Scenario

Ben was working very hard at FaanG industries to get a maximum percentage of the hike. He was talking about this with his HR as well. While he was preparing for a Salary Negotiation meeting, Ben received a phishing email and an attachment explaining to him a New Salary Negotiation process at the company. This resulted in the theft of the super-secret Database credentials of Ben. Necessary remediation steps were taken to reduce the damage. CISO advised the security team to study Ben's case, analyze the Evidence and prepare an Awareness workshop with technical details of the attack. Evidence and the necessary analysis tools were placed on the Desktop. Note: If prompted for Admin Privileges choose BTLOPlayer account.

Used Tools

- **Kernel EML Viewer:** Used to open the original phishing file and inspect its headers.
- **Noriben:** This is a python script that works with h Sysinternals Procmon to automatically collect, analyze, and report on runtime indicators of malware. In a nutshell, it iit allows you to run an applications, hit a keypress, and get a simple text report of the sample's activities. It can be downloaded in the following Github repository.

Questions

Q1) Submit the subject line of the phishing email (Format: Subject String)

The first question requieres us to open the SalaryRenegotiation.eml file that Ben has received and it is in the CollectedEvidence folder in the desktop with Kernel EML Viewer. So we can see the Subject is **Salary Renegotiations**.

Q2) Submit the FROM and TO addresses of the phishing email (Format: FromMailbox@domain.tld, ToMailbox@domain.tld)

We have to check the headers of the email next to the subject one, specifically the **FROM** and **TO**
headers. So the **FROM address** is: HR_Engineer@faang.com and the **TO address** is

Ben_Engineer@faang.com. So as we can see, the attacker created a phishing email where he stole the identity of someone inside the same organization as Ben.

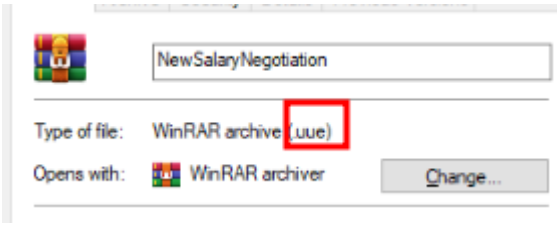
Q3) Submit the download link observed in the email attachment (Format: https://www.domain.tld/path/something)

So, to get this answer we need to open the PDF attached file. This file is in the CollectedEvidence folder and we have to open it with Adobe Acrobat. By positioning on top of the Download button we can get the URL. So the link is: **hxxps://www.dropbox[.]com/s/3dqft1ays1ltgrg/NewSalaryNegotiation.uue?dl=1**.

The link has been sanitized to avoid missclicks.

Q4) Submit the extension of the file that will be downloaded when the malicious link is clicked (format: .extension)

In the CollectedEvidence folder we can check the downloaded file. So for obtaining its extension we need to right click the file, open its properties and in the Type of file filed we can check that the extension is **.uue**

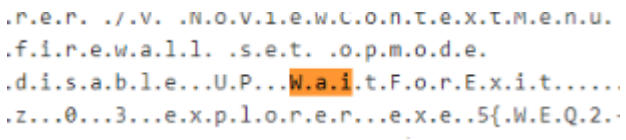


Q5) Submit the Mutex used by the malware sample (Format: {mutex})

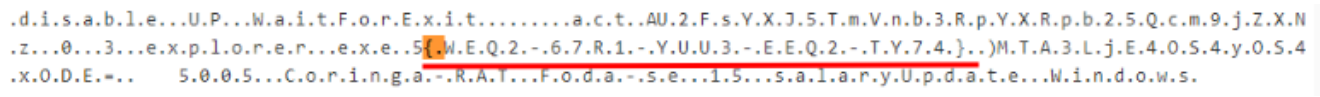
The term "mutex" typically stands for "mutual exclusion," which is a programming concept used to prevent multiple threads or processes from simultaneously accessing or modifying a shared resource. It's a synchronization mechanism used to avoid data corruption and race conditions in software.

In the context of malware or malicious files, the term "mutex" can have a different meaning. Some malware may use a mutex as a technique to ensure that only one instance of the malware runs on a system at a time. This can be used to maintain the malware's persistence on the infected system and avoid duplication.

So to obtain the mutex we must read the .exe file. To do so I have uploaded it into Cyberchef and I have filtered by the {} characters. In there I have found the WaitForExit string, which can reference a Mutex.



Now we need to search for the string used as mutex. To do so, we need to just follow the code and we will see that the value is **{WEQ2-67R1-YUU3-EEQ2-TY74}**.



