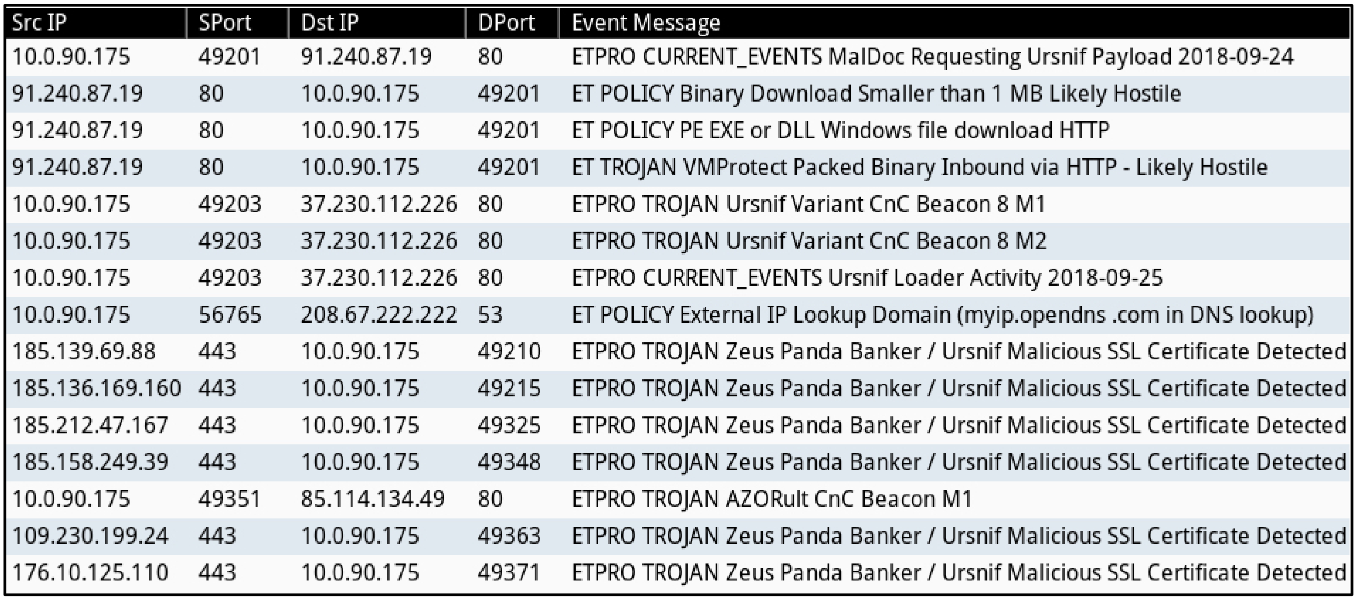
APRIL 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to exercise: https://www.malware-traffic-analysis.net/2019/04/15/index.html

Links to some tutorials I've written that should help with this exercise:

- Customizing Wireshark – Changing Your Column Display
- Using Wireshark: Identifying Hosts and Users
- Using Wireshark – Display Filter Expressions



Src IP	SPort	Dst IP	DPort	Event Message
10.0.90.175	49201	91.240.87.19	80	ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24
91.240.87.19	80	10.0.90.175	49201	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
91.240.87.19	80	10.0.90.175	49201	ET POLICY PE EXE or DLL Windows file download HTTP
91.240.87.19	80	10.0.90.175	49201	ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
10.0.90.175	49203	37.230.112.226	80	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1
10.0.90.175	49203	37.230.112.226	80	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M2
10.0.90.175	49203	37.230.112.226	80	ETPRO CURRENT_EVENTS Ursnif Loader Activity 2018-09-25
10.0.90.175	56765	208.67.222.222	53	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
185.139.69.88	443	10.0.90.175	49210	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
185.136.169.160	443	10.0.90.175	49215	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
185.212.47.167	443	10.0.90.175	49325	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
185.158.249.39	443	10.0.90.175	49348	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
10.0.90.175	49351	85.114.134.49	80	ETPRO TROJAN AZORult CnC Beacon M1
109.230.199.24	443	10.0.90.175	49363	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
176.10.125.110	443	10.0.90.175	49371	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected

Shown above: Alerts on the traffic from this exercise.

