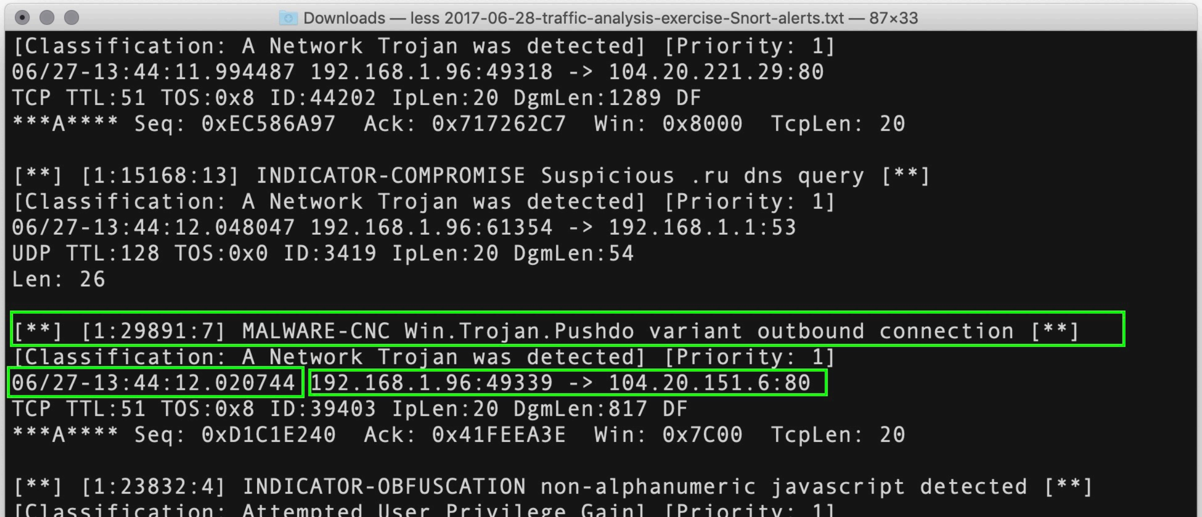
Post-Incident Report

Date of investigation	Today's Date
Date of incident	2017-06-27 at 13:38 GMT
Outcome	True Positive - Pushdo Malware Variant Found (or False Positive - 'reason why')
Action Taken	Identified Malware and infected host. Advise Firewall Rules to Block Traffic from Source. Advise reformatting infected computer or restoring to a backup prior to time of incident.
Reporting tool	Snort and Suratica Alerts
Attack vector (Web, Email, Network, etc.)	Web Malware Download
Source IP/email	maited.com/gerv.gun | 119.28.70.207
Source port	80
Destination IP/email	192.168.1.96
Destination port	49200

