

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.

1. Domain name of the users' custom site: frank-n-ted.com

a.

No.	Time	Source	Destination	Protocol	Length	Info
70168	738.121443	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xb...
70169	738.122321	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224...
70170	738.123150	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224...
70171	738.124029	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224...
70172	738.124870	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224...
70173	738.126151	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-8...
70174	738.127593	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 16...
70175	738.128784	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-8...
70176	738.129776	10.6.12.157	224.0.0.22	TCPDU2	62	Membership Report / Join group 224...

... 0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0xf643 [validation disabled]
[Header checksum status: Unverified]
Source: 10.6.12.157
Destination: 10.6.12.12
User Datagram Protocol, Src Port: 50264, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x838c
Protocol: 0x0000 Standard query
0000 98 40 bb 2a f7 e5 00 11 75 68 42 d3 08 00 45 00 .B.....uhB...E.
0010 00 40 17 a9 00 00 80 11 f6 43 0a 00 0c 9d 0a 0e ..L.....C....
0020 0c 0c c4 58 00 35 00 38 ff ae 83 8c 01 00 00 01 .X 5 8
0030 00 00 00 00 00 00 0e 66 72 61 6e 6b 2d 6e 2d 74 65f rank-n-t
0040 65 64 2d 64 63 0b 66 72 61 6e 6b 2d 6e 2d 74 65 ed-dc fr rank-n-te
0050 64 03 63 0f 6d 00 00 01 00 01 d.com ...

2. IP address of the Domain Controller (DC) of the AD network: 10.6.12.12

No.	Time	Source	Destination	Protocol	Length	Info
80960	840.470353500	10.6.12.157	10.6.12.12	TCP	66	[TCP Keep-Alive ACK] 49719 - 445 [ACK]
80961	840.471520100	10.6.12.203	10.6.12.12	DNS	80	Standard query 0x289a A wpad.frank-n-t...
80962	840.474012500	10.6.12.12	10.6.12.203	DNS	157	Standard query response 0x289a No such...
80963	840.475233700	10.6.12.203	10.6.12.12	DNS	76	Standard query 0x745e A wpad.localdomai...
80964	840.477648800	10.6.12.12	10.6.12.203	DNS	151	Standard query response 0x745e No such...
80965	840.482443100	10.6.12.157	10.6.12.12	DNS	80	Standard query 0x5025 A wpad.frank-n-t...
80966	840.482451700	10.6.12.12	10.6.12.157	DNS	157	Standard query response 0x5025 No such...
80967	840.482456200	10.6.12.12	10.6.12.203	TCP	55	[TCP Keep-Alive] 445 - 49719 [ACK] Seq...

... 0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x6837 [validation disabled]
[Header checksum status: Unverified]
Source: 10.6.12.203
Destination: 10.6.12.12
User Datagram Protocol, Src Port: 61694, Dst Port: 53
Source Port: 61694
Destination Port: 53

3. Name of the malware downloaded to the 10.6.12.203 machine: june11.dll

a.

No.	Time	Source	Destination	Protocol	Length	Info
73739	755.706356	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=222 Ack=489 W3
73746	755.718339	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
73767	755.830360	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=2945 W4
73770	755.858358	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=6629 W5
73786	755.930360	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=12769 W6
73803	756.026413	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=15225 W7
73804	756.026419	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=18909 W8
73811	756.130366	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=25049 W9
73822	756.236440	10.6.12.203	205.185.125.104	TCP	54	49739 -> 80 [ACK] Seq=480 Ack=32447 W10

```

Source: 10.6.12.203
Destination: 205.185.125.104
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
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=3mmhfnd8jp
  
```

b.

Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT
Location: http://205.185.125.104/files/june11.dll
Pragma: no-cache
Set-Cookie: _subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT;Max-Age=2678400;Path=/
Access-Control-Allow-Origin: *

GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

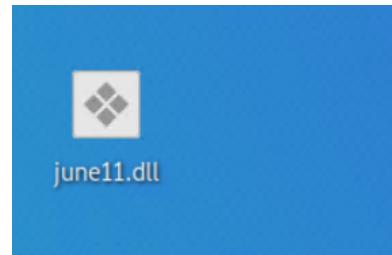
MZ.....@..... .!..L.!This
program cannot be run in DOS mode.

2 client pkts, 457 server pkts, 3 turns.

c.

Packet	Hostname	Content Type	Size	Filename
74436	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: june
 Help Save All Close Save



d.

4. Malware classification: Trojan.Mint.Zamg.O (highly likely)

A screenshot of a web browser window titled "VirusTotal - Free Online". The address bar shows the URL "https://www.virustotal.com/old-browsers/". The page displays the VirusTotal logo and a message: "This is a minimal interface for browsers that do not support full-fledged VirusTotal". Below this are three input fields: "File", "URL", and "Search". A "Browse..." button is followed by the file name "june11.dll". A "Upload" button is located below the file input field. At the bottom, there is a note: "By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more about VirusTotal."

a.

A screenshot of a web browser window titled "VirusTotal - Free Online". The address bar shows the URL "https://www.virustotal.com/old-browsers/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec". The page displays the VirusTotal logo and a message: "This is a minimal interface for browsers that do not support full-fledged VirusTotal". Below this is a detailed analysis box containing the following information:

SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Name: Googleupdate.exe
Detection ratio: 52/75

Security vendor	Result	Update
Bkav	malicious	20220726
Lionic	malicious	20220726
Elastic	malicious	20220623
MicroWorld-eScan	malicious	20220726
ALYac	malicious	20220726
Cylance	malicious	20220727
virsec	malicious	20220726

b.

The screenshot shows the VirusTotal search interface. At the top, there is a navigation bar with links for FILE, URL, and SEARCH. The SEARCH tab is currently selected. Below the navigation bar is a search bar containing the file hash: 2545b15483165d00d1b6d63d9fd0821d. To the right of the search bar is a large blue magnifying glass icon. Below the search bar, there is a note: "By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the [sharing of your Sample submission with the security community](#). Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)".

c.

The screenshot shows the VirusTotal analysis page for the file hash d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec. The page displays a red circular icon with the number 52, indicating 52 security vendors flagged the file as malicious. Below the icon, there is a "Community Score" bar. The main analysis section shows the file name Googleupdate.exe, its size (549.84 KB), and the date it was analyzed (2022-07-27 01:34:53 UTC). It also shows that the file was flagged as invalid-signature, overlay, pediI, signed, and spreader. The "DETECTION" tab is selected, showing a table of vendor findings:

Detection	Vendor	Signature	Notes
Ad-Aware	AhnLab-V3	Trojan.Mint.Zamg.O	Malware/Win32.RL_Generic.R346613
Alibaba	ALYac	TrojanSpy:Win32/Yakes.0454a340	Trojan.Mint.Zamg.O
Antiy-AVL	Arcabit	Trojan/Generic.ASCommon.1BE	Trojan.Mint.Zamg.O
Avast	AVG	Win32:DangerousSig [Tr]	Win32:DangerousSig [Tr]
Aurora (no cloud)	RisingDefender	TR/ANZ 71 cardar lardel	Trojan.Mint.Zamg.O

d.

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.

1. Information about the infected Windows machine:

- a. Host name: Rotterdam-PC
- b. IP address: 172.16.4.205
- c. MAC address: 00:59:07:b0:63:a4

d.

