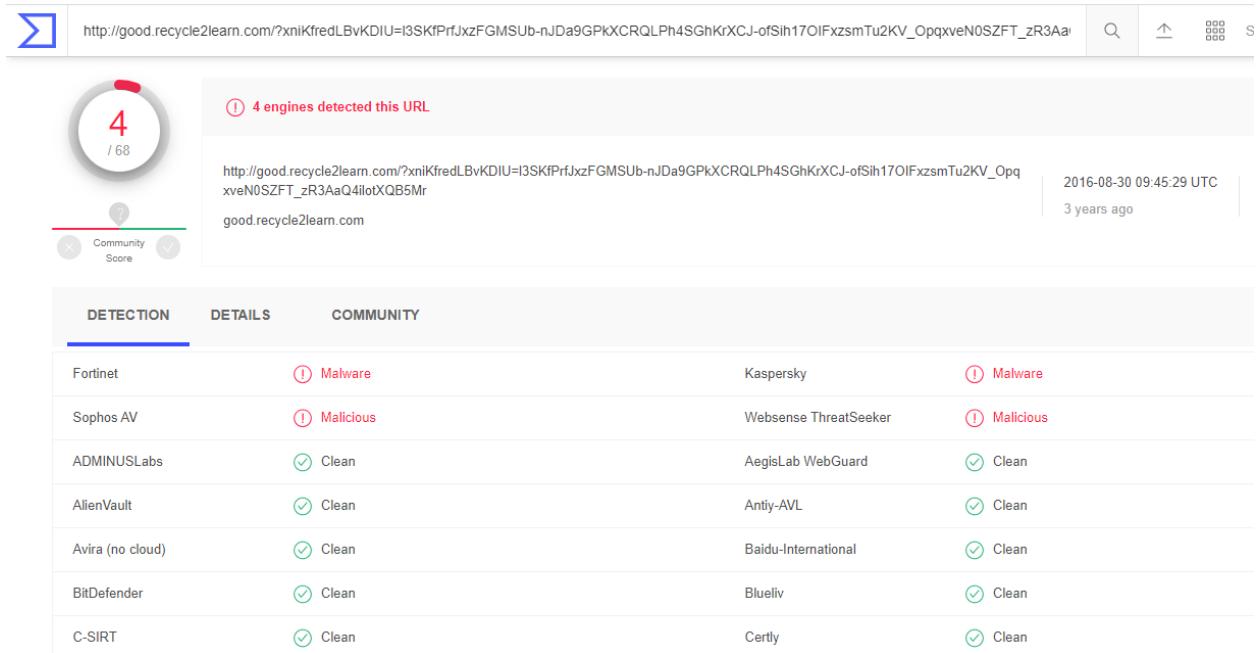
At first open those alerts we can see that the first alert is ET CURRENT\_EVENTS RIG Landing URI Struct March 20 2015.

Note: One of the most well-known exploit kits in the crimeware underground marketplaces, clearly dominating the overall exploit kits category during the last several months, is no other but the RIG EK. Many words have been poured on RIG's close ties to Ransomware.

2015-06-30 13:12:48 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Landing URI Struct March 20 2015	1	192.168.122.62	49174	46.39.45.65	80	TCP	good.recycle2learn.com
HTTP URI ...zwnEqWwx!WeioXW_RGJN1hM-5DAFrE92lyjx-cUlsN2wR7QumAGzO0ZUEgbmA									
HTTP Content-Type text/html									
HTTP Method GET									
HTTP User Agent ...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)									
HTTP Referrer <a href="http://www.floridablueline.com/">http://www.floridablueline.com/</a>									
HTTP Protocol HTTP/1.1									
HTTP Length 2542									
HTTP Status Code 200									



When we copy the Url to check on virustotal. We found that this is malware.



DETECTION	DETAILS	COMMUNITY
Fortinet	<span style="color: red;">!</span> Malware	Kaspersky <span style="color: red;">!</span> Malware
Sophos AV	<span style="color: red;">!</span> Malicious	Wesense ThreatSeeker <span style="color: red;">!</span> Malicious
ADMINUSLabs	<span style="color: green;">✓</span> Clean	AegisLab WebGuard <span style="color: green;">✓</span> Clean
AlienVault	<span style="color: green;">✓</span> Clean	Antiy-AVL <span style="color: green;">✓</span> Clean
Avira (no cloud)	<span style="color: green;">✓</span> Clean	Baidu-International <span style="color: green;">✓</span> Clean
BitDefender	<span style="color: green;">✓</span> Clean	Blueliv <span style="color: green;">✓</span> Clean
C-SIRT	<span style="color: green;">✓</span> Clean	Certy <span style="color: green;">✓</span> Clean

In the second alert ET CURRENT\_EVENTS RIG EK Landing March 20 2015 M2, we found that this alert is between good.recycle2learn.com and host on TCP protocol.

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-08-30 13:12:48 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG EK Landing March 20 2015 M2	1	 46.38.45.45	80	 192.168.122.62	49174	TCP	good.recycle2learn.com
HTTP URI /?xniKfredLBvKDIU=l3SKfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV_OpqxveN0SZFT_zR3AaQ4IotQB5MrPzwnEqWvxWeioXW_RGJN1hM-5DAFrE92lyjx-cUIsN2wR7QuAGzO0ZUEgbrA									
HTTP Content-Type text/html									
HTTP Method GET									
HTTP User Agent Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)									
HTTP Referrer http://www.floridablueline.com/									
HTTP Protocol HTTP/1.1									
HTTP Length 13477									
HTTP Status Code 200									

When we copy this url to virustotal.com to check detected engines. Screenshot is as a follow:



 http://good.recycle2learn.com/?xniKfredLBvKDIU=l3SKfPrfJxzFGMSUb-nJDa9GPKXCRQLPh4SGhKrXCJ-ofSih170lFxzsmTu2KV\_OpqxeN0SZFT\_zR3Aa...    



① 4 engines detected this URL

http://good.recycle2learn.com/?xniKfredLBvKDIU=l3SKfPrfJxzFGMSUb-nJDa9GPKXCRQLPh4SGhKrXCJ-ofSih170lFxzsmTu2KV\_OpqxeN0SZFT\_zR3Aa...  
good.recycle2learn.com

Community Score

2016-08-30 09:45:29 UTC  
3 years ago

DETECTION	DETAILS	COMMUNITY
Fortinet	① Malware	Kaspersky ① Malware
Sophos AV	① Malicious	Websense ThreatSeeker ① Malicious
ADMINUSLabs	✓ Clean	AegisLab WebGuard ✓ Clean
AlienVault	✓ Clean	Antly-AVL ✓ Clean
Avira (no cloud)	✓ Clean	Baidu-International ✓ Clean
BitDefender	✓ Clean	Blueliv ✓ Clean

Only one item available in File Transferred related to time 13:12:48

Timestamp	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Dest
2015-08-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	f1pqyf223t060r07...	f162bf38954f64dd8eef8359575b624b829e8598	208.113.214.198	192.168.122.62	HTTP	0
2015-08-30 13:12:47 Z	CMHhzK1MViIhV1X1U2j	f43ayx1vstbltts...	b69afac73df2f68c5b3deff516b1e418	208.113.214.198	192.168.122.62	HTTP	0
2015-08-30 13:12:48 Z	CocBdE3VP4U7EE8PX5	fead09nafx065ct...	4634a93760f14922d030e8d2ad497a19	208.113.214.198	192.168.122.62	HTTP	0
Mime Type text/html							
File Name null							
Total Bytes null							

The file type is text.html. And also, in NetworkMiner we can find that this packet that sent the frame is 811. The file type is swf.



NetworkMiner 2.5

File Tools Help

Select a network adapter in the list --

Hosts (14) Files (39) Images (2) Messages Credentials (2) Sessions (20) DNS (18) Parameters (754) Keywords Anomalies

Filter keyword:  Case sensitive  ExactPhrase  Any column

Fram...	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed...	Details
96	www.google.co.uk[2].cer	cer	1150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=
96	Google Internet Authority G2[2].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
96	Geo Trust Global CA[2].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Geo Trust Global CA, O=GeoTrust Inc.
105	google.com.cer	cer	1737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Moun
105	Google Internet Authority G2[3].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.
109	www.google.co.uk[3].cer	cer	1150 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=
109	Google Internet Authority G2[4].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.
317	google.com[1].cer	cer	1737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 U...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Moun
317	Google Internet Authority G2[5].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
317	Geo Trust Global CA[5].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 U...	C:\Users\beh...	TLS Certificate: CN=Geo Trust Global CA, O=GeoTrust Inc.
354	google.com[2].cer	cer	1737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Moun
354	Google Internet Authority G2[6].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.
365	google.com[3].cer	cer	1737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Moun
365	Google Internet Authority G2[7].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
365	Geo Trust Global CA[7].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Geo Trust Global CA, O=GeoTrust Inc.
377	google.com[4].cer	cer	1737 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN="google.com, O=Google Inc, L=Moun
377	Google Internet Authority G2[8].cer	cer	1012 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67 [www.google.co.uk] ...	TCP 443	192.168.122.62 (W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 U...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc.
512	url.8865CB3.html	html	1070 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (W...	TCP 49170	HttpGetNor...	2015-06-30 13:12:44 U...	C:\Users\beh...	www.google.co.uk?url=http://www.floridablueline.com/
515	favicon.ico	ico	5430 B	216.58.210.67 [www.google.co.uk] ...	TCP 80	192.168.122.62 (W...	TCP 49170	HttpGetNor...	2015-06-30 13:12:44 U...	C:\Users\beh...	www.google.co.uk/favicon.ico
524	index.html	html	829 B	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (W...	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 U...	C:\Users\beh...	www.floridablueline.com/
553	hnybx2w.php[1].html	html	265 B	208.113.214.190 [femandatur.com] ...	TCP 80	192.168.122.62 (W...	TCP 49172	HttpGetNor...	2015-06-30 13:12:45 U...	C:\Users\beh...	femandatur.com/Scripts/hnybx2w.php?id=960135
529	floridabluelineheader.jpg	jpg	183 79	192.254.234.118 [floridablueline.co...	TCP 80	192.168.122.62 (W...	TCP 49171	HttpGetNor...	2015-06-30 13:12:45 U...	C:\Users\beh...	www.floridablueline.com/floridabluelineheader.jpg
659	hnybx2w.php[1].html	html	323 B	208.113.214.190 [femandatur.com] ...	TCP 80	192.168.122.62 (W...	TCP 49173	HttpGetNor...	2015-06-30 13:12:46 U...	C:\Users\beh...	www.femandatur.com/Scripts/hnybx2w.php?id=960135
764	index.6558F0B7.html	html	142 97	46.30.45.65 [good.recycle2team.com] ...	TCP 80	192.168.122.62 (W...	TCP 49174	HttpGetNor...	2015-06-30 13:12:47 U...	C:\Users\beh...	good.recycle2team.com/index.php?xnKred.BvKDUI=35KFJzF.
811	index.php.swf	swf	15 763 B	46.30.45.65 [good.recycle2team.com] ...	TCP 80	192.168.122.62 (W...	TCP 49175	HttpGetNor...	2015-06-30 13:12:48 U...	C:\Users\beh...	good.recycle2team.com/index.php?xnKred.BvKDUI=35
841	version.xml11.6.602.html	html	351 B	23.10.250.43 [a123d.akamai.net] ...	TCP 80	192.168.122.62 (W...	TCP 49176	HttpGetNor...	2015-06-30 13:12:52 U...	C:\Users\beh...	fpdownload2.macromedia.com/get_flashplayer/update/cu
833	index.php.x-msdownload	x---	352 25...	46.30.45.65 [good.recycle2team.com] ...	TCP 80	192.168.122.62 (W...	TCP 49174	HttpGetNor...	2015-06-30 13:12:51 U...	C:\Users\beh...	good.recycle2team.com/index.php?xnKred.BvKDUI=35

Based on the virustotal report, this file is malware when we click on virustotal lookup in File Transferred.

 f85a194d8d84dce3447d1a8464cd516da23ec6edef3beaafe649b210f082ce9d |    

12 engines detected this file

f85a194d8d84dce3447d1a8464cd516da23ec6edef3beaafe649b210f082ce9d |  

DETECTION	DETAILS	COMMUNITY	
AegisLab	① Trojan HTML Generic 4ic	ESET-NOD32	① JS/Kryptik AVE
Ikarus	① JS Exploit	Kaspersky	① HEUR/Exploit Script Generic
McAfee-GW-Edition	① BehavesLike HTML ExploitBlacole.cr	Microsoft	① Trojan Script/Wacatac.C!ml
Qihoo-360	① Generic/Trojan Exploit.b4f	Rising	① Trojan Kryptik!8.8 (TOPIS:E.0xbvllh1xeV)
Sangfor Engine Zero	① Malware	Sophos AV	① Troj/ExpJS-KX
Symantec	① Trojan.Gen.7	ZoneAlarm by Check Point	① HEUR/Exploit Script Generic
Ad-Aware	② Undetected	AhnLab-V3	② Undetected



According to HTTP report on packettotal, we found that in time 13:12:48

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-08-30 13:12:48 Z	CTGj8I22yrRPVlOb	192.168.122.62	49175	46.38.45.65	80	1	GET	good.recycle2learn.com
URI	/index.php?xniKfredLBvKDIU=3SMIPrJxzFGMSUb-nJDa9GPXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqveN0S2FT_zR3AaQ4idtXQB5MrPzwmEqWwxWeioXW_RGJN1hM-5DAFrE92lyjx-cUlsNzwR7CumAGz00ZUEg0ogqAQlryIQ-Dbgf6V0ggEkgP2VlxrIUmityh42F28STNzKM							
Referrer	http://good.recycle2learn.com/?xniKfredLBvKDIU=3SMIPrJxzFGMSUb-nJDa9GPXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqveN0S2FT_zR3AaQ4idtXQB5Mr							
User Agent	...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) ˇ							
Request Body Length	0							
Response Body Length	15763							
Status Code	200							
Status Message	OK							
Info Code	null							
Info Message	null							
File	null							
Username	null							
Password	null							
Proxied	null							
Sender File IDs	null							
Sender Mime Types	null							
Recipient File IDs	TSQBL2N1BEPKA... 							
Recipient Mime Types	application/x-shockwave-flash							
Client Headers	ACCEPT,ACCEPT-LANGUAGE,REFERER,X-FLASH-VERSION,ACCEPT-ENCODING,USER-AGENT,HOST,CONNECTION							
Server Headers	null							
Cookie Variables	null							
URI Variables	/index.php?xniKfredLBvKDIU							

After, download the file and check it on virustotal, virustotal result check is shown as a follows:





University  
of Victoria

✗ 35 engines detected this file



Community  
Score

cf76f50d725d971469cc54c953be243722bfc4a853c12e4f95571e8a413eb489

index.php.BADF5050.x-shockwave-flash





VIRUSTOTAL

SUMMARY DETECTION DETAILS COMMUNITY 4

Scanner	Detection
Ad-Aware	Script.SWF.Exploit.CVE-2015-3105.C500
AegisLab	Hacktool.SWF.Agent.3lc
AhnLab-V3	SWF/Exploit
ALYac	Script.SWF.Exploit.CVE-2015-3105.C500
Antiy-AVL	Trojan[Exploit]/SWF.SWF.Generic
Arcabit	Script.SWF.Exploit.CVE-2015-3105.C500
Avast	SWF:Malware-gen [Tr]
AVG	SWF:Malware-gen [Tr]
Avira (no cloud)	EXP/Agent.EB.48
BitDefender	Script.SWF.Exploit.CVE-2015-3105.C500
CAT-QuickHeal	SWF.Kit.Nuclear.N
ClamAV	Swf.Exploit.Kit-99
Comodo	Malware@#2iqyxbwC2caZK

← → ⌛ ⌂ https://www.virustotal.com/gui/file/cf76f5c... ... ⌂ ⌂ ⌂

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter



## VIRUSTOTAL



SUMMARY

DETECTION

DETAILS

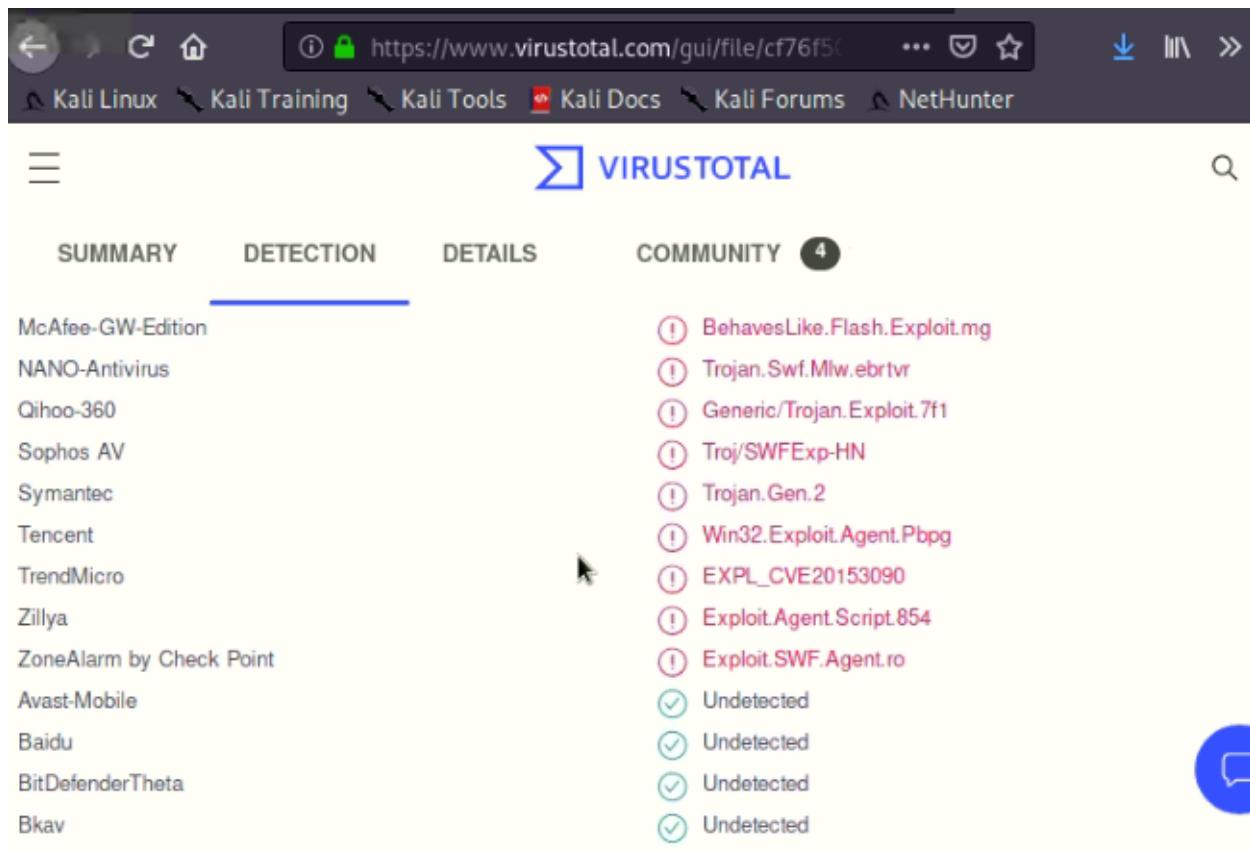
COMMUNITY

4

Cyren  
DrWeb  
Emsisoft  
eScan  
ESET-NOD32  
F-Prot  
F-Secure  
FireEye  
GData  
Ikarus  
Kaspersky  
MAX  
McAfee

