

Network Forensic Analysis Report

Time Thieves

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

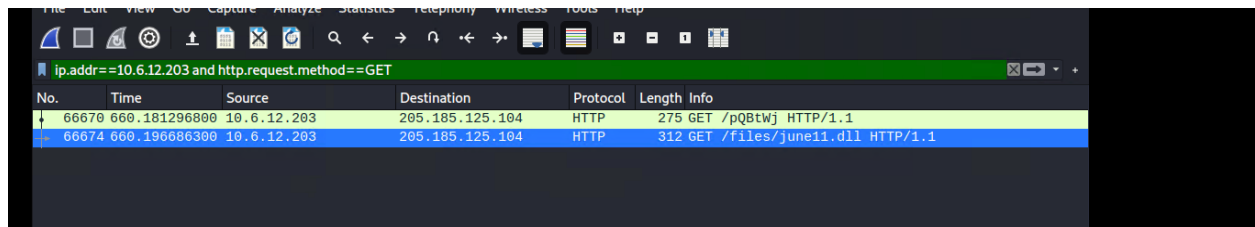
Frank-n-Ted.DC.frand-n-ted.com

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?

June11.dll

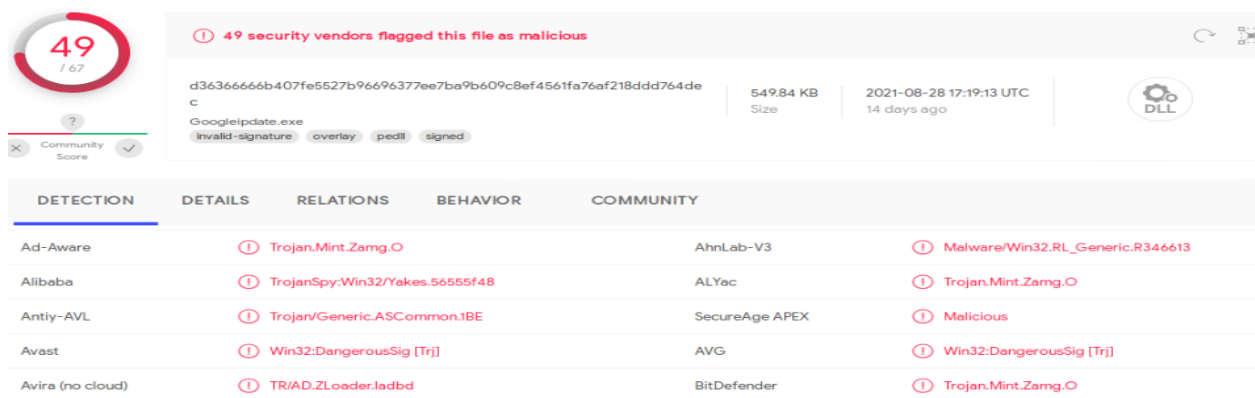


Wireshark packet capture showing traffic on interface eth0. The filter is `ip.addr==10.6.12.203 and http.request.method==GET`. The table below shows the first 2 packets.

No.	Time	Source	Destination	Protocol	Length	Info
66670	660.181296800	10.6.12.203	205.185.125.104	HTTP	275	GET /pQ8tWj HTTP/1.1
66674	660.196686300	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1

4. What kind of malware is this classified as?

Trojan



VirusShare analysis of a file. The file is `d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764de`, 549.84 KB, uploaded on 2021-08-28 17:19:13 UTC. The file is classified as malicious by 49 security vendors. The analysis shows the file is a Trojan, specifically `Trojan.Mint.Zamg.O`.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.Mint.Zamg.O			AhnLab-V3
Alibaba	① TrojanSpy:Win32/Yakes.56555f48			ALYac
Antiy-AVL	① Trojan/Generic.ASCommon.1BE			SecureAge APEX
Avast	① Win32:DangerousSig [Trj]			AVG
Avira (no cloud)	① TR/AD.ZLoader.ladbd			BitDefender

