

Un mal-where très malware

Analyse du Malware de Lancelot Vanrullen, Marc
Lichtner et Baptiste Sibellas

Par Ely Marthouret, Ewan Decima et Garance Frolla



Sommaire

Les strings
Les effets indésirables
Les debuggers
Les affichages de echo
VirtualProtect
Target Hash
Conclusion

Les strings

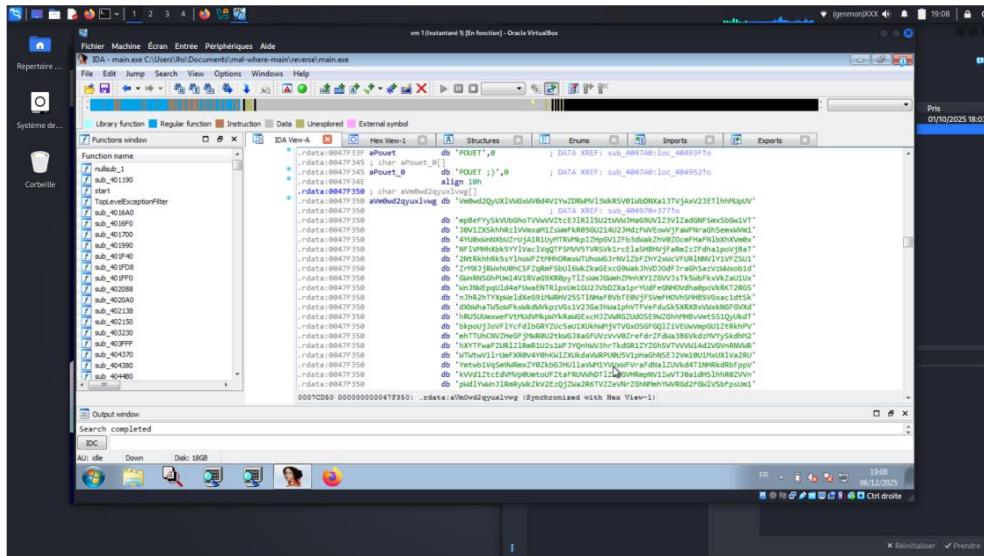
Localisation: 0047F350

Cette longue chaîne de caractères semble être une chaîne encodée en base64 car sa longueur est un multiple de 4 et termine par ==.

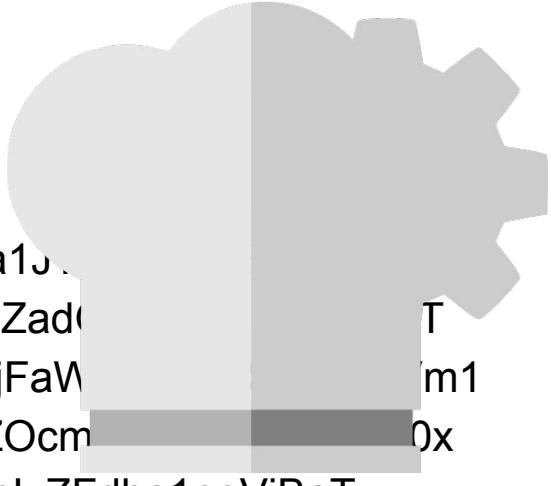
Les strings

Localisation: 0047F350

Cette longue chaîne de caractère semble être une chaîne encodée en base64 car sa longueur est un multiple de 4 et termine par ==.