Q6) The malware replicated itself in two locations to maintain persistence. Submit both locations according to the timeline - so submit the first file then the second file (Format: C:\path\file.ext, C:\path\file.ext)

For this question and the following, we must execute Noriben, so we open a Powershell terminal and we navigate to the following path: **C:\Users\BTLOTest\Desktop\Tools\Noriben-master** to then execute Noriben with **.\Noriben.py**

So, we descompress the malicious file and proceed to execute it. We can see that the decompressed file is an executable disguised as a PDF file. The file is using a double extension .pdf.exe, to confuse a inexpert user.

We execute the malware and let it run for some minutes (5 minutes aprox) to then hit CTRL+C. During this execution, I have been typing some characters into a Notepad since we know the malware has a keylogger behavior. So maybe, by typing some files storing the content will be generated.

First of all, we can see that the malware generates a file with path equal to **C:\Users\BTLOTest\AppData\Local\Microsoft\Windows\History\salaryhike\explorer.exe** .

Then, we can see that this second file has created anothe file with path **C:\Users\BTLOTest\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe**.

So these are the two generated persistence files.

```
File Activity:
==================
[DeleteFile] svchost.exe:6096 > %LocalAppData%\BIT1B72.tmp
[CreateFile] SalaryNegotiationProcess.pdf.exe:2120 > %LocalAppData%\Microsoft\Windows\History\salaryhike\explorer.exe
[CreateFile] SalaryNegotiationProcess.pdf.exe:2120 > %LocalAppData%\Microsoft\Windows\History\salaryhike\explorer.exe
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe
```

Q7) Name of the file created by the malware sample to store recorded keystrokes from the victim machine (Format: filename.extension)

We can highlight the events that have happened inside the Procmon GUI. So I have highlighted the CreateFile Event and I have checked some of them. We can see that the file with path **C:\Users\BTLOTest\AppData\Local\Microsoft\Windows\History\salaryhike\explorer.exe.tmp** has been created by the malware and it is being writeen by it. So we suppose that it is the file storing the keystrokes.

```
[CreateFile] SalaryNegotiationProcess.pdf.exe:2120 > %LocalAppData%\Microsoft\Windows\History\salaryhike\explorer.exe   [SHA256: 7908d484c4600c21ae791fe6751b005cdb1cb744239f9222c43bb418a58f676f]
[CreateFile] SalaryNegotiationProcess.pdf.exe:2120 > %LocalAppData%\Microsoft\Windows\History\salaryhike\explorer.exe   [SHA256: 7908d484c4600c21ae791fe6751b005cdb1cb744239f9222c43bb418a58f676f]
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe   [SHA256: 7908d484c4600c21ae791fe6751b005cdb1cb744239f9222c43bb418a58f676f]
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe   [SHA256: 7908d484c4600c21ae791fe6751b005cdb1cb744239f9222c43bb418a58f676f]
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe   [SHA256: 7908d484c4600c21ae791fe6751b005cdb1cb744239f9222c43bb418a58f676f]
[CreateFile] explorer.exe:6736 > %LocalAppData%\Microsoft\Windows\History\salaryhike\explorer.exe.tmp   [SHA256: 3549dba8034b128b46d1ed560cfe762435c77a380e39ef458882cddc2bf92784]
[CreateFile] explorer.exe:6736 > %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe   [SHA256: 7908d484c4600c21ae791fe6751b005cdb1cb744239f9222c43bb418a58f676f]
[CreateFile] explorer.exe:6736 > %LocalAppData%\Microsoft\Windows\History\salaryhike\explorer.exe.tmp   [SHA256: 3549dba8034b128b46d1ed560cfe762435c77a380e39ef458882cddc2bf92784]
```

Q8) Submit the command-and-control server IP address, and the port used for communication (Format: X.X.X.X:Port)

Finally, to obtain the IP address of the C2 server we need to execute the netstat command in a powershell. The netstat command returns the actual ongoing connections of the system. So as we can see, we have two connections where SYN flag was sent to initiate a connection.

```
PS C:\Users\BTLOTest> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.3.158:443         ip-10-0-16-156:28860   ESTABLISHED
  TCP    10.0.3.158:49700       52.94.56.191:https     ESTABLISHED
  TCP    10.0.3.158:50182       52.94.56.140:https     SYN_SENT
  TCP    10.0.3.158:50183       107.189.29.181:5005    SYN_SENT
  TCP    127.0.0.1:5900         EC2AMAZ-UUEMPAU:50160  ESTABLISHED
  TCP    127.0.0.1:50160        EC2AMAZ-UUEMPAU:5900   ESTABLISHED
PS C:\Users\BTLOTest>
```

The first one is to the port 443 of the IP 52.94.56.140 which is Amazon property. While the second one is 107.189.29.181 and using port 50160. This is a quite suspicious port and the

IP is marked as malware in the main malware platforms. So the answer is **107.189.29.181:50160**.