

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:

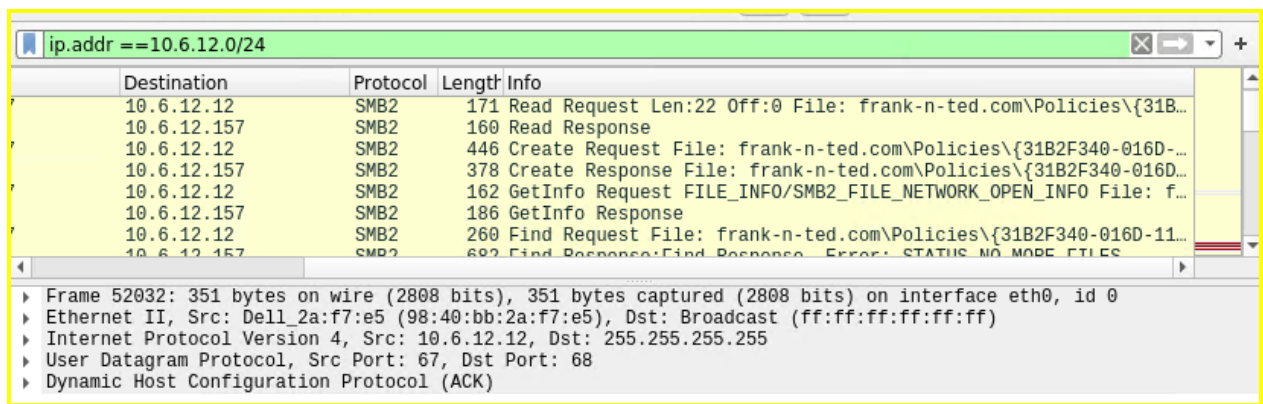
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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.frank-n-ted.com

Ip.addr ==10.6.12.0/24



	Destination	Protocol	Length	Info
	10.6.12.12	SMB2	171	Read Request Len:22 Off:0 File: frank-n-ted.com\Policies\{31B...
	10.6.12.157	SMB2	160	Read Response
	10.6.12.12	SMB2	446	Create Request File: frank-n-ted.com\Policies\{31B2F340-016D-...
	10.6.12.157	SMB2	378	Create Response File: frank-n-ted.com\Policies\{31B2F340-016D-...
	10.6.12.12	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: f...
	10.6.12.157	SMB2	186	GetInfo Response
	10.6.12.12	SMB2	260	Find Request File: frank-n-ted.com\Policies\{31B2F340-016D-11...
	10.6.12.157	SMB2	682	Find Response:Find Response Error: STATUS_NO_MORE_FILES

Frame 52032: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface eth0, id 0
Ethernet II, Src: Dell_2a:f7:e5 (98:40:bb:2a:f7:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.6.12.12, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)

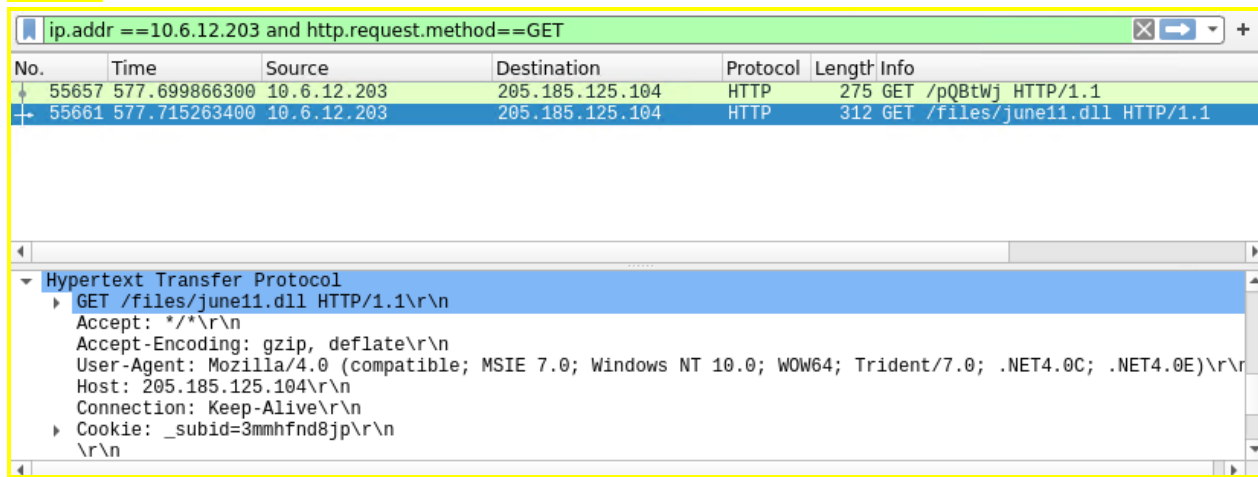
2. What is the IP address of the Domain Controller (DC) of the AD network?

IP Address is 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)

- 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.

