

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

```
Create Response File: frank-n-ted.com\Policies\{31B2F3:
GetInfo Response
GetInfo Response
Read Response
Create Response File: frank-n-ted.com\Policies\{31B2F3:
```

2. What is the IP address of the Domain Controller (DC) of the AD network?
10.6.12.12

04309	139.43/189900	10.6.12.12	10.6.12.197	DNS	188	Standard query response 0x1080 A CLIENT.WIN5.WINDOWS.COM
64891	738.57/882400	10.6.12.12	10.6.12.255	BROWSER	243	Host Announcement FRANK-N-TED-DC, Workstation, Server, b
64892	720.572/62400	10.6.12.12	10.6.12.255	ICMP	55	1760 Keep-Alive 445 40245 74631 Seq=2440 Ack=5260 Hu

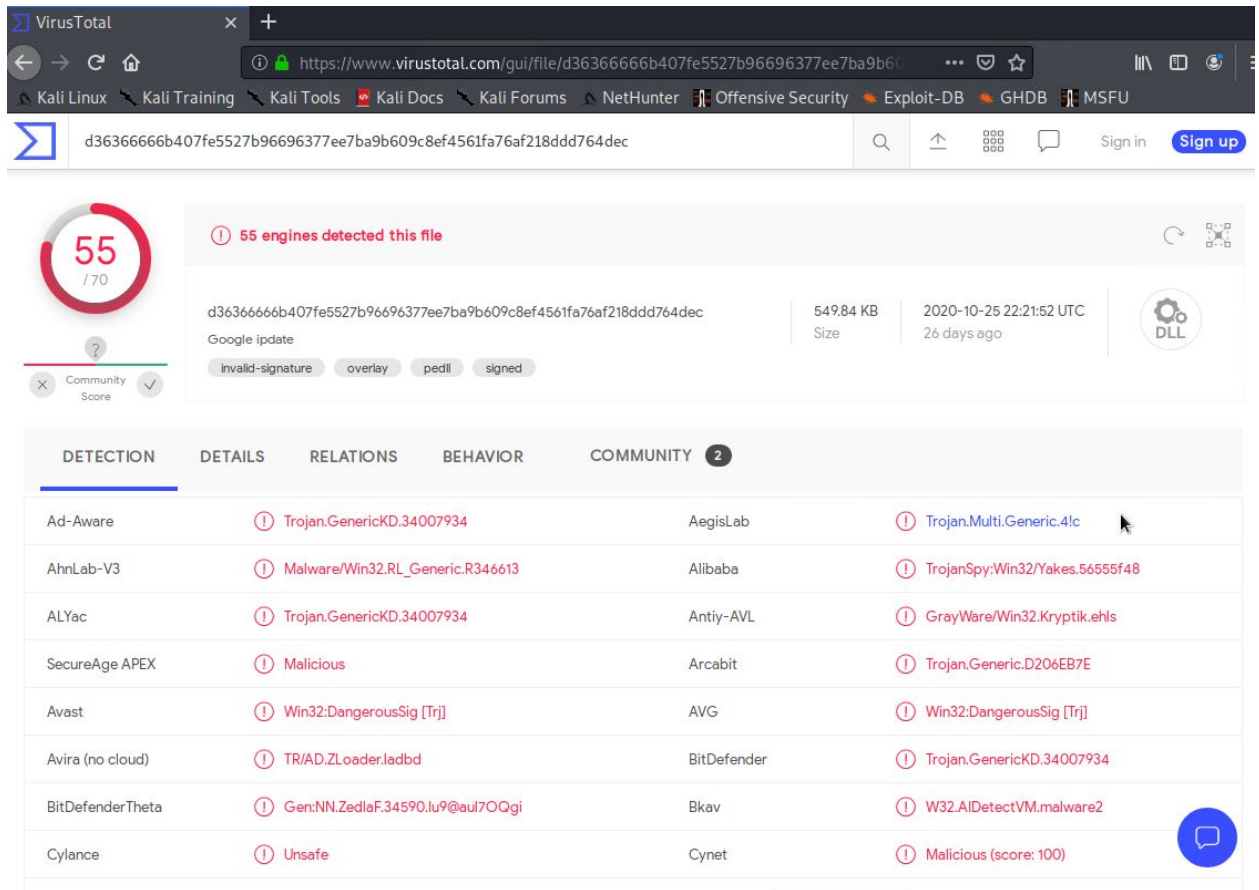
3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

june11.dll

57913	cardboardspaceshiptoy.com	text/html	241 bytes	invoice-8043
59388	205.185.125.104	application/octet-stream	563 kB	june11.dll
59690	enmkxdkhflwathairmk.com	text/html	205 bytes	next.php