No.	Time	Source	Destination	Protocol	Length	Info
15095	146.839797	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<00>
15096	146.841621	172.16.4.205	172.16.4.255	NBNS	110	Registration NB MIND-HAMMER<00>
15097	146.843326	172.16.4.205	172.16.4.255	NBNS	110	Registration NB ROTTERDAM-PC<20>
15098	146.844465	172.16.4.205	224.0.0.252	LLMNR	72	Standard query 0x5e92 ANY Rotterdam-PC
15099	146.845422	172.16.4.205	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
15100	146.846388	172.16.4.205	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252
15101	146.847589	172.16.4.205	224.0.0.252	LLMNR	72	Standard query 0x817a ANY Rotterdam-PC
15102	146.848695	172.16.4.205	224.0.0.252	LLMNR	72	Standard query 0x817a ANY Rotterdam-PC
15103	146.849647	172.16.4.205	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252

```
Total Length: 58
Identification: 0x0007 (7)
Flags: 0x0000
... 0 0000 0000 0000 = Fragment offset: 0
Time to live: 1
Protocol: UDP (17)
Header checksum: 0x27d3 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.4.205
Destination: 224.0.0.252
User Datagram Protocol, Src Port: 65159, Dst Port: 5355
Link-local Multicast Name Resolution (query)
```

e.

No.	Time	Source	Destination	Protocol	Length	Info
45160	560.894060	172.16.4.4	172.16.4.205	TCP	54	49155 → 49284 [ACK] Seq=1114 Ack=2982 Win=65536
45161	560.894926	172.16.4.4	172.16.4.205	TCP	54	49155 → 49284 [FIN, ACK] Seq=1114 Ack=2982 Win=65536
45162	560.895823	172.16.4.205	172.16.4.4	TCP	56	49284 → 49155 [ACK] Seq=2982 Ack=1115 Win=65536
45163	560.901214	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1
45164	560.901234	31.7.62.214	172.16.4.205	TCP	54	443 → 49255 [ACK] Seq=520 Ack=25596 Win=65536
45165	560.905702	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1
45166	560.906571	31.7.62.214	172.16.4.205	TCP	54	443 → 49255 [ACK] Seq=520 Ack=25824 Win=65536
45167	560.911083	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1
45168	560.911943	31.7.62.214	172.16.4.205	TCP	54	443 → 49255 [ACK] Seq=520 Ack=26052 Win=65536

```
Frame 45165: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits)
Ethernet II, Src: LenovoEM_B0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
  Destination: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
  Source: LenovoEM_B0:63:a4 (00:59:07:b0:63:a4)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 31.7.62.214
  Version: 4
  .... 0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCHP: CS0, ECN: Not-ECT)
    Total Length: 268
    Identification: 0x502a (20522)
    Flags: 0x4000, Don't fragment
```

2. Username of the Windows user whose computer is infected: matthijs.devries

a.

No.	Time	Source	Destination	Protocol	Length	Info
15327	147.800631	172.16.4.205	172.16.4.4	KRB5	292	AS-REQ
15334	147.816172	172.16.4.205	172.16.4.4	KRB5	372	AS-REQ
15336	147.844358	172.16.4.4	172.16.4.205	KRB5	242	AS-REP
15347	147.903676	172.16.4.4	172.16.4.205	KRB5	150	TGS-REP
15359	147.974342	172.16.4.4	172.16.4.205	KRB5	273	TGS-REP
26415	304.980330	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
26436	305.037444	172.16.4.4	172.16.4.205	KRB5	72	TGS-REP
44505	558.655960	172.16.4.4	172.16.4.205	KRB5	206	TGS-REP
44895	560.007463	172.16.4.4	172.16.4.205	KRB5	84	TGS-REP

```
msg-type: krb-as-req (10)
  padata: 1 item
  req-body
    Padding: 0
    kdc-options: 40810010
    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)
        since: 2037-09-13 02:48:05 (UTC)
```

