

Network Forensic

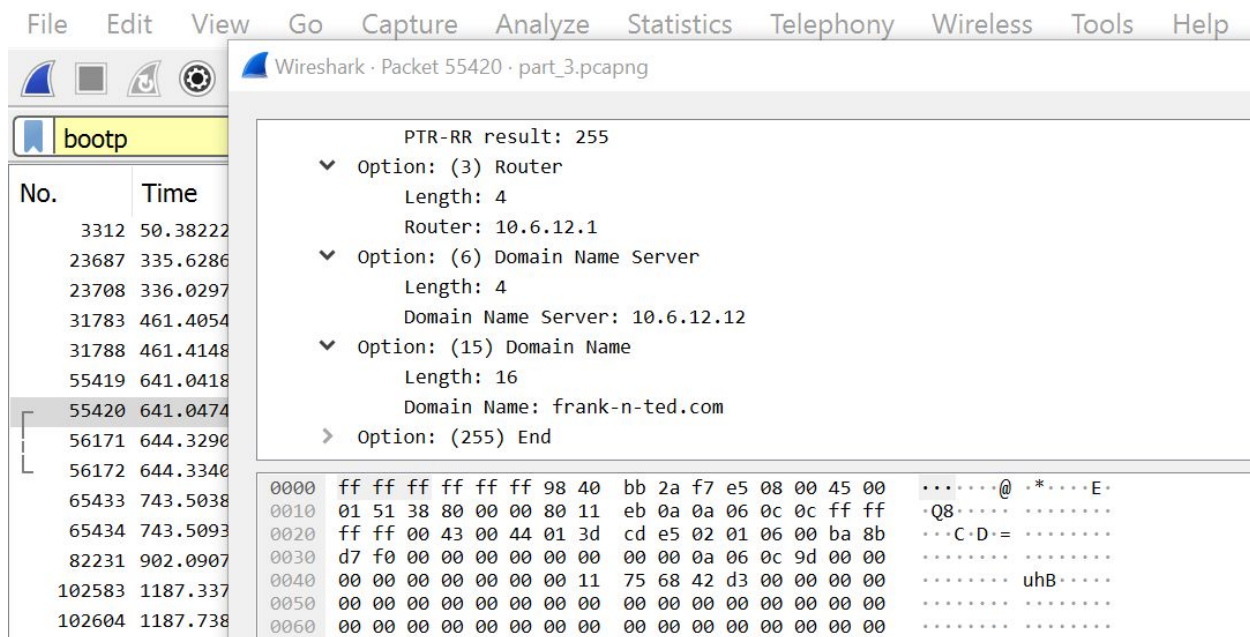
Analysis Report

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

Findings:



- Domain name of the users' custom site : **FRANK-N-TED.COM**
- IP address of the Domain Controller (DC) of the AD network : **10.6.12.12**
- Malware downloaded to the 10.6.12.203 machine: **june11.dll**
- Upload the file to [VirusTotal.com](https://www.virustotal.com) and check

X-CORP - SOC Infrastructure

The screenshot shows the VirusTotal web interface. The URL bar displays the file hash: `https://www.virustotal.com/gui/file/d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The file name is `d3636666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The file size is 549.84 KB, and it was uploaded on 2020-12-26 10:21:39 UTC (1 month ago). The file is a DLL. The detection status shows 56 engines detected this file, with a community score of 56/68. The file is classified as Trojan.Mint.Zamg.O by several engines.

| Engine | Detection |
|------------------|----------------------------------|
| Ad-Aware | Trojan.Mint.Zamg.O |
| AhnLab-V3 | Malware/Win32.RL_Generic.R346613 |
| ALYac | Trojan.Mint.Zamg.O |
| SecureAge APEX | Malicious |
| Avast | Win32:DangerousSig [Trj] |
| Avira (no cloud) | TR/AD.ZLoader.ladbd |
| AegisLab | Trojan.Multi.Generic.41c |
| Alibaba | TrojanSpy:Win32/Yakes.56555f48 |
| Antiy-AVL | GrayWare/Win32.Kryptik.ehls |
| Arcabit | Trojan.Mint.Zamg.O |
| AVG | Win32:DangerousSig [Trj] |
| BitDefender | Trojan.Mint.Zamg.O |

- Malware classification : **Trojan**

Vulnerable Windows Machine

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

- 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.

