Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

By: Byron Epp, Jake Lasecki, Jessica Suarez, Veronica Renaud, Robert Harmon, Robert Sutherland, and Martin Quiroga

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

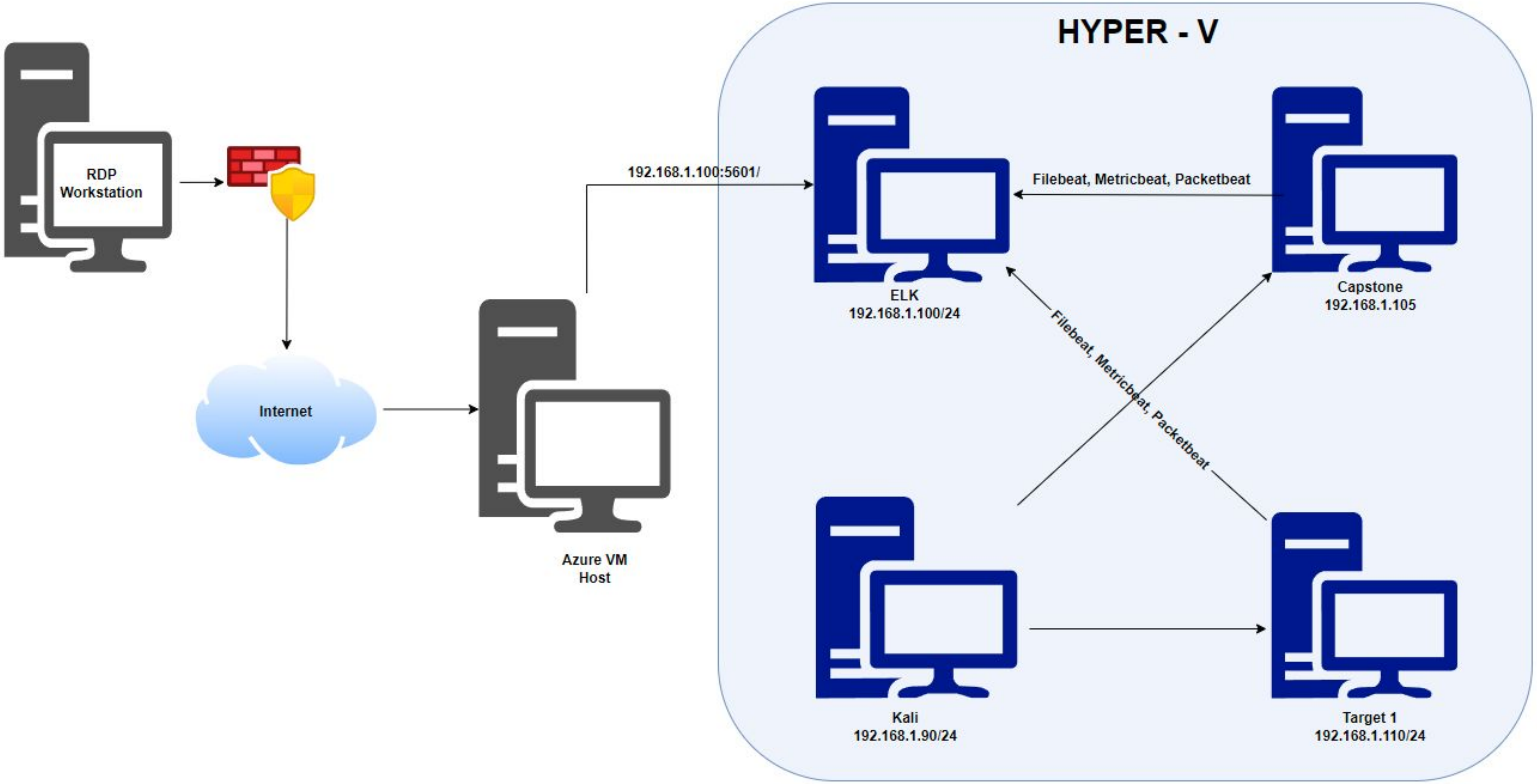
Traffic Profile

Normal Activity

Malicious Activity

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.90
OS:Linux 2.6.32
Hostname: Kali

