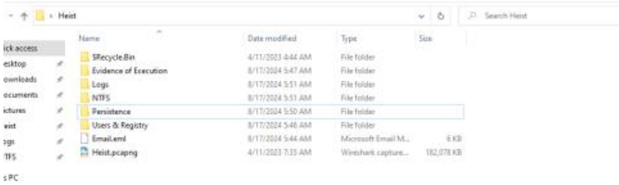
Heist - Walkthrough

Saturday, August 17, 2024 3:41 PM

Story:
Forela recently received complaints from viewers that the live stream on their YouTube channel was showing strange content.
Instead of the usual company content, the live stream showed videos promoting cryptocurrency scams.
The channel was used to showcase the company's products and services and provide educational content related to the industry they were in.
Alonzo Spire, the IT administrator of Forela, managed the YouTube channel.
The incident response team was notified of an incident as soon as complaints were received. Alonzo's system was triaged and artefacts were acquired from his system for forensics analysis to confirm how the company's channel got hacked.

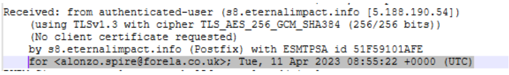
- I'm highly recommending to split the disk to parts:



Name	Date modified	Type	Size
$Recycle.Bin	4/11/2023 4:44 AM	File folder	
Evidence of Execution	8/17/2024 5:47 AM	File folder	
Logs	8/17/2024 5:51 AM	File folder	
NTFS	8/17/2024 5:51 AM	File folder	
Persistence	8/17/2024 5:50 AM	File folder	
Users & Registry	8/17/2024 5:46 AM	File folder	
Email.eml	8/17/2024 5:44 AM	Microsoft Email M...	6 KB
Heist.pcapng	4/11/2023 7:35 AM	Wireshark capture...	182,078 KB

Task1: **At what time was the suspected phishing email received in the victim's inbox? (UTC)**

- To find the answer, you should open the 'Email.eml' file via 'notepad++' and look for the 'Received' field:



```
Received: from authenticated-user (s8.eternalimpact.info [5.188.190.54])
    (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits))
    (No client certificate requested)
    by s8.eternalimpact.info (Postfix) with ESMTPSA id 51F59101AFE
    for <alonzo.spire@forela.co.uk>; Tue, 11 Apr 2023 08:55:22 +0000 (UTC)
```

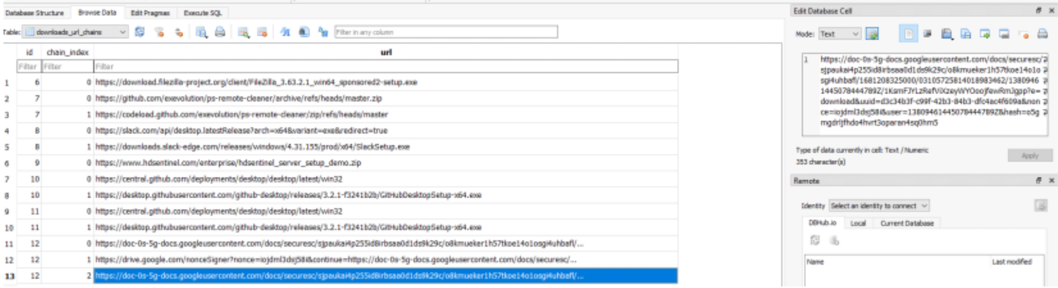
- This timestamp is when the email was processed by the sending server in UTC.
  This timestamp indicates that the email was sent from the sending server at 08:55:22 UTC.

Task2: **Please provide the download URL that was utilised to retrieve the file initially downloaded as part of this security event.**

- To find the specific download link from Google Drive in the context of your investigation, you should start by accessing the SQLite database from Alonzo's Google Chrome profile. This database is typically located in the user's profile directory, such as C:\Users\<YourUsername>\AppData\Local\Google\Chrome\User Data\Default on Windows.

- Once you have the database, open it in a SQLite viewer and navigate to the History database. Within this database, go to the downloads_url_chains table.

- I identified the relevant Google Drive URL and noticed to an another HTTP request inside of the URL request, which is the download URL.



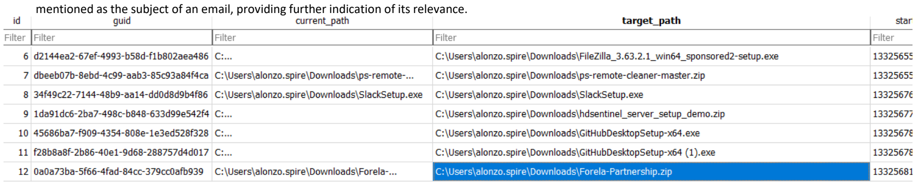
	id	chain_index	url
	Filter	Filter	Filter
1	6	0	https://download.filezilla-project.org/client/FileZilla_3.63.2.1_win64_sponsored2-setup.exe
2	7	0	https://github.com/exevolution/ps-remote-cleaner/archive/refs/heads/master.zip
3	7	1	https://codeload.github.com/exevolution/ps-remote-cleaner/zip/refs/heads/master
4	8	0	https://slack.com/api/desktop.latestRelease?arch=x64&variant=exe&redirect=true
5	8	1	https://downloads.slack-edge.com/releases/windows/4.31.155/prod/x64/SlackSetup.exe
6	9	0	https://www.hdsentinel.com/enterprise/hdsentinel_server_setup_demo.zip
7	10	0	https://central.github.com/deployments/desktop/desktop/latest/win32
8	10	1	https://desktop.githubusercontent.com/github-desktop/releases/3.2.1-f3241b2b/GitHubDesktopSetup-x64.exe
9	11	0	https://central.github.com/deployments/desktop/desktop/latest/win32
10	11	1	https://desktop.githubusercontent.com/github-desktop/releases/3.2.1-f3241b2b/GitHubDesktopSetup-x64.exe
11	12	0	https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1osgi4uhbafl/...
12	12	1	https://drive.google.com/nonceSigner?nonce=iojdml3dsj58i&continue=https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/...
13	12	2	https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1osgi4uhbafl/...

```
1    https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/
     sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1o
     sgi4uhbafl/1681208325000/03105725814018983462/1380946
     14450784447892/1KamFJYLzRafVlXzeyWYOoojfewRmJgpp?e=
     download&uuid=d3c34b3f-c99f-42b3-84b3-dfc4ac4f609a&non
     ce=iojdml3dsj58i&user=13809461445078444789Z&hash=o5g
     mgdrijfhdo4hvrt3oparan4sq0hm5
```

