

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?

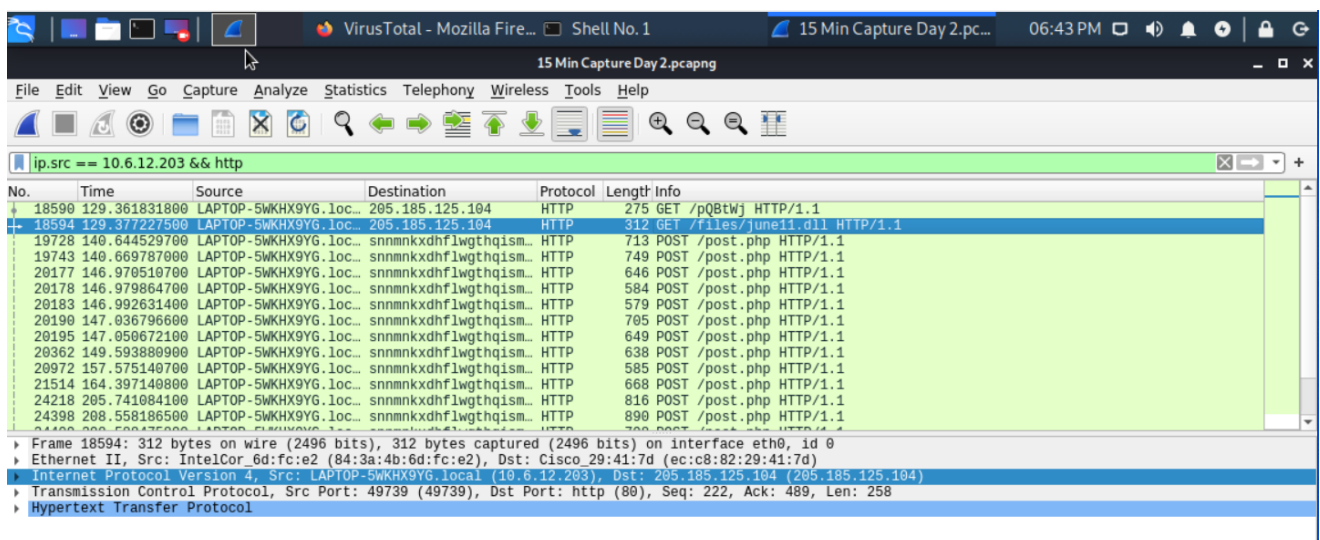
Frank-n-Ted-DC.frank-n-ted.com

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

10.6.12.12

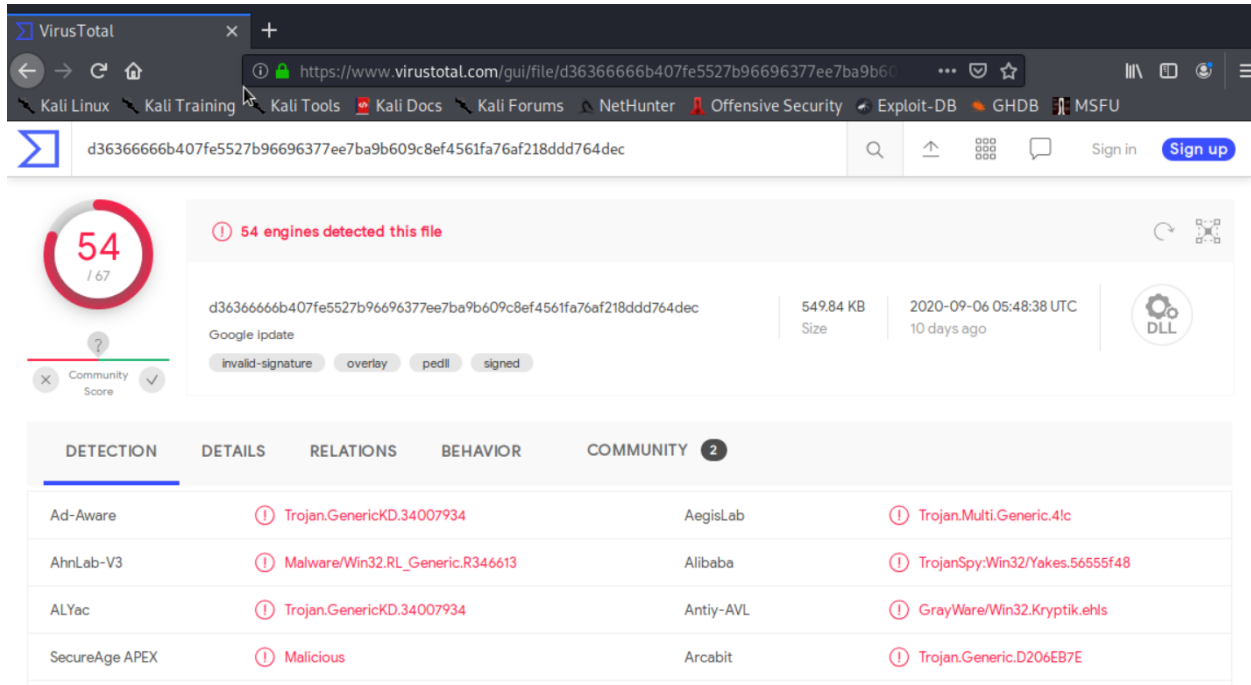
3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

