Hunter - Walkthrough

Friday, August 23, 2024 10:36 PM

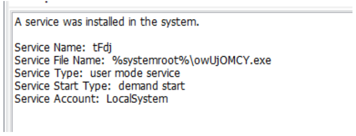
Story:
A SOC analyst received an alert about possible lateral movement and credential stuffing attacks. The alerts were not of high confidence and there was a chance of false positives as the SOC was newly deployed.
Upon further analysis and network analysis by senior soc analyst it was confirmed that 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 occurred.

Task1: What is the MITRE technique ID of the tactic used by the attacker to gain initial access to the system?

- Initially, I suspected that a user might have downloaded a malicious file and executed it manually. Upon reviewing Alonzo's Chrome history, I found that he had downloaded 'Process-Hacker,' 'PowerView,' and 'adaudit.ps1'—all tools associated with Active Directory and SQL Server enumeration. This suggests that the user's account was compromised. Additionally, I checked the Defender logs, which confirmed that a METERPRETER payload had been quarantined.

```
Start time:06-21-2023 17:34:08
Threat Name:Trojan:Win64/Meterpreter.E
Threat ID:2147721833
Action:quarantine
Resource action complete:Quarantine
Schema:shellopencmd
Path:HKLM\SOFTWARE\CLASSES\txtfile\shell\open\command\\
Threat ID:2147721833
Resource refcount:1
Result:0
Resource action complete:Quarantine
Schema:file
Path:\\?\C:\Users\alonzo.spire\notepad.exe
Threat ID:2147721833
Resource refcount:1
Result:0
Action replace successful on registry value:HKLM\SOFTWARE\CLASSES\txtfile\shell\open\command\\
Registry key:SOFTWARE\CLASSES\txtfile\shell\open\command
Value name:
Value data:%SystemRoot%\system32\NOTEPAD.EXE %1
```

- The Defender logs also provided a clue about when the attack occurred.
  I began by reviewing logs from 06/21/2023, including PowerShell logs, SMB logs, and Security logs.
  After several hours of searching, I discovered Event ID 7045 in the system logs, which indicates that a service was installed on the system with unusual name and path:



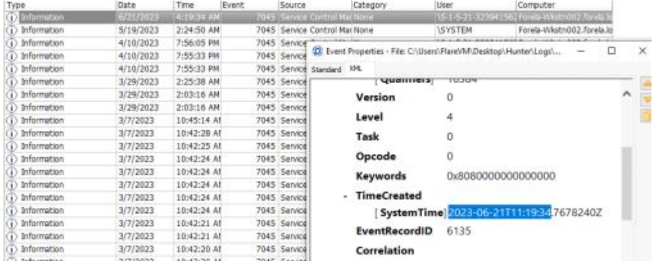
A service was installed in the system.

Service Name: tFdj
Service File Name: %systemroot%\owUjOMCY.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

- The answer is: **'T1569.002'** (Service Execution).
  Since this technique isn't categorized under the Initial Access tactic, the initial point of compromise remains unclear to me.

Task2: When did attacker gain a foothold on the system? (UTC)

- We already found the suspicious service installation of the host, I took the UTC timestamp to address this question:



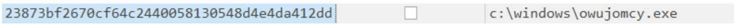
Type	Date	Time	Event	Source	Category	User	Computer
Information	6/21/2023	4:19:34 AM	7045	Service Control Mar	None	\S-1-5-21-32394156	Forela-Wkstn002.forela.lo
Information	5/19/2023	2:24:50 AM	7045	Service Control Mar	None	\SYSTEM	Forela-Wkstn002.forela.lo
Information	4/10/2023	7:56:05 PM	7045	Service			
Information	4/10/2023	7:55:33 PM	7045	Service			
Information	4/10/2023	7:55:33 PM	7045	Service			
Information	3/29/2023	2:25:38 AM	7045	Service			
Information	3/29/2023	2:03:16 AM	7045	Service			
Information	3/29/2023	2:03:16 AM	7045	Service			
Information	3/7/2023	10:45:14 AI	7045	Service			
Information	3/7/2023	10:42:28 AI	7045	Service			
Information	3/7/2023	10:42:25 AI	7045	Service			
Information	3/7/2023	10:42:24 AI	7045	Service			
Information	3/7/2023	10:42:24 AI	7045	Service			
Information	3/7/2023	10:42:24 AI	7045	Service			
Information	3/7/2023	10:42:24 AI	7045	Service			
Information	3/7/2023	10:42:24 AI	7045	Service			
Information	3/7/2023	10:42:21 AI	7045	Service			
Information	3/7/2023	10:42:21 AI	7045	Service			
Information	3/7/2023	10:42:20 AI	7045	Service			

Event Properties - File: C:\Users\FlareVM\Desktop\Hunter\Logs\...
Standard
XML

Version	0
Level	4
Task	0
Opcode	0
Keywords	0x8080000000000000
- TimeCreated	
[SystemTime]	2023-06-21T11:19:34.7678240Z
EventRecordID	6135
Correlation	

Task3: What's the SHA1 hash of the exe which gave remote access to the attacker?

