Network Traffic Analysis

Attack, Defense & Analysis of Vulnerable Networks

Presented by: Nick Bettis

Analysis performed for: Raven Security

Why should we monitor our network?

Network Traffic is your data, your security, and your privacy.

What is Network Traffic?

- Network traffic is all the communications that are sent to and from your network. Everytime you update your Facebook account, log in to your banking details, and download a new zoom wallpaper. It’s all network traffic!

What does network traffic look like?

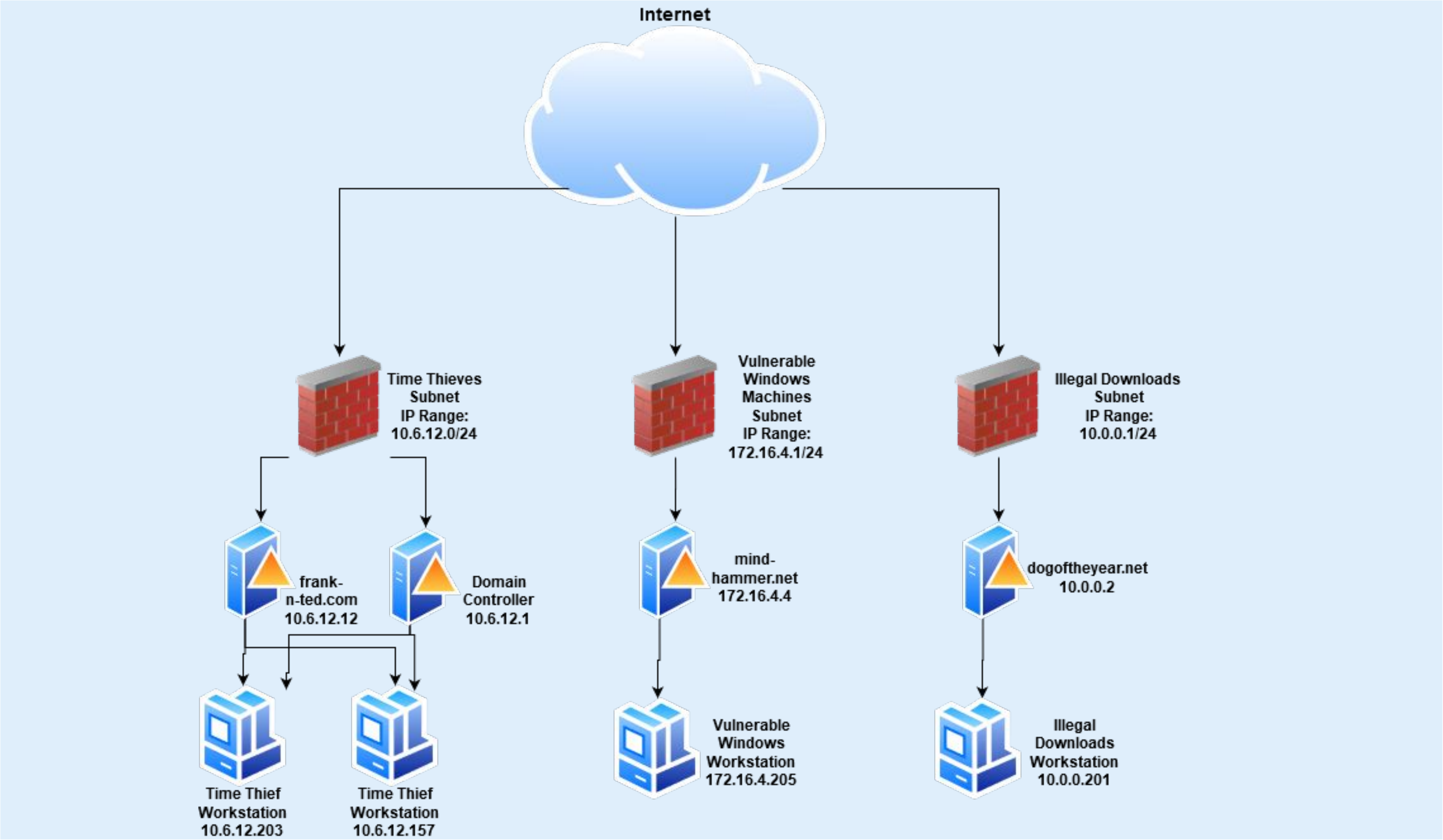
- Network traffic is packet data. What are packets? Packets are small portions of data that are sent to your network and reassembled by your computer resulting in communication.

