Network Analysis

Time Thieves

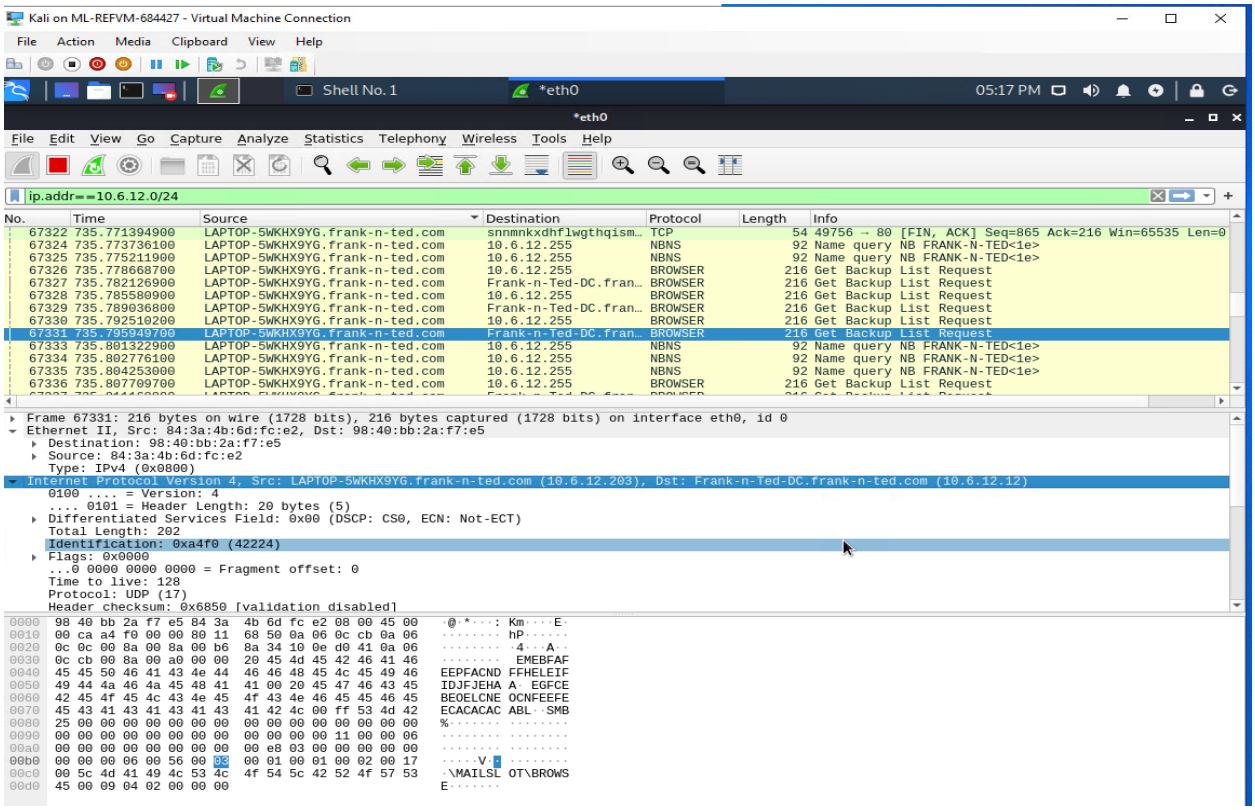
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- 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`.

What is the domain name of the users' custom site?