Strings



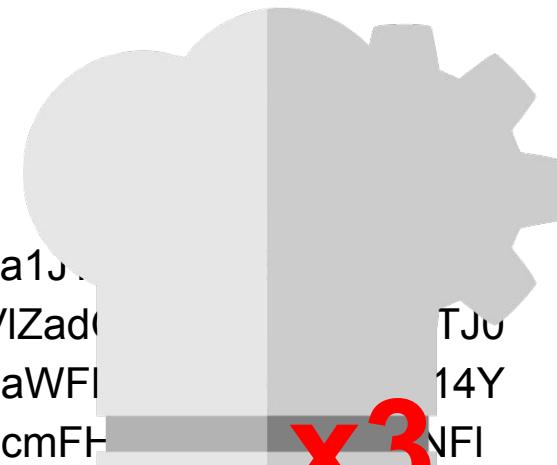
```
Vm0wd2QyUXIVWGxWV0d4V1YwZDRWMVI3WkRSV01WbDNXa1j .  
VmpBeFYySkVUbGhoTVVwVVZtcEJIRII5U2tWWJHaG9UVIZ3VIZad0  
J0V1ZXSkhhRzIVVmxaM1ZsWmFkR05GU214U2JHdzFWVEowVjFaW  
4YU0xWnNXbUZrUjA1R1UyMTRVMkpIZHpGV1ZFb3dWakZhV0ZOcm  
NFIVMHhXbk5YYIVaclVqQTFSMVV5TVRSVk1rcElaSHBHVjFaRmlzZF  
dha1poVjBaT  
2NtRkhhRk5sYIhoWFZtMHhORmxWTUhoWGJrNVIZbFZhY2xWcVF  
URINNVIY1VFZSU1  
ZrMXJjRWxhU0hCSFZqRmFSbUI6WkZkaGExcG9WakJhVDJOdF  
JraGhSazVzWWxob1d  
GWnRNSGhPUm14V1RVaG9XR0pyTIzsWmJG  
WmhZMnhXY1ZGVVJsTk5WbFkxV  
kZaU1  
UxWnJNWEpqUld4aFUwaENTRIpxUm1GU2JVbDZ  
Xa1prYUdFeGNHOV  
dha0poV  
kRKT2R  
GSnJhR2hTYXpW  
eIdXeG9iMWRHV25STINHaFBVbTE0VjFSVmFHOV  
hSMHB5VG  
xac1dtS  
kdXbWhaTW5oWFkxW  
kdWVkpzVGs1V2JGa3hWa1phV  
TFVeFduSk5XRXBxV  
Wxk [...]
```

Strings

Vm0wd2QyUXIVWGxWV0d4V1YwZDRWMVI3WkRSV01WbDNXa1J...
VmpBeFYySkVUbGhoTVVwVVZtcEJIRII5U2tWWJHaG9UVIZ3VIZad...
V1ZXSkhhRzlVVmxAM1ZsWmFkR05GU214U2JHdzFWVEowVjFaWF...
U0xWnNXbUZrUjA1R1UyMTRVMkpIZHpGV1ZFb3dWakZhV0ZOcmFH...
VMHhXbk5YYIVaclVqQTFSMVV5TVRSVk1rcElaSHBVjFaRmlzZFdh...
a1poVjBaT2NtRkhhR
k5sYIhoWFZtMHhORmxWTUhoWGJrNVIZbFZhY2xWcVFURINNVIY1VFZSU1ZrMXJjRWxh
U0hCSFZqRmFSbUI6WkZkaGExcG9WakJhVDJOdFJraGhSazVzWWxob1dGWnRNSGhPU
m14V1RVaG9XR0pyTlZsWmJGWhZMnhXY1ZGVVJsTk5WbFkxVkJzaU1UxWnJNWEpqUl
d [...] 

Strings

Vm0wd2QyUXIVWGxWV0d4V1YwZDRWMVI3WkRSV01WbDNXa1J...
VmpBeFYySkVUbGhoTVVwVVZtcEJIRII5U2tWWJHaG9UVIZ3VIZad...
V1ZXSkhhRzlVVmxAM1ZsWmFkR05GU214U2JHdzFWVEowVjFaWF...
U0xWnNXbUZrUjA1R1UyMTRVMkpIZHpGV1ZFb3dWakZhV0ZOcmFH...
VMHhXbk5YYIVaclVqQTFSMVV5TVRSVk1rcElaSHBVjFaRmlzZFdh...
a1poVjBaT2NtRkhhR
k5sYIhoWFZtMHhORmxWTUhoWGJrNVIZbFZhY2xWcVFURINNVIY1VFZSU1ZrMXJjRW
[...]