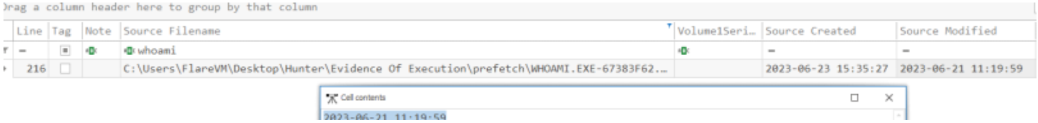
- I assumed that the service name might be the attacker's backdoor.
  I parsed the Amcache and searched for the suspicious process 'owUjOMCY.exe,' which led me to identify its SHA-1 hash.



23873bf2670cf64c2440058130548d4e4da412dd	□	c:\windows\owujomcy.exe

Task4: When was whoami command executed on the system by the attacker? (UTC)

- To address this question, I parsed the 'Perfetch' directory and searched 'Whoami'.
  I found the last execution was at **'2023-06-21 11:19:59'**



Line	Tag	Note	Source Filename	Volume1Seri...	Source Created	Source Modified
=	▣		whoami		=	=
216	□		C:\Users\FlareVM\Desktop\Hunter\Evidence Of Execution\prefetch\WHOAMI.EXE-67383F62...		2023-06-23 15:35:27	2023-06-21 11:19:59

2023-06-21 11:19:59

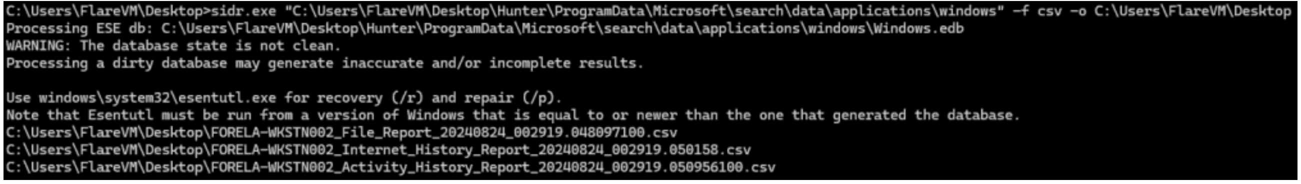
**Task5: We believe the attacker performed enumeration after gaining a foothold.
They likely discovered a PDF document containing RDP credentials for an administrator's workstation.
We believe the attacker accessed the contents of the file and utilized them to gain access to the endpoint.
Find a way to recover contents of the PDF file and confirm the password.**

- To recover the contents of the PDF, we first need to identify the file name and then retrieve its contents.
  I kept my 'Artifact Cheat Sheet' open throughout the process (published on GitHub) and recalled the 'Search Index' artifact.
  This database contains extensive data related to files, images, videos, directories, and other file types on Windows systems.
  It allows us to extract partial contents of various file types, such as DOCX, PDF, TXT, and even browser history, including history that has been deleted from the browser.

  Path: C:\%USERPROFILE%\ProgramData\Microsoft\Search\Data\Applications\Windows \Windows.edb

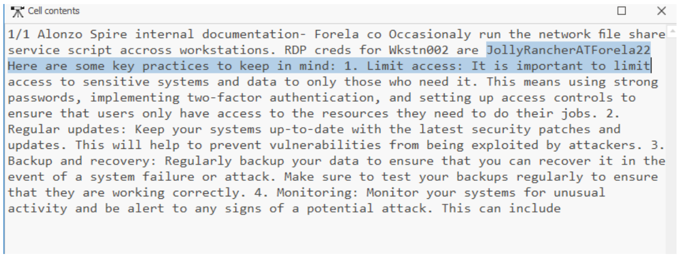
Tool: https://github.com/strozfriedberg/sidr