File name is june11.dll

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

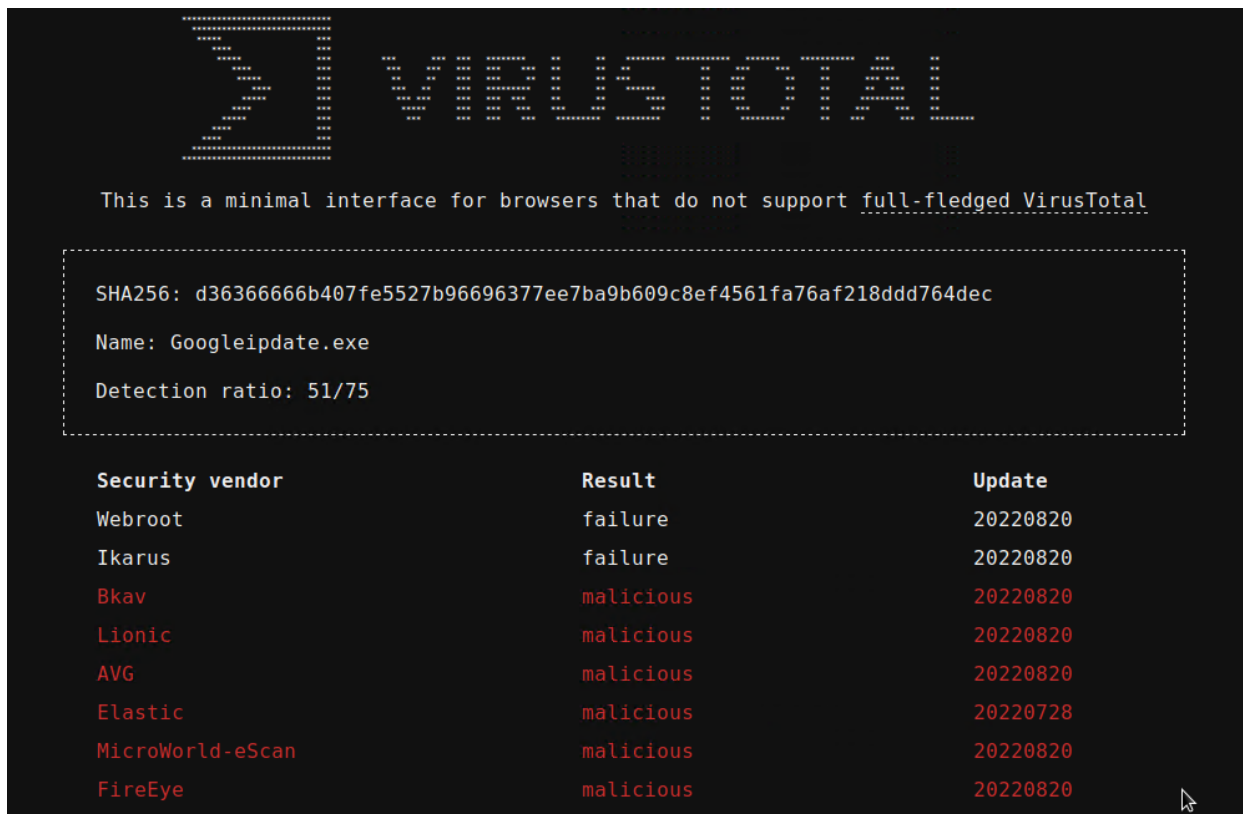


The image shows a Wireshark packet capture window with a filter set to 'ip.addr == 10.6.12.203 and http.request.method == GET'. Two packets are listed in the packet list pane. The second packet, number 55661, is selected and its details are shown in the packet details pane. The details pane shows the Hypertext Transfer Protocol section expanded, displaying the request line and various headers.

No.	Time	Source	Destination	Protocol	Length	Info
55657	577.699866300	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtwj HTTP/1.1
55661	577.715263400	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

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

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



Vulnerable Windows Machines

- 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.

1. Find the following information about the infected Windows machine:

`ip.src == 172.16.4.4 and kerberos.CNameString`

- Host name: **ROTTERDAM-PC**
- IP address: **172.16.4.205**
- MAC address: **00:59:07:b0:63:a4**

The image shows a Wireshark packet capture window. The top pane displays a list of packets filtered by `ip.src == 172.16.4.4 and kerberos.CNameString`. The list includes several TGS-REP and AS-REP packets from mind-hammer-dc.mind... to Rotterdam-PC.mind-h... The bottom pane shows the details of a selected frame (Frame 8531). The Ethernet II section shows the source as Dell_19:49:50 (a4:ba:db:19:49:50) and the destination as LenovoEM_b0:63:a4 (00:59:07:b0:63:a4). The IP section shows the source as 172.16.4.205 and the destination as 172.16.4.4. The TCP section shows the source port as 4444 and the destination port as 88. The packet bytes pane shows the raw data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
8520	126.985000900	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	206	TGS-REP
8531	127.042119300	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	72	TGS-REP
26564	380.660622400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	206	TGS-REP
26955	382.012137600	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	84	TGS-REP
80301	820.618390400	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	204	AS-REP
80313	820.681627100	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	219	TGS-REP
80354	820.922716100	mind-hammer-dc.mind...	Rotterdam-PC.mind-h...	KRB5	158	TGS-REP