IPv4:192.168.1.105
OS:Ubuntu
Hostname:Capstone

IPv4:192.168.1.100
OS:Linux
Hostname: ELK

IPv4:192.168.1.110
OS:Linux 3.2 - 4.9
Hostname: Target 1

Network Analysis Source

The Following Slides were completed using the provided pcap file from Gitlab

- Pcap file source: Gitlab
- Pcap file: “part_3”
- Analysis of this pcap file will show ip’s that are not native to the Azure Lab “Final” that was provided for this project

Source link:
https://ucsd.bootcampcontent.com/UCSD-Coding-Bootcamp/ucsd-sd-virt-cyber-pt-09-2021-u-c/-/tree/master/1-Lesson-Plans/24-Final-Project/Activities/Day-3-Wireshark/Unsolved

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Publicly available usernames	Anyone can enumerate the wordpress site to view usernames	Brute-force attacks are much easier if username is known
Credentials for DB stored in plain text	Someone who can get access to this machine can view credentials for DB	The DB contains password hashes for users, which can be cracked to obtain passwords
Weak passwords	Both users have short and simple passwords	These passwords can easily be brute-forced
Sudo misconfiguration	User Steven can run Python code with root privileges	An attacker with access to Steven’s account can gain root access

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 (15,195) 172.16.4.205 (15,149) 23.43.62.169 (6,934) 10.0.0.201 (2,235)	Machines that sent the most traffic.
Most Common Protocols	TCP (92,280), UDP (11,697), TLS (7200)	Three most common protocols on the network.
# of Unique IP Addresses	808 Unique IPv4 Addresses	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
Suspicious Species Identified	Trojan Torrents	Malware and suspicious activity identified on the Network

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Advertisement traffic frequently occurred for a variety of different items
- Frequent visits to a website titled frank-n-ted.com

Suspicious Activity

- Trojan malware downloaded
- “Torrent” activity on the network

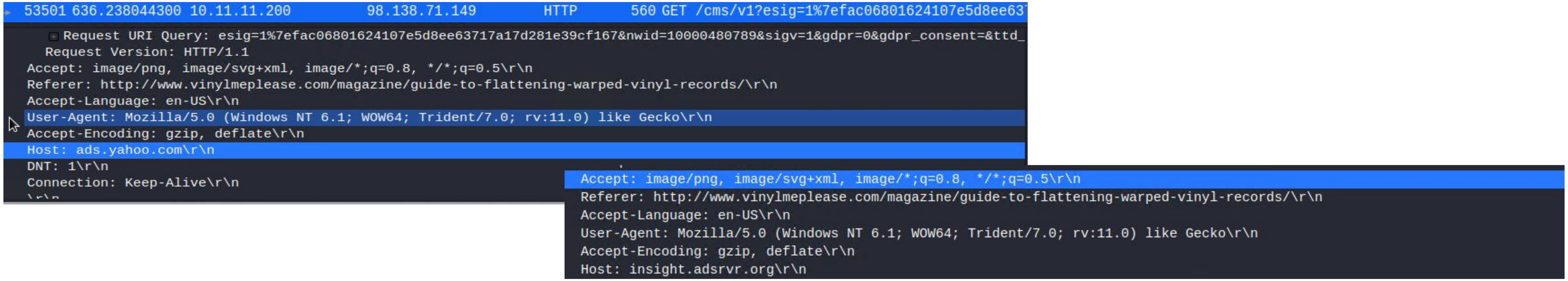
Normal Activity

Receiving Advertisement Traffic

Summarize the following:

- **What kind of traffic did you observe? Which protocol(s)?**
- The kind of traffic observed was advertisement images being served from a website the user was browsing. **HTTP/TCP** were the specific protocols.
- **What, specifically, was the user doing? Which site were they browsing?**

  The website currently being browsed is www.vinylmeplease.com/magazine/guide-to-flattening-warped-vinyl-records/ and the user was reading an article on a guide to flatten warped vinyls. The advertisements were images from yahoo and insight, that were both being referred to by that specific web host on the article that was being browsed.



```
53501 636.238044300 10.11.11.200          98.138.71.149         HTTP       560 GET /cms/v1?esig=1%7efac06801624107e5d8ee63
    ⊞ Request URI Query: esig=1%7efac06801624107e5d8ee63717a17d281e39cf167&nwid=10000480789&sigv=1&gdpr=0&gdpr_consent=&ttd_
   Request Version: HTTP/1.1
  Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5\r\n
  Referer: http://www.vinylmeplease.com/magazine/guide-to-flattening-warped-vinyl-records/\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: ads.yahoo.com\r\n
  DNT: 1\r\n
  Connection: Keep-Alive\r\n
  \r\n
```

```
Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5\r\n
Referer: http://www.vinylmeplease.com/magazine/guide-to-flattening-warped-vinyl-records/\r\n
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: insight.adsrvr.org\r\n
```

