

# 2018-10-31 - TRAFFIC ANALYSIS EXERCISE - HAPPY HALLOWEEN!

**Course Name:** Malware Analysis and Reverse Engineering (IAM302)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đình

## SCENARIO

Review the pcap and draft an incident report. Your report should contain:

- Date and time of the activity (in GMT or UTC)
- The account name or username from the infected Windows computer
- The host name of the infected Windows computer
- The MAC address of the infected Windows computer
- SHA256 file hashes for any malware from the pcap
- What type of infection this is

## Answer:

#1: Date and time of the activity (in GMT or UTC)

- 2018-10-31 15:33:05 UTC

#2: The account name or username from the infected Windows computer

- ichabod.crane

#3: The host name of the infected Windows computer

- Headless-PC

#4: The MAC address of the infected Windows computer

- 00:50:8b:2a:96:0a

#5: SHA256 file hashes for any malware from the pcap

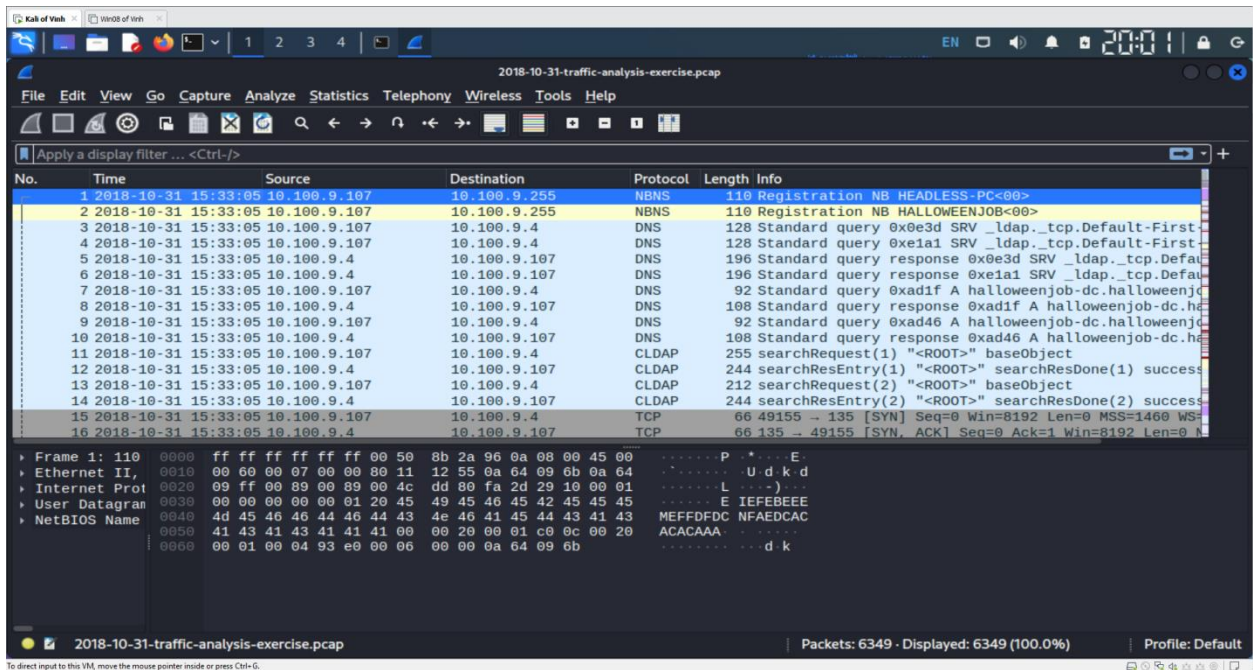
- 396223eeec49493a52dd9d8ba5348a332bf064483a358db79d8bb8d22e6eb62c

