Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

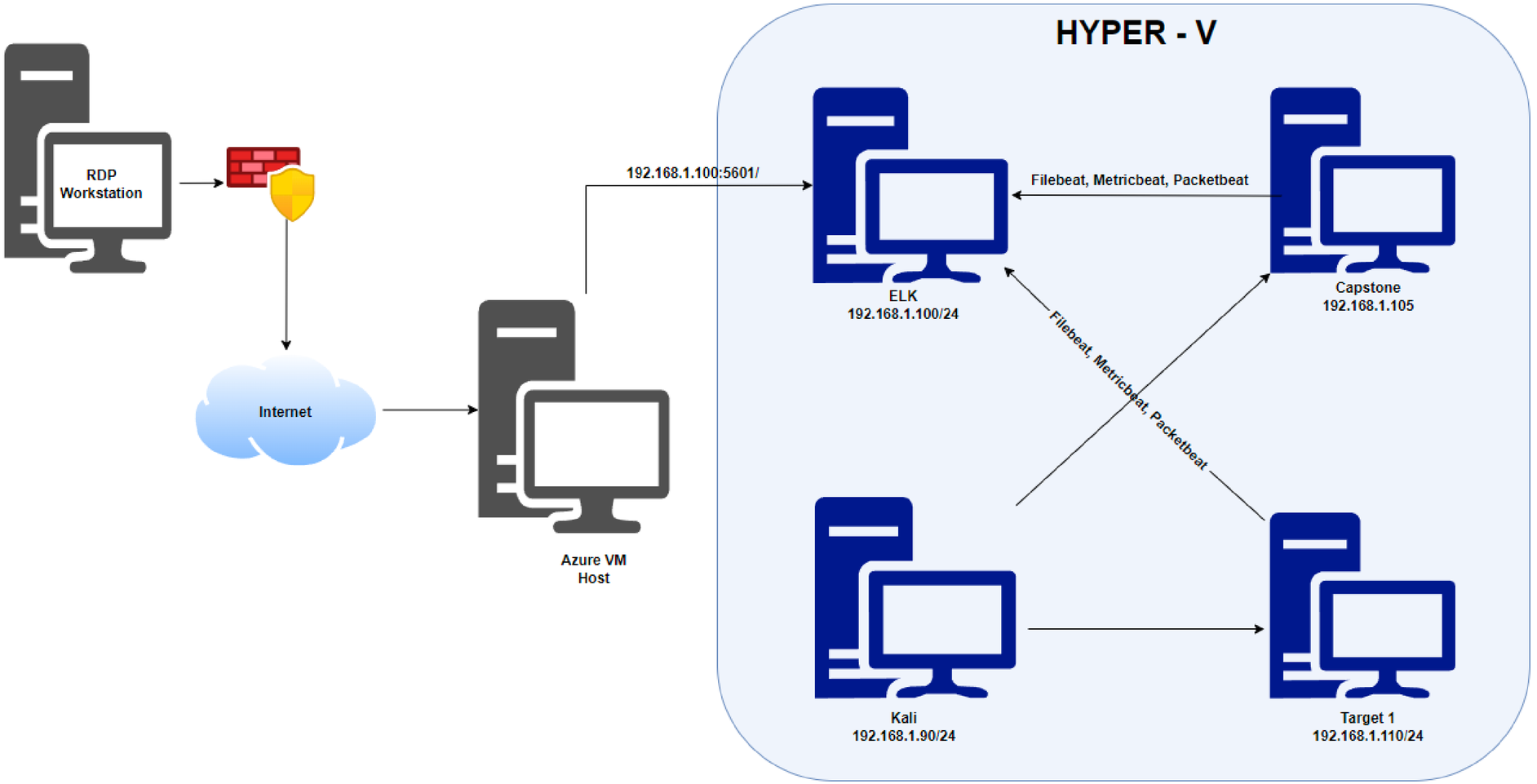
By: Byron Epp, Jake Lasecki, Jessica Suarez, Veronica Renaud, Robert Harmon, Robert Sutherland, and Martin Quiroga

