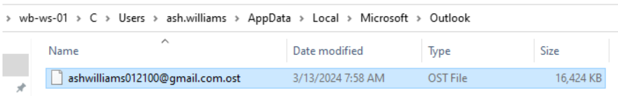
Heartbreaker Challenge

Sherlock Scenario
Delicate situation alert! The customer has just been alerted about concerning reports indicating a potential breach of their database, with information allegedly being circulated on the darknet market. As the Incident Responder, it's your responsibility to get to the bottom of it. Your task is to conduct an investigation into an email received by one of their employees, comprehending the implications, and uncovering any possible connections to the data breach. Focus on examining the artifacts provided by the customer to identify significant events that have occurred on the victim's workstation.

Task 1:
The victim received an email from an unidentified sender. What email address was used for the suspicious email?

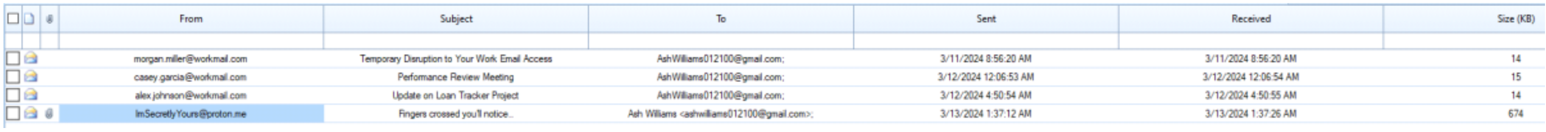
I searched for any App like Outlook in the user directory and found an OST file



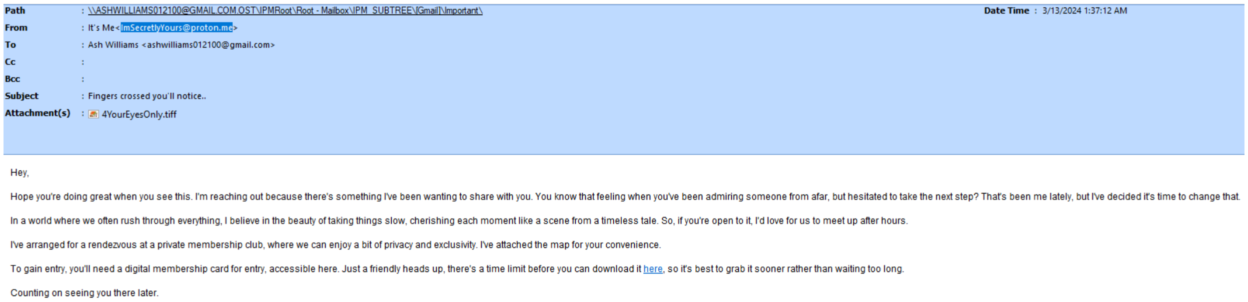
› wb-ws-01 › C › Users › ash.williams › AppData › Local › Microsoft › Outlook

Name	Date modified	Type	Size
ashwilliams012100@gmail.com.ost	3/13/2024 7:58 AM	OST File	16,424 KB

I downloaded "SysTools OST to PST Converter" and opened the OST file.
Then I went to the "Important" folder inside the Inbox and found the emails and 1 email with an attachement



From	Subject	To	Sent	Received	Size (KB)
morgan.miller@workmail.com	Temporary Disruption to Your Work Email Access	AshWilliams012100@gmail.com;	3/11/2024 8:56:20 AM	3/11/2024 8:56:20 AM	14
casey.garcia@workmail.com	Performance Review Meeting	AshWilliams012100@gmail.com;	3/12/2024 12:06:53 AM	3/12/2024 12:06:54 AM	15
alex.johnson@workmail.com	Update on Loan Tracker Project	AshWilliams012100@gmail.com;	3/12/2024 4:50:54 AM	3/12/2024 4:50:55 AM	14
ImSecretlyYours@proton.me	Fingers crossed you'll notice..	Ash Williams <ashwilliams012100@gmail.com>;	3/13/2024 1:37:12 AM	3/13/2024 1:37:26 AM	674



Path : \\ASHWILLIAMS012100@GMAIL.COM.OST\IPMRoot\Root - Mailbox\IPM_SUBTREE\[Gmail]\Important\
Date Time : 3/13/2024 1:37:12 AM
From : It's Me<ImSecretlyYours@proton.me>
To : Ash Williams <ashwilliams012100@gmail.com>
Cc :
Bcc :
Subject : Fingers crossed you'll notice..
Attachment(s) : 4YourEyesOnly.tiff

Hey,

Hope you're doing great when you see this. I'm reaching out because there's something I've been wanting to share with you. You know that feeling when you've been admiring someone from afar, but hesitated to take the next step? That's been me lately, but I've decided it's time to change that.

