

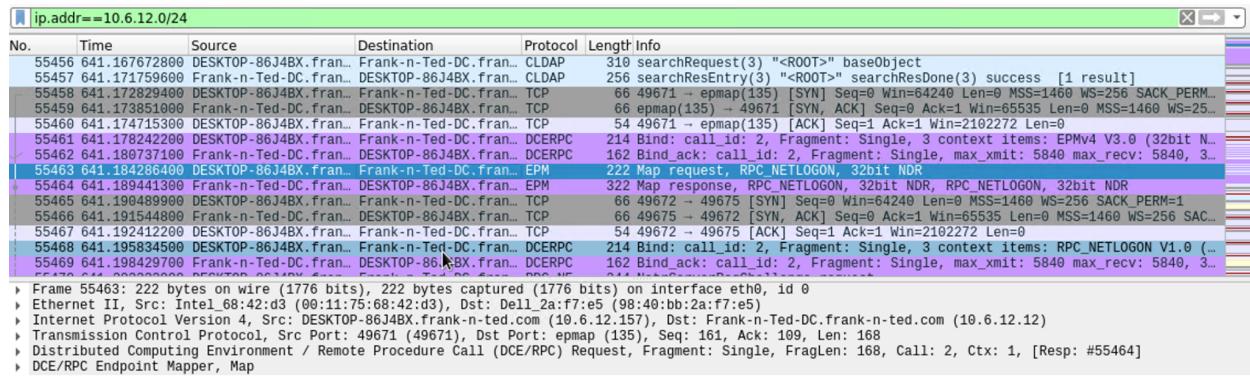
Network Analysis

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

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.

Name of the malware is June11.d11. They also tried downloading /pQBtWj but it didn't work.

ip.addr==10.6.12.203 and http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	Info
+ 58748	658.621258400	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
+ 58752	658.636633700	LAPTOP-5WKHX9YG.fra...	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

```

Frame 58748: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits) on interface eth0, id 0
Ethernet II, Src: IntelCor_6d:fce2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
Transmission Control Protocol, Src Port: 49739 (49739), Dst Port: http (80), Seq: 1, Ack: 1, Len: 221
    Source Port: 49739 (49739)
    Destination Port: http (80)
    [Stream index: 724]
    [TCP Segment Len: 221]
    Sequence number: 1 (relative sequence number)
    Sequence number (raw): 69156448
    [Next sequence number: 222 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    Acknowledgment number (raw): 2023968676
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 65535

```

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

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

53 / 69

53 security vendors flagged this file as malicious

53 / 69

Community Score

549.84 KB | 2021-06-05 03:21:09 UTC | 2 days ago | DLL

Community (2)

Detection	Details	Relations	Behavior	Community
Ad-Aware	Trojan.Mint.Zamg.O		AegisLab	Trojan.Win32.Yakes.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613		Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O		SecureAge APEX	Malicious
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.34722.lu9@aul7OQgi

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)

