Heist Challenge

Sherlock Scenario
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.

Task 1:
At what time was the suspected phishing email received in the victim's inbox? (UTC)

I checked the Email.eml file

```
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)
```

Answer: 2023-04-11 08:55:22

Task 2:
Please provide the download URL that was utilised to retrieve the file initially downloaded as part of this security event.

I checked the Chrome History and found several links of the Google drive and docs.
Then I found the correct URL at the "downloads_url_chains" table

11	12	0	https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1osgi4uhbafl/1681208325000/03105725814018983462/13809461445078444789Z/1KsmFJYLzRefViXzeyWYOoojfewRmJgpp?e=download&uuid=d3c34b3f-c99f-42b3-84b3-dfc4ac4f609a
12	12	1	https://drive.google.com/nonceSigner?nonce=iojdml3dsjS8i&continue=https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1osgi4uhbafl/1681208325000/03105725814018983462/13809461445078444789Z/1KsmFJYLzRefViXzeyWYOoojfewRmJgpp?..
13	12	2	https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1osgi4uhbafl/1681208325000/03105725814018983462/13809461445078444789Z/1KsmFJYLzRefViXzeyWYOoojfewRmJgpp?e=download&uuid=d3c34b3f-c99f-42b3-84b3-...

Answer: https://doc-0s-5g-docs.googleusercontent.com/docs/securesc/sjpaukai4p255id8irbsaa0d1ds9k29c/o8kmueker1h57tkoe14o1osgi4uhbafl/1681208325000/03105725814018983462/13809461445078444789Z/1KsmFJYLzRefViXzeyWYOoojfewRmJgpp?e=download&uuid=d3c34b3f-c99f-42b3-84b3-dfc4ac4f609a&nonce=iojdml3dsjS8i&user=13809461445078444789Z&hash=o5gmgdrljfhdo4hvrt3oparan4sq0hm5

Task 3:
What is the name of the file suspected to have been initially downloaded as part of this security event?

At the downloads table, the tab_url is "https://drive.google.com/drive/folders/1ZxG5yDGNVD_qlC8PXorVrTt6HwX3Vt1d"

tab_url
Filter
https://filezilla-project.org/download.php?platform=win64
https://drive.google.com/drive/folders/1ZxG5yDGNVD_qlC8PXorVrTt6HwX3Vt1d

So the target_path was "C:\Users\alonzo.spire\Downloads\Forela-Partnership.zip"

id	guid	current_path	target_path ▾¹
Filter	Filter	Filter	Filter
6	d2144ea2-67ef-4993-b58d-f1b802aea486	C:\Users\alonzo.spire\Downloads\FileZilla_3.63.2.1_win64_sponsored2-setup.exe	C:\Users\alonzo.spire\Downloads\FileZilla_3.63.2.1_win64_sponsored2-setup.exe
12	0a0a73ba-5f66-4fad-84cc-379cc0afb939	C:\Users\alonzo.spire\Downloads\Forela-Partnership.zip	C:\Users\alonzo.spire\Downloads\Forela-Partnership.zip

Answer: Forela-Partnership.zip

Task 4:
When was this file downloaded onto the system?

I have a Python script for webkit timestamp at the "start_time" - "13325681964931025"

target_path ▾¹	start_time
Filter	Filter
C:\Users\alonzo.spire\Downloads\FileZilla_3.63.2.1_win64_sponsored2-setup.exe	13325655398448472
C:\Users\alonzo.spire\Downloads\Forela-Partnership.zip	13325681964931025

```
from datetime import datetime, timedelta

def convert_webkit_timestamp(webkit_timestamp):
    # Convert microseconds to seconds
    seconds_since_1601 = webkit_timestamp / 1e6

    # Define the start date (January 1, 1601)
    epoch_start = datetime(1601, 1, 1)

    # Calculate the actual date and time
    visit_datetime = epoch_start + timedelta(seconds=seconds_since_1601)

    # Format the datetime in the desired format
    return visit_datetime.strftime('%Y-%m-%d %H:%M:%S')

# Example usage
webkit_timestamp = 13325681964931025
formatted_date = convert_webkit_timestamp(webkit_timestamp)
print(f"Formatted Date and Time: {formatted_date}")
```

```
C:\Users\Bubbi\Desktop
λ python hara.py
Formatted Date and Time: 2023-04-11 10:19:24
```

Answer: 2023-04-11 10:19:24

Task 5:
What is the name of the file that initiated malicious activity on the endpoint?

