TickTock Challenge

Sherlock Scenario
Gladys is a new joiner in the company, she has recieved 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.

Task 1:
What was the name of the executable that was uploaded as a C2 Agent?

I checked the user gladys files and found TeamViewer which I assumed maybe the hackers use to gain the initial access
I found the TeamViewer15_Logfile.log and opened it and searched for .exe

```
2023/05/04 11:21:30.830  4428       4688 G3   tvnetwork::StreamManagerInternals::ReadStreamParameters: type=6 (StreamType_File,
2023/05/04 11:21:30.996  4428       6012 G3   Write file C:\Users\gladys\Desktop\merlin.exe
2023/05/04 11:21:34.398  4428       6012 G3   Download from "merlin.exe" to "C:\Users\gladys\Desktop\merlin.exe" (10.95 MB)
```

Answer: merlin.exe

Task 2:
What was the session id for in the initial access?

While checking the logs inside the TeamViewer15_Logfile.log I found the session id

TeamViewer15_Logfile.log

```
2023/05/04 11:35:27.303  5716       2436 D3   SettingsIPCReception receive a SYNCHRONISE Settings command : UserSettings
2023/05/04 11:35:27.303  5716       2436 D3   IpcRemoteSettingsHandler::HandleCommand UserSettings process sends sync settings response to network.
2023/05/04 11:35:27.304  5716       5840 D3   Received Control_InitIPC_Response processtype=1
2023/05/04 11:35:27.305  5716       5840 D3   Received Control_InitIPC_Response runningProcesses=7
2023/05/04 11:35:27.309  5716       2436 D3   Received Control_InitIPC_Response processtype=2
2023/05/04 11:35:27.309  5716       2436 D3   IPCConnection: all processes 7 completely initialized
2023/05/04 11:35:27.313  5716        824 D3   InterProcessBase::ConnectToOtherProcess: Process connected to service.
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: 20230504T103558.360315
2023/05/04 11:35:27.435  5716       4292 D3   CLogin::run(), session id: -2102926010
```

Answer: -2102926010

Task 3:
The attacker attempted to set a BitLocker password on the C: drive what was the password?

I checked the Sysmon logs and found Base64

Description

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 09:56:32.836
{5080714d-8150-6453-0d03-000000000700}
3804
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.10240.16384 (th1.150709-1700)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -e
JABTAGUAYwB1AHIAZQBTAHQAcgBpAG4AZwAgAD0AIABDAG8AbgB2AGUAcgB0AFQAbwAtAFMAZQBjAHUAcgBlAFMAdAByAGkAbgBnACAAIgByAGUAYQBsAGwAeQBsAG8AbgBnAHAAYQBzAHMAdwBvAHIAZAAiACAALQBBAHMAUABsAGEAaQBuAFQAZQB4AHQAIAAtAEYAbwByAGMAZQAKAEUAbgBhAGIAbABlAC0AQgBpAHQATABvAGMAawBlAHIAIAAtAE0AbwB1AG4AdABQAG8AaQBuAHQAIAAiAEMAOgAiACAALQBFAG4AYwByAHkAcAB0AGkAbwBuAE0AZQB0AGgAbwBkAC AAQQBlAHMAMgA1ADYAIAAtAFUAcwBlAGQAUwBwAGEAYwBlAEEAbgBsAHkAIAAtAFAAaQBuACAAJABTAGUAYwB1AHIAZQBTAHQAcgBpAG4AZwAgAC0AVA VABQAE0AYQBuAGQAUABpAG4AUAByAG8AdABlAGMAdABvAHIA
C:\Users\gladys\Desktop\
DESKTOP-R30EAMH\gladys
{5080714d-427b-6452-6d5d-340000000000}
0x345d6d
3
High
MD5=190E6E0CDBEF529941D9E5F8F979F5D9,SHA256=8787D4B624880012ABDB442532BE762DB0361DECE169FEF9E1E877A9DF9E00CB,IMPHASH=44B4867FED7460EEC45FBEE7804BB612
{00000000-0000-0000-0000-000000000000}