- ! SWF/SWF/Exploit
- ! Exploit.SWF.1232
- ! Script.SWF.Exploit.CVE-2015-3105.C500 (B)
- ! Script.SWF.Exploit.CVE-2015-3105.C500
- ! SWF/Exploit.ExKit.AS
- ! SWF/SWF/Exploit
- ! Exploit.EXP/Agent.EB.48
- ! Script.SWF.Exploit.CVE-2015-3105.C500
- ! Script.SWF.Exploit.CVE-2015-3105.C500
- ! Trojan.SWF.Exploit
- ! Exploit.SWF.Agent.ro
- ! Malware (ai Score=100)
- ! SWF/Exploit-Rig.a





The screenshot shows the VirusTotal interface with the 'DETECTION' tab selected. On the left, a list of 17 antivirus engines and services (McAfee-GW-Edition, NANO-Antivirus, Qihoo-360, Sophos AV, Symantec, Tencent, TrendMicro, Zillya, ZoneAlarm by Check Point, Avast-Mobile, Baidu, BitDefenderTheta, Bkav) are listed. To the right, their detection results are shown in a grid. Most engines detect the file as malicious (indicated by red exclamation marks), while TrendMicro, Baidu, BitDefenderTheta, and Bkav detect it as undetected (indicated by green checkmarks). A blue speech bubble icon is visible on the right side.

Detection	McAfee-GW-Edition	NANO-Antivirus	Qihoo-360	Sophos AV	Symantec	Tencent	TrendMicro	Zillya	ZoneAlarm by Check Point	Avast-Mobile	Baidu	BitDefenderTheta	Bkav
Malicious	! BehavesLike.Flash.Exploit.mg	! Trojan.Swf.Mlw.ebrtv	! Generic/Trojan.Exploit.7f1	! Troj/SWFExp-HN	! Trojan.Gen.2	! Win32.Exploit.Agent.Pbpg	! EXPL_CVE20153090	! Exploit.Agent.Script.854	! Exploit.SWF.Agent.ro	Undetected	Undetected	Undetected	Undetected

In the connections Tab of packet total, we can see that connection established between host and good.recycle2learn.com. The duration is 67:17 seconds on http. The screenshot as a follows:



The screenshot shows the NetworkMiner tool interface with a single connection entry. The connection details are as follows:

Time	Source IP	Destination IP	Protocol	Duration	HTTP Status	HTTP Response Length	HTTP Headers
2015-06-30 13:12:48 Z	192.168.122.62	49175	tcp	67.17	724	1216	HTTP/1.1 200 OK

Below the table, the packet details are listed:

- Payload Bytes Received 15932
- Total Bytes Received 16536
- Missed Bytes 0
- Packets Sent 12
- Packets Received 15
- Originated Locally? null
- Tunnel Parent Connection ID (empty)
- Historv ShADadIR



Finally, in packettotal, suspicious activity occurred at 13:12:47. Based on the report we found only one suspicious activity in this packet captured.

After downloading the file on this part, we upload this file to virustotal.com. And we found that 35 engines were detected. The screenshots are shown as follows:

Malicious Activity   Suspicious Activity   Connections   DNS   HTTP   SSL Certificates   PKI (X.509)   Transferred Files   Strange Activity   Community Tags

Similar Packet Captures

Search in results

Timestamp	Connection ID	Alert Type	Alert Message	Alert Sub-message	Sender IP	Sender Port	Target IP
2015-08-30 13:12:47 Z	CtGI8l22yrRPVILob	TeamCymruMalwareHashRegistry:Match	Malware Hash Registry Detection rate: 39% Last seen: 2016-11-01 00:48:32	https://www.virustotal.com/en/search/?query=bc...b0765409e5ae0c53c46ce5be	192.168.122.62	49175	46.38.45.65

Target Port 80  
Sender IP (Derived) 192.168.122.62  
Sender Port (Derived) 80  
Target IP (Derived) 46.38.45.65  
Count/Status Code null  
Associated File ID FSQ00L2K0IBEPCKA...  
Associated File Mime-Type application/x-shockwave-flash  
Associated File Description ...GzO0ZUEgbogAQiryJQ-DbgN6V0ggEkqfPZVlqz7IQnmtayh42P28STNzkKM  
Transport Protocol Tcp

SUMMARY

DETECTION

DETAILS

COMMUNITY 4

x 35 engines detected this file

Community  
Score

cf76f50d725d971469cc54c953be243722bfc4a853c12e4f95571e8a413eb489

index.php.BADF050.x-shockwave-flash



SUMMARY

DETECTION

DETAILS

COMMUNITY

4

Ad-Aware	(?) Script.SWF.Exploit.CVE-2015-3105.C500
AegisLab	(!) Hacktool.SWF.Agent.3!c
AhnLab-V3	(!) SWF/Exploit
ALYac	(!) Script.SWF.Exploit.CVE-2015-3105.C500
Antiy-AVL	(!) Trojan[Exploit]/SWF.SWF.Generic
Arcabit	(!) Script.SWF.Exploit.CVE-2015-3105.C500
Avast	(?) SWF:Malware-gen [Tr]
AVG	(!) SWF:Malware-gen [Tr]
Avira (no cloud)	(!) EXP/Agent.EB.48
BitDefender	(!) Script.SWF.Exploit.CVE-2015-3105.C500
CAT-QuickHeal	(?) SWF.Kit.Nuclear.N
ClamAV	(!) Swf.Exploit.Kit-99
Comodo	(!) Malware@#2iqyxbwC2cazk



 VIRUSTOTAL

SUMMARY

DETECTION

DETAILS

COMMUNITY

4

Cyren	(!) SWF/SWF/Exploit
DrWeb	(!) Exploit.SWF.1232
Emsisoft	(!) Script.SWF.Exploit.CVE-2015-3105.C500 (B)
eScan	(!) Script.SWF.Exploit.CVE-2015-3105.C500
ESET-NOD32	(!) SWF/Exploit.ExKit.AS
F-Prot	(!) SWF/SWF/Exploit
F-Secure	(!) Exploit.EXP/Agent.EB.48
FireEye	(!) Script.SWF.Exploit.CVE-2015-3105.C500
GData	(!) Script.SWF.Exploit.CVE-2015-3105.C500
Ikarus	(!) Trojan.SWF.Exploit
Kaspersky	(!) Exploit.SWF.Agent.ro
MAX	(!) Malware (ai Score=100)
McAfee	(!) SWF/Exploit-Rig.a





SUMMARY

DETECTION

DETAILS

COMMUNITY

4

McAfee-GW-Edition

! BehavesLike.Flash.Exploit.mg

NANO-Antivirus

! Trojan.Swf.Mlw.ebrtvr

Qihoo-360

! Generic/Trojan.Exploit.7f1

Sophos AV

! Troj/SWFExp-HN

Symantec

! Trojan.Gen.2

Tencent

! Win32.Exploit.Agent.Pbpg

TrendMicro

! EXPL\_CVE20153090

Zillya

! Exploit.Agent.Script.854

ZoneAlarm by Check Point

! Exploit.SWF.Agent.ro

Avast-Mobile

✓ Undetected

Baidu

✓ Undetected

BitDefenderTheta

✓ Undetected

Bkav

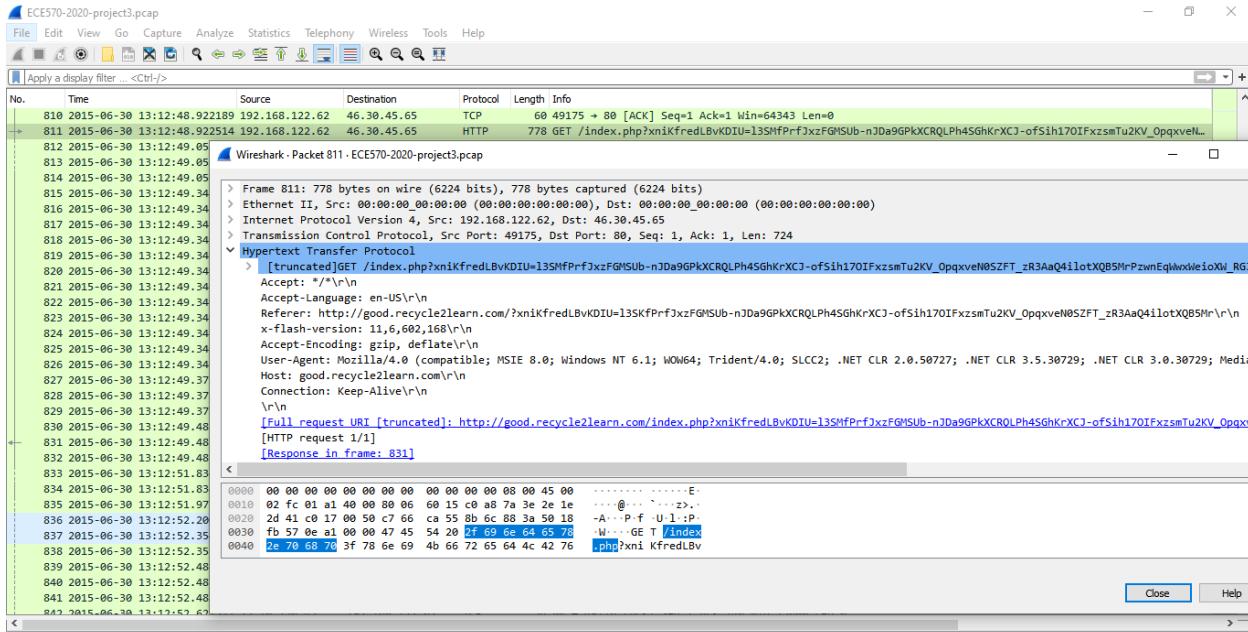
✓ Undetected

Note: all files transferred, packets are referred to [www.floridablueline.com](http://www.floridablueline.com)

And also in this site, when the host infected [www.good.recycled2learn.com](http://www.good.recycled2learn.com) then this site sent packet ACK to host 192.168.122.62.

According to wireshark capture file, when the host sent packet contains swf malware in frame 811, the website: [www.good.recycle2learn.com](http://www.good.recycle2learn.com) responded 192.168.122.62 on packet 831. The weird difference is time. At 13:12:48 192.168.122.62 sent a request GET http to 46.30.45.65 after a seconds, in 13:12:49 the 46.30.45.65 sent HTTP1.1 to the host.





Virustotal check of this URL that show in above picture indicates this URL is malware, shows as a follows:

Σ http://good.recycle2learn.com/index.php?xnikfredLBvKDIU=13SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV\_OpqxveN0SZFT

4 engines detected this URL

http://good.recycle2learn.com/index.php?xnikfredLBvKDIU=13SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV\_OpqxveN0SZFT\_zR3AaQ4il0tXQB5MrPzwnEqWwxWeiXW\_RGJN1hM-5DAFrE92lyx-cIUsN2wR7QumAGzO0ZUEgbogAQryJ Q-DbpgN6V0ggEkqfPZVlxq7lQnmtayah42P28STNzkKM 2016-08-02 17:51:04 UTC 4 years ago

Community Score

Detection	Details	Relations	Community
Fortinet	Malware	Kaspersky	Malware
Sophos AV	Malicious	Websense ThreatSeeker	Malicious
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Anti-AVL	Clean
Avira (no cloud)	Clean	Baidu-International	Clean

In time 13:12:49 In Files Transferred of packettotal, the file shockwave-flash is shown as a following picture:

Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth
+ 2015-06-30 13:12:45 Z	CMvAQV2OwfXQnWdhX2	<a href="#">F1PQYF22310GR07...</a>	1675befb11864f12ed74bd8dfae7e21c	f162bf3b954f649d8e8f8359077bd24bd29a8580	200.113.214.198	192.168.122.62	HTTP	0
+ 2015-06-30 13:12:47 Z	CMHzK1MVihv1X1U2j	<a href="#">FA3AYX1USTBLT5...</a>	b699faef73d2f168cb5b3afdf51ab51e418	713824abef3fa5a54457a4424cd6db08545d5d4b9a	200.113.214.198	192.168.122.62	HTTP	0
+ 2015-06-30 13:12:48 Z	CocBdE3VP4U7EE8PX5	<a href="#">FEEAQ9NAFX0NSCT...</a>	4634a99740f14922d030ed21dd097a18	b67777893cd8a315f781545e42e350be9f403c1e	46.38.45.65	192.168.122.62	HTTP	0
- 2015-06-30 13:12:49 Z	ClG18I22yRPVILob	<a href="#">FSQDRJ2CN1REPCK...</a>	4a08ca45360dd2ff528246915fd58da2	bc1b563479d2c1932ba765409e5ae8c53c4dcce5b8	46.38.45.65	192.168.122.62	HTTP	0

Mime Type application/x-shockwave-flash  
File Name null  
Total Bytes 15763

We know in frame 831 based on wireshark, between the website www.good.recycle2learn.com and 192.168.122.62 the HTTP connection established. And HTTP 1.1 200 OK.

After, click on virustotal.com lookup, the virustotal check shown as follows and 35 engines detected this file.

Σ cf76f50d725d971469cc54c953be243722bfc4a853c12e4f95571e8a413eb489| Search Upload Sign

 35 / 58
① 35 engines detected this file

cf76f50d725d971469cc54c953be243722bfc4a853c12e4f95571e8a413eb489  
 index.php.BADF5050.x-shockwave-flash

15.39 KB | 2020-06-08 10:48:24 UTC | 1 month ago | 

capabilities | cve-2015-3090 | cve-2015-3105 | exploit | flash | zlib

DETECTION	DETAILS	COMMUNITY	④
Ad-Aware	① Script.SWF.Exploit.CVE-2015-3105.C500	AegisLab	① Hacktool.SWF.Agent.3lc
AhnLab-V3	① SWF/Exploit	ALYac	① Script.SWF.Exploit.CVE-2015-3105.C500
Antiy-AVL	① Trojan[Exploit]/SWF.SWF.Generic	Arcabit	① Script.SWF.Exploit.CVE-2015-3105.C500
Avast	① SWF.Malware-gen [Trj]	AVG	① SWF.Malware-gen [Trj]
Avira (no cloud)	① EXP/Agent EB.48	BitDefender	① Script.SWF.Exploit.CVE-2015-3105.C500
CAT-QuickHeal	① SWF.Kit.Nuclear.N	ClamAV	① Swf Exploit.Kit-99
Comodo	① Malware@#2iqyxwbc2cazk	Cyren	① SWF/SWF/Exploit
DrWeb	① Exploit.SWF.1232	Emsisoft	① Script.SWF.Exploit.CVE-2015-3105.C50...
eScan	① Script.SWF.Exploit.CVE-2015-3105.C500	ESET-NOD32	① SWF/Exploit.ExKit.AS
F-Prot	① SWF/SWF/Exploit	F-Secure	① Exploit.EXP/Agent.EB.48
FireEye	① Script.SWF.Exploit.CVE-2015-3105.C500	GData	① Script.SWF.Exploit.CVE-2015-3105.C500
Ikarus	① Trojan.SWF.Exploit	Kaspersky	① Exploit.SWF.Agent.ro
MAX	① Malware (ai Score=100)	McAfee	① SWF/Exploit-Rig.a
McAfee-GW-Edition	① BehavesLike Flash.Exploit.mg	NANO-Antivirus	① Trojan.Swf.Mlw.ebrtv
Qihoo-360	① Generic/Trojan.Exploit.7f1	Sophos AV	① Troj/SWFEsp-HN
Symantec	① Trojan.Gen.2	Tencent	① Win32.Exploit.Agent.Pbpq
TrendMicro	① EXPL_CVE20153090	Zillya	① Exploit.Agent.Script.854
ZoneAlarm by Check Point	① Exploit.SWF.Agent.ro	Avast-Mobile	② Undetected
Baidu	② Undetected	BitDefenderTheta	② Undetected
Bkav	② Undetected	Fortinet	② Undetected
Jiangmin	② Undetected	K7AntiVirus	② Undetected

Compared with frame 811, at first the host sent HTTP requests to www.good.recycle2learn.com as a HTTP GET this file infected by 35 engines. And now





in frame 831 www.good.recycle2learn.com sent a file to the host. And this file is the same as before. Infected by 35 engines. We checked both files in Files Transferred of packet total.

After being infected www.good.recycle2learn.com by the host, two of them sent a lot of ACK together.