Frank-n-Ted-DC.frank-n-ted.com

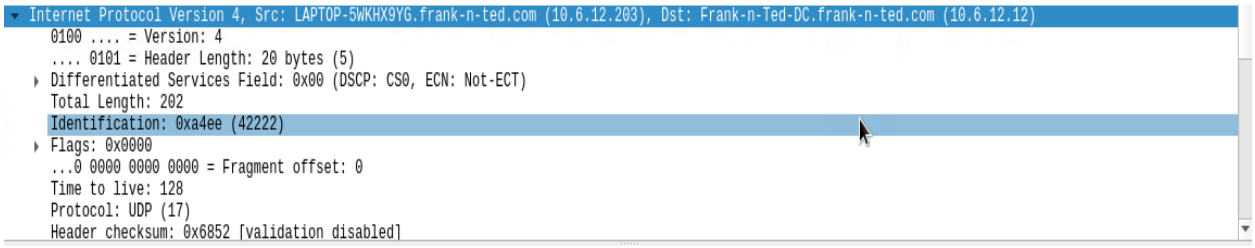
Filter: ip.addr==10.6.12.0/24



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

IP address is 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)

Filter: ip.addr==10.6.12.0/24

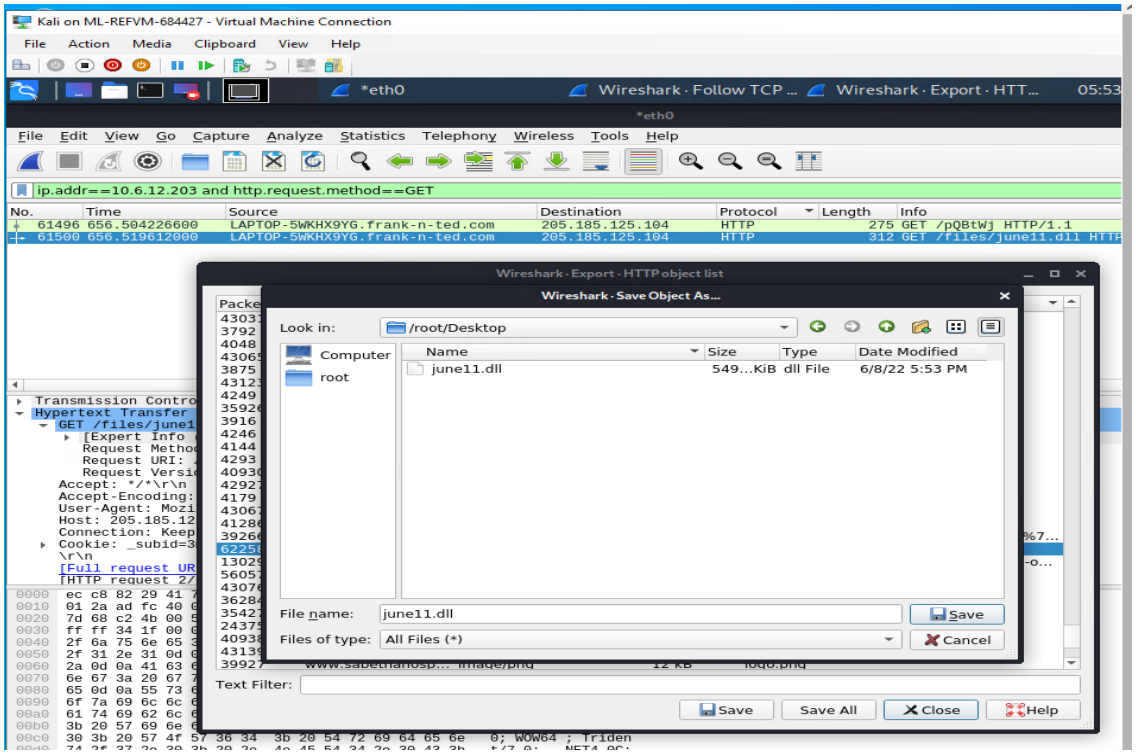


What is the name of the malware downloaded to the `10.6.12.203` machine? Once you have found the file, export it to your Kali machine's desktop.

Malware file is june11.dll.