No.	Time	Source	Destination	Protocol	Length	Info
3181	49.776799300	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	68	49162 → 49155 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3182	49.777852900	mind-hammer-dc.mind..	Rotterdam-PC.mind-h..	TCP	66	49155 → 49162 [SYN ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3183	49.778740500	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	56	49162 → 49155 [ACK] Seq=1 Ack=0 Win=65536 Len=0
3184	49.779832900	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	68	49163 → kerberos(88) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3185	49.781033200	mind-hammer-dc.mind..	Rotterdam-PC.mind-h..	TCP	66	kerberos(88) → 49163 [SYN ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3186	49.781929800	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	56	49163 → kerberos(88) [ACK] Seq=1 Ack=1 Win=65536 Len=0
3187	49.786544600	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	KRB5	297	AS-REQ
3188	49.792033500	mind-hammer-dc.mind..	Rotterdam-PC.mind-h..	KRB5	343	KRB_Error: KRB5KDC_ERR_PREAMTH_REQUIRED
3189	49.792925100	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	56	49163 → kerberos(88) [FIN, ACK] Seq=244 Ack=290 Win=65280 Len=0
3190	49.794006300	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	68	49164 → kerberos(88) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3191	49.795065200	mind-hammer-dc.mind..	Rotterdam-PC.mind-h..	TCP	66	kerberos(88) → 49164 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3192	49.795970300	mind-hammer-dc.mind..	Rotterdam-PC.mind-h..	TCP	54	kerberos(88) → 49163 [ACK] Seq=290 Ack=245 Win=131328 Len=0
3193	49.796795800	mind-hammer-dc.mind..	Rotterdam-PC.mind-h..	TCP	54	kerberos(88) → 49163 [RST, ACK] Seq=290 Ack=245 Win=0 Len=0
3194	49.797685700	Rotterdam-PC.mind-h..	mind-hammer-dc.mind..	TCP	56	49164 → kerberos(88) [ACK] Seq=1 Ack=1 Win=65536 Len=0

Frame 3182: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: Dell_19:49:50 (44:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Destination: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
Address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
...0..... = LG bit: Globally unique address (factory default)
...0..... = IG bit: Individual address (unicast)
Source: Dell_19:49:50 (44:ba:db:19:49:50)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: mind-hammer-dc.mind-hammer.net (172.16.4.4), Dst: Rotterdam-PC.mind-hammer.net (172.16.4.205)
Transmission Control Protocol, Src Port: 49155 (49155), Dst Port: 49162 (49162), Seq: 0, Ack: 1, Len: 0

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

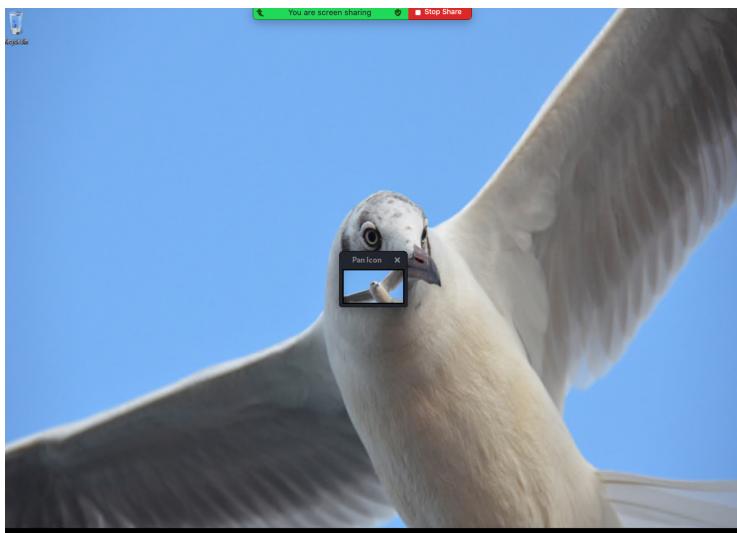
matthijs.devries

No.	Time	Source	Destination	Protocol	Length	Info
3187	49.786544600	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	297	AS-REQ
3195	49.803720100	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	377	AS-REQ
3197	49.831293000	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	204	AS-REP
3209	49.894459400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	219	TGS-REP
3250	50.135544700	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	158	TGS-REP
3270	50.241859400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	84	TGS-REP
3369	50.584361200	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	301	AS-REQ
3376	50.599992500	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	381	AS-REQ
3378	50.627492100	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	204	AS-REP
3390	50.688223400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	130	TGS-REP
3408	50.726684900	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	292	AS-REQ
3415	50.742235400	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	372	AS-REQ
3417	50.770347900	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	242	AS-REP
3428	50.829698200	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	150	TGS-REP
3440	50.884620000	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	270	TGS-REP
	0.. = unused21: False				
	0.. = unused22: False				
	0.. = unused23: False				
		0.... = unused24: False				
		.0.... = unused25: False				
		..0.... = disable-transited-check: False				
		..1.... = renewable-ok: True				
	 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.devries				