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

Looks to be a type of trojan



VirusTotal

https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

55 / 70

55 engines detected this file

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2020-10-25 22:21:52 UTC 26 days ago

Google update

invalid-signature overlay pedl signed

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 2
Ad-Aware	Trojan.GenericKD.34007934	AegisLab	Trojan.Multi.Generic.4lc	
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48	
ALYac	Trojan.GenericKD.34007934	Antiy-AVL	GrayWare/Win32.Kryptik.ehls	
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D206EB7E	
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]	
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.GenericKD.34007934	
BitDefenderTheta	Gen:NN.ZedlaF.34590.lu9@aui7OQgi	Bkav	W32.AIDetectVM.malware2	
Cylance	Unsafe	Cynet	Malicious (score: 100)	

Vulnerable Windows Machines

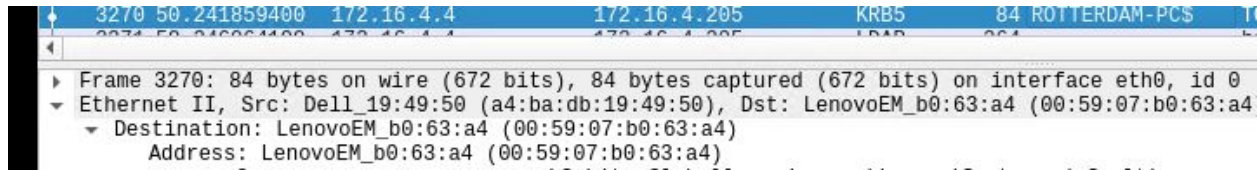
The Security team received reports of an infected Windows host on the network. They know the following:

- 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

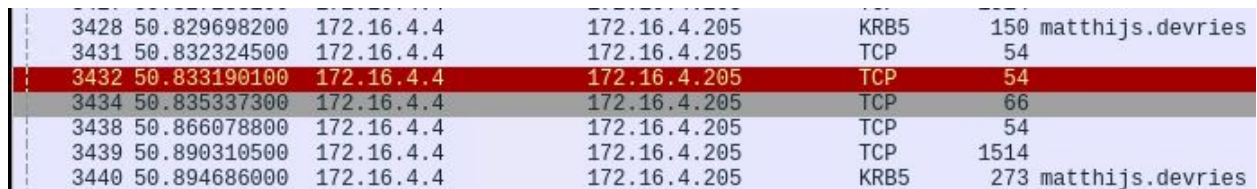


Wireshark packet capture details for frame 3270. The packet is an Ethernet II frame with source MAC Dell_19:49:50 (a4:ba:db:19:49:50) and destination MAC LenovoEM_b0:63:a4 (00:59:07:b0:63:a4). The destination address is also listed as LenovoEM_b0:63:a4 (00:59:07:b0:63:a4).

No.	Time	Source	Destination	Protocol	Length	Info
3270	50.241859400	172.16.4.4	172.16.4.205	KRB5	84	ROTTERDAM-PCS

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

Matthijs.devries



Wireshark packet capture list showing traffic to and from 172.16.4.205. The highlighted packet is frame 3432, which is a TCP packet from 172.16.4.4 to 172.16.4.205 on port 54.

