

Network Analysis

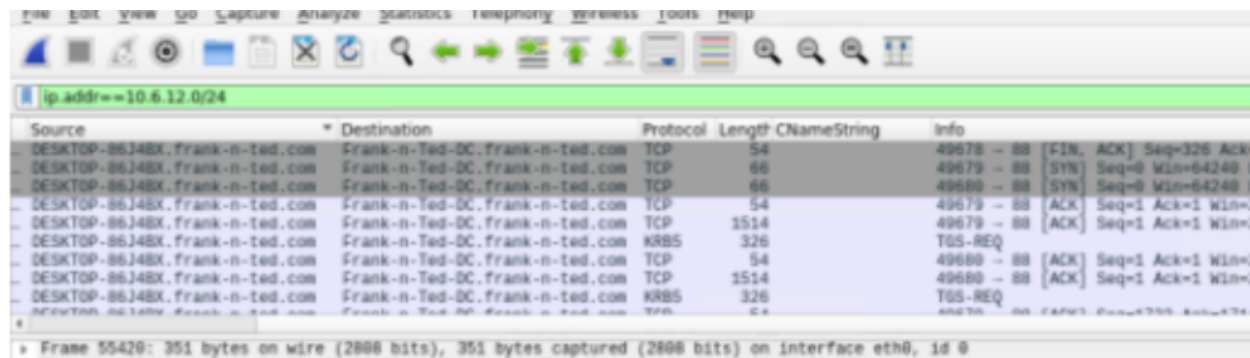
Time Thieves

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?
 - a. The domain name is Frank-n-Ted-DC.frank-n-ted.com
 - b. ip.addr==10.6.12.0/24



2. What is the IP address of the Domain Controller (DC) of the AD network?
 - a. IP of the domain Frank-n-Ted-DC.frank-n-ted.com
 - i. : 10.6.12.12

```

Internet Protocol Version 4, Src: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 337
  Identification: 0x3880 (14464)
  > Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0xeb0a [validation disabled]
  [Header checksum status: Unverified]
  Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)

```

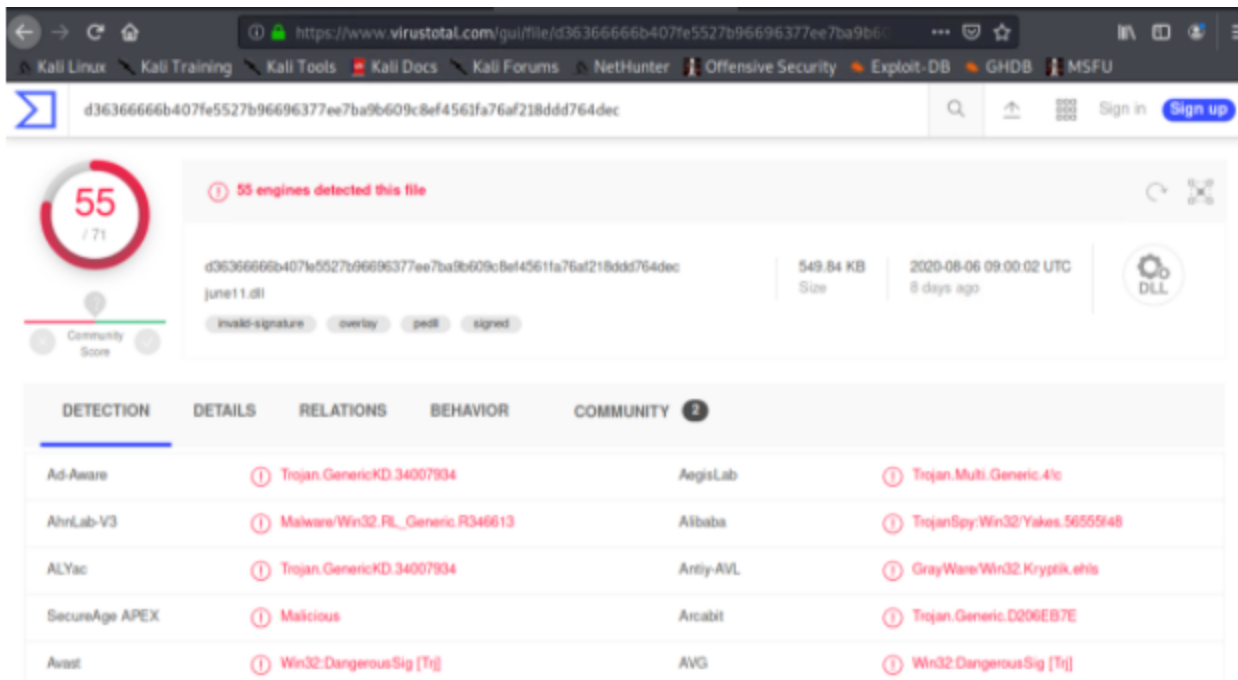
b.

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.

- a. Malware file is june11.dll
- b. ip.addr==10.16.12.302 and http.request.method==GET
 - i. File
 - ii. Export object
 - iii. HTTP...

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

- a. Trojan



The screenshot shows the VirusTotal.com interface for a file upload. The file is identified as 'june11.dll' with a size of 549.84 KB, uploaded on 2020-08-06 09:00:02 UTC. A red circle indicates that 55 out of 71 engines detected the file as malicious. The file is classified as a Trojan. Below the summary, a table lists the detection results from various security engines.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.GenericKD.34007904	AegisLab	① Trojan.Multi.Generic.4/c	
AhrLab-V3	① Malware/Win32.PIL.Generic.R346613	Alibaba	① TrojanSpy/Win32/Yakes.5655548	
ALYac	① Trojan.GenericKD.34007904	Antiy-AVL	① GrayWare/Win32.Kryptik.ehls	
SecureAge APEX	① Malicious	Arcabit	① Trojan.Generic.D206EB7E	
Avast	① Win32:DangerousSig [Trj]	AVG	① Win32:DangerousSig [Trj]	

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

2. What is the username of the Windows user whose computer is infected?
 - Matthijs.devries
 -
3. What are the IP addresses used in the actual infection traffic?
 - 172.16.4.205
 - 185.243.115.84
 - 166.62.11.64
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: BLANCO-DESKTOP

2. Which torrent file did the user download?

- File name: Betty_Boop_Rythm_on_the_Reservation.avi.torrent