#6: Type of infection

- Trickbot

## Detail:

- First frame: 2018-10-31 15:33:05 UTC



- Listing all participants of unique conversations within .pcap file:

```
(TouristV@kali)-[~/Downloads]
└─$ tshark -r 2018-10-31-traffic-analysis-exercise.pcap -T fields -e ip.addr | sort | uniq
10.100.9.107,10.100.9.255
10.100.9.107,10.100.9.4
10.100.9.107,151.101.184.193
10.100.9.107,173.171.132.82
10.100.9.107,176.58.123.25
10.100.9.107,192.35.177.64
10.100.9.107,224.0.0.22
10.100.9.107,224.0.0.252
10.100.9.107,23.62.239.8
10.100.9.107,255.255.255.255
10.100.9.107,34.233.102.38
10.100.9.107,37.120.182.208
10.100.9.107,42.115.91.177
10.100.9.107,46.173.214.185
10.100.9.107,51.68.170.57
10.100.9.107,82.222.40.119
10.100.9.4,10.100.9.107
151.101.184.193,10.100.9.107
173.171.132.82,10.100.9.107
176.58.123.25,10.100.9.107
192.35.177.64,10.100.9.107
23.62.239.8,10.100.9.107
34.233.102.38,10.100.9.107
37.120.182.208,10.100.9.107
42.115.91.177,10.100.9.107
46.173.214.185,10.100.9.107
51.68.170.57,10.100.9.107
82.222.40.119,10.100.9.107
```

- Check endpoints:

Wireshark - Endpoints - 2018-10-31-traffic-analysis-exercise.pcap

Endpoint Settings

- Name resolution
- Limit to display filter
- Copy
- Map
- Protocol
  - Bluetooth
  - DCCP
  - Ethernet
  - FC
  - FDDI
  - IEEE 802.11
  - IEEE 802.15.4
  - IPv4
  - IPv6
  - IPX
  - JXTA
  - MPTCP
  - NCP
- Filter list for specific type

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	C
10.100.9.4	1,554	677.867 KiB	1,554	100.00%	794	407.259 KiB	760	270.609 KiB		
10.100.9.107	6,349	5.010 MiB	6,349	100.00%	2,130	408.235 KiB	4,219	4.612 MiB		
10.100.9.255	40	4.895 KiB	40	100.00%	0	0 bytes	40	4.895 KiB		
23.62.239.8	10	832 bytes	10	100.00%	5	453 bytes	5	379 bytes		
34.233.102.38	8	785 bytes	8	100.00%	3	306 bytes	5	479 bytes		
37.120.182.208	11	1.003 KiB	11	100.00%	5	488 bytes	6	539 bytes		
42.115.91.177	277	51.610 KiB	277	100.00%	148	26.856 KiB	129	24.754 KiB		
46.173.214.185	293	326.808 KiB	293	100.00%	236	323.718 KiB	57	3.090 KiB		
51.68.170.57	3,220	3.272 MiB	3,220	100.00%	2,425	3.229 MiB	795	44.184 KiB		
82.222.40.119	324	190.517 KiB	324	100.00%	201	150.221 KiB	123	40.296 KiB		
151.101.184.193	536	509.850 KiB	536	100.00%	371	500.795 KiB	165	9.055 KiB		
173.171.132.82	41	8.769 KiB	41	100.00%	19	1.402 KiB	22	7.366 KiB		
176.58.123.25	18	4.806 KiB	18	100.00%	9	3.684 KiB	9	1.122 KiB		
192.35.177.64	8	1.763 KiB	8	100.00%	3	1.352 KiB	5	421 bytes		
224.0.0.22	3	162 bytes	3	100.00%	0	0 bytes	3	162 bytes		
224.0.0.252	4	270 bytes	4	100.00%	0	0 bytes	4	270 bytes		
255.255.255.255	2	684 bytes	2	100.00%	0	0 bytes	2	684 bytes		

- Filter on `http.request or ssl.handshake.type == 1` for web-based traffic, and I find the source IP address is 10.100.9.107. That's the Windows client.

2018-10-31-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: `http.request or ssl.handshake.type == 1`

