

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?

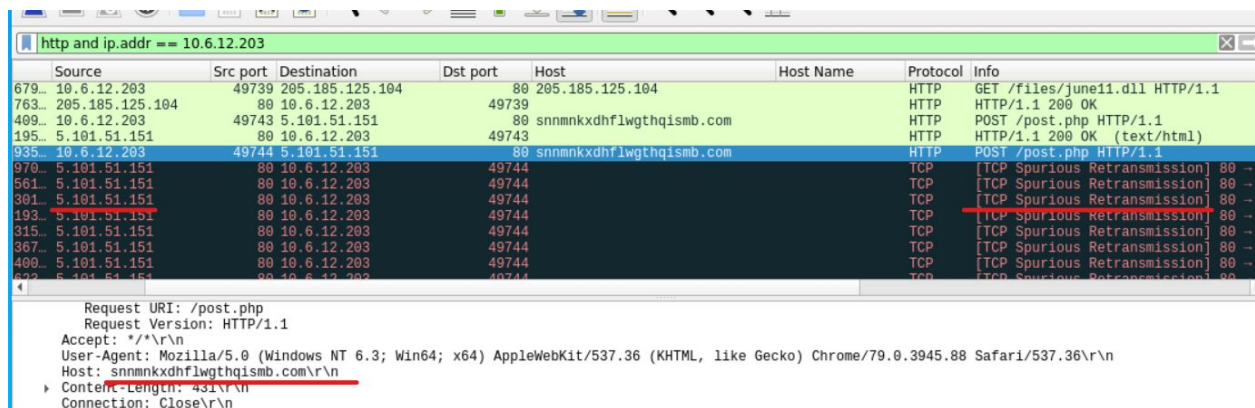
frank-n-ted.com

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.

<http://snnmnkxdhflwgthqismb.com/post.php>



The image shows a Wireshark packet capture window with the filter 'http and ip.addr == 10.6.12.203'. The packet list shows several HTTP requests and responses. The selected packet (935) is an HTTP POST request to 'http://snnmnkxdhflwgthqismb.com/post.php'. The packet details pane shows the request structure, including the URI, version, accept headers, user-agent, host, content-length, and connection.

No.	Source	Src port	Destination	Dst port	Host	Host Name	Protocol	Info
679	10.6.12.203	49739	205.185.125.104	80	205.185.125.104		HTTP	GET /files/june11.dll HTTP/1.1
763	205.185.125.104	80	10.6.12.203	49739			HTTP	HTTP/1.1 200 OK
409	10.6.12.203	49743	5.101.51.151	80	snnmnkxdhflwgthqismb.com		HTTP	POST /post.php HTTP/1.1
195	5.101.51.151	80	10.6.12.203	49743			HTTP	HTTP/1.1 200 OK (text/html)
935	10.6.12.203	49744	5.101.51.151	80	snnmnkxdhflwgthqismb.com		HTTP	POST /post.php HTTP/1.1
970	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
561	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
301	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
193	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
315	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
367	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
400	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →
622	5.101.51.151	80	10.6.12.203	49744			TCP	[TCP Spurious Retransmission] 80 →

Request URI: /post.php
Request Version: HTTP/1.1
Accept: */*\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36\r\n
Host: snnmnkxdhflwgthqismb.com\r\n
Content-Length: 431\r\n
Connection: Close\r\n

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

Malicious HTTP Response URL and php file

The screenshot shows the VirusTotal.com interface for the URL `http://snnmnkxdhflwgtqismb.com/post.php`. The browser's address bar shows the URL and a security warning. The page header includes navigation links like 'Kali Linux', 'Kali Training', etc. The main content area displays a '13 / 80' detection score and a warning '13 engines detected this URL'. Below this, a table shows the URL, status (200), content type (text/html; charset=UTF-8), and date (2020-06-11 06:42:28 UTC). A 'Community Score' section is also visible. At the bottom, a table lists detection results from various engines.

