PCAP Analysis Report

CryptoWall Ransomware (Angler EK)

(2015-07-24)

Investigation Using Zeek and Wireshark

Prepared by

Piyush K. Karn (252IS026)
Samyak Gedam (252IS032)

Email:

piyushkumar.252is026@nitk.edu.in
samyakgedam.252is032@nitk.edu.in

Department of Computer Science and Engineering (CSE)
National Institute of Technology Karnataka (NITK)
Surathkal, Mangalore-575025, India

Contents

1 Introduction

The report presents a detailed forensic analysis of a packet capture (PCAP) file, captured on July 24, 2015, following Snort alerts indicating a potential CryptoWall ransomware infection. CryptoWall is a notorious file-encrypting ransomware family that utilizes exploit kits for distribution and connects to Command and Control (C2) servers to manage encryption keys.

In this sample, we observed a Windows host visiting a legitimate website that had been compromised. The host was redirected to an exploit kit landing page, which delivered a malicious payload. The analysis of this malicious traffic is done using the Zeek Network Security Monitor and the Wireshark network analyzer tool. Our objective is to trace the key events in the traffic, identify the patient zero, and understand how the Angler Exploit Kit delivered the CryptoWall payload.

2 Objective

The objective is to reconstruct the complete infection lifecycle, beginning with benign user browsing activity and ending with the ransomware execution.

The key goals include:

- Identifying the infected host and its network behavior.
- Reconstructing the infection chain from initial access to exploit delivery.
- Detecting the exploit kit and understanding its mechanisms.
- Analyzing post-infection Command and Control (C2) activity.
- Extracting Indicators of Compromise (IOCs).
- Demonstrating how Zeek and Wireshark complement each other.

3 Scenario Overview

Snort alerts flagged suspicious outbound communication from internal host `192.168.137.85`, identifying potential CryptoWall activity. A PCAP file covering traffic from 14:56 to 15:04 UTC was collected, containing the entire infection sequence. A timestamp issue caused the date to appear as July 23, but it corresponds to July 24.

CryptoWall 3.0 was widespread in 2015 and often delivered through Angler Exploit Kit, known for exploiting Adobe Flash vulnerabilities.

The infection begins from a compromised legitimate website and progresses into a full ransomware deployment.

4 Infection Chain and Delivery Mechanism

The infection chain identified in this analysis does not rely on email phishing but rather a "Drive-by Download" mechanism utilizing a compromised legitimate website.

4.1 Compromised Landing Page

The victim initially visited a legitimate website,`www.twentyone-development.com`. This site had been compromised by attackers to host a malicious iframe or script redirection code.

4.2 Angler Exploit Kit Redirection

Upon visiting the compromised site, the victim's browser was silently redirected via an HTTP Referer chain to a malicious domain: `kiralyi.arcadiumentertainment.com`. This domain hosted the **Angler Exploit Kit**, a dominant exploit kit in 2015 known for targeting vulnerabilities in Adobe Flash Player and Microsoft Silverlight.

5 Methodology

The investigation used two complementary approaches:

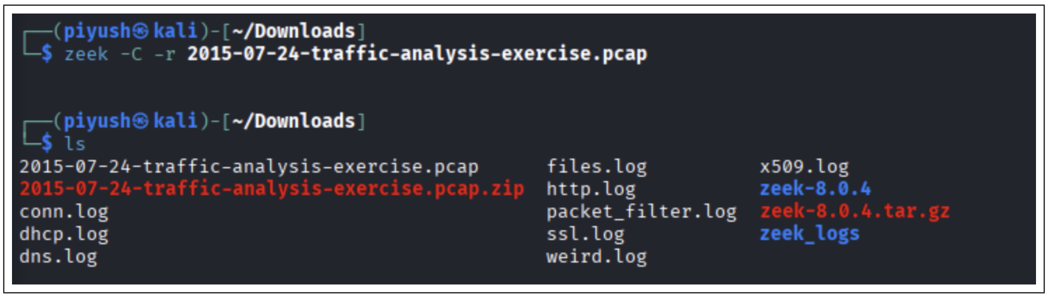
5.1 Zeek-Based Analysis

Zeek provided structured metadata through logs such as:

- `conn.log` – Connection metadata.
- `dns.log` – DNS queries and responses.
- `http.log` – Web requests and responses.
- `files.log` – File downloads and MIME types.

Zeek helped identify:

- Suspicious domain activity.
- HTTP redirection patterns.
- Malicious Flash exploit files.
- C2 connections.



```
┌──(piyush㉿kali)-[~/Downloads]
└─$ zeek -C -r 2015-07-24-traffic-analysis-exercise.pcap

┌──(piyush㉿kali)-[~/Downloads]
└─$ ls
2015-07-24-traffic-analysis-exercise.pcap      files.log          x509.log
2015-07-24-traffic-analysis-exercise.pcap.zip  http.log           zeek-8.0.4
conn.log                                       packet_filter.log  zeek-8.0.4.tar.gz
dhcp.log                                       ssl.log            zeek_logs
dns.log                                        weird.log
```

Figure 1: Zeek generated logs

5.2 Wireshark-Based Analysis

This section provides a comprehensive analysis of the malicious network activity captured in the file `2015-07-24-traffic-analysis-exercise.pcap`. Our goal is to identify the victim, reconstruct the attack, and confirm the payload.

Wireshark enabled packet-level inspection:

- Reconstructing malicious TCP streams.
- Extracting Flash exploit files.
- Recovering binary payloads.
- Visualizing ransom note retrieval.

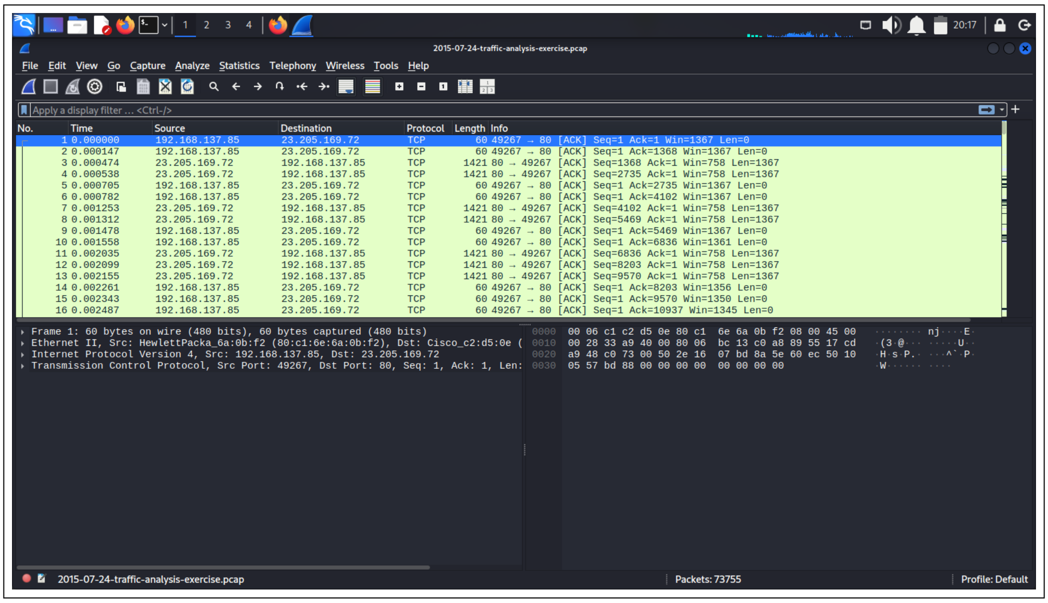
Together, Zeek and Wireshark provided full visibility of the attack chain.

5.3 Observed Protocols

The analysis revealed the following key protocols:

1. **HTTP:** Used for the initial browsing, the delivery of the exploit, and the downloading of the ransomware payload.
2. **DNS:** Heavy DNS traffic was observed as the malware attempted to resolve multiple C2 domains.

3. **TCP:** Facilitated the transport of the Flash exploit and the `application/octet-stream` payload.



2015-07-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
20:17

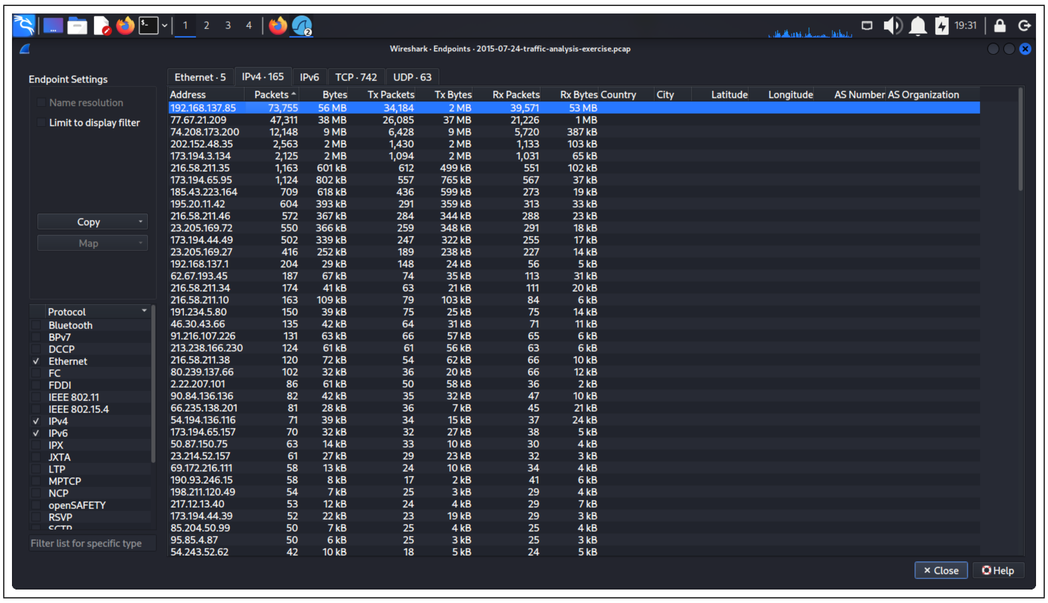
```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=1 Win=1367 Len=0
    2 0.000147   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=1368 Win=1367 Len=0
    3 0.000474   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=1368 Ack=1 Win=758 Len=1367
    4 0.000538   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=2735 Ack=1 Win=758 Len=1367
    5 0.000705   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=2735 Win=1367 Len=0
    6 0.000782   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=4102 Win=1367 Len=0
    7 0.001253   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=4102 Ack=1 Win=758 Len=1367
    8 0.001312   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=5469 Ack=1 Win=758 Len=1367
    9 0.001478   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=5469 Win=1367 Len=0
   10 0.001558   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=6836 Win=1361 Len=0
   11 0.002035   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=6836 Ack=1 Win=758 Len=1367
   12 0.002099   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=8203 Ack=1 Win=758 Len=1367
   13 0.002155   23.205.169.72    192.168.137.85   TCP      1421 80 → 49267 [ACK] Seq=9570 Ack=1 Win=758 Len=1367
   14 0.002261   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=8203 Win=1356 Len=0
   15 0.002343   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=9570 Win=1350 Len=0
   16 0.002487   192.168.137.85   23.205.169.72    TCP        60 49267 → 80 [ACK] Seq=1 Ack=10937 Win=1345 Len=0

› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
› Ethernet II, Src: HewlettPacka_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e (
› Internet Protocol Version 4, Src: 192.168.137.85, Dst: 23.205.169.72
› Transmission Control Protocol, Src Port: 49267, Dst Port: 80, Seq: 1, Ack: 1, Len:

0000  00 06 c1 c2 d5 0e 80 c1  6e 6a 0b f2 08 00 45 00   ········ nj····E·
0010  00 28 33 a9 40 00 80 06  bc 13 c0 a8 89 55 17 cd   ·(3·@··· ·····U··
0020  a9 48 c0 73 00 50 2e 16  07 bd 8a 5e 60 ec 50 10   ·H·s·P.· ···^`·P·
0030  05 57 bd 88 00 00 00 00  00 00 00 00               ·W······ ····

2015-07-24-traffic-analysis-exercise.pcap        Packets: 73755        Profile: Default
```