In time 13.12.51 based on packettotal report, HTTP Tab, we found an HTTP transaction between source IP which is host and target IP which is 46.30.45.65. The picture is as follows:

Malicious Activity Suspicious Activity Connections DNS **HTTP** SSL Certificates PKI (X.509) Transferred Files Strange Activity Community Tags

Similar Packet Captures

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host
2015-06-30 13:12:51 Z	CocBdE3VP4U7EE8PX5	192.168.1.22.62	49174	46.30.45.65	80	2	GET	good.recycle2learn.com

URI ...umAgzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlq;7lQnmtayh42P26QJA4 ↴  
Referrer null  
User Agent ....NET CLR 3.5.30729, .NET CLR 3.0.30729, Media Center PC 6.0) ↴  
Request Body Length 0  
Response Body Length 352256  
Status Code 200  
Status Message OK  
Info Code null  
Info Message null  
File null  
Username null  
Password null  
Proxied null  
Sender File IDs null  
Sender Mime Types null  
Recipient File IDs FHPMC7ASNOU... ↴  
Recipient Mime Types null  
Client Headers ACCEPT,ACCEPT-ENCODING,USER-AGENT,HOST,CONNECTION  
Server Headers null  
Cookie Variables null  
URI Variables /index.php?nikiforoff.ru&ID=1

Base on virustotal report, this file contains four detected engines, the screen shot as a follows:





SUMMARY

DETECTION

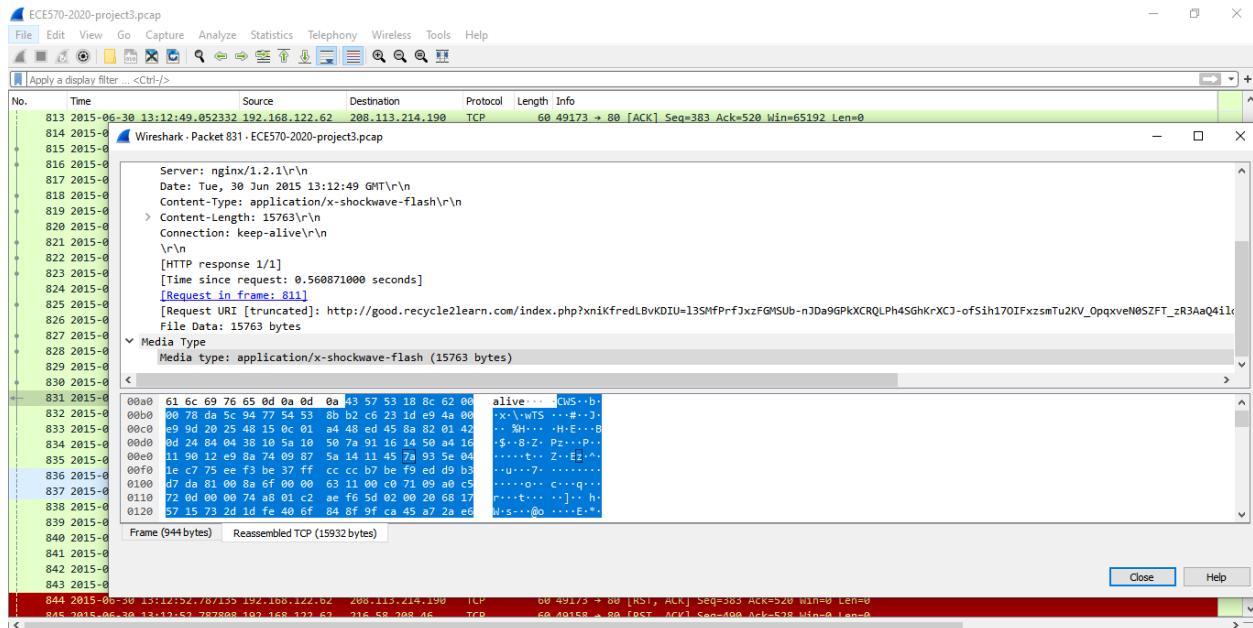
DETAILS

COMMUNITY

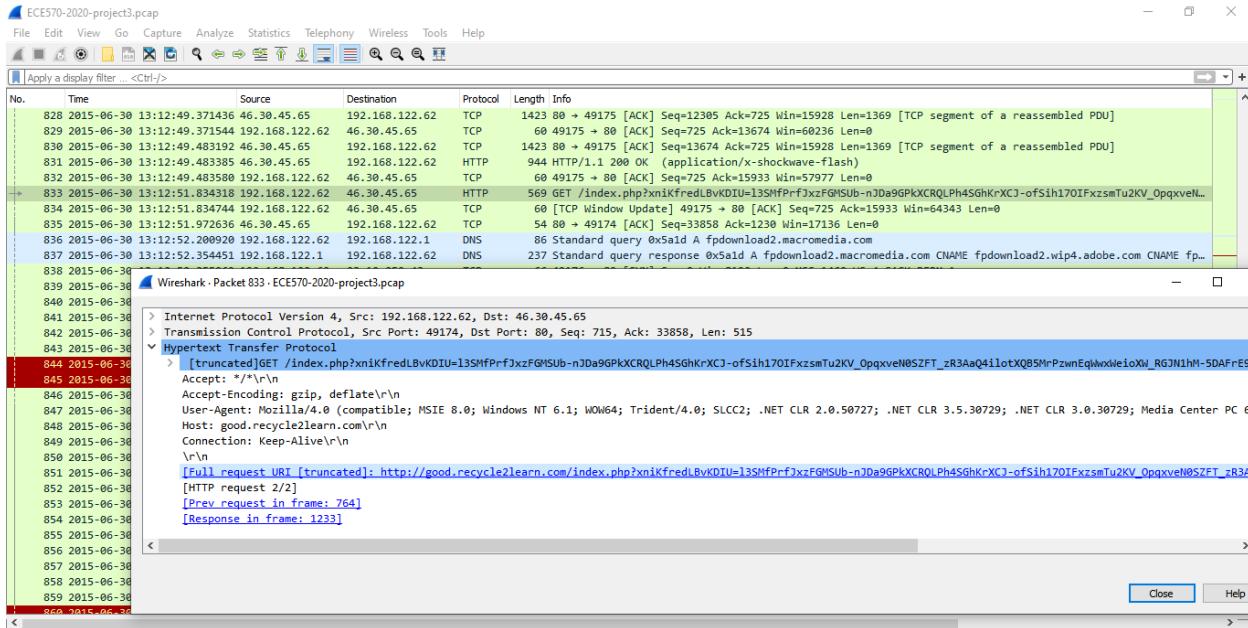
McAfee	<span>⚠️</span>	Artemis!9276A5680AC3
McAfee-GW-Edition	<span>⚠️</span>	Artemis!9276A5680AC3
Microsoft	<span>⚠️</span>	PUA:Win32/Presenoker
Sophos AV	<span>⚠️</span>	Troj/Miuref-AI
Ad-Aware	<span>✓</span>	Undetected
AegisLab	<span>✓</span>	Undetected
AhnLab-V3	<span>✓</span>	Undetected
ALYac	<span>✓</span>	Undetected
Antiy-AVL	<span>✓</span>	Undetected
Arcabit	<span>✓</span>	Undetected
Avast	<span>✓</span>	Undetected
Avast-Mobile	<span>✓</span>	Undetected
...		

Based on the wireshark report, frame 831 indicates that include media type.  
Application/X-shockwave flash.





Based on wireshark in frame 833 the GET HTTP request between 192.168.122.62 and 46.30.45.65 start.



The URL of above screenshot related to scripts that GET on virustotal check indicates this script is malware. The screen shot as a follows:

① 2 engines detected this URL

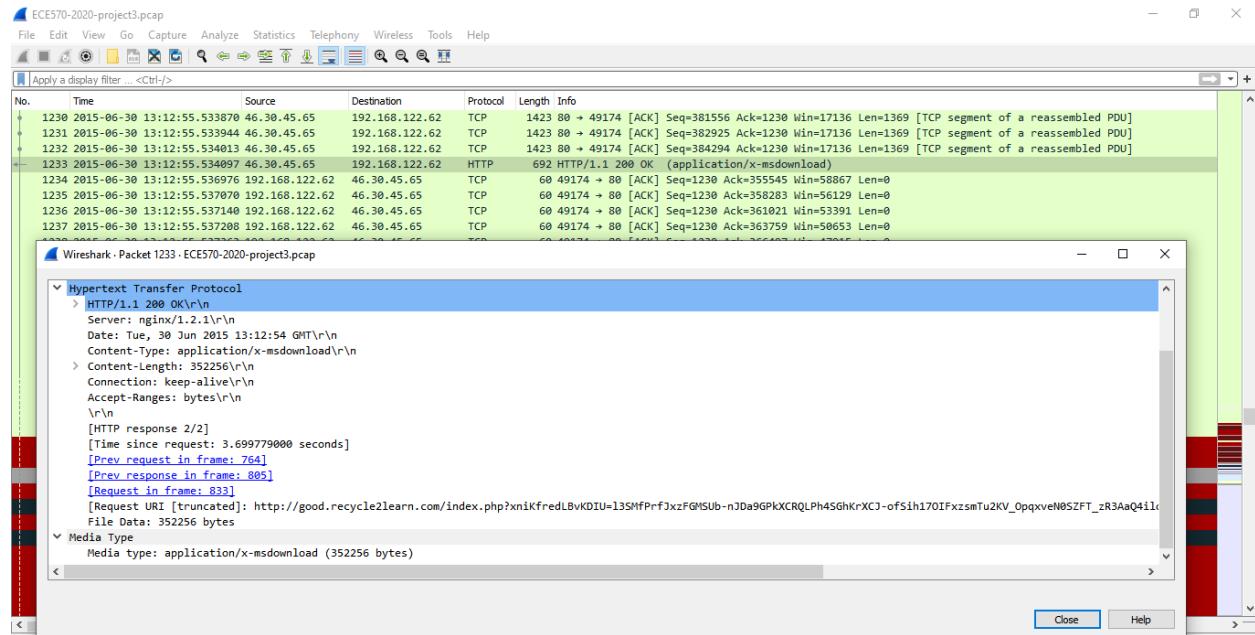
http://good.recycle2learn.com/index.php?xnikfredLBvKDIU=13SMPrfJxzFGMSub-nJDa9GPKXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV\_OpqxveN0SZFT\_zR3AaQ41lotXQ85MrPzwnEqjwxWeioXW\_RGJN1hM-5DAFrE9 2018-04-29 23:09:37 UTC 2 years ago

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware		Forcepoint ThreatSeeker ① Malicious
ADMINUSLabs	✓ Clean		AegisLab WebGuard ✓ Clean
AlienVault	✓ Clean		Antiy-AVL ✓ Clean
Baidu-International	✓ Clean		BitDefender ✓ Clean
Blueliv	✓ Clean		C-SIRT ✓ Clean

And also, we recognized that this frame was requested in frame 764. Moreover, the response of this request (frame 833) will be in frame 1233.

So, we will check frame 1233.

In frame 1233, application/x-msdownload is HTTP 200 OK. This frame response of frame 833 request.



In addition, this frame time at 13:12:55.

In frame 836, one request from the host windows machine to DNS sent for fpdownload.macromedia.com and response on frame 837.



ECE570-2020-project3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
831	2015-06-30 13:12:49.483385	46.30.45.65	192.168.122.62	HTTP	944	HTTP/1.1 200 OK (application/x-shockwave-flash)
832	2015-06-30 13:12:49.483588	192.168.122.62	46.30.45.65	TCP	60	49175 → 80 [ACK] Seq=725 Ack=15933 Win=57977 Len=0
833	2015-06-30 13:12:51.834318	192.168.122.62	46.30.45.65	HTTP	569	GET /index.php?xnlKFredLbVxDIU=135MPPrFixfGWSUb-nDae9GPkXCRQlPh4SGhKrXCJ-ofSih170IFxzsmTu2KV_0pqxveN...
834	2015-06-30 13:12:51.834744	192.168.122.62	46.30.45.65	TCP	60	[TCP Window Update] 49175 → 80 [ACK] Seq=725 Ack=15933 Win=64343 Len=0
835	2015-06-30 13:12:51.972636	46.30.45.65	192.168.122.62	TCP	54	80 → 49174 [ACK] Seq=33858 Ack=1230 Win=17136 Len=0
836	2015-06-30 13:12:52.200920	192.168.122.62	192.168.122.1	DNS	86	Standard query response 0x5a1d A fpdownload2.macromedia.com CNAME fpdownload2.wip4.adobe.com CNAME fp...
837	2015-06-30 13:12:52.354451	192.168.122.1	192.168.122.62	DNS	237	Standard query response 0x5a1d A fpdownload2.macromedia.com CNAME fpdownload2.wip4.adobe.com CNAME fp...
838	2015-06-30 13:12:52.355069	192.168.122.62	23.10.250.43	TCP	66	49176 → 80 [SYN] Seq=0 Win=8192 Len=1460 WS=4 SACK_PERM=1

Wireshark - Packet 836 - ECE570-2020-project3.pcap

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
> fpdownload2.macromedia.com: type A, class IN  
[Response In: 837]

Hex Dump:

```
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00
0010  00 48 01 ab 00 00 00 11 c3 69 c9 a8 7a 3e c0 a6 00
0020  7a 01 d3 70 00 35 00 34 4c 6b 5a 1d 01 00 00 01 00
0030  00 00 00 00 00 00 66 70 64 6f 77 6e 6c 67 61 00
0040  64 32 0a 6d 61 63 72 6f 6d 65 64 69 61 03 63 6f 00
0050  6d 00 00 01 00 01 m....
```

Close Help

After TCP handshaking in frame 841 GET flash player from IP 23.10.250.43

But in frame 843 HTTP response 404 Not found

839	2015-06-30 13:12:52.400027	23.10.250.43	192.168.122.62	TCP	60	49176 → 23.10.250.43 [ACK] Seq=726 Ack=15933 Win=64343000 Len=0 SACK_PERM=1 WS=4
840	2015-06-30 13:12:52.487476	192.168.122.62	23.10.250.43	TCP	60	49176 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0
841	2015-06-30 13:12:52.488103	192.168.122.62	23.10.250.43	HTTP	293	GET /get/flashplayer/update/current/install/version.xml11.6.602.168~installVector=1&lang=en&cpuWordLe...
842	2015-06-30 13:12:52.621327	23.10.250.43	192.168.122.62	TCP	54	80 → 49176 [ACK] Seq=1 Ack=240 Win=15680 Len=0
843	2015-06-30 13:12:52.786403	23.10.250.43	192.168.122.62	HTTP	574	HTTP/1.1 404 Not Found (text/html)

We check DNS in the packet total at the same time of this transfer.



Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Transaction ID	Query								
2015-06-30 13:12:52 Z	CKdhc21h1h9kqH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	23069	fpdownload2.macromedia.com								
Query Class Desc C_INTERNET																
Query Type 1																
Query Type Desc A																
Response Code 0																
Response Code Desc NOERROR																
Authoritative Answer? F																
Truncated? F																
Recursion Desired? T																
Recursion Available? T																
Answers	fpdownload2.wip4.adobe.com,fpdownload.macromedia.com.edgesuite.net,a1293.d.akamai.net,23.10.250.43,23.10.250.18															
TTLs	21078.000000,119.000000,21232.000000,19.000000,19.000000															
Authoritative Response null																
Additional Response(s) null																

HTTP in packet total checked. We found that at this time 13:12:51 and 13:12:52 we have tow information.

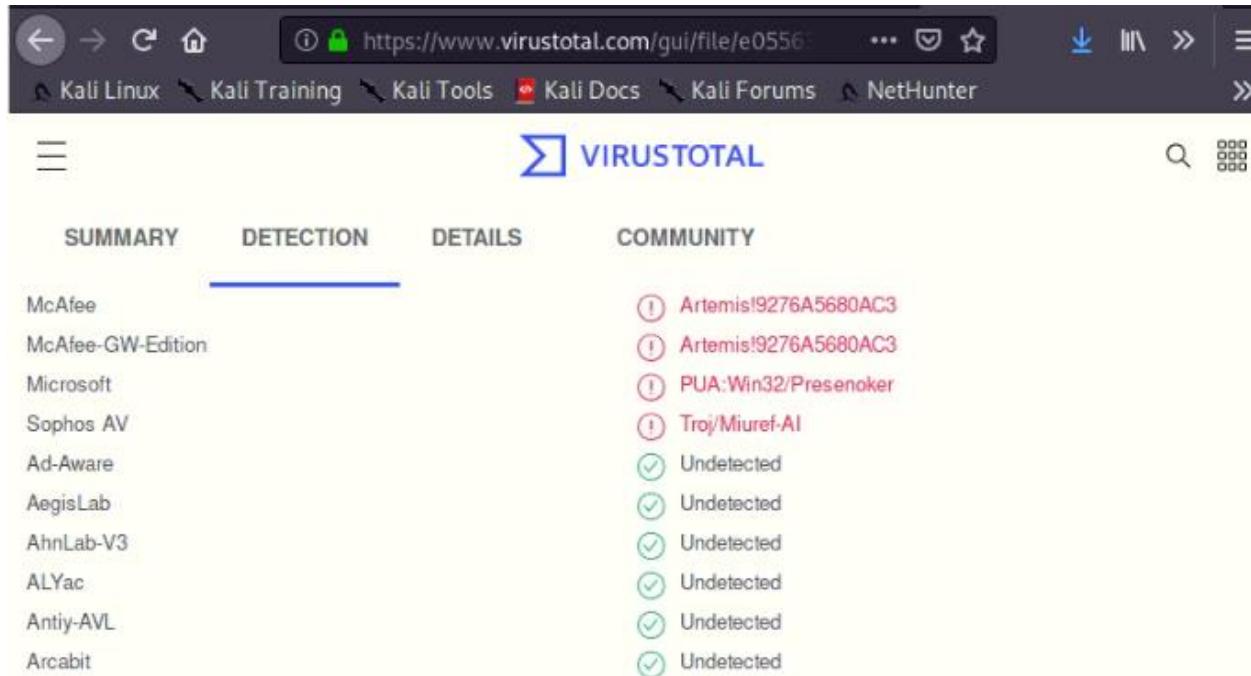
Malicious Activity	Suspicious Activity	Connections	DNS	HTTP	SSL Certificates	PKI (X.509)	Transferred Files	Strange Activity	Community Tags																																				
Similar Packet Captures																																													
<input type="text"/> Search in results																																													
  																																													
