

# 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](http://Frank-n-ted.com)

The image shows a Wireshark network traffic capture. The top pane displays a list of packets, with packet 65187 selected. The bottom pane shows the details of this packet, which is an LDAP search response. The details pane is expanded to show the 'LDAPMessage' section, which contains a 'searchResDone' entry. The 'searchResDone' entry includes a 'NameErr' (DSID: 03100288, problem 2001 (NO\_OBJECT), data 0, best match of: 'CN=Services,CN=Configuration,DC=frank-n-ted,DC=com'). The bottom pane also shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	CNameString	crealm	Info
65171	742.4195457...	10.6.12.203	10.6.12.12	LDAP	207			SASL GSS-API Integrity: sear
65172	742.4224931...	10.6.12.12	10.6.12.203	LDAP	184			SASL GSS-API Integrity: sear
65173	742.4257098...	10.6.12.203	10.6.12.12	LDAP	201			SASL GSS-API Integrity: sear
65174	742.4295032...	10.6.12.12	10.6.12.203	LDAP	237			SASL GSS-API Integrity: sear
65179	742.4655727...	10.6.12.203	10.6.12.12	LDAP	553			bindRequest(9) "<ROOT>" sasl
65181	742.4706343...	10.6.12.12	10.6.12.203	LDAP	264			bindResponse(9) success
65182	742.4728778...	10.6.12.203	10.6.12.12	LDAP	140			SASL GSS-API Integrity: sear
65185	742.5251066...	10.6.12.12	10.6.12.203	LDAP	234			SASL GSS-API Integrity: sear
65187	742.5303135...	10.6.12.203	10.6.12.12	LDAP	274			SASL GSS-API Integrity: sear
65188	742.5351174...	10.6.12.12	10.6.12.203	LDAP	390			SASL GSS-API Integrity: sear
65189	742.5366810...	10.6.12.203	10.6.12.12	LDAP	97			SASL GSS-API Integrity: unbi
65193	742.5408086...	10.6.12.203	10.6.12.12	LDAP	97			SASL GSS-API Integrity: unbi

Details of packet 65187 (LDAP):

- krb5\_blob: 050405ff000c000c000000003fb2ff1b489337005a2d4723...
- krb5\_tok\_id: KRB\_TOKEN\_CFX\_WRAP (0x0405)
- krb5\_cfx\_flags: 0x05, AcceptorSubkey, SendByAcceptor
- krb5\_filler: ff
- krb5\_cfx\_ec: 12
- krb5\_cfx\_rrc: 12
- krb5\_cfx\_seq: 1060695323
- krb5\_sgn\_cksum: 489337005a2d4723db1ed8cc
- GSS-API payload (214 bytes)
- LDAPMessage searchResDone(11) noSuchObject (00002080: NameErr: DSID=03100288, problem 2001 (NO\_OBJECT), data 0, best match of: 'CN=Services,CN=Configuration,DC=frank-n-ted,DC=com')
- [1 result]
- messageID: 11
- protocolOp: searchResDone (5)
- [Response To: 65187]

Raw packet data (hex):

```
0000 84 3a 4b 6d fc e2 98 40 bb 2a f7 e5 08 00 45 00  --:Km...@...E-
0010 01 1e 50 66 40 00 80 06 7c 91 0a 06 0c 0c 0a 06  --Pf@...|.....
0020 0c 0b 01 85 c2 6c 4c 83 9e fe c9 8d 6e 9c 50 18  --...1L...n-P-
0030 20 13 61 4b 00 00 00 00 00 f2 05 04 05 ff 00 0c  --aK.....
0040 00 0c 00 00 00 00 3f b2 ff 1b 48 93 37 00 5a 2d  --...?...H-7-Z-
0050 47 23 db 1e d8 cc 30 84 00 00 00 d0 02 01 0b 65  --G@...0.....e
0060 84 00 00 00 c7 0a 01 20 04 32 43 4e 3d 53 65 72  --.....2CN=Ser
0070 76 69 63 65 73 2c 43 4e 3d 43 6f 6e 66 69 67 75  --vices,CN=Configu
0080 72 61 74 69 6f 6e 2c 44 43 3d 66 72 61 6e 6b 2d  --ration,D C=frank
0090 6e 2d 74 65 64 2c 44 43 3d 63 6f 6d 04 84 00 00  --n-ted,DC=com...
00a0 00 8a 30 30 30 30 32 30 38 44 3a 20 4e 61 6d 65  --000020 80: Name
00b0 45 77 77 3a 20 44 53 40 44 7d 30 33 31 30 30 37  --Frr: NST D-031002
```

