Network Analysis-Wireshark: Summary of Operations

[Time Thieves](#)

[Vulnerable Windows Machines](#)

[Illegal Downloads](#)

Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?
    - The domain name of the users' custom site is frank-n-ted.com, which can be seen in the images shown below.

File Action Media Clipboard View Help
Shell No. 1
Shell No. 1
pcap
pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr ==10.6.12.0/24
No. Time Source Destination Pro
55420 641.047496500 Frank-n-Ted-DC.frank-n-ted.com 255.255.255.255 DH
55421 641.048373200 DESKTOP-86J4BX.frank-n-ted.com igmp.mcast.net IG
55422 641.049214500 DESKTOP-86J4BX.frank-n-ted.com igmp.mcast.net IG
55423 641.050071100 DESKTOP-86J4BX.frank-n-ted.com igmp.mcast.net IG
55424 641.050936500 DESKTOP-86J4BX.frank-n-ted.com igmp.mcast.net IG
55425 641.052219600 DESKTOP-86J4BX.frank-n-ted.com 224.0.0.251 MD
55426 641.053707000 DESKTOP-86J4BX.frank-n-ted.com 224.0.0.251 MD
55427 641.054843300 DESKTOP-86J4BX.frank-n-ted.com 224.0.0.252 LL
55428 641.055829300 DESKTOP-86J4BX.frank-n-ted.com igmp.mcast.net IG
Frame 55420: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on in
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), D
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)

Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
pcap
pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt
55838 642.805892700 DESKTOP-86J4BX.frank-n-ted.com Frank-n-Ted-DC.fran… TCP 151
55839 642.807551200 DESKTOP-86J4BX.frank-n-ted.com Frank-n-Ted-DC.fran… KRB5 10
55840 642.808395900 Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran… TCP 5
55841 642.832653700 Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran… TCP 151
55842 642.834745500 Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran… KRB5 13
55843 642.835595500 DESKTOP-86J4BX.frank-n-ted.com Frank-n-Ted-DC.fran… TCP 5
55844 642.836453900 DESKTOP-86J4BX.frank-n-ted.com Frank-n-Ted-DC.fran… TCP 5
55845 642.837317600 Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran… TCP 5
55846 642.838179500 Frank-n-Ted-DC.frank-n-ted.com DESKTOP-86J4BX.fran… TCP 5
Frame 55841: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interfac
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Intel_68:42:d3 (00:11:75:68:42:d
Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12), Dst: DESKTO

2. What is the IP address of the Domain Controller (DC) of the AD network?
    - The IP address of the Domain Controller in the Active Directory Network is 10.6.12.12, as shown in the images below.

3. What is the name of the malware downloaded to the 10.6.12.203 machine?
    - The malware that was downloaded is titled `june11.dll`, as shown in the image below.

Shell No. 1 | pcap | 07:55 PM | Lock Screen

pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.6.12.203 and http.request.method ==GET

No.	Time	Source	Destination	Protocol	Length	Info
58748	658.621258400	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
58752	658.636633700	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

```
    [Time since reference or first frame: 658.621258400 seconds]
    Frame Number: 58748
    Frame Length: 275 bytes (2200 bits)
    Capture Length: 275 bytes (2200 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: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 1, Ack: 1, Len: 221
0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A}·: Km····E·
0010  01 05 ad fa 40 00 80 06  ea 05 0a 06 0c cb cd b9   ····@··· ........
0020  7d 68 c2 4b 00 50 04 1f  3e 60 78 a3 4f a4 50 18   }h·K·P·· >`x·O·P·
0030  ff ff 62 af 00 00 47 45  54 20 2f 70 51 42 74 57   ··b···GE T /pQBtW
0040  6a 20 48 54 54 50 2f 31  2e 31 0d 0a 41 63 63 65   j HTTP/1 .1··Acce
0050  70 74 3a 20 2a 2f 2a 0d  0a 41 63 63 65 70 74 2d   pt: */*· ·Accept-
0060  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
0070  64 65 66 6c 61 74 65 0d  0a 55 73 65 72 2d 41 67   deflate· ·User-Ag
0080  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 34 2e 30   ent: Moz illa/4.0
0090  20 28 63 6f 6d 70 61 74  69 62 6c 65 3b 20 4d 53    (compat ible; MS
00a0  49 45 20 37 2e 30 3b 20  57 69 6e 64 6f 77 73 20   IE 7.0;  Windows
00b0  4e 54 20 31 30 2e 30 3b  20 57 4f 57 36 34 3b 20   NT 10.0;  WOW64;
00c0  54 72 69 64 65 6e 74 2f  37 2e 30 3b 20 2e 4e 45   Trident/ 7.0; .NE
```