Why does that matter?

- A network analyst can rebuild entire conversations, and see everything that is done on a network, if it is monitored. This means we can see when a problem arises, an attack is made, or even infected communications from your computer!

Network Topology
& Critical Vulnerabilities
# of Raven Security Systems.

Network Topology


Internet
Time Thieves Subnet IP Range: 10.6.12.0/24
Vulnerable Windows Machines Subnet IP Range: 172.16.4.1/24
Illegal Downloads Subnet IP Range: 10.0.0.1/24
frank-n-ted.com 10.6.12.12
Domain Controller 10.6.12.1
mind-hammer.net 172.16.4.4
dogoftheyear.net 10.0.0.2
Time Thief Workstation 10.6.12.203
Time Thief Workstation 10.6.12.157
Vulnerable Windows Workstation 172.16.4.205
Illegal Downloads Workstation 10.0.0.201

Subnet Time Thieves
Address Range:
10.6.12.1/24
OS: Windows
Active Directory:
frank-n-ted.com

Subnet Vulnerable Windows Machines
Address Range:
172.16.4.1/24
OS: Windows
Hostname:
mind-hammer.net

Subnet Illegal Downloads
Address Range:
10.0.0.1/24
OS: Windows
Hostname:dogoftheyear.net

Critical Vulnerabilities: Time Thieves

Our assessment uncovered the following critical vulnerabilities in the time thieves subnet.

Vulnerability	Description	Impact
CWE-269 Improper Privilege Management	Two employees had privileges that allowed them to circumvent security policies.	Users were able to execute system changes and download malware leading to a compromised network.
CWE-693 Protection Mechanism Failure	The devices on this subnet have no protection mechanism against viruses.	The malicious trojan was downloaded and possibly executed without any red flags.
CWE-441 Unintended Proxy or Intermediary	Users were able to make an active directory server	Users can bypass firewall rules and access restricted content

Critical Vulnerabilities: Vulnerable Windows Machines

Our assessment uncovered the following critical vulnerabilities in the vulnerable windows machine subnet.

Vulnerability	Description	Impact
CWE-693 Protection Mechanism Failure	The devices on this subnet have no protection mechanism against viruses.	User is vulnerable to viruses that steal her information and privacy.
CWE-359: Exposure of Private Personal Information to an Unauthorized Actor	User system is vulnerable and is sending private information including screen grabs and possibly keystrokes to a malicious actor.	Any passwords, or content the user accesses on this system are compromised. This could include very sensitive financial and personal data.

Critical Vulnerabilities: Illegal Downloads

Our assessment uncovered the following critical vulnerabilities in the illegal downloads subnet.

Vulnerability	Description	Impact
CWE-494: Download of Code Without Integrity Check	The users are allowed to download content, including safe legitimate torrents but are doing so without authenticating their integrity.	Torrents can harm systems either by copyright infringement or malicious code execution.
CWE-693 Protection Mechanism Failure	The devices on this subnet have no protection mechanism against viruses.	Content, including web traffic, that is unscanned can be potentially dangerous.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205>185.243.115.84> 10.0.0.201>166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	UDP>DNS>Data TCP>HTTP>Malformed Packet>SMB2 TLS.	Most common protocols on the network.
# of Unique IP Addresses	808 unique ipv4, 2 unique ipv6	Count of observed IP addresses.
Subnets	10.6.12.0/24 (Time Thieves) 172.16.4.0/24 (V.W.M.) 10.0.0.0/24 (Illegal Downloads)	Observed subnet ranges.
# of Malware Species	1 identified, more likely undetected.	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Our Time Thieves client’s normal activity is routine skype chats and http traffic.
- Our Vulnerable Windows client’s normal activity is posting to a blog.
- Our Illegal Downloads client’s normal activity is downloading operating systems via torrent.