- After the parsing, we received a several CSVs :



```
C:\Users\FlareVM\Desktop>sidr.exe "C:\Users\FlareVM\Desktop\Hunter\ProgramData\Microsoft\search\data\applications\windows" -f csv -o C:\Users\FlareVM\Desktop
Processing ESE db: C:\Users\FlareVM\Desktop\Hunter\ProgramData\Microsoft\search\data\applications\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.
C:\Users\FlareVM\Desktop\FORELA-WKSTN002_File_Report_20240824_002919.048097100.csv
C:\Users\FlareVM\Desktop\FORELA-WKSTN002_Internet_History_Report_20240824_002919.050158.csv
C:\Users\FlareVM\Desktop\FORELA-WKSTN002_Activity_History_Report_20240824_002919.050956100.csv
```

- I searched 'PDF' as keyword and found the document 'internal_documentation.pdf'.
  On 'System_Search_Auto' Summary.
  We able to see the PDF content:

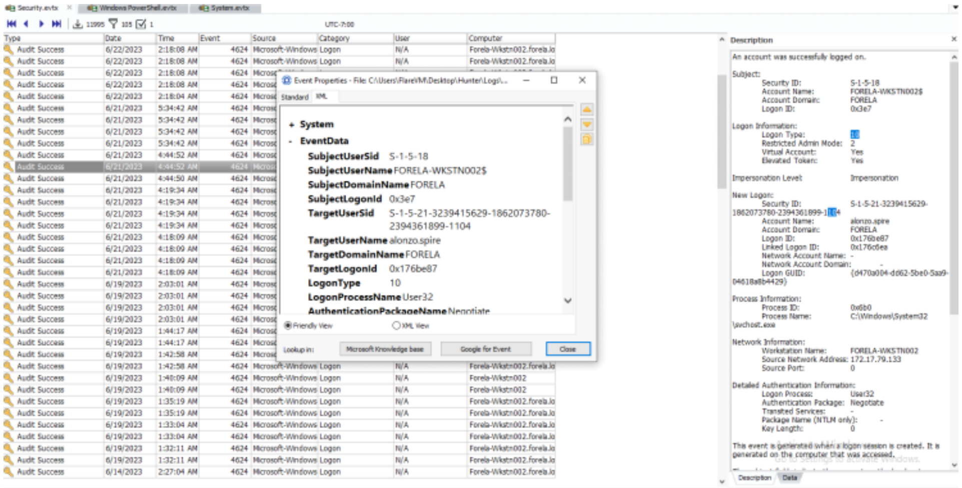


```
1/1 Alonzo Spire internal documentation- Forela co Occasionaly run the network file share
service script accross workstations. RDP creds for Wkstn002 are JollyRancherATForela22
Here are some key practices to keep in mind: 1. Limit access: It is important to limit
access to sensitive systems and data 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
```

- The password is: **JollyRancherATForela22**

Task6: At what time did the adversary initially authenticate utilizing RDP? (UTC)

- I used 'Event Log Explorer' and loaded the 'Security logs' and search event ID 4624 with logon type 10 which indicates as RDP logon:



Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	6/22/2023	2:18:08 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/22/2023	2:18:08 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/22/2023	2:18:08 AM	4624	Microsc			
Audit Success	6/22/2023	2:18:08 AM	4624	Microsc			
Audit Success	6/22/2023	2:18:04 AM	4624	Microsc			
Audit Success	6/21/2023	5:34:42 AM	4624	Microsc			
Audit Success	6/21/2023	5:34:42 AM	4624	Microsc			
Audit Success	6/21/2023	5:34:42 AM	4624	Microsc			
Audit Success	6/21/2023	5:34:42 AM	4624	Microsc			
Audit Success	6/21/2023	4:44:52 AM	4624	Microsc			
Audit Success	6/21/2023	4:44:52 AM	4624	Microsc			
Audit Success	6/21/2023	4:44:50 AM	4624	Microsc			
Audit Success	6/21/2023	4:19:34 AM	4624	Microsc			
Audit Success	6/21/2023	4:19:34 AM	4624	Microsc			
Audit Success	6/21/2023	4:19:34 AM	4624	Microsc			
Audit Success	6/21/2023	4:19:34 AM	4624	Microsc			
Audit Success	6/21/2023	4:18:09 AM	4624	Microsc			
Audit Success	6/21/2023	4:18:09 AM	4624	Microsc			
Audit Success	6/21/2023	4:18:09 AM	4624	Microsc			
Audit Success	6/21/2023	4:18:09 AM	4624	Microsc			
Audit Success	6/19/2023	2:03:01 AM	4624	Microsc			
Audit Success	6/19/2023	2:03:01 AM	4624	Microsc			
Audit Success	6/19/2023	2:03:01 AM	4624	Microsc			
Audit Success	6/19/2023	2:03:01 AM	4624	Microsc			
Audit Success	6/19/2023	1:44:17 AM	4624	Microsc			
Audit Success	6/19/2023	1:44:17 AM	4624	Microsc			
Audit Success	6/19/2023	1:42:58 AM	4624	Microsc			
Audit Success	6/19/2023	1:42:58 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/19/2023	1:40:09 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002
Audit Success	6/19/2023	1:40:09 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002
Audit Success	6/19/2023	1:35:19 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/19/2023	1:35:19 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/19/2023	1:33:04 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/19/2023	1:33:04 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/19/2023	1:32:11 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/19/2023	1:32:11 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo
Audit Success	6/14/2023	2:27:04 AM	4624	Microsoft-Windows	Logon	N/A	Forela-Wkstn002.forela.lo

