

Network Analysis

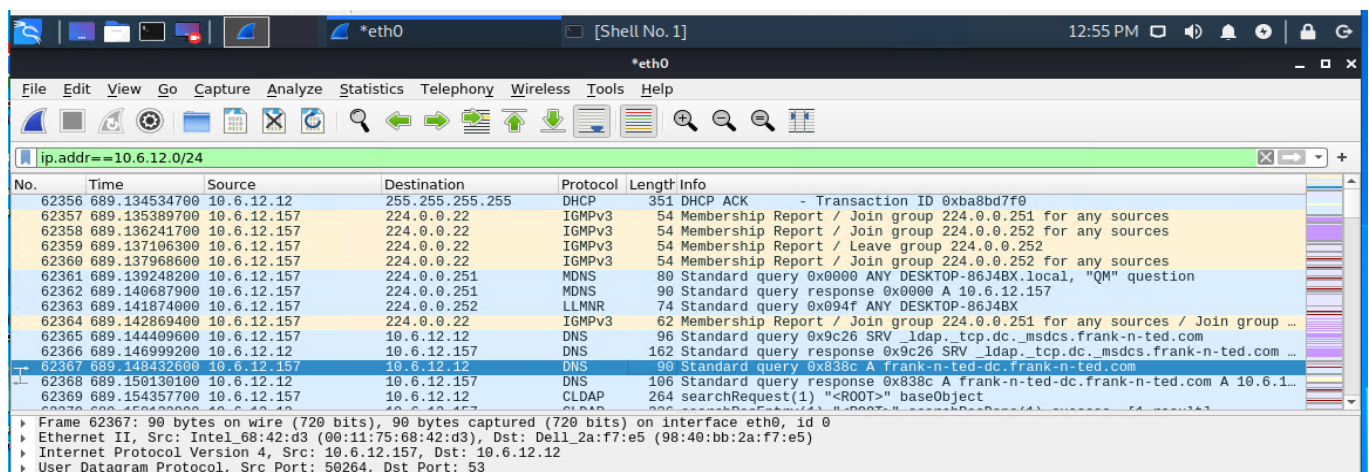
Time Thieves

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-DC.frand-n-ted.com
 - Filter used in Wireshark: ip.addr==10.6.12.0/24
 - Results:



The screenshot shows a Wireshark capture on interface eth0 with a filter of ip.addr==10.6.12.0/24. The packet list shows several DNS and LDAP messages. The packet details pane for packet 62367 shows a Standard query response from 10.6.12.12 to 10.6.12.157, containing a domain name 'frank-n-ted-dc.frank-n-ted.com'.

No.	Time	Source	Destination	Protocol	Length	Info
62356	689.134534700	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
62357	689.135389700	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
62358	689.136241700	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
62359	689.137106300	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
62360	689.137968600	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
62361	689.139248200	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
62362	689.140687900	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
62363	689.141874000	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
62364	689.142869400	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group ...
62365	689.144409600	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
62366	689.146999200	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com ...
62367	689.148432600	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
62368	689.150130100	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1...
62369	689.154357700	10.6.12.157	10.6.12.12	LDAP	264	searchRequest(1) "<R00T>" baseObject

2. What is the IP address of the Domain Controller (DC) of the AD network?
 - IP address is 10.6.12.12
 - Filter used in Wireshark: ip.addr==10.6.12.0/24
 - Results:

62367	689.148432600	10.6.12.157	10.6.12.12	DNS	9
62368	689.150130100	10.6.12.12	10.6.12.157	DNS	10
62369	689.154357700	10.6.12.157	10.6.12.12	CLDAP	26
62370	689.158432600	10.6.12.12	10.6.12.157	CLDAP	26

▶ Frame 62367: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on :
 ▼ Ethernet II, Src: Intel_68:42:d3 (00:11:75:68:42:d3), Dst: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
 ▶ Destination: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5)
 ▶ Source: Intel_68:42:d3 (00:11:75:68:42:d3)
 Type: IPv4 (0x0800)
 ▼ Internet Protocol Version 4, Src: 10.6.12.157, Dst: 10.6.12.12
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 76
 Identification: 0x17a9 (6057)
 ▶ Flags: 0x0000
 ... 0 0000 0000 0000 = Fragment offset: 0

- 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: june11.dll

ip.addr==10.6.12.0/24 and http.request.method==GET						
No.	Time	Source	Destination	Protocol	Length	Info
64973	700.405793800	10.6.12.157	172.93.120.242	HTTP	513	GET /logs/invoice-86495.doc HTTP/1.1
65982	706.708283900	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtwj HTTP/1.1
65986	706.723668100	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x018 (PSH, ACK)
 Window size value: 65535
 [Calculated window size: 65535]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x341f [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 ▶ [SEQ/ACK analysis]
 ▶ [Timestamps]
 TCP payload (258 bytes)
 ▼ Hypertext Transfer Protocol
 ▶ GET /files/june11.dll HTTP/1.1\r\n
 Accept: */*\r\n
 Accept-Encoding: gzip, deflate\r\n
 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
 Host: 205.185.125.104\r\n
 Connection: Keep-Alive\r\n
 ▶ Cookie: _subid=3mmhfd8jp\r\n
 \r\n
 [Full request URI: <http://205.185.125.104/files/june11.dll>]
 [HTTP request 2/2]
 [Prev request in frame: 65982]

- Filter used in Wireshark: ip.addr==10.6.12.203 and http.request.method==GET

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

51

/ 70

?