Suspicious Activity

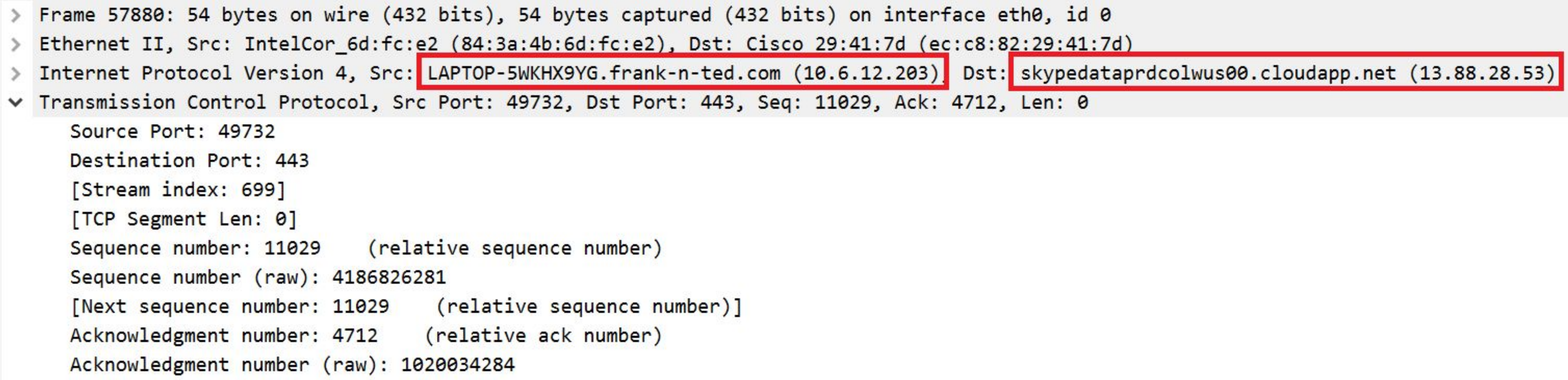
- Our Time Thieves client suspicious activity is setting up an active domain, watching youtube videos and downloading viruses.
- Our Vulnerable Windows client suspicious activity is unusually high traffic to a new IP.
- Our Illegal Downloads client suspicious activity is downloading torrented movies.

Normal Activity

[Time Thieves Normal Behavior]

Summarize the following:

- The most common legitimate protocols our time thieves utilize are TCP, and HTTP.
- The majority of valid transmissions seems to be the users connecting to skype and various websites most likely for business.



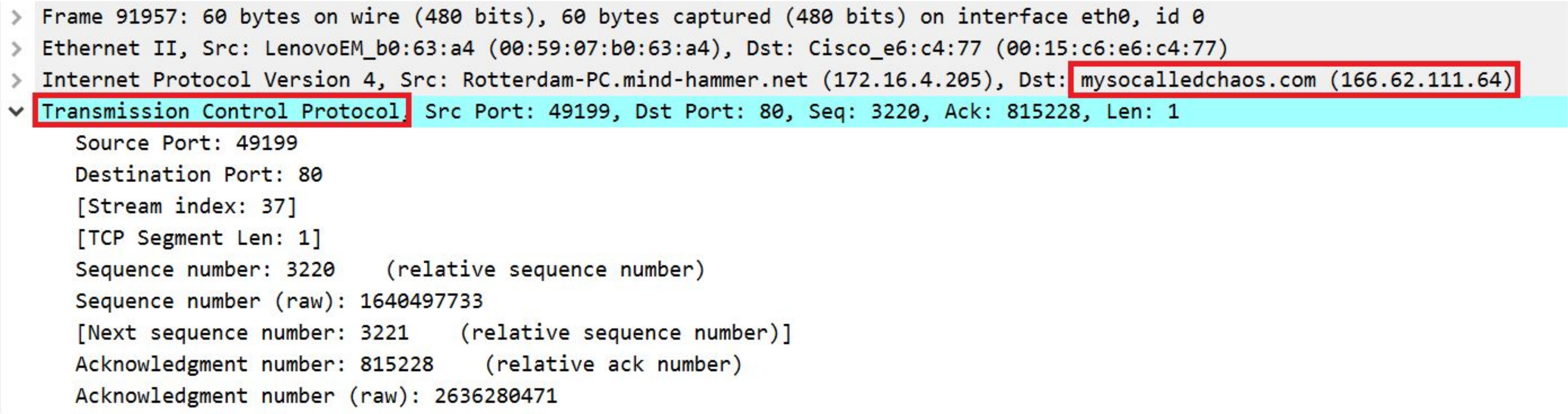
```
> Frame 57880: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
> Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: skypedataprdcolwus00.cloudapp.net (13.88.28.53)
v Transmission Control Protocol, Src Port: 49732, Dst Port: 443, Seq: 11029, Ack: 4712, Len: 0
     Source Port: 49732
     Destination Port: 443
     [Stream index: 699]
     [TCP Segment Len: 0]
     Sequence number: 11029    (relative sequence number)
     Sequence number (raw): 4186826281
     [Next sequence number: 11029    (relative sequence number)]
     Acknowledgment number: 4712    (relative ack number)
     Acknowledgment number (raw): 1020034284
```

- This is packet 57900 containing TCP skype data from our target time thief.