[Accessing personal domain]

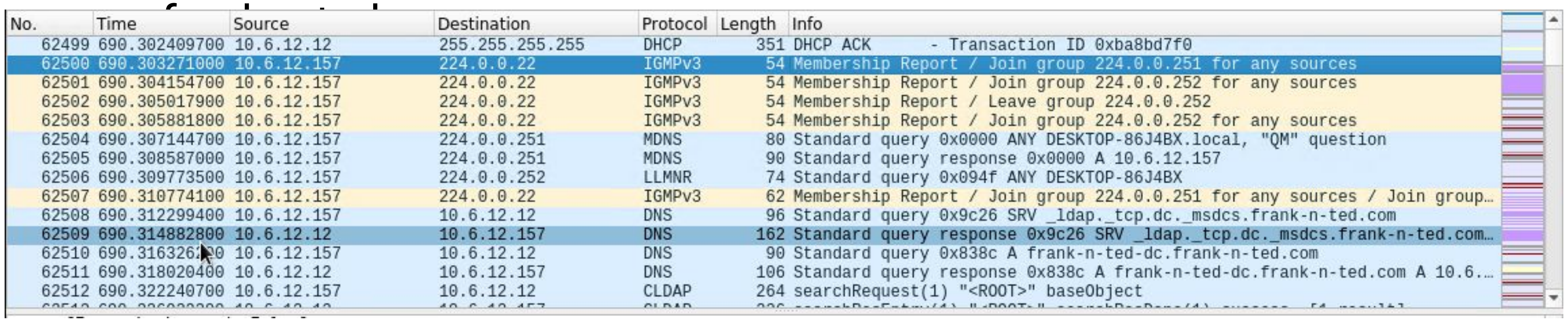
Summarize the following:

- **What kind of traffic did you observe? Which protocol(s)?**

  The traffic predominantly consists of TCP and IGMPv3 protocols where there is more activity taking place.

- **What, specifically, was the user doing? Which site were they browsing? Etc.**

  The user was making a transaction and has membership reports that the user was joining and leaving a



```
No.    Time           Source        Destination      Protocol Length Info
 62499 690.302409700 10.6.12.12    255.255.255.255  DHCP       351 DHCP ACK      - Transaction ID 0xba8bd7f0
 62500 690.303271000 10.6.12.157   224.0.0.22       IGMPv3      54 Membership Report / Join group 224.0.0.251 for any sources
 62501 690.304154700 10.6.12.157   224.0.0.22       IGMPv3      54 Membership Report / Join group 224.0.0.252 for any sources
 62502 690.305017900 10.6.12.157   224.0.0.22       IGMPv3      54 Membership Report / Leave group 224.0.0.252
 62503 690.305881800 10.6.12.157   224.0.0.22       IGMPv3      54 Membership Report / Join group 224.0.0.252 for any sources
 62504 690.307144700 10.6.12.157   224.0.0.251      MDNS        80 Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" question
 62505 690.308587000 10.6.12.157   224.0.0.251      MDNS        90 Standard query response 0x0000 A 10.6.12.157
 62506 690.309773500 10.6.12.157   224.0.0.252      LLMNR       74 Standard query 0x094f ANY DESKTOP-86J4BX
 62507 690.310774100 10.6.12.157   224.0.0.22       IGMPv3      62 Membership Report / Join group 224.0.0.251 for any sources / Join group…
 62508 690.312299400 10.6.12.157   10.6.12.12       DNS         96 Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
 62509 690.314882800 10.6.12.12    10.6.12.157      DNS        162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com…
 62510 690.316326 00 10.6.12.157   10.6.12.12       DNS         90 Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
 62511 690.318020400 10.6.12.12    10.6.12.157      DNS        106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.…
 62512 690.322240700 10.6.12.157   10.6.12.12       CLDAP      264 searchRequest(1) "<ROOT>" baseObject
```