Executive summary:

On Monday 2019-04-15 at 16:42 UTC, a Windows host used by Kim Jooyoung was infected with Ursnif. By 21:24 UTC, the same Windows host was also infected with AZORult malware.

Details of the infected Windows host:

- IP address: ***10.0.90.175***
- MAC address: ***d0:67:e5:b1:53:fa***
- Host name: ***SEOUL-4A67-PC***
- Windows user account name: ***kim.jooyoung***

Indicators of Compromise:

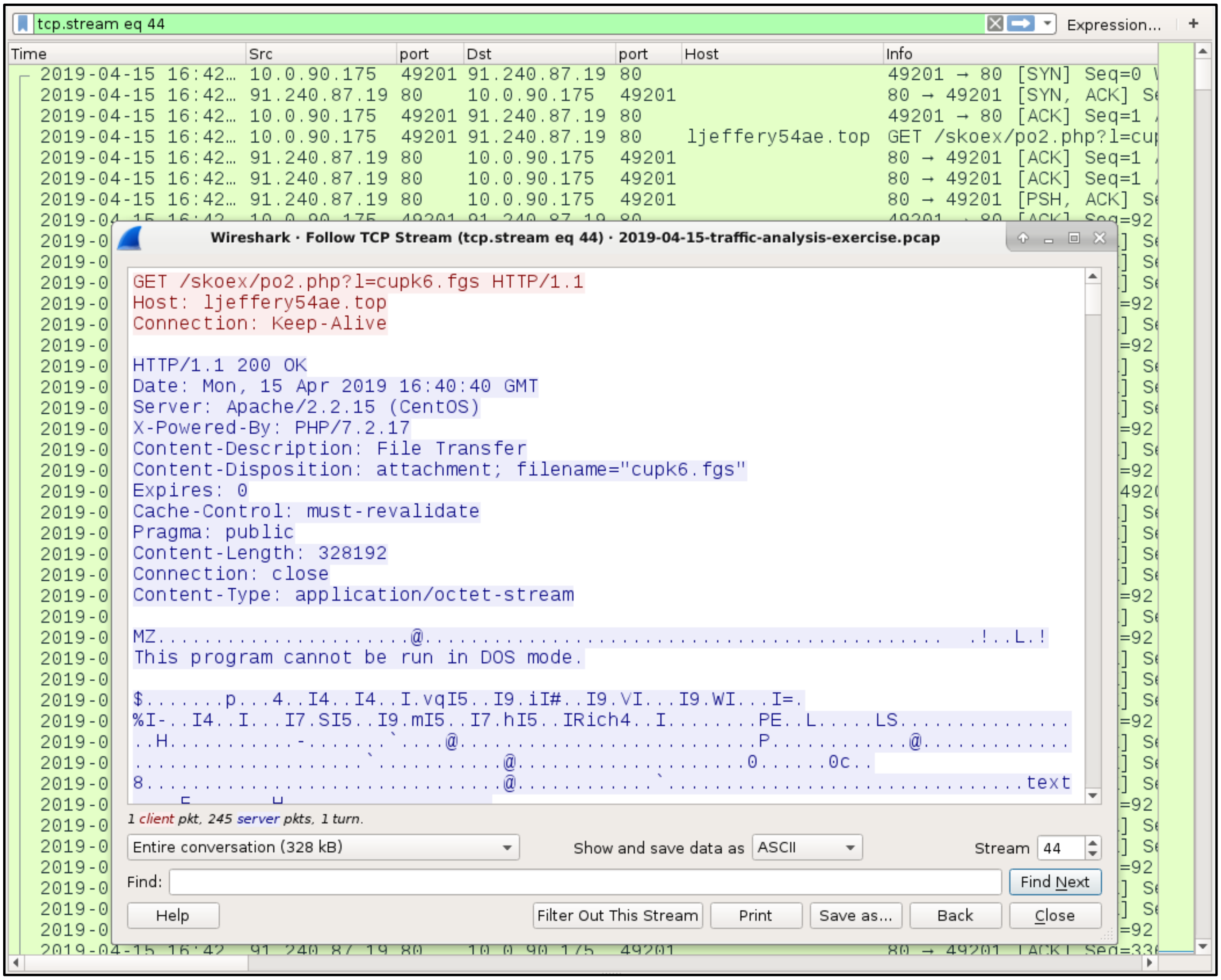
- 91.240.87.19 port 80 - ***ljeffery54ae.top*** - GET /skoex/po2.php?l=cupk6.fgs