[Vulnerable Windows Machine Normal Behavior]

Summarize the following:

- The vulnerable windows machine at 172.16.4.205 normally uses a lot of TCP and HTTP traffic in their day to day work.
- This user contacts her blog mysocalledchaos.com, instagram.com, and searches using mozilla firefox routinely.



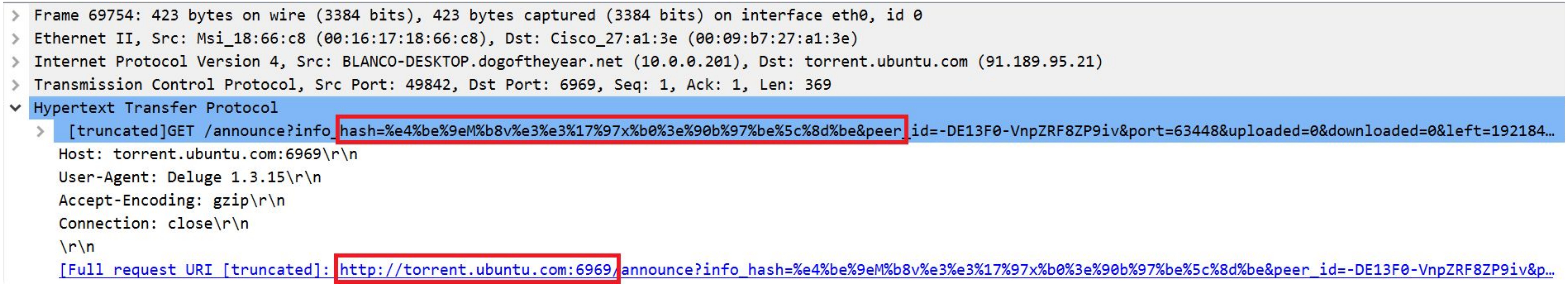
```
> Frame 91957: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
> Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
> Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: mysocalledchaos.com (166.62.111.64)
v Transmission Control Protocol, Src Port: 49199, Dst Port: 80, Seq: 3220, Ack: 815228, Len: 1
     Source Port: 49199
     Destination Port: 80
     [Stream index: 37]
     [TCP Segment Len: 1]
     Sequence number: 3220    (relative sequence number)
     Sequence number (raw): 1640497733
     [Next sequence number: 3221    (relative sequence number)]
     Acknowledgment number: 815228    (relative ack number)
     Acknowledgment number (raw): 2636280471
```

- This is packet 91957, a TCP/HTTP packet, showing the user connecting to mysocalledchaos.com.

[Illegal Downloads Normal Behavior]

Summarize the following:

- Our illegal downloads machine, 10.0.0.201 is allowed to use torrents if they are for legitimate purposes like downloading operating systems. This is done in HTTP traffic.
- We can see that this user did download a Linux torrent from torrent.ubuntu.com



```
> Frame 69754: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on interface eth0, id 0
> Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
> Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: torrent.ubuntu.com (91.189.95.21)
> Transmission Control Protocol, Src Port: 49842, Dst Port: 6969, Seq: 1, Ack: 1, Len: 369
v Hypertext Transfer Protocol
  > [truncated]GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&peer_id=-DE13F0-VnpZRF8ZP9iv&port=63448&uploaded=0&downloaded=0&left=192184…
    Host: torrent.ubuntu.com:6969\r\n
    User-Agent: Deluge 1.3.15\r\n
    Accept-Encoding: gzip\r\n
    Connection: close\r\n
    \r\n
    [Full request URI [truncated]: http://torrent.ubuntu.com:6969/announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&peer_id=-DE13F0-VnpZRF8ZP9iv&p…
```