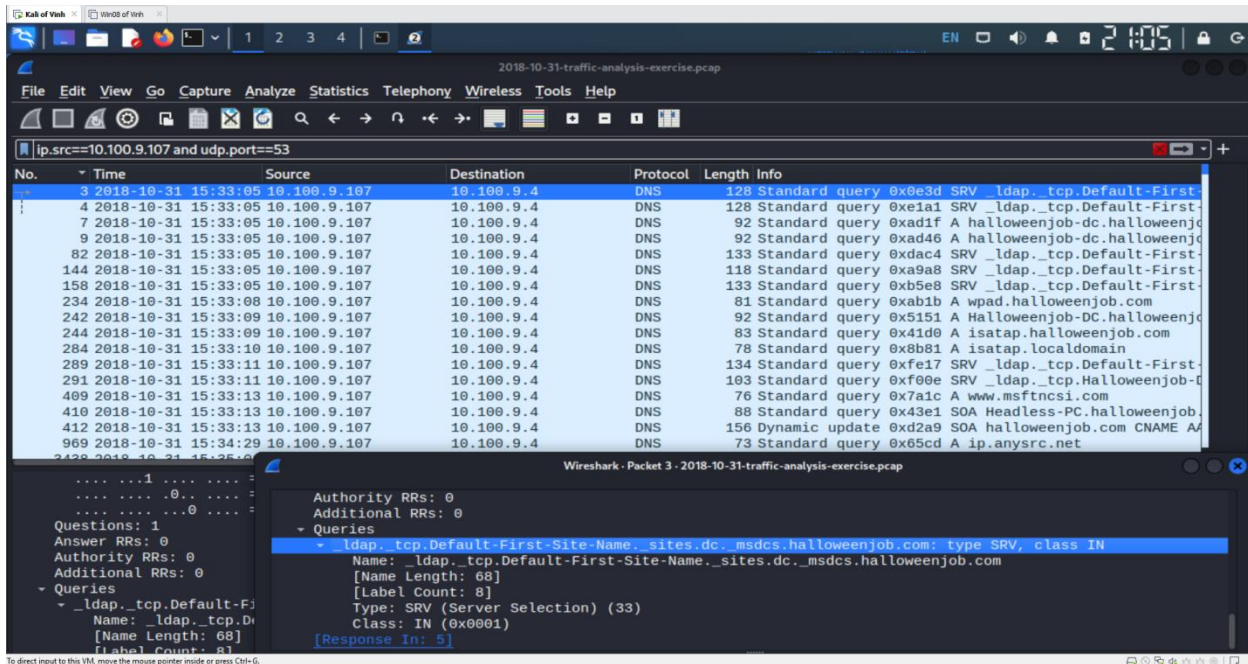
No.	Time	Source	Destination	Protocol	Length	Info
418	2018-10-31 15:33:13	10.100.9.107	23.62.239.8	HTTP	151	GET /ncsi.txt HTTP/1.1
679	2018-10-31 15:34:11	10.100.9.107	46.173.214.185	HTTP	128	GET /starttrack HTTP/1.1
974	2018-10-31 15:34:29	10.100.9.107	37.120.182.208	HTTP	257	GET /plain/clientip HTTP/1.1
981	2018-10-31 15:34:30	10.100.9.107	82.222.40.119	TLSv1	149	Client Hello
997	2018-10-31 15:34:32	10.100.9.107	51.68.170.57	TLSv1	149	Client Hello
3310	2018-10-31 15:34:50	10.100.9.107	82.222.40.119	TLSv1	149	Client Hello
3328	2018-10-31 15:34:51	10.100.9.107	82.222.40.119	TLSv1	149	Client Hello
3341	2018-10-31 15:34:52	10.100.9.107	82.222.40.119	TLSv1	149	Client Hello
3370	2018-10-31 15:34:54	10.100.9.107	173.171.132.82	HTTP	405	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C644
3418	2018-10-31 15:35:01	10.100.9.107	42.115.91.177	TLSv1	149	Client Hello
3498	2018-10-31 15:35:24	10.100.9.107	42.115.91.177	TLSv1	149	Client Hello
3517	2018-10-31 15:35:26	10.100.9.107	42.115.91.177	TLSv1	149	Client Hello
3533	2018-10-31 15:35:27	10.100.9.107	173.171.132.82	HTTP	340	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C644
3580	2018-10-31 15:35:33	10.100.9.107	42.115.91.177	TLSv1	149	Client Hello
4644	2018-10-31 15:35:45	10.100.9.107	34.233.102.38	HTTP	251	GET / HTTP/1.1
5165	2018-10-31 15:36:11	10.100.9.107	173.171.132.82	HTTP	280	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C644
5238	2018-10-31 15:40:39	10.100.9.107	42.115.91.177	TLSv1	181	Client Hello
5255	2018-10-31 15:44:09	10.100.9.107	42.115.91.177	TLSv1	181	Client Hello

[Time delta from previous captured frame: 0.000612000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 7.933251000 seconds]  
 Frame Number: 418  
 Frame Length: 151 bytes (1208 bits)  
 Capture Length: 151 bytes (1208 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:tcp:http]  
 [Coloring Rule Name: HTTP]  
 [Coloring Rule String: http || tcp.port == 80 || http2]