- 37.230.112.226 port 80 - ***ksoniay95ee.info*** - GET /images*/[long string of characters]*.avi
- 185.139.69.88 port 443 - ***zindv.club*** - HTTPS/SSL/TLR traffic
- 151.106.27.208 port 80 - ***151.106.27.208*** - GET /client.rar
- 185.136.169.160 port 443 - HTTPS/SSL/TLS traffic
- 185.212.47.167 port 443 - HTTPS/SSL/TLS traffic
- 89.163.144.224 port 80 - ***89.163.144.224*** - GET /klansfuuerifneiferunfasd/modules/client.rar
- 185.158.249.39 port 443 - ***adsfinder.xyz*** - HTTPS/SSL/TLR traffic
- 162.213.250.131 port 80 - ***162.213.250.131*** - GET /azor.rar
- 85.114.134.49 port 80 - ***85.114.134.49*** - POST /index.php
- 198.54.125.57 port 443 - HTTPS/SSL/TLS traffic
- 109.230.199.24 port 443 - ***qqtube.club*** - HTTPS/SSL/TLS traffic
- 198.54.115.33 port 443 - HTTPS/SSL/TLS traffic
- 176.10.125.110 port 443 - ***parolinos.xyz*** - HTTPS/SSL/TLS traffic
- 68.65.122.52 port 443 - HTTPS/SSL/TLS traffic

- DNS query for resolver1.opendns.com
- 208.67.222.222 UDP port 53 - DNS PTR query for 222.222.67.208.in-addr.arpa
- 208.67.222.222 UDP port 53 - DNS query for myip.opendns.com
- 208.91.197.91 port 443 - ***pompeiiii.org*** - attempted TCP connections

Ursnif EXE returned from ***ljeffery54ae.top*** - GET /skoex/po2.php?l=cupk6.fgs

- SHA256 hash: 50007a82f044a695ec9c1cfcc7a495211061112ea6a927710ebd3e6c4409e3a2
- File size: 328,192 bytes
- File location: hxxp://ljeffery54ae[.]top/skoex/po2.php?l=cupk6.fgs
- VirusTotal: https://www.virustotal.com/#/file/50007a82f044a695ec9c1cfcc7a495211061112ea6a927710ebd3e6c4409e3a2
- Any.Run analysis: https://app.any.run/tasks/68f334a8-a040-4472-8f10-0a4b467418c3
- CAPE sandbox: https://cape.contextis.com/analysis/67330/
- Reverse.it: https://www.reverse.it/sample/50007a82f044a695ec9c1cfcc7a495211061112ea6a927710ebd3e6c4409e3a2



```
tcp.stream eq 44

Time                 Src           port  Dst           port  Host               Info
2019-04-15 16:42…    10.0.90.175   49201 91.240.87.19  80                       49201 → 80 [SYN] Seq=0
2019-04-15 16:42…    91.240.87.19  80    10.0.90.175   49201                    80 → 49201 [SYN, ACK] Se
2019-04-15 16:42…    10.0.90.175   49201 91.240.87.19  80                       49201 → 80 [ACK] Seq=1
2019-04-15 16:42…    10.0.90.175   49201 91.240.87.19  80    ljeffery54ae.top   GET /skoex/po2.php?l=cup
2019-04-15 16:42…    91.240.87.19  80    10.0.90.175   49201                    80 → 49201 [ACK] Seq=1
2019-04-15 16:42…    91.240.87.19  80    10.0.90.175   49201                    80 → 49201 [ACK] Seq=1
2019-04-15 16:42…    91.240.87.19  80    10.0.90.175   49201                    80 → 49201 [PSH, ACK] Se
```