Finding the Infected Windows machine:

Wireshark Packet Analysis : Statistics

| Ethernet · 30 | | IPv4 · 808 | | IPv6 · 2 | | TCP · 1372 | | UDP · 1977 | |
|----------------|-------|------------|-------|------------|----------|------------|----------|------------|--|
| Address | Port | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | | |
| 172.16.4.205 | 49249 | 30,344 | 26M | 15,149 | 9831k | 15,195 | | | |
| 185.243.115.84 | 80 | 30,344 | 26M | 15,195 | 16M | 15,149 | | | |

| Ethernet · 30 | | IPv4 · 808 | | IPv6 · 2 | | TCP · 1372 | | UDP · 1977 | |
|----------------|---------|------------|------------|----------|------------|------------|---------|------------|--|
| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | | |
| 172.16.4.205 | 51,364 | 45M | 21,973 | 10M | 29,391 | 34M | — | | |
| 185.243.115.84 | 30,344 | 26M | 15,195 | 16M | 15,149 | 9831k | — | | |

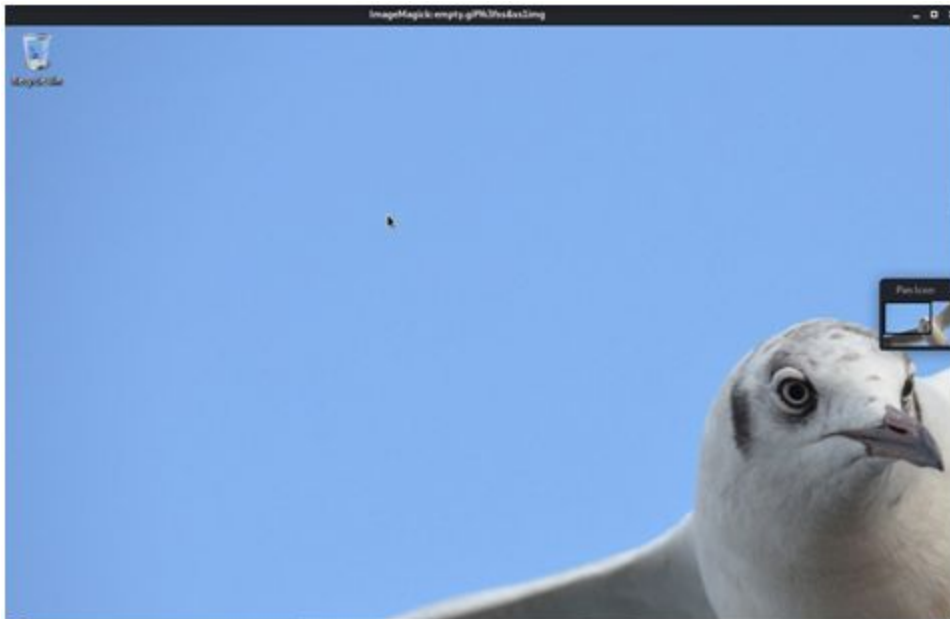
Wireshark Packet Analysis : Filter by IP

| ip.addr == 172.16.4.205 | | | | | | | |
|-------------------------|--------------|---------------|--------------|---|--------|------------------|---------|
| Packet list | | Narrow & Wide | | <input type="checkbox"/> Case sensitive | | Display filter | |
| No. | Time | Source | Destination | Protocol | Length | CNameString | Info |
| 3195 | 49.803720100 | 172.16.4.205 | 172.16.4.4 | KRB5 | 377 | rotterdam-pc\$ | AS-REQ |
| 3187 | 49.786544600 | 172.16.4.205 | 172.16.4.4 | KRB5 | 297 | rotterdam-pc\$ | AS-REQ |
| 3440 | 50.894686000 | 172.16.4.4 | 172.16.4.205 | KRB5 | 273 | matthijs.devries | TGS-REP |
| 3428 | 50.829698200 | 172.16.4.4 | 172.16.4.205 | KRB5 | 150 | matthijs.devries | TGS-REP |
| 3417 | 50.770347900 | 172.16.4.4 | 172.16.4.205 | KRB5 | 242 | matthijs.devries | AS-REP |