Decode from Base64 format

Simply enter your data then push the decode button.

```
JABTAGUAYwB1AHIAZQBTAHQAcgBpAG4AZwAgAD0AIABDAG8AbgB2AGUAcgB0AFQAbwAtAFMAZQBjAHUAcgBlAFMAdAByAGkAbgBnACAAIgByAGUAYQBsAGwAeQBsAG8AbgBnAHAAYQBzAHMAdwBvAHIAZAAiACAALQBBAHMAUABsAGEAaQBuAFQAZQB4AHQAIAAtAEYAbwByAGMAZQAKAEUAbgBhAGIAbABlAC0AQgBpAHQATABvAGMAawBlAHIAIAAtAE0AbwB1AG4AdABQAG8AaQBuAHQAIAAiAEMAOgAiACAALQBFAG4AYwByAHkAcAB0AGkAbwBuAE0AZQB0AGgAbwBkAC AAQQBlAHMAMgA1ADYAIAAtAFUAcwBlAGQAUwBwAGEAYwBlAEEAbgBsAHkAIAAtAFAAaQBuACAAJABTAGUAYwB1AHIAZQBTAHQAcgBpAG4AZwAgAC0AVA VABQAE0AYQBuAGQAUABpAG4AUAByAG8AdABlAGMAdABvAHIA
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

AUTO-DETECT — Source character set. Detected: UTF-16LE

Decode each line separately (useful for when you have multiple entries).

Live mode OFF — Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE — Decodes your data into the area below.

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

Answer: reallylongpassword

Task 4:
What name was used by the attacker?

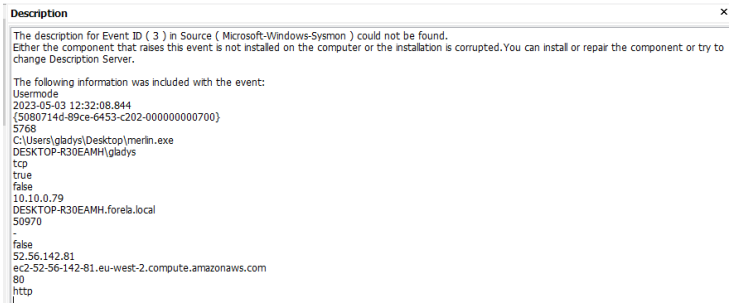
Checking the TeamViewer logs, I found the name next to a "participant"

```
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])
```

Answer: fritjof olfasson

Task 5:
What IP address did the C2 connect back to?

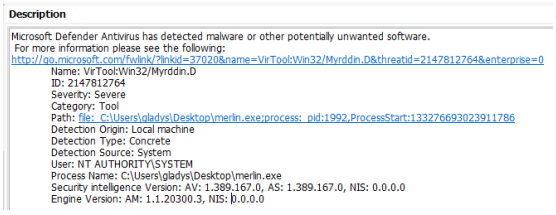
I Searched the Sysmon logs for event ID 3



Answer: 52.56.142.81

Task 6:
What category did Windows Defender give to the C2 binary file?

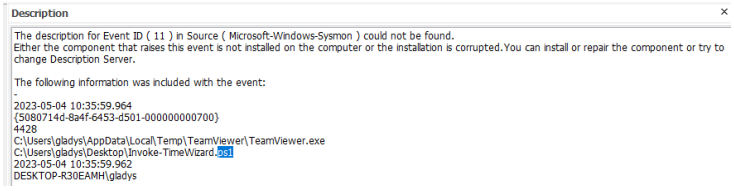
I checked the Windows Defender logs and checked the event ID 1116



Answer: VirTool:Win32/Myrddin.D

Task 7:
What was the filename of the powershell script the attackers used to manipulate time?

I checked the Sysmon logs and searched for ps1



Answer: Invoke-TimeWizard.ps1

Task 8:
What time did the initial access connection start?

I found it on the same answer from task 2 with the session id

```
2023/05/04 11:35:27.435  5716        4292 D3   CLogin::run(), session id: -2102926010
```

Answer: 2023/05/04 11:35:27

Task 9:
What is the SHA1 and SHA2 sum of the malicious binary?

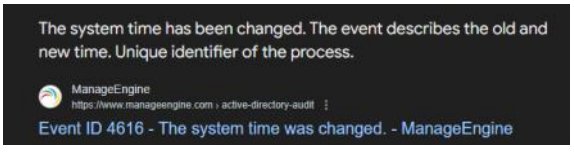
Checking Windows Defender logs from ProgramData "C:\Users\Bubble\Desktop\Collection\C\ProgramData\Microsoft\Windows Defender\Support" file "MPLog-07102015-052145.log"

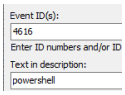
```
30041    SDN:Issuing SDN query for \\?\C:\Users\gladys\Desktop\merlin.exe (\\?\C:\Users\gladys\Desktop\merlin.exe) (sha1=ac688f1ba6d4b23899750b86521331d7f7ccfb69, sha2=42ec59f760d8b6a50bbc7187829f62c3b6b8e1b841164e7185f497eb7f3b4db9)
30042    SDN:SDN query completed: 00000000
```

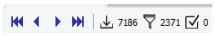
Answer:
ac688f1ba6d4b23899750b86521331d7f7ccfb69:42ec59f760d8b6a50bbc7187829f62c3b6b8e1b841164e
7185f497eb7f3b4db9

Task 10:
How many times did the powershell script change the time on the machine?

I searched the security logs for event ID 4616 and filtered for only powershell process







Answer: 2371

Task 11:
What is the SID of the victim user?

Saw it from the Sysmon logs

Answer: S-1-5-21-3720869868-2926106253-3446724670-1003