Wireshark · Follow TCP Stream (tcp.stream eq 44) · 2019-04-15-traffic-analysis-exercise.pcap

```
GET /skoex/po2.php?l=cupk6.fgs HTTP/1.1
Host: ljeffery54ae.top
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 15 Apr 2019 16:40:40 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/7.2.17
Content-Description: File Transfer
Content-Disposition: attachment; filename="cupk6.fgs"
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 328192
Connection: close
Content-Type: application/octet-stream

MZ......................@.........................................  .!..L.!
This program cannot be run in DOS mode.

$.......p...4..I4..I4..I.vqI5..I9.iI#..I9.VI...I9.WI...I=.
%I-..I4..I...I7.SI5..I9.mI5..I7.hI5..IRich4..I........PE..L.....LS...............
..H...........-.......`....@.........................P...........@.............
....................`..........@..................0......0c..
8..............................@...........`...............................text
```

1 client pkt, 245 server pkts, 1 turn.

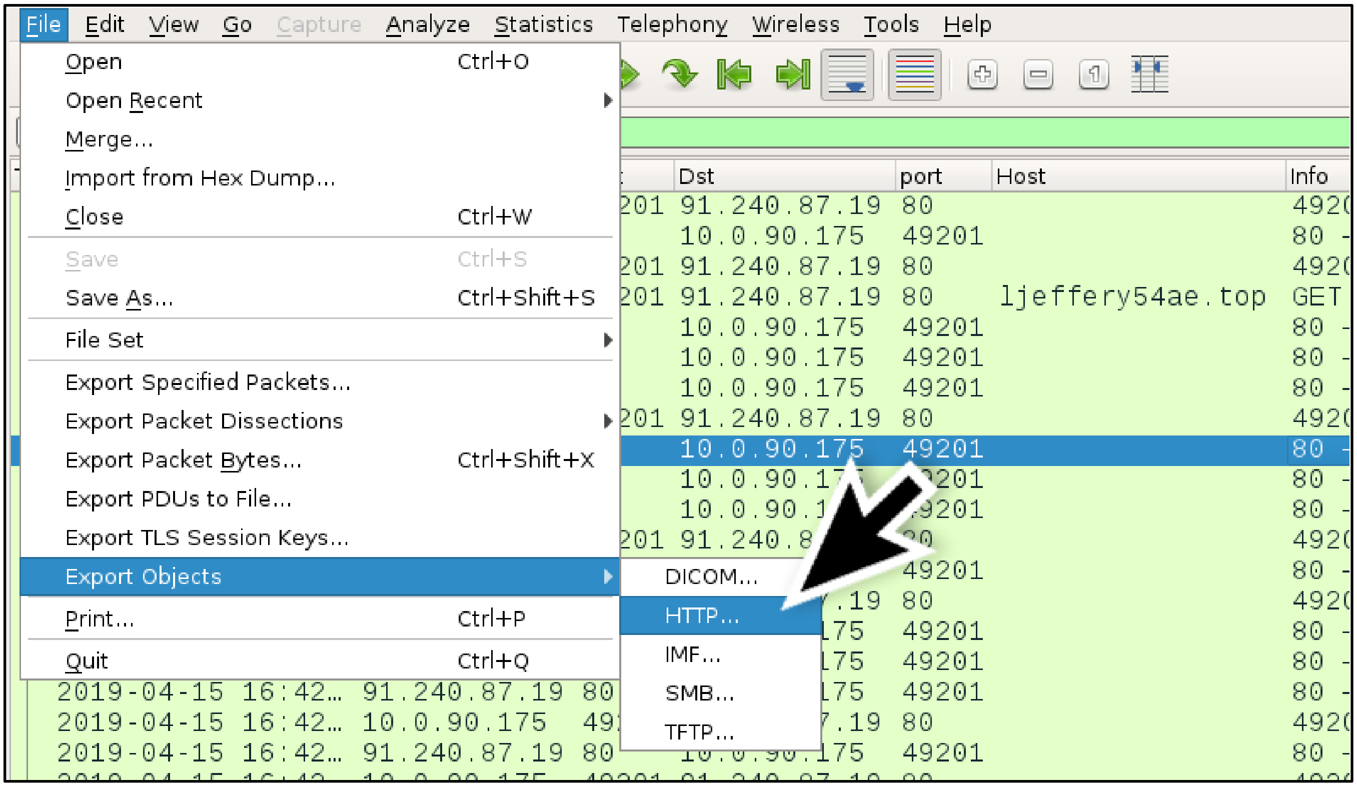
Entire conversation (328 kB)