Type of data currently in cell: Text / Numeric
353 character(s)

Task3: What is the name of the file suspected to have been initially downloaded as part of this security event?

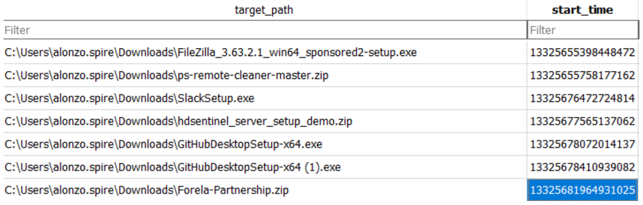
- In the SQLite database, navigating to the 'Downloads' table reveals that Alonzo downloaded a ZIP file identified as 'Forela-Partnership.zip' at the same timestamp. Additionally, this ZIP file is mentioned as the subject of an email, providing further indication of its relevance.



id	guid	current_path	target_path	star
Filter	Filter	Filter	Filter	Filter
6	d2144ea2-67ef-4993-b58d-f1b802aea486	C:...	C:\Users\alonzo.spire\Downloads\FileZilla_3.63.2.1_win64_sponsored2-setup.exe	13325655
7	dbeeb07b-8ebd-4c99-aab3-85c93a84f4ca	C:\Users\alonzo.spire\Downloads\ps-remote-...	C:\Users\alonzo.spire\Downloads\ps-remote-cleaner-master.zip	13325655
8	34f49c22-7144-48b9-aa14-dd0d8d9b4f86	C:\Users\alonzo.spire\Downloads\SlackSetup.exe	C:\Users\alonzo.spire\Downloads\SlackSetup.exe	13325676
9	1da91dc6-2ba7-498c-b848-633d99e542f4	C:...	C:\Users\alonzo.spire\Downloads\hdsentinel_server_setup_demo.zip	13325677
10	45686ba7-f909-4354-808e-1e3ed528f328	C:...	C:\Users\alonzo.spire\Downloads\GitHubDesktopSetup-x64.exe	13325678
11	f28b8a8f-2b86-40e1-9d68-288757d4d017	C:...	C:\Users\alonzo.spire\Downloads\GitHubDesktopSetup-x64 (1).exe	13325678
12	0a0a73ba-5f66-4fad-84cc-379cc0afb939	C:\Users\alonzo.spire\Downloads\Forela-...	C:\Users\alonzo.spire\Downloads\Forela-Partnership.zip	13325681

Task4: When was this file downloaded onto the system?

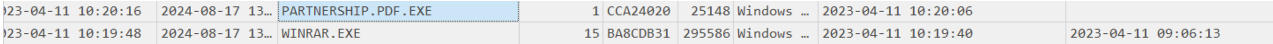
- **On the same table, we able to find the 'start_time' column which indicates when the file downloaded to the system.**
  The timestamp format is 'Webkit' you can use the website: https://www.epochconverter.com/webkit to convert it to UTC:



target_path	start_time
Filter	Filter
C:\Users\alonzo.spire\Downloads\FileZilla_3.63.2.1_win64_sponsored2-setup.exe	13325655398448472
C:\Users\alonzo.spire\Downloads\ps-remote-cleaner-master.zip	13325655758177162
C:\Users\alonzo.spire\Downloads\SlackSetup.exe	13325676472724814
C:\Users\alonzo.spire\Downloads\hdsentinel_server_setup_demo.zip	13325677565137062
C:\Users\alonzo.spire\Downloads\GitHubDesktopSetup-x64.exe	13325678072014137
C:\Users\alonzo.spire\Downloads\GitHubDesktopSetup-x64 (1).exe	13325678410939082
C:\Users\alonzo.spire\Downloads\Forela-Partnership.zip	13325681964931025

Task5: What is the name of the file that initiated malicious activity on the endpoint?