TJu
14Y
NFI
X3

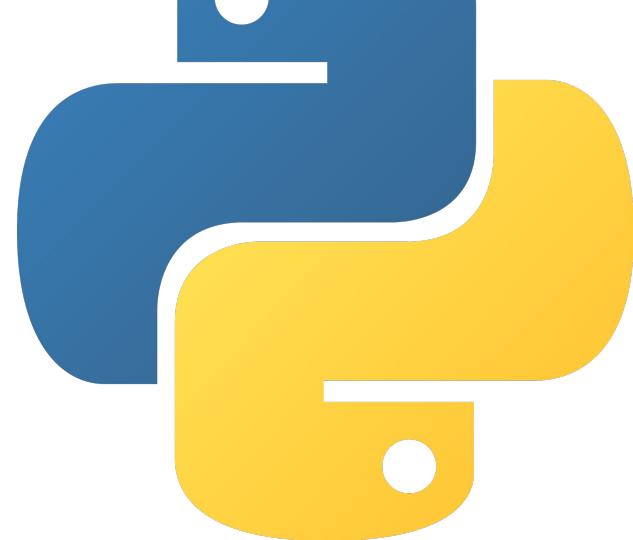
Strings

for loop + entropy +



Strings

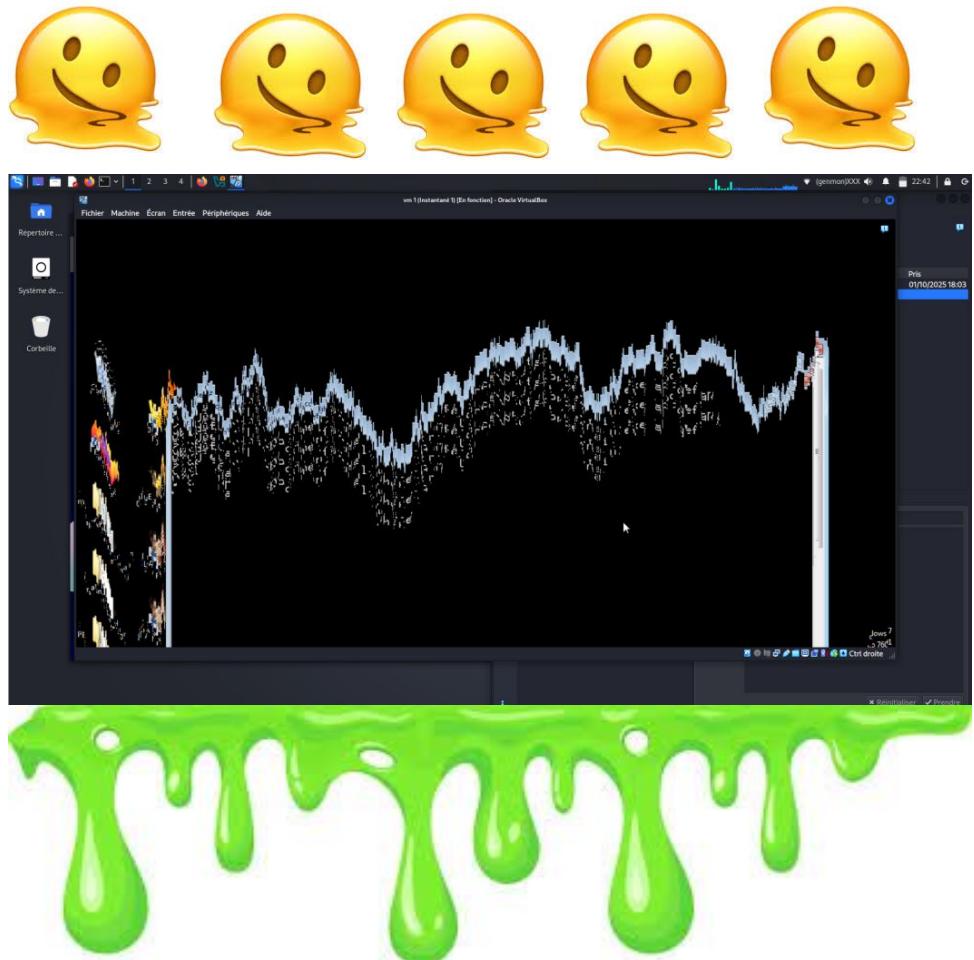
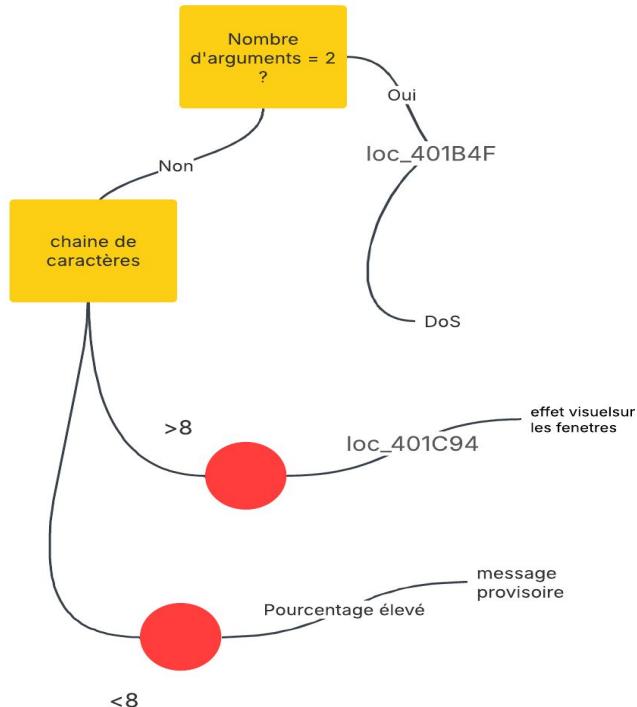
for loop + entropy +