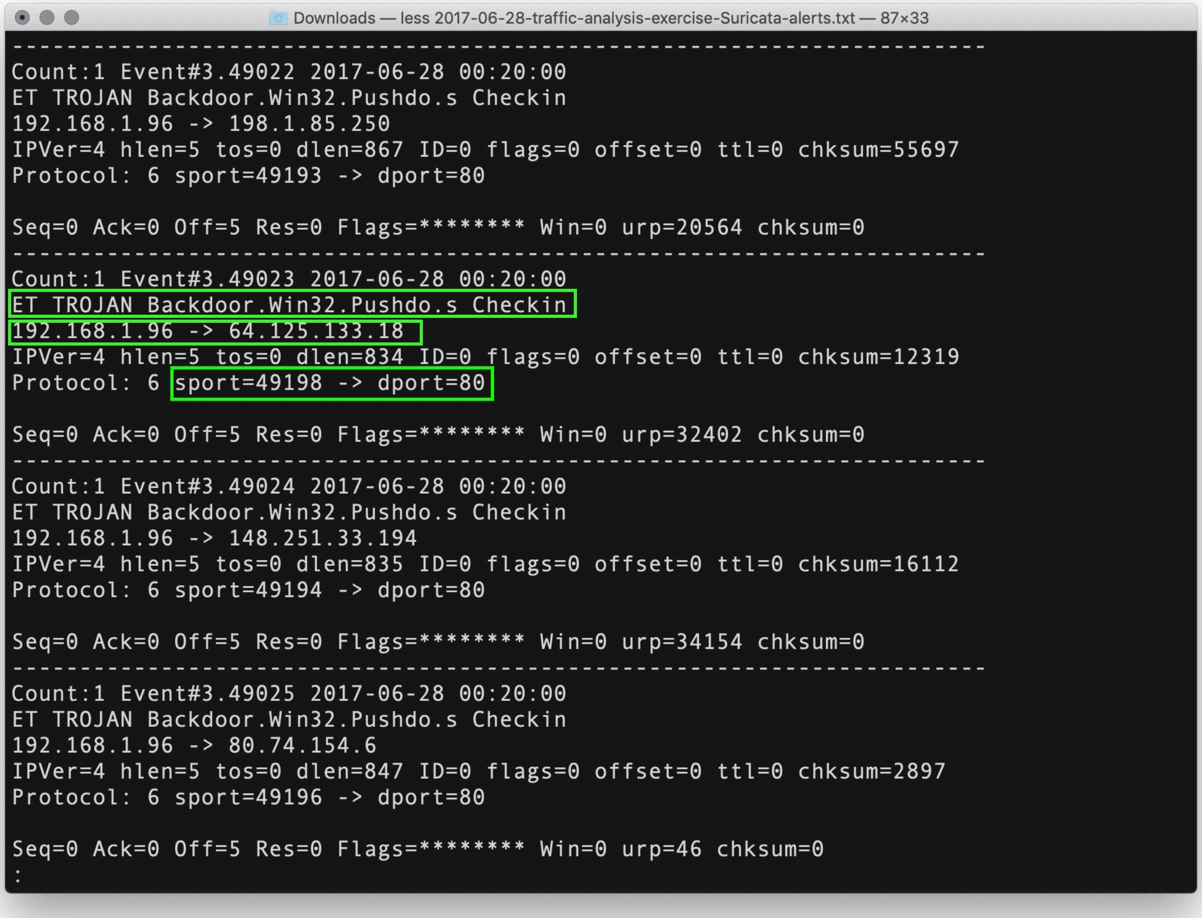
Narrative

- Alerted by Snort and Suricata:
  - "FILE-EXECUTABLE Portable Executable binary file magic detected"
  - "ET Trojan Backdoor.Win32.Pushdo.s Checkin"
  - "Malware-CNC Win.Trojan.Pushdo Variant Outbound Connection"
- Located Source/Destination IP Addresses and timestamp from Alerts:
  - Src/Prt: 119:28:70.207:80
  - Dst/Prt 192.168.1.96: 49148
- Identified and investigated a CVC alert that turned out to be a separate issue.