DETECTION	DETAILS	COMMUNITY
AegisLab WebGuard	ⓘ Malicious	Antiy-AVL ⓘ Malicious
Comodo Valkyrie Verdict	ⓘ Malicious	CRDF ⓘ Malicious
CyRadar	ⓘ Malicious	Dr.Web ⓘ Malicious
ESET	ⓘ Malware	Forcepoint ThreatSeeker ⓘ Malicious
Fortinet	ⓘ Malware	Google Safebrowsing ⓘ Phishing
Kaspersky	ⓘ Malware	Sophos AV ⓘ Malicious

HTTP Response ⓘ

Final URL

http://snnmnkxdhflwgtqismb.com/post.php

Serving IP Address

80.249.147.189

Status Code

200

Body SHA-256

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Headers

connection	close
content-length	0
content-type	text/html; charset=UTF-8
date	Thu, 11 Jun 2020 06:42:29 GMT
server	nginx

Vulnerable Windows Machines

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

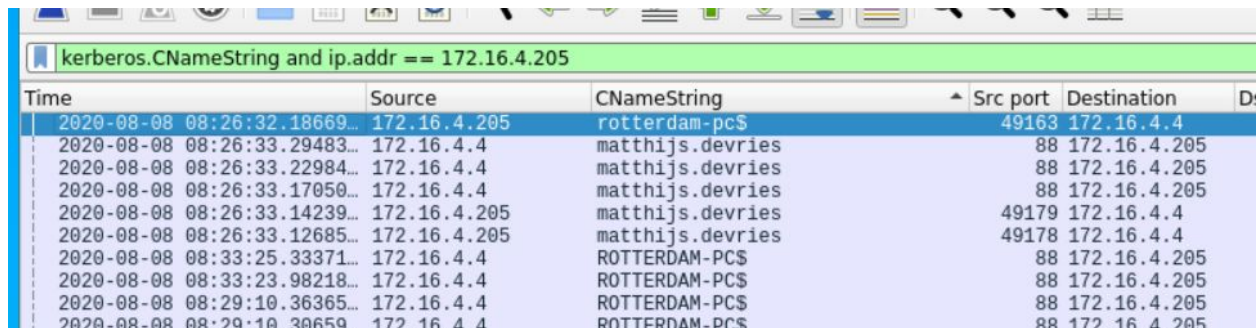
- Machines in the network live in the range 172.16.4.0/24.

- 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.mind-hammer.net
 - IP address: 172.16.4.205
 - MAC address: 00:59:07:b0:63:a4
2. What is the username of the Windows user whose computer is infected?

Username is matthijs.devries



Time	Source	CNameString	Src port	Destination	D
2020-08-08 08:26:32.18669...	172.16.4.205	rotterdam-pc\$	49163	172.16.4.4	
2020-08-08 08:26:33.29483...	172.16.4.4	matthijs.devries	88	172.16.4.205	
2020-08-08 08:26:33.22984...	172.16.4.4	matthijs.devries	88	172.16.4.205	
2020-08-08 08:26:33.17050...	172.16.4.4	matthijs.devries	88	172.16.4.205	
2020-08-08 08:26:33.14239...	172.16.4.205	matthijs.devries	49179	172.16.4.4	
2020-08-08 08:26:33.12685...	172.16.4.205	matthijs.devries	49178	172.16.4.4	
2020-08-08 08:33:25.33371...	172.16.4.4	ROTTERDAM-PC\$	88	172.16.4.205	
2020-08-08 08:33:23.98218...	172.16.4.4	ROTTERDAM-PC\$	88	172.16.4.205	
2020-08-08 08:29:10.36365...	172.16.4.4	ROTTERDAM-PC\$	88	172.16.4.205	
2020-08-08 08:29:10.30659...	172.16.4.4	ROTTERDAM-PC\$	88	172.16.4.205	

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

185.243.115.84 (b5689023.green.mattingsolutions.co) and 31.7.62.214 (fake url.htm)