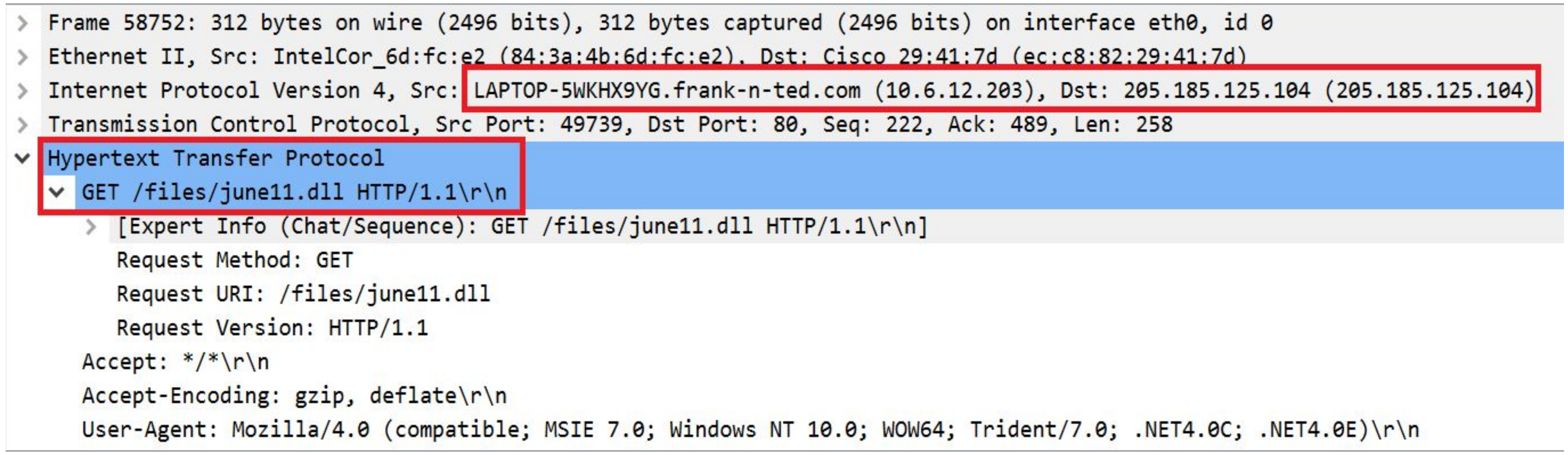
- This is packet 69754, a HTTP packet, of an Ubuntu torrent TCP stream that is perfectly fine with IT and is a normal practice for this workstation according to company policy.

Malicious Activity

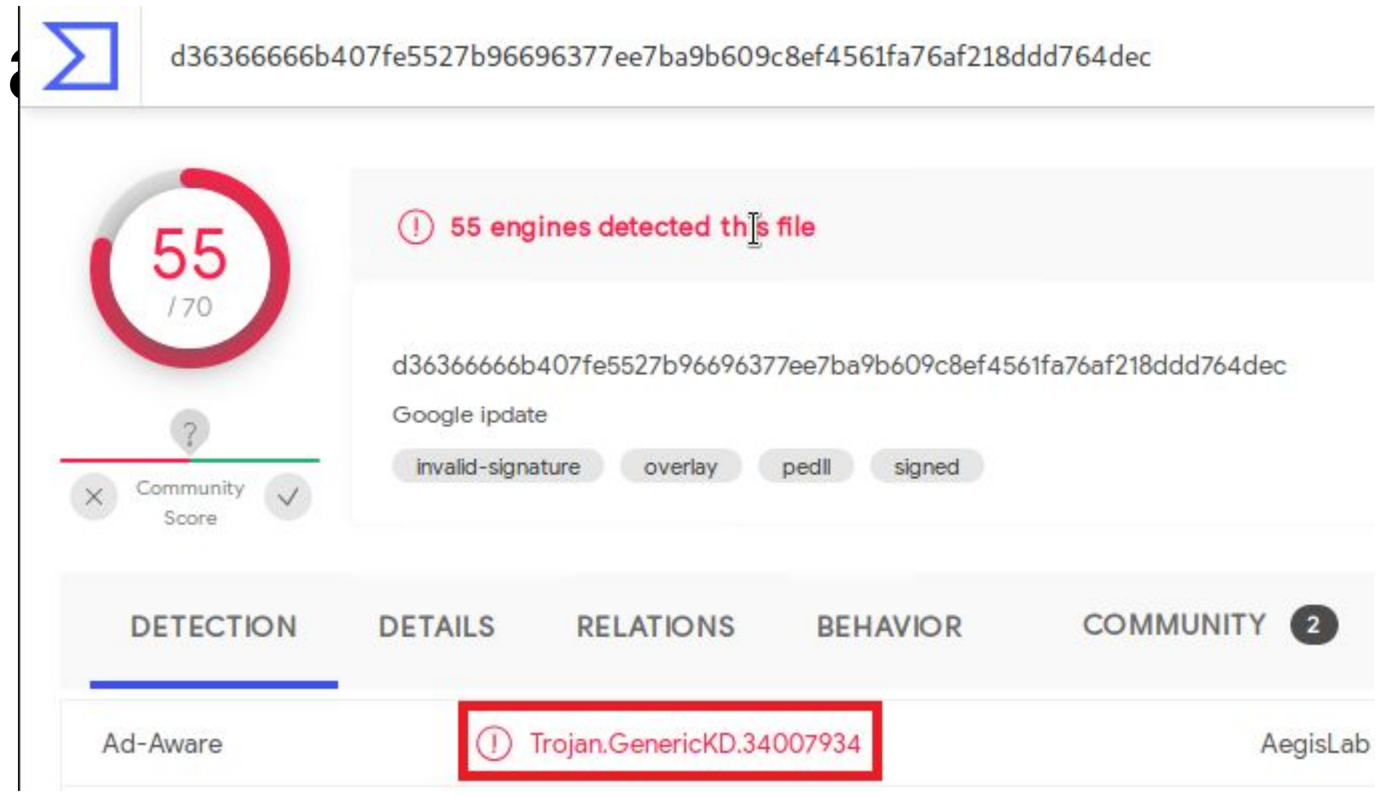
[Time Thieves Malicious Behavior]