Figure 2: PCAP File Opening in Wireshark

6 Key Findings

6.1 Network Entities

- **Victim Host:** `192.168.137.85` (Hostname: `Leonardo-PC`). Identified as the top talker in the capture with over 900 connections.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
192.168.137.85	73,755	56 MB	34,184	2 MB	39,571	53 MB						
77.67.21.209	47,311	38 MB	26,085	37 MB	21,226	1 MB						
74.208.173.200	12,148	9 MB	6,428	9 MB	5,720	387 kB						
202.152.48.35	2,563	2 MB	1,430	2 MB	1,133	103 kB						
173.194.3.134	2,125	2 MB	1,094	2 MB	1,031	65 kB						
216.58.211.35	1,163	601 kB	612	499 kB	551	102 kB						
173.194.65.95	1,124	802 kB	557	765 kB	567	37 kB						
185.43.223.164	709	618 kB	436	599 kB	273	19 kB						
195.20.11.42	604	393 kB	291	359 kB	313	33 kB						
216.58.211.46	572	367 kB	284	344 kB	288	23 kB						
23.205.169.72	550	366 kB	259	348 kB	291	18 kB						
173.194.44.49	502	339 kB	247	322 kB	255	17 kB						
23.205.169.27	416	252 kB	189	238 kB	227	14 kB						
192.168.137.1	204	29 kB	148	24 kB	56	5 kB						
62.67.193.45	187	67 kB	74	35 kB	113	31 kB						
216.58.211.34	174	41 kB	63	21 kB	111	20 kB						
216.58.211.10	163	109 kB	79	103 kB	84	6 kB						
191.234.5.80	150	39 kB	75	25 kB	75	14 kB						
46.30.43.66	135	42 kB	64	31 kB	71	11 kB						
91.216.107.226	131	63 kB	66	57 kB	65	6 kB						
213.238.166.230	124	61 kB	61	56 kB	63	6 kB						
216.58.211.38	120	72 kB	54	62 kB	66	10 kB						
80.239.137.66	102	32 kB	36	20 kB	66	12 kB						
2.22.207.101	86	61 kB	50	58 kB	36	2 kB						
90.84.136.136	82	42 kB	35	32 kB	47	10 kB						
66.235.138.201	81	28 kB	36	7 kB	45	21 kB						
54.194.136.116	71	39 kB	34	15 kB	37	24 kB						
173.194.65.157	70	32 kB	32	27 kB	38	5 kB						
50.87.150.75	63	14 kB	33	10 kB	30	4 kB						
23.214.52.157	61	27 kB	29	23 kB	32	3 kB						
69.172.216.111	58	13 kB	24	10 kB	34	4 kB						
190.93.246.15	58	8 kB	17	2 kB	41	6 kB						
198.211.120.49	54	7 kB	25	3 kB	29	4 kB						
217.12.13.40	53	12 kB	24	4 kB	29	7 kB						
173.194.44.39	52	22 kB	23	19 kB	29	3 kB						
85.204.50.99	50	7 kB	25	4 kB	25	4 kB						
95.85.4.87	50	6 kB	25	3 kB	25	3 kB						
54.243.52.62	42	10 kB	18	5 kB	24	5 kB						

Figure 3: 192.168.137.85 identified as Top talker

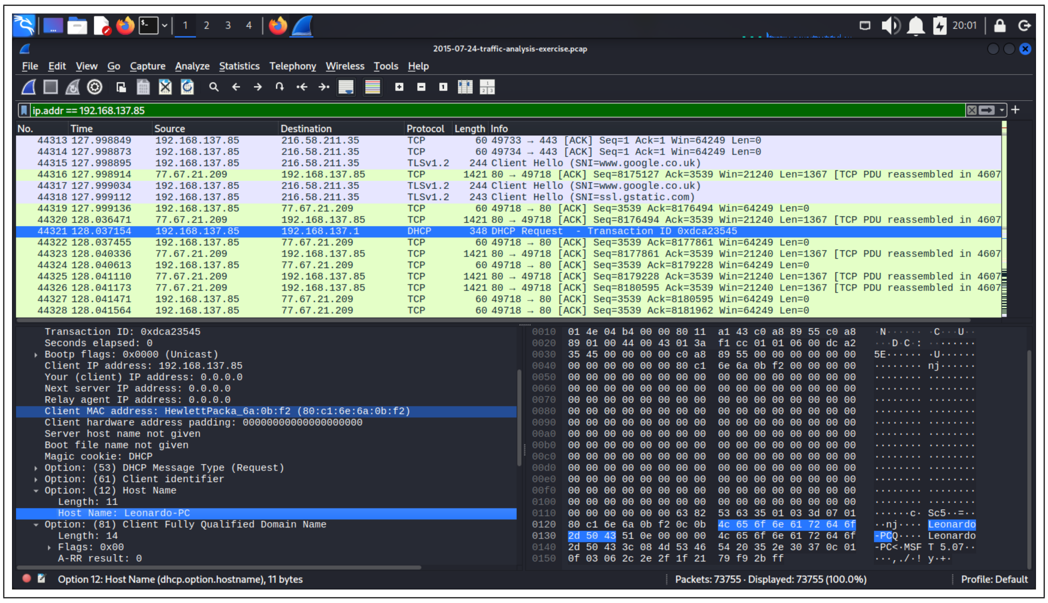
- **Exploit Kit Server:** `185.43.223.164` (Domain: `kiralyi.arcadiumentertainment.com`).
- **C2 Server:** `46.30.43.66` (Domain: `ministryordas.com`).

6.2 Victim Profiling

Using DHCP logs and HTTP User-Agent analysis, we profiled the victim machine:

- **OS:** Windows 7 (Windows NT 6.1)
- **Browser:** Internet Explorer 11 (Trident/7.0)
- **MAC Address:** `80:c1:6e:6a:0b:f2`

This configuration was highly susceptible to Flash-based exploits prevalent in 2015.


1 2 3 4
20:01
2015-07-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.137.85