june11.dll



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

june11.dll is classified as a malicious trojan horse



The screenshot shows the VirusTotal.com interface for a file analysis. The file hash is `d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The file is identified as `june11.dll` (549.84 KB, uploaded 10 days ago). It has a community score of 54/67 and is classified as a malicious trojan horse by 54 engines.

54 engines detected this file

File Hash: `d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`
Size: 549.84 KB
Uploaded: 2020-09-06 05:48:38 UTC (10 days ago)
File Type: DLL

Community Score: 54 / 67

File Properties: invalid-signature, overlay, pedll, signed

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Trojan.GenericKD.34007934	AegisLab	Trojan.Multi.Generic.4!c	
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48	
ALYac	Trojan.GenericKD.34007934	Antiy-AVL	GrayWare/Win32.Kryptik.ehls	
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D206EB7E	

Vulnerable Windows Machines

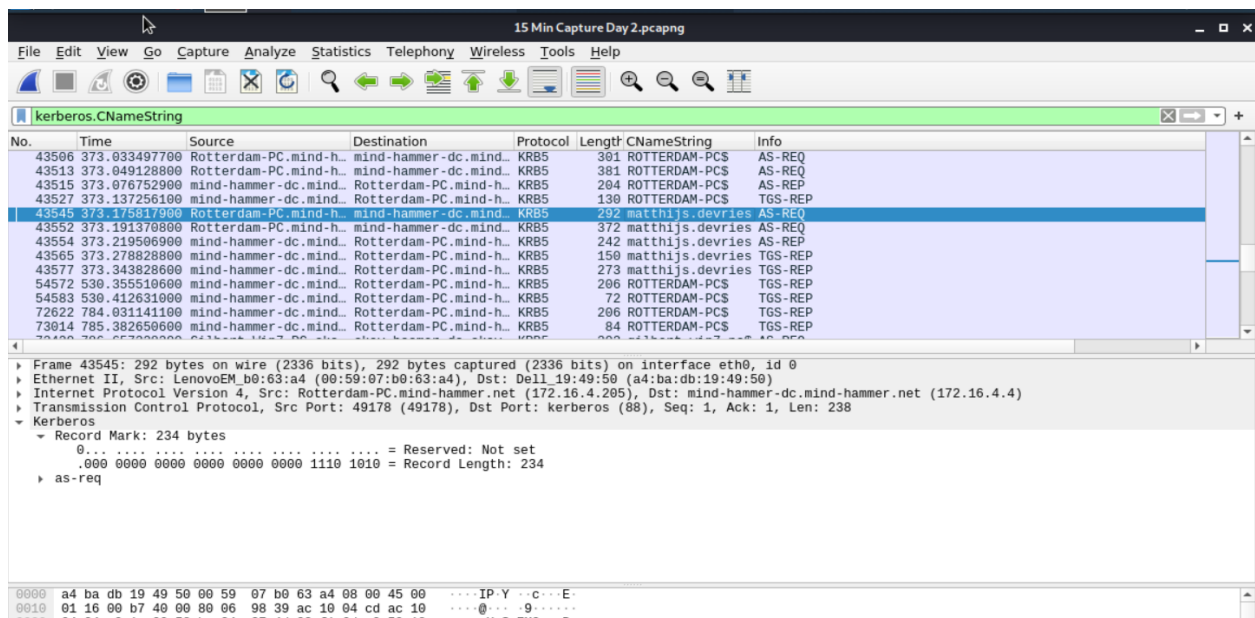
The Security team received reports of an infected Windows host on the network. They know the following:

- 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?