I searched in the MFT for ".\Users\alonzo.spire\Downloads" because I assumed the user extracted the Forela-Partnership.zip and opened the file.
Then I found a suspicious file with extension of .pdf.exe similar to the name of the Partnership

89200	☐	85324	4	213314	4	☑	.\Users\alonzo.spire\Downloads Partnership.pdf.exe

Answer: Partnership.pdf.exe

Task 6:
What file type was the malicious payload disguised as to deceive the user into executing it?

Same as task 5

Answer: pdf

Task 7:
From which directory path was the malicious file executed?

I checked the Prefetch and searched for the file Partnership.pdf.exe and then looked at the Files Loaded tab

```
\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\USER32.DLL,
\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\WOW64CPU.DLL,
\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSWOW64\NTDLL.DLL,
\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\DOCUMENTS\PARTNERSHIP.PDF.EXE,
```

Answer: C:\USERS\ALONZO.SPIRE\DOCUMENTS\

Task 8:

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

I searched in the MFT for ".\Users\alonzo.spire\Desktop" and then choose the extension .txt and found file named reminder.exe

Line	Tag	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name	Extension
=	▣	=	=	=	=	▣			= .txt
518906	☐	427727	2	213316	4	☑	.\Users\alonzo.spire\Desktop	reminder.txt	.txt

Then I took the Entry Number 427727 and used it with MFTECmd.exe --de command

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


C:\Users\Bubble\Desktop\EZTools>MFTECmd.exe -f C:\Users\Bubble\Desktop\Heist\Acquisition\C\$MFT --de 427727
```

Answer: Contact Pakistan operations team to get updates and assist them if needed

Task 9:
At what time was the malicious file was executed?

I searched in the Prefetch for "Partnership.pdf.exe" and took the Last Run timestamp

Executable Name	Run Count	Hash	Size	Version	Last Run
	=		=		=
PARTNERSHIP.PDF.EXE	1	CCA24020	25148	Windows …	2023-04-11 10:20:06

Answer: 2023-04-11 10:20:06

Task 10:
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)

Same log from task 9 and 7, I checked the Files Loaded tab and found the 2 files

```
\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\APPDATA\LOCAL\TEMP\IXP000.TMP\UN598654.EXE,
\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\APPDATA\LOCAL\TEMP\IXP000.TMP\SI168290.EXE
```

Answer: SI168290.EXE, UN598654.EXE

Task 11:
One of the files from Question 10 dropped two more files onto the system. What are the names of these files? (in alphabetical order)

I did the same thing like task 10

