

ANALYSE DU MALWARE

De Emy, Gautier et Yunqiao

Ibrahim MECIRDI
Abdelrahman RACHIDI

PLAN

1. Anti-Debugger
2. Contournement des anti-debugger
3. Chiffrement

Anti-Debugger

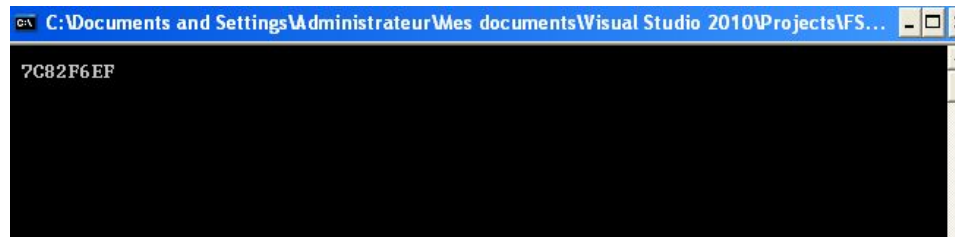
Présence d'anti-débugger visible :

```
call    ds:GetCurrentProcess
push    eax                ; hProcess
call    ds:CheckRemoteDebuggerPresent
push    offset unk_40A3EA
call    ebx ; printf
add     esp, 4
xor     edi, edi
test    eax, eax
jnz     loc_402236
```

Anti-Debugger

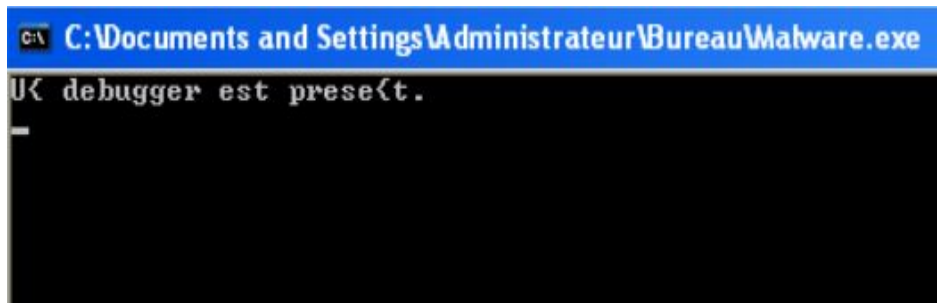
```
.text:00401DE3 lea     eax, [esp+0CCh+var_4]
.text:00401DE8 mov     large fs:0, eax
.text:00401DF0 mov     ebx, ds:printf
.text:00401DF6 lea     eax, [esp+0CCh+f101dProtect]
.text:00401DFA push    eax ; lpf101dProtect
.text:00401DFB push    40h ; f1NewProtect
.text:00401DFD push    6 ; dwSize
.text:00401DFF push    ebx ; lpAddress
.text:00401E00 call    ds:VirtualProtect
.text:00401E06 sub     esp, 1Ch
.text:00401E09 mov     esi, esp
.text:00401E0B mov     dword ptr [ebx], 82F6EF68h
.text:00401E11 mov     word ptr [ebx+4], 0C37Ch
.text:00401E17 mov     eax, offset aMalware ; "MALWARE"
```

```
printf("\n %p", IsDebuggerPresent);
```



IsDebuggerPresent -> printf

Anti-Debugger



```
C:\Documents and Settings\Administrateur\Bureau\Malware.exe
U< debugger est prese<t.
_
```

```
0000000000402250 mov     eax, offset aHQrohtttrRfgCe ; "H{ qrohtttr rfg cerfr{g."
0000000000402255 mov     [esp+0ECh+var_BC], esp
0000000000402259 mov     byte ptr [esi], 0
000000000040225C call    sub_402AC0
0000000000402261 lea     ecx, [esp+0ECh+var_84]
0000000000402265 call    loc_401A50
000000000040226A mov     byte ptr [esp+0ECh+var_4], 2
0000000000402272 mov     ecx, ds:?cout@std@@@3V?$basic_ostream@DU?$char_traits@D@std@@@1@A
```