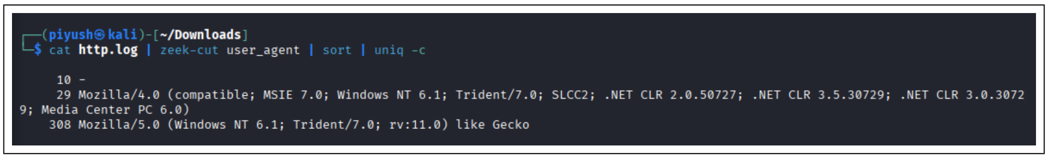
```
No.   Time        Source          Destination     Protocol Length Info
44313 127.998849  192.168.137.85  216.58.211.35   TCP        60 49733 → 443 [ACK] Seq=1 Ack=1 Win=64249 Len=0
44314 127.998873  192.168.137.85  216.58.211.35   TCP        60 49734 → 443 [ACK] Seq=1 Ack=1 Win=64249 Len=0
44315 127.998895  192.168.137.85  216.58.211.35   TLSv1.2   244 Client Hello (SNI=www.google.co.uk)
44316 127.998914  77.67.21.209    192.168.137.85  TCP      1421 80 → 49718 [ACK] Seq=8175127 Ack=3539 Win=21240 Len=1367 [TCP PDU reassembled in 4607
44317 127.999034  192.168.137.85  216.58.211.35   TLSv1.2   244 Client Hello (SNI=www.google.co.uk)
44318 127.999112  192.168.137.85  216.58.211.35   TLSv1.2   243 Client Hello (SNI=ssl.gstatic.com)
44319 127.999136  192.168.137.85  77.67.21.209    TCP        60 49718 → 80 [ACK] Seq=3539 Ack=8176494 Win=64249 Len=0
44320 128.036471  77.67.21.209    192.168.137.85  TCP      1421 80 → 49718 [ACK] Seq=8176494 Ack=3539 Win=21240 Len=1367 [TCP PDU reassembled in 4607
44321 128.037154  192.168.137.85  192.168.137.1   DHCP      348 DHCP Request  - Transaction ID 0xdca23545
44322 128.037455  192.168.137.85  77.67.21.209    TCP        60 49718 → 80 [ACK] Seq=3539 Ack=8177861 Win=64249 Len=0
44323 128.040336  77.67.21.209    192.168.137.85  TCP      1421 80 → 49718 [ACK] Seq=8177861 Ack=3539 Win=21240 Len=1367 [TCP PDU reassembled in 4607
44324 128.040613  192.168.137.85  77.67.21.209    TCP        60 49718 → 80 [ACK] Seq=3539 Ack=8179228 Win=64249 Len=0
44325 128.041110  77.67.21.209    192.168.137.85  TCP      1421 80 → 49718 [ACK] Seq=8179228 Ack=3539 Win=21240 Len=1367 [TCP PDU reassembled in 4607
44326 128.041173  77.67.21.209    192.168.137.85  TCP      1421 80 → 49718 [ACK] Seq=8180595 Ack=3539 Win=21240 Len=1367 [TCP PDU reassembled in 4607
44327 128.041471  192.168.137.85  77.67.21.209    TCP        60 49718 → 80 [ACK] Seq=3539 Ack=8180595 Win=64249 Len=0
44328 128.041564  192.168.137.85  77.67.21.209    TCP        60 49718 → 80 [ACK] Seq=3539 Ack=8181962 Win=64249 Len=0
```

```
    Transaction ID: 0xdca23545
    Seconds elapsed: 0
  › Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.137.85
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: HewlettPacka_6a:0b:f2 (80:c1:6e:6a:0b:f2)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (Request)
  › Option: (61) Client identifier
  ⌄ Option: (12) Host Name
      Length: 11
      Host Name: Leonardo-PC
  ⌄ Option: (81) Client Fully Qualified Domain Name
      Length: 14
    › Flags: 0x00
      A-RR result: 0
```

```
0010  01 4e 04 b4 00 00 80 11  a1 43 c0 a8 89 55 c0 a8   ·N······ ·C···U··
0020  89 01 00 44 00 43 01 3a  f1 cc 01 01 06 00 dc a2   ···D·C·: ········
0030  35 45 00 00 00 00 c0 a8  89 55 00 00 00 00 00 00   5E······ ·U······
0040  00 00 00 00 00 00 80 c1  6e 6a 0b f2 00 00 00 00   ········ nj······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  80 c1 6e 6a 0b f2 0c 0b  4c 65 6f 6e 61 72 64 6f   ··nj···· Leonardo
0130  2d 50 43 51 0e 00 00 00  4c 65 6f 6e 61 72 64 6f   -PCQ···· Leonardo
0140  2d 50 43 3c 08 4d 53 46  54 20 35 2e 30 37 0c 01   -PC<·MSF T 5.07··
0150  0f 03 06 2c 2e 2f 1f 21  79 f9 2b ff               ···,./·! y·+·
```

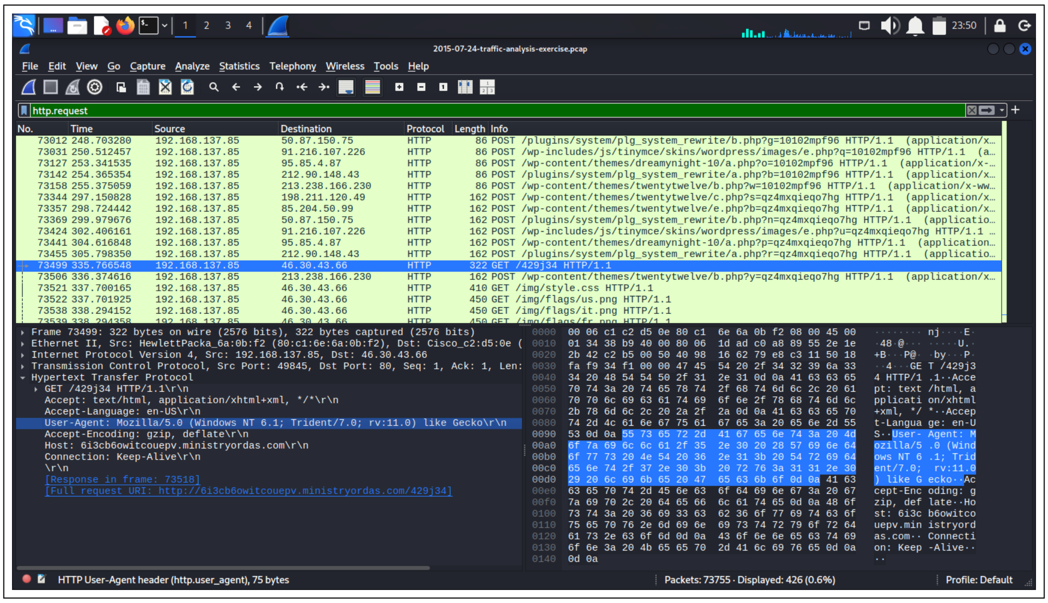
Option 12: Host Name (dhcp.option.hostname), 11 bytes | Packets: 73755 · Displayed: 73755 (100.0%) | Profile: Default

Figure 4: Finding Host Name and MAC address



```
┌──(piyush㉿kali)-[~/Downloads]
└─$ cat http.log | zeek-cut user_agent | sort | uniq -c

     10 -
     29 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.3072
9; Media Center PC 6.0)
    308 Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
```

Figure 5: Identifyting OS and Browser through Zeek


2015-07-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
23:50

```
http.request

No.   Time        Source          Destination     Protocol Length Info
73012 248.703280  192.168.137.85  50.87.150.75    HTTP      86 POST /plugins/system/plg_system_rewrite/b.php?g=10102mpf96 HTTP/1.1  (application/x…
73031 250.512457  192.168.137.85  91.216.107.226  HTTP      86 POST /wp-includes/js/tinymce/skins/wordpress/images/e.php?q=10102mpf96 HTTP/1.1  (a…
73127 253.341535  192.168.137.85  95.85.4.87      HTTP      86 POST /wp-content/themes/dreamynight-10/a.php?o=10102mpf96 HTTP/1.1  (application/x-…
73142 254.365354  192.168.137.85  212.90.148.43   HTTP      86 POST /plugins/system/plg_system_rewrite/a.php?b=10102mpf96 HTTP/1.1  (application/x…
73158 255.375059  192.168.137.85  213.238.166.230 HTTP      86 POST /wp-content/themes/twentytwelve/b.php?w=10102mpf96 HTTP/1.1  (application/x-ww…
73344 297.150828  192.168.137.85  198.211.120.49  HTTP     162 POST /wp-content/themes/twentytwelve/c.php?s=qz4mxqieqo7hg HTTP/1.1  (application/x…
73357 298.724442  192.168.137.85  85.204.50.99    HTTP     162 POST /wp-content/themes/twentytwelve/e.php?b=qz4mxqieqo7hg HTTP/1.1  (application/x…
73369 299.979676  192.168.137.85  50.87.150.75    HTTP     162 POST /plugins/system/plg_system_rewrite/b.php?n=qz4mxqieqo7hg HTTP/1.1  (applicatio…
73424 302.406161  192.168.137.85  91.216.107.226  HTTP     162 POST /wp-includes/js/tinymce/skins/wordpress/images/e.php?u=qz4mxqieqo7hg HTTP/1.1 …
73441 304.616848  192.168.137.85  95.85.4.87      HTTP     162 POST /wp-content/themes/dreamynight-10/a.php?p=qz4mxqieqo7hg HTTP/1.1  (application…
73455 305.798350  192.168.137.85  212.90.148.43   HTTP     162 POST /plugins/system/plg_system_rewrite/a.php?r=qz4mxqieqo7hg HTTP/1.1  (applicatio…
73499 335.766548  192.168.137.85  46.30.43.66     HTTP     322 GET /429j34 HTTP/1.1
73506 336.374616  192.168.137.85  213.238.166.230 HTTP     162 POST /wp-content/themes/twentytwelve/b.php?y=qz4mxqieqo7hg HTTP/1.1  (application/x…
73521 337.700165  192.168.137.85  46.30.43.66     HTTP     410 GET /img/style.css HTTP/1.1
73522 337.701925  192.168.137.85  46.30.43.66     HTTP     450 GET /img/flags/us.png HTTP/1.1
73538 338.294152  192.168.137.85  46.30.43.66     HTTP     450 GET /img/flags/it.png HTTP/1.1
73539 338.294358  192.168.137.85  46.30.43.66     HTTP     450 GET /img/flags/fr.png HTTP/1.1
```

```
› Frame 73499: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits)
› Ethernet II, Src: HewlettPacka_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e (
› Internet Protocol Version 4, Src: 192.168.137.85, Dst: 46.30.43.66
› Transmission Control Protocol, Src Port: 49845, Dst Port: 80, Seq: 1, Ack: 1, Len:
⌄ Hypertext Transfer Protocol
  › GET /429j34 HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: 6i3cb6owitcouepv.ministryordas.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Response in frame: 73518]
    [Full request URI: http://6i3cb6owitcouepv.ministryordas.com/429j34]
```

```
0000  00 06 c1 c2 d5 0e 80 c1  6e 6a 0b f2 08 00 45 00   ········ nj····E·
0010  01 34 38 b9 40 00 80 06  1d ad c0 a8 89 55 2e 1e   ·48·@··· ·····U.·
0020  2b 42 c2 b5 00 50 40 98  16 62 79 e8 c3 11 50 18   +B···P@· ·by···P·
0030  fa f9 34 f1 00 00 47 45  54 20 2f 34 32 39 6a 33   ··4···GE T /429j3
0040  34 20 48 54 54 50 2f 31  2e 31 0d 0a 41 63 63 65   4 HTTP/1 .1··Acce
0050  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 20 61   pt: text /html, a
0060  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
0070  2b 78 6d 6c 2c 20 2a 2f  2a 0d 0a 41 63 63 65 70   +xml, */ *··Accep
0080  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0090  53 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   S··User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00b0  6f 77 73 20 4e 54 20 36  2e 31 3b 20 54 72 69 64   ows NT 6 .1; Trid
00c0  65 6e 74 2f 37 2e 30 3b  20 72 76 3a 31 31 2e 30   ent/7.0;  rv:11.0
00d0  29 20 6c 69 6b 65 20 47  65 63 6b 6f 0d 0a 41 63   ) like G ecko··Ac
00e0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
00f0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 48 6f   zip, def late··Ho
0100  73 74 3a 20 36 69 33 63  62 36 6f 77 69 74 63 6f   st: 6i3c b6owitco
0110  75 65 70 76 2e 6d 69 6e  69 73 74 72 79 6f 72 64   uepv.min istryord
0120  61 73 2e 63 6f 6d 0d 0a  43 6f 6e 6e 65 63 74 69   as.com·· Connecti
0130  6f 6e 3a 20 4b 65 65 70  2d 41 6c 69 76 65 0d 0a   on: Keep -Alive··
0140  0d 0a                                              ··
```

```
HTTP User-Agent header (http.user_agent), 75 bytes        Packets: 73755 · Displayed: 426 (0.6%)        Profile: Default
```