Community Score

51 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa7

6af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedli signed spreader

549.84 KB

Size

2022-08-01 18:29:07 UTC

14 minutes ago

DLL

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

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
Antiy-AVL	Trojan/Generic.ASCommon.1BE	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

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:

- 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 used in Wireshark: ip.src==172.16.4.4 and kerberos.CNameString

ip.src==172.16.4.4 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
7676	98.714552800	172.16.4.4	172.16.4.205	KRB5	204	AS-REP
7688	98.775223300	172.16.4.4	172.16.4.205	KRB5	130	TGS-REP
7715	98.857385500	172.16.4.4	172.16.4.205	KRB5	242	AS-REP
7726	98.916726000	172.16.4.4	172.16.4.205	KRB5	150	TGS-REP
7738	98.981725000	172.16.4.4	172.16.4.205	KRB5	273	TGS-REP
18766	255.993411600	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
18777	256.050543400	172.16.4.4	172.16.4.205	KRB5	72	TGS-REP
36814	509.669022800	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
37204	511.020554000	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP

▾ padata-type: kRB5-PADATA-ETYPE-INF02 (19)
 ▾ padata-value: 303a3038a003020112a1311b2f4d494e442d48414d4d4552...
 ▾ ETYPE-INF02-ENTRY
 etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
 salt: MIND-HAMMER.NETHostrotterdam-pc.mind-hammer.net
 crealm: MIND-HAMMER.NET
 ▾ cname
 name-type: kRB5-NT-PRINCIPAL (1)
 ▾ cname-string: 1 item
 CNameString: ROTTERDAM-PC\$
 ▾ ticket
 tkt-vno: 5
 realm: MIND-HAMMER.NET

2. What is the username of the Windows user whose computer is infected?
 - Filter used in Wireshark: ip.src==172.16.4.205 and kerberos.CNameString
 - Username is mattijs.dervies

ip.src==172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
7489	97.873575300	172.16.4.205	172.16.4.4	KRB5	297	AS-REQ
7497	97.890755500	172.16.4.205	172.16.4.4	KRB5	377	AS-REQ
7667	98.671393000	172.16.4.205	172.16.4.4	KRB5	301	AS-REQ
7674	98.687031100	172.16.4.205	172.16.4.4	KRB5	381	AS-REQ
7706	98.813728400	172.16.4.205	172.16.4.4	KRB5	292	AS-REQ
7713	98.829266300	172.16.4.205	172.16.4.4	KRB5	372	AS-REQ

