

# Network Analysis

## Time Thieves

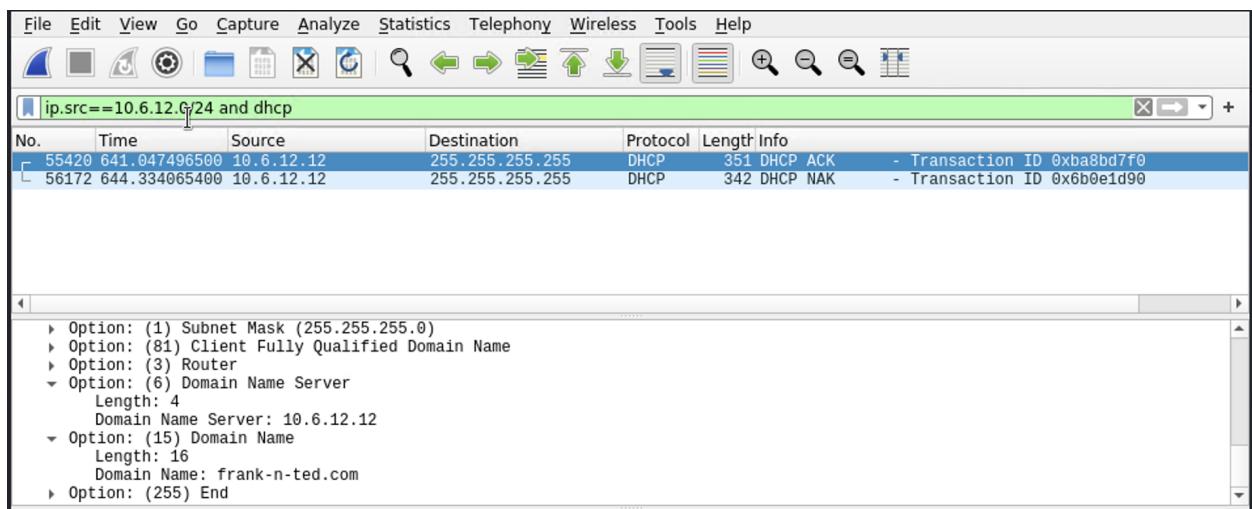
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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?

frank-n-ted.com



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

10.6.12.12

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.

## june11.dll

Screenshot of Wireshark showing network traffic for the IP address 10.6.12.203. The selected packet is a GET request to http://205.185.125.104/files/june11.dll.

```

Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
Host: 205.185.125.104\r\n
Connection: Keep-Alive\r\n
Cookie: _subid=3mmhfd8jp\r\n
[Full request URI: http://205.185.125.104/files/june11.dll]
[HTTP request 2/2]
[Prev request in frame: 58748]
[Response in frame: 59388]

```

Hex dump of the selected packet:

```

0000 ec c8 82 29 41 7d 84 3a 4b 6c e2 08 00 45 00 :...A) : Km...E
0010 01 2a ad fc 40 00 80 06 e9 d0 0a 06 0c cb cd b9 *...@...
0020 7d 68 c2 4b 00 50 04 1f 3f 3d 78 a3 51 8c 50 18 }h K P. ?=x Q P
0030 ff ff 34 1f 00 00 47 45 54 20 2f 66 69 6c 65 73 .4. GE T /files
0040 2f 6a 75 6e 65 31 31 2e 64 6c 6c 20 48 54 54 50 /june11. dll HTTP
0050 2f 31 2e 31 0d 0a 41 63 63 65 78 74 3a 20 2a 2f /1.1. Ac cept: */
0060 2a 0d 0a 41 63 63 65 70 74 2a 45 6e 63 6f 64 69 *. Accep t-Encodi
0070 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 ng: gzip , deflat
0080 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d e. User- Agent: M
0090 6f 7a 69 6c 6c 61 2f 34 2e 30 28 63 6f 6d 70 ozilla/4. 0 (comp
00a0 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 37 2e 30 atible; MSIE 7.0

```

Source or Destination Address: IPv4 address | Packets: 104286 · Displayed: 32 (0.0%) | Profile: Default

4. Upload the file to [VirusTotal.com](#). What kind of malware is this classified as?
- Based on the VirusTotal analysis vendors overwhelmingly identify this as a Trojan

VirusTotal analysis for file d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764d.

**53** / 68 security vendors flagged this file as malicious

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.Mint.Zamg.O		AhnLab-V3	① Malware/Win32.RL_Generic.R346613
Alibaba	① TrojanSpy:Win32/Yakes.56555f48		Antiy-AVL	① Trojan/Generic.ASCCommon.IBE
SecureAge APEX	① Malicious		Avast	① Win32:DangerousSig [Tr]

## 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

The Wireshark interface displays a list of network captures. The current capture is titled "ip.addr==172.16.4.205 and kerberos.CNameString". The packet list shows several KRB5 protocol entries, with the last one selected. The details pane shows the structure of the selected message:

- tgs-req**:
  - pvno: 5
  - msg-type: krb-tgs-req (13)
  - crealm: MIND-HAMMER.NET
- cname**:
  - name-type: KRB5-NT-PRINCIPAL (1)
  - cname-string: 1 item
    - CNameString: ROTTERDAM-PCS\$
- ticket**
- enc-part**

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

matthijs.devries

Frame 3417: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits) on interface eth0, id 0

Ethernet II, Src: Dell\_19:19:50 (a4:ba:db:19:49:50), Dst: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)

Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205

Transmission Control Protocol, Src Port: 88, Dst Port: 49179, Seq: 1461, Ack: 319, Len: 188

[2 Reassembled TCP Segments (1648 bytes): #3416(1460), #3417(188)]

Kerberos

- > Record Mark: 1644 bytes
  - 0... = Reserved: Not set
  - .000 0000 0000 0000 0110 0110 1100 = Record Length: 1644
- > as-rep
  - pvno: 5
  - msg-type: krb-as-rep (11)
  - > padata: 1 item
  - realm: MIND-HAMMER.NET
  - > cname
    - name-type: kRB5-NT-PRINCIPAL (1)
    - > cname-string: 1 item
    - CNameString: matthijs.devries
  - > ticket
  - > enc-part

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

31.7.62.214, 185.243.115.84, 166.62.111.64

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

2. Which torrent file did the user download?

Betty\_Boop\_Rhythm\_on\_the\_reservation.avi.torrent