<table border="1"><thead><tr><th>Timestamp</th><th>Connection ID</th><th>Sender IP</th><th>Sender Port</th><th>Target IP</th><th>Target Port</th><th>Transaction Depth</th><th>Method</th><th>Host</th></tr></thead><tbody><tr><td>2015-06-30 13:12:51 Z</td><td>CocBdE3VP4U7EE8PX5</td><td>192.168.122.62</td><td>49174</td><td>46.30.45.65</td><td>80</td><td>2</td><td>GET</td><td>good.recycle2learn.com</td></tr><tr><td>2015-06-30 13:12:52 Z</td><td>CIOXLi293JVZ3O168h</td><td>192.168.122.62</td><td>49176</td><td>23.48.258.43</td><td>80</td><td>1</td><td>GET</td><td>fpdownload2.macromedia.com</td></tr><tr><td>2015-06-30 13:12:55 Z</td><td>CALygR1JnJXOgNnETj</td><td>192.168.122.62</td><td>49171</td><td>192.254.234.118</td><td>80</td><td>3</td><td>GET</td><td>www.floridablueine.com</td></tr></tbody></table>										Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host	2015-06-30 13:12:51 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	2	GET	good.recycle2learn.com	2015-06-30 13:12:52 Z	CIOXLi293JVZ3O168h	192.168.122.62	49176	23.48.258.43	80	1	GET	fpdownload2.macromedia.com	2015-06-30 13:12:55 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	3	GET	www.floridablueine.com
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transaction Depth	Method	Host																																					
2015-06-30 13:12:51 Z	CocBdE3VP4U7EE8PX5	192.168.122.62	49174	46.30.45.65	80	2	GET	good.recycle2learn.com																																					
2015-06-30 13:12:52 Z	CIOXLi293JVZ3O168h	192.168.122.62	49176	23.48.258.43	80	1	GET	fpdownload2.macromedia.com																																					
2015-06-30 13:12:55 Z	CALygR1JnJXOgNnETj	192.168.122.62	49171	192.254.234.118	80	3	GET	www.floridablueine.com																																					

The first one occurs at 13:12:51 and contains one file. In this file 192.168.122.62 as a sender and 46.30.45.65 is as a target on host that is good.recycle2learn.com



URI	...umAGzOZUEgbogAQIryJQ-DbpgN6V0ggDE3KPZViqx7IQnmtayh42P26QJA4
Referrer	null
User Agent	... .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) v
Request Body Length	0
Response Body Length	352256
Status Code	200
Status Message	OK
Info Code	null
Info Message	null
File	null
Username	null
Password	null
Proxied	null
Sender File IDs	null
Sender Mime Types	null
Recipient File IDs	<a href="#">788PNCM7ASNOLUN...</a>
Recipient Mime Types	null
Client Headers	ACCEPT,ACCEPT-ENCODING,USER-AGENT,HOST,CONNECTION
Server Headers	null
Cookie Variables	null

When we downloaded this file and checked it on vius total we found that this file is malware.



VIRUSTOTAL

SUMMARY	DETECTION	DETAILS	COMMUNITY
McAfee	Artemis!	9276A5680AC3	
McAfee-GW-Edition	Artemis!	9276A5680AC3	
Microsoft	PUA:Win32/Presenoker		
Sophos AV	Troj/Miuref-A!		
Ad-Aware	Undetected		
AegisLab	Undetected		
AhnLab-V3	Undetected		
ALYac	Undetected		
AntiAVL	Undetected		
Arcabit	Undetected		



The first one occurs at 13:12:52 and contains one file and contains one file. In this file 192.168.122.62 as a sender and 46.30.45.65 is as a target on host that is fpdownload2.macromedia.com

⌚	2015-06-30 13:12:52 Z	CtOXLi293JVZ3Ot68h	192.168.122.62	49176	23.10.258.43	80	1	GET	fpdownload2.macromedia.com
URI	...p;cpuWordLength=64&playerType=ax&os=win&osVer=13 ↴								
Referrer	null								
User Agent	Shockwave Flash								
Request Body Length	0								
Response Body Length	351								
Status Code	404								
Status Message	Not Found								
Info Code	null								
Info Message	null								
File	null								
Username	null								
Password	null								
Proxied	null								
Sender File IDs	null								
Sender Mime Types	null								
Recipient File IDs	<a href="#">DRAFT CANNONICALLY</a>								
Recipient Mime Types	text/html								
Client Headers	USER-AGENT,HOST,CACHE-CONTROL								

When we downloaded this file and checked it on vius total we found that this file is clean.



Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

## VIRUSTOTAL

SUMMARY DETECTION DETAILS COMMUNITY

Ad-Aware	Undetected
AegisLab	Undetected
AhnLab-V3	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected
Avast-Mobile	Undetected
AVG	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
BitDefenderTheta	Undetected

And also, in Transferred Files we have one transfer packets at the time 13:12:45

Malicious Activity Suspicious Activity Connections DNS HTTP SSL Certificates PKI (X.509) **Transferred Files** Strange Activity Community Tags

Similar Packet Captures

Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/s	Sent To Host/s	Source	Depth
+ 2016-09-30 13:12:52 Z	CtOXLi293JVZ3O168h	<a href="#">FDF1C139C9BQV...</a>	5af46fe993cadc3bde5528d5036b105b	8ae090d66ebedc31e9a0255fedba3ac8e13db0952a	<a href="#">23.10.256.43</a>	<a href="#">192.168.122.62</a>	HTTP	0
- 2016-09-30 13:12:54 Z	CocBdE3VP4U7EE8PX5	<a href="#">FIRPMQn7ASNQUL...</a>	e0756a379d0fc5cc8f5ca38d7d996fc9d	x1a9b3f5bc705d1f844f7xaed6581bbfd50927hc	<a href="#">46.30.45.65</a>	<a href="#">192.168.122.62</a>	HTTP	0

Mime Type null

Lookup this file in virustotal indicates that 4 engines detected this file.

e0556309465133abf377027ffef6cb09371fb34657fc1051a770d22930f7aae|

**4 engines detected this file**

e0556309465133abf377027ffef6cb09371fb34657fc1051a770d22930f7aae  
index.php.B91C7116.x-msdownload

344.00 KB | 2020-06-02 10:29:16 UTC  
Size | 2 months ago

DETECTION	DETAILS	COMMUNITY
McAfee	ArtemisI9276A5680AC3	McAfee-GW-Edition
Microsoft	PUA-Win32/Presenoker	Sophos AV
Ad-Aware	Undetected	AegisLab
AhnLab-V3	Undetected	ALYac
Anti-AVL	Undetected	Arcabit
Avast	Undetected	Avast-Mobile

Based on Malicious activity report on packet total, two report occurs at 13:12:54

+ 2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015	1	192.168.122.62	49174	46.38.45.65	80	TCP	good.recycle2learn.com
+ 2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary	1	46.38.45.65	80	192.168.122.62	49174	TCP	good.recycle2learn.com

The first alert is ET CURRENT\_EVENTS RIG Payload URI Struct March 20 2015. This alert is related to good.recycle2learn.com and occurs at 13:12:54. **HTTP Content-Type** application/x-msdownload. And also between host and good.recycle2learn.com.

+ 2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015	1	192.168.122.62	49174	46.38.45.65	80	TCP	good.recycle2learn.com
HTTP URI ...umAgzO0ZUEgbogAQlyJQ-DbgN6V0ggDE3KPZVlx7lQnmtayh42P26QJA4 ▾									
HTTP Content-Type application/x-msdownload									
HTTP Method GET									
HTTP User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) ▾									
HTTP Referrer None									
HTTP Protocol HTTP/1.1									
HTTP Length 2551									
HTTP Status Code 200									



For the past year, Rig EK has been using Flash exploits based on CVE-2018-8174 as noted in this May 2018 blog post from @kafeine. Since then, other sources have reported Rig EK delivering a variety of malware like the Grobios Trojan or malware based on a Monero cryptocurrency miner. Like other EKs, Rig EK is most often used in malvertising distribution campaigns. In today's infection, Rig EK delivered AZORult, and the infection followed-up with other malware I was unable to identify.



The last alert is ET CURRENT\_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary. This alert is related to good.recycle2learn.com and occurs at 13:12:54. **HTTP Content-Type** application/x-msdownload. And also between good.recycle2learn.com and host.

2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary (1)	46.30.45.65	80	192.168.122.62	49174	TCP	good.recycle2learn.com
HTTP URI ...umAgzO0ZUEgbogAQIryJQ-DbpgN6V0ggDE3KPZViqx7Qnmtayh42P26QJA4								
HTTP Content-Type application/x-msdownload								
HTTP Method GET								
HTTP User Agent ...NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0) v								
HTTP Referrer None								
HTTP Protocol HTTP/1.1								
HTTP Length 43593								
HTTP Status Code 200								

CryptoWall is a family of file-encrypting Ransomware that first appeared in early 2014. It is notable for its use of unbreakable AES encryption, unique CHM infection mechanism, and robust C2 activity over the Tor anonymous network. The miscreants running the CryptoWall operation also provide a free single-use decryption service to prove they hold the keys necessary to restore the hijacked files.



So, the website www.good.recycle2learn.com with IP address 46.30.45.65 is the site that delivered the Malware and ransomware that explain completely on question 4.



4. Identify the type of malware involved and check the payload by running the associated file (or files) against an online virus checker (i.e. VirusTotal).

According to the packet total report on Malicious activity. Two activities occur at time 13:12:54 which have an alert for network trojan . All two alerts explain separately. The screen shots are in following pictures:



The first alert is ET CURRENT\_EVENTS RIG Payload URI Struct March 20 2015.

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-03-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015	1	192.168.122.62	49174	46.38.45.65	80	TCP	good.recycle2learn.com
HTTP URI ...umAGzO0ZUEgbogAQiryJQ-DbpgN6V0ggDE3KPZVlx7Qnmtayh42P26QJA4									
HTTP Content-Type application/x-msdownload									
HTTP Method GET									
HTTP User Agent ....NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)									
HTTP Referrer None									
HTTP Protocol HTTP/1.1									
HTTP Length 2551									
HTTP Status Code 200									

For the past year, Rig EK has been using Flash exploits based on CVE-2018-8174 as noted in this May 2018 blog post from @kafeine. Since then, other sources have reported Rig EK delivering a variety of malware like the Grobios Trojan or malware based on a Monero cryptocurrency miner. Like other EKs, Rig EK is most often used in malvertising distribution campaigns. In today's infection, Rig EK delivered AZORult, and the infection followed-up with other malware I was unable to identify.

The second alert is ET CURRENT\_EVENTS Cryptowall docs campaign Sept 2015 . encrypted binary (1).



Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname
2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary (1)	1		80		49174	TCP	good.recycle2learn.com
HTTP URI ...umAGzO0ZUEgbogAQiryJQ-DbpgN6V0ggDE3KPZVlx7lQnmtayh42P26QjA4									
HTTP Content-Type application/x-msdownload									
HTTP Method GET									
HTTP User Agent .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0									
HTTP Referrer None									
HTTP Protocol HTTP/1.1									
HTTP Length 43593									
HTTP Status Code 200									

CryptoWall is a family of file-encrypting Ransomware that first appeared in early 2014. It is notable for its use of unbreakable AES encryption, unique CHM infection mechanism, and robust C2 activity over the Tor anonymous network. The miscreants running the CryptoWall operation also provide a free single-use decryption service to prove they hold the keys necessary to restore the hijacked files.

In Connections Tab of packet total we found information based on time after 13:12:54.

Malicious Activity	Suspicious Activity	Connections	DNS	HTTP	SSL Certificates	PKI (X.509)	Transferred Files	Strange Activity	Community Tags	
Similar Packet Captures										
<input type="text"/> Search in results										
										
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent
2015-06-30 13:12:46 Z	CMvAQV20wXQmWdhX2		49172		80	tcp	http		378	630
2015-06-30 13:12:45 Z	CR9n6sdRd00MDUCG8		54137		53	udp	dns		37	65
2015-06-30 13:12:46 Z	CMHzK1MVlnV1X1U2		49173		80	tcp	http		382	634
2015-06-30 13:12:47 Z	Cf09Qe4APdPX0dSMLI		59978		53	udp	dns		40	68
2015-06-30 13:12:47 Z	CecBdE3VP4U7EE8PX5		49174		80	tcp	http		1229	7801
2015-06-30 13:12:48 Z	CIG@Q2yrRPVILob		49175		80	tcp	http		724	1216
2015-06-30 13:12:52 Z	CKdhc21h1h9kqH5m2g		54128		53	udp	dns		44	72
2015-06-30 13:12:52 Z	CHOXLi293JvZ3Cn68h		49176		80	tcp	http		239	451
2015-06-30 13:13:14 Z	CqnBgD4OYTuQ3Bn3Wa		49177		443	tcp	null		0	52

Both parts are explained step by step.





2015-06-30 13:12:52 z	CKdh21h1h9kqH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	dns	0.15	44	72
-----------------------	-------------------	----------------	-------	---------------	----	-----	-----	------	----	----

Payload Bytes Received 195

Total Bytes Received 223

Missed Bytes 0

### Packets Sent 1

## Packets Received 1

Originated Locally? null

## Tunnel Parent Co

Page | 1520

Page 10 of 10

100

Rechtsanwalt Sven F.

1 / 2

Page 15 of 15

Based on the NetworkMiner report, from 13:12:51 to 13:12:55 we have two frames that transfer a file in network.

NetworkMiner 2.5																						
File	Tools	Help	Select a network adapter in the list --																			
Hosts (14)			File (39)			Images (2)			Messages		Credentials (2)		Sessions (20)		DNS (18)		Parameters (754)		Keywords		Anomalies	
Filter keyword:												<input type="checkbox"/>	Case sensitive	<input checked="" type="checkbox"/>	ExactPhrase	<input type="checkbox"/>	Any column	<input type="checkbox"/>	Clear	<input type="checkbox"/>	App	
Frame	Filename	E...	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed	Details											
96	www.google.co.uk[2].cer	cer	1 150 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=...									
96	Google Internet Authority G2[2].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog...									
96	GeoTrust Global CA[2].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49161	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
105	google.com.cer	cer	1 737 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN= google.com, O=Google Inc, L=Mour...									
105	Google Internet Authority G2[3].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN= Google Internet Authority G2, O=Goog...									
105	GeoTrust Global CA[3].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49164	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
109	www.google.co.uk[3].cer	cer	1 150 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=www.google.co.uk, O=Google Inc, L=...									
109	Google Internet Authority G2[4].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=Google Internet Authority G2, O=Goog...									
109	GeoTrust Global CA[4].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49163	TlsCertificate	2015-06-30 13:11:53 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
317	google.com[1].cer	cer	1 737 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN= google.com, O=Google Inc, L=Mour...									
317	Google Internet Authority G2[5].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN= Google Internet Authority G2, O=Goog...									
317	GeoTrust Global CA[5].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49165	TlsCertificate	2015-06-30 13:11:54 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
354	google.com[2].cer	cer	1 737 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN= google.com, O=Google Inc, L=Mour...									
354	Google Internet Authority G2[6].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN= Google Internet Authority G2, O=Goog...									
354	GeoTrust Global CA[6].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49167	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
365	google.com[3].cer	cer	1 737 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN= google.com, O=Google Inc, L=Mour...									
365	Google Internet Authority G2[7].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN= Google Internet Authority G2, O=Goog...									
365	GeoTrust Global CA[7].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49168	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
377	google.com[4].cer	cer	1 737 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN= google.com, O=Google Inc, L=Mour...									
377	Google Internet Authority G2[8].cer	cer	1 012 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN= Google Internet Authority G2, O=Goog...									
377	GeoTrust Global CA[8].cer	cer	897 B	216.58.210.67	[www.google.co.uk]	... TCP 443	192.168.122.62	(W...	TCP 49169	TlsCertificate	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
512	url.86865C5B3.html	html	1 070 B	216.58.210.67	[www.google.co.uk]	... TCP 80	192.168.122.62	(W...	TCP 49170	HttpGetN...	2015-06-30 13:11:57 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
515	favicon.ico	ico	5 430 B	216.58.210.67	[www.google.co.uk]	... TCP 80	192.168.122.62	(W...	TCP 49170	HttpGetN...	2015-06-30 13:12:44 ...	C:\Users\beh...	TLS Certificate: CN= google.com, O=Google Inc, L=Mour...									
524	index.html	html	829 B	192.254.234.118	floridablueline.com	... TCP 80	192.168.122.62	(W...	TCP 49171	HttpGetChu...	2015-06-30 13:12:44 ...	C:\Users\beh...	TLS Certificate: CN=GeoTrust Global CA, O=GeoTrust Inc...									
553	hnybx2w.php	html	265 B	103.113.214.190	femandatur.com	... TCP 80	192.168.122.62	(W...	TCP 49172	HttpGetN...	2015-06-30 13:12:45 ...	C:\Users\beh...	TLS Certificate: CN=femandatur.com, O=...									
529	floridabluelineheader.jpg	jpg	183.79 B	192.254.234.118	floridablueline.co...	... TCP 80	192.168.122.62	(W...	TCP 49171	HttpGetN...	2015-06-30 13:12:45 ...	C:\Users\beh...	TLS Certificate: CN=floridablueline.com/floridabluelineheader.jpg									
659	hnybx2w.php[1].html	html	323 B	208.113.214.190	femandatur.com	... TCP 80	192.168.122.62	(W...	TCP 49173	HttpGetN...	2015-06-30 13:12:46 ...	C:\Users\beh...	TLS Certificate: CN=femandatur.com/Scripts/hnybx2w.php[1]									
764	index.655880B7.html	html	147.90 B	40.30.45.65	good.recycleteam.com	... TCP 80	192.168.122.62	(W...	TCP 49174	HttpGetN...	2015-06-30 13:12:47 ...	C:\Users\beh...	TLS Certificate: CN=good.recycleteam.com/Xmpred.BKUDI3SKPfJkz...									
811	index.php.swf	swf	15 763 B	45.30.45.65	good.recycleteam.com	... TCP 80	192.168.122.62	(W...	TCP 49175	HttpGetN...	2015-06-30 13:12:48 ...	C:\Users\beh...	TLS Certificate: CN=good.recycleteam.com/index.php?Xmpred.BKUDI4L3S...									
841	version.xml[11.6.602].html	html	351 B	23.10.250.43	123.9.amana.net	... TCP 80	192.168.122.62	(W...	TCP 49176	HttpGetN...	2015-06-30 13:12:52 ...	C:\Users\beh...	TLS Certificate: CN=download2.macromedia.com/get/flashplayer/update/c...									
833	index.php.xmldownload	x...	352.25 B	46.30.45.65	good.recycleteam.com	... TCP 80	192.168.122.62	(W...	TCP 49174	HttpGetN...	2015-06-30 13:12:51 ...	C:\Users\beh...	TLS Certificate: CN=good.recycleteam.com/index.php?Xmpred.BKUD11TS...									