Vulnerable Windows Machine

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.src==172.16.4.4 and kerberos.CNameString		
No.	Time	Source
3319	51.391270600	172.16.4.4
3331	51.454512400	172.16.4.4
3372	51.695589100	172.16.4.4
3392	51.801890100	172.16.4.4
3496	52.187545300	172.16.4.4
3508	52.248171300	172.16.4.4
3535	52.330387000	172.16.4.4
3546	52.389745900	172.16.4.4
3558	52.454746100	172.16.4.4

as-rep

pvno: 5

msg-type: krb-as-rep (11)

padata: 1 item

crealm: MIND-HAMMER.NET

cname

name-type: kRB5-NT-PRINCIPAL (1)

cname-string: 1 item

CNameString: ROTTERDAM-PC\$

ip.src==172.16.4.4 and kerberos.CNameString					
No.	Time	Source	Destination	Protocol	Length
3319	51.391270600	172.16.4.4	172.16.4.205	KRB5	204
3331	51.454512400	172.16.4.4	172.16.4.205	KRB5	219
3372	51.695589100	172.16.4.4	172.16.4.205	KRB5	158
3392	51.801890100	172.16.4.4	172.16.4.205	KRB5	84
3496	52.187545300	172.16.4.4	172.16.4.205	KRB5	204
3508	52.248171300	172.16.4.4	172.16.4.205	KRB5	130
3535	52.330387000	172.16.4.4	172.16.4.205	KRB5	242
3546	52.389745900	172.16.4.4	172.16.4.205	KRB5	150
3558	52.454746100	172.16.4.4	172.16.4.205	KRB5	273

Frame 3392: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface

Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM_b0:63:a4

Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205

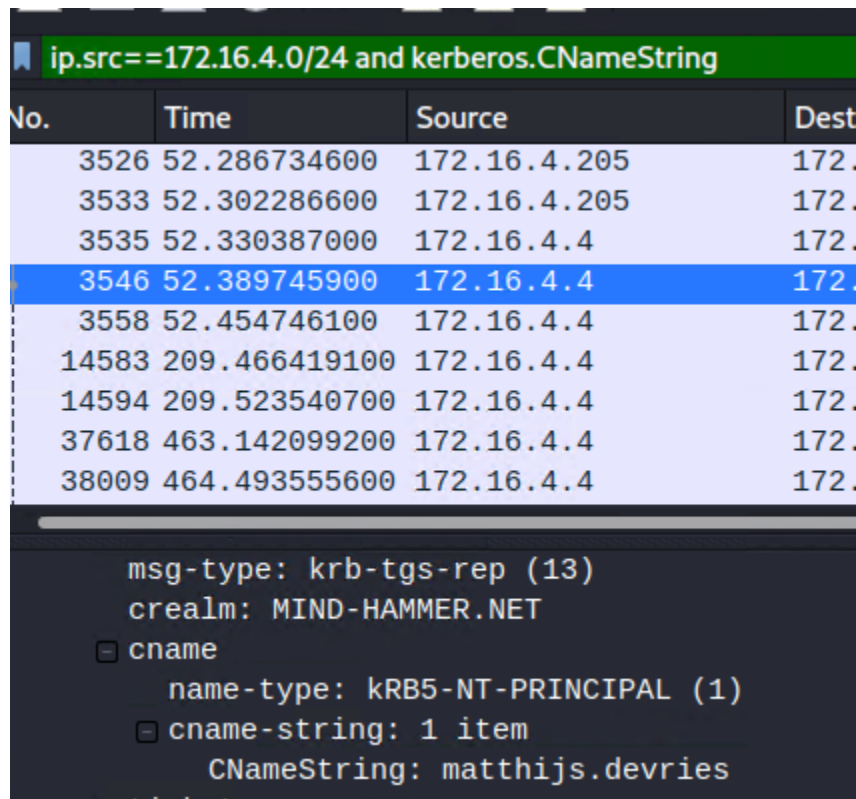
Transmission Control Protocol, Src Port: 88, Dst Port: 49168, Seq: 1461, Ack

[2 Reassembled TCP Segments (1490 bytes): #3391(1460), #3392(30)]

```
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Dell_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM
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
.... ...0 .... = IG bit: Individual address (unicast)
```