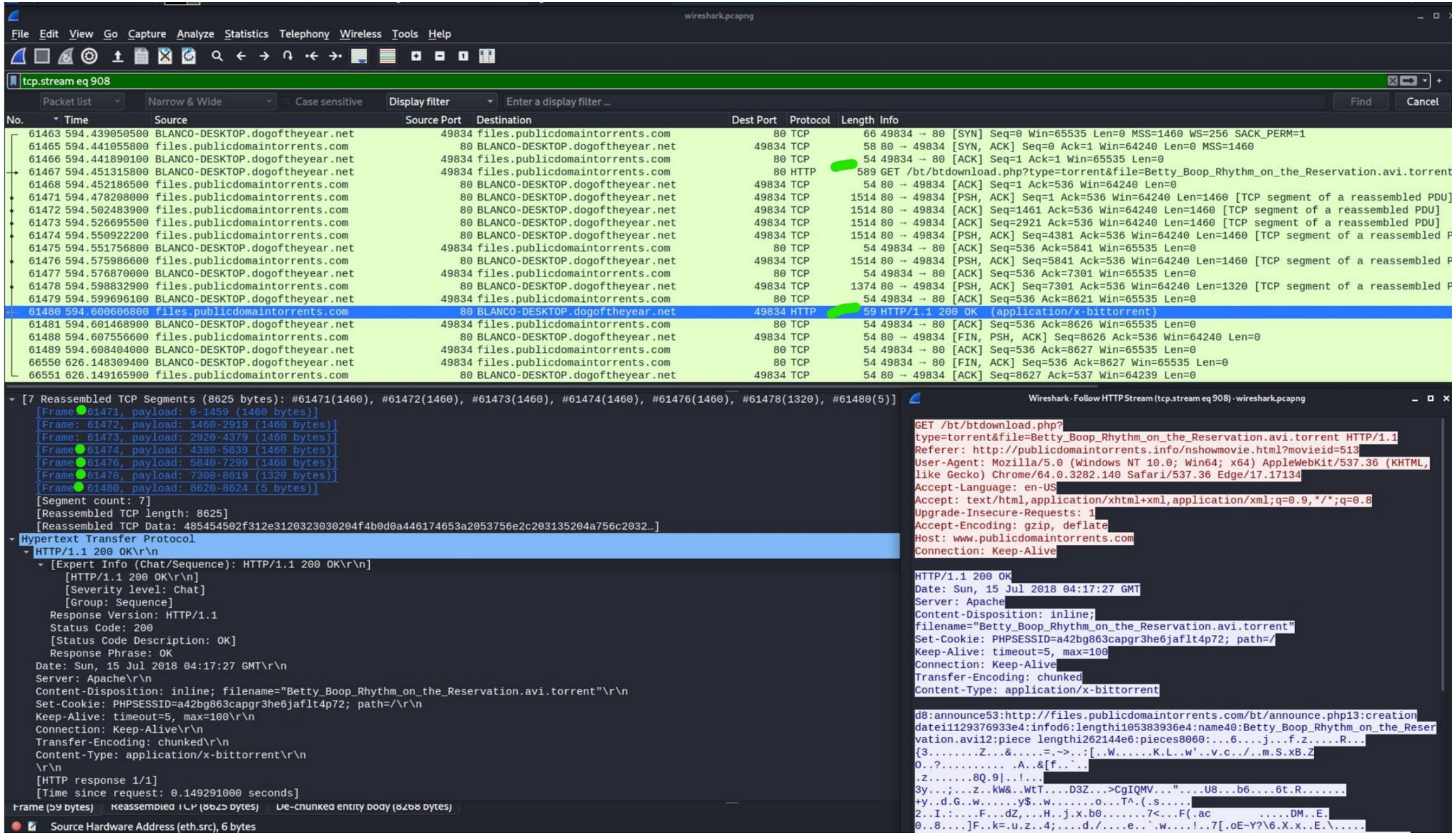
- **Include a description of any interesting files.**

  There are numerous requests for the frank-and-ted domain where there are transactions from a DESKTOP-86J4BX shown in a number of packets.