Note: CNameString values for hostnames always end with a \$ (dollar sign), while user account names do not.

X-CORP - SOC Infrastructure

1. Information about the infected Windows machine:
 - Host name : **ROTTERDAM-PC**
 - IP address : **172.16.4.205**
 - MAC address : **00:59:07:b0:63:a4**
2. Username of the Windows user whose computer is infected: **matthijs.devries**
3. IP addresses used in the actual infection traffic:
 - **31.7.62.214**
 - **185.243.115.84**
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.

Findings:

1. Information about the machine with IP address 10.0.0.201:

| ip.addr == 10.0.0.201 | | | | | | |
|-----------------------|---------------|------------|-------------|----------|--------|--------------|
| No. | Time | Source | Destination | Protocol | Length | CNameString |
| 67035 | 751.185656900 | 10.0.0.201 | 10.0.0.2 | TCP | 54 | |
| 67036 | 751.190289600 | 10.0.0.201 | 10.0.0.2 | KRB5 | 290 | elmer.blanco |
| 67037 | 751.194358200 | 10.0.0.2 | 10.0.0.201 | KRB5 | 254 | |
| 67038 | 751.195214100 | 10.0.0.201 | 10.0.0.2 | TCP | 54 | |
| 67039 | 751.196073800 | 10.0.0.2 | 10.0.0.201 | TCP | 54 | |

▼ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Dell_f4:3b:96 (00:12:3f:f4:3b:96)

▼ Destination: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
Address: Dell_f4:3b:96 (00:12:3f:f4:3b:96)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0 = IG bit: Individual address (unicast)

▼ Source: Msi_18:66:c8 (00:16:17:18:66:c8)
Address: Msi_18:66:c8 (00:16:17:18:66:c8)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

X-CORP - SOC Infrastructure

| ip.addr == 10.0.0.201 | | | | | | |
|-----------------------|---------------|------------|-------------|----------|--------|--------------|
| No. | Time | Source | Destination | Protocol | Length | CNameString |
| 67035 | 751.185656900 | 10.0.0.201 | 10.0.0.2 | TCP | 54 | |
| 67036 | 751.190289600 | 10.0.0.201 | 10.0.0.2 | KRB5 | 290 | elmer.blanco |
| 67037 | 751.194358200 | 10.0.0.2 | 10.0.0.201 | KRB5 | 254 | |
| 67038 | 751.195214100 | 10.0.0.201 | 10.0.0.2 | TCP | 54 | |
| 67039 | 751.196073800 | 10.0.0.2 | 10.0.0.201 | TCP | 54 | |

> kdc-options: 40810010

▼ cname

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

▼ cname-string: 1 item

CNameString: elmer.blanco

realm: DOGOFTHEYEAR

▼ sname

name-type: kRB5-NT-SRV-INST (2)

▼ sname-string: 2 items

SNameString: krbtgt

SNameString: DOGOFTHEYEAR

till: 2037-09-13 02:48:05 (UTC)

rtime: 2037-09-13 02:48:05 (UTC)

nonce: 634194387

> etype: 6 items

▼ addresses: 1 item BLANCO-DESKTOP<20>

▼ HostAddress BLANCO-DESKTOP<20>

addr-type: nETBIOS (20)

NetBIOS Name: BLANCO-DESKTOP<20> (Server service)

- MAC address : **Msi_18:66:c8 (00:16:17:18:66:c8)**
- Windows username : **elmer.blanco**
- OS version : **Windows NT 10.0**