No.	Time	Source	Destination	Protocol	Length	Info
3428	50.829698200	172.16.4.4	172.16.4.205	KRB5	150	matthijs.devries
3431	50.832324500	172.16.4.4	172.16.4.205	TCP	54	
3432	50.833190100	172.16.4.4	172.16.4.205	TCP	54	
3434	50.835337300	172.16.4.4	172.16.4.205	TCP	66	
3438	50.866078800	172.16.4.4	172.16.4.205	TCP	54	
3439	50.890310500	172.16.4.4	172.16.4.205	TCP	1514	
3440	50.894686000	172.16.4.4	172.16.4.205	KRB5	273	matthijs.devries

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

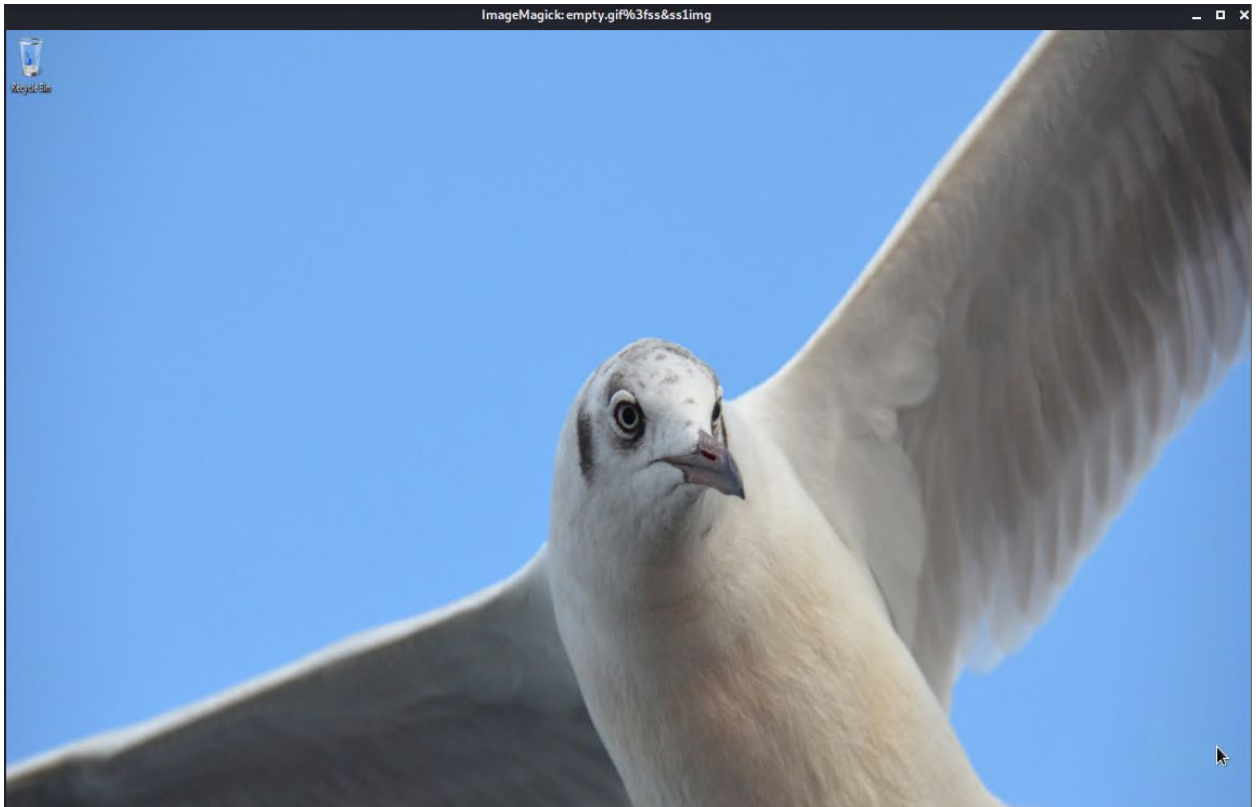
185.243.115.84

172.16.4.205

31.7.62.214

172.16.4.4

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 blanco-desktop

- OS version Windows 10

The image shows a Wireshark packet capture. The top pane displays a list of packets, including several KRB5 messages and TCP segments. The bottom pane shows the details of a selected frame (Frame 65526), indicating it is 381 bytes on wire and captured on interface eth0. The Ethernet II details show the source as Msi_18:66:c8 and the destination as Dell_f4:3b:96. The HTTP details show the User-Agent as Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134.