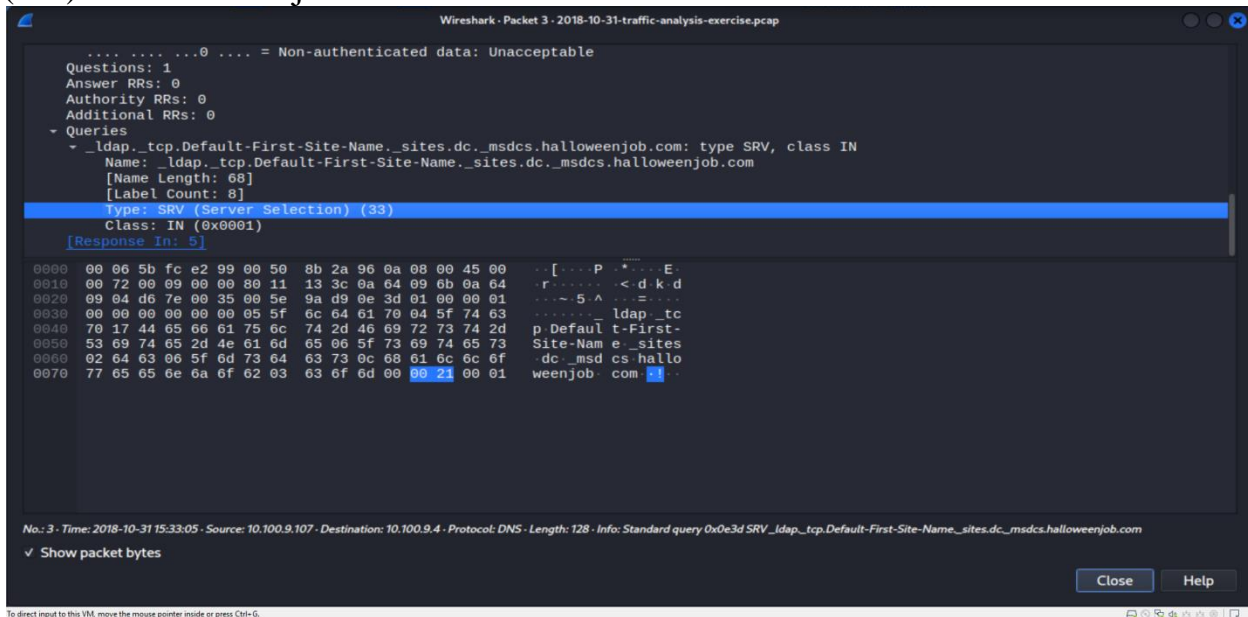
Ethernet II, Src: RealtekP (08:00:27:00:00:00), Dst: Cisco-e1:59:04 (08:02:7d:e1:59:04)

- Let's say IP 10.100.9.107 is the victim's computer while IP 10.100.9.4 is another local node of some sort. Let's prove this assumption by filtering DNS query packets with a source address of 10.100.9.107. The resulting output will show the source address polling its DNS server, usually done before authenticating to a domain and/or communicating with HTTP servers.





- With this result, I can now start to deduce some things. For example, we see 10.100.9.4 used exclusively by 10.100.9.107 to resolve multiple IP addresses. I also see a few queries for SRV records used to determine which nodes are serving different applications. Example frame #3 shows looking for a Domain Controller (DC) for halloweenjob.com.



- Frame #410, I also see a single Dynamic update for a SOA record.

Kali of Vulk x VM of job x

Wireshark - Packet 410 - 2018-10-31-traffic-analysis-exercise.pcap

.....0 .... = Non-authenticated data: Unacceptable

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0

Queries

- Headless-PC.halloweenjob.com: type SOA, class IN
  - Name: Headless-PC.halloweenjob.com
  - [Name Length: 28]
  - [Label Count: 3]
  - Type: SOA (Start of a zone of Authority) (6)
  - Class: IN (0x0001)

[Response in: 411]

0000	00 06 5b fc e2 99 00 50	8b 2a 96 0a 08 00 45 00	..[....P.....E..
0010	00 4a 00 ec 00 00 80 11	12 81 0a 64 09 6b 0a 64	..J.....d.k.d
0020	09 04 f8 02 00 35 00 36	49 36 43 e1 01 00 00 01	.....5.6 I6C....
0030	00 00 00 00 00 00 0b 48	65 61 64 6c 65 73 73 2d	.....H eadless-
0040	50 43 0c 68 61 6c 6c 6f	77 65 65 6e 6a 6f 62 03	PC.hallo weenjob-
0050	63 6f 6d 00 00 00 00 01		com .x..

