Network Analysis

Time Thieves

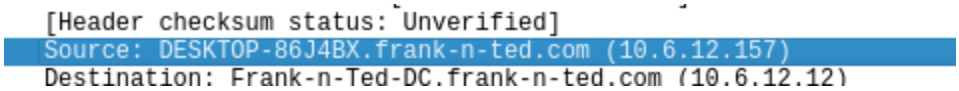
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- **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
   Hostnames:
   Desktop-86j4bx.frank-n-ted.com (10.6.12.157)
   Laptop-5wkhx9yg.frank-n-ted.com (10.6.12.203)

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. What kind of malware is this classified as?**
   Trojan

Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Trojan.Mint.Zamg.O	Avast	Win32:DangerousSig [Trj]
Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34712.lu9@aul7OQgi
W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Unsafe	Cynet	Malicious (score: 100)
Trojan.Inject3.53106	Elastic	Malicious (high Confidence)

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
    - **IP address:** 172.16.4.205
    - **MAC address:** 00:58:07:b0:63:a4

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

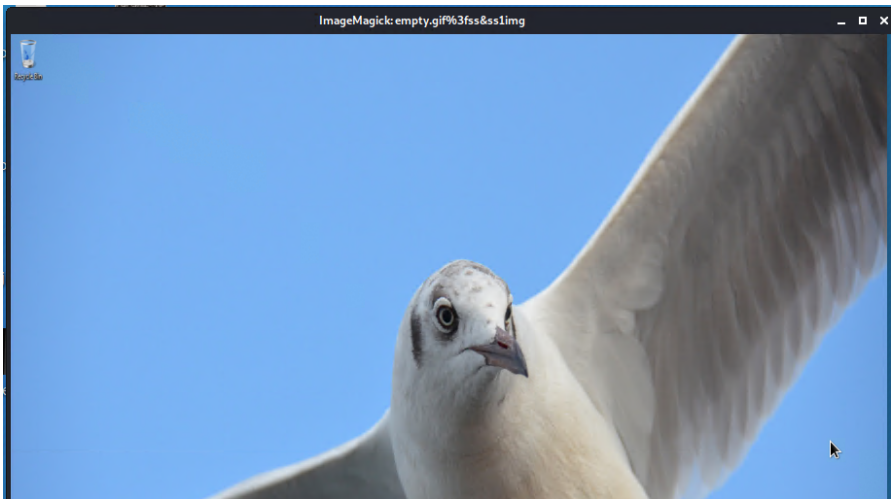
	Time	Source	Destination	Protocol	Length	CNameString
57607	488.183362000	mind-hammer-dc.mind…	Rotterdam-PC.mind-h…	KRB5	273	matthijs.devries
57595	488.118406700	mind-hammer-dc.mind…	Rotterdam-PC.mind-h…	KRB5	150	matthijs.devries
57584	488.059034700	mind-hammer-dc.mind…	Rotterdam-PC.mind-h…	KRB5	242	matthijs.devries
68702	645.273978600	mind-hammer-dc.mind…	Rotterdam-PC.mind-h…	KRB5	72	ROTTERDAM-PC$
68691	645.216951500	mind-hammer-dc.mind…	Rotterdam-PC.mind-h…	KRB5	206	ROTTERDAM-PC$

3. **What are the IP addresses used in the actual infection traffic?**
   Infected machine: 172.16.4.205
   Machines in conversation: 185.243.115.84, 166.62.111.64

Ethernet · 78 | IPv4 · 880 | IPv6 · 2 | TCP · 1040 | UDP · 1835

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	Bi
172.16.4.205	185.243.115.84	14,963	13 M	7,412	4,686 k	7,551	8,487 k	0.000000	798.6294	46 k	
10.0.0.201	64.187.66.143	9,181	6,842 k	4,209	272 k	4,972	6,569 k	356.744127	535.2381	4,075	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	488.449942	149.9895	422 k	

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 in your Network Report:

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
    - **Host Name:** BLANCO-DESKTOP

2. **Which torrent file did the user download?**
    Betty_Boop_Rhythm_on_the_Reservation.av1.torrent