2. Which torrent file did the user download?

The image shows the 'Wireshark - Export - HTTP object list' window. It displays a table of resources downloaded from publicdomaintorrents.info. The table includes columns for Packet, Hostname, Content Type, Size, and Filename. The resources include various JavaScript files, images, and fonts. The 'Text Filter' field is empty, and the 'Save' button is highlighted.

Packet	Hostname	Content Type	Size	Filename
41679	www.googletagmanager.com	text/javascript	52 kB	gpt.js
67384	publicdomaintorrents.info	image/jpeg	1,764 bytes	googlevid.jpg
4020	mysocalledchaos.com	application/javascript	1,266 bytes	global.js?ver=1
3921	mysocalledchaos.com	application/javascript	945 bytes	gingeranalytics
38751	www.sabethahospital.com	text/html	37 kB	getpage.php?n
5072	pixel.wp.com	image/gif	50 bytes	g.gif?v=ext&js=
49925	djnf6e5yirys.cloudfront.net	application/javascript	122 kB	friendbuy.min.js
35198	img.timeinc.net	application/javascript	319 bytes	frequency_capp
41593	www.iphonehacks.com	application/javascript	91 kB	foundation.min
4768	mysocalledchaos.com	font/woff2	77 kB	fontawesome-w
42023	www.iphonehacks.com	application/octet-stream	71 kB	fontawesome-w
3713	maxcdn.bootstrapcdn.com	text/css	31 kB	font-awesome.r
3846	mysocalledchaos.com	text/css	31 kB	font-awesome.r
41350	www.iphonehacks.com	text/css	29 kB	font-awesome.r
38994	www.sabethahospital.com	text/css	30 kB	font-awesome.r
6463	mysocalledchaos.com	image/jpeg	389 kB	fleshy-in-this-2
35091	img.timeinc.net	text/css	21 kB	fixed-header-f
12409	ball.dardavies.com	image/png	6,069 bytes	firefox.png
12893	ball.dardavies.com	image/x-icon	5,430 bytes	firefox.ico
37168	fonts.timeinc.net	application/font-woff2	11 kB	fc4554834092c
53967	www.iphonehacks.com	image/png	569 bytes	favicon.png
67813	publicdomaintorrents.info	image/x-icon	3,638 bytes	favicon.ico
53966	www.iphonehacks.com	image/x-icon	1,150 bytes	favicon.ico
41306	img.timeinc.net	image/x-icon	1,150 bytes	favicon.ico
41000	www.sabethahospital.com	text/plain	894 bytes	favicon.ico
32471	31.7.62.214	application/x-www-form-urlencoded	36 bytes	fakeurl.htm
32469	31.7.62.214	application/x-www-form-urlencoded	36 bytes	fakeurl.htm

22	publicdomaintorrents.info	image/gif	916 bytes	yellow-star.gif
66	publicdomaintorrents.info	text/html	281 bytes	usercomments.html?movieid=513
27	publicdomaintorrents.info	image/gif	10 kB	srsbanner.gif
24	publicdomaintorrents.info	image/gif	2,708 bytes	rentme.gif
63	publicdomaintorrents.info	image/gif	572 bytes	psp.gif
30	publicdomaintorrents.info	image/jpeg	19 kB	pdheader.jpg
67	publicdomaintorrents.info	image/jpeg	910 bytes	pda.jpg
65	publicdomaintorrents.info	text/html	10 kB	nshowmovie.html?movieid=513
06	publicdomaintorrents.info	text/html	16 kB	nshowcat.html?category=animation
64	publicdomaintorrents.info	image/jpeg	517 bytes	ipod.jpg
58	publicdomaintorrents.info	image/png	7,922 bytes	hdsale.png
84	publicdomaintorrents.info	image/jpeg	1,764 bytes	googlevid.jpg
13	publicdomaintorrents.info	image/x-icon	3,638 bytes	favicon.ico
26	publicdomaintorrents.info	image/jpeg	568 bytes	divxi.jpg
17	publicdomaintorrents.info	image/jpeg	152 kB	bettyboopyrthmonthereservationgrab.jpg



btdownload.php%3
ftype=torrent&file
=Betty_Boop_Rhyt
hm_on_the_Reser
vation.avi.torrent