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

The image shows a Wireshark packet capture window with the filter 'ip.addr == 10.6.12.203'. The packet list shows several packets, with packet 58752 selected. The packet details pane shows the following structure:

- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (258 bytes)
- Hypertext Transfer Protocol
  - GET /files/june11.dll HTTP/1.1\r\n
    - [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
    - Request Method: GET
    - Request URI: /files/june11.dll
    - Request Version: HTTP/1.1
    - Accept: \*/\*\r\n
    - Accept-Encoding: gzip, deflate\r\n

The packet bytes pane shows the raw data of the selected packet, including the HTTP request line and headers.

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

Trojan

VirusTotal - File - d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec - Mozilla Firefox

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

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

49 / 67

49 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB Size

2021-08-28 17:19:13 UTC 1 month ago

GoogleIpdate.exe

invalid-signature overlay pedll signed

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	SecureAge APEX	Malicious
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34110.lu9@aul7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100%
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

The screenshot shows the Wireshark network protocol analyzer interface. At the top, the IP address is set to 172.16.4.4. The interface is divided into three main panes:

- Packet List Pane (Top):** Displays a list of captured packets. The selected packet is number 14045, which is a TGS-REP message from 172.16.4.4 to 172.16.4.4. The packet details show it is a Kerberos (KRB5) message of type 206 (TGS-REP) with a length of 130 bytes.
- Packet Details Pane (Middle):** Provides a hierarchical view of the selected packet's structure. It shows the following fields:
  - msg-type:** krb-tgs-rep (13)
  - crealm:** MIND-HAMMER.NET
  - cname:**
    - name-type:** kRB5-NT-PRINCIPAL (1)
    - cname-string:** 1 item (matthijs.devries)
  - ticket:**
    - tki-vno:** 5
    - realm:** MIND-HAMMER.NET
    - sname:**
    - enc-part:**
- Packet Bytes Pane (Bottom):** Shows the raw hexadecimal and ASCII data of the selected packet. The data starts with 7c 11 0e 4f 42 b7 cd 9e da 2d 7f fe 76 df a6 01 and continues with various hexadecimal values.

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?

**185.243.115.84, 166.62.11.64, 172.16.4.205**

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**

ip.addr == 10.0.0.2								
Interface	Channel		802.11 Preferences					
No.	Time	Source	Destination	Protocol	Length	CNameString	crealm	Info
67080	751.37958...	10.0.0.2	10.0.0.201	KRB5	383	elmer.blanco	DOGOFtheyear...	TGS-REP
67058	751.29473...	10.0.0.2	10.0.0.201	KRB5	175	elmer.blanco	DOGOFtheyear...	TGS-REP
67046	751.23386...	10.0.0.2	10.0.0.201	KRB5	237	elmer.blanco	DOGOFtheyear...	AS-REP
67044	751.20583...	10.0.0.201	10.0.0.2	KRB5	370	elmer.blanco		AS-REQ
67036	751.19028...	10.0.0.201	10.0.0.2	KRB5	290	elmer.blanco		AS-REQ
65725	744.60148...	10.0.0.201	10.0.0.2	KRB5	382	blanco-desktop\$		AS-REQ
65712	744.57281...	10.0.0.201	10.0.0.2	KRB5	301	blanco-desktop\$		AS-REQ
65625	744.25567...	10.0.0.201	10.0.0.2	KRB5	381	blanco-desktop\$		AS-REQ
65617	744.23944...	10.0.0.201	10.0.0.2	KRB5	301	blanco-desktop\$		AS-REQ
65544	743.88410...	10.0.0.201	10.0.0.2	KRB5	382	blanco-desktop\$		AS-REQ
65530	743.83619...	10.0.0.201	10.0.0.2	KRB5	301	blanco-desktop\$		AS-REQ
65526	743.82838...	10.0.0.201	10.0.0.2	KRB5	381	blanco-desktop\$		AS-REQ

  

[Coloring Rule Name: TCP]  
[Coloring Rule String: tcp]  
- Ethernet II, Src: Dell\_f4:3b:96 (00:12:3f:f4:3b:96), Dst: Msi\_18:66:c8 (00:16:17:18:66:c8)  
- Destination: Msi\_18:66:c8 (00:16:17:18:66:c8)  
Address: Msi\_18:66:c8 (00:16:17:18:66:c8)  
... .. = LG bit: Globally unique address (factory default)  
... .. = IG bit: Individual address (unicast)  
- Source: Dell\_f4:3b:96 (00:12:3f:f4:3b:96)  
Address: Dell\_f4:3b:96 (00:12:3f:f4:3b:96)  
... .. = LG bit: Globally unique address (factory default)  
... .. = IG bit: Individual address (unicast)  
Type: IPv4 (0x00000000)