```
\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\APPDATA\LOCAL\TEMP\IXP001.TMP\PRO5093.EXE,
\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\APPDATA\LOCAL\TEMP\IXP001.TMP\QU2705.EXE
```

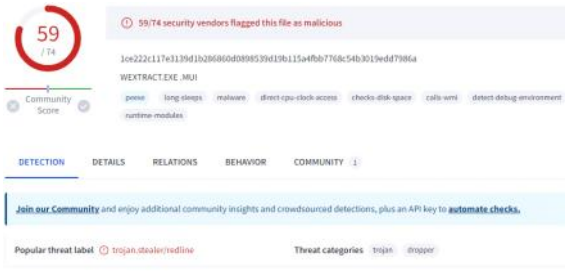
Answer: PRO5093.EXE, QU2705.EXE

Task 12:
What's the malicious C2 IP Address and port?

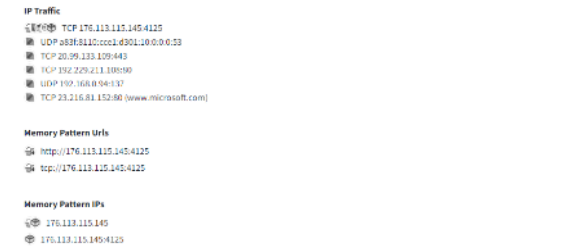
I searched on the Amcache for the malicious file Partnership.pdf.exe

SHA1	Is Os Component	Full Path
	▣	
4497fa1407ff15dbec75f30a6c694b006919aa97	☐	c:\users\alonzo.spire\documents\partnership.pdf.exe

Then I copied the SHA1 and checked it on Virus Total - 4497fa1407ff15dbec75f30a6c694b006919aa97



I checked the Behavior tab



Answer: 176.113.115.145:4125

Task 13:
What's the malware family of the malicious file?

Same as task 12

Answer: redline

Task 14:
Which malicious file exfiltrated data from the endpoint?

I filtered in Wireshark for the C2 IP "ip.addr == 176.113.115.145"
Then I followed the TCP Stream and saw a path with the file name "qu2705" from task 11

```
.
authorization..ns1. 050a19e1db4d0024b0f23b37dcf961f4D...'v.',.J.T.[....D,D*...D.......V.B.
.B...b...i.E.. E912D56B3150DDB765130685 6DF9286BE...(UTC+05:00) Islamabad, KarachiE...UNKNOWNE.....E.....E!.>C:\Users\alonzo.spire\AppData\Local\Temp\IXP001.TMP\qu2705.exe
```

Answer: C:\USERS\ALONZO.SPIRE\APPDATA\LOCAL\TEMP\IXP001.TMP\QU2705.EXE

Task 15:
What's the process ID of the malicious file used to exfiltrate data?

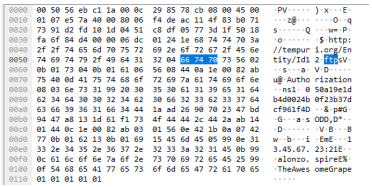
I searched for the file name "qu2705" inside the TCP Stream

```
ID: 3924, Name: qu2705.exe,
```

Answer: 3924

Task 16:
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?

I searched on Wireshark for "FTP" until I saw some packet with a data contains alonzo.spire which also come from the C2 IP 176.113.115.145



I followed the TCP Stream and searched for alonzo and found some IP with a string that look like a password

Answer: 13.45.67.23:TheAwesomeGrape

Task 17:
What was the password of the YouTube channel which was hacked?

Same thing as task 16, while seaching for alonzo I found some strings related to youtube

Answer: yoUKnoWnoThiNGJoNSNoW

Task 18:
Alonzo reported unauthorised use of his credit card and assumed his card details were stolen. Please confirm his credit card number.

I copied some of the TCP Stream text to ChatGPT and asked him to can I find the credit card number. ChatGPT recommended to use regex for 16 digits characters like a card number so I told him to build a Python script.

```
import re

# File path to your text file
file_path = r"C:\Users\Bubble\Desktop\file.txt"

# Regular expression to match exactly 16-digit sequences
cc_regex = re.compile(r"\b\d{16}\b")

# Function to search for 16-digit numbers in the file
def find_credit_card_numbers(file_path):
    credit_card_numbers = [] # List to store all 16-digit numbers
    with open(file_path, 'r') as file:
        content = file.readlines()