- To address this question, we need to identify process executions on the system.
  I parsed the Prefetch directory using PECMD and searched for timestamps around '2023-04-11 10:19:24,' as we know the ZIP file was downloaded during this timeframe. During this search, I found the suspicious process:



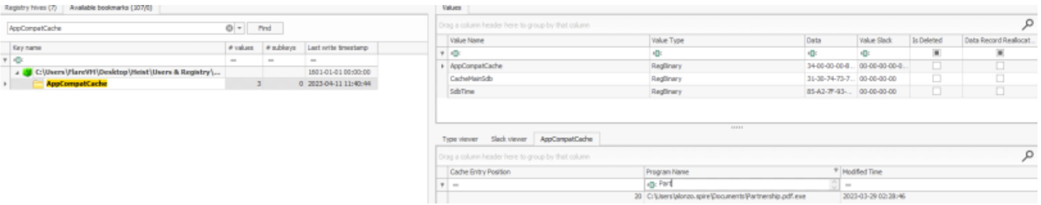
23-04-11 10:20:16	2024-08-17 13…	PARTNERSHIP.PDF.EXE	1	CCA24020	25148	Windows …	2023-04-11 10:20:06	
23-04-11 10:19:48	2024-08-17 13…	WINRAR.EXE	15	BA8CDB31	295586	Windows …	2023-04-11 10:19:40	2023-04-11 09:06:13

Task6: What file type was the malicious payload disguised as to deceive the user into executing it?

- We able to see the answer in the file name:
  Parthership.**pdf**.exe

Task7: From which directory path was the malicious file executed?

- Now, because we know it's not a PDF file it’s an executable we should look for executions.
  I used 'RegistryExplorer' to export the 'Shimcache' to find the path:



Registry hives (7) | Available bookmarks (107/0)

AppCompatCache | Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\FlareVM\Desktop\Heist\Users & Registry\...			1601-01-01 00:00:00
AppCompatCache	3	0	2023-04-11 11:40:44

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocat...
AppCompatCache	RegBinary	34-00-00-00-8...	00-00-00-00-0...	☐	☐
CacheMainSdb	RegBinary	31-30-74-73-7...	00-00-00-00	☐	☐
SdbTime	RegBinary	85-A2-7F-93-...	00-00-00-00	☐	☐

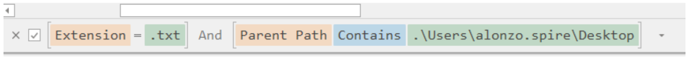
Type viewer | Slack viewer | AppCompatCache

Drag a column header here to group by that column

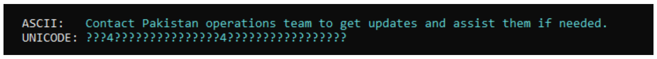
Cache Entry Position	Program Name	Modified Time
	Part	
20	C:\Users\alonzo.spire\Documents\Partnership.pdf.exe	2023-03-29 02:28:46

Task8: There was a file on users desktop with a note. What were the contents of the note?

- To address this question, I parsed the MFT using 'MFTEcmd.exe' and filtered for files on Alonzo's desktop with the extension '.txt'.
  I found only one '.txt' file, named 'reminder.txt'.
  Using the entry number '427727', I extracted its content with the '--de' flag via MFTEcmd.



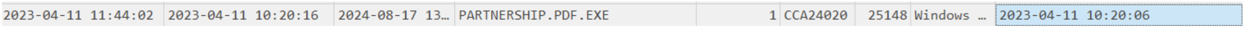
× ☑ Extension = .txt And Parent Path Contains .\Users\alonzo.spire\Desktop



```
ASCII:   Contact Pakistan operations team to get updates and assist them if needed.
UNICODE: ???4????????????????4?????????????????
```

Task9: At what time was the malicious file was executed?

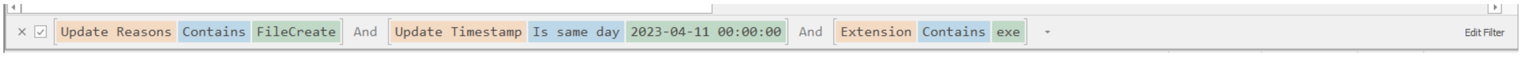
- We can find the answer on the parsed 'Prefetch' file:



2023-04-11 11:44:02	2023-04-11 10:20:16	2024-08-17 13…	PARTNERSHIP.PDF.EXE	1	CCA24020	25148	Windows …	2023-04-11 10:20:06

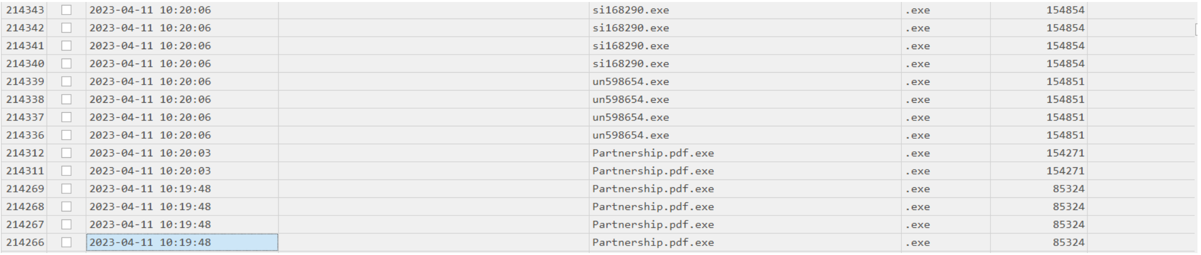
Task10: The malicious file dropped 2 files on the system which performed further actions on the endpoint. What's the name of these 2 files? (alphabetical order)

- I opened our MFT-parsed CSV and filtered it to find file creation events around the time of the suspicious file execution, which was at "2023-04-11 10:19:48".
  I searched for 'FileCreate' entries around this timestamp and identified the strange files that were created immediately after the execution.



