

Network Analysis

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?

Domain name: frank-n- Ted-DC.frank-n-ted.com

The image shows a Wireshark network traffic capture. The top toolbar includes menus like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the toolbar is a filter bar with the expression `ip.addr == 10.6.12.0/24`. The main packet list shows several packets, with packet 68133 selected. A tooltip for packet 68133 shows 'Source address' pointing to the source IP 10.6.12.12. The packet details pane for packet 68133 shows the following structure:

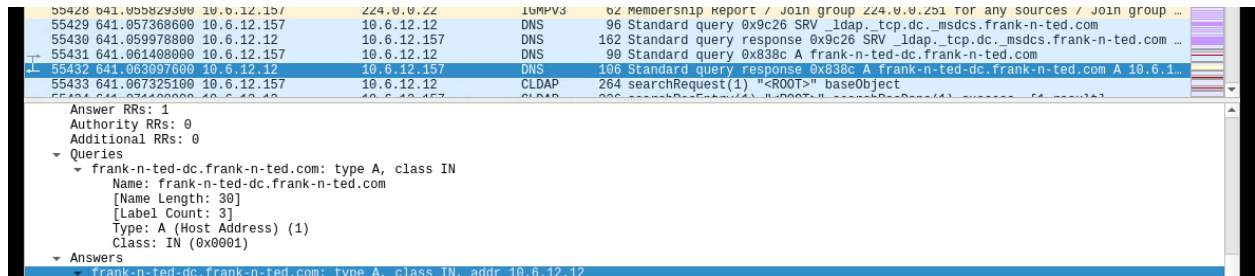
- Frame 68133: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0
- Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 10.6.12.12, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 67, Dst Port: 68
- Dynamic Host Configuration Protocol (ACK)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII column shows the following characters: `.....@-*.E.`

2. What is the IP address of the Domain Controller (DC) of the AD network?

Ip address: 10.6.12.12 frank-n- Ted-DC.frank-n-ted.com

Filter: ip.addr 10.6.12.0/24

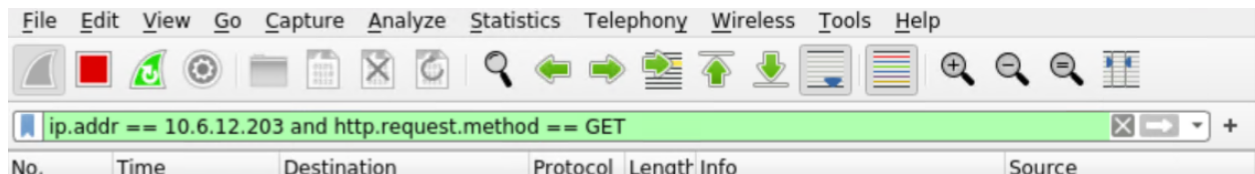


3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

File: june11.dll

Virus: Malware

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



4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?

This kind of malware is a TROJAN.

The screenshot shows the VirusTotal web interface. The browser's address bar displays the URL `https://www.virustotal.com/gui/url/e70c46b564e2c7a9d38f0f94cbfafbfb2d30/`. The page title is "VirusTotal - URL - e70c4". The main content area shows a URL analysis for `http://205.185.125.104/files/june11.dll`. A large red circle with the number "6" indicates that 6 security vendors have flagged this URL as malicious. Below this, a table displays the following information:

URL	Status	Content Type	Submission Date
<code>http://205.185.125.104/files/june11.dll</code>	404	text/html; charset=UTF-8	2021-11-28 21:25:51 UTC
<code>205.185.125.104</code>			5 months ago

The page also includes a "Community Score" section with a question mark icon, and tabs for "DETECTION", "DETAILS", and "COMMUNITY". The "DETAILS" tab is currently selected, showing categories, history, and HTTP response information.

Categories

Vendor	Category
Forcepoint ThreatSeeker	malicious web sites
Sophos	spyware and malware
Comodo Valkyrie Verdict	unknown
Webroot	Malware Sites

History

Event	Date
First Submission	2020-06-12 04:14:29 UTC
Last Submission	2021-11-28 21:25:51 UTC
Last Analysis	2021-11-28 21:25:51 UTC

HTTP Response

Final URL

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

Filter: ip.src==172.16.4.4 and kerberos.CNameString

The image shows a Wireshark network traffic capture. The filter bar at the top displays the filter: `ip.src==172.16.4.4 and kerberos.CNameString`. The packet list shows several Kerberos messages (AS-REP and TGS-REP) from source 172.16.4.4 to destination 172.16.4.205. The selected packet (No. 17266) is an AS-REP message. The packet details pane shows the following structure:

- Frame 17266: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface eth0, id 0
- Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
- Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
- Source: Dell_19:49:50 (a4:ba:db:19:49:50)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 190

The packet bytes pane shows the raw data of the packet, including the IP header and the beginning of the Kerberos message.

2. What is the username of the Windows user whose computer is infected?

Username: matthijs.devries

Filter: ip.src==172.16.4.205 and kerberos.CNameString

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
15556	149.848730300	172.16.4.205	172.16.4.4	KRB5	372	AS-REQ
15549	149.833181700	172.16.4.205	172.16.4.4	KRB5	292	AS-REQ
15517	149.706495400	172.16.4.205	172.16.4.4	KRB5	381	AS-REQ
15510	149.690858700	172.16.4.205	172.16.4.4	KRB5	301	AS-REQ
15340	148.910222300	172.16.4.205	172.16.4.4	KRB5	377	AS-REQ
15332	148.893035700	172.16.4.205	172.16.4.4	KRB5	297	AS-REQ

Transmission Control Protocol, Src Port: 49179, Dst Port: 88, Seq: 1, Ack: 1, Len: 318