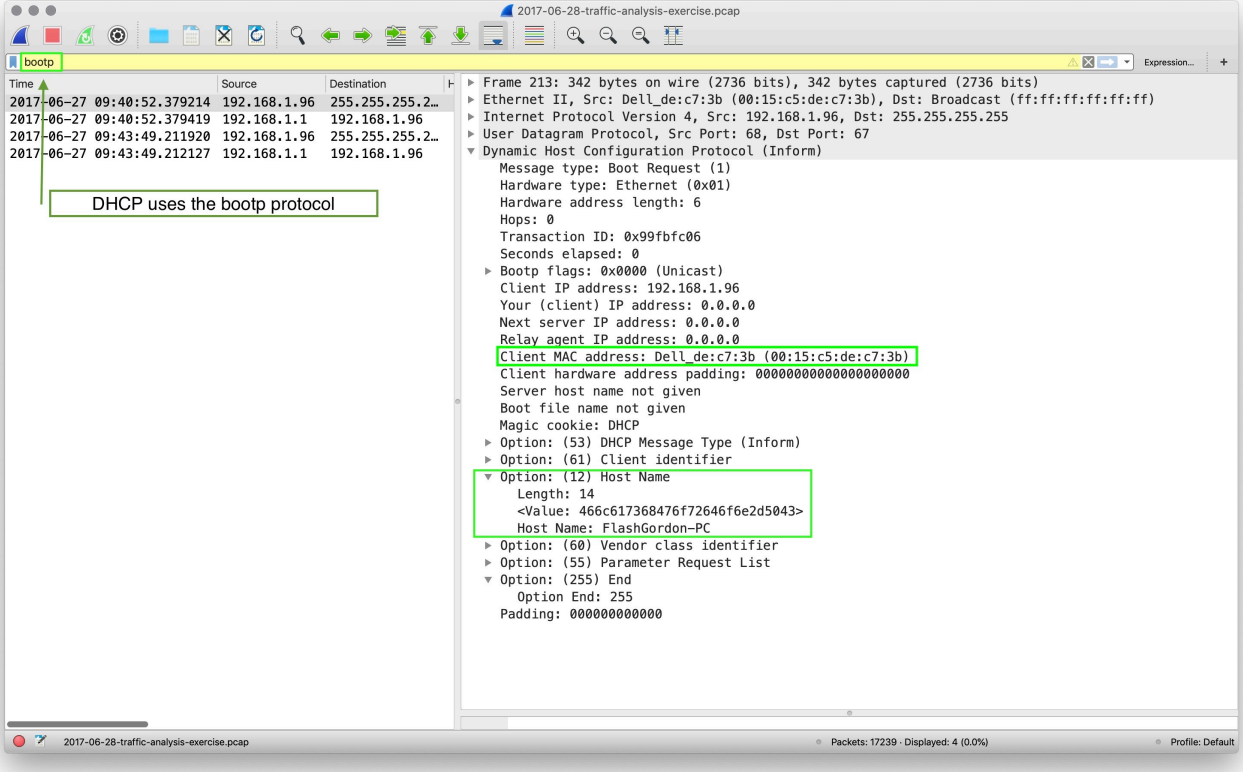
Downloads — less 2017-06-28-traffic-analysis-exercise-Snort-alerts.txt — 87×33

```
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:11.994487 192.168.1.96:49318 -> 104.20.221.29:80
TCP TTL:51 TOS:0x8 ID:44202 IpLen:20 DgmLen:1289 DF
***A**** Seq: 0xEC586A97  Ack: 0x717262C7  Win: 0x8000  TcpLen: 20

[**] [1:15168:13] INDICATOR-COMPROMISE Suspicious .ru dns query [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.048047 192.168.1.96:61354 -> 192.168.1.1:53
UDP TTL:128 TOS:0x0 ID:3419 IpLen:20 DgmLen:54
Len: 26

[**] [1:29891:7] MALWARE-CNC Win.Trojan.Pushdo variant outbound connection [**]
[Classification: A Network Trojan was detected] [Priority: 1]
06/27-13:44:12.020744 192.168.1.96:49339 -> 104.20.151.6:80
TCP TTL:51 TOS:0x8 ID:39403 IpLen:20 DgmLen:817 DF
***A**** Seq: 0xD1C1E240  Ack: 0x41FEEA3E  Win: 0x7C00  TcpLen: 20

[**] [1:23832:4] INDICATOR-OBFUSCATION non-alphanumeric javascript detected [**]
[Classification: Attempted User Privilege Gain] [Priority: 1]
```