- Downloaded Torrent file details :

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

X-CORP - SOC Infrastructure

| Text Filter: torrent | | Content Type: All Content-Types | | |
|----------------------|------------------------------------|---------------------------------|------------|---|
| Packet | Hostname | Content Type | Size | Filename |
| 67327 | publicdomaintorrents.info | image/gif | 10kB | srsbanner.gif |
| 67358 | publicdomaintorrents.info | image/png | 7922 bytes | hdsale.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 | 1764 bytes | googlevid.jpg |
| 67424 | publicdomaintorrents.info | image/gif | 2708 bytes | rentme.gif |
| 67430 | publicdomaintorrents.info | image/jpeg | 19kB | pdheader.jpg |
| 67813 | publicdomaintorrents.info | image/x-icon | 3638 bytes | favicon.ico |
| 69165 | publicdomaintorrents.info | text/html | 10kB | nshowmovie.html?movieid=513 |
| 69417 | publicdomaintorrents.info | image/jpeg | 152kB | bettyboopyrthmontherreservationgrab.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%3A%221%22%2C%22tag%22%3A%22public |
| 69719 | www.publicdomaintorrents.com | application/x-bittorrent | 8268 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%e3%17%97x%b0%3e%90b%97%be%5c%8d? |
| 69995 | files.publicdomaintorrents.com | text/html | 553 bytes | announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60% |
| 70098 | tracker.publicdomaintorrents.co... | text/plain | 40 bytes | announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe |
| 70127 | files.publicdomaintorrents.com | text/html | 320 bytes | scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe |
| 70176 | tracker.publicdomaintorrents.co... | text/plain | 171 bytes | scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe |

part_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

| No. | Time | Source | Destination | Protocol | Length | SSID | WPA Versi | BSS Id | Info |
|-------|---------------|------------|-----------------|----------|--------|------|-----------|--------|---|
| 69884 | 771.009423800 | 10.0.0.201 | 239.255.255.250 | SSDP | 142 | | | | M-SEARCH * HTTP/1.1 |
| 69883 | 771.007154800 | 10.0.0.201 | 239.255.255.250 | SSDP | 142 | | | | M-SEARCH * HTTP/1.1 |
| 69754 | 770.572697300 | 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%97%be%5c%8d? |
| 69750 | 770.563257500 | 10.0.0.201 | 140.211.166.134 | HTTP | 195 | | | | GET /version-1.0 HTTP/1.1 |
| 69732 | 770.532212100 | 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 |
| 69730 | 770.527609800 | 10.0.0.201 | 239.255.255.250 | SSDP | 142 | | | | M-SEARCH * HTTP/1.1 |
| 69706 | 770.366956400 | 10.0.0.201 | 168.215.194.14 | HTTP | 589 | | | | GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent |
| 69542 | 769.560506300 | 10.0.0.201 | 52.94.233.131 | HTTP | 1067 | | | | GET /1/associates-ads/1/OP/?cb=1531628232 |

Encapsulation type: Ethernet (1)
Arrival Time: Jun 30, 2020 10:06:31.413273900 US Mountain Standard Time
[Time shift for this packet: 0.00000000 seconds]
Epoch Time: 1593536791.413273900 seconds
[Time delta from previous captured frame: 0.009429400 seconds]
[Time delta from previous displayed frame: 0.806450100 seconds]
[Time since reference or first frame: 770.366956400 seconds]
Frame Number: 69706

0000 00 09 b7 27 a1 3e 00 16 17 18 66 c8 08 00 45 00 ...>...f...E..
0010 02 3f 76 d1 40 00 80 06 0c 39 0a 00 00 c9 a8 d7 ..?v.@...9...v..
0020 c2 0e c2 aa 00 50 97 b7 b1 25 75 99 6b 48 50 18 ...P...%u.kHP..
0030 ff ff 31 06 00 00 47 45 54 20 2f 62 74 2f 62 74 ..1...GE T /bt/bt