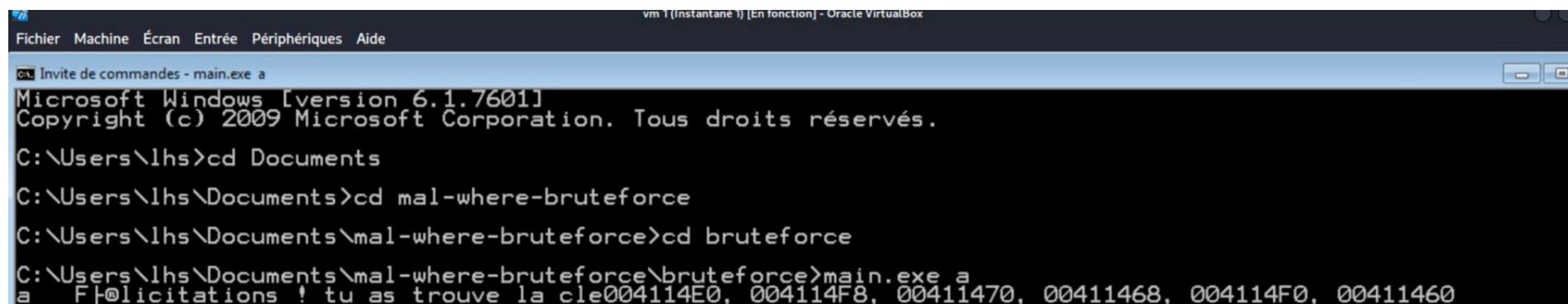
= Hop là on n'oublie pas de s'amuser

Les effets indésirables

Localisation: 0x00401BAF, 0x004019EA



Les affichages d'écho



Fichier Machine Écran Entrée Périphériques Aide

cmd Invite de commandes - main.exe a

Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\lhs>cd Documents

C:\Users\lhs\Documents>cd mal-where-bruteforce

C:\Users\lhs\Documents\mal-where-bruteforce>cd bruteforce

C:\Users\lhs\Documents\mal-where-bruteforce\bruteforce>main.exe a
a F@licitations ! tu as trouve la cle004114E0, 004114F8, 00411470, 00411468, 004114F0, 00411460

ht (c) 2009 Microsoft Corporation. Tous droits réservés.

s\lhs>cd Documents

s\lhs\Documents>cd mal-where-bruteforce

s\lhs\Documents\mal-where-bruteforce>cd bruteforce

s\lhs\Documents\mal-where-bruteforce\bruteforce>main.exe a
licitations ! tu as trouve la cle 004114E0, 004114F8, 00411470, 00411468, 004114F0, 0

strlen

free

malloc

memcpy

loc_4114F8

printf



Petit prince

Deadcode

if (10 - 5 < 0) : print

(



)

IsDebuggerPresent

Localisation : 0x004049C7

- Le programme interroge le système pour vérifier le drapeau BeingDebugged dans le bloc d'environnement du processus (PEB).
- **Si un débogueur est détecté** : L'instruction de saut (jnz) redirige le flux vers loc_404BCE. Ce bloc nettoie la pile et quitte la fonction immédiatement, rendant le malware inerte.
- **Si aucun débogueur n'est détecté** : Le programme poursuit son exécution normalement vers la charge utile (payload), qui contient les manipulations graphiques malveillantes.