One is x-msdownload on frame 833 at 13:12:51. And the other is index.php.swf is a macromedia flash player on frame 841 at 13:12:53. Networkminer helps to find a frame number. So, based on frame number the capture in wireshark is as follows:



Wireshark - ECE570-2020-project3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
831	2015-06-30 13:12:49.483385	46.30.45.65	192.168.122.62	HTTP	944	HTTP/1.1 200 OK (application/x-shockwave-flash)
832	2015-06-30 13:12:49.483580	192.168.122.62	46.30.45.65	TCP	60	49175 → 80 [ACK] Seq=725 Ack=15933 Win=57977 Len=0
833	2015-06-30 13:12:51.834318	192.168.122.62	46.30.45.65	HTTP	569	GET /index.php?xniKfredLBvKDIU=l3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV_Opxv...
834	2015-06-30 13:12:51.834744	192.168.122.62	46.30.45.65	TCP	60	[TCP Window Update] 49175 → 80 [ACK] Seq=725 Ack=15933 Win=64343 Len=0
835	2015-06-30 13:12:51.972636	46.30.45.65	192.168.122.62	TCP	54	80 → 49174 [ACK] Seq=38858 Ack=1230 Win=17136 Len=0
836	2015-06-30 13:12:52.200920	192.168.122.62	192.168.122.1	DNS	86	Standard query 0x5A1D A fpdownload2.macromedia.com CNAME fpdownload2.wip4.adobe.com CNAME fp...
837	2015-06-30 13:12:52.354451	192.168.122.1	192.168.122.62	DNS	237	Standard query response 0x5A1D A fpdownload2.macromedia.com CNAME fpdownload2.wip4.adobe.com CNAME fp...
838	2015-06-30 13:12:52.355669	192.168.122.62	23.10.250.43	TCP	66	49176 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
839	2015-06-30 13:12:52.486624	23.10.250.43	192.168.122.62	TCP	66	80 → 49176 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=32
840	2015-06-30 13:12:52.487476	192.168.122.62	23.10.250.43	TCP	60	49176 → 80 [ACK] Seq=1 Ack=1 Win=65712 Len=0

Wireshark - Packet 833 - ECE570-2020-project3.pcap

> Internet Protocol Version 4, Src: 192.168.122.62, Dst: 46.30.45.65

> Transmission Control Protocol, Src Port: 49174, Dst Port: 80, Seq: 715, Ack: 33858, Len: 515

  > Hypertext Transfer Protocol

    > [truncated]GET /index.php?xniKfredLBvKDIU=l3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV\_Opxv...

    Accept: \*/\*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Host: good.recycle2learn.com)\r\nConnection: Keep-Alive\r\n\r\n[Full request URI [truncated]: http://good.recycle2learn.com/index.php?xniKfredLBvKDIU=l3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV\_Opxv...

  [HTTP request 2/2]

  [Prev request in frame: 764]

  [Response in frame: 1233]

No.: 833 - Time: 2015-06-30 13:12:51.834318 - Source: 192.168.122.62 - Destination: 46.30.45.65 - Protocol: HTTP - Length: 569 - Info: ...\_zR3AaQ4iloxQXB5MrPzwnEqWwxWeioXW\_RGJN1hM-5DAFrE92lyjx-cUlsN2wR7QumAGzO0ZUEgbogAQIryJQ-DbpgN6V0ggDE3KPZVlqx7IQnmtayh42P26QjA4

Close Help

Frame 833, host machine(192.168.122.62) sent GET HTTP request to 46.30.45.65 . Based on frame details this frame is requested from frame 764 previously and will be responded to in 1233.

We checked the URL in virus total and found this URL is malware and malicious.

[http://good.recycle2learn.com/index.php?xniKfredLBvKDIU=l3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV\\_Opxv...](http://good.recycle2learn.com/index.php?xniKfredLBvKDIU=l3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSih170IFxzsmTu2KV_Opxv...)

2 engines detected this URL

http://good.recycle2learn.com/index.php?xniKfredLBvKDIU=i3SMfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-ofSh170lfxxsmTu2KV\_OpgxveN0SZFT\_zR3AaQ4ilotXQB5MrPzwnEqWwxWeiXW\_RGJN1hM-5DAFrE92lyjx-cUlsN2wR7QumAgnO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlqx7IQnmtayh42P26QjA4

good.recycle2learn.com

2018-04-29 23:09:37 UTC  
2 years ago

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware	Forcepoint ThreatSeeker	① Malicious
ADMINUSLabs	✓ Clean	AegisLab WebGuard	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean
Bitdefender	✓ Clean	SIFT	✓ Clean

Community Score

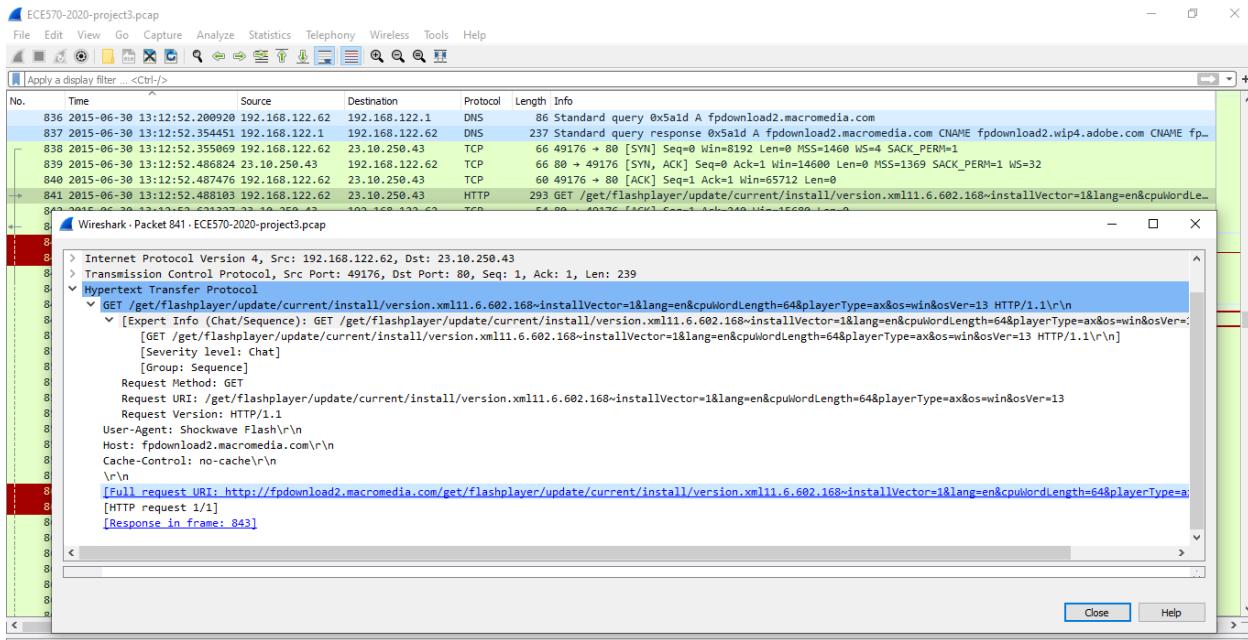
Community Score

The IP address of this site ([www.good.recycle2learn.com](http://www.good.recycle2learn.com)) checked in [ipvoid.com](http://ipvoid.com) to know about situation

Analysis Date	2020-07-31 00:21:17
Elapsed Time	2 seconds
Blacklist Status	BLACKLISTED 1/114
IP Address	<a href="#">46.30.45.65</a> Find Sites   IP Whois
Reverse DNS	serv1.abitec.ru
ASN	<a href="#">AS210079</a>
ASN Owner	EuroByte LLC
ISP	EuroByte LLC
Continent	Europe
Country Code	 (RU) Russia
Latitude / Longitude	55.7386 / 37.6068 <a href="#">Google Map</a>
City	Unknown

In packet 841





User agent here is shockwave flash which we found it malicious with 35 engines in packet 831, host is fpdownload, which is some kind of upgrading the flash player.

URL

<http://fpdownload2.macromedia.com/get/flashplayer/update/current/install/version.xml11.6.602.168~installVector=1&lang=en&cpuWordLength=64&playerType=ax&os=win&osVer=13>

 <http://fpdownload2.macromedia.com/get/flashplayer/update/current/install/version.xml11.6.602.168~i>    Sign in



No engines detected this URL

<http://fpdownload2.macromedia.com/get/flashplayer/update/current/install/version.xml11.6.602.168~installVector=1&lang=en&cpuWordLength=64&playerType=ax&os=win&osVer=13>

Community Score

404 Status

text/html; c... Content Type

2018-06-29 14:17:16 UTC

2 years ago

DETECTION	DETAILS	RELATIONS	COMMUNITY
ADMINUSLabs	 Clean		AegisLab WebGuard  Clean
AlienVault	 Clean		Antiy-AVL  Clean
Avira (no cloud)	 Clean		Baidu-International  Clean
BitDefender	 Clean		Blueliv  Clean

## In another Tab DNS we found a little information

	2018-06-30 13:12:52Z	CKdhc21h1h9kqH5m2g	192.168.122.62	54128	192.168.122.1	53	udp	23069	fpdownload2.macromedia.com 
<b>Query Class Desc C_INTERNET</b>									
Query Type 1									
Query Type Desc A									
Response Code 0									
Response Code Desc NOERROR									
Authoritative Answer? F									
Truncated? F									
Recursion Desired? T									
Recursion Available? T									
Answers ...m.edgesuite.net,a1293.d.akamai.net,23.10.250.43,23.10.250.18									
TTLs 21078.000000,119.000000,21232.000000,19.000000,19.000000									
Authoritative Response null									
Additional Response(s) null									



In the context of a cyber-attack, a payload is the component of the attack which causes harm to the victim. Much like the Greek soldiers hiding inside the wooden horse in the tale of the Trojan Horse, a malicious payload can sit harmlessly for some time until triggered.

Attackers must first find a method to deliver the malicious payload onto the victim's computer. DNS hijacking is a common example of payload delivery techniques.

Once a payload is in place, it will usually sit dormant until being executed. An attacker can select from many different ways to execute a malicious payload. Some common ways to execute a malicious payload:

**Opening an executable file:** For example a victim downloads an email attachment that they believe to be a piece of pirated software and they double-click on the installation file which executes the payload.

**Setting off a specific set of behavioral conditions:** This is known as a logic bomb. For example, an unscrupulous employee might integrate a logic bomb into his company's network that continually checks to see if that employee is still on the payroll. When he is no longer on the payroll, the logic bomb will meet its condition and the malicious payload will be executed.

**Opening certain non-executable files:** Even some non-executable files can contain malicious payloads. For example there are attacks where malicious payloads are hidden in .PNG image files. When a victim opens these image files, the payload is executed.



So, we export both HTTP and FILES TRANSFER from the packet total.

## HTTP payload page1

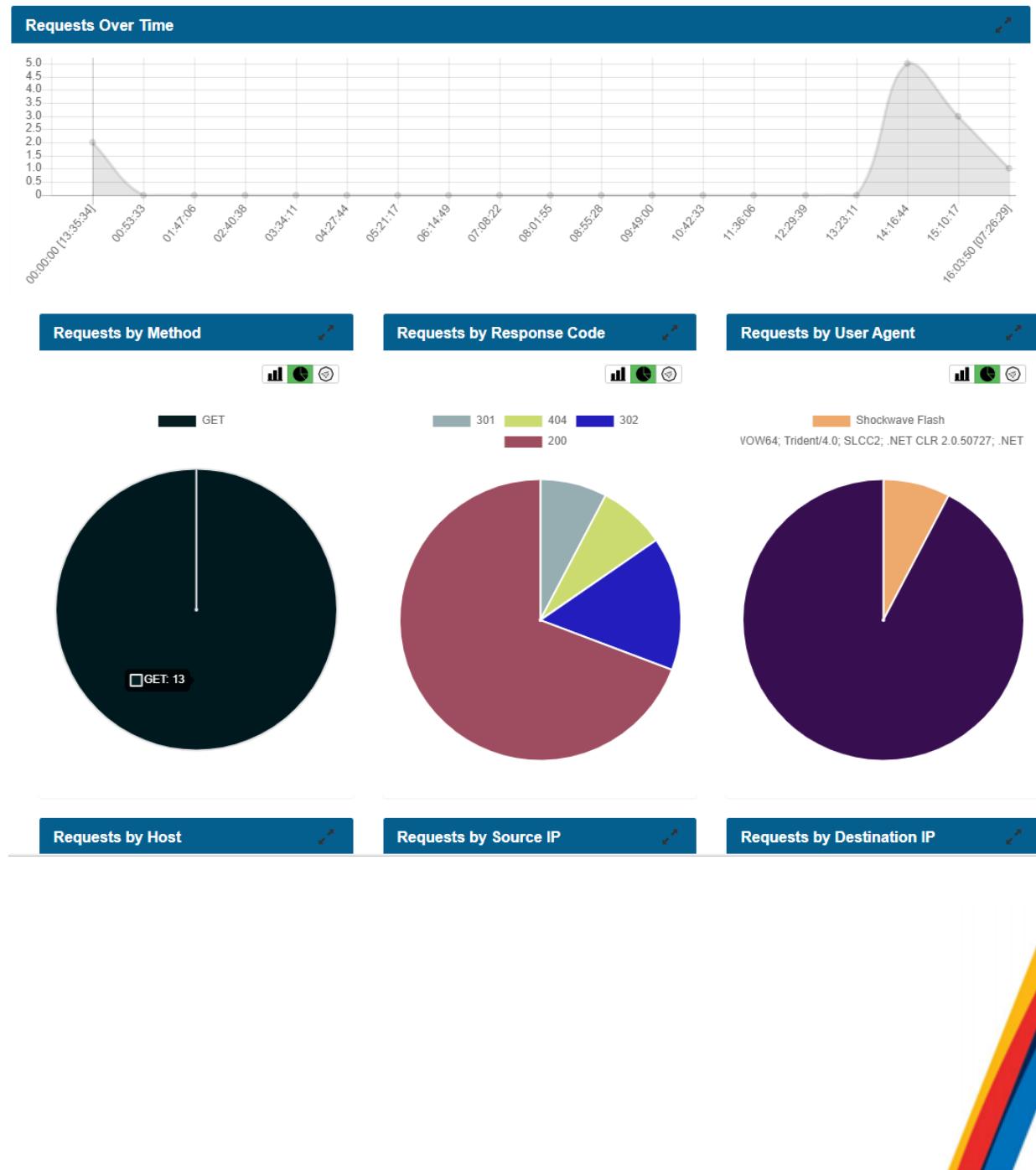
Timestamp	Connectic Sender IP	Sender Pc Target IP	Target Port	Transactic	Meth	Host	URI	Referrer	User Agent	Request B	Response
2015-06-30 13:11:51 Z	Cs8Y2Q2y	192.168.122.62	49158	216.58.208.46	80	1	GET google.comÃ	/	null	....NET CLR 3.5.3	0 261
2015-06-30 13:11:51 Z	CMuHRO3	192.168.122.62	49159	216.58.210.67	80	1	GET www.google.co.ukÃ	?gfe_rd=cr&ei=l5WSVaxXXFrI	null	....NET CLR 3.5.3	0 277
2015-06-30 13:12:44 Z	CIFU4P2T	192.168.122.62	49170	216.58.210.67	80	1	GET www.google.co.ukÃ	...amp;ved=0CBQQFjAA&usg	null	....NET CLR 3.5.3	0 1070
2015-06-30 13:12:44 Z	CIFU4P2T	192.168.122.62	49170	216.58.210.67	80	2	GET www.google.co.ukÃ	/favicon.ico	null	....NET CLR 3.5.3	0 5430
2015-06-30 13:12:44 Z	CALygR1Jr	192.168.122.62	49171	192.254.234.118	80	1	GET www.floridablueline.comÃ	/	....amp;ved	....NET CLR 3.5.3	0 829
2015-06-30 13:12:45 Z	CALygR1Jr	192.168.122.62	49171	192.254.234.118	80	2	GET www.floridablueline.comÃ	/floridabluelineheader.jpg	http://www....NET CLR 3.5.3	0 183799	
2015-06-30 13:12:45 Z	CMVaAQV2	192.168.122.62	49172	208.113.214.190	80	1	GET fernandatur.comÃ	/Scripts/hqnybx2w.php?id=9	http://www....NET CLR 3.5.3	0 265	
2015-06-30 13:12:46 Z	CMHHzK11	192.168.122.62	49173	208.113.214.190	80	1	GET www.fernandatur.comÃ	/Scripts/hqnybx2w.php?id=9	http://www....NET CLR 3.5.3	0 323	
2015-06-30 13:12:47 Z	CocBdE3V	192.168.122.62	49174	46.30.45.65	80	1	GET good.recycle2learn.com	...zwnEqVwxWeioxW_RGN	http://www....NET CLR 3.5.3	0 142971	
2015-06-30 13:12:48 Z	CtGi8l22yi	192.168.122.62	49175	46.30.45.65	80	1	GET good.recycle2learn.com	...GzO0ZUEgbogAQIryJQ-Dbp	...4SGhKrX ....NET CLR 3.5.3	0 15763	
2015-06-30 13:12:51 Z	CocBdE3V	192.168.122.62	49174	46.30.45.65	80	2	GET good.recycle2learn.com	...umAGzO0ZUEgbogAQIryJQ	null	....NET CLR 3.5.3	0 352256
2015-06-30 13:12:52 Z	CtOXU293	192.168.122.62	49176	23.10.250.43	80	1	GET fpdownload2.macromedia.c	...;cpuWordLength=64&play	null	Shockwave Flash	0 351
2015-06-30 13:12:55 Z	CALygR1Jr	192.168.122.62	49171	192.254.234.118	80	3	GET www.floridablueline.comÃ	/favicon.ico	null	....NET CLR 3.5.3	0 0