In a world where we often rush through everything, I believe in the beauty of taking things slow, cherishing each moment like a scene from a timeless tale. So, if you're open to it, I'd love for us to meet up after hours.

I've arranged for a rendezvous at a private membership club, where we can enjoy a bit of privacy and exclusivity. I've attached the map for your convenience.

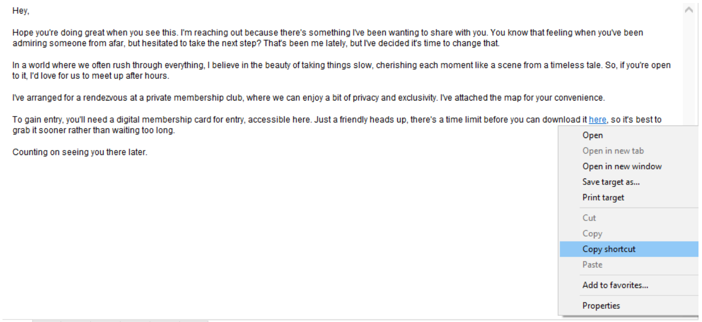
To gain entry, you'll need a digital membership card for entry, accessible here. Just a friendly heads up, there's a time limit before you can download it here, so it's best to grab it sooner rather than waiting too long.

Counting on seeing you there later.

Answer: ImSecretlyYours@proton.me

Task 2:
It appears there's a link within the email. Can you provide the complete URL where the malicious binary file was hosted?

I tried to copy the link from SysTools tool from task 1 by it was broken so I used another tool "MailsDaddy Free OST Viewer"



Hey,

Hope you're doing great when you see this. I'm reaching out because there's something I've been wanting to share with you. You know that feeling when you've been admiring someone from afar, but hesitated to take the next step? That's been me lately, but I've decided it's time to change that.

In a world where we often rush through everything, I believe in the beauty of taking things slow, cherishing each moment like a scene from a timeless tale. So, if you're open to it, I'd love for us to meet up after hours.

I've arranged for a rendezvous at a private membership club, where we can enjoy a bit of privacy and exclusivity. I've attached the map for your convenience.

To gain entry, you'll need a digital membership card for entry, accessible here. Just a friendly heads up, there's a time limit before you can download it here, so it's best to grab it sooner rather than waiting too long.

Counting on seeing you there later.

Answer: http://44.206.187.144:9000/Superstar_MemberCard.tiff.exe

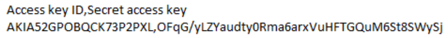
Task 3:
The threat actor managed to identify the victim's AWS credentials. From which file type did the threat actor extract these credentials?

By thinking how the attacker will find the credentials if they only exist in the mail I thought if the user was compromised by the Phishing attachment so he probably extract the credentials from the OST files

Answer: .ost

Task 4:
Provide the actual IAM credentials of the victim found within the artifacts.

Inside the OST file in the "Drafts" tab

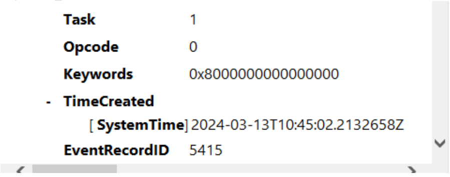


```
Access key ID,Secret access key
AKIA52GPOBQCK73P2PXL,OFqG/yLZYaudty0Rma6arxVuHFTGQuM6St8SWySj
```

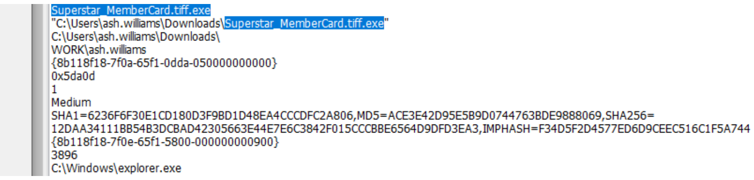
Answer: AKIA52GPOBQCK73P2PXL:OFqG/yLZYaudty0Rma6arxVuHFTGQuM6St8SWySj

Task 5:
When (UTC) was the malicious binary activated on the victim's workstation?

Checked the Sysmon logs and filtered for event ID 1 and the name of the binary Superstar_MemberCard.tiff.exe



Task	1
Opcode	0
Keywords	0x8000000000000000
- **TimeCreated**	
[**SystemTime**]	2024-03-13T10:45:02.2132658Z
EventRecordID	5415