  

0010	00 a1 07 5e 40 00 00 06	de 2e 0a 00 00 02 0a 00	...^@... ..
0020	00 c9 00 58 c2 52 9f ae	f9 44 05 89 c7 64 50 18	...X.R... .D...dP...
0030	08 05 f3 27 00 00 d1 f8	de 9e e2 21 0c 7b 3d e0	...'. .... !. (=
0040	53 d7 61 9f 6b 62 8a 62	1a 88 5f 0d 35 8c 0f f3	S-a-kb-b ..._5...
0050	a2 51 ab 94 ed 7e 79 d0	02 1d df 23 53 55 a1 c4	-Q-...y- ...#SU...
0060	4c 02 4b 72 46 8c 2c 3b	00 56 e8 73 d2 3a c8 2f	L-KrF...; V-s-:/
0070	80 42 20 3a a2 6e ee df	aa e7 a2 7f 1e 1e 4c 2f	-B : n... ..L/
0080	04 54 3c 47 ce 92 9d dd	19 2e f0 39 cb 22 81 55	-T<G-... ..9"-U
0090	29 da 0e 80 9b 30 35 54	0e d8 74 8b 1a 98 86 f5	)-...05T -t-...
00a0	ad f6 7e 84 dc b0 6b 6e	07 12 d1 0f b1 70 fe	-...-kn ...-p-

2. Which torrent file did the user download?

[Betty\\_Boop\\_Rythm\\_on\\_the\\_Reservation.avi.torrent](#)



ip.addr == 10.0.0.201 && http

InterfaceChannel
802.11 Preferences

Packet listNarrow & WideCase sensitiveStringaviFindCancel

No.	Time	Source	Destination	Protocol	Length	CN	crea	Tex	Info
69756	770.57776	140.211.166.134	10.0.0.201	HTTP	264	✓	HTTP/1.1 200 OK		
69719	770.51624	168.215.194.14	10.0.0.201	HTTP	59	✓	HTTP/1.1 200 OK	(application/x-bittorrent)	
69602	769.67581	52.94.233.131	10.0.0.201	HTTP	254	✓	HTTP/1.1 200 OK	(GIF89a)	
69479	769.06425	72.21.202.62	10.0.0.201	HTTP	1310	✓	HTTP/1.1 200 OK	(text/html)	
69466	768.90266	168.215.194.14	10.0.0.201	HTTP	59	✓	HTTP/1.1 200 OK	(text/html)	
69456	768.88389	52.94.240.125	10.0.0.201	HTTP	1227	✓	HTTP/1.1 200 OK	(text/javascript)	
69426	768.61015	168.215.194.14	10.0.0.201	HTTP	865	✓	HTTP/1.1 200 OK	(JPEG JFIF image)	
69422	768.57814	168.215.194.14	10.0.0.201	HTTP	1212	✓	HTTP/1.1 200 OK	(GIF89a)	
69420	768.55788	52.94.240.125	10.0.0.201	HTTP	375	✓	HTTP/1.1 200 OK	(text/javascript)	

Response Phrase: OK  
Date: Sun, 15 Jul 2018 04:17:27 GMT\r\n  
Server: Apache\r\n  
Content-Disposition: inline; filename="Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent"\r\n  
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/\r\n  
Keep-Alive: timeout=5, max=100\r\n  
Connection: Keep-Alive\r\n  
Transfer-Encoding: chunked\r\n  
Content-Type: application/x-bittorrent\r\n  
\r\n  
[HTTP response 1/1]  
[Time since request: 0.149293500 seconds]  
[Request in frame: 69706]  
[Request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the\_Reservation]

0000 00 16 17 18 66 c8 00 09 b7 27 a1 3e 08 00 45 00 ....f...'.>..E.  
0010 00 2d 24 34 00 00 80 06 a0 e8 a8 d7 c2 0e 0a 00 --\$4.....  
0020 00 c9 00 50 c2 aa 75 99 8c f4 97 b7 b3 3c 50 18 ...P..u.....<P-  
0030 fa f0 ea 90 00 00 30 0d 0a 0d 0a .....0-...