

Network Analysis

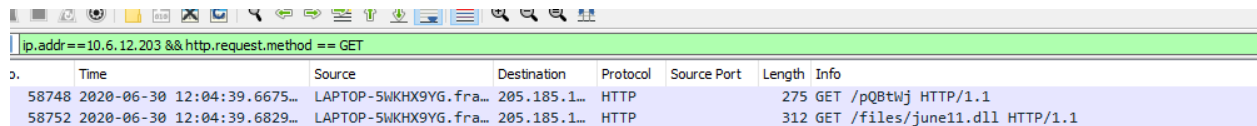
Time Thieves

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**
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.d11**



No.	Time	Source	Destination	Protocol	Source Port	Length	Info
58748	2020-06-30 12:04:39.6675...	LAPTOP-5WKHX9YG.fra...	205.185.1...	HTTP		275	GET /pQ8twj HTTP/1.1
58752	2020-06-30 12:04:39.6829...	LAPTOP-5WKHX9YG.fra...	205.185.1...	HTTP		312	GET /files/june11.dll HTTP/1.1

ip

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

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)**

ip.addr == 172.16.4.4

No.	Time	Source	Destination	Protocol	Source Port	Length	Info
32452	2020-06-30 12:01:24.8576...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	389 → 49286 [ACK] Seq=4287 Ack=2951.
32453	2020-06-30 12:01:24.8584...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	389 → 49286 [RST, ACK] Seq=4287 Ack=.
32454	2020-06-30 12:01:24.8593...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		56	49283 → 135 [FIN, ACK] Seq=497 Ack=.
32455	2020-06-30 12:01:24.8602...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		56	49285 → 49158 [FIN, ACK] Seq=1265 A.
32456	2020-06-30 12:01:24.8611...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	135 → 49283 [ACK] Seq=549 Ack=498 W.
32457	2020-06-30 12:01:24.8620...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	49158 → 49285 [FIN, ACK] Seq=1129 A.
32458	2020-06-30 12:01:24.8628...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	135 → 49283 [FIN, ACK] Seq=549 Ack=.
32459	2020-06-30 12:01:24.8637...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		56	49285 → 49158 [ACK] Seq=1266 Ack=11.
32460	2020-06-30 12:01:24.8646...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		56	49283 → 135 [ACK] Seq=498 Ack=550 W.
32461	2020-06-30 12:01:24.8655...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		56	49284 → 49155 [FIN, ACK] Seq=2981 A.
32462	2020-06-30 12:01:24.8664...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	49155 → 49284 [ACK] Seq=1114 Ack=29.
32463	2020-06-30 12:01:24.8672...	mind-hammer-dc.mind...	Rotterdam...	TCP		54	49155 → 49284 [FIN, ACK] Seq=1114 A.
32464	2020-06-30 12:01:24.8681...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		56	49284 → 49155 [ACK] Seq=2982 Ack=11.
82100	2020-06-30 12:08:42.5316...	Rotterdam-PC.mind-h...	mind-hamm...	TCP		68	[TCP Retransmission] 49162 → 49155 .

Frame 32464: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface eth0, id 0
Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_19:49:50 (a4:ba:db:19:49:50)
Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: mind-hammer-dc.mind-hammer.net (172.16.4.4)
Transmission Control Protocol, Src Port: 49284, Dst Port: 49155, Seq: 2982, Ack: 1115, Len: 0
VSS Monitoring Ethernet trailer, Source Port: 41087

- What is the username of the Windows user whose computer is infected?
matthijs.devries
- What are the IP addresses used in the actual infection traffic? **172.16.4.205, 185.243.115.84, 166.62.11.64**
- 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:

- 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 **win 64**

```
✓ Hypertext Transfer Protocol
> GET /psp.gif HTTP/1.1\r\n
Referer: http://publicdomaintorrents.info/nshowcat.ht
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n
\r\n
```

- Which torrent file did the user download?
Betty_noop_rythm_on_the_reservation.avitorrent

ip.addr==10.0.0.201 and http.request.method==GET							
Io.	Time	Source	Destination	Protocol	Source Port	Length	Info
69126	2020-06-30 12:06:26.1818...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		534	GET /nshowmovie.html?movieid=513 HTTP/1.1
69142	2020-06-30 12:06:26.3095...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		471	GET /yellow-star.gif HTTP/1.1
69150	2020-06-30 12:06:26.3259...	BLANCO-DESKTOP.dogo...	pagead46...	HTTP		434	GET /pagead/show_ads.js HTTP/1.1
69155	2020-06-30 12:06:26.3364...	BLANCO-DESKTOP.dogo...	digg.com	HTTP		412	GET /tools/diggthis.js HTTP/1.1
69167	2020-06-30 12:06:26.4627...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		500	GET /grabs/bettybooprythmonthereserva...
69213	2020-06-30 12:06:26.8842...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		465	GET /divxi.jpg HTTP/1.1
69298	2020-06-30 12:06:27.9041...	BLANCO-DESKTOP.dogo...	www.assoc...	HTTP		415	GET /s/ads.js HTTP/1.1
69347	2020-06-30 12:06:28.6316...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		531	GET /usercomments.html?movieid=513 HT...
69434	2020-06-30 12:06:29.6715...	BLANCO-DESKTOP.dogo...	www.assoc...	HTTP		427	GET /s/ads-common.js HTTP/1.1
69470	2020-06-30 12:06:29.9658...	BLANCO-DESKTOP.dogo...	rcm-na.as...	HTTP		885	GET /e/cm?t=publicdomai0f-20&o=1&p=48...
69542	2020-06-30 12:06:30.6068...	BLANCO-DESKTOP.dogo...	fls-na.am...	HTTP		1067	GET /1/associates-ads/1/OP/?cb=153162...
69706	2020-06-30 12:06:31.4132...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		589	GET /bt/btdownload.php?type=torrent&f...
69750	2020-06-30 12:06:31.6095...	BLANCO-DESKTOP.dogo...	ftp.osuos...	HTTP		195	GET /version-1.0 HTTP/1.1
69754	2020-06-30 12:06:31.6190...	BLANCO-DESKTOP.dogo...	torrent.u...	HTTP		423	GET /announce?info_hash=%e4%be%9e%b8...
69980	2020-06-30 12:06:32.2774...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		434	GET /bt/announce.php?info_hash=%1d%da...
70010	2020-06-30 12:06:32.3541...	BLANCO-DESKTOP.dogo...	moonstar...	HTTP		434	GET /announce?info_hash=%1d%da%0d%ha...
70122	2020-06-30 12:06:32.6372...	BLANCO-DESKTOP.dogo...	files.pub...	HTTP		253	GET /bt/scrape.php?info hash=%1d%da%0...

> 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:a1:3e (00:09:b7:27:a1:3e)

> Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)

> Transmission Control Protocol, Src Port: 49834, Dst Port: 80, Seq: 1, Ack: 1, Len: 535

```
✓ Hypertext Transfer Protocol
> GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
```