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

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

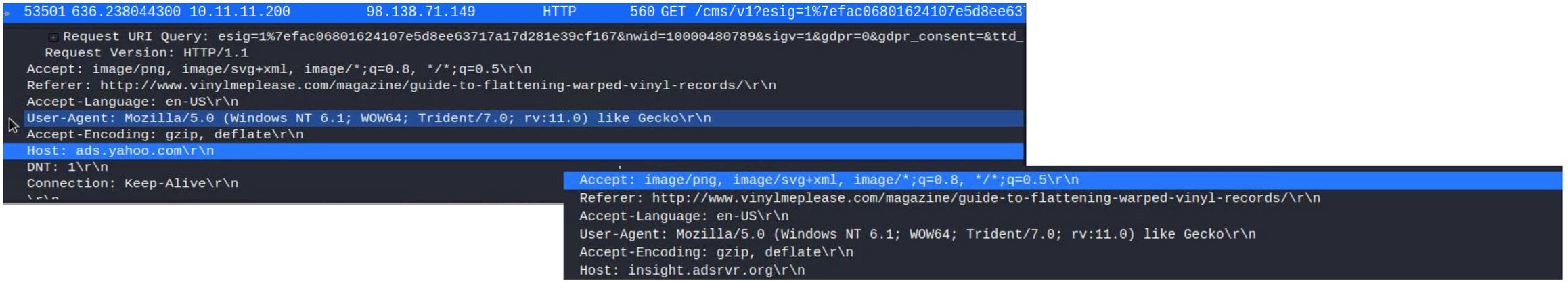
Normal Activity

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.



[Accessing personal domain]

Summarize the following:

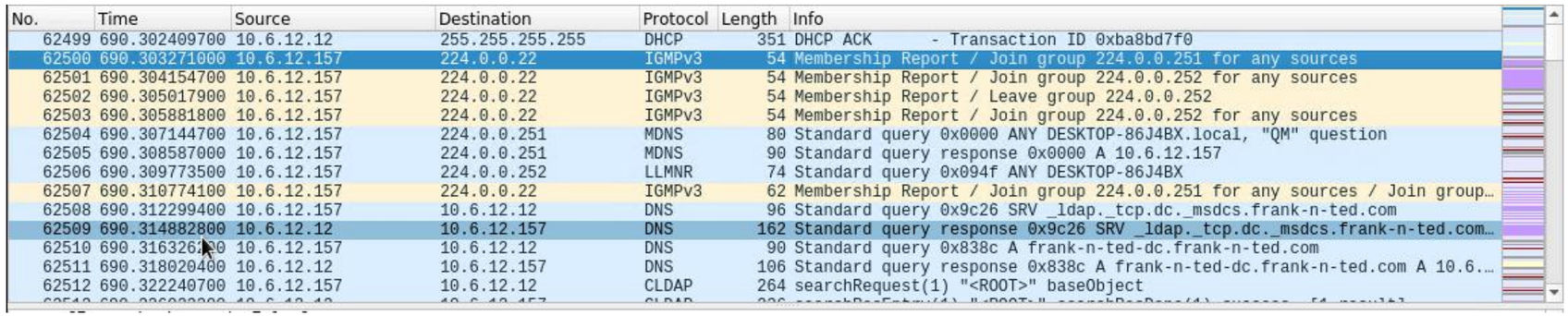
- **What kind of traffic did you observe? Which protocol(s)?**

  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 group. frank-n-ted.com

- **Include screenshots of packets justifying your conclusions.**



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	690.316326200	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