3. What are the IP addresses used in the actual infection traffic? 185.243.115.84

172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	77 k
172.16.4.205	172.217.4.163	186	120 k	80	7,366	106	113 k	57.647373	995.1059	59
172.16.4.205	216.58.193.200	142	118 k	52	3,772	90	114 k	62.525786	990.2284	30
172.16.4.205	172.217.14.74	126	85 k	52	5,266	74	80 k	56.656829	996.0983	42
172.16.4.205	209.197.3.15	120	51 k	50	5,824	70	46 k	51.825217	1000.7020	46
172.16.4.205	192.0.73.2	134	43 k	66	7,380	68	35 k	54.233958	998.5679	59
172.16.4.205	192.0.76.3	96	29 k	46	5,634	50	23 k	54.231850	998.5710	45
172.16.4.205	192.0.77.32	66	26 k	30	3,874	36	22 k	54.232902	998.5575	31
172.16.4.205	192.0.77.48	66	20 k	32	4,000	34	16 k	62.526845	990.2769	32
172.16.4.205	216.58.193.202	26	4,700	14	1,584	12	3,116	51.828373	1001.4519	12
172.16.4.205	172.16.4.255	24	2,640	24	2,640	0	0	49.765858	852.3077	24
172.16.4.205	205.185.216.10	10	2,372	5	524	5	1,848	461.267315	0.1411	29 k
172.16.4.205	239.255.255.250	12	2,100	12	2,100	0	0	240.322914	855.7223	19
172.16.4.205	195.171.92.116	17	1,788	10	836	7	952	336.031816	853.7480	7
172.16.4.205	184.50.26.32	20	1,716	10	794	10	922	50.387494	851.7212	7
172.16.4.205	255.255.255.255	5	1,710	5	1,710	0	0	50.382223	1137.3560	12
172.16.4.205	224.0.0.22	16	960	16	960	0	0	49.771477	1042.4728	7
172.16.4.205	224.0.0.252	10	720	10	720	0	0	49.770532	852.3245	6

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

No.	Time	Source	Destination	Protocol	Length	Info
65732	744.637837100	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	250	AS-REP
65745	744.704098600	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	293	TGS-REP
65798	745.008607500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	227	TGS-REP
65827	745.174120600	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	293	TGS-REP
65839	745.233051500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	114	TGS-REP
66970	751.007645200	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	302	AS-REQ
66978	751.024207500	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	382	AS-REQ
66980	751.052436500	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	250	AS-REP
66992	751.115116900	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	199	TGS-REP
67036	751.190289600	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	290	AS-REQ
67044	751.205833000	BLANCO-DESKTOP.dogo...	DogOfTheYear-DC.dog...	KRB5	370	AS-REQ
67046	751.233860000	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	237	AS-REP
67058	751.294737700	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	175	TGS-REP
67080	751.379585100	DogOfTheYear-DC.dog...	BLANCO-DESKTOP.dogo...	KRB5	303	TGS-REP


```
.... .0. = renew: False
.... .0 = validate: False
- cName
  name-type: KRB5-NT-PRINCIPAL (1)
  - cname-string: 1 item
    CNameString: elmer.blanco
    realm: DOGOFTHEYEAR
- sName
  name-type: KRB5-NT-SRV-INST (2)
  - sname-string: 2 items
    SNameString: krbtgt
    SNameString: DOGOFTHEYEAR
  till: 2037-09-13 02:48:05 (UTC)
  rtime: 2037-09-13 02:48:05 (UTC)
  nonce: 634194387
```

- OS version windows NT 10.0;

```
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513
User-Agent: 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
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: www.publicdomaintorrents.com
Connection: Keep-Alive
```