Event Properties - File: C:\Users\FlareVM\Desktop\Hunter\Logs\...
Standard
XML

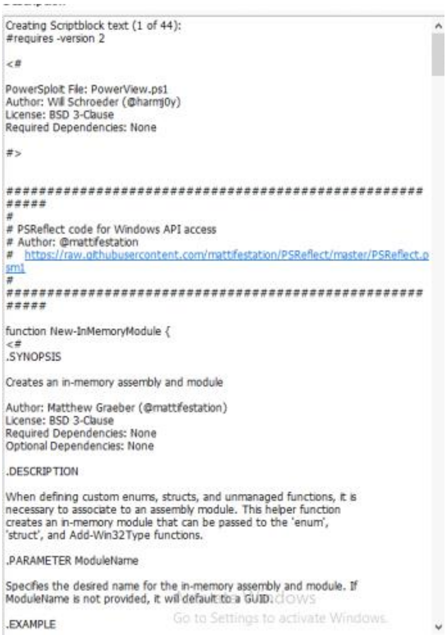
```
+ System
- EventData
    SubjectUserSid          S-1-5-18
    SubjectUserName         FORELA-WKSTN002$
    SubjectDomainName       FORELA
    SubjectLogonId          0x3e7
    TargetUserSid           S-1-5-21-3239415629-1862073780-
                            2394361899-1104
    TargetUserName          alonzo.spire
    TargetDomainName        FORELA
    TargetLogonId           0x176be87
    LogonType               10
    LogonProcessName        User32
    AuthenticationPackageName Negotiate
```

● Friendly View ○ XML View

```
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:  2
        Virtual Account:        Yes
        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

This event is generated when a logon session is created. It is
generated on the computer that was accessed.
```

Task7: 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.

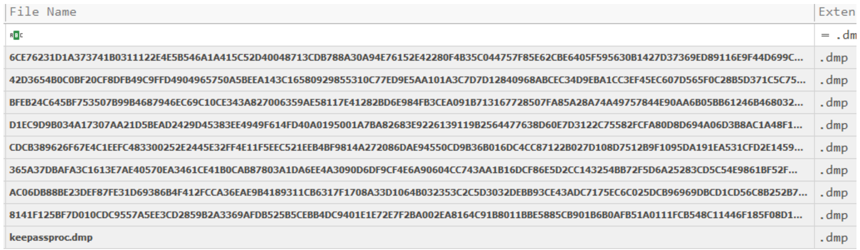
- We already found it on the beginning of the sherlock (Chrome history), you able to load to 'Event log explorer' the PowerShell Operational logs and filter event ID 4104 to see the execution of PowerView.ps1:



```
Creating Scriptblock text (1 of 44):
#requires -version 2

<#

PowerSploit File: PowerView.ps1
Author: Will Schroeder (@harmj0y)
License: BSD 3-Clause
Required Dependencies: None

#>


########################################################
#####
#
# PSReflect code for Windows API access
# Author: @mattifestation
#   https://raw.githubusercontent.com/mattifestation/PSReflect/master/PSReflect.psm1
#
########################################################
#####

function New-InMemoryModule {
<#
.SYNOPSIS

Creates an in-memory assembly and module

Author: Matthew Graeber (@mattifestation)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.DESCRIPTION

When defining custom enums, structs, and unmanaged functions, it is
necessary to associate to an assembly module. This helper function
creates an in-memory module that can be passed to the 'enum',
'struct', and Add-Win32Type functions.

.PARAMETER ModuleName

Specifies the desired name for the in-memory assembly and module. If
ModuleName is not provided, it will default to a GUID.

.EXAMPLE
```

Task8: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?