Malicious Activity

Torrent (Betty_Boo_Rhythm_on_the Reservation.avi.torrent)

The following Summarizes the Torrent via Wireshark


wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 908
Packet list
Narrow & Wide
Case sensitive
Display filter
Enter a display filter ...
Find
Cancel
Frame (59 bytes)
Reassembled TCP (8625 bytes)
De-chunked entity body (8268 bytes)
Source Hardware Address (eth.src), 6 bytes
Wireshark · Follow HTTP Stream (tcp.stream eq 908) · wireshark.pcapng

```
No.    Time          Source                          Source Port Destination                     Dest Port Protocol Length Info
61463 594.439050500 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     66 49834 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
61465 594.441055800 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP     58 80 → 49834 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
61466 594.441890100 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
61467 594.451315800 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 HTTP   589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
61468 594.452186500 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP     54 80 → 49834 [ACK] Seq=1 Ack=536 Win=64240 Len=0
61471 594.478208000 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP   1514 80 → 49834 [PSH, ACK] Seq=1 Ack=536 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
61472 594.502483900 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP   1514 80 → 49834 [ACK] Seq=1461 Ack=536 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
61473 594.526695500 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP   1514 80 → 49834 [ACK] Seq=2921 Ack=536 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
61474 594.550922200 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP   1514 80 → 49834 [PSH, ACK] Seq=4381 Ack=536 Win=64240 Len=1460 [TCP segment of a reassembled P
61475 594.551756800 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [ACK] Seq=536 Ack=5841 Win=65535 Len=0
61476 594.575986600 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP   1514 80 → 49834 [PSH, ACK] Seq=5841 Ack=536 Win=64240 Len=1460 [TCP segment of a reassembled P
61477 594.576870000 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [ACK] Seq=536 Ack=7301 Win=65535 Len=0
61478 594.598832900 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP   1374 80 → 49834 [PSH, ACK] Seq=7301 Ack=536 Win=64240 Len=1320 [TCP segment of a reassembled P
61479 594.599696100 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [ACK] Seq=536 Ack=8621 Win=65535 Len=0
61480 594.600606800 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 HTTP    59 HTTP/1.1 200 OK  (application/x-bittorrent)
61481 594.601468900 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [ACK] Seq=536 Ack=8626 Win=65535 Len=0
61488 594.607556600 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP     54 80 → 49834 [FIN, PSH, ACK] Seq=8626 Ack=536 Win=64240 Len=0
61489 594.608404000 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [ACK] Seq=536 Ack=8627 Win=65535 Len=0
66550 626.148309400 BLANCO-DESKTOP.dogoftheyear.net    49834 files.publicdomaintorrents.com       80 TCP     54 49834 → 80 [FIN, ACK] Seq=536 Ack=8627 Win=65535 Len=0
66551 626.149165900 files.publicdomaintorrents.com        80 BLANCO-DESKTOP.dogoftheyear.net   49834 TCP     54 80 → 49834 [ACK] Seq=8627 Ack=537 Win=64239 Len=0
```

```
[7 Reassembled TCP Segments (8625 bytes): #61471(1460), #61472(1460), #61473(1460), #61474(1460), #61476(1460), #61478(1320), #61480(5)]
  [Frame 61471, payload: 0-1459 (1460 bytes)]
  [Frame: 61472, payload: 1460-2919 (1460 bytes)]
  [Frame: 61473, payload: 2920-4379 (1460 bytes)]
  [Frame 61474, payload: 4380-5839 (1460 bytes)]
  [Frame 61476, payload: 5840-7299 (1460 bytes)]
  [Frame 61478, payload: 7300-8619 (1320 bytes)]
  [Frame 61480, payload: 8620-8624 (5 bytes)]
  [Segment count: 7]
  [Reassembled TCP length: 8625]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203135204a756c2032…]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Sun, 15 Jul 2018 04:17:27 GMT\r\n
  Server: Apache\r\n
  Content-Disposition: inline; filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"\r\n
  Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Transfer-Encoding: chunked\r\n
  Content-Type: application/x-bittorrent\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.149291000 seconds]
```

```
GET /bt/btdownload.php?
type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: www.publicdomaintorrents.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Jul 2018 04:17:27 GMT
Server: Apache
Content-Disposition: inline;
filename="Betty_Boop_Rhythm_on_the_Reservation.avi.torrent"
Set-Cookie: PHPSESSID=a42bg863capgr3he6jaflt4p72; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/x-bittorrent

d8:announce53:http://files.publicdomaintorrents.com/bt/announce.php13:creation
datei1129376933e4:infod6:lengthi105383936e4:name40:Betty_Boop_Rhythm_on_the_Reser
vation.avi12:piece lengthi262144e6:pieces8060:...6....j...f.z.....R...
{3........Z...&.....=.~>..:[..W......K.L..w'..v.c../..m.S.xB.Z
O..?.......... .A..&[f..`..
.z.......8Q.9|..!...
3y...;...z..kW&..WtT....D3Z...>CgIQMV..."....U8...b6....6t.R.......
+y..d.G..w......y$..w.......o...T^.(.s.....
2..I.:....F...dZ,...H..j.x.b0.......7<...F(.ac        .....DM..E.
0..8....]F..k=.u.z..4;....d./....e..`.w....!..7[.oE~Y?\6.X.x..E.\.....
```