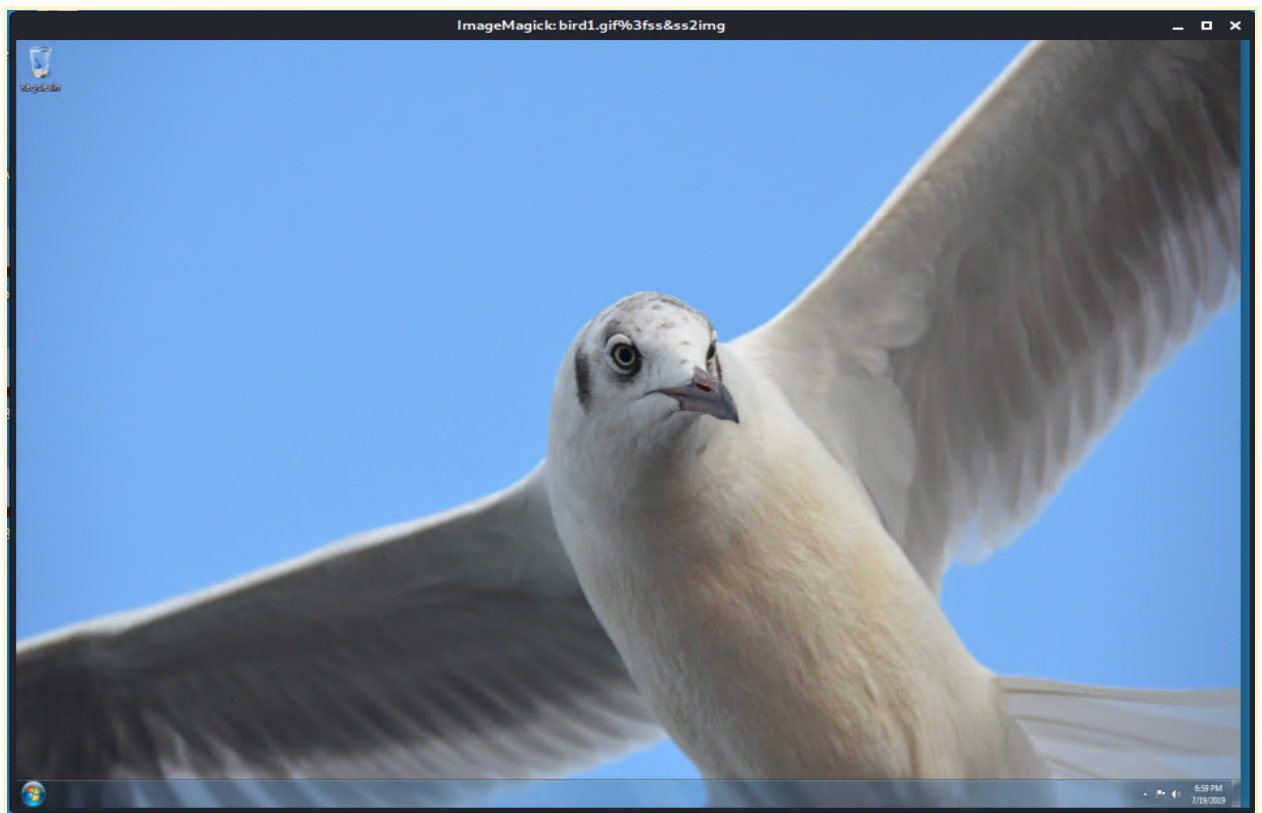
.... 0... = enc-tkt-in-skey: False
0.. = unused29: False
0. = renew: False
0 = validate: False
 ▾ cname
 name-type: kRB5-NT-PRINCIPAL (1)
 ▾ cname-string: 1 item
 CNameString: matthijs.dervies
 realm: MIND-HAMMER
 ▾ sname
 name-type: kRB5-NT-SRV-INST (2)
 ▾ sname-string: 2 items
 CNameString: kbtst

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

- IP addresses- 172.16.4.205, 185.243.115.84, 166.62.11.64

Ethernet · 76 IPv4 · 531 IPv6 · 8 TCP · 749 UDP · 1290								
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Ratio
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	2
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	5
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	1
192.168.1.90	192.168.1.100	3,466	15 M	2,275	15 M	1,191	336 k	6
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	6
10.0.0.201	64.187.66.143	2,465	1,851 k	1,122	72 k	1,343	1,779 k	5
10.6.12.12	10.6.12.157	1,129	303 k	533	146 k	596	157 k	6
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	5
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	6
10.6.12.12	10.6.12.203	1,069	291 k	488	135 k	581	155 k	6
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	4
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	5
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	5
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	5
10.6.12.203	205.185.125.104	638	596 k	180	10 k	458	586 k	7
10.11.11.179	143.204.29.89	449	295 k	217	22 k	232	273 k	5
10.11.11.11	10.11.11.179	440	43 k	112	17 k	328	26 k	5
10.11.11.11	10.11.11.195	418	35 k	103	10 k	315	25 k	5
---	---	---	---	---	---	---	---	---

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 in your Network Report:

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
 - Computer host name: BLANCO-DESKTOP

No.	Time	Source	Destination	Protocol	Length	Info
76799	817.864554	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
76820	817.984438	10.0.0.201	10.0.0.2	KRB5	381	AS-REQ
76824	817.992230	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
76838	818.040158	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
76924	818.395513	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
76932	818.411737	10.0.0.201	10.0.0.2	KRB5	381	AS-REQ
77015	818.728874	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
77028	818.757567	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
78357	825.163700	10.0.0.201	10.0.0.2	KRB5	302	AS-REQ
78365	825.180232	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
78423	825.346355	10.0.0.201	10.0.0.2	KRB5	290	AS-REQ
78431	825.361894	10.0.0.201	10.0.0.2	KRB5	370	AS-REQ

TCP payload (327 bytes)	
[PDU Size: 327]	
Kerberos	
Record Mark: 323 bytes	
as-req	
pvno: 5	
msg-type: krb-as-req (10)	
padata: 2 items	
req-body	
Padding: 0	
kdc-options: 40810010	
cname	
name-type: KRB5-NT-PRINCIPAL (1)	
cname-string: 1 item	
CNameString: blanco-desktop\$	
realm: D0G0FTHEYEAR.NET	

2. Which torrent file did the user download?
 - The torrent downloaded
**Betty_Boop_Rythm_on_the_Reservation.avi.torrent.
 - Filter: ip.addr==10.0.0.201 and http.request.method==GET

[illegible]