3. The IP addresses used in the actual infection traffic: 185.243.115.84 and 172.16.4.205

Wireshark - Conversations · packetcapture.pcap

Ethernet - 75 IPv4 - 880 IPv6 TCP - 1031 UDP - 1798

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	293.228265	265.0412
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	148.235193	149.9677
192.168.1.90	192.168.1.100	4,807	21 M	3,021	21 M	1,786	461 k	0.228795	855.2135
10.0.0.201	64.187.66.143	4,688	3,493 k	2,148	139 k	2,540	3,354 k	17.025526	129.8125
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	766.964670	67.9986
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	78.665165	66.9060
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	668.991461	66.7937
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	741.417934	99.1499
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	738.131305	102.3739
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	561.152573	176.9288
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	713.304236	22.4926
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	146.850733	414.0451
10.0.0.2	10.0.0.201	843	211 k	406	107 k	437	103 k	1.348694	845.2436
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	565.404477	172.6836
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	572.493770	94.0159

a.

4. The desktop background of the Windows host

No. ▲ Time S Search for strings containing narrow (UTF-8 and ASCII) or wide (UTF-16) characters.

No.	Time	S	Search for strings containing narrow (UTF-8 and ASCII) or wide (UTF-16) characters.	Destination	Protocol	Length	Info
36279	432.688990	1	(UTF-8 and ASCII) or wide (UTF-16) characters.	185.243.115.84	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
36278	432.683761	1		185.243.115.84	TCP	547	49249 → 80 [PSH, ACK] Seq=20538 Ack=8227236 Win=1
36276	432.675016	1		185.243.115.84	TCP	60	49249 → 80 [ACK] Seq=20538 Ack=8227236 Win=1
36276	432.674037	1		185.243.115.84	TCP	1411	[TCP Retransmission] 80 → 49249 [ACK] Seq=8224734 Ack=8224734 Win=1
36275	432.651485	1		185.243.115.84	TCP	66	49249 → 80 [ACK] Seq=20538 Ack=8224734 Win=1
36274	432.656540	1		185.243.115.84	TCP	1411	[TCP Retransmission] 80 → 49249 [ACK] Seq=8224734 Ack=8224734 Win=1
36273	432.627835	1		185.243.115.84	TCP	1199	Continuation
36272	432.608668	1		185.243.115.84	TCP	54	[TCP Previous segment not captured] 80 → 49249 [ACK] Seq=8223377 Ack=20538 Win=1
36271	432.607856	1		185.243.115.84	TCP	1411	80 → 49249 [ACK] Seq=8223377 Ack=20538 Win=1
36270	432.585238	1		185.243.115.84	HTTP	1411	Continuation
36269	432.562655	1		185.243.115.84	TCP	1411	80 → 49249 [ACK] Seq=8220663 Ack=20538 Win=1

```

Content-Type: application/x-www-form-urlencoded\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 1.1.432.5623; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E)\r\n
Host: b5689023.green.mattingsolutions.co\r\n
Content-Length: 272\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://b5689023.green.mattingsolutions.co/empty.gif]
[HTTP request 3/5]
[Prev request in frame: 25429]
[Response in frame: 36282]
[Next request in frame: 36270]

```

a.