Figure 6: Identifyting OS and Browser on Wireshark

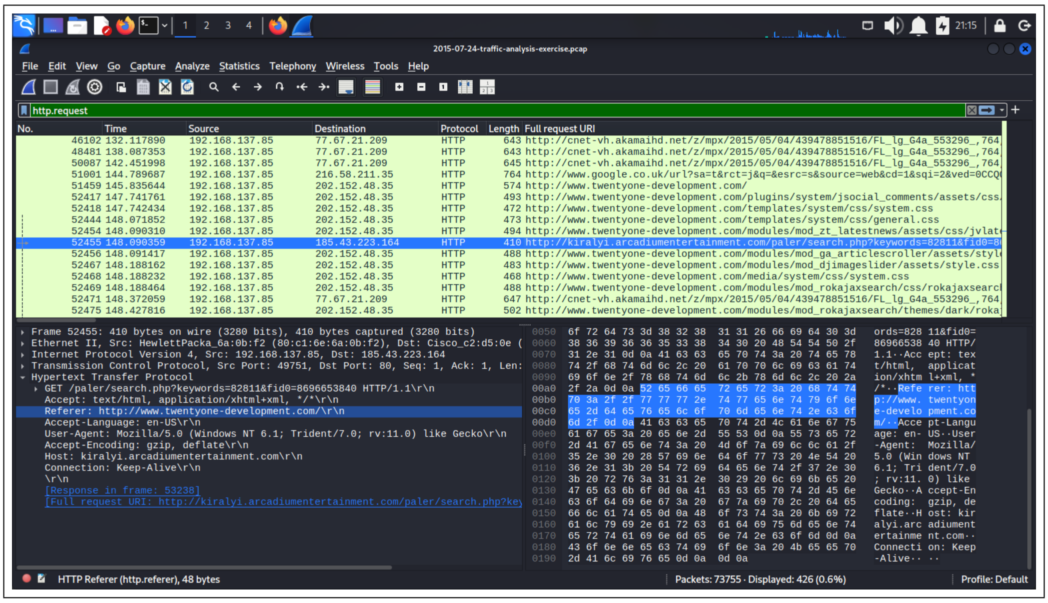
6.3 Infection Vector

The user visited:

- `www.twentyone-development.com` (compromised site)

which redirected to:

- `kiralyi.arcadiumentertainment.com` (Angler Exploit Kit)


2015-07-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
21:15

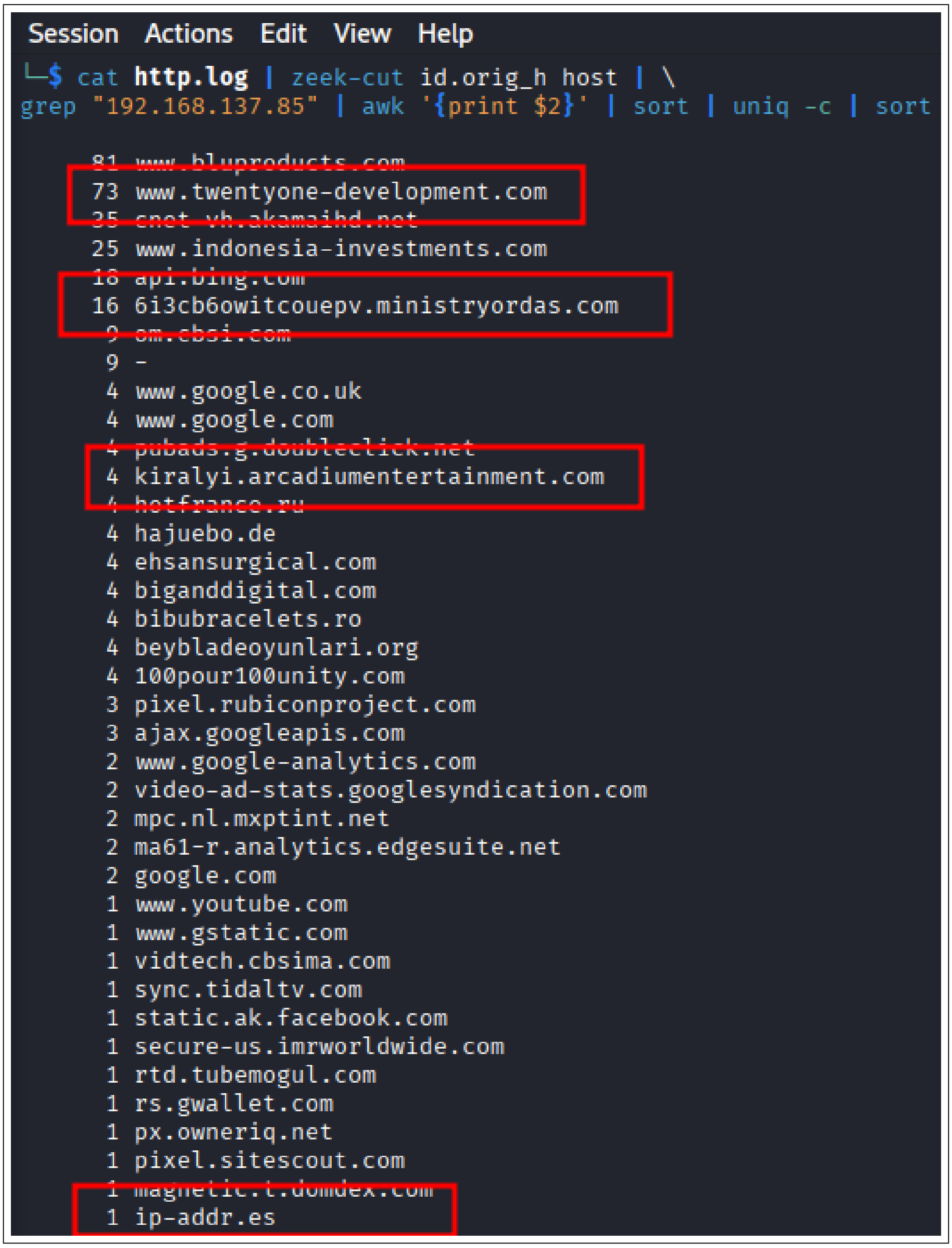
```
http.request

No.   Time        Source          Destination     Protocol Length Full request URI
46102 132.117890  192.168.137.85  77.67.21.209    HTTP     643 http://cnet-vh.akamaihd.net/z/mpx/2015/05/04/439478851516/FL_lg_G4a_553296_,764
48481 138.087353  192.168.137.85  77.67.21.209    HTTP     643 http://cnet-vh.akamaihd.net/z/mpx/2015/05/04/439478851516/FL_lg_G4a_553296_,764
50087 142.451998  192.168.137.85  77.67.21.209    HTTP     645 http://cnet-vh.akamaihd.net/z/mpx/2015/05/04/439478851516/FL_lg_G4a_553296_,764
51001 144.789687  192.168.137.85  216.58.211.35   HTTP     764 http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CCQ
51459 145.835644  192.168.137.85  202.152.48.35   HTTP     574 http://www.twentyone-development.com/
52417 147.741761  192.168.137.85  202.152.48.35   HTTP     493 http://www.twentyone-development.com/plugins/system/jsocial_comments/assets/css/
52418 147.742434  192.168.137.85  202.152.48.35   HTTP     472 http://www.twentyone-development.com/templates/system/css/system.css
52444 148.071852  192.168.137.85  202.152.48.35   HTTP     473 http://www.twentyone-development.com/templates/system/css/general.css
52454 148.090310  192.168.137.85  202.152.48.35   HTTP     494 http://www.twentyone-development.com/modules/mod_zt_latestnews/assets/css/jvlate
52455 148.090359  192.168.137.85  185.43.223.164  HTTP     410 http://kiralyi.arcadiumentertainment.com/paler/search.php?keywords=82811&fid0=8
52456 148.091417  192.168.137.85  202.152.48.35   HTTP     488 http://www.twentyone-development.com/modules/mod_ga_articlescroller/assets/style
52467 148.188162  192.168.137.85  202.152.48.35   HTTP     483 http://www.twentyone-development.com/modules/mod_djimageslider/assets/style.css
52468 148.188232  192.168.137.85  202.152.48.35   HTTP     468 http://www.twentyone-development.com/media/system/css/system.css
52469 148.188464  192.168.137.85  202.152.48.35   HTTP     488 http://www.twentyone-development.com/modules/mod_rokajaxsearch/css/rokajaxsearch
52471 148.372059  192.168.137.85  77.67.21.209    HTTP     647 http://cnet-vh.akamaihd.net/z/mpx/2015/05/04/439478851516/FL_lg_G4a_553296_,764
52475 148.427816  192.168.137.85  202.152.48.35   HTTP     502 http://www.twentyone-development.com/modules/mod_rokajaxsearch/themes/dark/roka
```

```
› Frame 52455: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits)
› Ethernet II, Src: HewlettPacka_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e (
› Internet Protocol Version 4, Src: 192.168.137.85, Dst: 185.43.223.164
› Transmission Control Protocol, Src Port: 49751, Dst Port: 80, Seq: 1, Ack: 1, Len:
⌄ Hypertext Transfer Protocol
  › GET /paler/search.php?keywords=82811&fid0=8696653840 HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, */*\r\n
    Referer: http://www.twentyone-development.com/\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: kiralyi.arcadiumentertainment.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Response in frame: 53238]
    [Full request URI: http://kiralyi.arcadiumentertainment.com/paler/search.php?key
```

```
0050  6f 72 64 73 3d 38 32 38  31 31 26 66 69 64 30 3d   ords=828 11&fid0=
0060  38 36 39 36 36 35 33 38  34 30 20 48 54 54 50 2f   86966538 40 HTTP/
0070  31 2e 31 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   1.1··Acc ept: tex
0080  74 2f 68 74 6d 6c 2c 20  61 70 70 6c 69 63 61 74   t/html,  applicat
0090  69 6f 6e 2f 78 68 74 6d  6c 2b 78 6d 6c 2c 20 2a   ion/xhtm l+xml, *
00a0  2f 2a 0d 0a 52 65 66 65  72 65 72 3a 20 68 74 74   /*··Refe rer: htt
00b0  70 3a 2f 2f 77 77 77 2e  74 77 65 6e 74 79 6f 6e   p://www. twentyon
00c0  65 2d 64 65 76 65 6c 6f  70 6d 65 6e 74 2e 63 6f   e-develo pment.co
00d0  6d 2f 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   m/··Acce pt-Langu
00e0  61 67 65 3a 20 65 6e 2d  55 53 0d 0a 55 73 65 72   age: en- US··User
00f0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0100  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
0110  36 2e 31 3b 20 54 72 69  64 65 6e 74 2f 37 2e 30   6.1; Tri dent/7.0
0120  3b 20 72 76 3a 31 31 2e  30 29 20 6c 69 6b 65 20   ; rv:11. 0) like
0130  47 65 63 6b 6f 0d 0a 41  63 63 65 70 74 2d 45 6e   Gecko··A ccept-En
0140  63 6f 64 69 6e 67 3a 20  67 7a 69 70 2c 20 64 65   coding:  gzip, de
0150  66 6c 61 74 65 0d 0a 48  6f 73 74 3a 20 6b 69 72   flate··H ost: kir
0160  61 6c 79 69 2e 61 72 63  61 64 69 75 6d 65 6e 74   alyi.arc adiument
0170  65 72 74 61 69 6e 6d 65  6e 74 2e 63 6f 6d 0d 0a   ertainme nt.com··
0180  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: Keep
0190  2d 41 6c 69 76 65 0d 0a  0d 0a                    -Alive·· ··
```

```
HTTP Referer (http.referer), 48 bytes        Packets: 73755 · Displayed: 426 (0.6%)        Profile: Default
```