The username is matthijs.devries



No.	Time	Source	Destination	Protocol	Length	CNameString	Info
43506	373.833497700	Rotterdam-PC.mind-h.	mind-hammer-dc.mind-h.	KRB5	301	ROTTERDAM-PCS	AS-REQ
43513	373.849128800	Rotterdam-PC.mind-h.	mind-hammer-dc.mind-h.	KRB5	381	ROTTERDAM-PCS	AS-REQ
43515	373.876752900	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	204	ROTTERDAM-PCS	AS-REP
43527	373.137256100	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	130	ROTTERDAM-PCS	TGS-REP
43545	373.175817900	Rotterdam-PC.mind-h.	mind-hammer-dc.mind-h.	KRB5	292	matthijs.devries	AS-REQ
43552	373.191370800	Rotterdam-PC.mind-h.	mind-hammer-dc.mind-h.	KRB5	372	matthijs.devries	AS-REQ
43554	373.219506900	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	242	matthijs.devries	AS-REP
43565	373.278828800	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	150	matthijs.devries	TGS-REP
43577	373.343828600	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	273	matthijs.devries	TGS-REP
54572	530.355510800	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	206	ROTTERDAM-PCS	TGS-REP
54583	530.412631900	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	72	ROTTERDAM-PCS	TGS-REP
72622	784.031141100	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	206	ROTTERDAM-PCS	TGS-REP
73014	785.382650600	mind-hammer-dc.mind.	Rotterdam-PC.mind-h.	KRB5	84	ROTTERDAM-PCS	TGS-REP

Frame 43545: 292 bytes on wire (2336 bits), 292 bytes captured (2336 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: 49178 (49178), Dst Port: kerberos (88), Seq: 1, Ack: 1, Len: 238
Kerberos
Record Mark: 234 bytes
0... .. = Reserved: Not set
0000 0000 0000 0000 0000 0000 1110 1010 = Record Length: 234
as-req

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

185.243.115.84,

166.62.111.64

Wireshark - Conversations - Admin Support > tcpdump											
Ethernet · 76		IPv4 · 879		IPv6 · 2		TCP · 1107		UDP · 1814			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	518.603450	265.0412	240 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	373.610393	149.9677	422 k	
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,217 k	42.658102	918.5023	1,959	
192.168.1.90	192.168.1.100	5,860	27 M	3,756	26 M	2,104	568 k	0.653392	967.7679	222 k	
10.0.0.201	64.187.66.143	4,688	3,493 k	2,148	139 k	2,540	3,354 k	242.400728	129.8125	8,574	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	140.631323	67.9985	491 k	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	304.040368	66.9059	8,605	
10.11.11.200	104.18.74.113	2,158	1,394 k	1,022	69 k	1,136	1,324 k	86.970854	874.2001	640	
10.6.12.12	10.6.12.157	1,999	522 k	932	250 k	1,067	271 k	111.797969	855.0862	2,348	
10.6.12.12	10.6.12.203	1,904	493 k	864	231 k	1,040	262 k	115.086014	854.0142	2,166	
10.11.11.11	10.11.11.200	1,571	273 k	692	123 k	879	150 k	0.057437	963.3991	1,022	
10.11.11.217	172.217.6.162	1,394	809 k	682	70 k	712	738 k	1.634808	958.1931	592	
10.11.11.11	10.11.11.203	1,100	220 k	435	95 k	665	124 k	7.343076	956.1202	802	
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	214.259839	89.6854	11 k	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	372.226267	414.0447	1,862	

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: 00:09:b7:27:a1:3e
 - Windows username: BLANCO-DESKTOP
 - OS version: Windows NT 10.0
2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