Downloads — less 2017-06-28-traffic-analysis-exercise-Suricata-alerts.txt — 87×33

```
------------------------------------------------------------------------
Count:1 Event#3.49022 2017-06-28 00:20:00
ET TROJAN Backdoor.Win32.Pushdo.s Checkin
192.168.1.96 -> 198.1.85.250
IPVer=4 hlen=5 tos=0 dlen=867 ID=0 flags=0 offset=0 ttl=0 chksum=55697
Protocol: 6 sport=49193 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=20564 chksum=0
------------------------------------------------------------------------
Count:1 Event#3.49023 2017-06-28 00:20:00
ET TROJAN Backdoor.Win32.Pushdo.s Checkin
192.168.1.96 -> 64.125.133.18
IPVer=4 hlen=5 tos=0 dlen=834 ID=0 flags=0 offset=0 ttl=0 chksum=12319
Protocol: 6 sport=49198 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=32402 chksum=0
------------------------------------------------------------------------
Count:1 Event#3.49024 2017-06-28 00:20:00
ET TROJAN Backdoor.Win32.Pushdo.s Checkin
192.168.1.96 -> 148.251.33.194
IPVer=4 hlen=5 tos=0 dlen=835 ID=0 flags=0 offset=0 ttl=0 chksum=16112
Protocol: 6 sport=49194 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=34154 chksum=0
------------------------------------------------------------------------
Count:1 Event#3.49025 2017-06-28 00:20:00
ET TROJAN Backdoor.Win32.Pushdo.s Checkin
192.168.1.96 -> 80.74.154.6
IPVer=4 hlen=5 tos=0 dlen=847 ID=0 flags=0 offset=0 ttl=0 chksum=2897
Protocol: 6 sport=49196 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=46 chksum=0
:
```

- Identified Hostname and MacAddress of infected computer in pacp:
  - MAC: 00:15:c5:de:c7:3b
  - Host Name: FlashGordon-PC