× ☑ Update Reasons Contains FileCreate And Update Timestamp Is same day 2023-04-11 00:00:00 And Extension Contains exe

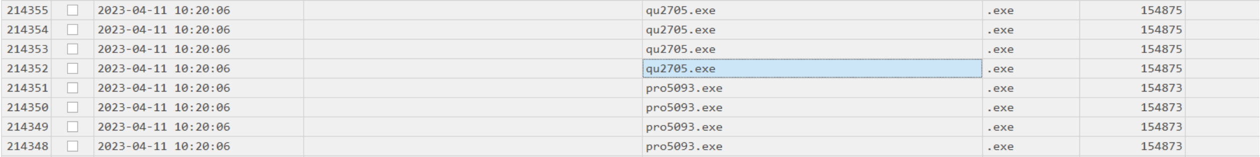
Edit Filter



214343	☐	2023-04-11 10:20:06		si168290.exe	.exe	154854
214342	☐	2023-04-11 10:20:06		si168290.exe	.exe	154854
214341	☐	2023-04-11 10:20:06		si168290.exe	.exe	154854
214340	☐	2023-04-11 10:20:06		si168290.exe	.exe	154854
214339	☐	2023-04-11 10:20:06		un598654.exe	.exe	154851
214338	☐	2023-04-11 10:20:06		un598654.exe	.exe	154851
214337	☐	2023-04-11 10:20:06		un598654.exe	.exe	154851
214336	☐	2023-04-11 10:20:06		un598654.exe	.exe	154851
214312	☐	2023-04-11 10:20:03		Partnership.pdf.exe	.exe	154271
214311	☐	2023-04-11 10:20:03		Partnership.pdf.exe	.exe	154271
214269	☐	2023-04-11 10:19:48		Partnership.pdf.exe	.exe	85324
214268	☐	2023-04-11 10:19:48		Partnership.pdf.exe	.exe	85324
214267	☐	2023-04-11 10:19:48		Partnership.pdf.exe	.exe	85324
214266	☐	2023-04-11 10:19:48		Partnership.pdf.exe	.exe	85324

Task11: One of the files from Question 10 dropped two more files onto the system. What are the names of these files? (in alphabetical order)

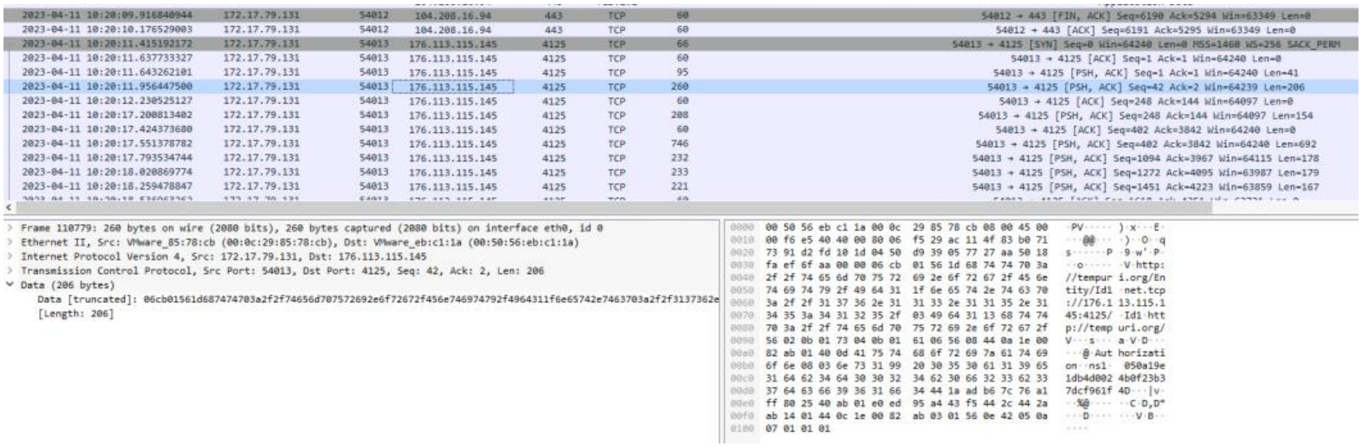
- We able to see it right after the files from the previous question created:



214355	☐	2023-04-11 10:20:06		qu2705.exe	.exe	154875
214354	☐	2023-04-11 10:20:06		qu2705.exe	.exe	154875
214353	☐	2023-04-11 10:20:06		qu2705.exe	.exe	154875
214352	☐	2023-04-11 10:20:06		qu2705.exe	.exe	154875
214351	☐	2023-04-11 10:20:06		pro5093.exe	.exe	154873
214350	☐	2023-04-11 10:20:06		pro5093.exe	.exe	154873
214349	☐	2023-04-11 10:20:06		pro5093.exe	.exe	154873
214348	☐	2023-04-11 10:20:06		pro5093.exe	.exe	154873

Task12: What's the malicious C2 IP Address and port?