CheckRemoteDebuggerPresent

Localisation: 0x004044DF

Si un débogueur est détecté, l'exécution est interrompue immédiatement (nettoyage et sortie).

Il y a une instruction conditionnelle trompeuse : js sur un résultat toujours positif. Ce bloc caché contient l'appel à puts permettant d'afficher une chaîne secrète.

Une chaîne ("VIXTXhXWGhhU0ZaV1lsaFNWViZxUmt0WGJGcDBU") a été identifiée à l'offset 0x47F307.



CheckRemoteDebuggerPresent

Localisation: 0x004044DF

Tentative de déchiffrer la chaîne :

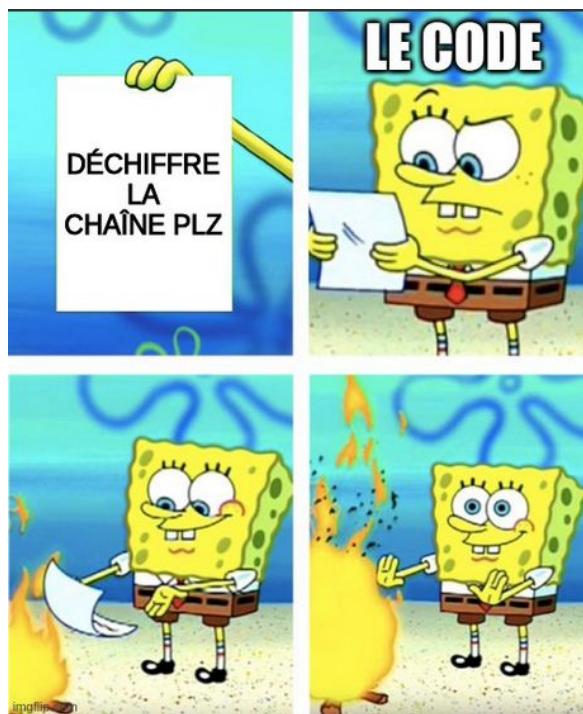
VIXTXhXWGhhU0ZaV1lSaFNWVIZxUmt0WG
JGcDBU