✓ Show packet bytes

Close Help

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

```
TouristV@kali: ~/Downloads
File Actions Edit View Help
(TouristV@kali)~/Downloads$ tshark -r 2018-10-31-traffic-analysis-exercise.pcap -V 'frame.number==410' -V
Frame 410: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 31, 2018 11:33:13.190487000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1540999993.190487000 seconds
[Time delta from previous captured frame: 0.058006000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 7.831155000 seconds]
Frame Number: 410
Frame Length: 88 bytes (704 bits)
Capture Length: 88 bytes (704 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:dns]
Ethernet II, Src: HewlettP_2a:96:0a (00:50:8b:2a:96:0a), Dst: Dell_fc:e2:99 (00:06:5b:fc:e2:99)
Destination: Dell_fc:e2:99 (00:06:5b:fc:e2:99)
Address: Dell_fc:e2:99 (00:06:5b:fc:e2:99)
.... 0... .. = LG bit: Globally unique address (factory default)
.... 0... .. = IG bit: Individual address (unicast)
Source: HewlettP_2a:96:0a (00:50:8b:2a:96:0a)
Address: HewlettP_2a:96:0a (00:50:8b:2a:96:0a)
.... 0... .. = LG bit: Globally unique address (factory default)
.... 0... .. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.100.9.107, Dst: 10.100.9.4
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... 00 .. = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 74
Identification: 0x00ec (236)
000. .... = Flags: 0x0
0... .. = Reserved bit: Not set
..0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set

[Header checksum status: Unverified]
Source Address: 10.100.9.107
Destination Address: 10.100.9.4
User Datagram Protocol, Src Port: 63490, Dst Port: 53
Source Port: 63490
Destination Port: 53
Length: 54
Checksum: 0x4936 [unverified]
[Checksum Status: Unverified]
[Stream index: 25]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]
UDP payload (46 bytes)
Domain Name System (query)
Transaction ID: 0x43e1
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
..000 0... .. = Opcode: Standard query (0)
.... 0... .. = Truncated: Message is not truncated
.... 1... .. = Recursion desired: Do query recursively
.... 0... .. = Z: reserved (0)
.... 0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
Headless-PC.halloweenjob.com: type SOA, class IN
Name: Headless-PC.halloweenjob.com
[Name Length: 28]
[Label Count: 3]
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

➔ The Dynamic update is 10.100.9.107 giving its MAC address (00:50:8b:2a:96:0a) and hostname (Headless-PC) to the local DNS server.

- Search the .pcap for HTTP requests

2018-10-31-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==10.100.9.107 and http

No.	Time	Source	Destination	Protocol	Length	Info
418	2018-10-31 15:33:13	10.100.9.107	23.62.239.8	HTTP	151	GET /ncsi.txt HTTP/1.1
679	2018-10-31 15:34:11	10.100.9.107	46.173.214.185	HTTP	128	GET /startr.ack HTTP/1.1
974	2018-10-31 15:34:29	10.100.9.107	37.120.182.208	HTTP	257	GET /plain/clientip HTTP/1.1
3370	2018-10-31 15:34:54	10.100.9.107	173.171.132.82	HTTP	405	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C64A0DFEC
3533	2018-10-31 15:35:27	10.100.9.107	173.171.132.82	HTTP	340	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C64A0DFEC
4644	2018-10-31 15:35:45	10.100.9.107	34.233.102.38	HTTP	251	GET / HTTP/1.1
5165	2018-10-31 15:36:11	10.100.9.107	173.171.132.82	HTTP	280	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C64A0DFEC
6109	2018-10-31 15:45:45	10.100.9.107	192.35.177.64	HTTP	193	GET /roots/dstrootcax3.p7c HTTP/1.1

[Time delta from previous captured frame: 0.000612000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 7.933251000 seconds]  
Frame Number: 418  
Frame Length: 151 bytes (1208 bits)  
Capture Length: 151 bytes (1208 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http]  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
Ethernet II, Src: Hewlett-Packard 28:90:50:08:2a:06, Dst: Cisco 01:50:50:00:00:00 (08:00:27:0d:01:50:00:00)

- The first HTTP request is frame #418 could be of interest as it is only a few frames away from the previous DNS query we analyzed is #410. Yet, it's actually benign as Microsoft systems are typically configured with a service called [Network Connectivity Status Indicator \(NCSI\)](#).

- The second HTTP request however (frame #679), is not benign. Let's download a .csv file containing a list of known malicious IP addresses to search it for the HTTP server at 46.173.214.185.



Kali of VmKali of Vm

Wireshark - Packet 679 - 2018-10-31-traffic-analysis-exercise.pcap

TCP payload (74 bytes)  
 - Hypertext Transfer Protocol  
 GET /starttr.ack HTTP/1.1\r\n  
 [Expert Info (Chat/Sequence): GET /starttr.ack HTTP/1.1\r\n]  
 [GET /starttr.ack HTTP/1.1\r\n]  
 [Severity level: Chat]  
 [Group: Sequence]  
 Request Method: GET  
 Request URI: /starttr.ack  
 Request Version: HTTP/1.1  
 Host: 46.173.214.185\r\n\r\n  
 Connection: Keep-Alive\r\n\r\n  