- To find the answer for this question, I filtered the PCAP file we received to the execution timestamp via the our internal source IP, we found a communication with external address via unusual port:



```
2023-04-11 10:20:09.916840944   172.17.79.131   54012   104.208.16.94     443    TCP   60    54012 → 443 [FIN, ACK] Seq=6190 Ack=5294 Win=63349 Len=0
2023-04-11 10:20:10.176529003   172.17.79.131   54012   104.208.16.94     443    TCP   60    54012 → 443 [ACK] Seq=6191 Ack=5295 Win=63349 Len=0
2023-04-11 10:20:11.415192172   172.17.79.131   54013   176.113.115.145   4125   TCP   66    54013 → 4125 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2023-04-11 10:20:11.637733327   172.17.79.131   54013   176.113.115.145   4125   TCP   60    54013 → 4125 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2023-04-11 10:20:11.643262101   172.17.79.131   54013   176.113.115.145   4125   TCP   95    54013 → 4125 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=41
2023-04-11 10:20:11.956447500   172.17.79.131   54013   176.113.115.145   4125   TCP   260   54013 → 4125 [PSH, ACK] Seq=42 Ack=2 Win=64239 Len=206
2023-04-11 10:20:12.230525127   172.17.79.131   54013   176.113.115.145   4125   TCP   60    54013 → 4125 [ACK] Seq=248 Ack=144 Win=64097 Len=0
2023-04-11 10:20:17.200813402   172.17.79.131   54013   176.113.115.145   4125   TCP   208   54013 → 4125 [PSH, ACK] Seq=248 Ack=144 Win=64097 Len=154
2023-04-11 10:20:17.424373680   172.17.79.131   54013   176.113.115.145   4125   TCP   60    54013 → 4125 [ACK] Seq=402 Ack=3842 Win=64240 Len=0
2023-04-11 10:20:17.551378782   172.17.79.131   54013   176.113.115.145   4125   TCP   746   54013 → 4125 [PSH, ACK] Seq=402 Ack=3842 Win=64240 Len=692
2023-04-11 10:20:17.793534744   172.17.79.131   54013   176.113.115.145   4125   TCP   232   54013 → 4125 [PSH, ACK] Seq=1094 Ack=3967 Win=64115 Len=178
2023-04-11 10:20:18.020869774   172.17.79.131   54013   176.113.115.145   4125   TCP   233   54013 → 4125 [PSH, ACK] Seq=1272 Ack=4095 Win=63987 Len=179
2023-04-11 10:20:18.259478847   172.17.79.131   54013   176.113.115.145   4125   TCP   221   54013 → 4125 [PSH, ACK] Seq=1451 Ack=4223 Win=63859 Len=167
```

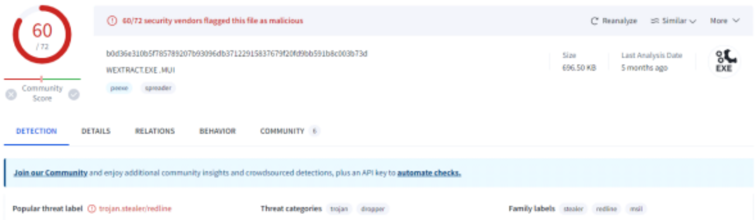
```
> Frame 110779: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_85:78:cb (00:0c:29:85:78:cb), Dst: VMware_eb:c1:1a (00:50:56:eb:c1:1a)
> Internet Protocol Version 4, Src: 172.17.79.131, Dst: 176.113.115.145
> Transmission Control Protocol, Src Port: 54013, Dst Port: 4125, Seq: 42, Ack: 2, Len: 206
v Data (206 bytes)
    Data [truncated]: 06cb01561d687474703a2f2f74656d707572692e6f72672f456e746974792f4964311f6e65742e7463703a2f2f3137362e
    [Length: 206]
```

```
0000  00 50 56 eb c1 1a 00 0c  29 85 78 cb 08 00 45 00   ·PV·····)·x···E·
0010  00 f6 e5 40 40 00 80 06  f5 29 ac 11 4f 83 b0 71   ···@@····)··O··q
0020  73 91 d2 fd 10 1d 04 50  d9 39 05 77 27 aa 50 18   s······P·9·w'·P·
0030  fa ef 6f aa 00 00 06 cb  01 56 1d 68 74 74 70 3a   ··o······V·http:
0040  2f 2f 74 65 6d 70 75 72  69 2e 6f 72 67 2f 45 6e   //tempur i.org/En
0050  74 69 74 79 2f 49 64 31  1f 6e 65 74 2e 74 63 70   tity/Id1 ·net.tcp
0060  3a 2f 2f 31 37 36 2e 31  31 33 2e 31 31 35 2e 31   ://176.1 13.115.1
0070  34 35 3a 34 31 32 35 2f  03 49 64 31 13 68 74 74   45:4125/ ·Id1·htt
0080  70 3a 2f 2f 74 65 6d 70  75 72 69 2e 6f 72 67 2f   p://temp uri.org/
0090  56 02 0b 01 73 04 0b 01  61 06 56 08 44 0a 1e 00   V···s··· a·V·D···
00a0  82 ab 01 40 0d 41 75 74  68 6f 72 69 7a 61 74 69   ···@·Aut horizati
00b0  6f 6e 08 03 6e 73 31 99  20 30 35 30 61 31 39 65   on··ns1·  050a19e
00c0  31 64 62 34 64 30 30 32  34 62 30 66 32 33 62 33   1db4d002 4b0f23b3
00d0  37 64 63 66 39 36 31 66  34 44 1a ad b6 7c 76 a1   7dcf961f 4D···|v·
00e0  ff 80 25 40 ab 01 e0 ed  95 a4 43 f5 44 2c 44 2a   ··%@···· ··C·D,D*
00f0  ab 14 01 44 0c 1e 00 82  ab 03 01 56 0e 42 05 0a   ···D···· ···V·B··
0100  07 01 01 01                                        ····
```

Task13: What's the malware family of the malicious file?

- **I searched the C2 address and the port on 'Google' I found the malware in 'MalwareBazar' it's a Redline stealer which related to this type of C2:**

https://bazaar.abuse.ch/sample/b0d36e310b5f785789207b93096db37122915837679f20fd9bb591b8c003b73d/



60/72 security vendors flagged this file as malicious

b0d36e310b5f785789207b93096db37122915837679f20fd9bb591b8c003b73d

WEXTRACT.EXE .MUI

Size 696.50 KB

Last Analysis Date 5 months ago

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

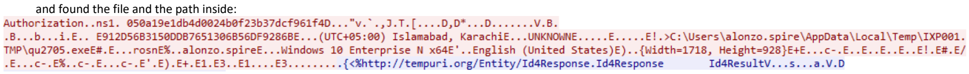
Popular threat label trojan.stealer/redline

Threat categories trojan dropper

Family labels stealer redline msil

Task14:Which malicious file exfiltrated data from the endpoint?

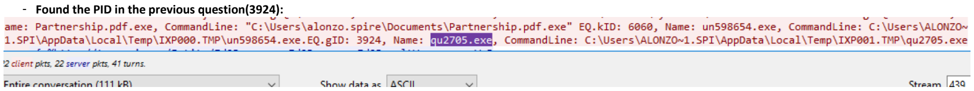
- To find the answer for this question, I followed the TCP stream of the communication with the C2 and found the file and the path inside:



```
Authorization..ns1. 050a19e1db4d0024b0f23b37dcf961f4D..."v.`.,J.T.[....D,D*...D.......V.B.
.B...b...i.E.. E912D56B3150DDB7651306B56DF9286BE...(UTC+05:00) Islamabad, KarachiE...UNKNOWNE.....E.....E!.>C:\Users\alonzo.spire\AppData\Local\Temp\IXP001.
TMP\qu2705.exeE#.E...rosnE%..alonzo.spireE...Windows 10 Enterprise N x64E'..English (United States)E)..{Width=1718, Height=928}E+E...c-.E..E..E..E..E!.E#.E/
.E...c-.E%..c-.E...c-.E'.E).E+.E1.E3..E1....E3.........{<%http://tempuri.org/Entity/Id4Response.Id4Response       Id4ResultV...s...a.V.D
```

Task15:What's the process ID of the malicious file used to exfiltrate data?

- **Found the PID in the previous question(3924):**



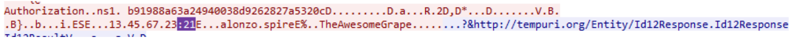
```
ame: Partnership.pdf.exe, CommandLine: "C:\Users\alonzo.spire\Documents\Partnership.pdf.exe" EQ.kID: 6060, Name: un598654.exe, CommandLine: C:\Users\ALONZO~
1.SPI\AppData\Local\Temp\IXP000.TMP\un598654.exe.EQ.gID: 3924, Name: qu2705.exe, CommandLine: C:\Users\ALONZO~1.SPI\AppData\Local\Temp\IXP001.TMP\qu2705.exe
```

2 client pkts, 22 server pkts, 41 turns.

Entire conversation (111 kB) Show data as ASCII Stream 439

Task16: There was another alert after this incident of data exfiltration from another FTP server hosting critical files. Our TI team believe there may have been an internal credential leak. What's the IP address and the password of the FTP server which Alonzo had access to?

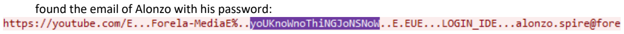
- This was a tough one, I initially thought we would find the answer in the TCP stream, so I searched for keywords like 'FTP', 'Alonozo', 'PASS', and 'USER'.
  Eventually, I searched for ':21' and successfully found the IP address, username, and password:



```
Authorization..ns1. b91988a63a24940038d9262827a5320cD.........D.a...R.2D,D*...D.......V.B.
.B}..b...i.ESE...13.45.67.23:21E...alonzo.spireE%..TheAwesomeGrape........?&http://tempuri.org/Entity/Id12Response.Id12Response
```

Task17: What was the password of the YouTube channel which was hacked?

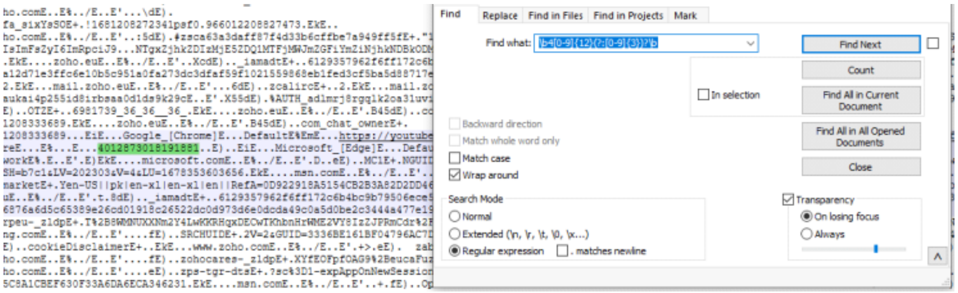
- To address this question, I searched on the 'TCP Stream' of the Redline stealer 'youtube.com' and found the email of Alonzo with his password:



```
https://youtube.com/E...Forela-MediaE%..yoUKnoWnoThiNGJoNSNoW..E.EUE...LOGIN_IDE...alonzo.spire@fore
```

Task18: Alonzo reported unauthorized use of his credit card and assumed his card details were stolen. Please confirm his credit card number.