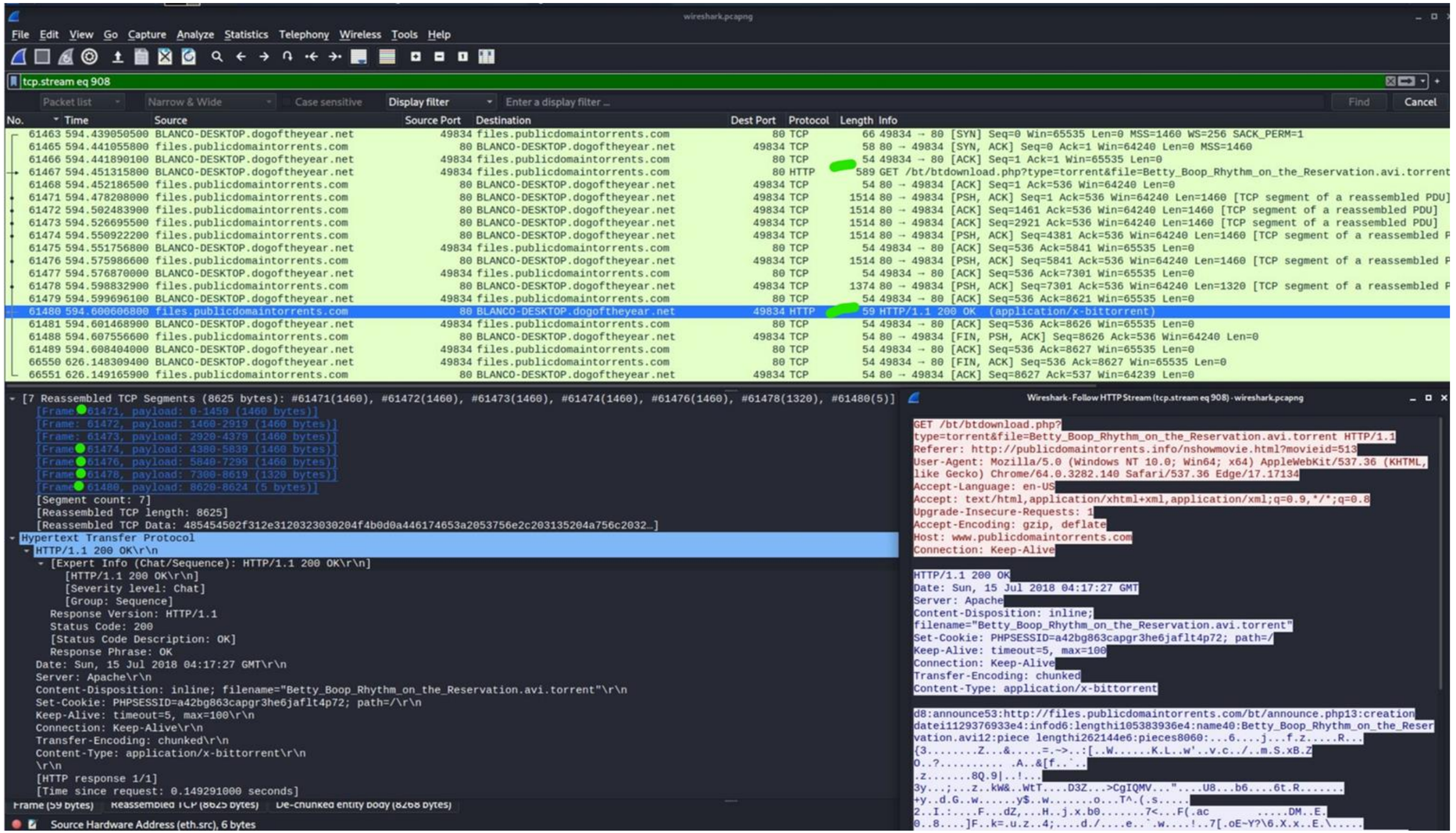
- **Include a description of any interesting files.**

  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



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 longer 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.