 [Full request URI: http://46.173.214.185/starttr.ack]  
 [HTTP request 1/1]  
 [Response in frame: 966]

0000 00 02 7d e1 59 04 00 50 8b 2a 96 0a 08 00 45 00 ...Y.P...E.  
 0010 00 72 01 76 40 00 80 06 df da 0a 64 09 6b 2e ad ...r.v...d.k..  
 0020 d6 b9 c0 30 00 50 3c ed 61 5f 18 26 6c 86 50 18 ...0.P...a.&l.P..  
 0030 fa f0 4d c8 00 00 47 45 54 20 2f 73 74 61 72 74 ...M...GE T /start  
 0040 72 2e 61 63 6b 20 48 54 54 50 2f 31 2e 31 0d 0a ...r.ack HT TP/1.1..  
 0050 48 6f 73 74 3a 20 34 36 2e 31 37 33 2e 32 31 34 ...Host: 46 .173.214  
 0060 2e 31 38 35 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ...185..Co nnection  
 0070 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a ...: Keep-A live....

✓ Show packet bytes

Close Help

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

2018-10-31-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Ctrl+O  
 Open Recent  
 Merge...  
 Import from Hex Dump...  
 Close Ctrl+W  
 Save Ctrl+S  
 Save As... Ctrl+Shift+S  
 File Set  
 Export Specified Packets...  
 Export Packet Dissections  
 Export Packet Bytes... Ctrl+Shift+X  
 Export PDUs to File...  
 Strip Headers...  
 Export TLS Session Keys...  
 Export Objects  
 Print... Ctrl+P  
 Quit Ctrl+Q

Destination	Protocol	Length	Info
23.62.239.8	HTTP	151	GET /ncsi.txt HTTP/1.1
46.173.214.185	HTTP	128	GET /starttr.ack HTTP/1.1
37.120.182.208	HTTP	257	GET /plain/clientip HTTP/1.1
173.171.132.82	HTTP	405	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C64A0DFEC
173.171.132.82	HTTP	340	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C64A0DFEC
34.233.102.38	HTTP	251	GET / HTTP/1.1
173.171.132.82	HTTP	280	POST /sat91/HEADLESS-PC_W617601.88AD32764B61024C64A0DFEC
192.35.177.64	HTTP	193	GET /roots/dstrootcax3.p7c HTTP/1.1

Frame Number: 679  
 Frame Length: 128 bytes (1024 bits)  
 Capture Length: 128 bytes (1024 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:tcp:http]  
 [Coloring Rule Name: HTTP]  
 [Coloring Rule String: http || tcp.port == 80 || http2]

0000 00 02 7d e1 59 04 00 50 8b 2a 96 0a 08 00 45 00 ...Y.P...E.  
 0010 00 72 01 76 40 00 80 06 df da 0a 64 09 6b 2e ad ...r.v...d.k..  
 0020 d6 b9 c0 30 00 50 3c ed 61 5f 18 26 6c 86 50 18 ...0.P...a.&l.P..  
 0030 fa f0 4d c8 00 00 47 45 54 20 2f 73 74 61 72 74 ...M...GE T /start  
 0040 72 2e 61 63 6b 20 48 54 54 50 2f 31 2e 31 0d 0a ...r.ack HT TP/1.1..  
 0050 48 6f 73 74 3a 20 34 36 2e 31 37 33 2e 32 31 34 ...Host: 46 .173.214  
 0060 2e 31 38 35 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ...185..Co nnection  
 0070 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a ...: Keep-A live....

- Find IP 46.173.214.185 on [URLhaus](http://URLhaus.com) | [Browse \(abuse.ch\)](http://Browse.abuse.ch) and see detail



Kali of Web x Wind of Web x

URLhaus | Browse x +

https://urlhaus.abuse.ch/browse.php?search=46.173.214.185

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Rawsec's CyberSecurit...

**URLhaus** by ABUSE.ch

Browse API Feeds Statistics About

## Submit a URL

In order to submit a URL to URLhaus, you need to login with your Twitter account

## Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url\_status:online **Search**

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2018-10-30 17:23:02	<a href="http://46.173.214.185/startr.ack">http://46.173.214.185/startr.ack</a>	Offline	Trickbot	Anonymous

Previous Next

© abuse.ch 2023

---

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

Kali of Web x Wind of Web x

URLhaus | http://46.173.214.185 x +

https://urlhaus.abuse.ch/url/72453/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Rawsec's CyberSecurit...

**URLhaus** by ABUSE.ch

Browse API Feeds Statistics About

Actions

ID:	72453
URL:	<a href="http://46.173.214.185/startr.ack">http://46.173.214.185/startr.ack</a>
URL Status:	Offline
Host:	<a href="http://46.173.214.185">46.173.214.185</a>
Date added:	2018-10-30 17:23:02 UTC
Last online:	2018-11-01 20:XX:XX UTC
Threat:	Malware download
Google Safe Browsing:	Clean
Reporter:	Anonymous
Abuse complaint sent (?):	Yes (2018-10-30 17:24:02 UTC to abuse[at]inoviencia[dot]ru)
Takedown time:	2 days, 2 hours, 56 minutes (down since 2018-11-01 20:20:55 UTC)
Tags:	Trickbot

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

- Find who downloaded the malware

**Wireshark Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
47	2018-10-31 15:33:05	10.100.9.107	10.100.9.4	KRB5	298	AS-REQ
55	2018-10-31 15:33:05	10.100.9.107	10.100.9.4	KRB5	378	AS-REQ
96	2018-10-31 15:33:05	10.100.9.107	10.100.9.4	KRB5	298	AS-REQ
106	2018-10-31 15:33:05	10.100.9.107	10.100.9.4	KRB5	378	AS-REQ
456	2018-10-31 15:33:16	10.100.9.107	10.100.9.4	KRB5	298	AS-REQ
464	2018-10-31 15:33:16	10.100.9.107	10.100.9.4	KRB5	378	AS-REQ
500	2018-10-31 15:33:27	10.100.9.107	10.100.9.4	KRB5	291	AS-REQ
508	2018-10-31 15:33:27	10.100.9.107	10.100.9.4	KRB5	371	AS-REQ

**Terminal Output:**