Kerberos

- Record Mark: 314 bytes
- as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - padata: 2 items
 - req-body
 - padding: 0
 - kdc-options: 40810010
 - cname
 - name-type: KRB5-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: matthijs.devries
 - realm: MIND-HAMMER
 - sname

```

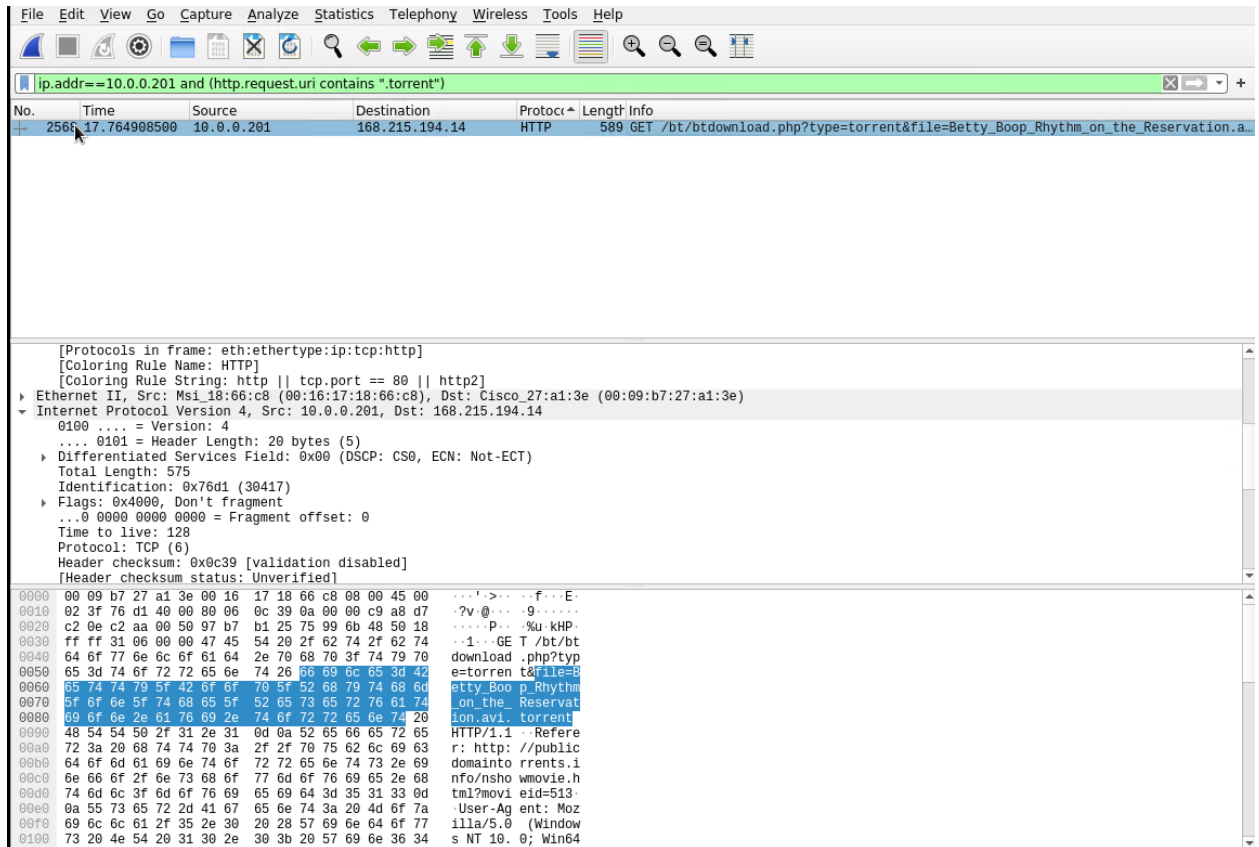
0070 c6 50 ed 05 f9 b1 ab 1f dd 87 19 78 aa e1 0a a7 .P.....x...
0080 fe eb 31 e9 f9 65 4b 8c e9 35 b7 b8 d1 e6 58 0c ..1..eK..5...X
0090 ba 78 7a e6 fc c9 1c 51 25 cf 9d 89 3f 3b 30 11 .xz....Q %...?;0
00a0 a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01 .....0...
00b0 ff a4 81 c0 30 81 bd a0 07 03 05 00 40 81 00 10 ....0...@...
00c0 a1 1d 30 1b a0 03 02 01 01 a1 14 30 12 1b 10 6d ..0.....0...m
00d0 61 74 74 68 69 6a 73 2e 64 65 76 72 69 65 73 atthijs.devries
00e0 0d 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 a3 20 ...MIND- HAMMER
00f0 30 1e a0 03 02 01 02 a1 17 30 15 1b 06 6b 72 62 0.....0...krb
0100 74 67 74 1b 0b 4d 49 4e 44 2d 48 41 4d 4d 45 52 tgt..MIN D-HAMMER
0110 a5 11 18 0f 32 30 33 37 30 39 31 33 30 32 34 38 ....2037 09130248
0120 30 35 5a a6 11 18 0f 32 30 33 37 30 39 31 33 30 05Z...2 03709130
0130 32 34 38 30 35 5a a7 06 02 04 25 a0 57 52 a8 15 24805Z...%.WR..
0140 30 13 02 01 12 02 01 11 02 01 17 02 01 18 02 02 0.....
0150 ff 79 02 01 03 a9 1d 30 1b 30 19 a0 03 02 01 14 .y.....0..0....

```

3. What are the IP addresses used in the actual infection traffic?

Ip address that infect traffic is 168.215.104.14

Filter: ip.addr==10.0.0.201 and (http.request.uri contains".torrent")



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
 - Windows username
 - OS version

2. Which torrent file did the user download?