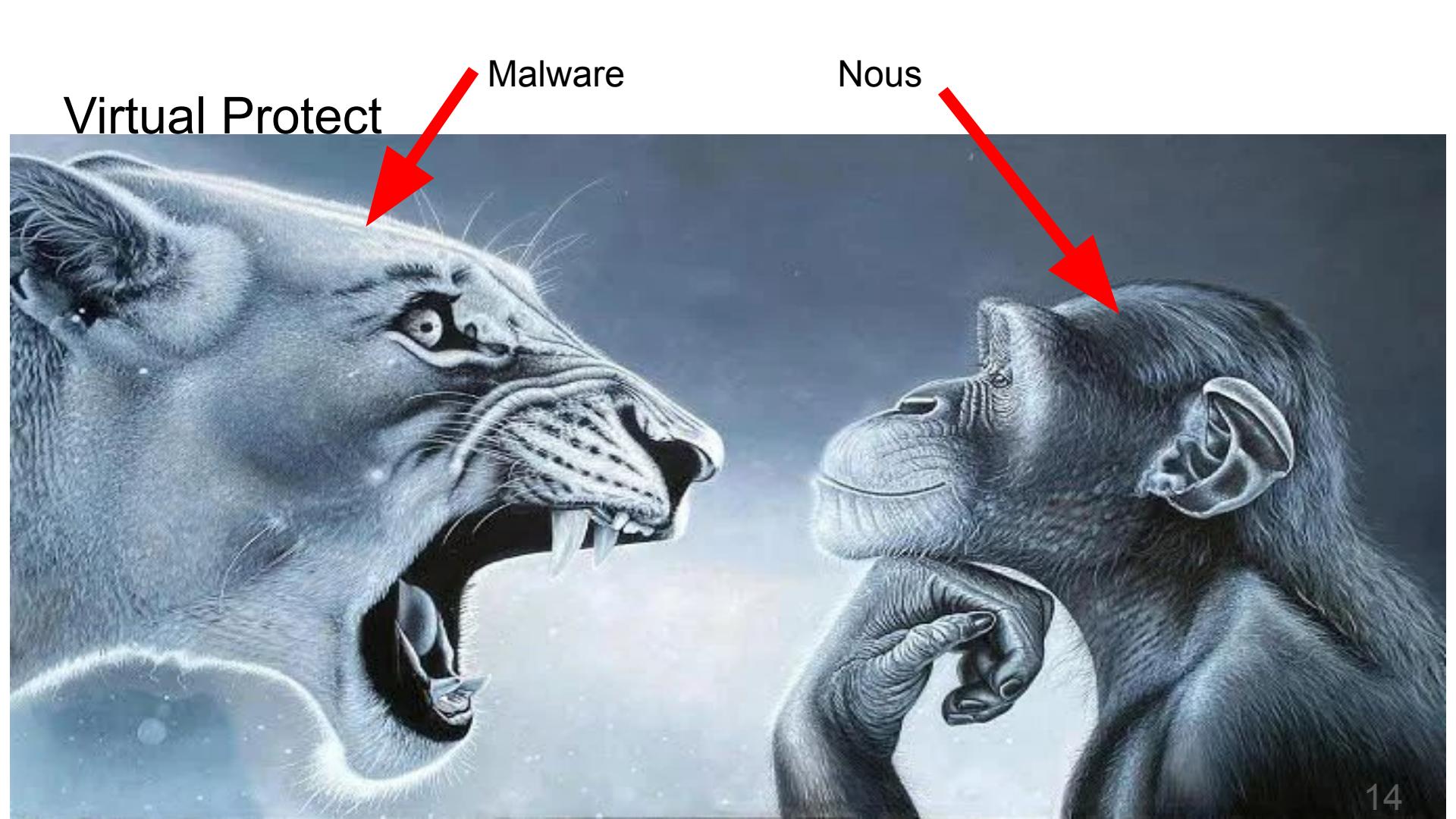
CyberChef

Analyse de puts : c'est bien la fonction standard de windows qui affiche ce qu'on lui donne

Nous avons forcé le saut vers la zone interdite

Mais nous n'avons pas réussi à voir ce qu'il affichait car le programme ferme tout lorsqu'on l'exécute. Sûrement car il détecte qu'il a été modifié.