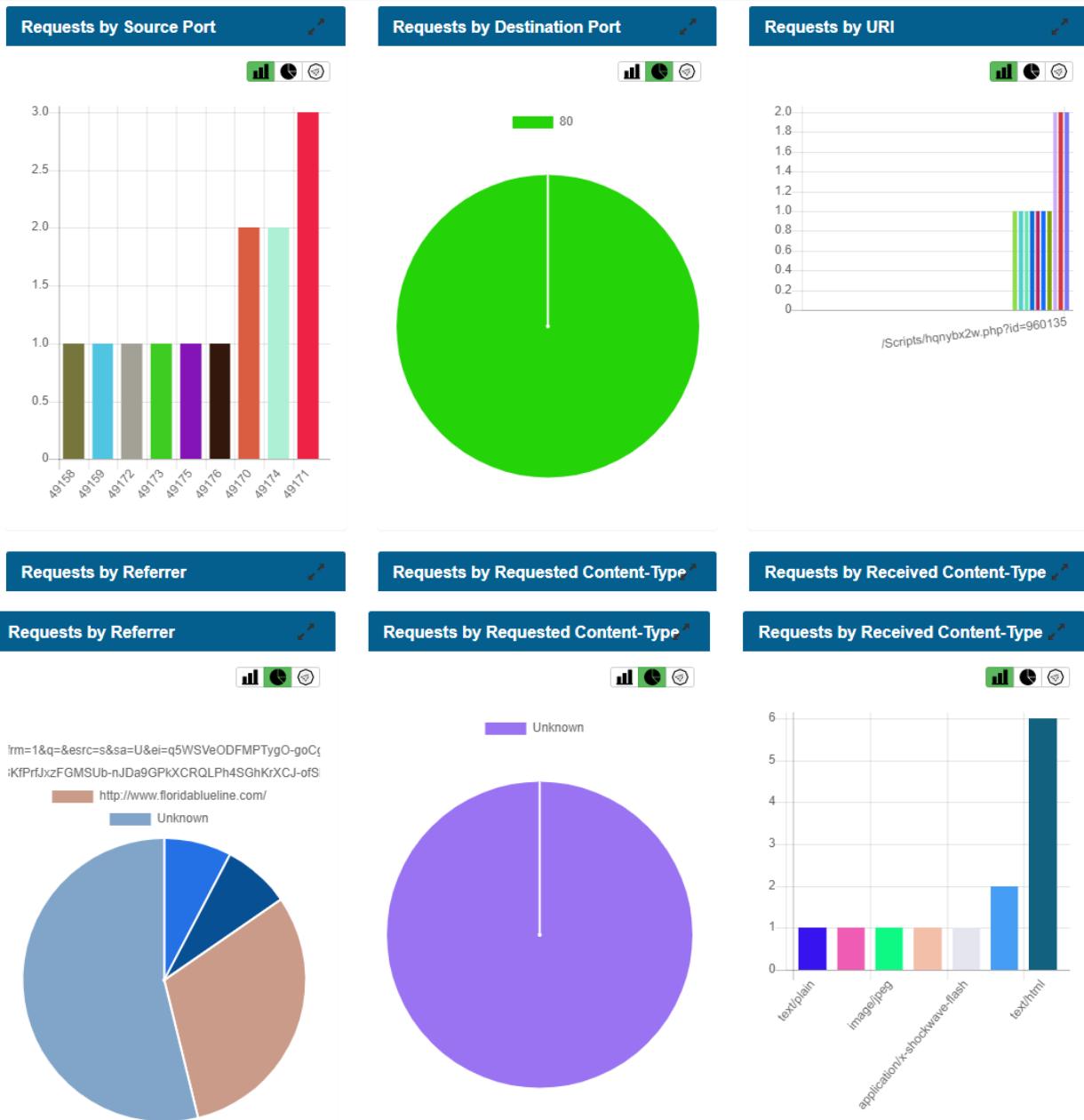
## Page2

Request	B	Response	Status	Coc	Status	Me	Info	Code	Info	Mess	File	Username	Password	Proxied	Sender	Fil	Sender	Mi	Recipient	Recipient	Client	He	Server	He	Cookie	Va	URI	Variables
0	261	302	Found	null	null	null	null	null	null	null	null	FZUYUM11	text/html	ACCEPT,A	null	null	/											
0	277	302	Found	null	null	null	null	null	null	null	null	FQFIU3F	text/html	ACCEPT,A	null	null	/										?gfe_rd,ei	
0	1070	200	OK	null	null	null	null	null	null	null	null	FVBLH1F	text/plain	ACCEPT,A	null	null										PREF,NID,	/url?url,rct,frm,q,esid	
0	5430	200	OK	null	null	null	null	null	null	null	null	FB9ZM13K	image/x-i	ACCEPT,A	null	null											PREF,NID,	/favicon.ico
0	829	200	OK	null	null	null	null	null	null	null	null	FIA3OB1ZE	text/html	ACCEPT,Ri	null	null											null	/
0	183799	200	OK	null	null	null	null	null	null	null	null	FIC2IDEN	image/jpe	ACCEPT,Ri	null	null											null	/floridablueheadlinehead
0	265	301	Moved Per	null	null	null	null	null	null	null	null	FIPQYF2ZZ	text/html	ACCEPT,Ri	null	null											null	/Scripts/hqnybx2w,p
0	323	200	OK	null	null	null	null	null	null	null	null	F4IAYX1V	application	ACCEPT,Ri	null	null											null	/Scripts/hqnybx2w,p
0	142971	200	OK	null	null	null	null	null	null	null	null	FEEAQSN	text/html	ACCEPT,Ri	null	null											null	/?xn1KfrediBvKDIU
0	15763	200	OK	null	null	null	null	null	null	null	null	FSQGD12C	application	ACCEPT,A	null	null											null	/index.php?xn1Kfredi
0	352256	200	OK	null	null	null	null	null	null	null	null	FHRPWCV	null	ACCEPT,A	null	null											null	/index.php?xn1Kfredi
0	351	404	Not Found	null	null	null	null	null	null	null	null	FDFE1CAJF	text/html	USER-AGE	null	null											...602.168~installVec	
0	0	200	OK	null	null	null	null	null	null	null	null	ACCEPT,A	null	null													null	/favicon.ico

### Diagram of HTTP report on packettotal







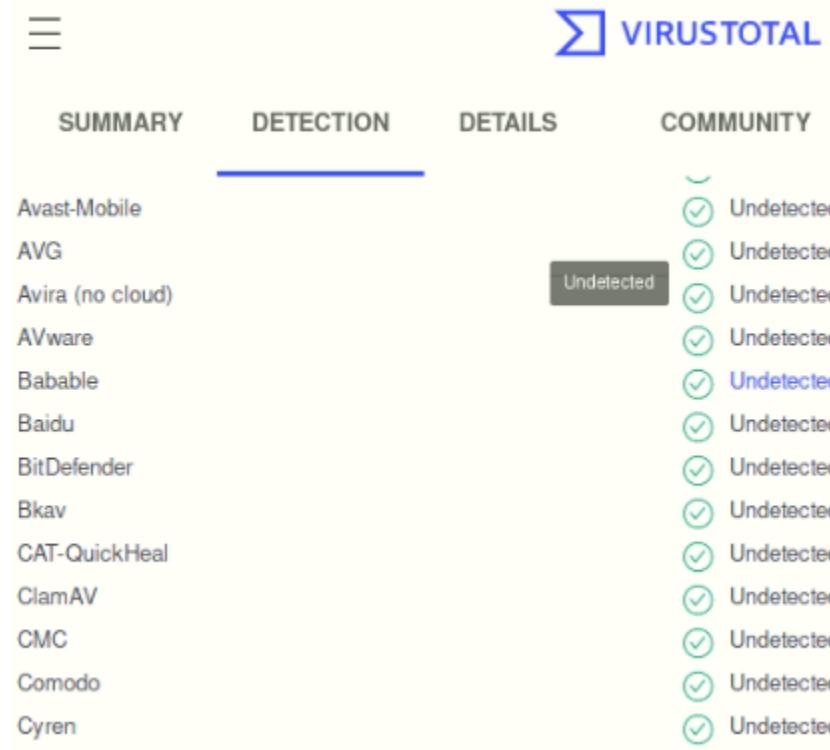
The Files Transfer payload as follows:



1	Timestamp	Connection IDs	Artifact	MD5 Hash	SHA1 Hash	Originated From Host/: Sent To Host/s	Source	Depth	Mime Type	File Name	Total Bytes
2	2015-06-30 13:12:44 Z	CIFU4P2TqMgvSgfc62	FVBL1H1FVSERAS 1332bd535c01fd4 da951504bb632 216.58.210.67			192.168.122.62	HTTP	0	text/plain	null	null
3	2015-06-30 13:12:44 Z	CIFU4P2TqMgvSgfc62	FB9ZMI3KOMATO a300693728f5caa'e2020bf4f2b65f 216.58.210.67			192.168.122.62	HTTP	0	image/x-icon	null	null
4	2015-06-30 13:12:45 Z	CALygR1JnXOgNnETj	FIA30B1ZBQ86MY 6535a237a2652f5462fdab7eaaf516 192.254.234.118			192.168.122.62	HTTP	0	text/html	null	null
5	2015-06-30 13:12:45 Z	CALygR1JnXOgNnETj	FIC2ID2ENIQ6Z2U cb5d1061b1ef3b28fbec3e6569cef 192.254.234.118			192.168.122.62	HTTP	0	image/jpeg	null	183799
6	2015-06-30 13:12:45 Z	CMvAQV20wfxQnWdf	FIPQYF2ZJIGRO7 1675befb11864f1 f162b138954f6a 208.113.214.190			192.168.122.62	HTTP	0	text/html	null	null
7	2015-06-30 13:12:47 Z	CMHzKLIVvh1X1U2	F4JAYX1VSTBLTT5 b69afaef73df2f68r713824ab0f35a5 208.113.214.190			192.168.122.62	HTTP	0	application/javascript	null	null
8	2015-06-30 13:12:48 Z	CocBdE3VP4U7E8PX5	FEEAQ5NAFXOGSI 4634a93740f1492 b8777893cd3 146.30.45.65			192.168.122.62	HTTP	0	text/html	null	null
9	2015-06-30 13:12:49 Z	CtGibl22yrRPVILob	FSQGDLCN1BEPC 4a08a4536b6b62f bcc562479d2c1 46.30.45.65			192.168.122.62	HTTP	0	application/x-shockwave	null	15763
10	2015-06-30 13:12:52 Z	CtoXLI293JVZ3O168n	FDFE1C4JMCXQBC 58f46f6f93cadc3b 8ae69b66ebe0 23.10.250.43			192.168.122.62	HTTP	0	text/html	null	351
11	2015-06-30 13:12:54 Z	CocBdE3VP4U7E8PX5	FHRPWCV7ASNO eb756a359d0c5e a1a9b3f5bc705c 46.30.45.65			192.168.122.62	HTTP	0	null	null	352256

Screen shots of all HTTP payloads are as a following pictures respectively based on table above:

Google.com



SUMMARY	DETECTION	DETAILS	COMMUNITY
Avast-Mobile			<input checked="" type="checkbox"/> Undetected
AVG			<input checked="" type="checkbox"/> Undetected
Avira (no cloud)		<span style="background-color: #ccc; padding: 2px;">Undetected</span>	<input checked="" type="checkbox"/> Undetected
AVware			<input checked="" type="checkbox"/> Undetected
Babable			<input checked="" type="checkbox"/> Undetected
Baidu			<input checked="" type="checkbox"/> Undetected
BitDefender			<input checked="" type="checkbox"/> Undetected
Bkav			<input checked="" type="checkbox"/> Undetected
CAT-QuickHeal			<input checked="" type="checkbox"/> Undetected
ClamAV			<input checked="" type="checkbox"/> Undetected
CMC			<input checked="" type="checkbox"/> Undetected
Comodo			<input checked="" type="checkbox"/> Undetected
Cyren			<input checked="" type="checkbox"/> Undetected

www.google.co.uk





SUMMARY

DETECTION

DETAILS

COMMUNITY

Avast-Mobile		Undetected
AVG		Undetected
Avira (no cloud)		Undetected
AVware		Undetected
Babable		Undetected
Baidu		Undetected
BitDefender		Undetected
Bkav		Undetected
CAT-QuickHeal		Undetected
ClamAV	Undetected	Undetected
CMC		Undetected
Comodo		Undetected
Cyren		Undetected

[www.google.co.uk](http://www.google.co.uk)



SUMMARY

DETECTION

DETAILS

COMMUNITY

Avast-Mobile		Undetected
AVG		Undetected
Avira (no cloud)		Undetected
AVware	Undetected	Undetected
Babable		Undetected
Baidu		Undetected
BitDefender		Undetected
Bkav		Undetected
CAT-QuickHeal		Undetected
ClamAV		Undetected
CMC		Undetected
Comodo		Undetected
Cyren		Undetected

[www.google.co.uk](http://www.google.co.uk)

SUMMARY

DETECTION

DETAILS

RELATIONS

C

Avast-Mobile	Undetected
AVG	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
BitDefender	Undetected
BitDefenderTheta	Undetected
Bkav	Undetected
CAT-QuickHeal	Undetected
ClamAV	Undetected
CMC	Undetected
Comodo	Undetected
Cyren	Undetected
DrWeb	Undetected





## SUMMARY

## DETECTION

## DETAILS

## COMMUNITY

Ad-Aware	(!) Trojan.GenericKD.31150873
AegisLab	(!) Trojan.Script.Generic.4!c
AhnLab-V3	(!) HTML/Redirect
ALYac	(!) Trojan.GenericKD.31150873
Antiy-AVL	(!) Trojan/JS.Redirector.nt
Arcabit	(!) Trojan.Generic.D1DB5319
Avast	(!) HTML:Includer-BR [Trj]
AVG	(!) HTML:Includer-BR [Trj]
Avira (no cloud)	(!) HTML/Rce.Gen2
BitDefender	(!) Trojan.GenericKD.31150873
CAT-QuickHeal	(!) JS.Redirector.AN
Emsisoft	(!) Trojan.GenericKD.31150873 (B)
eScan	(!) Trojan.GenericKD.31150873
F-Secure	(!) Malware.HTML/Rce.Gen2
FireEye	(!) Trojan.GenericKD.31150873
Fortinet	(!) HTML/InjectedPhp.NZltr
GData	(!) Script.Packed.IFrame.K@gen
Ikarus	(!) Trojan.Script
Kaspersky	(!) HEUR:Trojan.Script.Generic
MAX	(!) Malware (ai Score=99)
Microsoft	(!) Trojan:HTML/Redirector.EP
NANO-Antivirus	(!) Trojan.Html.Iframe.dcipov
Qihoo-360	(!) Generic/Trojan.Script.ed4
Sophos AV	(!) Troj/JSRedir-NZ
Symantec	(!) Trojan.Gen.2



VIPRE  
ZoneAlarm by Check Point  
Avast-Mobile  
Baidu  
BitDefenderTheta

- (!) LooksLike.JS.Redirector.nt (v)
- (!) HEUR:Trojan.Script.Generic
- (✓) Undetected
- (✓) Undetected
- (✓) Undetected

27 transcripts, malware found

[www.floridablueline.com](http://www.floridablueline.com)

 VIRUSTOTAL

SUMMARY	DETECTION	DETAILS	COMMUNITY
Ad-Aware		(✓) Undetected	
AegisLab		(✓) Undetected	
AhnLab-V3		(✓) Undetected	
ALYac		(✓) Undetected	
Antiy-AVL		(✓) Undetected	
Arcabit		(✓) Undetected	
Avast		(✓) Undetected	
Avast-Mobile		(✓) Undetected	
AVG		(✓) Undetected	
Avira (no cloud)		(✓) Undetected	
AVware		(✓) Undetected	
Babable		(✓) Undetected	
Baidu		(✓) Undetected	
...		...	

[Fernandatur.com](http://Fernandatur.com)





SUMMARY

DETECTION

DETAILS

COMMUNITY

Ad-Aware	 Undetected
AegisLab	 Undetected
AhnLab-V3	 Undetected
ALYac	 Undetected
Antiy-AVL	 Undetected
Arcabit	 Undetected
Avast	 Undetected
Avast-Mobile	 Undetected
AVG	 Undetected
Avira (no cloud)	 Undetected
AVware	 Undetected
Babable	 Undetected
Baidu	 Undetected





SUMMARY

DETECTION

DETAILS

COMMUNITY

AegisLab		(!) Script.Troj.Gen!c
Avast		(!) JS:Iframe-EOD [Trj]
AVG		(!) JS:Iframe-EOD [Trj]
Bkav		(!) JS.elframeDwNMe.FE8B
GData		(!) Script.Trojan.Redirector.AZ
Ikarus		(!) HTML.Framer
Qihoo-360		(!) Virus.js.qexvmc.1
TrendMicro-HouseCall		(!) Suspicious_GEN.F47V0731
Ad-Aware	✓ Undetected	
AhnLab-V3	✓ Undetected	
ALYac	✓ Undetected	
Antiy-AVL	✓ Undetected	
Arcabit	✓ Undetected	
...	...	...