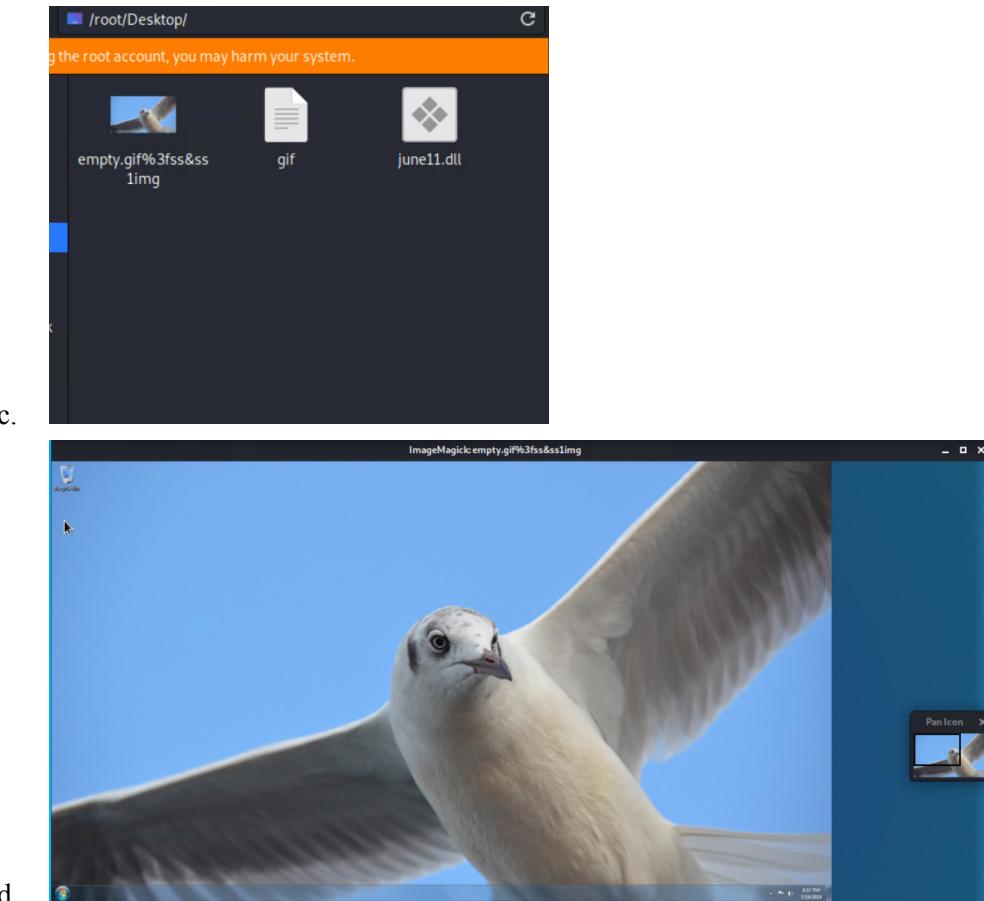
Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
40370	b5689023.green.mattingsoluti...		3,592 kB	empty.gif?ss&ss1img
44407	b5689023.green.mattingsoluti...		3,592 kB	empty.gif?ss&ss2img

Text Filter: ss&ss

Save All Close Save

b.



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.

1. Find the following information about the machine with IP address 10.0.0.201:
 - a. MAC address: 00:16:17:18:66:c8
 - b. Windows username: elmer.blanco
 - c. OS version: Windows 10.0

d.

ip.addr==10.0.0.201 && dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
80999	840.583287	10.0.0.1	10.0.0.201	DHCP	342	DHCP ACK - Transaction ID 0x20640255
Frame 80999: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) 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) Source: Cisco_27:a1:3e (00:09:b7:27:a1:3e) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.201 0100 = Version: 4 ... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x10 (DSSCP: Unknown, ECN: Not-ECT) Total Length: 328 Identification: 0x0000 (0) Flags: 0x0000 ... 0 0000 0000 0000 = Fragment offset: 0 Time to live: 16						

e.

ip.src==10.0.0.201 && kerberos.CNameString						
No.	Time	Source	Destination	Protocol	Length	Info
65617	744.239448800	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
65625	744.255672900	10.0.0.201	10.0.0.2	KRB5	381	AS-REQ
65712	744.572819700	10.0.0.201	10.0.0.2	KRB5	301	AS-REQ
65725	744.601486200	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
66970	751.007645200	10.0.0.201	10.0.0.2	KRB5	302	AS-REQ
66978	751.024207500	10.0.0.201	10.0.0.2	KRB5	382	AS-REQ
67036	751.190289600	10.0.0.201	10.0.0.2	KRB5	290	AS-REQ
67044	751.205833000	10.0.0.201	10.0.0.2	KRB5	370	AS-REQ
padata: 2 items req-body Padding: 0 kdc-options: 40810010 chame name-type: KRB5-NT-PRINCIPAL (1) cname-string: 1 item CNameString: elmer.blanco realm: DOGOFTHEYEAR sname till: 2037-09-13 02:48:05 (UTC) rtime: 2037-09-13 02:48:05 (UTC) nonce: 634194364 etype: 6 items addresses: 1 item BLANCO-DESKTOP<20>						