Summarize the following:

- We observed TCP, LDAP, and Kerberos which can be normal activity, however this was to a new active directory frank-n-ted.com.
- The user has setup an Active Directory windows server and is using it to watch youtube.com while on the job. They also downloaded a virus that contains a trojan and malicious traffic was seen going to e a



```
> Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
> Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
> Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
v Hypertext Transfer Protocol
  v GET /files/june11.dll HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /files/june11.dll
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
```



d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

55 /70

55 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google ipdate

invalid-signature overlay pedll signed

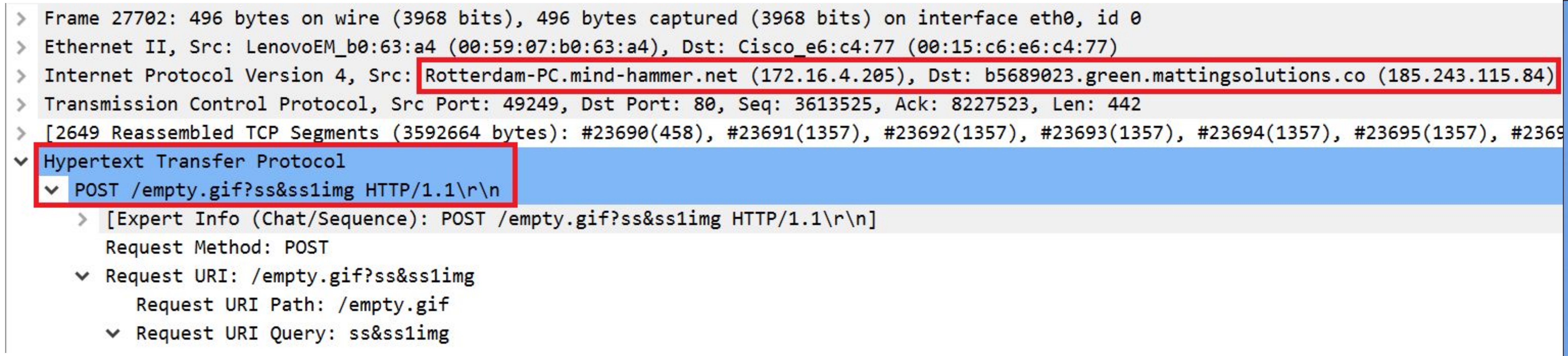
Ad-Aware Trojan.GenericKD.34007934 AegisLab

- This is a packet showing a download of a trojan which was analyzed using virustotal.com and recognized by 55 virus engines.