 VIRUSTOTAL

SUMMARY

DETECTION

DETAILS

COMMUNITY

AegisLab	!	Trojan.HTML.Generic.4!c
ESET-NOD32	!	JS/Kryptik.AVE
Ikarus	!	JS.Exploit
Kaspersky	!	HEUR:Exploit.Script.Generic
McAfee-GW-Edition	!	BehavesLike.HTML.ExploitBlacole.cr
Microsoft	!	Trojan:Script/Wacatac.C!ml
Qihoo-360	!	Generic/Trojan.Exploit.b4f
Rising	!	Trojan.Kryptik!8.8 (TOPIS:E0:0xbvllh1xeV)
Sangfor Engine Zero	!	Malware
Sophos AV	!	Troj/ExpJS-KX
Symantec	!	Trojan.Gen.7
ZoneAlarm by Check Point	!	HEUR:Exploit.Script.Generic
Ad-Aware	✓	Undetected

Good.recycle2learn.com



SUMMARY

DETECTION

DETAILS

COMMUNITY

4

Ad-Aware	!	Script.SWF.Exploit.CVE-2015-3105.C500
AegisLab	!	Hacktool.SWF.Agent.3!c
AhnLab-V3	!	SWF/Exploit
ALYac	!	Script.SWF.Exploit.CVE-2015-3105.C500
Antiy-AVL	!	Trojan[Exploit]/SWF.SWF.Generic
Arcabit	!	Script.SWF.Exploit.CVE-2015-3105.C500
Avast	!	SWF:Malware-gen [Tr]
AVG	!	SWF:Malware-gen [Tr]
Avira (no cloud)	!	EXP/Agent.EB.48
BitDefender	!	Script.SWF.Exploit.CVE-2015-3105.C500
CAT-QuickHeal	!	SWF.Kit.Nuclear.N
ClamAV	!	Swf.Exploit.Kit-99
Comodo	!	Malware@#2iqyxwbc2cazk



Cyren	!	SWF/SWF/Exploit
DrWeb	!	Exploit.SWF.1232
Emsisoft	!	Script.SWF.Exploit.CVE-2015-3105.C500 (B)
eScan	!	Script.SWF.Exploit.CVE-2015-3105.C500
ESET-NOD32	!	SWF/Exploit.ExKit.AS
F-Prot	!	SWF/SWF/Exploit
F-Secure	!	Exploit.EXP/Agent.EB.48
FireEye	!	Script.SWF.Exploit.CVE-2015-3105.C500
GData	!	Script.SWF.Exploit.CVE-2015-3105.C500
Ikarus	!	Trojan.SWF.Exploit
Kaspersky	!	Exploit.SWF.Agent.ro
MAX	!	Malware (ai Score=100)
<hr/>		
McAfee	!	SWF/Exploit-Rig.a
McAfee-GW-Edition	!	BehavesLike.Flash.Exploit.mg
NANO-Antivirus	!	Trojan.Swf.Mlw.ebrtv
Qihoo-360	!	Generic/Trojan.Exploit.7f1
Sophos AV	!	Troj/SWFExp-HN
Symantec	!	Trojan.Gen.2
Tencent	!	Win32.Exploit.Agent.Pbpg
TrendMicro	!	EXPL_CVE20153090
Zillya	!	Exploit.Agent.Script.854
ZoneAlarm by Check Point	!	Exploit.SWF.Agent.ro
Avast-Mobile	✓	Undetected
Baidu	✓	Undetected
BitDefenderTheta	✓	Undetected

35 engines detected malware, trojan scripts,swf exploit

Good.recycle2learn.com



 VIRUSTOTAL

SUMMARY

DETECTION

DETAILS

COMMUNITY

Fortinet		 Undetected
GData		 Undetected
Ikarus		 Undetected
Jiangmin		 Undetected
K7AntiVirus		 Undetected
K7GW		 Undetected
Kaspersky		 Undetected
Kingsoft		 Undetected
Malwarebytes		 Undetected
MAX		 Undetected
MaxSecure		 Undetected
NANO-Antivirus		 Undetected
Panda		 Undetected

Fpdownload2.macromedia.com





## SUMMARY

## DETECTION

## DETAILS

## COMMUNITY

Ad-Aware	 Undetected
AegisLab	 Undetected
AhnLab-V3	 Undetected
ALYac	 Undetected
Antiy-AVL	 Undetected
Arcabit	 Undetected
Avast	 Undetected
Avast-Mobile	 Undetected
AVG	 Undetected
Avira (no cloud)	 Undetected
Baidu	 Undetected
BitDefender	 Undetected
BitDefenderTheta	 Undetected



192.168.122.62 (Windows)

- IP: 192.168.122.62
- MAC: 000000000000
- NIC Vendor: XEROX CORPORATION
- MAC Age: 2000-09-08
- Hostname:
- OS: Windows
  - TTL: 128 (distance: 0)
  - Open TCP Ports:
    - Sent: 768 packets (69,734 Bytes), 0.00% cleartext (0 of 0 Bytes)
    - Received: 1209 packets (1,516,720 Bytes), 0.00% cleartext (0 of 0 Bytes)
  - Incoming sessions: 0
  - Outgoing sessions: 21
- Host Details
  - Queried NetBIOS names : \*<00>
  - Queried DNS names : google.com,www.google.co.uk,ssl.gstatic.com,clients1.google.co.uk,www.florid
  - Web Browser User-Agent 1 : Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4
  - Web Browser User-Agent 2 : Shockwave Flash
  - Device Category : Windows
  - JA3 Hashes : 4d7a28d6f2263ed61de88ca66eb011e3
  - JA3 Fingerprint 4d7a28d6f2263ed61de88ca66eb011e3 : Test FP: Nuclear Exploit Kit, Malware Test F
  - HTTP header: x-flash-version 1 : 11,6,602,168

JA3: 4d7a28d6f2263ed61de88ca66eb011e3

It is a fingerprint for Emotet.

In these malware examples, the command and control server always responds to the malware client in exactly the same way, it does not deviate. So even though the traffic is encrypted and one may not know the command and control server's IPs or domains as they are constantly changing,

In this pcap file we have windows update, and messages like Hello Client.and also the first frames of pcap has a lot of TLS files. These are weird, so based on the behaviour of packets in wireshark and searching on the internet we found some clues.

Some part of our pcap file that include windows update, and messages like Hello Client is as a follows:



18 2013-06-30 13:11:51.928384 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
19 2013-06-30 13:11:52.062651 216.56.218.67	192.168.122.62	TCP	00 443 + 443 [SYN, ACK] Seq=1 Win=12000 Len=0 MSS=1300 SACK_PERM=1 Len=128
20 2013-06-30 13:11:53.051936 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
21 2013-06-30 13:11:53.055613 192.168.122.62	216.56.218.67	TLSv1.2	213 Client Hello
22 2013-06-30 13:11:53.055613 216.56.218.67	192.168.122.62	TCP	00 443 + 443 [TCP Window Update] Seq=11300 Win=62380 Len=0
24 2013-06-30 13:11:53.215604 216.56.218.67	192.168.122.62	TLSv1.2	1423 Server Hello
25 2013-06-30 13:11:53.215604 216.56.218.67	192.168.122.62	TCP	00 443 [ACK] Seq=11300 Win=62380 Len=0
26 2013-06-30 13:11:53.216424 216.56.218.67	192.168.122.62	TLSv1.2	841 Certificate, Server Key Exchange, Server Hello Done
27 2013-06-30 13:11:53.216424 216.56.218.67	192.168.122.62	TCP	00 49108 + 443 [ACK] Seq=11300 Win=62380 Len=0
28 2013-06-30 13:11:52.245528 192.168.122.62	216.56.218.67	TLSv1.2	284 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29 2013-06-30 13:11:52.378853 216.56.218.67	192.168.122.62	TLSv1.2	129 Change Cipher Spec, Encrypted Handshake Message
30 2013-06-30 13:11:52.418634 192.168.122.62	216.56.218.67	TLSv1.2	875 Application Data
31 2013-06-30 13:11:52.418634 216.56.218.67	192.168.122.62	TCP	00 443 + 49108 Seq=1001 Ack=1158 Win=46728 Len=0
32 2013-06-30 13:11:52.609698 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
33 2013-06-30 13:11:52.609698 216.56.220.87	192.168.122.62	TLSv1.2	1419 Application Data
34 2013-06-30 13:11:52.609789 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
35 2013-06-30 13:11:52.609789 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACK] Seq=11308 Ack=6331 Win=65512 Len=0
36 2013-06-30 13:11:52.609789 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
37 2013-06-30 13:11:52.609789 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
38 2013-06-30 13:11:52.609789 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
39 2013-06-30 13:11:52.609789 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACK] Seq=11308 Ack=9961 Win=65512 Len=0
40 2013-06-30 13:11:52.609789 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
41 2013-06-30 13:11:52.609801 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
42 2013-06-30 13:11:52.609814 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
43 2013-06-30 13:11:52.609821 216.56.218.67	192.168.122.62	TLSv1.2	1419 Application Data
44 2013-06-30 13:11:52.609839 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACE] Seq=11309 Ack=11791 Win=0
45 2013-06-30 13:11:52.609839 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACK] Seq=11309 Ack=14521 Win=62380 Len=0
46 2013-06-30 13:11:52.609851 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACK] Seq=11309 Ack=17251 Win=65508 Len=0
47 2013-06-30 13:11:52.609851 192.168.122.62	216.56.218.67	TCP	00 [TCP Window Update] 49108 + 443 [ACK] Seq=11309 Ack=17251 Win=65508 Len=0
48 2013-06-30 13:11:52.744423 216.56.218.67	192.168.122.62	TLSv1.2	1423 Application Data
49 2013-06-30 13:11:52.744604 216.56.218.67	192.168.122.62	TLSv1.2	1423 Application Data
50 2013-06-30 13:11:52.744849 192.168.122.62	216.56.218.67	TCP	00 49108 + 443 [ACK] Seq=11309 Ack=19969 Win=65712 Len=0

TLS and it's predecessor, SSL, are used to encrypt communication for both common applications, to keep your data secure, and malware, so it can hide in the noise. To initiate a SSL session, a client will send a SSL Client Hello packet following the TCP 3-way handshake. This packet and the way in which it is generated is dependent on packages and methods used when building the client application. The server, if accepting SSL connections, will respond with a SSL Server Hello packet that is formulated based on server-side libraries and configurations as well as details in the Client Hello. Because SSL negotiations are transmitted in the clear, it's possible to fingerprint and identify client applications using the details in the SSL Client Hello packet.

The JA3 method is used to gather the decimal values of the bytes for the following fields in the Client Hello packet: Version, Accepted Ciphers, List of Extensions, Elliptic Curves, and Elliptic Curve Formats. It then concatenates those values together in order, using a "," to delimit each field and a "-" to delimit each value in each field.

Emotet is a Trojan that do infection via malicious script, macro-enabled document files, or malicious JavaScript file. Emotet may try to persuade users to click the malicious files.



5. Identify other malicious hosts or sites with which the compromised host interacted. Only malicious hosts should be included in this list. Provide your response in a table listing the following.

Table below includes all probable malicious hosts/websites which host IP 192.168.122.62. Even though we explained some of them in above questions

Host name/URL	IP Address	Role	service	Communication protocol	Start Date/time	End date/time
floridablueline.com, www.floridablueline.com	192.254.234.118	Compromised website	http	tcp	13:12:44	13:13:55
fernandatur.com, www.fernandatur.com	208.113.214.190	Redirect host	http	tcp	13:12:44	13:13:55
good.recycle2learn.com	46.30.45.65	Delivered malware	http	tcp	13:12:47	13:13:55
a1293.d.akamai.net, fpdownload.macromedia.com.edgesuite.net, fpdownload2.macromedia.com	23.10.250.43	Web Server banner  Not found for get flash player update	http	tcp	13:12:52	13:13:55



---	43.225.38.217	Encrypted traffic	null	tcp	13:13:14	13:15:25
time.microsoft.aka dns.net, time.windows.co m	23.99.222.162	Looks not malicious	null	udp	13:16:13	13:16:14
---	111.121.193.242	Spam traffic	null	tcp	13:15:55	13:15:58
---	78.129.168.237	Traffic	null	udp	13:16:17	13:16:20
Unknown host	37.55.107.202	Continus traffic	null	tcp	13:16:28	13:17:45
a1293.d.akamai.net , fpdownload.macro media.com.edgesui te.net	23.10.250.18	DNS hijacking, MAC spoofing	null	tcp		

For IP 43.225.38.217 shows TCp traffic and also one engin found it malicious



lo.	Time	Source	Destination	Protocol	Length	Info
1253	2015-06-30 13:13:14.087639	192.168.122.62	43.225.38.217	TCP	66	49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1254	2015-06-30 13:13:14.481484	43.225.38.217	192.168.122.62	TCP	54	443 → 49177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1255	2015-06-30 13:13:14.990962	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1256	2015-06-30 13:13:15.391086	43.225.38.217	192.168.122.62	TCP	54	443 → 49177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1257	2015-06-30 13:13:15.895782	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49177 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
1262	2015-06-30 13:13:16.290494	43.225.38.217	192.168.122.62	TCP	54	443 → 49177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1264	2015-06-30 13:13:16.688117	192.168.122.62	43.225.38.217	TCP	66	49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1265	2015-06-30 13:13:16.688117	43.225.38.217	192.168.122.62	TCP	54	443 → 49178 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1266	2015-06-30 13:13:17.204972	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49178 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1267	2015-06-30 13:13:47.597715	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1268	2015-06-30 13:13:48.109606	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
1269	2015-06-30 13:13:48.502958	43.225.38.217	192.168.122.62	TCP	54	443 → 49178 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1276	2015-06-30 13:14:18.503667	192.168.122.62	43.225.38.217	TCP	66	49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1277	2015-06-30 13:14:18.901948	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1278	2015-06-30 13:14:19.407842	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1279	2015-06-30 13:14:19.808323	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1280	2015-06-30 13:14:26.310993	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49179 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
1281	2015-06-30 13:14:26.704101	43.225.38.217	192.168.122.62	TCP	54	443 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1282	2015-06-30 13:14:50.716365	192.168.122.62	43.225.38.217	TCP	66	49188 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1283	2015-06-30 13:14:51.111412	43.225.38.217	192.168.122.62	TCP	54	443 → 49188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1284	2015-06-30 13:14:51.620631	192.168.122.62	43.225.38.217	TCP	66	[TCP Retransmission] 49188 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1285	2015-06-30 13:14:52.012913	43.225.38.217	192.168.122.62	TCP	54	443 → 49188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1286	2015-06-30 13:14:52.525314	192.168.122.62	43.225.38.217	TCP	62	[TCP Retransmission] 49188 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
1287	2015-06-30 13:14:52.591570	43.225.38.217	192.168.122.62	TCP	54	443 → 49188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1288	2015-06-30 13:15:22.930091	192.168.122.62	43.225.38.217	TCP	66	49188 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1289	2015-06-30 13:15:23.315772	43.225.38.217	192.168.122.62	TCP	54	443 → 49181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Search in results												
Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	Service	Duration	Payload Bytes Sent	Total Bytes Sent	Payload Bytes Received	Total t
2015-06-30 13:13:15.2	CWNUC20jUEEsTdN3b	192.168.122.62	49177	43.225.38.217	443	tcp	null	0.10	0	48	0	40
2015-06-30 13:13:46.2	CxkLlp3FbMMHN2QJQd	192.168.122.62	49178	43.225.38.217	443	tcp	null	0.20	0	52	0	40
2015-06-30 13:13:47.2	CVAlDQ2kkMnJ65wd2	192.168.122.62	49178	43.225.38.217	443	tcp	null	0.30	0	52	0	40
2015-06-30 13:13:48.2	C21jhEr8Y0TT6pg78	192.168.122.62	49178	43.225.38.217	443	tcp	null	0.30	0	48	0	40
2015-06-30 13:14:18.2	CfjLHP1lfJ4s9AkMj	192.168.122.62	49179	43.225.38.217	443	tcp	null	0.40	0	52	0	40
2015-06-30 13:14:19.2	CQslh24UhMcYUp1Tjd	192.168.122.62	49179	43.225.38.217	443	tcp	null	0.40	0	52	0	40
2015-06-30 13:14:20.2	CXpopX29JQlyXQ3B43	192.168.122.62	49179	43.225.38.217	443	tcp	null	0.30	0	48	0	40
2015-06-30 13:14:50.2	CUCxOsG2O1ldSAID8	192.168.122.62	49180	43.225.38.217	443	tcp	null	0.40	0	52	0	40
2015-06-30 13:14:51.2	CtgvUJ1jVhGkeeAvI	192.168.122.62	49180	43.225.38.217	443	tcp	null	0.30	0	52	0	40
2015-06-30 13:14:52.2	Ccu86e4PUcYOZl6EI	192.168.122.62	49180	43.225.38.217	443	tcp	null	0.20	0	48	0	40

Σ http://43.225.38.217/

1
/ 77

Community Score
ip

DETECTION
DETAILS
COMMUNITY

Forcepoint ThreatSeeker	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean
Anti-AVL	Clean	Artists Against 419	Clean



## For IP 111.121.193.242 virus total shows malicious and also listed in blacklist Ip

No.	Time	Source	Destination	Protocol	Length	Info
1294	2015-06-30 13:15:55.097179	192.168.122.62	111.121.193.242	TCP	66	49182 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1295	2015-06-30 13:15:55.454649	111.121.193.242	192.168.122.62	TCP	66	443 → 49182 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1369 SACK_PERM=1 WS=128
1296	2015-06-30 13:15:55.455112	192.168.122.62	111.121.193.242	TCP	68	49182 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1297	2015-06-30 13:15:56.830888	111.121.193.242	192.168.122.62	TCP	66	[TCP Retransmission] 443 → 49182 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1536 SACK_PERM=1
1298	2015-06-30 13:15:56.831472	192.168.122.62	111.121.193.242	TCP	66	[TCP Dup ACK 1296#1] 49182 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 SLE=0 SR=0
1299	2015-06-30 13:15:57.185829	111.121.193.242	192.168.122.62	SSL	254	Continuation Data
1300	2015-06-30 13:15:57.186605	192.168.122.62	111.121.193.242	SSL	195	Continuation Data
1301	2015-06-30 13:15:58.279407	192.168.122.62	111.121.193.242	TCP	195	[TCP Retransmission] 49182 → 443 [PSH, ACK] Seq=1 Ack=201 Win=65280 Len=141
1302	2015-06-30 13:15:58.641349	111.121.193.242	192.168.122.62	TCP	54	443 → 49182 [ACK] Seq=201 Ack=142 Win=15744 Len=0
1303	2015-06-30 13:15:58.642908	111.121.193.242	192.168.122.62	SSL	797	Continuation Data
1304	2015-06-30 13:15:58.642952	111.121.193.242	192.168.122.62	TCP	54	443 → 49182 [FIN, ACK] Seq=944 Ack=142 Win=15744 Len=0
1305	2015-06-30 13:15:58.643523	192.168.122.62	111.121.193.242	TCP	60	49182 → 443 [ACK] Seq=142 Ack=945 Win=64768 Len=0
1306	2015-06-30 13:15:58.644153	192.168.122.62	111.121.193.242	TCP	60	49182 → 443 [FIN, ACK] Seq=142 Ack=945 Win=64768 Len=0
1307	2015-06-30 13:15:59.010839	111.121.193.242	192.168.122.62	TCP	54	443 → 49182 [ACK] Seq=945 Ack=143 Win=15744 Len=0