Virtual Protect

Malware

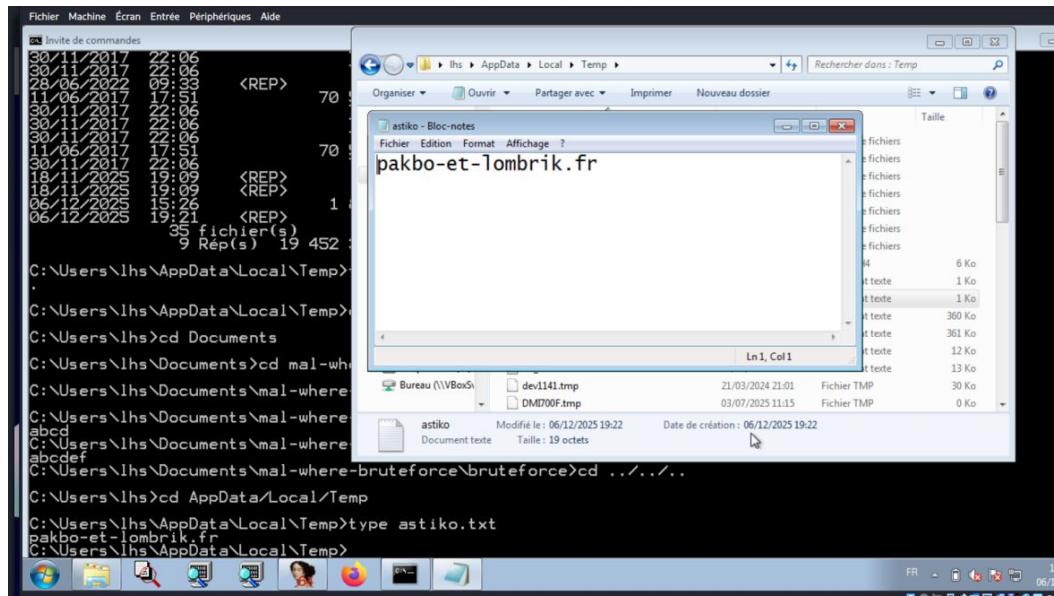
Nous

Virtual Protect

- Ecriture dans TEMP de 20 octets
- Clé de chiffrement symétrique :