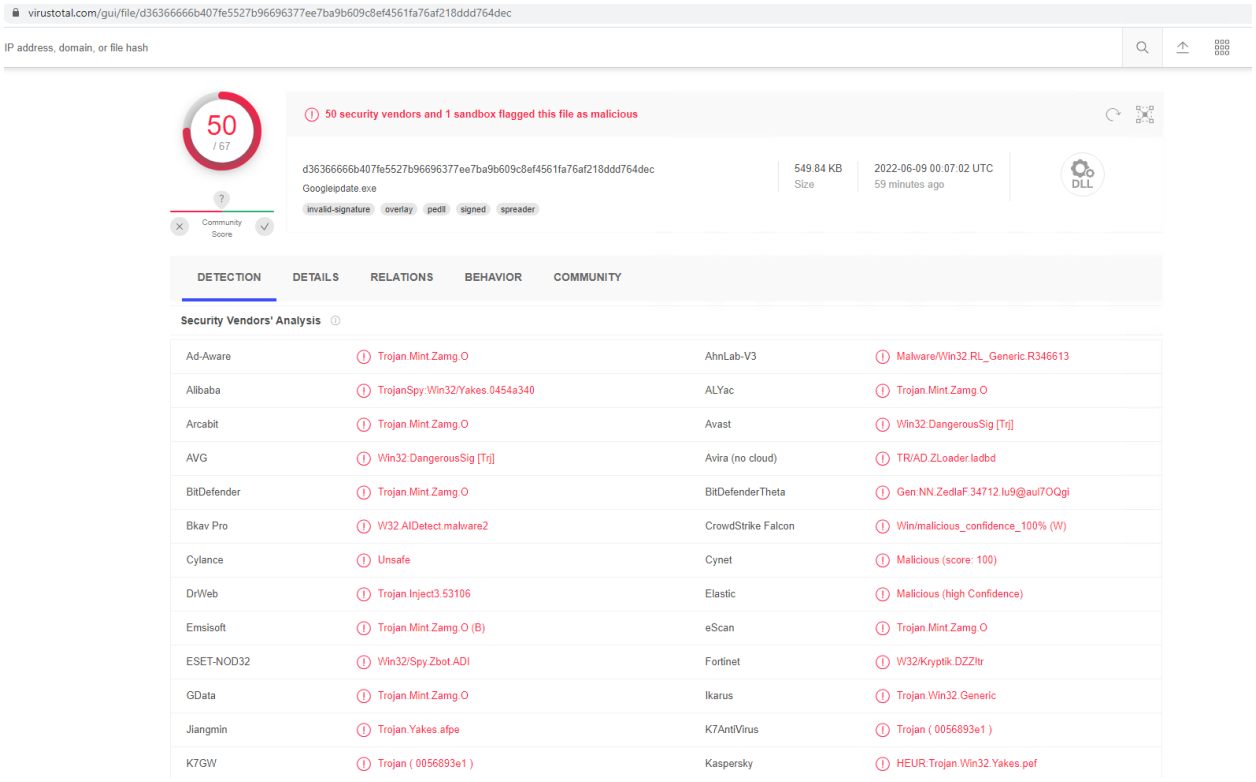
Filter: ip.addr==10.16.12.203 and http.request.method==GET

Export: File > Export Objects > HTTP



Upload the file to VirusTotal.com. What kind of malware is this classified as?

This type of malware is classified as a Trojan.



Vulnerable Windows Machines

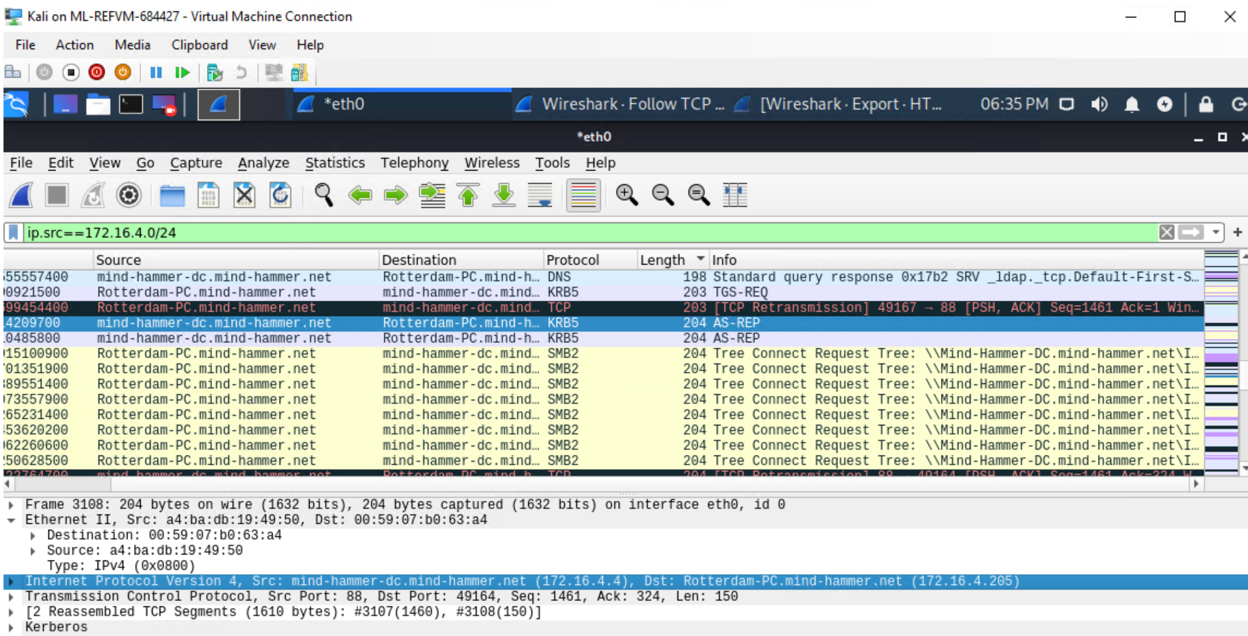
The Security team received reports of an infected Windows host on the network. They know the following:

- 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**

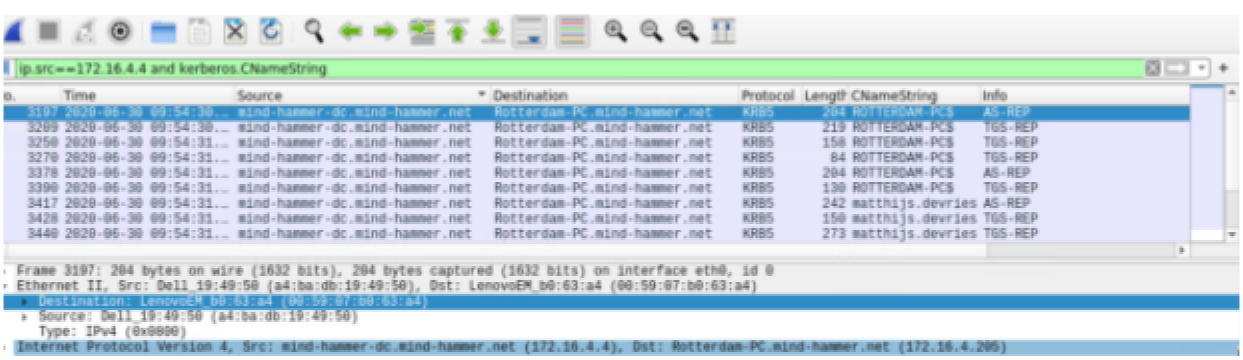
- **Screenshot evidence:**



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

The username is matthijs.devries.

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



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

Based on the Conversations statistics and then filtering by the highest number of packets between IPs, 172.16.4.205, 185.243.115.84, 166.62.11.64 are the infected traffic.

Referencing 185.243.115.84 (b569023.green.mattingsolutions.co) there is a large amount of POST methods of empty.gif being sent without any originating GET request. This is suspicious and odd.

Statistics > Conversations > IPv4 (tab) > Packets (high to low)

Filter: ip.addr==172.16.4.205 and ip.addr==185.243.115.84