Σ http://111.121.193.242/

3 / 72

Community Score

3 engines detected this URL

http://111.121.193.242/

111.121.193.242

ip

text/html; charset=UTF-8

Content Type

2020-01-16 23:27:19 UTC

6 months ago

DETECTION	DETAILS	COMMUNITY	
Comodo Valkyrie Verdict	① Malware	CRDF	① Malicious
Fortinet	① Malware	Forcepoint ThreatSeeker	② Spam
Spamhaus	② Spam	ADMINUSLabs	③ Clean
AegisLab WebGuard	④ Clean	AlienVault	④ Clean
Antiv-AVI	⑤ Clean	Avira (no cloud)	⑤ Clean

Check IP Address

### IP Address Information

Analysis Date	2020-08-03 00:21:06
Elapsed Time	1 seconds
Blacklist Status	BLACKLISTED 1/114
IP Address	<b>111.121.193.242</b> <a href="#">Find Sites</a>   <a href="#">IP Whois</a>
Reverse DNS	Unknown
ASN	AS4134
ASN Owner	Chinanet
ISP	China Telecom
Continent	Asia
Country Code	CN (CN) China
Latitude / Longitude	34.7725 / 113.7266 <a href="#">Google Map</a>
City	Unknown
Region	Unknown

### For IP 78.129.168.237

No.	Time	Source	Destination	Protocol	Length	Info
1314	2015-06-30 13:16:17.839748	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00>
1315	2015-06-30 13:16:19.339174	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00>
1316	2015-06-30 13:16:20.852737	192.168.122.62	78.129.168.237	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00>



http://78.129.168.237/



No engines detected this URL

http://78.129.168.237/  
78.129.168.237

2016-08-20 07:11:49 UTC  
4 years ago

	DETECTION	DETAILS	COMMUNITY
ADMINUSLabs	 Clean		AegisLab WebGuard  Clean
AlienVault	 Clean		Anty-AVL  Clean

## Whois

See <http://www.ripe.net/db/support/db-terms-conditions.txt>

Note: this output has been filtered.  
To receive output for a database update, use the "-B" flag.

Information related to '78.129.128.0 - 78.129.255.255'

Abuse contact for '78.129.128.0 - 78.129.255.255' is [abuse@rapidswitch.com](mailto:abuse@rapidswitch.com)

inetnum: 78.129.128.0 - 78.129.255.255  
netname: UK-RAPIDSWITCH-20070418  
country: GB  
org: ORG-RL20-RIPE  
admin-c: AR6363-RIPE  
tech-c: AR6363-RIPE  
status: ALLOCATED PA

For IP 37.55.107.202





The screenshot shows the NetworkMiner interface with the following details:

- Selected Node:** 37.55.107.202
- IP:** 37.55.107.202
- MAC:** 000000000000
- NIC Vendor:** XEROX CORPORATION
- MAC Age:** 2000-09-08
- Hostname:** Unknown
- OS:** Unknown
- TTL:** 116 (distance: 12)
- Open TCP Ports:** 6998

**TCP 6998 - Entropy (in \ out):** 92.19 \ 100.00 Typical data (in \ out): `µl]é(UAa@Vfý "%A=Húša \ =úb)éY!";@DobíleñéñéA±-ó5`

- Sent:** 436 packets (602,192 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Received:** 225 packets (9,425 Bytes), 0.00% cleartext (0 of 0 Bytes)

**Incoming sessions:** 1

- Server:** 37.55.107.202 TCP 6998
  - Server:** 37.55.107.202 TCP 6998 (582002 data bytes sent), Client: 192.168.122.62 (Windows) TCP 49183 (389 data bytes sent), Session start: 2015-06-30 13:16:28 UTC, Session end: 2015-06-30 13:17:45 UTC

**Outgoing sessions:** 0

For IP 192.254.234.118 (detailed screenshot provided in Q2 and 3 to avoid repetition)

For IP 208.113.214.190 (detailed screenshot provided in Q2 and 3 to avoid repetition)

 <http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135>   



① 5 engines detected this URL

<http://www.fernandatur.com/Scripts/hqnybx2w.php?id=960135>

www.fernandatur.com

404 Status

text/html; charset=iso-8859-1 Content Type

2019-05-09 00:55:33 UTC

1 year ago

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	① Malware		CyRadar ① Malicious
Dr.Web	① Malicious		Forcepoint ThreatSeeker ① Malicious
Sophos AV	① Malicious		ADMINUSLabs ✓ Clean
AegisLab WebGuard	✓ Clean		AlienVault ✓ Clean
Antiy-AVL	✓ Clean		BADWARE.INFO ✓ Clean
Baidu-International	✓ Clean		BitDefender ✓ Clean

For IP 46.30.45.65 ( detailed screenshot provided in Q2 and 3 to avoid repetition)

Analysis Date	2020-07-31 00:21:17
Elapsed Time	2 seconds
Blacklist Status	BLACKLISTED 1/114
IP Address	<a href="#">46.30.45.65</a> Find Sites   IP Whois
Reverse DNS	serv1.abitec.ru
ASN	AS210079
ASN Owner	EuroByte LLC
ISP	EuroByte LLC
Continent	Europe
Country Code	 (RU) Russia
Latitude / Longitude	55.7386 / 37.6068 <a href="#">Google Map</a>
City	Unknown



 [http://good.recycle2learn.com/?xniKfredLBvKDIU=i3SKIPrlJxZFGMSUb-nJDa9GPkXCRQLPh4SGnKXCJ-oSihi170IFxzsmTu2KV\\_OpgxveN0SZFT\\_zR3Aa](http://good.recycle2learn.com/?xniKfredLBvKDIU=i3SKIPrlJxZFGMSUb-nJDa9GPkXCRQLPh4SGnKXCJ-oSihi170IFxzsmTu2KV_OpgxveN0SZFT_zR3Aa)    

  
① 4 engines detected this URL.

[http://good.recycle2learn.com/?xniKfredLBvKDIU=i3SKIPrlJxZFGMSUb-nJDa9GPkXCRQLPh4SGnKXCJ-oSihi170IFxzsmTu2KV\\_OpgxveN0SZFT\\_zR3Aa](http://good.recycle2learn.com/?xniKfredLBvKDIU=i3SKIPrlJxZFGMSUb-nJDa9GPkXCRQLPh4SGnKXCJ-oSihi170IFxzsmTu2KV_OpgxveN0SZFT_zR3Aa) 2016-08-30 09:45:29 UTC  
3 years ago

DETECTION	DETAILS	COMMUNITY
Fortinet	<span style="color: red;">①</span> Malware	Kaspersky
Sophos AV	<span style="color: red;">①</span> Malicious	Websense ThreatSeeker
ADMINUSLab9	<span style="color: green;">✓</span> Clean	AegisLab WebGuard
AlienVault	<span style="color: green;">✓</span> Clean	Anti-AVL
Avira (no cloud)	<span style="color: green;">✓</span> Clean	Baidu-International
BitDefender	<span style="color: green;">✓</span> Clean	Blueliv
C-SIRT	<span style="color: green;">✓</span> Clean	Certy

 [cf76f50d725d971469cc54c953be243722bf4a853c12e4f95571e8a413eb489](http://good.recycle2learn.com/cf76f50d725d971469cc54c953be243722bf4a853c12e4f95571e8a413eb489)    

  
① 35 engines detected this file.

[cf76f50d725d971469cc54c953be243722bf4a853c12e4f95571e8a413eb489](http://good.recycle2learn.com/cf76f50d725d971469cc54c953be243722bf4a853c12e4f95571e8a413eb489) 15.39 KB 2020-06-08 10:48:24 UTC  
Size 1 month ago



DETECTION	DETAILS	COMMUNITY
Ad-Aware	<span style="color: red;">①</span> Script.SWF.Exploit.CVE-2015-3105.C500	AegisLab
AhnLab-V3	<span style="color: red;">①</span> SWF/Exploit	ALYac
Anti-AVL	<span style="color: red;">①</span> Trojan[Exploit]/SWF.SWF.Generic	Arcabit
Avast	<span style="color: red;">①</span> SWF-Malware-gen [Tr]	AVG
Avira (no cloud)	<span style="color: red;">①</span> EXP/Agent.EB.48	BitDefender
CAT-QuickHeal	<span style="color: red;">①</span> SWF.Kit.Nuclear.N	ClamAV
Comodo	<span style="color: red;">①</span> Malware@#2iqyxbw2czk	Cyren

For IP 23.10.250.18



```
23.10.250.18 [a1293.d.akamai.net] [fpdownload.macromedia.com.edgesuite.net]
IP: 23.10.250.18
MAC: Unknown
NIC Vendor: Unknown
Hostname: a1293.d.akamai.net, fpdownload.macromedia.com.edgesuite.net
OS: Unknown
TTL: Unknown
Open TCP Ports:
  ↳ Sent: 0 packets (0 Bytes), 0.00% cleartext (0 of 0 Bytes)
  ↲ Received: 0 packets (0 Bytes), 0.00% cleartext (0 of 0 Bytes)
  Incoming sessions: 0
  Outgoing sessions: 0
23.10.250.43 [a1293.d.akamai.net] [fpdownload.macromedia.com.edgesuite.net] [fpdownload2.macromedia.com]
IP: 23.10.250.43
MAC: 000000000000
NIC Vendor: XEROX CORPORATION
MAC Age: 9/8/2000
Hostname: a1293.d.akamai.net, fpdownload.macromedia.com.edgesuite.net, fpdownload2.macromedia.com
OS: Unknown
TTL: 58 (distance: 6)
Open TCP Ports: 80 (Http)
  ↳ Sent: 3 packets (652 Bytes), 0.00% cleartext (0 of 0 Bytes)
  ↲ Received: 5 packets (451 Bytes), 0.00% cleartext (0 of 0 Bytes)
  Incoming sessions: 1
    ↳ Server: 23.10.250.43 [a1293.d.akamai.net] [fpdownload.macromedia.com.edgesuite.net] [fpdownload2.macromedia.com] TCP 80
      ↳ Server: 23.10.250.43 [a1293.d.akamai.net] [fpdownload.macromedia.com.edgesuite.net] [fpdownload2.macromedia.com] TCP 80 (520 data bytes sent), Client: 192.168.122.62 (Windows) TCP 49176 (239 data bytes sent), Session start: 2015-06-30 13:12:52
    Outgoing sessions: 0
  Host Details
    Web Server Banner 1 : TCP 80 : Apache
```

Attacker uses IP address 23.10.250.43 the server ip address is 23.10.250.18 for web server banner in fact Mac spoofing and DNS hijacking.

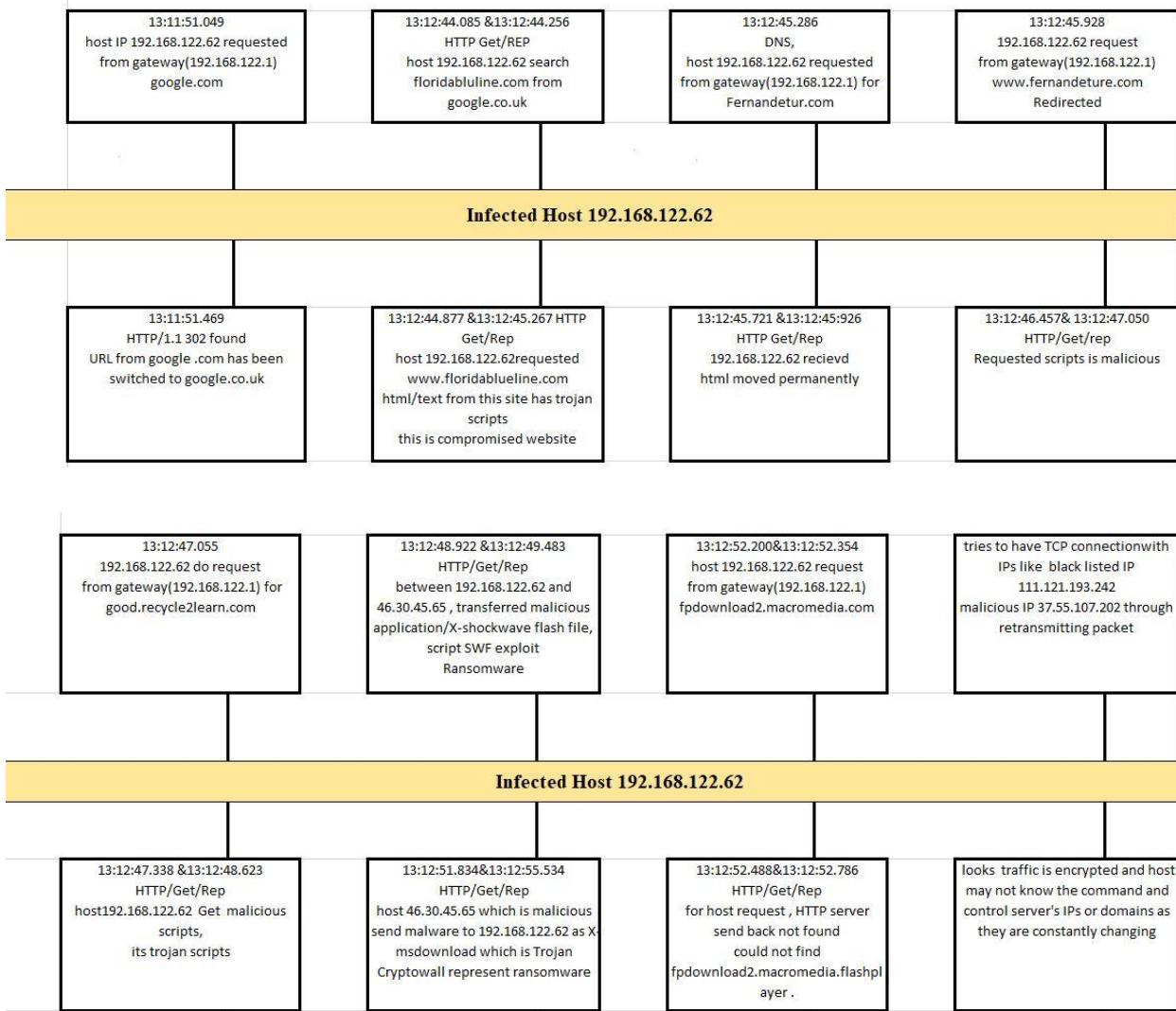
6. Give an outline of the attack scenario by describing it in a few paragraphs and by providing a graphical sketch. The attack scenario must include both the infection and post-infection steps

From the first point User in host IP 192.168.122.62 wants to access the web site “www.google.com”, so they type www.google.com in to their browser and after usual DNS resolution to find IP address for www.google.com, 216.58.208.46, a connection is initiated via TCP to the web server( SYN,SYN/ACK,ACK) ,in this process in packet 8 through HTTP1/1 “302 found” from google.com it switched to google.co.uk. From there user search for floridablueline.com, but we see in packet 524 through 527 when the host received text/html from floridablueline, this file recognized malicious with 27 engines by virustotal. So the infection process starts , and in this website another jpeg file which looks clean but as an interchange file back to the host . floridablueline is the compromised website.

From this point host 192.168.122.62 request access to fernandatur.com, however through transferring several packets we see in packet 553/575 HTTP server respond back with permanent moved, redirection occurred to www.fernandatur.com and that text/html file is script malware. By checking the script within GET request come up from 192.168.122.62 has trojan and script malware. From this point host forwarded to good.recycle2learn.com with IP 46.30.45.65 which is in blacklisted IP address, from packet 758 access requested and packet 764 HTTP when access requested, we have trojan scripts and based on analysis tools and virus total, we have ET CURRENT\_EVENTS RIG EK Landing and ET CURRENT\_EVENTS Cryptowall docs campaign that represent ransomware. Means the attacker uses script malware and tries to force the host to update and get it infected. We see the host through packet 811/831 received x-shockwave flash which was found by 35 engines in virus total malware, so from this point the attacker has complete control. And another Host IPs address after that which some of them are malicious like 43.225.38.217 and blacklisted like 111.121.193.242 and they have retransmitted continuos TCP connection with 192.168.122.62 and looks is in add-arp which instead of giving back domain name just give the host IPs. so look the traffic is encrypted and host may not know the command and control server's IPs or domains as they are constantly changing.In this



scenario may be attacker uses IP address 23.10.250.43 the server ip address is 23.10.250.18 for web server banner in fact Mac spoofing.



( based on the question body we provided answers on text and graph sketch. All screenshots related to attack scenarios shown in above questions to avoid repetition)



## 7. Discuss remediation and mitigation solutions for such threats.

Most ransomware occurred because of user-initiated actions such as clicking on malicious links or visiting a malicious or compromised website. In this threat user went to compromised website, floridablue, and then clicked on malicious links which redirect it to malicious website and got infected. Mitigating the risk of ransomware can be done by several methods like regularly scanning the system and network with antivirus program let automatically update the signature. And use whitelisting software which prevent unauthorised applications from executing.adding a warning banner to all emails which remind users about checking security of popups and attachments.

Try to keep all hardware, operating systems, software and applications patched and up to date to have fewer vulnerabilities.

And try to do regularly and automatically backup files, even though it will not stop malware but can make damage of that attack much less.

Another important action to avoid ransomware is training end users about phishing and be aware before visiting unknown websites and also close their browser when they do not use it and stop installing software or giving administrative privileges without knowing the source.