Show and save data as ASCII

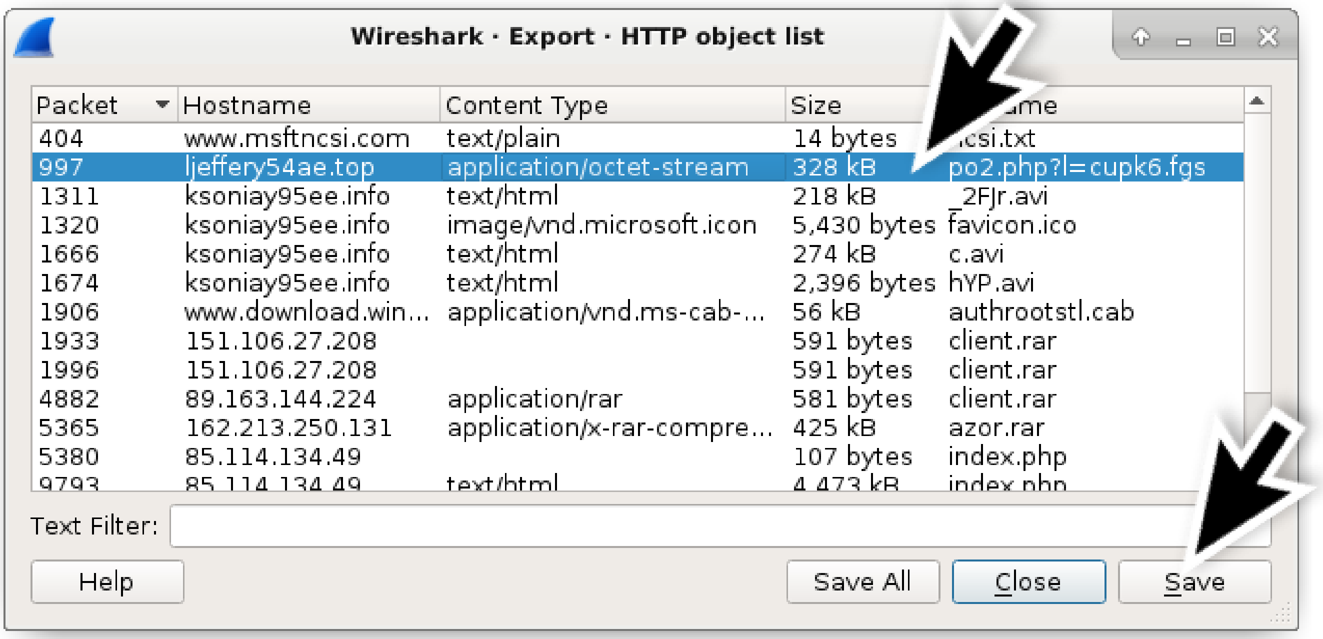
Stream 44

Shown above: The only executable we can extract from the pcap.

APRIL 2019 TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: Using the export HTTP Objects menu to get that executable.



Packet	Hostname	Content Type	Size	Filename
404	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
997	ljeffery54ae.top	application/octet-stream	328 kB	po2.php?l=cupk6.fgs
1311	ksoniay95ee.info	text/html	218 kB	_2FJr.avi
1320	ksoniay95ee.info	image/vnd.microsoft.icon	5,430 bytes	favicon.ico
1666	ksoniay95ee.info	text/html	274 kB	c.avi
1674	ksoniay95ee.info	text/html	2,396 bytes	hYP.avi
1906	www.download.win…	application/vnd.ms-cab-…	56 kB	authrootstl.cab
1933	151.106.27.208		591 bytes	client.rar
1996	151.106.27.208		591 bytes	client.rar
4882	89.163.144.224	application/rar	581 bytes	client.rar
5365	162.213.250.131	application/x-rar-compre…	425 kB	azor.rar
5380	85.114.134.49		107 bytes	index.php
9793	85.114.134.49	text/html	4,473 kB	index.php

Shown above: Exporting the EXE returned from ljeffery54ae.top