Search:
ip.addr == 10.0.0.201 and http contains .torrent

Torrent: Allows peer to peer sharing through series of packets.

It's called theft since you are not paying for it.

http://publicdomaintorrents.info/nshowmovie

Source Address:
files.publicdomaintorrents.com

IP Address: 168.215.194.13

Media type: application/x-bittorrent

LEGALITIES:

If done for non-copyrighted materials or content you have rights to; the service is not illegal.

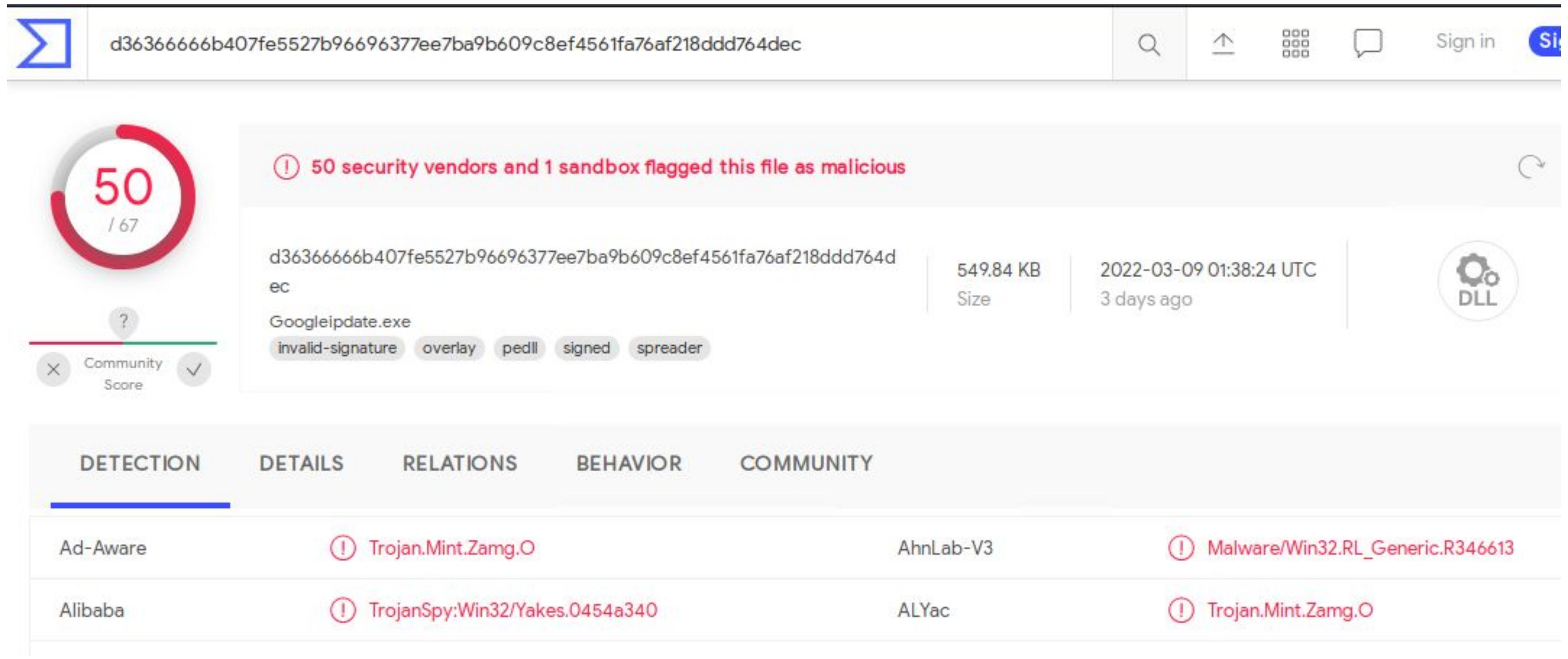
Guilty of Infringement:
Pursuant to 17 U.S. Code § 504 et seq.; 3 years; pay up to $150,000/content

https://codes.findlaw.com/us/title-17-copyrights/17-usc-sect-504.html

[June 11.dll]