17.91142...	b5689023.green.ma...	80 Rotterdam-PC.mind...	49249		HTTP	Continuation
17.95402...	b5689023.green.ma...	80 Rotterdam-PC.mind...	49249		HTTP	Continuation
18.01519...	Rotterdam-PC.mind...	49249 b5689023.green.ma...	80	<u>b5689023.green.mattingsoluti...</u>	HTTP	POST /empty.gif HTTP/1.1 (app)
18.02234...	b5689023.green.ma...	80 Rotterdam-PC.mind...	49249		HTTP	HTTP/1.1 200 OK
19.23621...	Rotterdam-PC.mind...	49255 31.7.62.214	443	31.7.62.214	HTTP	POST http://31.7.62.214/fakeur...
19.24097...	Rotterdam-PC.mind...	49256 geograph.netsuppor...	80	geo.netsupportsoftware.com	HTTP	GET /location/loca.asp HTTP/1.1
19.91390...	31.7.62.214	443 Rotterdam-PC.mind...	49255		HTTP	HTTP/1.1 200 OK (application/)
19.92168...	Rotterdam-PC.mind...	49255 31.7.62.214	443	31.7.62.214	HTTP	POST http://31.7.62.214/fakeur...
20.47049...	geograph.netsuppo...	80 Rotterdam-PC.mind...	49256		HTTP	HTTP/1.1 200 OK (text/html)
20.47740...	31.7.62.214	443 Rotterdam-PC.mind...	49255		HTTP	HTTP/1.1 200 OK (application/)

TCP payload (214 bytes)						
Hypertext Transfer Protocol						
[Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]						
[Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]						
[Severity level: Warning]						
[Group: Security]						
POST http://31.7.62.214/fakeur1.htm HTTP/1.1\n						
[Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeur1.htm HTTP/1.1\n]						
[POST http://31.7.62.214/fakeur1.htm HTTP/1.1\n]						
[Severity level: Chat]						

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

http and ip.addr == 10.0.0.201

Time	Source	Src port	Destination	Dst port	Host
2020-08-08 08:24:03.02280...	10.0.0.201	49757	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.13263...	10.0.0.201	49756	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.35952...	168.215.194.14	80	10.0.0.201	49757	
2020-08-08 08:24:03.36800...	10.0.0.201	49757	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.56522...	168.215.194.14	80	10.0.0.201	49756	
2020-08-08 08:24:03.57272...	10.0.0.201	49761	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.58106...	10.0.0.201	49760	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.59045...	10.0.0.201	49759	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.59880...	10.0.0.201	49758	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.60725...	10.0.0.201	49756	168.215.194.14	80	publicdomain
2020-08-08 08:24:03.62600...	10.0.0.201	49764	172.217.9.2	80	pagead2.goog
2020-08-08 08:24:03.76613...	168.215.194.14	80	10.0.0.201	49757	
2020-08-08 08:24:03.77842...	10.0.0.201	49757	168.215.194.14	80	publicdomain

[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
▼ Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:a1:3e), 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)

kerberos.CNameString and ip.addr == 10.0.0.201

Time	Source	CNameString	Src port	Destination
2020-08-08 08:24:02.07120...	10.0.0.2	elmer.blanco	88	10.0.0.201
2020-08-08 08:24:01.98635...	10.0.0.2	elmer.blanco	88	10.0.0.201
2020-08-08 08:24:01.92547...	10.0.0.2	elmer.blanco	88	10.0.0.201
2020-08-08 08:24:01.89744...	10.0.0.201	elmer.blanco	49745	10.0.0.2
2020-08-08 08:24:01.88189...	10.0.0.201	elmer.blanco	49744	10.0.0.2
2020-08-08 08:23:55.29310...	10.0.0.201	blanco-desktop\$	49691	10.0.0.2
2020-08-08 08:23:55.26441...	10.0.0.201	blanco-desktop\$	49690	10.0.0.2
2020-08-08 08:23:54.94728...	10.0.0.201	blanco-desktop\$	49683	10.0.0.2
2020-08-08 08:23:54.93106...	10.0.0.201	blanco-desktop\$	49682	10.0.0.2
2020-08-08 08:23:54.57570...	10.0.0.201	blanco-desktop\$	49679	10.0.0.2
2020-08-08 08:23:54.52777...	10.0.0.201	blanco-desktop\$	49678	10.0.0.2
2020-08-08 08:23:54.52002...	10.0.0.201	blanco-desktop\$	49677	10.0.0.2
2020-08-08 08:23:54.40000...	10.0.0.201	blanco-desktop\$	49675	10.0.0.2