Frame 8531: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0, id 0
Ethernet II, Src: Dell_19:49:50 (a4: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 (a4:ba:db:19:49:50)
Address: Dell_19:49:50 (a4:ba:db:19:49:50)
...0... = LG bit: Globally unique address (factory default)

0000 00 59 07 b0 63 a4 a4 ba db 19 49 50 08 00 45 00 .Y..c...IP..E.
0010 00 3a 0d 43 40 00 80 06 8c 89 ac 10 04 04 ac 10 :.C@.....
0020 04 cd 00 58 c0 64 04 bf cc 16 2b 35 2f 6e 50 18 ...X.d...+5/nP.
0030 02 01 25 6c 00 00 01 b4 a8 44 cb 3a e8 1a a1 d3 ...%l...D:....
0040 cd 99 07 f5 2e 17 38 5e8^

Frame (72 bytes) Reassembled TCP (1478 bytes)

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

The username is matthijs.devries

ip.src == 172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
80291	820.573710700	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	297	AS-REQ
80299	820.590889200	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	377	AS-REQ
80469	821.371530200	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	301	AS-REQ
80476	821.387161300	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	381	AS-REQ
80508	821.513841300	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	292	AS-REQ
80515	821.529402100	Rotterdam-PC.mind-h...	mind-hammer-dc.mind...	KRB5	372	AS-REQ

▼ cname
 name-type: KRB5-NT-PRINCIPAL (1)
 ▼ cname-string: 1 item
 CNameString: matthijs.devries
 realm: MIND-HAMMER
 ▶ sname
 till: 2037-09-13 02:48:05 (UTC)
 rtime: 2037-09-13 02:48:05 (UTC)
 nonce: 631265106

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

The IP used in the infection traffic are 172.16.4.205, 185.243.115.84, 166.62.111.64

ip.src == 172.16.4.205 and ip.addr == 185.243.115.84

No.	Time	Source	Destination	Protocol	Length	Info
7449	115.232944500	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	66	49249 → http(80) [SYN] Seq=0
7452	115.236016600	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → http(80) [ACK] Seq=1
7453	115.244751500	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	546	49249 → http(80) [PSH, ACK] S
7454	115.246773000	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	126	POST /empty.gif HTTP/1.1 (ap
7466	115.367501900	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → http(80) [ACK] Seq=56
7471	115.437716000	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → http(80) [ACK] Seq=56
7472	115.438621600	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → http(80) [ACK] Seq=56
7473	115.439400200	Rotterdam-PC.mind-h...	b5689023.green.matt...	TCP	60	49249 → http(80) [ACK] Seq=56

Frame 26476: 60 bytes on wire (480 bits) captured on interface eth0

Ethernet II, Src: LenovoEM-b0:08:00:27:7d:11, Dst: 08:00:27:7d:11:11

Internet Protocol Version 4, Src: 172.16.4.205, Destination: 185.243.115.84

0100 = Version: 4

.... 0101 = Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0x3d1e (15550)

Flags: 0x4000, Don't fragment

Window: 0

Sequence Number: 0

Payload Length: 0

Protocol: 6 (TCP)

Options: (0) No options

Wireshark - Conversations - eth0

Ethernet · 76	IPv4 · 879	IPv6 · 2	TCP · 1074	UDP · 1815			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
172.16.4.205	185.243.115.84	36,952	33 M	19,616	15 M	17,336	1
166.62.111.64	172.16.4.205	22,111	22 M	16,022	22 M	6,089	43
192.168.1.90	192.168.1.100	9,556	43 M	6,219	43 M	3,337	93
10.0.0.201	64.187.66.143	9,376	6,986 k	4,296	278 k	5,080	6,700
5.101.51.151	10.6.12.203	8,652	8,493 k	6,524	8,355 k	2,128	13
10.0.0.201	23.43.62.169	8,014	8,161 k	2,620	143 k	5,394	8,014
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,211
10.6.12.12	10.6.12.203	2,776	700 k	1,240	323 k	1,536	37
10.6.12.12	10.6.12.157	2,632	661 k	1,216	313 k	1,416	34
10.11.11.11	10.11.11.200	2,200	439 k	986	197 k	1,214	24
10.0.0.2	10.0.0.201	2,166	532 k	1,040	267 k	1,126	26
10.11.11.200	104.18.74.113	2,158	1,394 k	1,022	69 k	1,136	1,320
172.16.4.4	172.16.4.205	1,902	455 k	918	193 k	984	26
10.11.11.11	10.11.11.203	1,686	379 k	702	166 k	984	21
10.11.11.179	13.33.255.25	1,456	1,040 k	678	69 k	778	97
10.11.11.217	172.217.6.162	1,394	809 k	682	70 k	712	73
10.6.12.203	205.185.125.104	1,294	1,198 k	370	20 k	924	1,170
10.0.0.201	172.217.9.2	1,132	565 k	542	63 k	590	50

☐ Name resolution

☐ Limit to display filter

☐ Absolute start time

Conversation Types ▼

Copy

Follow Stream...

Graph...

Close

Help

4. As a bonus, retrieve the desktop background of the Windows host.