Shell No. 1 | Shell No. 1 | Shell No. 1 | pcap | Wireshark · _ | 02:14 PM

Wireshark · Follow HTTP Stream (tcp.stream eq 724) · pcap

File Edit View Go

tcp.stream eq 724

No.	Time
58745	658.615056
58746	658.615975
58747	658.616839
58748	658.621258
58749	658.622127
58750	658.630781
58751	658.631653
58752	658.636633
58753	658.637670

Frame 58748: 275
Ethernet II, Src:
Internet Protocol
Transmission Cont
Hypertext Transfe

```
GET /pQBtWj HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-
Age=2678400;Path=/
Access-Control-Allow-Origin: *

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
```

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (564 kB) | Show and save data as ASCII

Find: | Find

Help | Filter Out This Stream | Print | Save as... | Back | Close

pcap

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?
    - This malware is classified as a .dll file that executes another .exe file called googleipdate.exe, as shown in the image below.

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
   - Host name: ROTTERDAM-PC
   - IP address: 172.16.4.205
   - MAC address: (00:59:07:b0:63:a4)

Bananas - Mozill...
Shell No. 1
pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.16.4.4 and kerberos.CNameString
No. Time Source Destination
3415 50.742235400 Rotterdam-PC.mind-hammer.net mind-hammer-dc.m
3197 49.831293000 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
3209 49.894459400 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
3250 50.135544700 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
3270 50.241859400 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
3378 50.627492100 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
3390 50.688223400 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
3417 50.770347900 mind-hammer-dc.mind-hammer.net Rotterdam-PC.min
Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:
Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
.... ..0. .... = LG bit: Globally unique address (fac
....0 .... = IG bit: Individual address (unicast)
Source: Dell_19:49:50 (a4:ba:db:19:49:50)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: mind-hammer-dc.mind-hammer.net (172.16.

pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.16.4.4 and kerberos.CNameString
No. Time Source Destination
3197 49.831293000 mind-hammer-dc.mind-hammer.net Rotterdam-PC.mi
3209 49.894459400 mind-hammer-dc.mind-hammer.net Rotterdam-PC.mi
3250 50.135544700 mind-hammer-dc.mind-hammer.net Rotterdam-PC.mi
3270 50.241859400 mind-hammer-dc.mind-hammer.net Rotterdam-PC.mi
3378 50.627492100 mind-hammer-dc.mind-hammer.net Rotterdam-PC.mi
[Reassembled TCP Data: 000006556d8206513082064da003020105a10302010da3
Kerberos
Record Mark: 1621 bytes
0... .... = Reserved: Not set
.000 0000 0000 0000 0000 0110 0101 0101 = Record Length: 1621
tgs-rep
pvno: 5
msg-type: krb-tgs-rep (13)
crealm: MIND-HAMMER.NET
cname
name-type: kRB5-NT-PRINCIPAL (1)
cname-string: 1 item
ticket

2. What is the username of the Windows user whose computer is infected?
    - The username of the Windows user whose computer is infected is matthijs.devries, as shown in the images below.

3. What are the IP addresses used in the actual infection traffic?
    - A packet size of -30344, coming from IPs 172.16.4.205 and 185.243.115.84, is considered suspicious, as 185.243.115.84 ties back to green.mattingsolutions.co, which, VirusTotal shows as a malicious URL.

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A
172.16.4.205	185.243.115.84	30,344	26 M	15,149	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	
172.16.4.4	172.16.4.205	1,417	339 k	680	
10.6.12.12	10.6.12.203	1,388	350 k	620	
10.6.12.12	10.6.12.157	1,316	330 k	608	
10.11.11.11	10.11.11.200	1,100	219 k	493	
10.0.0.2	10.0.0.201	1,083	266 k	520	
10.11.11.200	104.18.74.113	1,079	697 k	511	
10.11.11.11	10.11.11.203	843	189 k	351	
10.11.11.179	13.33.255.25	728	520 k	339	
31.13.70.52	172.16.4.205	726	479 k	436	
93.95.100.178	172.16.4.205	722	419 k	418	