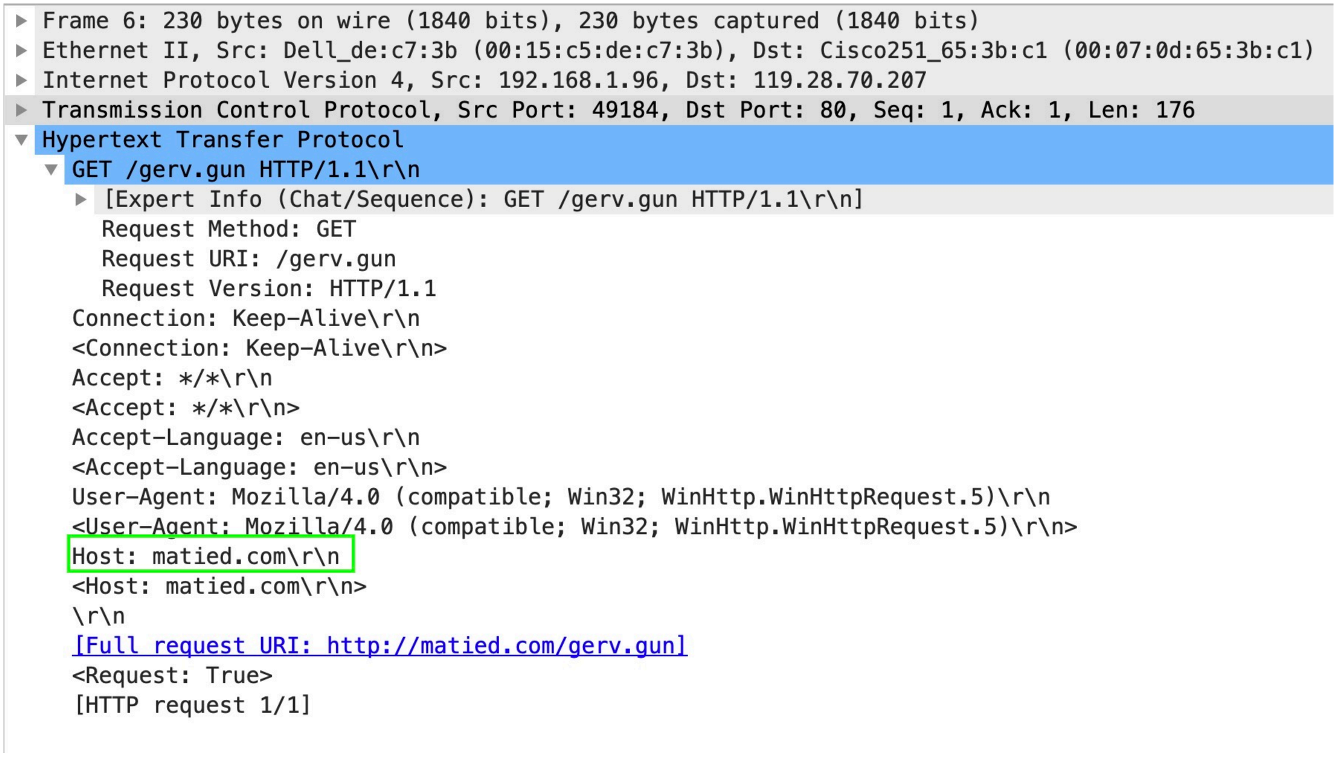

2017-06-28-traffic-analysis-exercise.pcap
bootp
Expression...
+
DHCP uses the bootp protocol
2017-06-28-traffic-analysis-exercise.pcap
Packets: 17239 · Displayed: 4 (0.0%)
Profile: Default

```
Time                        Source         Destination
2017-06-27 09:40:52.379214  192.168.1.96   255.255.255.2…
2017-06-27 09:40:52.379419  192.168.1.1    192.168.1.96
2017-06-27 09:43:49.211920  192.168.1.96   255.255.255.2…
2017-06-27 09:43:49.212127  192.168.1.1    192.168.1.96
```

```
▶ Frame 213: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Dell_de:c7:3b (00:15:c5:de:c7:3b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 192.168.1.96, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Dynamic Host Configuration Protocol (Inform)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x99fbfc06
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.1.96
    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: Dell_de:c7:3b (00:15:c5:de:c7:3b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Inform)
  ▶ Option: (61) Client identifier
  ▼ Option: (12) Host Name
      Length: 14
      <Value: 466c617368476f72646f6e2d5043>
      Host Name: FlashGordon-PC
  ▶ Option: (60) Vendor class identifier
  ▶ Option: (55) Parameter Request List
  ▼ Option: (255) End
      Option End: 255
    Padding: 000000000000
```