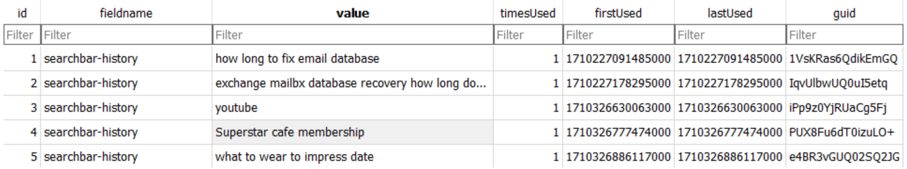


```
Superstar_MemberCard.tiff.exe
"C:\Users\ash.williams\Downloads\Superstar_MemberCard.tiff.exe"
C:\Users\ash.williams\Downloads\
WORK\ash.williams
{8b118f18-7f0a-65f1-0dda-050000000000}
0x5da0d
1
Medium
SHA1=6236F6F30E1CD180D3F9BD1D48EA4CCCDFC2A806,MD5=ACE3E42D95E5B9D0744763BDE9888069,SHA256=
12DAA34111BB54B3DCBAD42305663E44E7E6C3842F015CCCBBE6564D9DFD3EA3,IMPHASH=F34D5F2D4577ED6D9CEEC516C1F5A744
{8b118f18-7f0e-65f1-5800-000000000900}
3896
C:\Windows\explorer.exe
```

Answer: 2024-03-13 10:45:02

Task 6:
Following the download and execution of the binary file, the victim attempted to search for specific keywords on the internet. What were those keywords?

First, I tried to use DB Browser on the History of the edge and I didn't find anything.
Then I saw the Mozilla folder and also found some connections in the Sysmon which the user was downloaded the attachment from Mozilla
Inside the Mozilla Firefox folder I opened the "formhistory.sqlite"

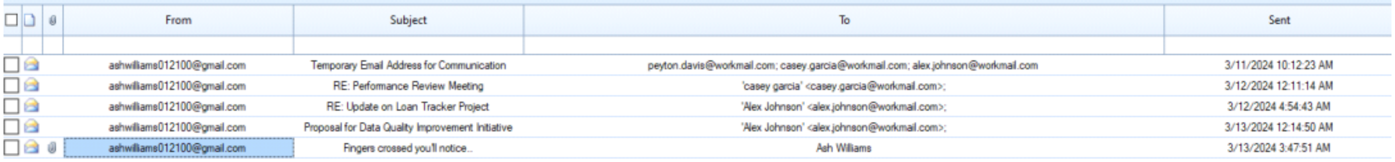


id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	searchbar-history	how long to fix email database	1	1710227091485000	1710227091485000	1VsKRas6QdikEmGQ
2	searchbar-history	exchange mailbx database recovery how long do...	1	1710227178295000	1710227178295000	IqvUlbwUQ0uI5etq
3	searchbar-history	youtube	1	1710326630063000	1710326630063000	iPp9z0YjRUaCg5Fj
4	searchbar-history	Superstar cafe membership	1	1710326777474000	1710326777474000	PUX8Fu6dT0izuLO+
5	searchbar-history	what to wear to impress date	1	1710326886117000	1710326886117000	e4BR3vGUQ02SQ2JG

Answer: Superstar cafe membership

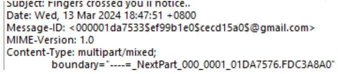
Task 7:
At what time (UTC) did the binary successfully send an identical malicious email from the victim's machine to all the contacts?

I used the SysTools tool again to check this and searched in the Sent items the time



☐			From	Subject	To	Sent
☐			ashwilliams012100@gmail.com	Temporary Email Address for Communication	peyton.davis@workmail.com; casey.garcia@workmail.com; alex.johnson@workmail.com	3/11/2024 10:12:23 AM
☐			ashwilliams012100@gmail.com	RE: Performance Review Meeting	'casey garcia' <casey.garcia@workmail.com>;	3/12/2024 12:11:14 AM
☐			ashwilliams012100@gmail.com	RE: Update on Loan Tracker Project	'Alex Johnson' <alex.johnson@workmail.com>;	3/12/2024 4:54:43 AM
☐			ashwilliams012100@gmail.com	Proposal for Data Quality Improvement Initiative	'Alex Johnson' <alex.johnson@workmail.com>;	3/13/2024 12:14:50 AM
☐			ashwilliams012100@gmail.com	Fingers crossed you'll notice..	Ash Williams	3/13/2024 3:47:51 AM

Then Inside the Message Header I saw another timestamp



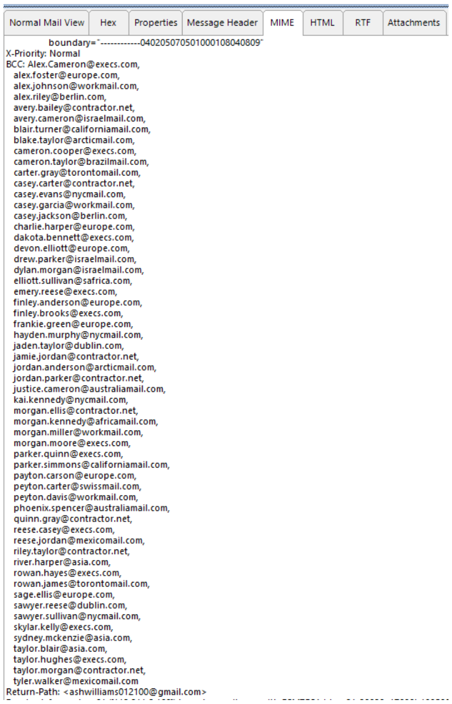
```
Subject: Fingers crossed you'll notice..
Date: Wed, 13 Mar 2024 18:47:51 +0800
Message-ID: <000001da7533$ef99b1e0$cecd15a0$@gmail.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0001_01DA7576.FDC3A8A0"
```

Then I asked the ChatGPT what is the UTC

Answer: 2024-03-13 10:47:51

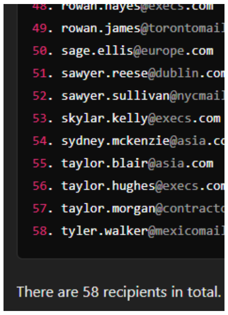
Task 8:
How many recipients were targeted by the distribution of the said email excluding the victim's email account?

Inside the MIME tab from the email there is all the recipients



```
        boundary="------------040205070501000108040809"
X-Priority: Normal
BCC: Alex.Cameron@execs.com,
  alex.foster@europe.com,
  alex.johnson@workmail.com,
  alex.riley@berlin.com,
  avery.bailey@contractor.net,
  avery.cameron@israelmail.com,
  blair.turner@californiamail.com,
  blake.taylor@arcticmail.com,
  cameron.cooper@execs.com,
  cameron.taylor@brazilmail.com,
  carter.gray@torontomail.com,
  casey.carter@contractor.net,
  casey.evans@nycmail.com,
  casey.garcia@workmail.com,
  casey.jackson@berlin.com,
  charlie.harper@europe.com,
  dakota.bennett@execs.com,
  devon.elliott@europe.com,
  drew.parker@israelmail.com,
  dylan.morgan@israelmail.com,
  elliott.sullivan@safrica.com,
  emery.reese@execs.com,
  finley.anderson@europe.com,
  finley.brooks@execs.com,
  frankie.green@europe.com,
  hayden.murphy@nycmail.com,
  jaden.taylor@dublin.com,
  jamie.jordan@contractor.net,
  jordan.anderson@arcticmail.com,
  jordan.parker@contractor.net,
  justice.cameron@australiamail.com,
  kai.kennedy@nycmail.com,
  morgan.ellis@contractor.net,
  morgan.kennedy@africamail.com,
  morgan.miller@workmail.com,
  morgan.moore@execs.com,
  parker.quinn@execs.com,
  parker.simmons@californiamail.com,
  payton.carson@europe.com,
  peyton.carter@swissmail.com,
  peyton.davis@workmail.com,
  phoenix.spencer@australiamail.com,
  quinn.gray@contractor.net,
  reese.casey@execs.com,
  reese.jordan@mexicomail.com,
  riley.taylor@contractor.net,
  river.harper@asia.com,
  rowan.hayes@execs.com,
  rowan.james@torontomail.com,
  sage.ellis@europe.com,
  sawyer.reese@dublin.com,
  sawyer.sullivan@nycmail.com,
  skylar.kelly@execs.com,
  sydney.mckenzie@asia.com,
  taylor.blair@asia.com,
  taylor.hughes@execs.com,
  taylor.morgan@contractor.net,
  tyler.walker@mexicomail.com
Return-Path: <ashwilliams012100@gmail.com>
```

I copied and paste it to ChatGPT to count for me how many are they



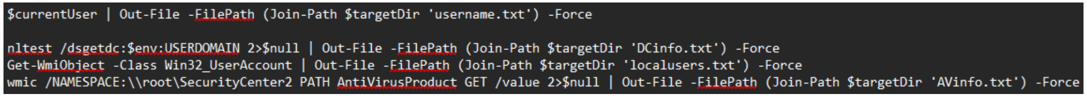
```
48. rowan.hayes@execs.com
49. rowan.james@torontomail
50. sage.ellis@europe.com
51. sawyer.reese@dublin.com
52. sawyer.sullivan@nycmail
53. skylar.kelly@execs.com
54. sydney.mckenzie@asia.co
55. taylor.blair@asia.com
56. taylor.hughes@execs.com
57. taylor.morgan@contracto
58. tyler.walker@mexicomail
```

There are 58 recipients in total.

Answer: 58

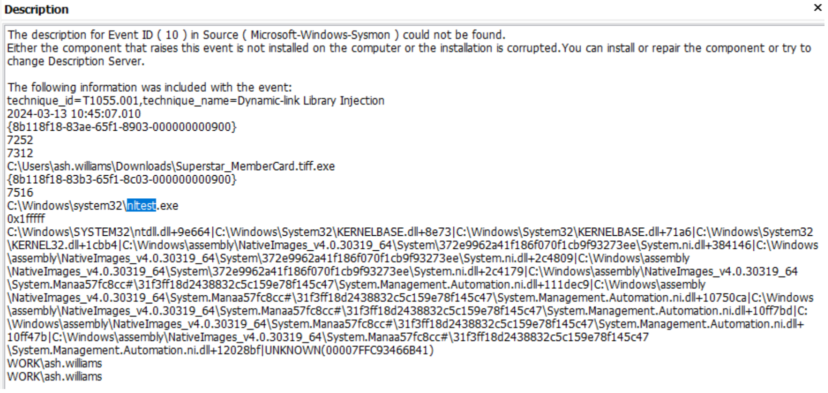
Task 9:
Which legitimate program was utilized to obtain details regarding the domain controller?

This answer I found from the first challenge which called "Heartbreaker-Continuum"
The last challenge was a malware analysis given the same malware. So after analyzed the malware I had the code



```
$currentUser | Out-File -FilePath (Join-Path $targetDir 'username.txt') -Force

nltest /dsgetdc:$env:USERDOMAIN 2>$null | Out-File -FilePath (Join-Path $targetDir 'DCinfo.txt') -Force
Get-WmiObject -Class Win32_UserAccount | Out-File -FilePath (Join-Path $targetDir 'localusers.txt') -Force
wmic /NAMESPACE:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value 2>$null | Out-File -FilePath (Join-Path $targetDir 'AVinfo.txt') -Force
```

Just for the practice, I searched in Sysmon "nltest" without event ID and the results was with event ID10
which is
"Process Access"

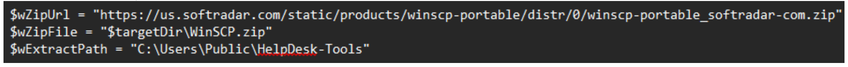


```
The description for Event ID ( 10 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to
change Description Server.

The following information was included with the event:
technique_id=T1055.001,technique_name=Dynamic-link Library Injection
2024-03-13 10:45:07.010
{8b118f18-83ae-65f1-8903-000000000900}
7252
7312
C:\Users\ash.williams\Downloads\Superstar_MemberCard.tiff.exe
{8b118f18-83b3-65f1-8c03-000000000900}
7516
C:\Windows\system32\nltest.exe
0x1fffff
C:\Windows\SYSTEM32\ntdll.dll+9e664|C:\Windows\System32\KERNELBASE.dll+8e73|C:\Windows\System32\KERNELBASE.dll+71a6|C:\Windows\System32
\KERNEL32.dll+1cbb4|C:\Windows\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll+384146|C:\Windows
\assembly\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll+2c4809|C:\Windows\assembly
\NativeImages_v4.0.30319_64\System\372e9962a41f186f070f1cb9f93273ee\System.ni.dll+2c4179|C:\Windows\assembly\NativeImages_v4.0.30319_64
\System.Manaa57fc8cc#\31f3ff18d2438832c5c159e78f145c47\System.Management.Automation.ni.dll+111dec9|C:\Windows\assembly
\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\31f3ff18d2438832c5c159e78f145c47\System.Management.Automation.ni.dll+10750ca|C:\Windows
\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\31f3ff18d2438832c5c159e78f145c47\System.Management.Automation.ni.dll+10ff7bd|C:
\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\31f3ff18d2438832c5c159e78f145c47\System.Management.Automation.ni.dll+
10ff47b|C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\31f3ff18d2438832c5c159e78f145c47
\System.Management.Automation.ni.dll+12028bf|UNKNOWN(00007FFC93466B41)
WORK\ash.williams
WORK\ash.williams
```

Answer: nltest.exe

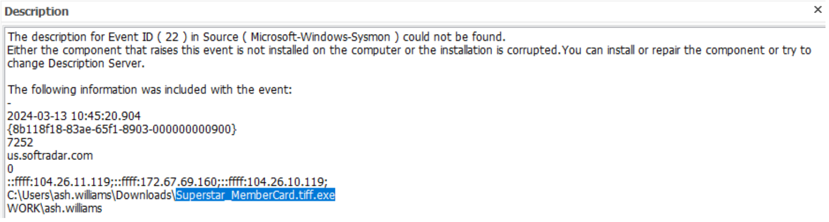
Task 10:
Specify the domain (including sub-domain if applicable) that was used to download the tool for exfiltration.

Same as task 9, I already have the code from the malware



```
$wZipUrl = "https://us.softradar.com/static/products/winscp-portable/distr/0/winscp-portable_softradar-com.zip"
$wZipFile = "$targetDir\WinSCP.zip"
$wExtractPath = "C:\Users\Public\HelpDesk-Tools"
```

Just for the practice, the way to find this answer is to search for event ID 22 in Sysmon which is a DNS Event
I filtered event ID 22 with the name of the binary Superstar_MemberCard.tiff.exe

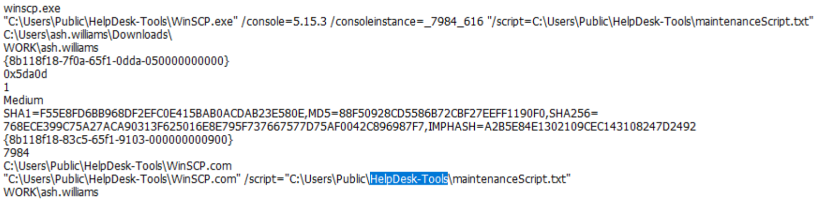


```
The description for Event ID ( 22 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to
change Description Server.

The following information was included with the event:
-
2024-03-13 10:45:20.904
{8b118f18-83ae-65f1-8903-000000000900}
7252
us.softradar.com
0
::ffff:104.26.11.119;::ffff:172.67.69.160;::ffff:104.26.10.119;
C:\Users\ash.williams\Downloads\Superstar_MemberCard.tiff.exe
WORK\ash.williams
```

Answer: us.softradar.com

Task 11:
The threat actor attempted to conceal the tool to elude suspicion. Can you specify the name of the folder used to store and hide the file transfer program?

In the Sysmon event ID 1 I found some path after saw the WinSCP

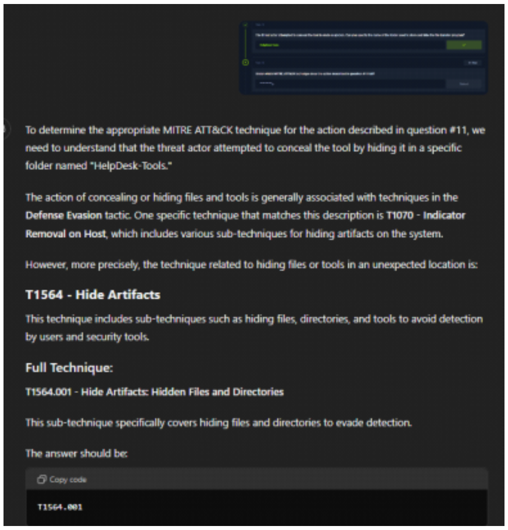


```
winscp.exe
"C:\Users\Public\HelpDesk-Tools\WinSCP.exe" /console=5.15.3 /consoleinstance=_7984_616 "/script=C:\Users\Public\HelpDesk-Tools\maintenanceScript.txt"
C:\Users\ash.williams\Downloads\
WORK\ash.williams
{8b118f18-7f0a-65f1-0dda-050000000000}
0x5da0d
1
Medium
SHA1=F55E8FD6BB968DF2EFC0E415BAB0ACDAB23E580E,MD5=88F50928CD5586B72CBF27EEFF1190F0,SHA256=
768ECE399C75A27ACA90313F625016E8E795F737667577D75AF0042C896987F7,IMPHASH=A2B5E84E1302109CEC143108247D2492
{8b118f18-83c5-65f1-9103-000000000900}
7984
C:\Users\Public\HelpDesk-Tools\WinSCP.com
"C:\Users\Public\HelpDesk-Tools\WinSCP.com" /script="C:\Users\Public\HelpDesk-Tools\maintenanceScript.txt"
WORK\ash.williams
```

Answer: HelpDesk-Tools

Task 12:
Under which MITRE ATT&CK technique does the action described in question #11 fall?

I asked the ChatGPT



To determine the appropriate MITRE ATT&CK technique for the action described in question #11, we need to understand that the threat actor attempted to conceal the tool by hiding it in a specific folder named "HelpDesk-Tools."

The action of concealing or hiding files and tools is generally associated with techniques in the **Defense Evasion** tactic. One specific technique that matches this description is **T1070 - Indicator Removal on Host**, which includes various sub-techniques for hiding artifacts on the system.

However, more precisely, the technique related to hiding files or tools in an unexpected location is:

T1564 - Hide Artifacts

This technique includes sub-techniques such as hiding files, directories, and tools to avoid detection by users and security tools.

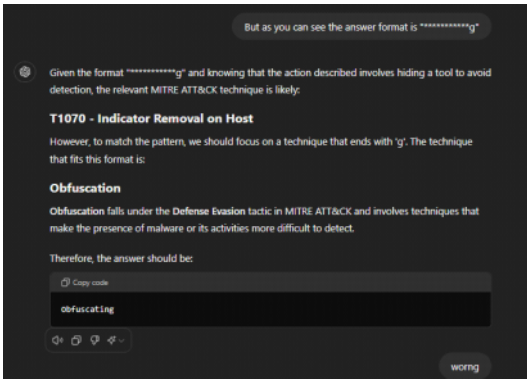
Full Technique:

T1564.001 - Hide Artifacts: Hidden Files and Directories

This sub-technique specifically covers hiding files and directories to evade detection.

The answer should be:

```
T1564.001
```



But as you can see the answer format is "************g"

Given the format "************g" and knowing that the action described involves hiding a tool to avoid detection, the relevant MITRE ATT&CK technique is likely:

T1070 - Indicator Removal on Host

However, to match the pattern, we should focus on a technique that ends with 'g'. The technique that fits this format is:

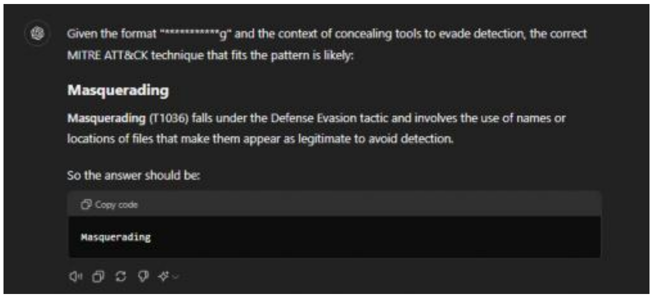
Obfuscation

Obfuscation falls under the **Defense Evasion** tactic in MITRE ATT&CK and involves techniques that make the presence of malware or its activities more difficult to detect.

Therefore, the answer should be:

```
obfuscating
```

worng



Given the format "**********g" and the context of concealing tools to evade detection, the correct MITRE ATT&CK technique that fits the pattern is likely:

Masquerading

Masquerading (T1036) falls under the Defense Evasion tactic and involves the use of names or locations of files that make them appear as legitimate to avoid detection.

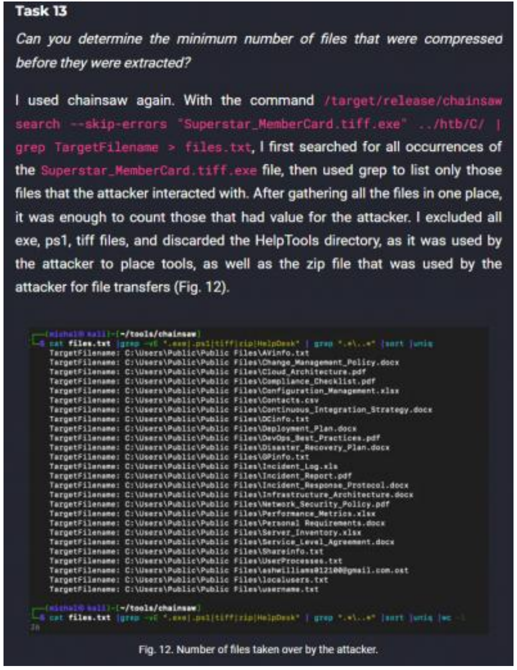
So the answer should be:

```
Masquerading
```

Answer: Masquerading

Task 13:
Can you determine the minimum number of files that were compressed before they were extracted?

I didn't manage to find the answer, I used the Writeup



Task 13

Can you determine the minimum number of files that were compressed before they were extracted?

I used chainsaw again. With the command `/target/release/chainsaw search --skip-errors "Superstar_MemberCard.tiff.exe" ../htb/C/ | grep TargetFilename > files.txt`, I first searched for all occurrences of the `Superstar_MemberCard.tiff.exe` file, then used grep to list only those files that the attacker interacted with. After gathering all the files in one place, it was enough to count those that had value for the attacker. I excluded all exe, ps1, tiff files, and discarded the HelpTools directory, as it was used by the attacker to place tools, as well as the zip file that was used by the attacker for file transfers (Fig. 12).