Trojan Virus:

- We could observe HTTP GET traffic downloading a file from Frank n Ted, which happened on Friday, June 12th.
- They downloaded a file named June 11.dll which seemed a little suspicious.
- Upon further inspection, we found out that many security vendors had flagged that file for containing a Trojan Virus.



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

50 / 67

50 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

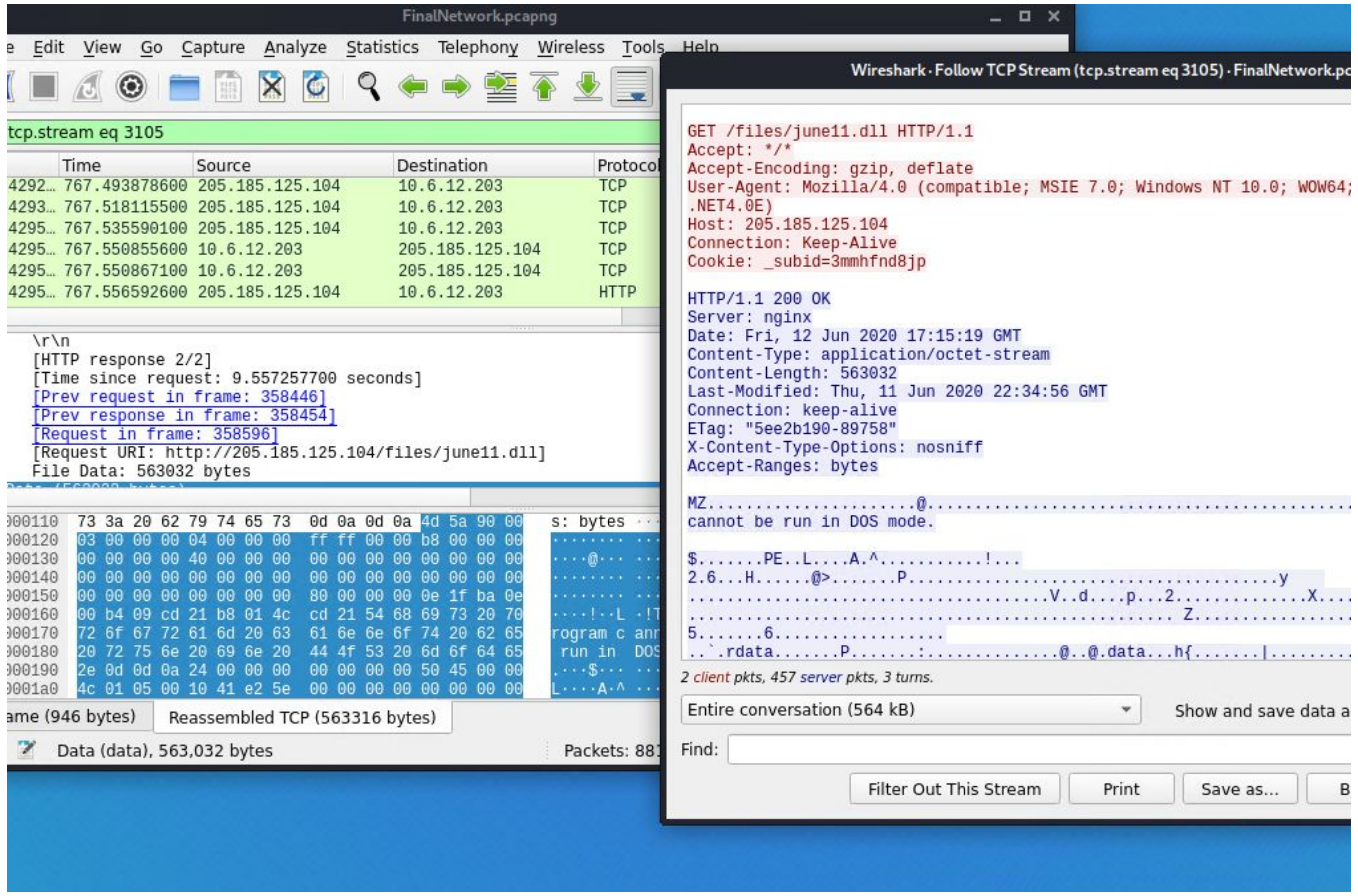
Googleipdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB
Size