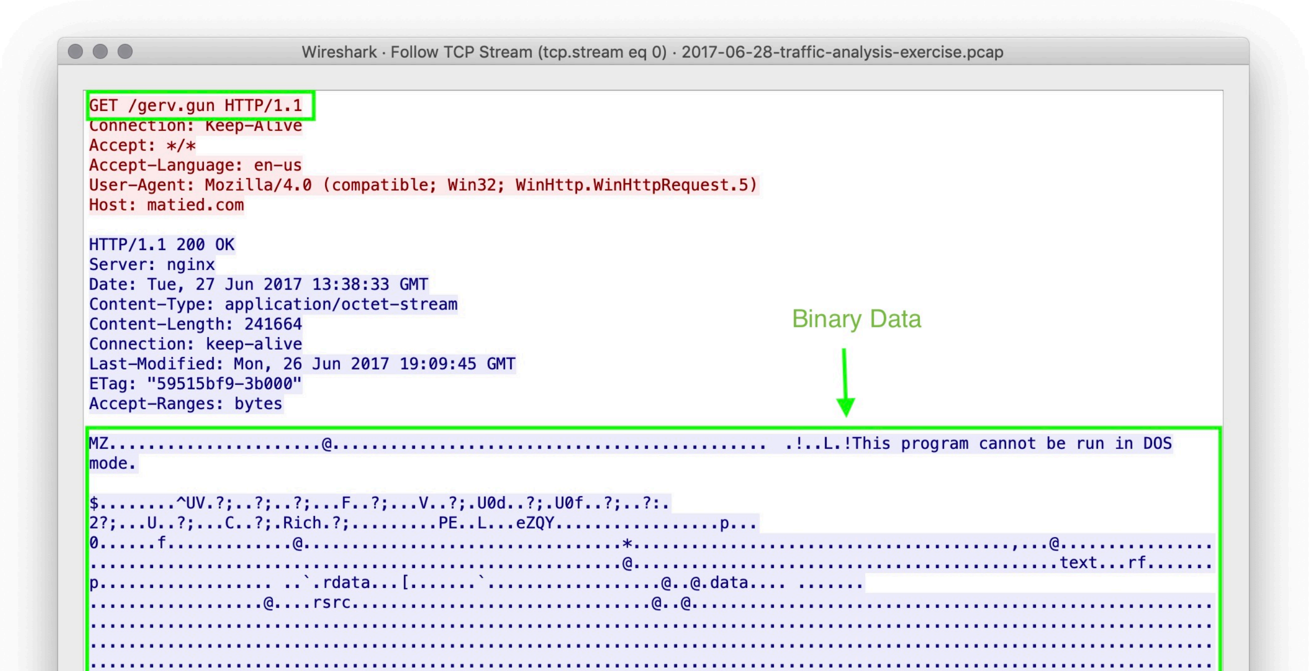
Post-Incident Report

- Identified download link of Pushdo in pcap HTTP traffic:
  - maited.com/gerv.gun



```
▶ Frame 6: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)
▶ Ethernet II, Src: Dell_de:c7:3b (00:15:c5:de:c7:3b), Dst: Cisco251_65:3b:c1 (00:07:0d:65:3b:c1)
▶ Internet Protocol Version 4, Src: 192.168.1.96, Dst: 119.28.70.207
▶ Transmission Control Protocol, Src Port: 49184, Dst Port: 80, Seq: 1, Ack: 1, Len: 176
▼ Hypertext Transfer Protocol
  ▼ GET /gerv.gun HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /gerv.gun HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /gerv.gun
      Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    <Connection: Keep-Alive\r\n>
    Accept: */*\r\n
    <Accept: */*\r\n>
    Accept-Language: en-us\r\n
    <Accept-Language: en-us\r\n>
    User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)\r\n
    <User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)\r\n>
    Host: matied.com\r\n
    <Host: matied.com\r\n>
    \r\n
    [Full request URI: http://matied.com/gerv.gun]
    <Request: True>
    [HTTP request 1/1]
```

- Followed the TCP Stream and found binary downloaded:
  - Tue, 27 Jun 2017 13:38 GMT