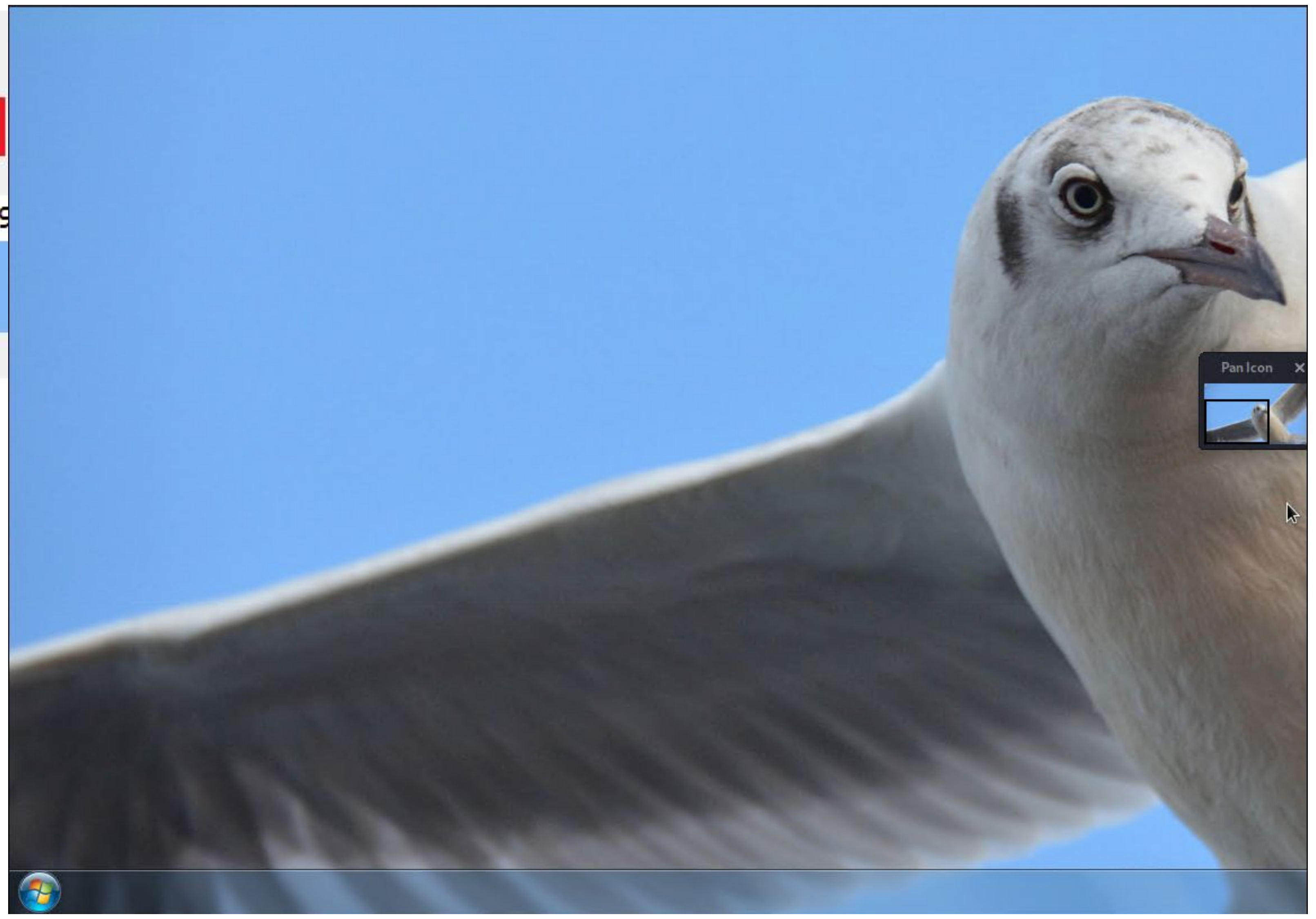
[Vulnerable Windows Machine Malicious Behavior]

Summarize the following:

- Our malicious behavior appears to be all TCP and HTTP traffic.
- The user, or most likely the command and control server was making the target user download a bunch of gifs, screenshot their desktop and possibly send keylogging data.



```
> Frame 27702: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface eth0, id 0
> Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Cisco_e6:c4:77 (00:15:c6:e6:c4:77)
> Internet Protocol Version 4, Src: Rotterdam-PC.mind-hammer.net (172.16.4.205), Dst: b5689023.green.mattingsolutions.co (185.243.115.84)
> Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 3613525, Ack: 8227523, Len: 442
> [2649 Reassembled TCP Segments (3592664 bytes): #23690(458), #23691(1357), #23692(1357), #23693(1357), #23694(1357), #23695(1357), #2369
v Hypertext Transfer Protocol
  v POST /empty.gif?ss&ss1img HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): POST /empty.gif?ss&ss1img HTTP/1.1\r\n]
      Request Method: POST
    v Request URI: /empty.gif?ss&ss1img
        Request URI Path: /empty.gif
      v Request URI Query: ss&ss1img
```