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

matthijs.devries

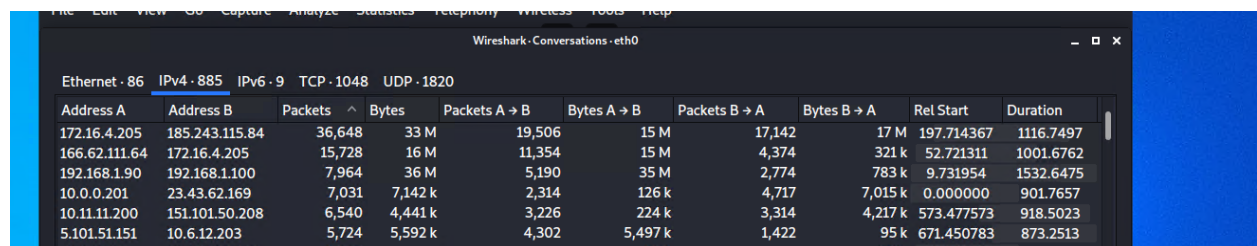


No.	Time	Source	Dest
3526	52.286734600	172.16.4.205	172.
3533	52.302286600	172.16.4.205	172.
3535	52.330387000	172.16.4.4	172.
3546	52.389745900	172.16.4.4	172.
3558	52.454746100	172.16.4.4	172.
14583	209.466419100	172.16.4.4	172.
14594	209.523540700	172.16.4.4	172.
37618	463.142099200	172.16.4.4	172.
38009	464.493555600	172.16.4.4	172.

msg-type: krb-tgs-rep (13)
crealm: MIND-HAMMER.NET
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?

172.16.4.205, 185.243.115.84, 166.62.11.64



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	36,648	33 M	19,506	15 M	17,142	17 M	197.714367	1116.7497
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	52.721311	1001.6762
192.168.1.90	192.168.1.100	7,964	36 M	5,190	35 M	2,774	783 k	9.731954	1532.6475
10.0.0.201	23.43.62.169	7,031	7,142 k	2,314	126 k	4,717	7,015 k	0.000000	901.7657
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,217 k	573.477573	918.5023
5.101.51.151	10.6.12.203	5,724	5,592 k	4,302	5,497 k	1,422	95 k	671.450783	873.2513
10.0.0.201	64.107.66.113	4,882	2,537 k	2,335	144 k	2,548	2,403 k	40.006037	854.0167