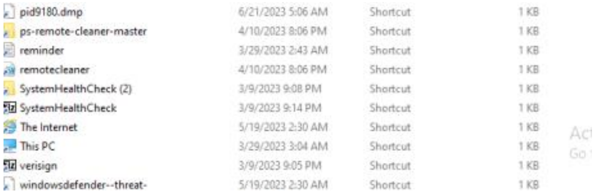
- At Task 9, we were asked to identify the name of the initial dump file. By filtering for files with the .dmp extension, I discovered a process dump named '**keepassproc.dmp**', which was a dump of the KeePass application. This indicates that the threat actor was specifically interested in the KeePass database.



File Name	Exten
ABC	= .dm
6CE76231D1A373741B0311122E4E5B546A1A415C52D40048713CDB788A30A94E76152E42280F4B35C044757F85E62CBE6405F595630B1427D37369ED89116E9F44D699C...	.dmp
42D3654B0C0BF20CF8DFB49C9FFD4904965750A5BEEA143C16580929855310C77ED9E5AA101A3C7D7D12840968ABCEC34D9EBA1CC3EF45EC607D565F0C28B5D371C5C75...	.dmp
BFEB24C645BF753507B99B4687946EC69C10CE343A827006359AE58117E41282BD6E984FB3CEA091B713167728507FA85A28A74A49757844E90AA6B05BB61246B468032...	.dmp
D1EC9D9B034A17307AA21D5BEAD2429D45383EE4949F614FD40A0195001A7BA82683E9226139119B2564477638D60E7D3122C75582FCFA80D8D694A06D3B8AC1A48F1...	.dmp
CDCB389626F67E4C1EEFC483300252E2445E32FF4E11F5EEC521EEB4BF9814A272086DAE94550CD9B36B016DC4CC87122B027D108D7512B9F1095DA191EA531CFD2E1459...	.dmp
365A37DBAFA3C1613E7AE40570EA3461CE41B0CAB87803A1DA6EE4A3090D6DF9CF4E6A90604CC743AA1B16DCF86E5D2CC143254BB72F5D6A25283CD5C54E9861BF52F...	.dmp
AC06DB88BE23DEF87FE31D69386B4F412FCCA36EAE9B4189311CB6317F1708A33D1064B032353C2C5D3032DEBB93CE43ADC7175EC6C025DCB96969DBCD1CD56C8B252B7...	.dmp
8141F125BF7D010CDC9557A5EE3CD2859B2A3369AFDB525B5CEBB4DC9401E1E72E7F2BA002EA8164C91B8011BBE5885CB901B6B0AFB51A0111FCB548C11446F185F08D1...	.dmp
keepassproc.dmp	.dmp

Task9: What was the name of the initial dump file?

- Initially, I searched the MFT and Search Index for any '.dmp' files and discovered 'keepassproc.dmp,' suggesting that the attacker was specifically interested in the KeePass database.
  However, this wasn't the correct answer. I then navigated to the 'Recent' directory of the user, which tracks recently used applications, and found the correct answer there.

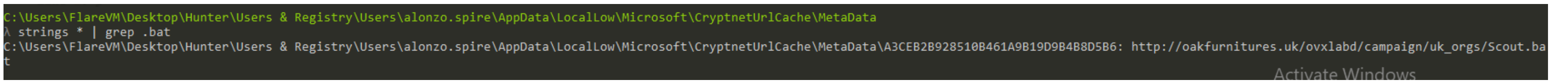


```
pid9180.dmp                 6/21/2023 5:06 AM    Shortcut    1 KB
ps-remote-cleaner-master    4/10/2023 8:06 PM    Shortcut    1 KB
reminder                    3/29/2023 2:43 AM    Shortcut    1 KB
remotecleaner               4/10/2023 8:06 PM    Shortcut    1 KB
SystemHealthCheck (2)       3/9/2023 9:08 PM     Shortcut    1 KB
SystemHealthCheck           3/9/2023 9:14 PM     Shortcut    1 KB
The Internet                5/19/2023 2:30 AM    Shortcut    1 KB
This PC                     3/29/2023 3:04 AM    Shortcut    1 KB
verisign                    3/9/2023 9:05 PM     Shortcut    1 KB
windowsdefender--threat-    5/19/2023 2:30 AM    Shortcut    1 KB
```

Task10: The attackers downloaded a custom batch script from their C2 server. What is the full C2 domain url from where it was downloaded?