2022-03-09 01:38:24 UTC
3 days ago

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O



tcp.stream eq 3105

```
     Time          Source            Destination       Protocol
4292… 767.493878600 205.185.125.104  10.6.12.203       TCP
4293… 767.518115500 205.185.125.104  10.6.12.203       TCP
4295… 767.535590100 205.185.125.104  10.6.12.203       TCP
4295… 767.550855600 10.6.12.203      205.185.125.104   TCP
4295… 767.550867100 10.6.12.203      205.185.125.104   TCP
4295… 767.556592600 205.185.125.104  10.6.12.203       HTTP
```

```
\r\n
[HTTP response 2/2]
[Time since request: 9.557257700 seconds]
[Prev request in frame: 358446]
[Prev response in frame: 358454]
[Request in frame: 358596]
[Request URI: http://205.185.125.104/files/june11.dll]
File Data: 563032 bytes
```

```
000110  73 3a 20 62 79 74 65 73  0d 0a 0d 0a 4d 5a 90 00   s: bytes ····
000120  03 00 00 00 04 00 00 00  ff ff 00 00 b8 00 00 00   ········ ···
000130  00 00 00 00 40 00 00 00  00 00 00 00 00 00 00 00   ····@··· ···
000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ···
000150  00 00 00 00 00 00 00 00  80 00 00 00 0e 1f ba 0e   ········ ···
000160  00 b4 09 cd 21 b8 01 4c  cd 21 54 68 69 73 20 70   ····!··L ·!T
000170  72 6f 67 72 61 6d 20 63  61 6e 6e 6f 74 20 62 65   rogram c ann
000180  20 72 75 6e 20 69 6e 20  44 4f 53 20 6d 6f 64 65    run in  DOS
000190  2e 0d 0d 0a 24 00 00 00  00 00 00 00 50 45 00 00   .···$··· ···
0001a0  4c 01 05 00 10 41 e2 5e  00 00 00 00 00 00 00 00   L····A·^ ···
```

Reassembled TCP (563316 bytes)

Data (data), 563,032 bytes — Packets: 881

Wireshark · Follow TCP Stream (tcp.stream eq 3105) · FinalNetwork.pc

```
GET /files/june11.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64;
.NET4.0E)
Host: 205.185.125.104
Connection: Keep-Alive
Cookie: _subid=3mmhfnd8jp

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Jun 2020 17:15:19 GMT
Content-Type: application/octet-stream
Content-Length: 563032
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT
Connection: keep-alive
ETag: "5ee2b190-89758"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

MZ.......................@...........................................
cannot be run in DOS mode.

$.......PE..L....A.^............!...
2.6...H......@>.......P.................................y
....................................V..d....p...2..............X....
..................................................Z...............
5.......6...................
..`.rdata.......P.......:..............@..@.data...h{.......|........
```

2 client pkts, 457 server pkts, 3 turns.

Entire conversation (564 kB)

Suggested Mitigation Techniques

- [June 11.dll (Trojan)]
  - An active and updated anti-malware/virus monitor
  - Configure network devices to only run trusted applications and file-types
  - Educate employees to avoid visiting suspicious or unfamiliar sites and downloading uncommonly used files
  - Establish content specific filters

- Torrent (Betty_Boo_Rhythm_on_the Reservation.avi.torrent)
  - Establish company policy for release of liability to any damages from illegal activity on the company's devices;
  - Any and all criminal fines should be paid by the employee;
  - Any illegal activity is grounds for immediate termination;
  - Blacklist torrent sites on the company network; and
  - Establish content filters for any torrent file.

Sources: https://www.cisa.gov/uscert/sites/default/files/publications/malware-threats-mitigation.pdf

The End