```

(TouristV@kali) ~/Downloads
$ tshark -r 2018-10-31-traffic-analysis-exercise.pcap -Y 'ip.src==10.100.9.107 and kerberos.CNameString' -V | grep CNameString
CNameString: headless-pc$
CNameString: headless-pc$
CNameString: headless-pc$
CNameString: headless-pc$
CNameString: HEADLESS-PC$
CNameString: HEADLESS-PC$
CNameString: ichabod.crane
CNameString: ichabod.crane
  
```

- Let's take a step back and filter for frames containing this username for reference.

Kali of Vm x Vmware of Vm x

2018-10-31-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos.CNameString==ichabod.crane

No.	Time	Source	Destination	Protocol	Length	Info
500	2018-10-31 15:33:27	10.100.9.107	10.100.9.4	KRB5	291	AS-REQ
508	2018-10-31 15:33:27	10.100.9.107	10.100.9.4	KRB5	371	AS-REQ
510	2018-10-31 15:33:27	10.100.9.4	10.100.9.107	KRB5	224	AS-REP
522	2018-10-31 15:33:27	10.100.9.4	10.100.9.107	KRB5	132	TGS-REP
536	2018-10-31 15:33:27	10.100.9.4	10.100.9.107	KRB5	262	TGS-REP
567	2018-10-31 15:33:27	10.100.9.4	10.100.9.107	KRB5	246	TGS-REP
603	2018-10-31 15:33:27	10.100.9.4	10.100.9.107	KRB5	246	TGS-REP
615	2018-10-31 15:33:27	10.100.9.4	10.100.9.107	KRB5	110	TGS-REP

[Time delta from previous captured frame: 0.000015000 seconds]  
[Time delta from previous displayed frame: 0.003492000 seconds]  
[Time since reference or first frame: 21.782791000 seconds]  
Frame Number: 522  
Frame Length: 132 bytes (1056 bits)  
Capture Length: 132 bytes (1056 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:kerberos]  
[Coloring Rule Name: TCP]  
[Coloring Rule String: tcp]

Ethernet II, Src: RealtekU (08:00:5b:fc:a2:99), Dst: HsaulenTB (9a:96:0a:00:50:8b), 2a:96:0a

0000 00 50 8b 2a 96 0a 00 06 5b fc  
0010 00 76 0a d4 40 00 80 06 c8 77  
0020 09 6b 00 58 c0 28 04 9c a3 28  
0030 01 00 a0 fb 00 00 44 73 cb 90  
0040 dd e5 53 e3 d8 61 37 cf e0 41  
0050 92 4e ff 53 9f a0 2d a2 bc bf  
0060 62 38 77 fe 4d 4b 70 31 e0 6a  
0070 0b ce 8c eb 1e ad 1a 3e 87 bd  
0080 82 76 f8 75

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

- the SHA256 file hash

TouristV@kali: ~/Downloads

File Actions Edit View Help