        # Loop through each line to search for 16-digit numbers
        for line_num, line in enumerate(content, 1):
            matches = cc_regex.findall(line)
            if matches:
                credit_card_numbers.extend(matches)
                print(f"Line {line_num}: {matches}")

    return credit_card_numbers

# Execute the search and collect 16-digit numbers
credit_card_numbers = find_credit_card_numbers(file_path)

# Print the complete list of detected 16-digit numbers
print("\nList of detected 16-digit numbers:")
print(credit_card_numbers)
```

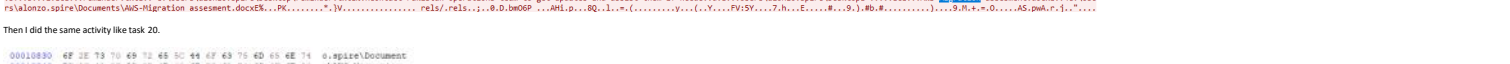
```
C:\Users\Bubble\Desktop
λ python hara.py
Line 386: ['1809936145018042', '1809936145018042', '1809936145016661']
Line 390: ['5432079189712224']
Line 392: ['4012873018191881']
Line 394: ['7208294490084863']
Line 471: ['1681204696177197']

List of detected 16-digit numbers:
['1809936145018042', '1809936145018042', '1809936145016661', '5432079189712224', '4012873018191881', '7208294490084863', '1681204696177197']
```

Answer: 4012873018191881

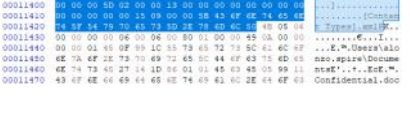
Task 19:
A migration plan document was also stolen in the attack which included some sensitive internal information. Who sent the document to Alonzo?

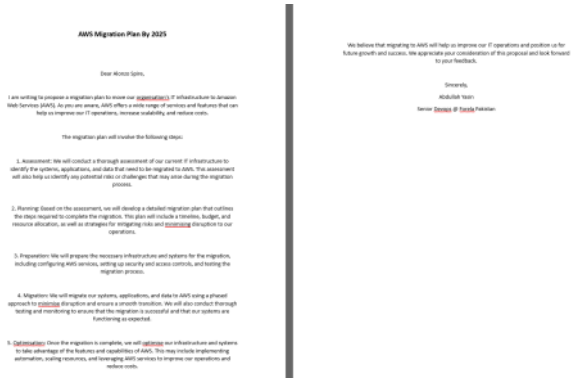
This is was last question for me, I first completed task 20 so I did the same like task 20.

Inside the TCP stream I searched for migration and found the filename and path



Then I did the same activity like task 20.





AWS Migration Plan By 2025

Dear Alonzo Spire,

I am writing to propose a migration plan to move our organization's IT infrastructure to Amazon Web Services (AWS). As you are aware, AWS offers a wide range of services and features that can help us improve our IT operations, increase scalability, and reduce costs.

The migration plan will involve the following steps:

1. Assessment: We will conduct a thorough assessment of our current IT infrastructure to identify the systems, applications, and data that need to be migrated to AWS. This assessment will also help us identify any potential risks or challenges that may arise during the migration process.

2. Planning: Based on the assessment, we will develop a detailed migration plan that outlines the steps required to complete the migration. This plan will include a timeline, budget, and resource allocation, as well as strategies for mitigating risks and minimizing disruption to our operations.

3. Preparation: We will prepare the necessary infrastructure and systems for the migration, including configuring AWS services, setting up security and access controls, and testing the migration process.

4. Migration: We will migrate our systems, applications, and data to AWS using a phased approach to minimize disruption and ensure a smooth transition. We will also conduct thorough testing and monitoring to ensure that the migration is successful and that our systems are functioning as expected.

5. Optimization: Once the migration is complete, we will optimize our infrastructure and systems to take advantage of the features and capabilities of AWS. This may include implementing automation, scaling resources, and leveraging AWS services to improve our operations and reduce costs.

We believe that migrating to AWS will help us improve our IT operations and position us for future growth and success. We appreciate your consideration of this proposal and look forward to your feedback.

Sincerely,

Abdullah Yasin

Senior Devops @ Forela Pakistan

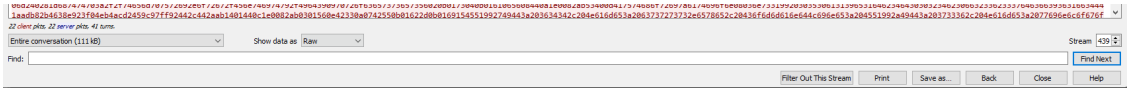
Answer: Abdullah Yasin

Task 20:
Forela is planning to upgrade its infrastructure as its expanding globally. What's the date when the infrastructure will be upgraded?

Inside the TCP Stream, I searched for "infra" and found the file from the path "C:\Users\alonzo.spire\Documents\Infra upgrade.docx"