▼ Frame 7890: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface eth0, id 0

020-08-08 08:24:03.57272...	10.0.0.201	49761	168.215.194.14	80	publicdomain	torrents.info
020-08-08 08:24:03.58106...	10.0.0.201	49760	168.215.194.14	80	publicdomain	torrents.info
020-08-08 08:24:03.59045...	10.0.0.201	49759	168.215.194.14	80	publicdomain	torrents.info
020-08-08 08:24:03.59880...	10.0.0.201	49758	168.215.194.14	80	publicdomain	torrents.info
020-08-08 08:24:03.60725...	10.0.0.201	49756	168.215.194.14	80	publicdomain	torrents.info
020-08-08 08:24:03.62600...	10.0.0.201	49764	172.217.9.2	80	pagead2.googlesyndication.com	
020-08-08 08:24:03.76613...	168.215.194.14	80	10.0.0.201	49757		
020-08-08 08:24:03.77842...	10.0.0.201	49757	168.215.194.14	80	publicdomain	torrents.info

[Group: Sequence]
Request Method: GET
Request URI: /psp.gif
Request Version: HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n
Accept: image/png, image/svg+xml, image/*;q=0.8,*/*;q=0.5\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari:
Host: publicdomaintorrents.info\r\n
Connection: Keep-Alive\r\n\r\n

2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi video file.

Time	Source	Src port	Destination	Dst port	Host	Host Name
2020-08-08 08:24:17.54943...	10.0.0.201	49821	52.94.240.125	80	www.assoc-amazon.com	
2020-08-08 08:24:18.27690...	10.0.0.201	49818	168.215.194.14	80	publicdomaintorrents.info	
2020-08-08 08:24:19.31690...	10.0.0.201	49822	52.94.240.125	80	ir-na.amazon-adsystem.com	
2020-08-08 08:24:19.61111...	10.0.0.201	49824	72.21.202.62	80	rcm-na.amazon-adsystem.com	
2020-08-08 08:24:20.25211...	10.0.0.201	49831	52.94.233.131	80	fls-na.amazon-adsystem.com	
2020-08-08 08:24:21.05856...	10.0.0.201	49834	168.215.194.14	80	www.publicdomaintorrents.com	
2020-08-08 08:24:21.25488...	10.0.0.201	49841	140.211.166.134	80	download.deluge-torrent.org	
2020-08-08 08:24:21.26429...	10.0.0.201	49842	91.189.95.21	6969	torrent.ubuntu.com:6969	
2020-08-08 08:24:21.92275...	10.0.0.201	49847	168.215.194.14	80	files.publicdomaintorrents.c...	
2020-08-08 08:24:21.99945...	10.0.0.201	49848	168.215.195.227	6969	tracker.publicdomaintorrents...	
2020-08-08 08:24:22.28254...	10.0.0.201	49849	168.215.194.14	80	files.publicdomaintorrents.c...	
2020-08-08 08:24:22.32891...	10.0.0.201	49850	168.215.195.227	6969	tracker.publicdomaintorrents...	
2020-08-08 08:25:24.25365...	10.0.0.201	49850	72.21.01.20	80	ocsp.digicert.com	

```

TCP payload (535 bytes)
▼ Hypertext Transfer Protocol
  ▼ GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1]
      [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
    ▼ Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      Request URI Path: /bt/btdownload.php
      ▼ Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
        Request URI Query Parameter: type=torrent
        Request URI Query Parameter: file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      Request Version: HTTP/1.1
      Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n

```