Figure 7: Finding the Infection Vector



```
└─$ cat http.log | zeek-cut id.orig_h host | \
grep "192.168.137.85" | awk '{print $2}' | sort | uniq -c | sort

     81 www.bluproducts.com
     73 www.twentyone-development.com
     35 cnet.vh.akamaihd.net
     25 www.indonesia-investments.com
     18 api.bing.com
     16 6i3cb6owitcouepv.ministryordas.com
      9 om.cbsi.com
      9 -
      4 www.google.co.uk
      4 www.google.com
      4 pubads.g.doubleclick.net
      4 kiralyi.arcadiumentertainment.com
      4 hotfrance.ru
      4 hajuebo.de
      4 ehsansurgical.com
      4 biganddigital.com
      4 bibubracelets.ro
      4 beybladeoyunlari.org
      4 100pour100unity.com
      3 pixel.rubiconproject.com
      3 ajax.googleapis.com
      2 www.google-analytics.com
      2 video-ad-stats.googlesyndication.com
      2 mpc.nl.mxptint.net
      2 ma61-r.analytics.edgesuite.net
      2 google.com
      1 www.youtube.com
      1 www.gstatic.com
      1 vidtech.cbsima.com
      1 sync.tidaltv.com
      1 static.ak.facebook.com
      1 secure-us.imrworldwide.com
      1 rtd.tubemogul.com
      1 rs.gwallet.com
      1 px.owneriq.net
      1 pixel.sitescout.com
      1 magnetic.t.domdex.com
      1 ip-addr.es
```

Figure 8: Finding the Infection Vector on zeek

6.4 Exploit Delivery

Exploit: The server sent a file with Content-Type `application/x-shockwave-flash`. This confirms the Angler EK used a Flash vulnerability to breach the browser.

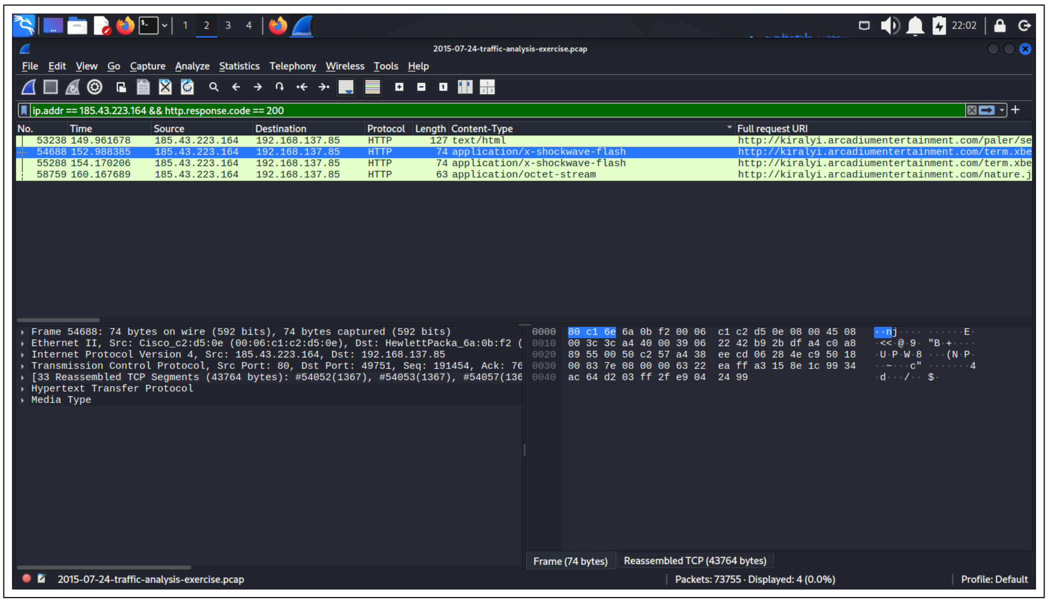
- fingerprinted the browser,
- identified vulnerable Flash Player,

- delivered malicious `.swf` files.

6.5 Payload Deployment

Payload: Immediately following the exploit, a file with Content-Type `application/octet-stream` was transferred. This encrypted binary is the CryptoWall 3.0 ransomware.
CryptoWall payload delivered as:

- MIME type: `application/octet-stream`,
- followed by immediate execution.


2015-07-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
22:02

```
ip.addr == 185.43.223.164 && http.response.code == 200
```

```
No.   Time       Source          Destination     Protocol Length Content-Type                     Full request URI
53238 149.961678 185.43.223.164  192.168.137.85  HTTP     127    text/html                        http://kiralyi.arcadiumentertainment.com/paler/se
54688 152.988385 185.43.223.164  192.168.137.85  HTTP     74     application/x-shockwave-flash    http://kiralyi.arcadiumentertainment.com/term.xbe
55288 154.170206 185.43.223.164  192.168.137.85  HTTP     74     application/x-shockwave-flash    http://kiralyi.arcadiumentertainment.com/term.xbe
58759 160.167689 185.43.223.164  192.168.137.85  HTTP     63     application/octet-stream         http://kiralyi.arcadiumentertainment.com/nature.j
```

```
Frame 54688: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Cisco_c2:d5:0e (00:06:c1:c2:d5:0e), Dst: HewlettPacka_6a:0b:f2 (
Internet Protocol Version 4, Src: 185.43.223.164, Dst: 192.168.137.85
Transmission Control Protocol, Src Port: 80, Dst Port: 49751, Seq: 191454, Ack: 76
[33 Reassembled TCP Segments (43764 bytes): #54052(1367), #54053(1367), #54057(136
Hypertext Transfer Protocol
Media Type
```

```
0000  80 c1 6e 6a 0b f2 00 06  c1 c2 d5 0e 08 00 45 08   ··nj···· ······E·
0010  00 3c 3c a4 40 00 39 06  22 42 b9 2b df a4 c0 a8   ·<<·@·9· "B·+····
0020  89 55 00 50 c2 57 a4 38  ee cd 06 28 4e c9 50 18   ·U·P·W·8 ···(N·P·
0030  00 83 7e 08 00 00 63 22  ea ff a3 15 8e 1c 99 34   ··~···c" ·······4
0040  ac 64 d2 03 ff 2f e9 04  24 99                     ·d···/·· $·
```

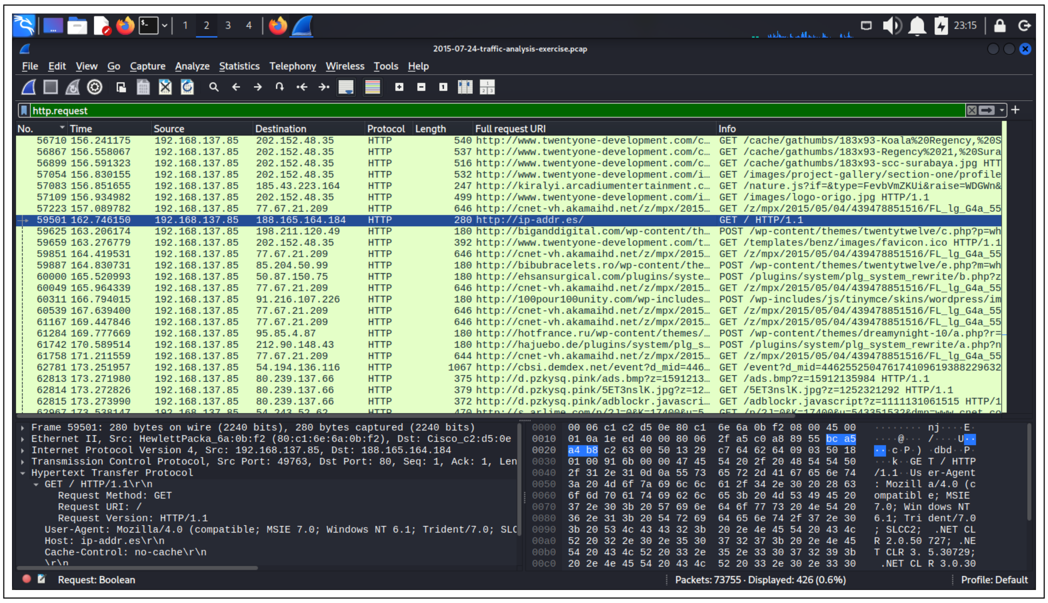
```
Frame (74 bytes)   Reassembled TCP (43764 bytes)
2015-07-24-traffic-analysis-exercise.pcap    Packets: 73755 · Displayed: 4 (0.0%)    Profile: Default
```