- I searched the parsed 'Search Index' database for the '.bat' extension and found a file named scout.bat in C:\Users\alonzo.spire\Pictures\. I then searched for scout.bat across all challenge files and found it referenced in a parsed Prefetch file. The file paths identified were:
  - \VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\IE\OOI66Y9I\SCOUT[1].BAT
  - \VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\PICTURES\SCOUTFF

- This indicated that the 'certutil' utility was likely used to download the file.
  After extensive searching, I eventually found the URL associated with scout.bat in the \Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ directory.
  This directory contains evidence of files downloaded using CertUtil as a download cradle, storing both the content and metadata of these files.

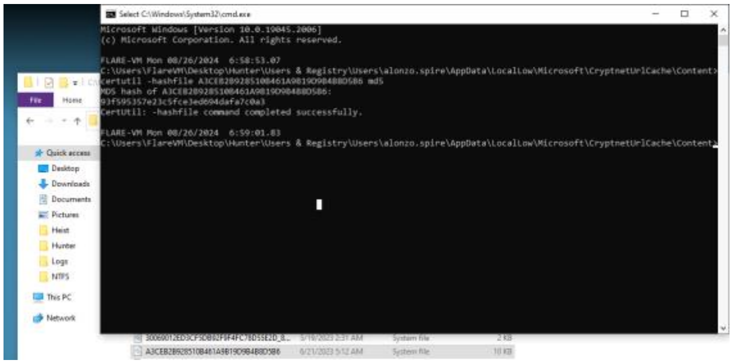


```
C:\Users\FlareVM\Desktop\Hunter\Users & Registry\Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData
λ strings * | grep .bat
C:\Users\FlareVM\Desktop\Hunter\Users & Registry\Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A3CEB2B928510B461A9B19D9B4B8D5B6: http://oakfurnitures.uk/ovxlabd/campaign/uk_orgs/Scout.ba
t
```

Task11: Whats the MD5 hash of the batch script?

- First, I found the content via the 'Search Index', I tried to save it to a new document and extract the hash without success.

- I found the directory C:\Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content and located a file named A3CEB2B928510B461A9B19D9B4B8D5B6, which matched the one we identified earlier. This file stood out because it was 10 KB in size, while all the others were only 1 KB.
  When I opened the file in Notepad, I discovered it contained a script.
  I then used the certutil utility to extract the hash from the file.



```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM Mon 08/26/2024  6:58:53.07
C:\Users\FlareVM\Desktop\Hunter\Users & Registry\Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content>
certutil -hashfile A3CEB289285108461A9819D984B8D5B6 md5
MD5 hash of A3CEB289285108461A9819D984B8D5B6:
93f595357e23c5fce3ed694dafa7c0a3
CertUtil: -hashfile command completed successfully.

FLARE-VM Mon 08/26/2024  6:59:01.83
C:\Users\FlareVM\Desktop\Hunter\Users & Registry\Users\alonzo.spire\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content>
```

30069012ED3CF5DB82F8F4FC7BD55E2D_8...	5/19/2023 2:31 AM	System file	2 KB
A3CEB289285108461A9819D984B8D5B6	6/21/2023 5:12 AM	System file	10 KB

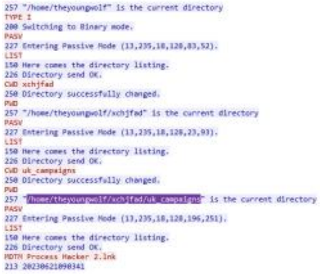
Task12: The attackers tried to exfiltrate the data to their FTP server but couldn't connect to it. The threat intelligence team wants you to collect more TTPs (Tactics, Techniques, and Procedures) and IOCs (Indicators of Compromise) related to the adversary.
It would be really helpful for the TI team 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?

- Initially, I tried to find the answer in Wireshark but could only see the successful login event. Then I remembered seeing FileZilla on the Desktop during my file examination. I navigated to Users \alonzo.spire\AppData\Roaming\FileZilla to investigate further and found the recentservers.xml file. Inside, I discovered the RecentServer content, and the password was encoded in base64. I decoded it and found the answer.

```
            <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>
```

Task13: 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?