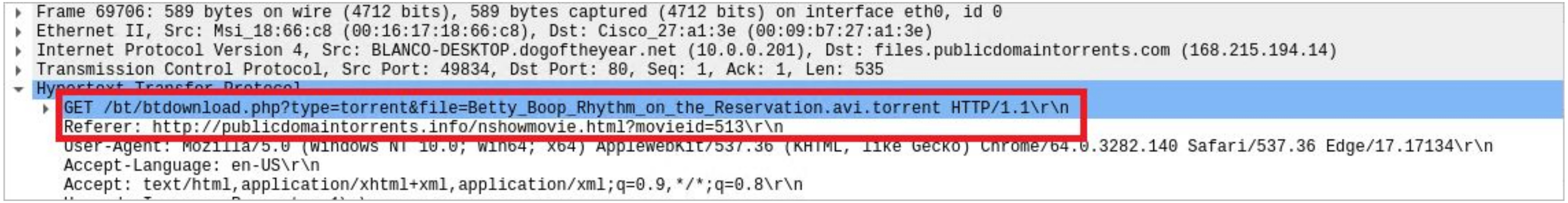


- Packet 27702 is a HTTP POST request sending a screenshot of the users wallpaper background. This indicated this computer has been compromised and is sending sensitive data to a cnc server. This could also mean that there are more malicious files in the network that our capture didn't find.

[Illegal Downloads Malicious Behavior]

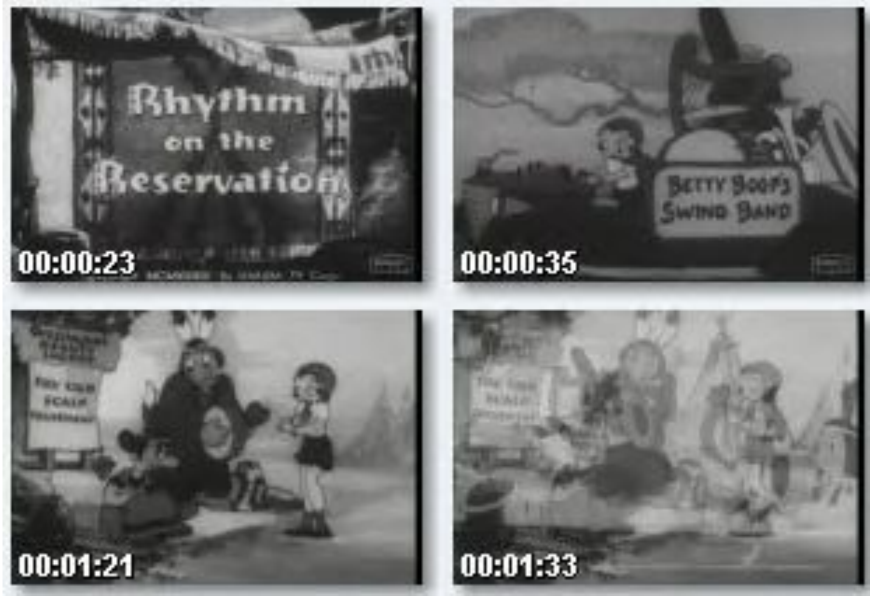
Summarize the following:

- We observed HTTP traffic that was not normal or within company policy.
- The user was downloading torrents on publicdomaintorrents.com and watching movies at work.Technically this is not illegal as public domain content is not copyright however it is stealing company time and shows the capability of the target to download torrents that could be illegal.



```
▸ Frame 69706: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
▸ Transmission Control Protocol, Src Port: 49834, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
▾ Hypertext Transfer Protocol
  ▸ GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
    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\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
```

- This is a packet containing a movie torrent download from the site publicdomaintorrents.com and below is a screen grab of their torrented movie showing time stamps.



What steps can we take to protect ourselves?

Protect your data!

I recommend the following:

- Update your systems to the latest version after testing their implementation in a sandbox environment.
- If you are an enterprise, use an intrusion prevention system, or I.P.S. for short. At the very least an intrusion detection system, or I.D.S.
    - E.L.K is an open source and free intrusion detection system that can notify you when something goes wrong.
    - Splunk is an industry leading intrusion prevention system, and SIEM (security information and event management) system that will monitor your network and can even stop malicious activity in its tracks.
- Utilize antivirus so that if a malicious file is downloaded you have a second line of defense.
- Ensure the principle of least privilege is applied.

What if I’m not a business?

You can still keep your data safe!

- Update your systems to the latest version.
- Know what sites you are using. Are they encrypted?

- Don’t connect to networks you don’t trust.
  - Mobile data is often much safer than an open network.
- Use an antivirus
- Use a password management tool like LastPass

LastPass•••|

Questions?