Contournement des techniques d'anti-debugging

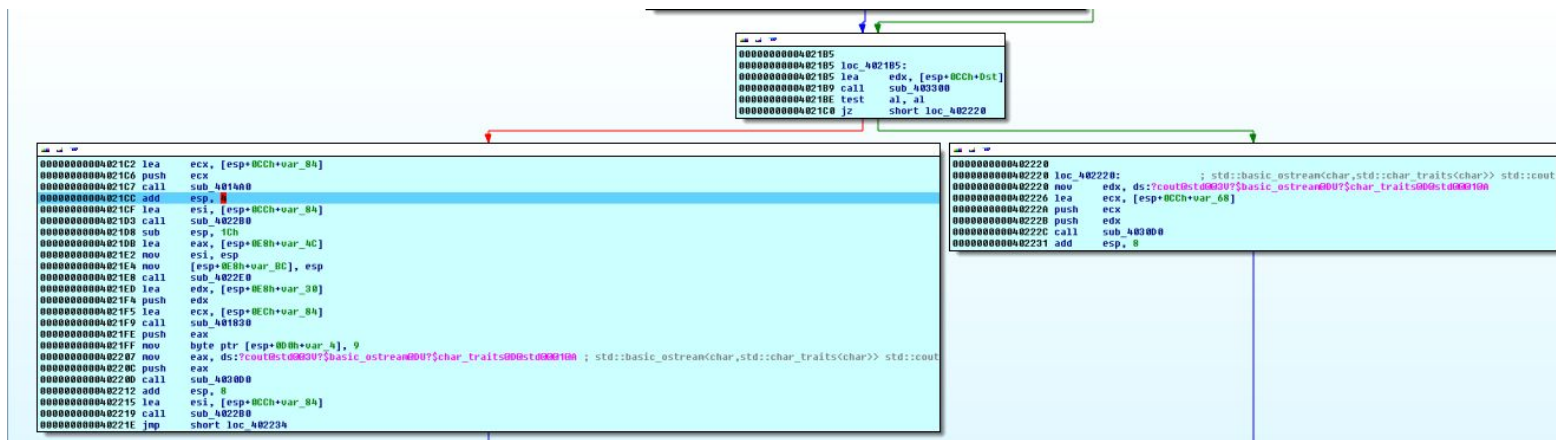
modification de la valeur des registres eax et edi

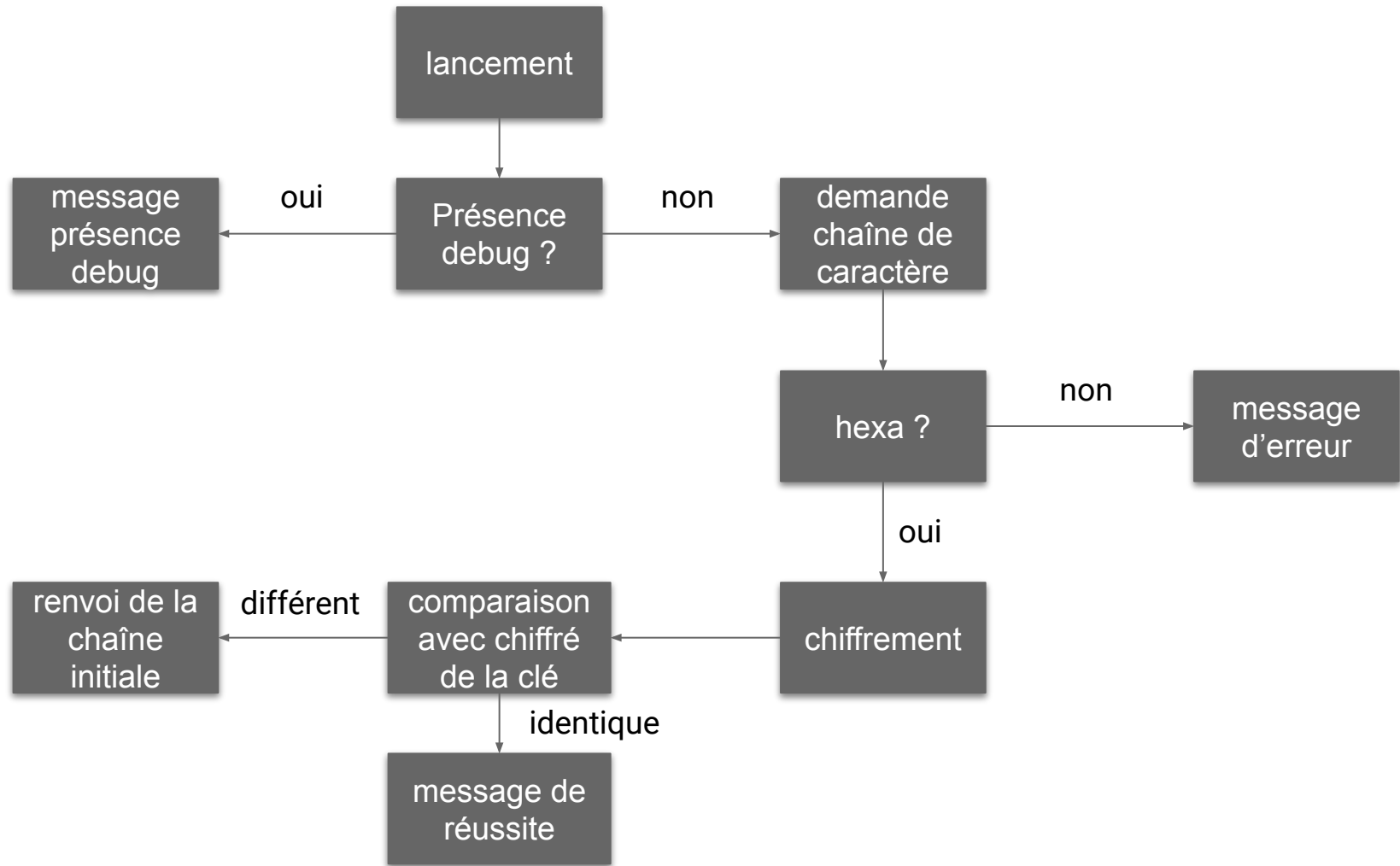
```
.text:00401E9F call ds:CheckRemoteDebuggerPresent
.text:00401EA5 push offset unk_40A3EA
.text:00401EAA call ebx ; printf
.text:00401EAC add esp, 4
.text:00401EAF xor edi, edi
.text:00401EB1 test eax, eax
.text:00401EB3 jnz loc_402236
.text:00401EB9 cmp [esp+0CCCh+pbDebuggerPresent], edi
.text:00401EBD jnz loc_402236
.text:00401EC3 mov esi, 0Fh
.text:00401EC8 mov [esp+0CCCh+var_8C], esi
```

```
RAX 0000000000000001
RBX 0000000078B056B4 msucr100.dll:msucr100_printf
RCX 000000000012FE7C Stack[00000760]:000000000012FE7C
RDX 000000007C91E514 ntdll.dll:ntdll_KiFastSystemCallRet
RSI 000000000012FF2C Stack[00000760]:000000000012FF2C
RDI 0000000000000000
RBP 000000000012FF7C Stack[00000760]:000000000012FF7C
RSP 000000000012FEAC Stack[00000760]:000000000012FEAC
RIP 0000000000401EB1 _main+101
```