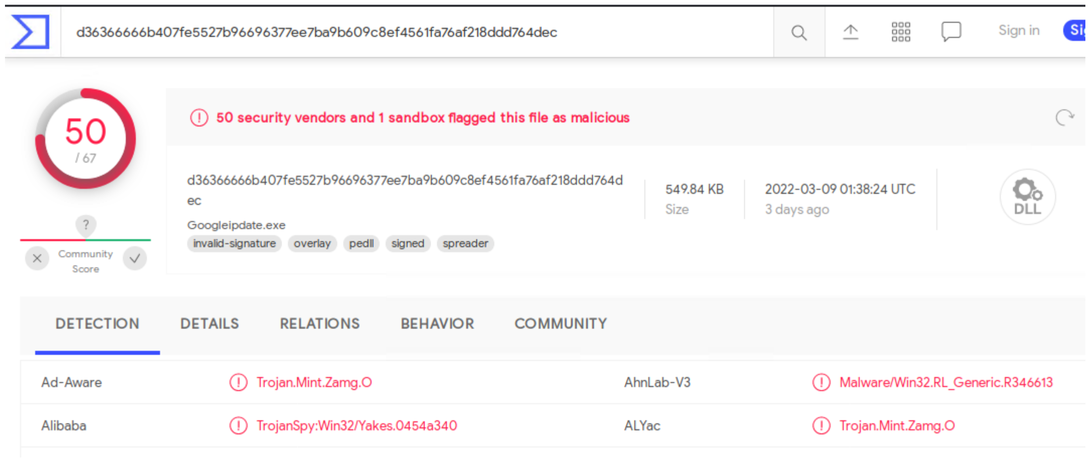
Guilty of Infringement:
Pursuant to 17 U.S. Code § 504 et seq.; 3 years; pay up to $150,000/content

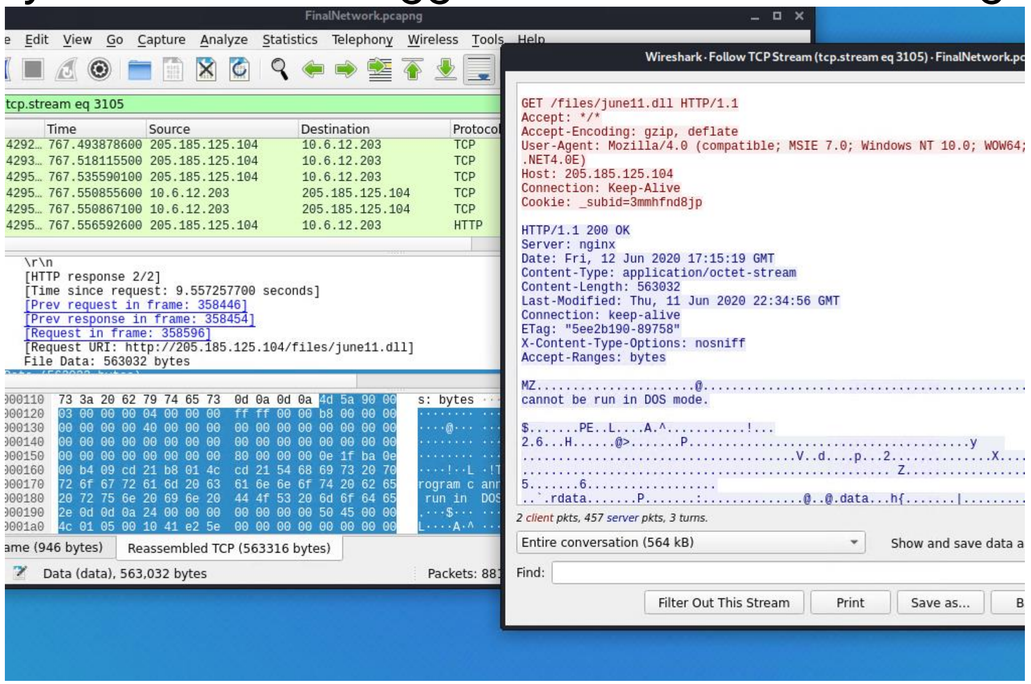
https://codes.findlaw.com/us/title-17-copyrights/17-usc-sect-504.html

[June 11.dll (Trojan)]

Summarize the following:

- On Friday June 12th, we could observe HTTP GET traffic downloading a file from Frank n Ted.
- 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.





Suggested Mitigation Techniques

- [June 11.dll (Trojan)]
  - Active anti-malware 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 a company policy for release of liability to any illegal activity on the company's website; any criminal fines should be paid by the employee.
  - Any illegal activity is grounds for immediate termination.
  - Block torrent websites and/or set an alert for any association of the term in the HTTP request protocol

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

The End