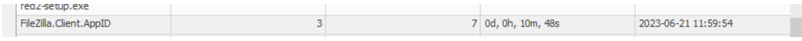
- When I search the answer to the previous question, I filtered FTP in Wireshark and followed the TCP stream of the conversation and found the answer:



```
257 "/home/theyoungwolf" is the current directory
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (13,235,18,128,83,52).
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD xchjfad
250 Directory successfully changed.
PWD
257 "/home/theyoungwolf/xchjfad" is the current directory
PASV
227 Entering Passive Mode (13,235,18,128,23,93).
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD uk_campaigns
250 Directory successfully changed.
PWD
257 "/home/theyoungwolf/xchjfad/uk_campaigns" is the current directory
PASV
227 Entering Passive Mode (13,235,18,128,196,251).
LIST
150 Here comes the directory listing.
226 Directory send OK.
MDTM Process Hacker 2.lnk
213 20230621090341
```

Task14: For how long did the tool used for exfiltrating data, run before being closed? (Answer in seconds)

- We know that the data exfiltration was performed using FileZilla, so I used the 'UserAssist' registry artifact to determine how long FileZilla was in use.



redz-setup.exe				
FileZilla.Client.AppID	3	7	0d, 0h, 10m, 48s	2023-06-21 11:59:54

- NTUSER\Software\Microsoft\Windows\CurrectVersion\Explorer\UserAssist

Task15: 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?

- First, I searched for the keyword 'Project' in the parsed 'Search Index' CSV. I found 'redacted-project.zip' located in 'C:\Users\alonzo.spire\Documents'. Since the ZIP file was in this location, I searched the path and found the file 'REDACTED_SENSITIVE', which is the answer:

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

Task16: What specific CVE did the attacker exploit to gain access to the sensitive contents?

- We already found that the attacker performed a process dump of KeePass, which contains sensitive passwords. **CVE-2023-32784** allows the recovery of the cleartext master password from a memory dump. |
  The memory dump can be a KeePass process dump, a swap file (pagefile.sys), a hibernation file (hiberfil.sys), or a RAM dump of the entire system.

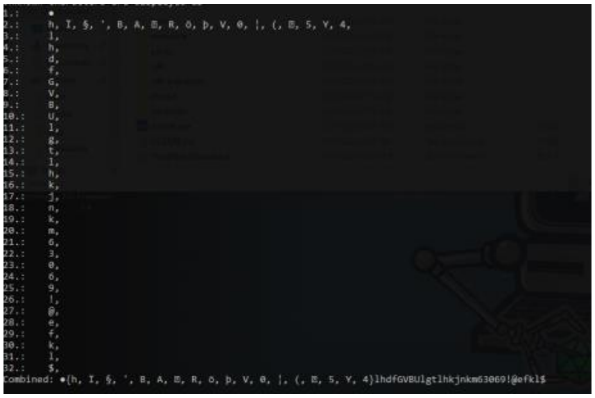
Task 17: Find a way to access the sensitive information. The information was related to development of an internal application. What is the suggested name for this app?

- While navigating through Wireshark, I identified that the attacker exfiltrated several files, including a 'Keepass.db' file. To exploit the vulnerability and access the database, we need to extract the dump of the Keepass process that the attacker obtained. I exported this file from Wireshark, but it is password-protected.

- During our investigation, we found a password in the configuration files of FileZilla for the user 'CyberJunkie'. The password was base64 encoded as 'VGhlQXdlc29tZUdyYXBl', which decodes to

'UionskHGTLDS'. This password is used to unlock the ZIP file containing the Keepass process dump.

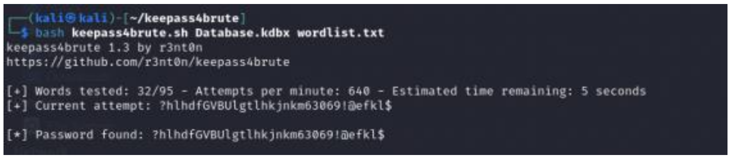
- Next, we need to exploit a known vulnerability to extract the 'Master Key' from the Keepass database. I used this proof-of-concept tool: https://github.com/vdohney/keepass-password-dumper, to perform the operation.



```
1.:     ●
2.:     h, I, §, ', B, A, ▥, R, o, þ, V, ə, ¦, (, ▥, 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.:    $,
Combined: ●{h, I, §, ', B, A, ▥, R, o, þ, V, ə, ¦, (, ▥, 5, Y, 4}lhdfGVBUlgtlhkjnkm63069!@efkl$
```

As you can see, the first character is missing.
We need to create a wordlist.
Syntax: ***hlhdfGVBUlgtlhkjnkm63069!@efkl$**