- For this challenge, I reached out to a friend who had previously solved it.
  Given that we were dealing with stealer malware, I suspected that stolen media might be found in the TCP stream of the command-and-control server.
  To aid in the search, I asked ChatGPT for a regex pattern for credit card numbers and found the answer using the following regex: \b4[0-9]{12}(?:[0-9]{3})?\b.



```
ho.comE..E%../E..E'...\dE).
fa_sixYsSOE+.!1681208272341psf0.966012208827473.EkE..
ho.comE..E%../E..E'..:5dE).#zsca63a3daff87f4d33b6cffbe7a949ff5fE+."1
IsImFsZyI6ImRpciJ9...NTgxZjhkZDIzMjE5ZDQ1MTFjMWJmZGFiYmZiNjhkNDBkODM
.EkE....zoho.euE..E%../E..E'..XcdE).._iamadtE+..6129357962f6ff172c6b
a12d71e3ffc6e10b5c951a0fa273dc3dfaf59f1021559868eb1fed3cf5ba5d88717e
2.EkE...mail.zoho.euE..E%../E..E'...6dE)..zcalircE+..2.EkE...mail.zo
aukai4p255id8irbsaa0d1ds9k29cE..E'.X55dE).%AUTH_adlmrj8rgqlk2oa31uvi
E)..OTZE+..6981739_36_36__36_.EkE....zoho.euE..E%../E..E'.B45dE)..co
1208333689.EkE....zoho.euE..E%../E..E'.B45dE)..com_chat_ownerE+.
1208333689...EiE...Google_[Chrome]E...DefaultE%EmE...https://youtube
reE...E%...E...4012873018191881..E)..EiE...Microsoft_[Edge]E...Defau
workE%.E..E'.E)EkE....microsoft.comE..E%../E..E'.D..eE)..MC1E+.NGUID
SH=b7c1&LV=202303&V=4&LU=1678353603656.EkE....msn.comE..E%../E..E'..
marketE+.Yen-US||pk|en-xl|en-xl|en||RefA=0D922918A5154CB2B3A82D2DD46
uE..E%../E..E'.t.8dE).._iamadtE+..6129357962f6ff172c6b4bc9b79506ece5
6876a6d5c65389e26cd01918c26522dc0d973d6e0dcda49c0a5d0be2c3444a477e19
rpeu-_zldpE+.T%2B8WMNUXXNm2Y4LwKKRHqxDECwTKhbnHrWME2VY8IzZJPRmCdr%2F
ng.comE..E%../E..E'....fE)..SRCHUIDE+.2V=2&GUID=3336BE161BF04796AC7D
E)..cookieDisclaimerE+..EkE...www.zoho.comE..E%../E..E'.+>.eE).  zab
ho.comE..E%../E..E'....fE)..zohocares-_zldpE+.XYfEOFpfOAG9%2BeucaFuz
ho.comE..E%../E..E'....eE)..zps-tgr-dtsE+.?sc%3D1-expAppOnNewSession
5C8A1CBEF630F33A6DA6ECA346231.EkE....msn.comE..E%../E..E'..+.fE)..Op
```

Find what: \b4[0-9]{12}(?:[0-9]{3})?\b

☐ In selection

☐ Backward direction
☐ Match whole word only
☐ Match case
☑ Wrap around

Search Mode
○ Normal
○ Extended (\n, \r, \t, \0, \x...)
● Regular expression ☐ . matches newline

☑ Transparency
● On losing focus
○ Always

Task19: A migration plan document was also stolen in the attack which included some sensitive internal information. Who sent the document to Alonzo?

- I filtered in the TCP stream 'AWS' and found the document 'AWS-Migration assesment.docx'.
  I saved all the TCP-Stream as '.docx' file and opened the file and found the answer:

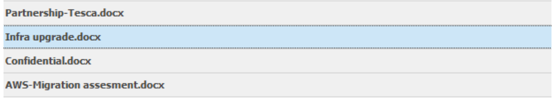
Sincerely,

Abdullah Yasin

Senior Devops @ Forela Pakistan

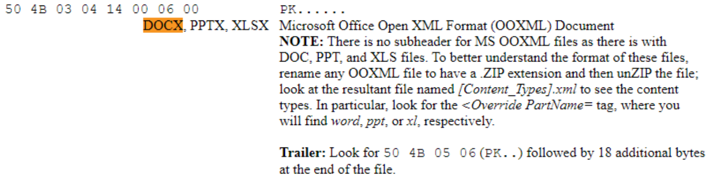
Task20: **Forela is planning to upgrade its infrastructure as its expanding globally. What's the date when the infrastructure will be upgraded?**

- I filtered via the parsed MFT, the documents folder of the compromised account and found the relevant files:



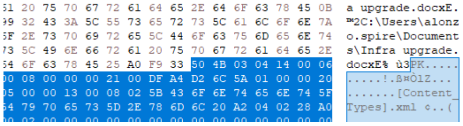
Partnership-Tesca.docx
Infra upgrade.docx
Confidential.docx
AWS-Migration assesment.docx

- We will focus on 'infra upgrade.docx'.
  I saved the TCP-Stream in 'Raw' format and found the signature of 'docx' file in Garykessler.net website:

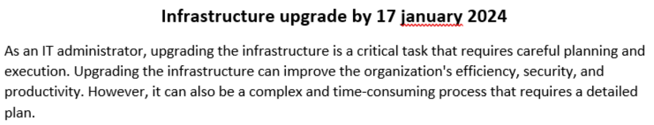


50 4B 03 04 14 00 06 00	PK......
DOCX, PPTX, XLSX	Microsoft Office Open XML Format (OOXML) Document **NOTE:** There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively. **Trailer:** Look for 50 4B 05 06 (PK..) followed by 18 additional bytes at the end of the file.

- I opened the RAW format via 'HxD' and found when the file starts and when it ends.
  I copy the data to a new file and saved it as 'docx' and found the answer:



```
51 20 75 70 67 72 61 64 65 2E 64 6F 63 78 45 0B  a upgrade.docxE.
99 32 43 3A 5C 55 73 65 72 73 5C 61 6C 6F 6E 7A  ™2C:\Users\alonz
5F 2E 73 70 69 72 65 5C 44 6F 63 75 6D 65 6E 74  o.spire\Document
73 5C 49 6E 66 72 61 20 75 70 67 72 61 64 65 2E  s\Infra upgrade.
54 6F 63 78 45 25 A0 F9 33 50 4B 03 04 14 00 06  docxE% ù3PK.....
00 08 00 00 00 21 00 DF A4 D2 6C 5A 01 00 00 20  .....!.ß¤ÒlZ...
05 00 00 13 00 08 02 5B 43 6F 6E 74 65 6E 74 5F  .......[Content_
54 79 70 65 73 5D 2E 78 6D 6C 20 A2 04 02 28 A0  Types].xml ¢..(
00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



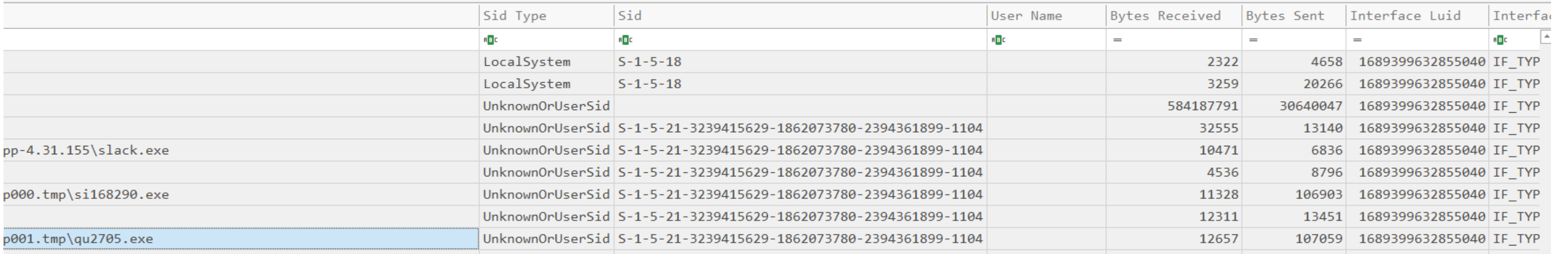
Infrastructure upgrade by 17 january 2024

As an IT administrator, upgrading the infrastructure is a critical task that requires careful planning and execution. Upgrading the infrastructure can improve the organization's efficiency, security, and productivity. However, it can also be a complex and time-consuming process that requires a detailed plan.

Task21: **How many bytes of data were sent by the malicious process found in question 14? Please note - the PCAP data does not provide the answer.**

- Initially, I attempted to find the answer using firewall logs, but I was unsuccessful.
  I always keep my 'CheatSheet' open for reference.
  I noticed the 'SRUM DB' artifact, which tracks 30 to 60 days of system resource usage, including application resource usage, energy usage, Windows push notifications, network connectivity, and data usage.
  I used 'SrumEcmd' to parse the database.

- I found the answer via the parsed 'NetworkUsages' CSV:



	Sid Type	Sid	User Name	Bytes Received	Bytes Sent	Interface Luid	Interfa
	ABC	ABC	ABC	=	=	=	ABC
	LocalSystem	S-1-5-18		2322	4658	1689399632855040	IF_TYP
	LocalSystem	S-1-5-18		3259	20266	1689399632855040	IF_TYP
	UnknownOrUserSid			584187791	30640047	1689399632855040	IF_TYP
	UnknownOrUserSid	S-1-5-21-3239415629-1862073780-2394361899-1104		32555	13140	1689399632855040	IF_TYP
pp-4.31.155\slack.exe	UnknownOrUserSid	S-1-5-21-3239415629-1862073780-2394361899-1104		10471	6836	1689399632855040	IF_TYP
	UnknownOrUserSid	S-1-5-21-3239415629-1862073780-2394361899-1104		4536	8796	1689399632855040	IF_TYP
p000.tmp\si168290.exe	UnknownOrUserSid	S-1-5-21-3239415629-1862073780-2394361899-1104		11328	106903	1689399632855040	IF_TYP
	UnknownOrUserSid	S-1-5-21-3239415629-1862073780-2394361899-1104		12311	13451	1689399632855040	IF_TYP
p001.tmp\qu2705.exe	UnknownOrUserSid	S-1-5-21-3239415629-1862073780-2394361899-1104		12657	107059	1689399632855040	IF_TYP