Figure 9: The Exploit & Payload

6.6 Post-Infection Behavior (C2)

Following the payload execution, the malware exhibited characteristic ”Phone Home” behavior:

- **IP Check:** A GET request to `ip-addr.es` was observed. This is a common technique for malware to identify the public IP of the infected machine.
  - C2 domains contacted:
    `ip-addr.es`



2015-07-24-traffic-analysis-exercise.pcap

```
http.request

No.   Time        Source          Destination     Protocol Length Full request URI                              Info
56710 156.241175  192.168.137.85  202.152.48.35   HTTP      540 http://www.twentyone-development.com/c…  GET /cache/gathumbs/183x93-Koala%20Regency,%20S
56867 156.558067  192.168.137.85  202.152.48.35   HTTP      537 http://www.twentyone-development.com/c…  GET /cache/gathumbs/183x93-Regency%2021,%20Sura
56899 156.591323  192.168.137.85  202.152.48.35   HTTP      516 http://www.twentyone-development.com/c…  GET /cache/gathumbs/183x93-scc-surabaya.jpg HTT
57054 156.830155  192.168.137.85  202.152.48.35   HTTP      532 http://www.twentyone-development.com/i…  GET /images/project-gallery/section-one/profile
57083 156.851655  192.168.137.85  185.43.223.164  HTTP      247 http://kiralyi.arcadiumentertainment.c…  GET /nature.js?if=&type=FevbVmZKUi&raise=WDGWn&
57109 156.934982  192.168.137.85  202.152.48.35   HTTP      499 http://www.twentyone-development.com/i…  GET /images/logo-origo.jpg HTTP/1.1
57223 157.089782  192.168.137.85  77.67.21.209    HTTP      646 http://cnet-vh.akamaihd.net/z/mpx/2015…  GET /z/mpx/2015/05/04/439478851516/FL_lg_G4a_55
59501 162.746150  192.168.137.85  188.165.164.184 HTTP      280 http://ip-addr.es/                       GET / HTTP/1.1
59625 163.206174  192.168.137.85  198.211.120.49  HTTP      180 http://biganddigital.com/wp-content/th…  POST /wp-content/themes/twentytwelve/c.php?p=wh
59659 163.276779  192.168.137.85  202.152.48.35   HTTP      392 http://www.twentyone-development.com/t…  GET /templates/benz/images/favicon.ico HTTP/1.1
59851 164.419531  192.168.137.85  77.67.21.209    HTTP      646 http://cnet-vh.akamaihd.net/z/mpx/2015…  GET /z/mpx/2015/05/04/439478851516/FL_lg_G4a_55
59887 164.830731  192.168.137.85  85.204.50.99    HTTP      180 http://bibubracelets.ro/wp-content/the…  POST /wp-content/themes/twentytwelve/e.php?m=wh
60000 165.520993  192.168.137.85  50.87.150.75    HTTP      180 http://ehsansurgical.com/plugins/syste…  POST /plugins/system/plg_system_rewrite/b.php?z
60049 165.964339  192.168.137.85  77.67.21.209    HTTP      646 http://cnet-vh.akamaihd.net/z/mpx/2015…  GET /z/mpx/2015/05/04/439478851516/FL_lg_G4a_55
60311 166.794015  192.168.137.85  91.216.107.226  HTTP      180 http://100pour100unity.com/wp-includes…  POST /wp-includes/js/tinymce/skins/wordpress/im
60539 167.639400  192.168.137.85  77.67.21.209    HTTP      646 http://cnet-vh.akamaihd.net/z/mpx/2015…  GET /z/mpx/2015/05/04/439478851516/FL_lg_G4a_55
61167 169.447846  192.168.137.85  77.67.21.209    HTTP      646 http://cnet-vh.akamaihd.net/z/mpx/2015…  GET /z/mpx/2015/05/04/439478851516/FL_lg_G4a_55
61284 169.777669  192.168.137.85  95.85.4.87      HTTP      180 http://hotfrance.ru/wp-content/themes/…  POST /wp-content/themes/dreamynight-10/a.php?r=
61742 170.589514  192.168.137.85  212.90.148.43   HTTP      180 http://hajuebo.de/plugins/system/plg_s…  POST /plugins/system/plg_system_rewrite/a.php?n
61758 171.211559  192.168.137.85  77.67.21.209    HTTP      644 http://cnet-vh.akamaihd.net/z/mpx/2015…  GET /z/mpx/2015/05/04/439478851516/FL_lg_G4a_55
62781 173.251957  192.168.137.85  54.194.136.116  HTTP     1067 http://cbsi.demdex.net/event?d_mid=446…  GET /event?d_mid=44625525047617410961938822963 2
62813 173.271980  192.168.137.85  80.239.137.66   HTTP      375 http://d.pzkysq.pink/ads.bmp?z=1591213…  GET /ads.bmp?z=15912135984 HTTP/1.1
62814 173.272826  192.168.137.85  80.239.137.66   HTTP      379 http://d.pzkysq.pink/5ET3nslK.jpg?z=12…  GET /5ET3nslK.jpg?z=1252321292 HTTP/1.1
62815 173.273990  192.168.137.85  80.239.137.66   HTTP      372 http://d.pzkysq.pink/adblockr.javascri…  GET /adblockr.javascript?z=1111131061515 HTTP/1
```

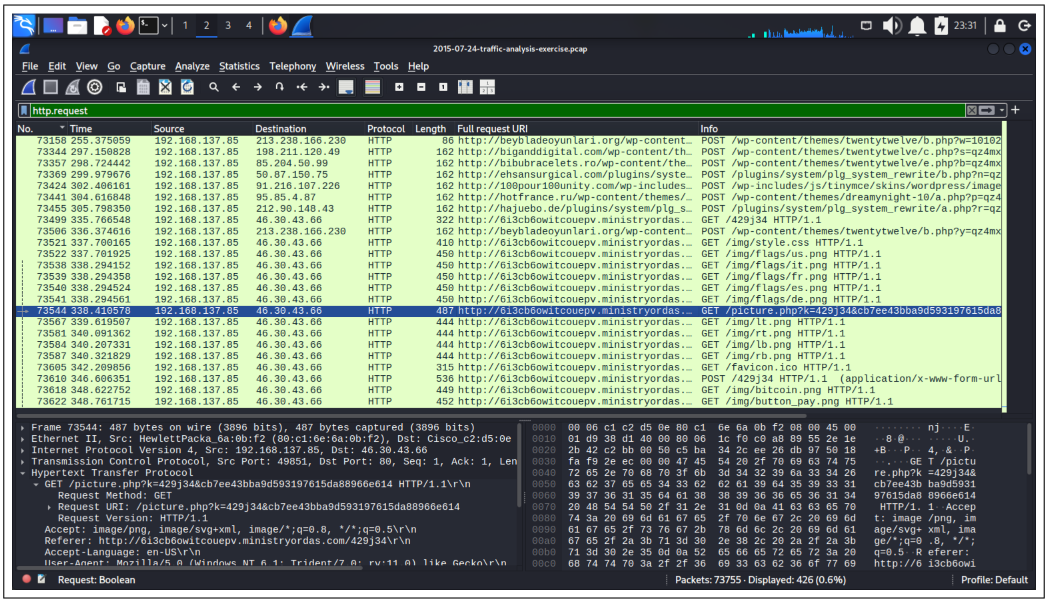
```
▸ Frame 59501: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits)
▸ Ethernet II, Src: HewlettPacka_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e
▸ Internet Protocol Version 4, Src: 192.168.137.85, Dst: 188.165.164.184
▸ Transmission Control Protocol, Src Port: 49763, Dst Port: 80, Seq: 1, Ack: 1, Len
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLC
    Host: ip-addr.es\r\n
    Cache-Control: no-cache\r\n
    \r\n
```

```
0000  00 06 c1 c2 d5 0e 80 c1  6e 6a 0b f2 08 00 45 00   ········ nj····E·
0010  01 0a 1e ed 40 00 80 06  2f a5 c0 a8 89 55 bc a5   ····@··· /····U··
0020  a4 b8 c2 63 00 50 13 29  c7 64 62 64 09 03 50 18   ···c·P·) ·dbd··P·
0030  01 00 91 6b 00 00 47 45  54 20 2f 20 48 54 54 50   ···k··GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0050  3a 20 4d 6f 7a 69 6c 6c  61 2f 34 2e 30 20 28 63   : Mozill a/4.0 (c
0060  6f 6d 70 61 74 69 62 6c  65 3b 20 4d 53 49 45 20   ompatibl e; MSIE 
0070  37 2e 30 3b 20 57 69 6e  64 6f 77 73 20 4e 54 20   7.0; Win dows NT 
0080  36 2e 31 3b 20 54 72 69  64 65 6e 74 2f 37 2e 30   6.1; Tri dent/7.0
0090  3b 20 53 4c 43 43 32 3b  20 2e 4e 45 54 20 43 4c   ; SLCC2;  .NET CL
00a0  52 20 32 2e 30 2e 35 30  37 32 37 3b 20 2e 4e 45   R 2.0.50 727; .NE
00b0  54 20 43 4c 52 20 33 2e  35 2e 33 30 37 32 39 3b   T CLR 3. 5.30729;
00c0  20 2e 4e 45 54 20 43 4c  52 20 33 2e 30 2e 33 30    .NET CL R 3.0.30
```