2. Which torrent file did the user download?

```

ip.addr==10.0.0.201 and http.request.method==GET
No. Time Source Destination Protocol Length Info
69213 765.837950500 BLANCO-DESKTOP.dog... files.publicdomaint... HTTP 465 GET /divxi.jpg HTTP/1.1
69298 766.857883600 BLANCO-DESKTOP.dog... www.assoc-amazon.com HTTP 415 GET /s/ads.js HTTP/1.1
69347 767.585292600 BLANCO-DESKTOP.dog... files.publicdomaint... HTTP 531 GET /usercomments.html?movieid=513 HTTP/1.1
69434 768.625230500 BLANCO-DESKTOP.dog... www.assoc-amazon.com HTTP 427 GET /s/ads-common.js HTTP/1.1
69470 768.919511100 BLANCO-DESKTOP.dog... rcm-na.assoc-amazon.. HTTP 885 GET /e/cm?t=publicdomai0f-20&e=1&p=4&l=opl&pv=1d=40C236A13FD00B68&ref=ur...
69542 769.560560300 BLANCO-DESKTOP.dog... fls-na.amazon-adsys.. HTTP 1067 GET /1/associates-ads/1/Op/?cb=1531628232887&p=%7B%22program%22%3A%221K...
+ 69706 770.366956400 BLANCO-DESKTOP.dog... files.publicdomaint... HTTP 569 GET /bt/btdownload.php?type=torrent&file=betty_Boop_Rhythm_on_the_Reserv...
69750 770.563257500 BLANCO-DESKTOP.dog... ftp.osuosl.org HTTP 195 GET /version.1.0 HTTP/1.1
69754 770.572679300 BLANCO-DESKTOP.dog... torrent.ubuntu.com HTTP 423 GET /announce?info_hash=%E4%be%9eMkb8vE3e3%1797x%b0%3e%90b%97%be%5c%8...
69981 771.231145500 BLANCO-DESKTOP.dog... files.publicdomaint... HTTP 434 GET /bt/announce.php?info_hash=%1d%da%0d%Ha%98%bd%81%5c%7d%2%ee%836o%93%...
70010 771.307842200 BLANCO-DESKTOP.dog... moonstar.publicdoma... HTTP 434 GET /announce?info_hash=%1d%da%0d%Ha%98%bd%81%5c%7d%2%ee%836o%93%09y%60...
70122 771.3590958400 BLANCO-DESKTOP.dog... files.publicdomaint... HTTP 253 GET /bt/scrape.php?info_hash=%1d%da%0d%Ha%8%98%bd%81%5c%7d2%ee%836o%03%09...
70144 771.637310900 BLANCO-DESKTOP.dog... moonstar.publicdoma... HTTP 253 GET /scrape?info_hash=%1d%da%0d%Ha%98%bd%81%5c%7d%2%ee%836o%03%09y%60%fe...
77816 833.561991600 BLANCO-DESKTOP.dog... cs9.wac.phicn.net HTTP 288 GET /MFewTzBNMsesSTAjBgUrDgMCGjUAABSAQYBmQ2awN1H6Dohk2FsBYgF7vQuA95QN...
77816.000 833.561991600 BLANCO-DESKTOP.dog... files.publicdomaintor... HTTP 200 GET /bt/btdownload.php?type=torrent&file=betty_Boop_Rhythm_on_the_Reserv...
> Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
  Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:1:a3e (00:09:b7:27:a1:3e)
    + Destination: Cisco_27:27:a1:3e (00:09:b7:27:a1:3e)
      Address: Cisco_27:27:a1:3e (00:09:b7:27:a1:3e)
      ....0. .... .... .... = LG bit: Globally unique address (factory default)
      ....0. .... .... .... = IG bit: Individual address (unicast)
    - Source: Msi_18:66:c8 (00:16:17:18:66:c8)
      Address: Msi_18:66:c8 (00:16:17:18:66:c8)
      ....0. .... .... .... = LG bit: Globally unique address (factory default)
      ....0. .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
    0100 .... = Version: 4
    ....0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

```