pakbo-et-lombrik.fr

- 414 octets chiffré
- code spaghetti

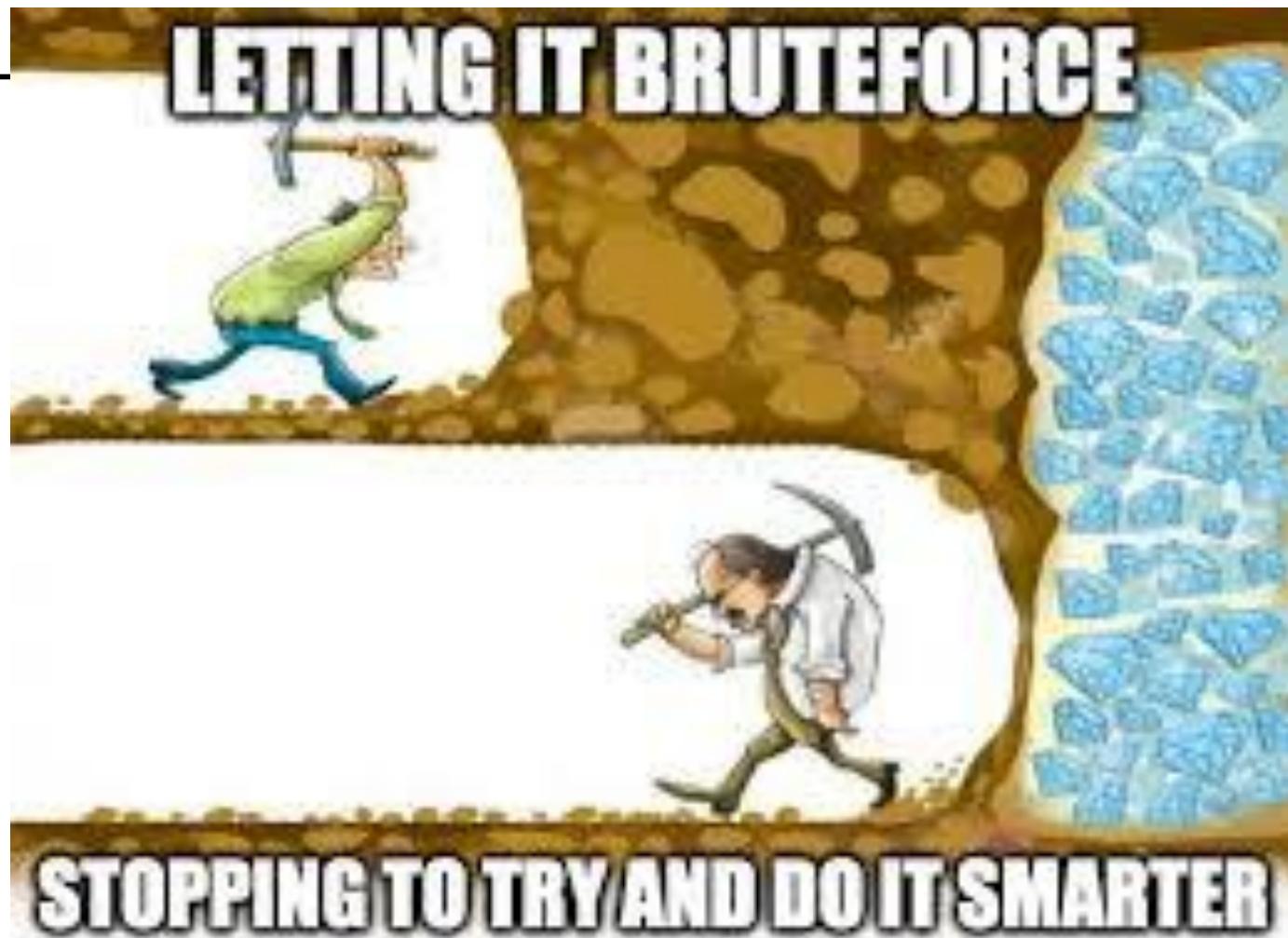


Target Hash

bea8e217036cb3b738e207fe5d40266828bc1969fd8538d533ea39f4e40ffc8f

[DEBUG] Hash validation: PASSED | Checksum: 0xDEADBEEF

Target H



Target Hash



Process Name	% CPU	CPU Time	Threads	Idle Wa
Python	100.0	19.49	2	
Python	99.9	19.51	2	
Python	99.8	19.51	2	
Python	99.8	19.50	2	
Python	99.8	19.51	2	
Python	99.7	19.49	2	

OU

Target Hash

bea8e217036cb3b738e207fe5d40266828bc1969fd8538d533ea39f4e40ffc8f



$\text{SHA-256}(1234) = 03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4$

Target Hash

20

- Vérification d'intégrité dans dword_478854
- Patch ?

```
.text:00409AB0
.text:00409AB0          public TlsCallback_0
.text:00409AB0 TlsCallback_0    proc near      ; CODE XREF: sub_401190+110tp
.text:00409AB0                      ; DATA XREF: .rdata:off_560880+o .
.text:00409AB0 var_1C           = dword ptr -1Ch
.text:00409AB0 var_18           = dword ptr -18h
.text:00409AB0 var_14           = dword ptr -14h
.text:00409AB0 arg_0            = dword ptr 4
.text:00409AB0 arg_4            = dword ptr 8
.text:00409AB0 arg_8            = dword ptr 0Ch
.text:00409AB0
.v. .text:00409AB0          push  ebx
.text:00409AB1          sub   esp, 18h
.text:00409AB4          cmp   dword_478854, 2
.text:00409ABB          mov   eax, [esp+1Ch+arg_4]
.text:00409ABF          jz    short loc_409ACB
.text:00409AC1          mov   dword_478854, 2
.text:00409ACB
.loc_409ACB:           ; CODE XREF: TlsCallback_0+F+j
.text:00409ACB          cmp   eax, 2
.text:00409AC8          jz    short loc_409AE1
.text:00409AD0          cmp   eax, 1
.text:00409AD3          jz    short loc_409B10
.text:00409AD5
.loc_409AD5:           ; CODE XREF: TlsCallback_0+3C+j
                           ; TlsCallback_0+7C+j
.text:00409AD5          mov   eax, 1
.text:00409ADA          add   esp, 18h
.text:00409ADD          pop   ebx
.text:00409ADE          retn  0Ch
```

```
.text:0040203F          sub_401FF0
.text:004020EF          sub_4020A0
.text:00402CD4          sub_402150
.text:00402E2F          sub_402150
.text:00402F99          sub_402150
.text:004031AA          sub_402150
.text:0040370C          sub_403230
.text:00403A74          sub_403230
.text:00403A88          sub_403230
.text:00403AFC          sub_403230
.text:00403B40          sub_403230
.text:00403B7E          sub_403230
.text:00403BBC          sub_403230
.text:00403C00          sub_403230
.text:00403C3E          sub_403230
.text:00403C7C          sub_403230
.text:00403CC0          sub_403230
.text:00403D04          sub_403230
.text:00403D48          sub_403230
.text:00403D82          sub_403230
.text:00403DDF          sub_403230
.text:00409AB4          TlsCallback_0
.text:00409AC1          TlsCallback_0
.text:004116E3          sub_4116E0
.text:00411703          sub_411700
.text:00412070          sub_412010
.text:0041215F          sub_412130
.text:004121EF          sub_4121C0
.text:00416BB2
.text:00416C03
.text:00416DE2
```

Conclusion

malware ou goodware ?