Request: Boolean | Packets: 73755 · Displayed: 426 (0.6%) | Profile: Default

Figure 10: The Ip Check

– 6i3cb6owitcouepv.ministryordas.com



2015-07-24-traffic-analysis-exercise.pcap

```
http.request

No.   Time        Source          Destination     Protocol Length Full request URI                              Info
73158 255.375059  192.168.137.85  213.238.166.230 HTTP       86 http://beybladeoyunlari.org/wp-content…  POST /wp-content/themes/twentytwelve/b.php?w=10102
73344 297.150828  192.168.137.85  198.211.120.49  HTTP      162 http://biganddigital.com/wp-content/th…  POST /wp-content/themes/twentytwelve/c.php?s=qz4mx
73357 298.724442  192.168.137.85  85.204.50.99    HTTP      162 http://bibubracelets.ro/wp-content/the…  POST /wp-content/themes/twentytwelve/e.php?b=qz4mx
73369 299.979676  192.168.137.85  50.87.150.75    HTTP      162 http://ehsansurgical.com/plugins/syste…  POST /plugins/system/plg_system_rewrite/b.php?n=qz
73424 302.406161  192.168.137.85  91.216.107.226  HTTP      162 http://100pour100unity.com/wp-includes…  POST /wp-includes/js/tinymce/skins/wordpress/image
73441 304.616848  192.168.137.85  95.85.4.87      HTTP      162 http://hotfrance.ru/wp-content/themes/…  POST /wp-content/themes/dreamynight-10/a.php?p=qz4
73455 305.798350  192.168.137.85  212.90.148.43   HTTP      162 http://hajuebo.de/plugins/system/plg_s…  POST /plugins/system/plg_system_rewrite/a.php?r=qz
73499 335.766548  192.168.137.85  46.30.43.66     HTTP      322 http://6i3cb6owitcouepv.ministryordas.…  GET /429j34 HTTP/1.1
73506 336.374616  192.168.137.85  213.238.166.230 HTTP      162 http://beybladeoyunlari.org/wp-content…  POST /wp-content/themes/twentytwelve/b.php?y=qz4mx
73521 337.700165  192.168.137.85  46.30.43.66     HTTP      410 http://6i3cb6owitcouepv.ministryordas.…  GET /img/style.css HTTP/1.1
73522 337.701925  192.168.137.85  46.30.43.66     HTTP      450 http://6i3cb6owitcouepv.ministryordas.…  GET /img/flags/us.png HTTP/1.1
73538 338.294152  192.168.137.85  46.30.43.66     HTTP      450 http://6i3cb6owitcouepv.ministryordas.…  GET /img/flags/it.png HTTP/1.1
73539 338.294358  192.168.137.85  46.30.43.66     HTTP      450 http://6i3cb6owitcouepv.ministryordas.…  GET /img/flags/fr.png HTTP/1.1
73540 338.294524  192.168.137.85  46.30.43.66     HTTP      450 http://6i3cb6owitcouepv.ministryordas.…  GET /img/flags/es.png HTTP/1.1
73541 338.294561  192.168.137.85  46.30.43.66     HTTP      450 http://6i3cb6owitcouepv.ministryordas.…  GET /img/flags/de.png HTTP/1.1
73544 338.410578  192.168.137.85  46.30.43.66     HTTP      487 http://6i3cb6owitcouepv.ministryordas.…  GET /picture.php?k=429j34&cb7ee43bba9d593197615da8
73567 339.619507  192.168.137.85  46.30.43.66     HTTP      444 http://6i3cb6owitcouepv.ministryordas.…  GET /img/lt.png HTTP/1.1
73581 340.091362  192.168.137.85  46.30.43.66     HTTP      444 http://6i3cb6owitcouepv.ministryordas.…  GET /img/rt.png HTTP/1.1
73584 340.207331  192.168.137.85  46.30.43.66     HTTP      444 http://6i3cb6owitcouepv.ministryordas.…  GET /img/lb.png HTTP/1.1
73587 340.321829  192.168.137.85  46.30.43.66     HTTP      444 http://6i3cb6owitcouepv.ministryordas.…  GET /img/rb.png HTTP/1.1
73605 342.209856  192.168.137.85  46.30.43.66     HTTP      315 http://6i3cb6owitcouepv.ministryordas.…  GET /favicon.ico HTTP/1.1
73610 346.606351  192.168.137.85  46.30.43.66     HTTP      536 http://6i3cb6owitcouepv.ministryordas.…  POST /429j34 HTTP/1.1  (application/x-www-form-url
73618 348.622752  192.168.137.85  46.30.43.66     HTTP      449 http://6i3cb6owitcouepv.ministryordas.…  GET /img/bitcoin.png HTTP/1.1
73622 348.761715  192.168.137.85  46.30.43.66     HTTP      452 http://6i3cb6owitcouepv.ministryordas.…  GET /img/button_pay.png HTTP/1.1
```

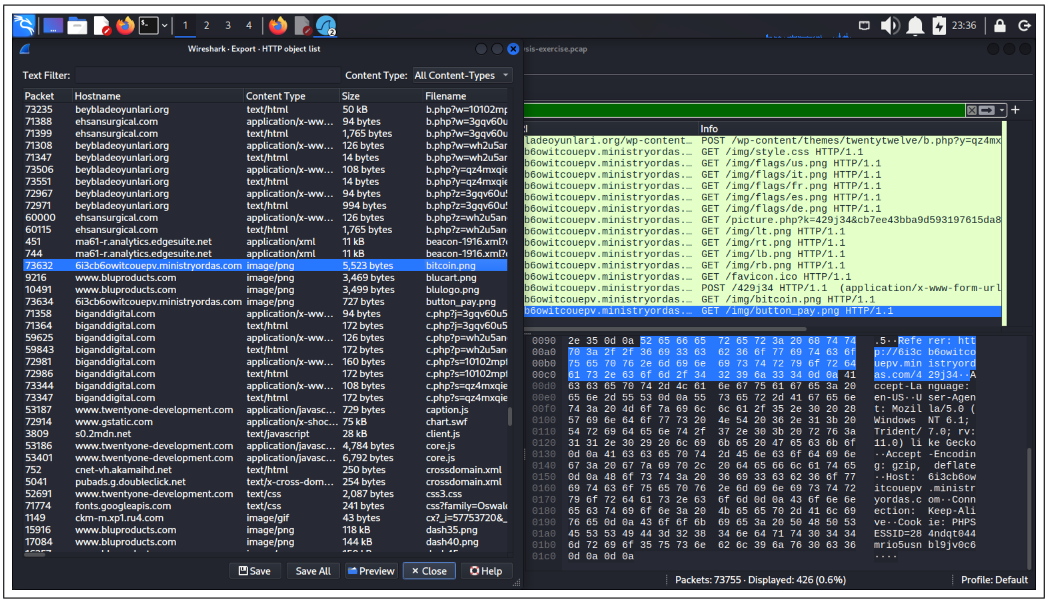
```
▸ Frame 73544: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits)
▸ Ethernet II, Src: HewlettPacka_6a:0b:f2 (80:c1:6e:6a:0b:f2), Dst: Cisco_c2:d5:0e
▸ Internet Protocol Version 4, Src: 192.168.137.85, Dst: 46.30.43.66
▸ Transmission Control Protocol, Src Port: 49851, Dst Port: 80, Seq: 1, Ack: 1, Len
▾ Hypertext Transfer Protocol
  ▾ GET /picture.php?k=429j34&cb7ee43bba9d593197615da88966e614 HTTP/1.1\r\n
      Request Method: GET
    ▸ Request URI: /picture.php?k=429j34&cb7ee43bba9d593197615da88966e614
      Request Version: HTTP/1.1
    Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5\r\n
    Referer: http://6i3cb6owitcouepv.ministryordas.com/429j34\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
```

```
0000  00 06 c1 c2 d5 0e 80 c1  6e 6a 0b f2 08 00 45 00   ········ nj····E·
0010  01 d9 38 d1 40 00 80 06  1c f0 c0 a8 89 55 2e 1e   ··8·@··· ·····U.·
0020  2b 42 c2 bb 00 50 c5 ba  34 2c ee 26 db 97 50 18   +B···P·· 4,·&··P·
0030  fa f9 2e ec 00 00 47 45  54 20 2f 70 69 63 74 75   ··.···GE T /pictu
0040  72 65 2e 70 68 70 3f 6b  3d 34 32 39 6a 33 34 26   re.php?k =429j34&
0050  63 62 37 65 65 34 33 62  62 61 39 64 35 39 33 31   cb7ee43b ba9d5931
0060  39 37 36 31 35 64 61 38  38 39 36 36 65 36 31 34   97615da8 8966e614
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 41 63 63 65 70    HTTP/1. 1··Accep
0080  74 3a 20 69 6d 61 67 65  2f 70 6e 67 2c 20 69 6d   t: image /png, im
0090  61 67 65 2f 73 76 67 2b  78 6d 6c 2c 20 69 6d 61   age/svg+ xml, ima
00a0  67 65 2f 2a 3b 71 3d 30  2e 38 2c 20 2a 2f 2a 3b   ge/*;q=0 .8, */*;
00b0  71 3d 30 2e 35 0d 0a 52  65 66 65 72 65 72 3a 20   q=0.5··R eferer: 
00c0  68 74 74 70 3a 2f 2f 36  69 33 63 62 36 6f 77 69   http://6 i3cb6owi
```

Request: Boolean | Packets: 73755 · Displayed: 426 (0.6%) | Profile: Default

Figure 11: The C2 Callback

- **Ransom Note Generation:** The infected host made HTTP GET requests to `ministryordas.com` to retrieve image assets, specifically `bitcoin.png` and `button_pay.png`.



Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
73235	beybladeoyunlari.org	text/html	50 kB	b.php?w=10102mp
71388	ehsansurgical.com	application/x-ww...	94 bytes	b.php?w=3gqv60u
71399	ehsansurgical.com	text/html	1,765 bytes	b.php?w=3gqv60u
71308	beybladeoyunlari.org	application/x-ww...	126 bytes	b.php?w=wh2u5ar
71347	beybladeoyunlari.org	text/html	14 bytes	b.php?w=wh2u5ar
73506	beybladeoyunlari.org	application/x-ww...	108 bytes	b.php?y=qz4mxqie
73551	beybladeoyunlari.org	text/html	14 bytes	b.php?y=qz4mxqie
72967	beybladeoyunlari.org	application/x-ww...	94 bytes	b.php?z=3gqv60u5
72971	beybladeoyunlari.org	text/html	994 bytes	b.php?z=3gqv60u5
60000	ehsansurgical.com	application/x-ww...	126 bytes	b.php?z=wh2u5an
60115	ehsansurgical.com	text/html	1,765 bytes	b.php?z=wh2u5an
451	ma61-r.analytics.edgesuite.net	application/xml	11 kB	beacon-1916.xml?
744	ma61-r.analytics.edgesuite.net	application/xml	11 kB	beacon-1916.xml?
73632	6i3cb6owitcouepv.ministryordas.com	image/png	5,523 bytes	bitcoin.png
9216	www.bluproducts.com	image/png	3,469 bytes	blucart.png
10491	www.bluproducts.com	image/png	3,499 bytes	blulogo.png
73634	6i3cb6owitcouepv.ministryordas.com	image/png	727 bytes	button_pay.png
71358	biganddigital.com	application/x-ww...	94 bytes	c.php?j=3gqv60u5
71364	biganddigital.com	text/html	172 bytes	c.php?j=3gqv60u5
59625	biganddigital.com	application/x-ww...	126 bytes	c.php?p=wh2u5an
59843	biganddigital.com	text/html	172 bytes	c.php?p=wh2u5an
72981	biganddigital.com	application/x-ww...	160 bytes	c.php?s=10102mpt
72986	biganddigital.com	text/html	172 bytes	c.php?s=10102mpt
73344	biganddigital.com	application/x-ww...	108 bytes	c.php?s=qz4mxqie
73347	biganddigital.com	text/html	172 bytes	c.php?s=qz4mxqie
53187	www.twentyone-development.com	application/javasc...	729 bytes	caption.js
72914	www.gstatic.com	application/x-shoc...	75 kB	chart.swf
3809	s0.2mdn.net	text/javascript	28 kB	client.js
53186	www.twentyone-development.com	application/javasc...	4,784 bytes	core.js
53401	www.twentyone-development.com	application/javasc...	6,792 bytes	core.js
752	cnet-vh.akamaihd.net	text/html	250 bytes	crossdomain.xml
5041	pubads.g.doubleclick.net	text/x-cross-dom...	254 bytes	crossdomain.xml
52691	www.twentyone-development.com	text/css	2,087 bytes	css3.css
71774	fonts.googleapis.com	text/css	241 bytes	css?family=Oswald
1149	ckm-m.xp1.ru4.com	image/gif	43 bytes	cx?_i=57753720&_
15916	www.bluproducts.com	image/png	118 kB	dash35.png
17084	www.bluproducts.com	image/png	144 kB	dash40.png

```
l                                          Info
ladeoyunlari.org/wp-content…  POST /wp-content/themes/twentytwelve/b.php?y=qz4mx
b6owitcouepv.ministryordas.…  GET /img/style.css HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/flags/us.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/flags/it.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/flags/fr.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/flags/es.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/flags/de.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /picture.php?k=429j34&cb7ee43bba9d593197615da8
b6owitcouepv.ministryordas.…  GET /img/lt.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/rt.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/lb.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/rb.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /favicon.ico HTTP/1.1
b6owitcouepv.ministryordas.…  POST /429j34 HTTP/1.1  (application/x-www-form-url
b6owitcouepv.ministryordas.…  GET /img/bitcoin.png HTTP/1.1
b6owitcouepv.ministryordas.…  GET /img/button_pay.png HTTP/1.1
```

```
0090  2e 35 0d 0a 52 65 66 65  72 65 72 3a 20 68 74 74   .5··Refe rer: htt
00a0  70 3a 2f 2f 36 69 33 63  62 36 6f 77 69 74 63 6f   p://6i3c b6owitco
00b0  75 65 70 76 2e 6d 69 6e  69 73 74 72 79 6f 72 64   uepv.min istryord
00c0  61 73 2e 63 6f 6d 2f 34  32 39 6a 33 34 0d 0a 41   as.com/4 29j34··A
00d0  63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20   ccept-La nguage: 
00e0  65 6e 2d 55 53 0d 0a 55  73 65 72 2d 41 67 65 6e   en-US··U ser-Agen
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0100  57 69 6e 64 6f 77 73 20  4e 54 20 36 2e 31 3b 20   Windows  NT 6.1; 
0110  54 72 69 64 65 6e 74 2f  37 2e 30 3b 20 72 76 3a   Trident/ 7.0; rv:
0120  31 31 2e 30 29 20 6c 69  6b 65 20 47 65 63 6b 6f   11.0) li ke Gecko
0130  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0140  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0150  0d 0a 48 6f 73 74 3a 20  36 69 33 63 62 36 6f 77   ··Host:  6i3cb6ow
0160  69 74 63 6f 75 65 70 76  2e 6d 69 6e 69 73 74 72   itcouepv .ministr
0170  79 6f 72 64 61 73 2e 63  6f 6d 0d 0a 43 6f 6e 6e   yordas.c om··Conn
0180  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
0190  76 65 0d 0a 43 6f 6f 6b  69 65 3a 20 50 48 50 53   ve··Cook ie: PHPS
01a0  45 53 53 49 44 3d 32 38  34 6e 64 71 74 30 34 34   ESSID=28 4ndqt044
01b0  6d 72 69 6f 35 75 73 6e  62 6c 39 6a 76 30 63 36   mrio5usn bl9jv0c6
01c0  0d 0a 0d 0a                                        ····
```

Packets: 73755 · Displayed: 426 (0.6%) Profile: Default

Figure 12: The Ransom Note Indicators

Downloaded assets:

- `bitcoin.png`, `button_pay.png`, `flags/us.png`

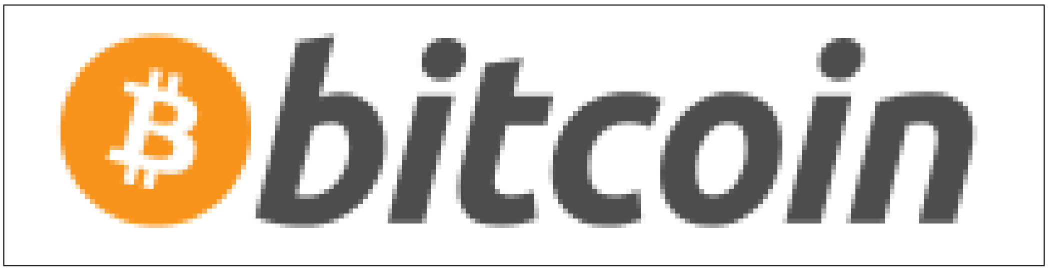


Figure 13: Recovered visual assets used in the ransomware payment portal

These confirm ransomware execution.

7 Indicators of Compromise (IOCs)

The following Indicators of Compromise were identified from the PCAP analysis, corresponding to the attacker infrastructure and compromised domains.

Network IOCs

- **Compromised Referrer:** `twentyone-development.com`
- **Exploit Kit Domain:** `kiralyi.arcadiumentertainment.com` (185.43.223.164)

- **Ransomware C2 Domain:** `6i3cb6owitcouepv.ministryordas.com` (`46.30.43.66`)
- **IP Check Domain:** `ip-addr.es` (`188.165.164.184`)

Table 1: Indicators of Compromise (IoCs)

Type	**Indicator**	**Description**
Domain	kiralyi.arcadiumentertainment.com	Angler EK landing page
IP Address	185.43.223.164	Exploit Kit server
Domain	ip-addr.es	C2 callback
Domain	6i3cb6owitcouepv.ministryordas.com	Ransom note delivery
Files	bitcoin.png, button_pay.png	Ransom note images

8 Attack Chain Reconstruction

1. User visits compromised website.
2. Hidden redirect triggers Angler Exploit Kit.
3. EK fingerprints system and selects Flash exploit.
4. Malicious Flash files delivered.
5. CryptoWall payload downloaded.
6. Malware executes and contacts C2 servers.
7. Ransom note components retrieved.

9 Protocol Analysis

9.1 Malicious Protocols

DNS – Domain lookups for EK and C2 servers. **HTTP** – Exploit delivery, payload transfer, ransom note retrieval.

9.2 Normal Background Protocols

- DHCP – IP configuration
- ARP – Local address resolution
- LLMNR / NetBIOS – Local network discovery
- SSL/TLS – Legitimate encrypted browsing

10 Conclusion

The PCAP analysis clearly indicates that the host **Leonardo-PC** was infected with **CryptoWall 3.0** via a drive-by download attack. The victim visited a compromised page which redirected them to the Angler Exploit Kit. The kit leveraged a Flash Player vulnerability to install the ransomware. Post-infection traffic confirmed the successful execution through C2 callbacks and the retrieval of ransom note graphical assets.

The infection chain confirms:

- Angler Exploit Kit successfully exploited a Flash vulnerability.
- CryptoWall ransomware executed on the victim host.
- C2 communications and ransom page assets were retrieved.

Zeek provided high-level insights while Wireshark validated payloads and malicious resources. Together, they allowed complete reconstruction of the attack.

Appendix A: Zeek Commands Used

`Command`	**Purpose**
`zeek -C -r 2015-07-24-traffic-analysis-exercise.pcap`	Run Zeek on the PCAP to generate all logs.
`cat dns.log | zeek-cut ts id.orig_h query answers`	Extract DNS queries and responses.
`cat http.log | zeek-cut ts id.orig_h host uri`	List all HTTP requests with full URLs.
`grep -Ei "swf|js" http.log`	Identify exploit files and suspicious JavaScript.
`grep -E "bitcoin|flags" http.log`	Detect ransom note retrieval.

Appendix B: Wireshark Filters Used

Filter	**Purpose**
`http && ip.addr == 192.168.137.85`	All HTTP traffic of victim host.
`dns && ip.addr == 192.168.137.85`	DNS queries from victim.
`ip.addr == 185.43.223.164`	Traffic to exploit kit server.
`frame contains "bitcoin.png"`	Identify ransom note images.