2. Torrent file the user download: Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

a.

```

ip.addr==10.0.0.201 && http.request
No. Time Source Destination Protocol Length Info
69347 767.585292600 10.0.0.201 168.215.194.14 HTTP 531 GET /usercomments.html?movieid=513 HTT
69434 768.625230500 10.0.0.201 52.94.240.125 HTTP 427 GET /s/ads-common.js HTTP/1.1
69470 768.919511100 10.0.0.201 72.21.202.62 HTTP 885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&
69542 769.560506300 10.0.0.201 52.94.233.131 HTTP 1067 GET /1/associates-ads/1/OP/?cb=1531628
69706 770.366956400 10.0.0.201 168.215.194.14 HTTP 589 GET /bt/btdownload.php?type=torrent&fi
69730 770.527609800 10.0.0.201 239.255.255.250 SSDP 142 M-SEARCH * HTTP/1.1
69731 770.529887200 10.0.0.201 239.255.255.250 SSDP 142 M-SEARCH * HTTP/1.1
69732 770.532212100 10.0.0.201 239.255.255.250 SSDP 142 M-SEARCH * HTTP/1.1
69750 770.563257500 10.0.0.201 140.211.166.134 HTTP 195 GET /version-1.0 HTTP/1.1

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: 10.0.0.201, Dst: 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
        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\r\n
        Accept-Language: en-US\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
        Upgrade-Insecure-Requests: 1\r\n
        Accept-Encoding: gzip, deflate\r\n
        Host: www.publicdomaintorrents.com\r\n
        Connection: Keep-Alive\r\n
\r\n

```

b.

Packet	Hostname	Content Type	Size	Filename
67306	publicdomaintorrents.info	text/html	16 kB	nshowcat.html?category=animation
67327	publicdomaintorrents.info	image/gif	10 kB	srsbanner.gif
67358	publicdomaintorrents.info	image/png	7,922 bytes	hsale.png
67363	publicdomaintorrents.info	image/gif	572 bytes	psp.gif
67364	publicdomaintorrents.info	image/jpeg	517 bytes	ipod.jpg
67367	publicdomaintorrents.info	image/jpeg	910 bytes	pda.jpg
67384	publicdomaintorrents.info	image/jpeg	1,764 bytes	googlevid.jpg
67424	publicdomaintorrents.info	image/gif	2,708 bytes	rentme.gif
67430	publicdomaintorrents.info	image/jpeg	19 kB	pdheader.jpg
67813	publicdomaintorrents.info	image/x-icon	3,638 bytes	favicon.ico
69165	publicdomaintorrents.info	text/html	10 kB	nshowmovie.html?movieid=513
69417	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
69422	publicdomaintorrents.info	image/gif	916 bytes	yellow-star.gif
69426	publicdomaintorrents.info	image/jpeg	568 bytes	divxi.jpg
69466	publicdomaintorrents.info	text/html	281 bytes	usercomments.html?movieid=513
69602	fls-na.amazon-adsystem.com	image/gif	43 bytes	?cb=1531628232887&p=%7B%22program%22%
69719	www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
69756	download.deluge-torrent.org		7 bytes	version-1.0
69761	torrent.ubuntu.com:6969	text/plain	431 bytes	announce?info_hash=%e4%be%9eM%b8v%e3%
69995	files.publicdomaintorrents.com	text/html	553 bbytes	announce.php?info hash=%1d%da%0d%a%8%

Text Filter: torrent