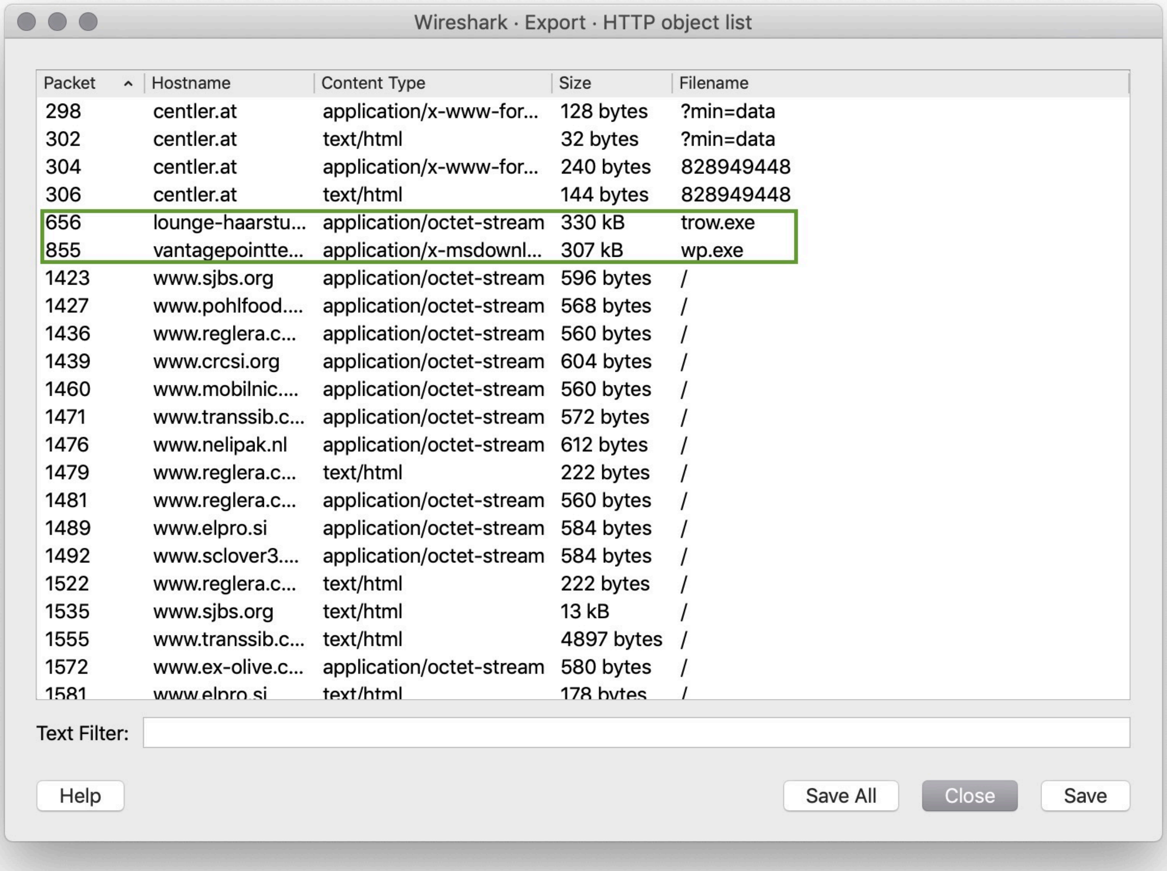


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2017-06-28-traffic-analysis-exercise.pcap
Binary Data

```
GET /gerv.gun HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: matied.com

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 27 Jun 2017 13:38:33 GMT
Content-Type: application/octet-stream
Content-Length: 241664
Connection: keep-alive
Last-Modified: Mon, 26 Jun 2017 19:09:45 GMT
ETag: "59515bf9-3b000"
Accept-Ranges: bytes

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

$........^UV.?;..?;..?;...F..?;...V..?;.U0d..?;.U0f..?;..?:.
2?;...U..?;...C..?;.Rich.?;.........PE..L...eZQY................p...
0.....f............@..............................*.................................,...@...............
..................................................@.........................................text...rf.......
p................. ..`.rdata...[.......`.................@..@.data.... .......
.................@....rsrc...........................@..@...........................................
....................................................................................................
....................................................................................................
....................................................................................................
```

Post-Incident Report

- Exported HTTP objects and found more malware downloaded:
  - trow.exe
  - wp.exe



Packet	Hostname	Content Type	Size	Filename
298	centler.at	application/x-www-for...	128 bytes	?min=data
302	centler.at	text/html	32 bytes	?min=data
304	centler.at	application/x-www-for...	240 bytes	828949448
306	centler.at	text/html	144 bytes	828949448
656	lounge-haarstu...	application/octet-stream	330 kB	trow.exe
855	vantagepointte...	application/x-msdownl...	307 kB	wp.exe
1423	www.sjbs.org	application/octet-stream	596 bytes	/
1427	www.pohlfood....	application/octet-stream	568 bytes	/
1436	www.reglera.c...	application/octet-stream	560 bytes	/
1439	www.crcsi.org	application/octet-stream	604 bytes	/
1460	www.mobilnic....	application/octet-stream	560 bytes	/
1471	www.transsib.c...	application/octet-stream	572 bytes	/
1476	www.nelipak.nl	application/octet-stream	612 bytes	/
1479	www.reglera.c...	text/html	222 bytes	/
1481	www.reglera.c...	application/octet-stream	560 bytes	/
1489	www.elpro.si	application/octet-stream	584 bytes	/
1492	www.sclover3....	application/octet-stream	584 bytes	/
1522	www.reglera.c...	text/html	222 bytes	/
1535	www.sjbs.org	text/html	13 kB	/
1555	www.transsib.c...	text/html	4897 bytes	/
1572	www.ex-olive.c...	application/octet-stream	580 bytes	/
1581	www.elpro.si	text/html	178 bytes	/

- Uploaded MD5 hashes to virus total for confirmation:
  - fb75d4f81be51074bb4147e781e5b402 trow.exe
  - 4da48f6423d5f7d75de281a674c2e620 wp.exe
- Used Wireshark to identify possible iptables rules to block traffic from source:

  - # IPv4 destination address.
    - iptables --append INPUT --in-interface eth0 --source 119.28.70.207/32 --jump DROP