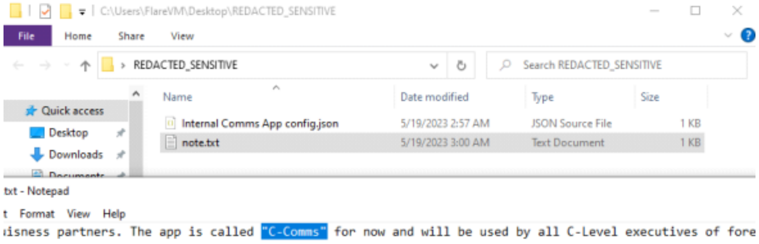
I asked from ChatGPT to build for me a bash script that generate all the available characters and created a list.



```
┌──(kali㉿kali)-[~/keepass4brute]
└─$ bash keepass4brute.sh Database.kdbx wordlist.txt
keepass4brute 1.3 by r3nt0n
https://github.com/r3nt0n/keepass4brute

[+] Words tested: 32/95 - Attempts per minute: 640 - Estimated time remaining: 5 seconds
[+] Current attempt: ?hlhdfGVBUlgtlhkjnkm63069!@efkl$

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

Now, After we hacked the password of the DB, we able to check the DB information.
I found the password for the sensitive project.

I extracted the 'Sensitive Project' and found a file with the name of the application:

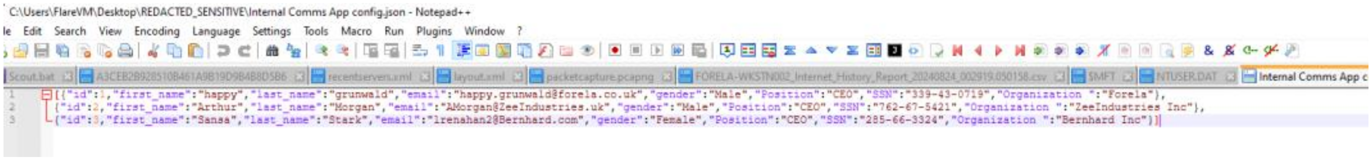


Name	Date modified	Type	Size
Internal Comms App config.json	5/19/2023 2:57 AM	JSON Source File	1 KB
note.txt	5/19/2023 3:00 AM	Text Document	1 KB

```
isness partners. The app is called "C-Comms" for now and will be used by all C-Level executives of fore
```

Task18: SSN were also part of the sensitive project which was exfiltrated by the attacker. What is the SSN number of Arthur Morgan from zeeindustries?

To address this question, you should open the 'Internal Comms App config' file with Notepad++ and locate Arthur Morgan's SSN.

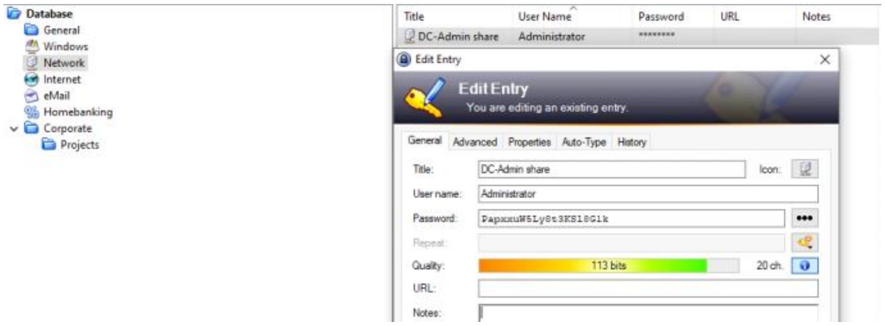


C:\Users\FlareVM\Desktop\REDACTED_SENSITIVE\Internal Comms App config.json - Notepad++
le Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Scout.bat
A3CEB2B928510B461A9B19D984B8D5B6
recentservers.xml
layout.xml
packetcapture.pcapng
FORELA-WKSTN002_Internet_History_Report_20240824_002919.050158.csv
SMFT
NTUSER.DAT
Internal Comms App c

```
[{"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"}]
```

Task19: We believe the domain admin credentials have been leaked in this incident. Please confirm the Domain Admin password?

- You can find the password of the Domain Admin in KeePass DB:



Title	User Name	Password	URL	Notes
DC-Admin share	Administrator	********		

Title: DC-Admin share
User name: Administrator
Password: PapxxuW5Ly8t3KS18G1k
Repeat:
Quality: 113 bits 20 ch.
URL:
Notes: