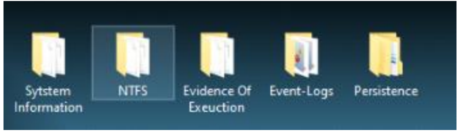
TickTock - Walkthrough

Monday, August 12, 2024 5:29 PM

Story:

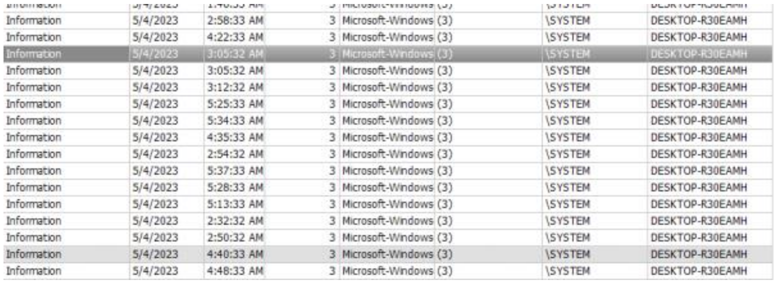
Gladys is a new joiner in the company, she has received an email informing her that the IT department is due to do some work on her PC, she is guided to call the IT team where they will inform her on how to allow them remote access.
The IT team however are actually a group of hackers that are attempting to attack Forela.

- I highly suggesting to split the image to:

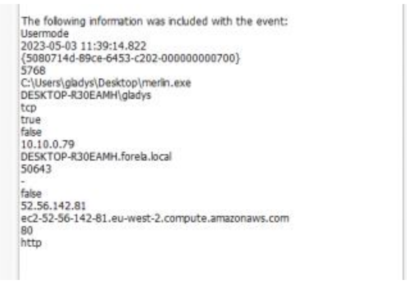


Task1: What was the name of the executable that was uploaded as a C2 Agent?

- I searched Sysmon logs for Event ID 3, which relates to network connections, and found high communication from the user "gladys" to an EC2 address (52.56.142.81) on port 80.
  A suspicious file named "**merlin.exe**" was involved in these communications.



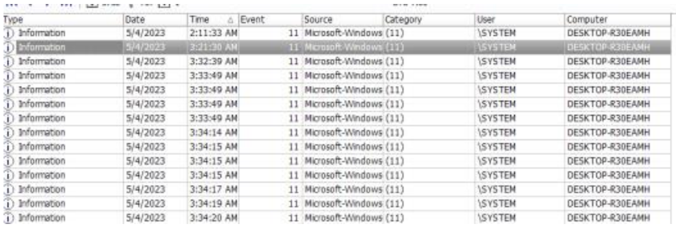
Information	5/4/2023	2:58:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:22:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:05:32 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:05:32 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:12:32 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:25:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:34:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:35:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	2:54:32 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:37:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:28:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:13:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	2:32:32 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	2:50:32 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:40:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:48:33 AM	3	Microsoft-Windows	(3)	\SYSTEM	DESKTOP-R30EAMH



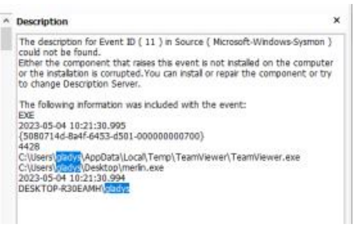
```
The following information was included with the event:
Usermode
2023-05-03 11:39:14.822
{5080714d-89ce-6453-c202-000000000700}
5768
C:\Users\gladys\Desktop\merlin.exe
DESKTOP-R30EAMH\gladys
tcp
true
false
10.10.0.79
DESKTOP-R30EAMH.forela.local
50643
-
false
52.56.142.81
ec2-52-56-142-81.eu-west-2.compute.amazonaws.com
80
http
```

Task2: What was the session id for in the initial access?

- I searched Sysmon logs for Event ID 11, which relates to file creation, and found that the file merlin.exe was created via TeamViewer.exe.



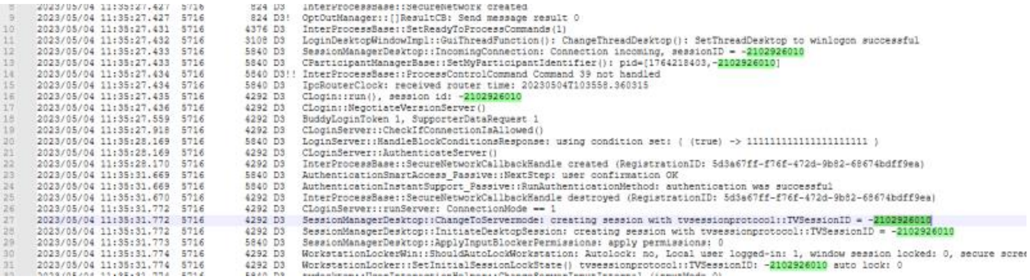
Type	Date	Time	Event	Source	Category	User	Computer
Information	5/4/2023	2:11:33 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:21:30 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:32:39 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:33:49 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:33:49 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:33:49 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:33:49 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:14 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:15 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:15 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:15 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:17 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:19 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:34:20 AM	11	Microsoft-Windows	(11)	\SYSTEM	DESKTOP-R30EAMH



Description

```
The description for Event ID ( 11 ) 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:
EXE
2023-05-04 10:21:30.995
{5080714d-8a4f-6453-d501-000000000700}
4428
C:\Users\gladys\AppData\Local\Temp\TeamViewer\TeamViewer.exe
C:\Users\gladys\Desktop\merlin.exe
2023-05-04 10:21:30.994
DESKTOP-R30EAMH\gladys
```

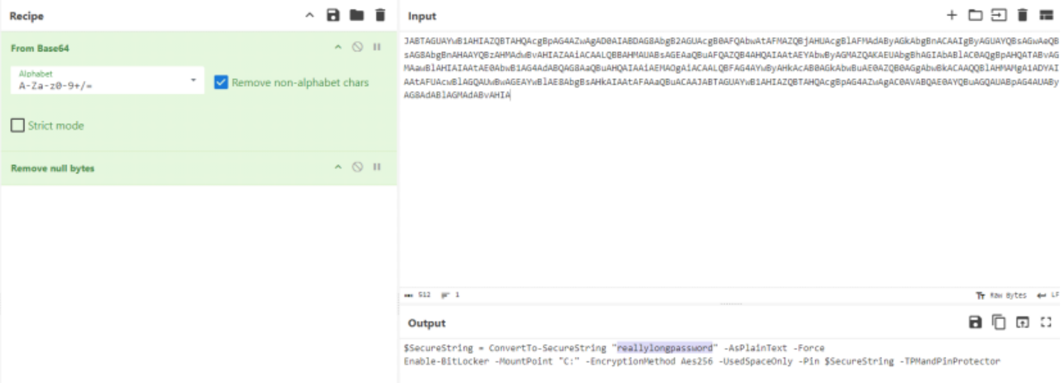
- I accessed to Teamviewer logs which located at 'C:\Users\\Users\gladys\AppData\Local\TeamViewer\Logs'.
  And search for 'session' and found the session ID:



```
2023/05/04 11:35:27.427  5716        824 D3   InterProcessBase::SecureNetwork created
2023/05/04 11:35:27.427  5716        824 D3!  OptOutManager::[]ResultCB: Send message result 0
2023/05/04 11:35:27.431  5716       4376 D3   InterProcessBase::SetReadyToProcessCommands(1)
2023/05/04 11:35:27.432  5716       3108 D3   LoginDesktopWindowImpl::GuiThreadFunction(): ChangeThreadDesktop(): SetThreadDesktop to winlogon successful
2023/05/04 11:35:27.433  5716       5840 D3   SessionManagerDesktop::IncomingConnection: Connection incoming, sessionID = -2102926010
2023/05/04 11:35:27.433  5716       5840 D3   CParticipantManagerBase::SetMyParticipantIdentifier(): pid=[1764218403,-2102926010]
2023/05/04 11:35:27.434  5716       5840 D3!! InterProcessBase::ProcessControlCommand Command 39 not handled
2023/05/04 11:35:27.434  5716       5840 D3   IpcRouterClock: received router time: 20230504T103558.960315
2023/05/04 11:35:27.435  5716       4292 D3   CLogin::run(), session id: -2102926010
2023/05/04 11:35:27.436  5716       4292 D3   CLogin::NegotiateVersionServer()
2023/05/04 11:35:27.559  5716       4292 D3   BuddyLoginToken 1, SupporterDataRequest 1
2023/05/04 11:35:27.918  5716       4292 D3   CLoginServer::CheckIfConnectionIsAllowed()
2023/05/04 11:35:28.169  5716       5840 D3   LoginServer::HandleBlockConditionsResponse: using condition set: ( (true) -> 11111111111111111111 )
2023/05/04 11:35:28.169  5716       4292 D3   CLoginServer::AuthenticateServer()
2023/05/04 11:35:28.170  5716       4292 D3   InterProcessBase::SecureNetworkCallbackHandle created (RegistrationID: 5d3a67ff-f76f-472d-9b82-68674bdff9ea)
2023/05/04 11:35:31.669  5716       5840 D3   AuthenticationSmartAccess_Passive::NextStep: user confirmation OK
2023/05/04 11:35:31.669  5716       5840 D3   AuthenticationInstantSupport_Passive::RunAuthenticationMethod: authentication was successful
2023/05/04 11:35:31.670  5716       4292 D3   InterProcessBase::SecureNetworkCallbackHandle destroyed (RegistrationID: 5d3a67ff-f76f-472d-9b82-68674bdff9ea)
2023/05/04 11:35:31.772  5716       4292 D3   CLoginServer::runServer: ConnectionMode == 1
2023/05/04 11:35:31.772  5716       4292 D3   SessionManagerDesktop::ChangeToServermode: creating session with tvsessionprotocol::TVSessionID = -2102926010
2023/05/04 11:35:31.772  5716       4292 D3   SessionManagerDesktop::InitiateDesktopSession: creating session with tvsessionprotocol::TVSessionID = -2102926010
2023/05/04 11:35:31.773  5716       5840 D3   SessionManagerDesktop::ApplyInputBlockerPermissions: apply permissions: 0
2023/05/04 11:35:31.774  5716       4292 D3   WorkstationLockerWin::ShouldAutoLockWorkstation: Autolock: no, Local user logged-in: 1, window session locked: 0, secure scre
2023/05/04 11:35:31.774  5716       4292 D3   WorkstationLocker::SetInitialSessionLockState() tvsessionprotocol::TVSessionID: -2102926010 auto lock: 0
```

Task3: The attacker attempted to set a bitlocker password on the C: drive what was the password?

- As before, I checked the 'Sysmon' logs and filtered only Event ID - 1 which related to process creation.
  The first log was of Powershell.exe encoded base64 command.
  I decoded it via Cyberchef and found the answer:



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

Remove null bytes

Input

```
JABTAGUAYwB1AHIAZQBTAHQAcgBpAG4AZwAgAD0AIABDAG8AbgB2AGUAcgB0AFQAbwAtAFMAZQBjAHUAcgBlAFMAdAByAGkAbgBnACAAIgByAGUAYQBsAGwAeQB
sAG8AbgBnAHAAYQBzAHMAdwBvAHIAZAAiACAALQBBAHMAUABsAGEAaQBuAFQAZQB4AHQAIAAtAEYAbwByAGMAZQAKAEUAbgBhAGIAbABlAC0AQgBpAHQATABvAG
MAawBlAHIAIAAtAE0AbwB1AG4AdABQAG8AaQBuAHQAIAAiAEMAOgAiACAALQBFAG4AYwByAHkAcAB0AGkAbwBuAE0AZQB0AGgAbwBkACAAQQBlAHMAMgA1ADYAI
AAtAFUAcwBlAGQAUwBwAGEAYwBlAE8AbgBsAHkAIAAtAFAAaQBuACAAJABTAGUAYwB1AHIAZQBTAHQAcgBpAG4AZwAgAC0AVABQAE0AYQBuAGQAUABpAG4AUABy
AG8AdABlAGMAdABvAHIA
```

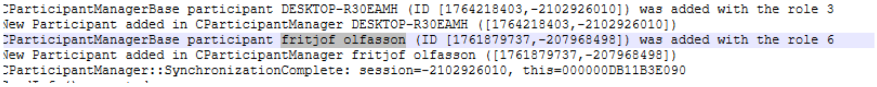
512 1 Raw bytes LF

Output

```
$SecureString = ConvertTo-SecureString "reallylongpassword" -AsPlainText -Force
Enable-BitLocker -MountPoint "C:" -EncryptionMethod Aes256 -UsedSpaceOnly -Pin $SecureString -TPMandPinProtector
```

Task4: What name was used by the attacker?

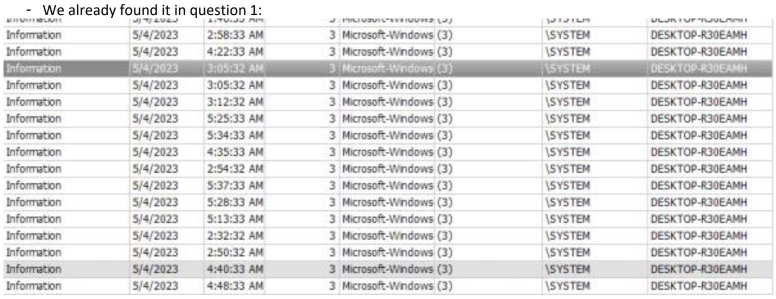
- That was a tricky one! After some time, I eventually found the answer in the TeamViewer logs:



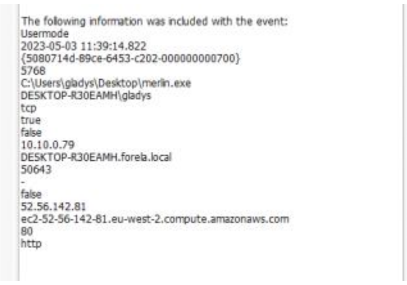
```
CParticipantManagerBase participant DESKTOP-R30EAMH (ID [1764218403,-2102926010]) was added with the role 3
New Participant added in CParticipantManager DESKTOP-R30EAMH ([1764218403,-2102926010])
CParticipantManagerBase participant fritjof olfasson (ID [1761879737,-207968498]) was added with the role 6
New Participant added in CParticipantManager fritjof olfasson ([1761879737,-207968498])
CParticipantManager::SynchronizationComplete: session=-2102926010, this=000000DB11B3E090
```

Task5: What IP address did the C2 connect back to?

- We already found it in question 1:



Information	5/4/2023	2:58:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:22:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:05:32 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:05:32 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	3:12:32 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:25:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:34:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:35:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	2:54:32 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:37:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:28:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	5:13:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	2:32:32 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	2:50:32 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:40:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH
Information	5/4/2023	4:48:33 AM	3	Microsoft-Windows (3)	\SYSTEM	DESKTOP-R30EAMH



```
The following information was included with the event:
Usermode
2023-05-03 11:39:14.822
{5080714d-89ce-6453-c202-000000000700}
5768
C:\Users\gladys\Desktop\merlin.exe
DESKTOP-R30EAMH\gladys
tcp
true
false
10.10.0.79
DESKTOP-R30EAMH.forela.local
50643
-
false
52.56.142.81
ec2-52-56-142-81.eu-west-2.compute.amazonaws.com
80
http
```

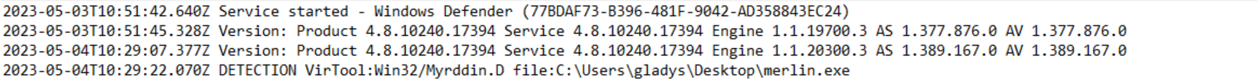
Task6: What category did Windows Defender give to the C2 binary file?

When I split the image into parts, I found the Defender logs identified by the name **MPDetection-05032023-114843.log.**
The real location of this Defender log file is typically:

'C:\ProgramData\Microsoft\Windows Defender\Platform\<version>\'

-

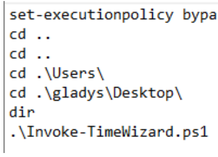
I found the answer there:



```
2023-05-03T10:51:42.640Z Service started - Windows Defender (77BDAF73-B396-481F-9042-AD358843EC24)
2023-05-03T10:51:45.328Z Version: Product 4.8.10240.17394 Service 4.8.10240.17394 Engine 1.1.19700.3 AS 1.377.876.0 AV 1.377.876.0
2023-05-04T10:29:07.377Z Version: Product 4.8.10240.17394 Service 4.8.10240.17394 Engine 1.1.20300.3 AS 1.389.167.0 AV 1.389.167.0
2023-05-04T10:29:22.070Z DETECTION VirTool:Win32/Myrddin.D file:C:\Users\gladys\Desktop\merlin.exe
```

Task7: What was the filename of the powershell script the attackers used to manipulate time?

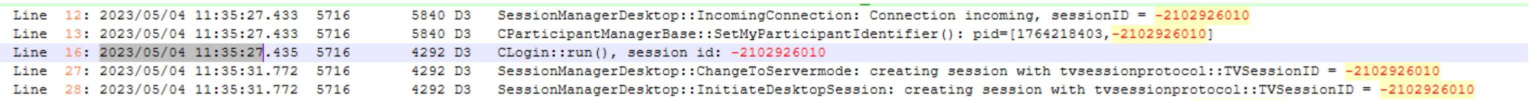
- For this question we should check the Powershell history file, which found in 'C:\Users\gladys\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline'
  You can open the file via notepad and find the answer:



```
set-executionpolicy bypass
cd ..
cd ..
cd .\Users\
cd .\gladys\Desktop\
dir
.\Invoke-TimeWizard.ps1
```

Task8: What time did the initial access connection start?

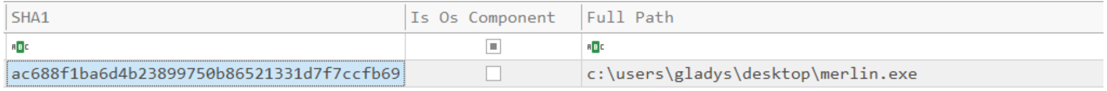
- Found the answer via the session ID we found earlier:



```
Line  12: 2023/05/04 11:35:27.433  5716         5840 D3   SessionManagerDesktop::IncomingConnection: Connection incoming, sessionID = -2102926010
Line  13: 2023/05/04 11:35:27.433  5716         5840 D3   CParticipantManagerBase::SetMyParticipantIdentifier(): pid=[1764218403,-2102926010]
Line  16: 2023/05/04 11:35:27.435  5716         4292 D3   CLogin::run(), session id: -2102926010
Line  27: 2023/05/04 11:35:31.772  5716         4292 D3   SessionManagerDesktop::ChangeToServermode: creating session with tvsessionprotocol::TVSessionID = -2102926010
Line  28: 2023/05/04 11:35:31.772  5716         4292 D3   SessionManagerDesktop::InitiateDesktopSession: creating session with tvsessionprotocol::TVSessionID = -2102926010
```

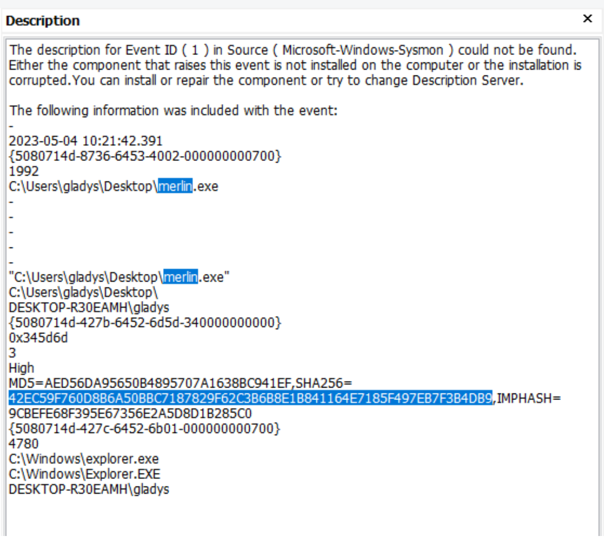
Task9: What is the SHA1 and SHA2 sum of the malicious binary?

- **I found the SHA1 of the process with 'AmacheParser.exe':**



SHA1	Is Os Component	Full Path
	■	
ac688f1ba6d4b23899750b86521331d7f7ccfb69	☐	c:\users\gladys\desktop\merlin.exe

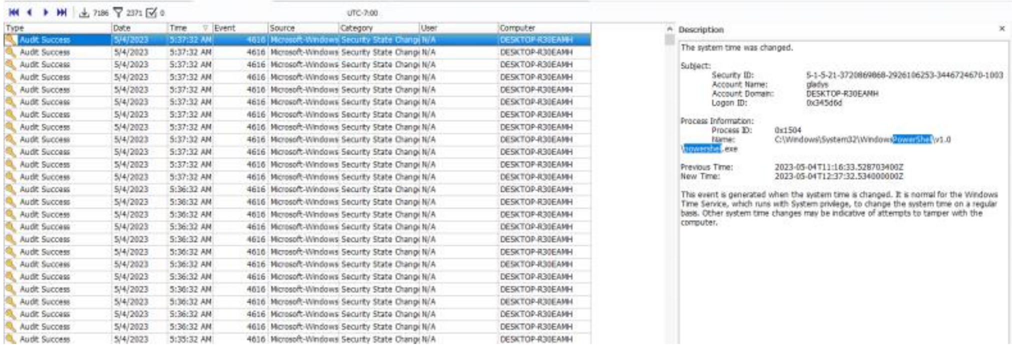
- **The SHA256 I found via 'Sysmon' Logs:**



```
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:

-
2023-05-04 10:21:42.391
{5080714d-8736-6453-4002-000000000700}
1992
C:\Users\gladys\Desktop\merlin.exe
-
-
-
-
-
"C:\Users\gladys\Desktop\merlin.exe"
C:\Users\gladys\Desktop\
DESKTOP-R30EAMH\gladys
{5080714d-427b-6452-6d5d-340000000000}
0x345d6d
3
High
MD5=AED56DA95650B4895707A1638BC941EF,SHA256=
42EC59F760D8B6A50BBC7187829F62C3B6B8E1B841164E7185F497EB7F3B4DB9,IMPHASH=
9CBEFE68F395E67356E2A5D8D1B285C0
{5080714d-427c-6452-6b01-000000000700}
4780
C:\Windows\explorer.exe
C:\Windows\Explorer.EXE
DESKTOP-R30EAMH\gladys
```

Task10: How many times did the PowerShell script change the time on the machine?

- To investigate how many times the PowerShell script changed the time on the machine, focus on security logs with Event ID 4616.
  This event indicates when the system time was changed, showing the old and new system times, the user who made the change, and the program used.
  Filter these events to look specifically for PowerShell activity.

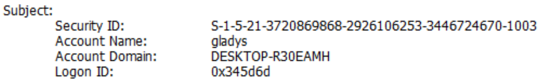


Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:37:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:36:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH
Audit Success	5/4/2023	5:35:32 AM	4616	Microsoft-Windows	Security State Chang	N/A	DESKTOP-R30EAMH

```
The system time was changed.

Subject:
        Security ID:            S-1-5-21-3720869868-2926106253-3446724670-1003
        Account Name:           gladys
        Account Domain:         DESKTOP-R30EAMH
        Logon ID:               0x345d6d

Process Information:
        Process ID:     0x1504
        Name:           C:\Windows\System32\WindowsPowerShell\v1.0
\powershell.exe

Previous Time:          2023-05-04T11:16:33.528703400Z
New Time:               2023-05-04T12:37:32.534000000Z

This event is generated when the system time is changed. It is normal for the Windows
Time Service, which runs with System privilege, to change the system time on a regular
basis. Other system time changes may be indicative of attempts to tamper with the
computer.
```

Task11: What is the SID of the victim user?

- **We can see it almost in every log:**



```
Subject:
        Security ID:            S-1-5-21-3720869868-2926106253-3446724670-1003
        Account Name:           gladys
        Account Domain:         DESKTOP-R30EAMH
        Logon ID:               0x345d6d
```

-