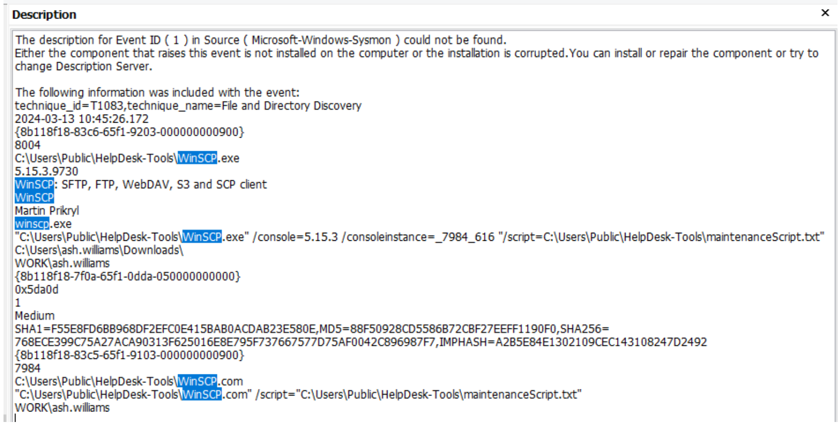
```
┌──(michal㉿kali)-[~/tools/chainsaw]
└─$ cat files.txt |grep -vE ".exe|.ps1|tiff|zip|HelpDesk" | grep ".*\..*" |sort |uniq
    TargetFilename: C:\Users\Public\Public Files\AVinfo.txt
    TargetFilename: C:\Users\Public\Public Files\Change_Management_Policy.docx
    TargetFilename: C:\Users\Public\Public Files\Cloud_Architecture.pdf
    TargetFilename: C:\Users\Public\Public Files\Compliance_Checklist.pdf
    TargetFilename: C:\Users\Public\Public Files\Configuration_Management.xlsx
    TargetFilename: C:\Users\Public\Public Files\Contacts.csv
    TargetFilename: C:\Users\Public\Public Files\Continuous_Integration_Strategy.docx
    TargetFilename: C:\Users\Public\Public Files\DCinfo.txt
    TargetFilename: C:\Users\Public\Public Files\Deployment_Plan.docx
    TargetFilename: C:\Users\Public\Public Files\DevOps_Best_Practices.pdf
    TargetFilename: C:\Users\Public\Public Files\Disaster_Recovery_Plan.docx
    TargetFilename: C:\Users\Public\Public Files\GPinfo.txt
    TargetFilename: C:\Users\Public\Public Files\Incident_Log.xls
    TargetFilename: C:\Users\Public\Public Files\Incident_Report.pdf
    TargetFilename: C:\Users\Public\Public Files\Incident_Response_Protocol.docx
    TargetFilename: C:\Users\Public\Public Files\Infrastructure_Architecture.docx
    TargetFilename: C:\Users\Public\Public Files\Network_Security_Policy.pdf
    TargetFilename: C:\Users\Public\Public Files\Performance_Metrics.xlsx
    TargetFilename: C:\Users\Public\Public Files\Personal Requirements.docx
    TargetFilename: C:\Users\Public\Public Files\Server_Inventory.xlsx
    TargetFilename: C:\Users\Public\Public Files\Service_Level_Agreement.docx
    TargetFilename: C:\Users\Public\Public Files\Shareinfo.txt
    TargetFilename: C:\Users\Public\Public Files\UserProcesses.txt
    TargetFilename: C:\Users\Public\Public Files\ashwilliams012100@gmail.com.ost
    TargetFilename: C:\Users\Public\Public Files\localusers.txt
    TargetFilename: C:\Users\Public\Public Files\username.txt

┌──(michal㉿kali)-[~/tools/chainsaw]
└─$ cat files.txt |grep -vE ".exe|.ps1|tiff|zip|HelpDesk" | grep ".*\..*" |sort |uniq |wc -l
26
```

Fig. 12. Number of files taken over by the attacker.

Answer: 26

Task 14:
To exfiltrate data from the victim's workstation, the binary executed a command. Can you provide the complete command used for this action?

I saw a lot of events related to WinSCP, also from the last challenge when I had the code of the malware.
I searched in Sysmon for WinSCP and found the arguments



```
The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to
change Description Server.

The following information was included with the event:
technique_id=T1083,technique_name=File and Directory Discovery
2024-03-13 10:45:26.172
{8b118f18-83c6-65f1-9203-000000000900}
8004
C:\Users\Public\HelpDesk-Tools\WinSCP.exe
5.15.3.9730
WinSCP: SFTP, FTP, WebDAV, S3 and SCP client
WinSCP
Martin Prikryl
winscp.exe
"C:\Users\Public\HelpDesk-Tools\WinSCP.exe" /console=5.15.3 /consoleinstance=_7984_616 "/script=C:\Users\Public\HelpDesk-Tools\maintenanceScript.txt"
C:\Users\ash.williams\Downloads\
WORK\ash.williams
{8b118f18-7f0a-65f1-0dda-050000000000}
0x5da0d
1
Medium
SHA1=F55E8FD6BB968DF2EFC0E415BAB0ACDAB23E580E,MD5=88F50928CD5586B72CBF27EEFF1190F0,SHA256=
768ECE399C75A27ACA90313F625016E8E795F737667577D75AF0042C896987F7,IMPHASH=A2B5E84E1302109CEC143108247D2492
{8b118f18-83c5-65f1-9103-000000000900}
7984
C:\Users\Public\HelpDesk-Tools\WinSCP.com
"C:\Users\Public\HelpDesk-Tools\WinSCP.com" /script="C:\Users\Public\HelpDesk-Tools\maintenanceScript.txt"
WORK\ash.williams
```

Answer: "C:\Users\Public\HelpDesk-Tools\WinSCP.com" /script="C:\Users\Public\HelpDesk-Tools
\maintenanceScript.txt"