

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

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, filtered by 'ip.addr==10.6.12.0/24'. The middle pane shows the details of the selected packet (No. 67331), which is an Internet Protocol Version 4 (IPv4) packet. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
67322	735.771394900	LAPTOP-5WKHX9YG.frank-n-ted.com	snmknxdhflwgtqism...	TCP	54	49756 → 80 [FIN, ACK] Seq=865 Ack=216 Win=65535 Len=0
67324	735.773736100	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	NBNS	92	Name query NB FRANK-N-TED<1e>
67325	735.775211900	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	NBNS	92	Name query NB FRANK-N-TED<1e>
67326	735.778668700	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	BROWSER	216	Get Backup List Request
67327	735.782126900	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.fran...	BROWSER	216	Get Backup List Request
67328	735.785586900	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	BROWSER	216	Get Backup List Request
67329	735.789036800	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.fran...	BROWSER	216	Get Backup List Request
67330	735.792510200	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	BROWSER	216	Get Backup List Request
67331	735.801322900	LAPTOP-5WKHX9YG.frank-n-ted.com	Frank-n-Ted-DC.fran...	BROWSER	216	Get Backup List Request
67334	735.802776100	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	NBNS	92	Name query NB FRANK-N-TED<1e>
67335	735.804253000	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	NBNS	92	Name query NB FRANK-N-TED<1e>
67336	735.807709700	LAPTOP-5WKHX9YG.frank-n-ted.com	10.6.12.255	BROWSER	216	Get Backup List Request

Frame 67331: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface eth0, id 0

Ethernet II, Src: 84:3a:4b:6d:fc:e2, Dst: 98:40:bb:2a:f7:e5

Destination: 98:40:bb:2a:f7:e5

Source: 84:3a:4b:6d:fc:e2

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 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: 202

Identification: 0xa4f0 (42224)

Flags: 0x0000

... 0 0000 0000 0000 = Fragment offset: 0

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x6850 [validation disabled]

0000 98 40 bb 2a f7 e5 84 3a 4b 6d fc e2 08 00 45 00 .@...: Km...E

0010 00 ca a4 f0 00 00 11 68 50 0a 06 0c cd 0a 06 nP...

0020 0c 0c 00 8a 00 8a 00 b6 8a 34 10 0e d0 41 0a 06 4...A...

0030 0c cb 00 8a 00 a0 00 00 29 45 4d 45 42 46 41 46 EMEBFAC

0040 45 45 50 46 41 43 4e 44 46 46 48 45 4c 45 49 46 EEPFACND FFHELEIF

0050 49 44 4a 46 4a 45 48 41 41 00 20 45 47 46 43 45 IDJFJEHA A EGFCE

0060 42 45 4f 45 4c 43 4e 45 4f 43 4e 46 45 45 46 45 BEOELNE OCNFEFE

0070 45 43 41 43 41 43 41 43 41 42 4c 00 ff 53 4d 42 ECACACAC ABL SMB

0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %.....

0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 06

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00b0 00 00 00 06 00 56 00 00 01 00 01 00 02 00 17V

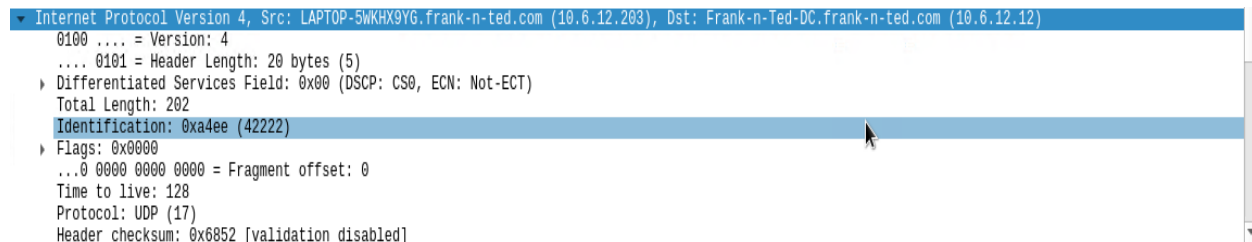
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53 .\MAILSL OT\BROWS

00d0 45 00 09 04 02 00 00 00 E.....

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

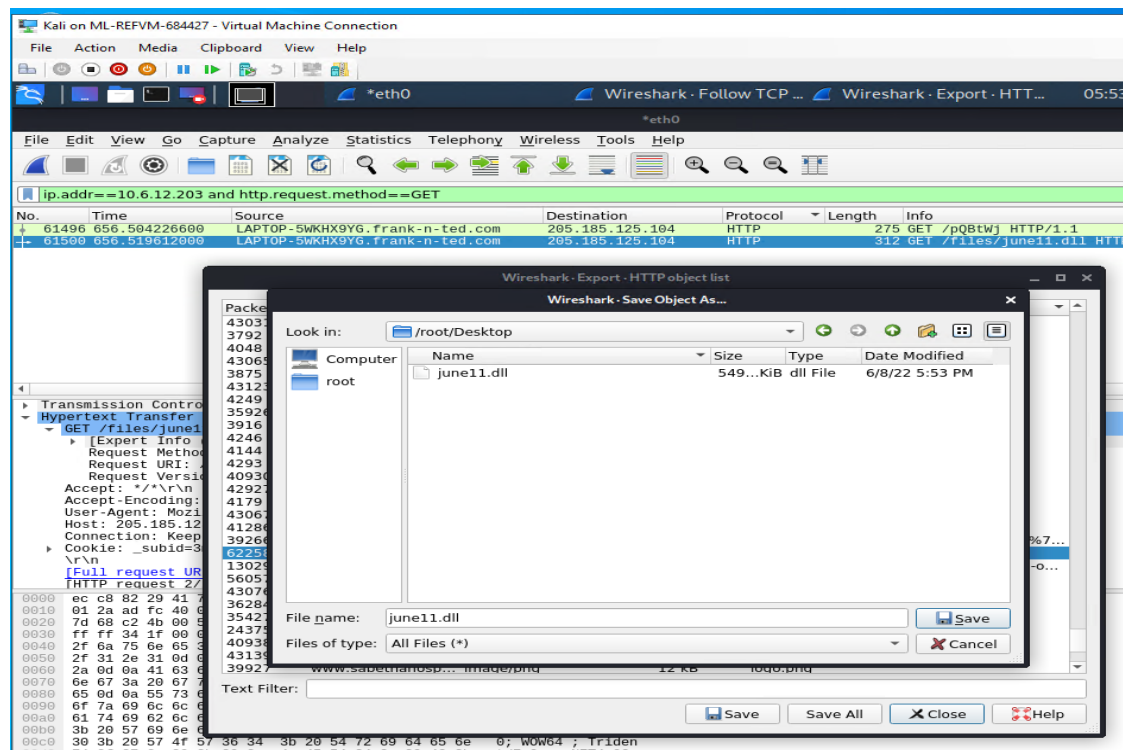


What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

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](https://www.virustotal.com). What kind of malware is this classified as?

This type of malware is classified as a Trojan.

virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

IP address, domain, or file hash

50 / 67

50 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Googleipdate.exe

549.84 KB
Size

2022-06-09 00:07:02 UTC
59 minutes ago

invalid-signature overlay pedt signed spreader

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL.Generic.R346613
Alibaba	TrojanSpy.Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Arcabit	Trojan.Mint.Zamg.O	Avast	Win32.DangerousSig [Trj]
AVG	Win32.DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen.NN.ZedlaF.34712.lu9@au170Qgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Inject3.53106	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Mint.Zamg.O (B)	eScan	Trojan.Mint.Zamg.O
ESET-NOD32	Win32/Spy.Zbot.ADI	Fortinet	W32/Kryptik.DZZlr
GData	Trojan.Mint.Zamg.O	Ikarus	Trojan.Win32.Generic
Jiangmin	Trojan.Yakes.afpe	K7AntiVirus	Trojan (0056893e1)
K7GW	Trojan (0056893e1)	Kaspersky	HEUR:Trojan.Win32.Yakes.pdf

Vulnerable Windows Machines

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

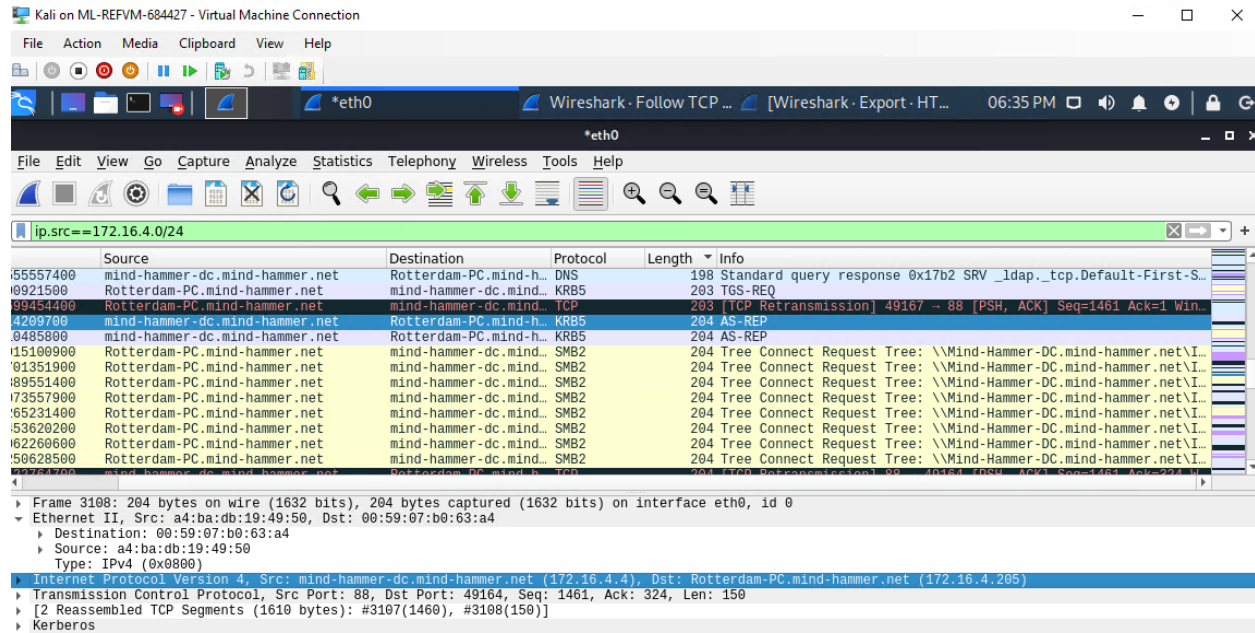
- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

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

