

Network Analysis

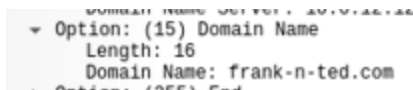
Time Thieves

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.

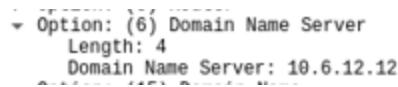
You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site? **frank-n-ted.com**



```
Option: (15) Domain Name
Length: 16
Domain Name: frank-n-ted.com
```

2. What is the IP address of the Domain Controller (DC) of the AD network?
10.6.12.12



```
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 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**
HTTP/1.1\r\n



```
for payload (200 bytes)
Hypertext Transfer Protocol
  GET /files/june11.dll HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /files
```

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

55

/ 70

?

Community Score

55 security vendors and 1 sandbox flagged this file as malicious

d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

549.84 KB

2022-08-20 15:58:35 UTC

Googleipdate.exe

Size

12 minutes ago

invalid-signature overlay peddl signed spreader

DLL

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy.Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	GrayWare/Win32.Kryptik.ehls	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32.DangerousSig [Trj]	AVG	Win32.DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34606.lu9@au!7OQgi	Bkav Pro	W32.AIDetect.malware2
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DrWeb	Trojan.Inject3.53106
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Mint.Zamg.O (B)
eScan	Trojan.Mint.Zamg.O	ESET-NOD32	Win32/Spy.Zbot.ADI
F-Secure	Trojan.TR/AD.ZLoader.ladbd	Fortinet	W32/Kryptik.DZZ!tr
GData	Trojan.Mint.Zamg.O	Google	Detected

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: **00:59:07:b0:63:a4**

```

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)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: mind-hammer-dc.mind-hammer.net (172.16.4.4), Dst: Rotterdam-PC.mind-hammer.net (172.16.4.205)
Transmission Control Protocol, Src Port: 49155, Dst Port: 49162, Seq: 0, Ack: 1, Len: 0

```

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

```

cname-string: 1 item
  CNameString: matthijs.devries
  realm: MIND-HAMMER

```

3. What is the IP address used in the actual infection traffic? **172.16.4.205**

ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84 && http.request.method == POST						
No.	Time	Source	Destination	Protocol	Length	CNameString
11663	168.334616800	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	126	POST /empty.gif HTTP/1.1 (application/x-www-form-urle
11744	168.961634200	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	534	POST /empty.gif HTTP/1.1 (application/x-www-form-urle
22566	307.781483600	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www-form-urle
26638	370.622100100	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	498	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)
30682	433.348594100	Rotterdam-PC.mind-h...	b5689023.green.matt...	HTTP	1366	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)

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