```
E...Users\alonzo.spire\Documents\'.....EcE...Infra upgrade.docxE..2C:\Users\alonzo.spire\Documents\Infra upgrade.docxE%
```

Then I changed the TCP Stream from "ASCII" to "Raw" and clicked on "Save as"

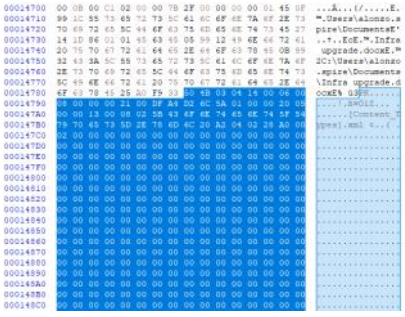


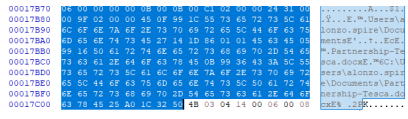
Then I opened the file with "HxD" but first, there is a website "https://www.garykessler.net/library/file_sigs.html" which is a signatures table for files extensions. I searched in the website for "DOCX" which shows how the HEX should look like while searching for it in "HxD"

The HEX for DOCX

`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.
`50 4B 03 04 14 00 08 00`		`PK.....`

Inside HxD I searched for "docx" and found the file name and the path we found in the TCP Stream. Then I copied the 50 4B which is also the "PK" like the picture said from Gary Kessler website and scrolled down until I found another docx file that start with 50 4B





I copied it and open a new tab in HxD paste it and saved it as filename.docx and opened it

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.

The first step in an infrastructure upgrade plan is to assess the current state of the infrastructure. This includes identifying the hardware, software, and network components that need to be upgraded, as well as any potential risks or vulnerabilities. Once the assessment is complete, it is important to define the goals and objectives of the upgrade, such as improving performance, increasing capacity, or enhancing security.

Next, it is important to develop a detailed plan that outlines the steps required to complete the upgrade. This plan should include a timeline, budget, and resource allocation. It should also identify any potential risks or challenges that may arise during the upgrade process and outline strategies for mitigating those risks.

Once the plan is in place, it is time to execute the upgrade. This may involve installing new hardware or software, configuring network components, and testing the new infrastructure to ensure that it meets the organization's needs and requirements. It is important to communicate the upgrade plan and its impact to all stakeholders, including employees and customers, to minimize disruption and ensure a smooth transition.

Finally, it is important to monitor the new infrastructure and make any necessary adjustments or improvements. This may involve regular maintenance, updates, and security audits to ensure that the infrastructure remains secure, reliable, and efficient.

Keeping all this in mind, it would be cost effective and secure to move into hybrid environment by connecting out AWS and On prem infrastructure. This way we can slowly fully migrate into the cloud in the future. I have tasked "Abdullah Yasin", our dev in Lahore, Pakistan to create this plan and send it to me. I will present that in our quarterly meeting

By following a detailed infrastructure upgrade plan, I can help ensure that the organization's IT infrastructure remains up-to-date and meets the evolving needs of the business.

Answer: 2024-01-17

Task 21:
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.

I checked the SRUM artifact and checked the NetwrokUsages and searched for the file from task 14 "QU2705"

Exe Info	Sid Type	Sid	User Name	Bytes Received	Bytes Sent
=	=	=	=	=	=
\device\harddiskvolume3\users\alonzo.spire\appdata\local\temp\isp001.tmp\qu2705.exe	UnknownOrUserSid	S-1-5-21-323941629-1062073780-2394361899-1104		32657	107059

Answer: 107059