File Action Media Clipboard View Help
Bana... Shell ... Shell ... pcap [Wire... Wires... Wires... Wires... 09:49 PM
pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 172.16.4.205 and ip.addr==185.243.115.84
Time Source Destination Protocol Length CNameString Info
13010 196.168142500 172.16.4.205 185.243.115.84 HTTP 126 POST /empty.…
13014 196.171971700 185.243.115.84 172.16.4.205 TCP 54 80 → 49249 […
13015 196.172857200 185.243.115.84 172.16.4.205 TCP 54 80 → 49249 […
13016 196.195438500 185.243.115.84 172.16.4.205 TCP 1411 80 → 49249 […
13017 196.218020100 185.243.115.84 172.16.4.205 TCP 1411 80 → 49249 […
13018 196.240629400 185.243.115.84 172.16.4.205 TCP 1411 80 → 49249 […
13019 196.242754800 185.243.115.84 172.16.4.205 TCP 135 80 → 49249 […
13020 196.265314700 185.243.115.84 172.16.4.205 TCP 1411 80 → 49249 […
13021 196.287901400 185.243.115.84 172.16.4.205 TCP 1411 80 → 49249 […
Source Port: 49249
Destination Port: 80
[Stream index: 87]
[TCP Segment Len: 72]
Sequence number: 493 (relative sequence number)
Sequence number (raw): 2570700152
[Next sequence number: 565 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1924424570

Bana... Shell ... Shell ... pcap
pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tool
ip.addr == 172.16.4.205 and ip.addr==185.243.115.84
Time Source Destination
13010 196.168142500 Rotterdam-PC.mind-hammer.net b5689023.gr
13014 196.171971700 b5689023.green.mattingsolutions.co Rotterdam-P
13015 196.172857200 b5689023.green.mattingsolutions.co Rotterdam-P
13016 196.195438500 b5689023.green.mattingsolutions.co Rotterdam-P
13017 196.218020100 b5689023.green.mattingsolutions.co Rotterdam-P
13018 196.240629400 b5689023.green.mattingsolutions.co Rotterdam-P
13019 196.242754800 b5689023.green.mattingsolutions.co Rotterdam-P
13020 196.265314700 b5689023.green.mattingsolutions.co Rotterdam-P
13021 196.287901400 b5689023.green.mattingsolutions.co Rotterdam-P
Source Port: 49249
Destination Port: 80
[Stream index: 87]
[TCP Segment Len: 72]
Sequence number: 493 (relative sequence number)
Sequence number (raw): 2570700152
[Next sequence number: 565 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1924424570

4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

> IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address 10.0.0.201:
    - MAC address: 00:16:17:18:66:c8
    - Windows username: elmer.blanco
    - OS version: Windows NT 10.0; Win64; x64

2. Which torrent file did the user download?
    - The torrent file `Betty_Boop_Rhythm_on_the_Reservation.avi.torrent` was downloaded by the user.

Wireshark · Follow TCP Stream (tcp.stream eq 943) · pcap
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: www.publicdomaintorrents.com
Connection: Keep-Alive
HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:27 GMT
Server: Apache
Content-Disposition: inline;
filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/x-bittorrent
204c
d8:announce53:http://files.publicdomaintorrents.com/bt/announce.php13:creation datei1129376933e4:infod6:lengthi105383936e4:name40:Betty_Boop_Rhythm_on_the_Reservation.avi12:piece lengthi262144e6:pieces8060:...6....j...f.z.....R...
1 client pkt, 7 server pkts, 1 turn.
Entire conversation (9,160 bytes)
Show and save data as ASCII
Stream 943
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox
https://www.virustotal.com/old-browsers/file/7e395128e0e194b54667bf066636
This is a minimal interface for browsers that do not support full-fledged VirusTotal
SHA256: 7e395128e0e194b54667bf066636362ac899fe553860c32d0049319ad46975a0
Name: btdownload.php%3ftype=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
Detection ratio: 0/72
Security vendor | Result | Update
tehtris | type-unsupported | 20220603
Alibaba | type-unsupported | 20190527
CrowdStrike | type-unsupported | -
SymantecMobileInsight | type-unsupported | 20220208
Elastic | type-unsupported | 20220520
APEX | type-unsupported | 20220601
Trustlook | type-unsupported | 20220603
Trapmine | type-unsupported | 20220526