```

(TouristV@kali) ~/Downloads
$ tshark -r 2018-10-31-traffic-analysis-exercise.pcap --export-objects http.evidence
1 0.000000 10.100.9.107 → 10.100.9.255 NBNS 110 Registration NB HEADLESS-PC<00>
2 0.000001 10.100.9.107 → 10.100.9.255 NBNS 110 Registration NB HALLOWEENJOB<00>
3 0.026204 10.100.9.107 → 10.100.9.4 DNS 128 Standard query 0xe3d SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.halloweenjob.com
4 0.027929 10.100.9.107 → 10.100.9.4 DNS 128 Standard query 0xe1a SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.halloweenjob.com
5 0.027929 10.100.9.4 → 10.100.9.107 DNS 196 Standard query response 0xe3d SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.halloweenjob.com
6 0.027930 10.100.9.4 → 10.100.9.107 DNS 196 Standard query response 0xe1a SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.halloweenjob.com
7 0.033225 10.100.9.107 → 10.100.9.4 DNS 92 Standard query 0xad1f A halloweenjob-dc.halloweenjob.com
8 0.033225 10.100.9.4 → 10.100.9.107 DNS 108 Standard query response 0xad1f A halloweenjob-dc.halloweenjob.com A 10.100.9.4
9 0.033226 10.100.9.107 → 10.100.9.4 DNS 92 Standard query 0xad46 A halloweenjob-dc.halloweenjob.com
10 0.033226 10.100.9.4 → 10.100.9.107 DNS 108 Standard query response 0xad46 A halloweenjob-dc.halloweenjob.com A 10.100.9.4
11 0.048371 10.100.9.107 → 10.100.9.4 CLDAP 255 searchRequest(1) "<ROOT>" baseObject
12 0.048372 10.100.9.4 → 10.100.9.107 CLDAP 244 searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
13 0.052364 10.100.9.107 → 10.100.9.4 CLDAP 212 searchRequest(2) "<ROOT>" baseObject
14 0.052365 10.100.9.4 → 10.100.9.107 CLDAP 244 searchResEntry(2) "<ROOT>" searchResDone(2) success [1 result]
15 0.148228 10.100.9.107 → 10.100.9.4 TCP 66 49155 → 135 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
16 0.148313 10.100.9.4 → 10.100.9.107 TCP 66 135 → 49155 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
17 0.149293 10.100.9.107 → 10.100.9.4 TCP 54 49155 → 135 [ACK] Seq=1 Ack=1 Win=65536 Len=0
18 0.156096 10.100.9.107 → 10.100.9.4 DCERPC 214 Bind: call_id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-9812-4540-0300-000000000000)
19 0.156238 10.100.9.4 → 10.100.9.107 DCERPC 162 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
20 0.157058 10.100.9.107 → 10.100.9.4 EPM 222 Map request, RPC_NETLOGON, 32bit NDR
21 0.157059 10.100.9.4 → 10.100.9.107 EPM 222 Map response, RPC_NETLOGON, 32bit NDR, RPC_NETLOGON, 32bit NDR
22 0.170229 10.100.9.107 → 10.100.9.4 TCP 66 49156 → 49158 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
23 0.170230 10.100.9.4 → 10.100.9.107 TCP 66 49158 → 49156 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
24 0.170978 10.100.9.107 → 10.100.9.4 TCP 54 49156 → 49158 [ACK] Seq=1 Ack=1 Win=65536 Len=0
25 0.171725 10.100.9.107 → 10.100.9.4 DCERPC 214 Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
26 0.171726 10.100.9.4 → 10.100.9.107 DCERPC 162 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
27 0.172569 10.100.9.107 → 10.100.9.4 RPC_NETLOGON 238 NetrServerReqChallenge request,
28 0.172594 10.100.9.4 → 10.100.9.107 RPC_NETLOGON 90 NetrServerReqChallenge response
29 0.173820 10.100.9.107 → 10.100.9.4 RPC_NETLOGON 298 NetrServerAuthenticate3 request

```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