Illegal Downloads

1. Find the following information about the machine with IP address `10.0.0.201`:

- MAC address

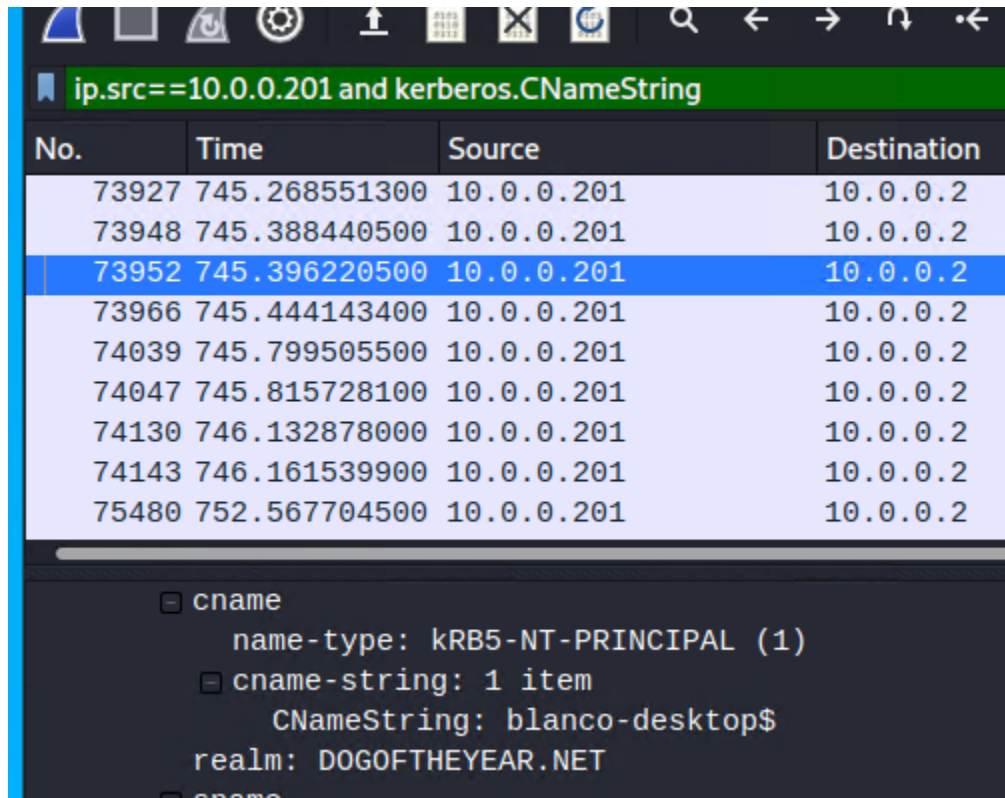
00:16:17:18:66:c8

- Windows username

elmer.blanco

- OS version

BLANCO-DESKTOP



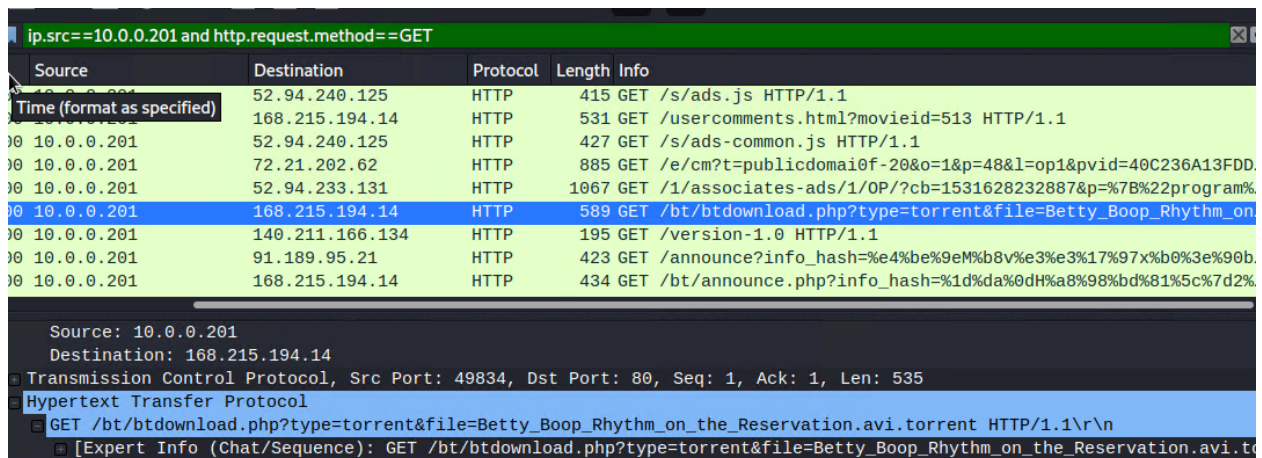
ip.src==10.0.0.201 and kerberos.CNameString

No.	Time	Source	Destination
73927	745.268551300	10.0.0.201	10.0.0.2
73948	745.388440500	10.0.0.201	10.0.0.2
73952	745.396220500	10.0.0.201	10.0.0.2
73966	745.444143400	10.0.0.201	10.0.0.2
74039	745.799505500	10.0.0.201	10.0.0.2
74047	745.815728100	10.0.0.201	10.0.0.2
74130	746.132878000	10.0.0.201	10.0.0.2
74143	746.161539900	10.0.0.201	10.0.0.2
75480	752.567704500	10.0.0.201	10.0.0.2

[-] cname
name-type: kRB5-NT-PRINCIPAL (1)
[-] cname-string: 1 item
CNameString: blanco-desktop\$
realm: DOGOFTHEYEAR.NET

2. Which torrent file did the user download?

Betty_Boop_Rythm_on_the_Reservation.avi.torrent



ip.src==10.0.0.201 and http.request.method==GET

Source	Destination	Protocol	Length	Info
10.0.0.201	52.94.240.125	HTTP	415	GET /s/ads.js HTTP/1.1
10.0.0.201	168.215.194.14	HTTP	531	GET /usercomments.html?movieid=513 HTTP/1.1
10.0.0.201	52.94.240.125	HTTP	427	GET /s/ads-common.js HTTP/1.1
10.0.0.201	72.21.202.62	HTTP	885	GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD
10.0.0.201	52.94.233.131	HTTP	1067	GET /1/associates-ads/1/0P/?cb=1531628232887&p=%7B%22program%
10.0.0.201	168.215.194.14	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on
10.0.0.201	140.211.166.134	HTTP	195	GET /version-1.0 HTTP/1.1
10.0.0.201	91.189.95.21	HTTP	423	GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b
10.0.0.201	168.215.194.14	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%

Source: 10.0.0.201
Destination: 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
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.t