Identification du message de réussite

```
C:\ C:\Documents and Settings\Administrateur\Mes documents\Malware.exe
afffffaaaaaaaaaaaaaaaaaaaa4
Bravo ! Tu as trouve LACLESECRETE
```





Chiffrement

Clé chiffrée :

```
aJkjjkkkjjjkkjj db 'jkjjkkkjjjkkkjkkkjkkjjjjkjkkjkjjkkjkjjkkjkjkjjkkkjkkjjkkjj'  
                    ; DATA XREF: sub_403300:loc_40331B↑o  
db 'kkjkjjkkjjkkkjkkkjkkjjjjkkjjkjkkjkjjkkjkjjkkjkjjkkjkjj'  
db 'kkjkjjkkjjjjjjkkjkjkjjkkjkjjkkjjjjkkjkjjkkjkjkjjkkjkjj'  
db 'jjkkjjkkjjjjjjkkjkjkjjkkjkjjjjkkjjkkjkjjkkjkjjkkjkjjkk'  
db 'kkjkjjkkjkjjjjkkjjjjkjkkjkjjkkjjjjkkjkjjkkjjjjkkjjjjkkjj'  
db 'jjjjkkjkjjjjjjkkjjkkjjjjkkjjjjkkjjjjkkjjjjkkjjk',0
```

Composée uniquement de j et de k (432 caractères)

-> semblable à un codage binaire

chiffrement par substitution 1 caractère -> une chaîne de 8 caractères composée de j et k

Chiffrement

Remplissage à la main d'un dictionnaire à l'aide
du contournement de l'anti-debugger

```
dico = {}  
dico["jkjkkkj"] = "a"  
dico["jjkkjjj"] = "b"  
dico["kkjjjjj"] = "c"  
dico["jjjjjjkk"] = "d"  
dico["jjkkjjkk"] = "e"  
dico["jkjkkjk"] = "f"  
dico["jkjjjjjk"] = "A"  
dico["jkjjjjkj"] = "B"  
dico["jkjjjjkk"] = "C"  
dico["jkjjjkjj"] = "D"  
dico["jkjjjkjk"] = "E"  
dico["jkjjkkj"] = "F"  
dico["jjkkjjjj"] = "0"  
dico["jjkkjjjk"] = "1"  
dico["jjkkjjkj"] = "2"  
dico["jjkkjjkk"] = "3"  
dico["jjkkjkjj"] = "4"  
dico["jjkkjkjk"] = "5"  
dico["jjkkjkkj"] = "6"  
dico["jjkkjkkk"] = "7"  
dico["jjkkkjjj"] = "8"  
dico["jjkkkjkk"] = "9"
```

Chiffrement

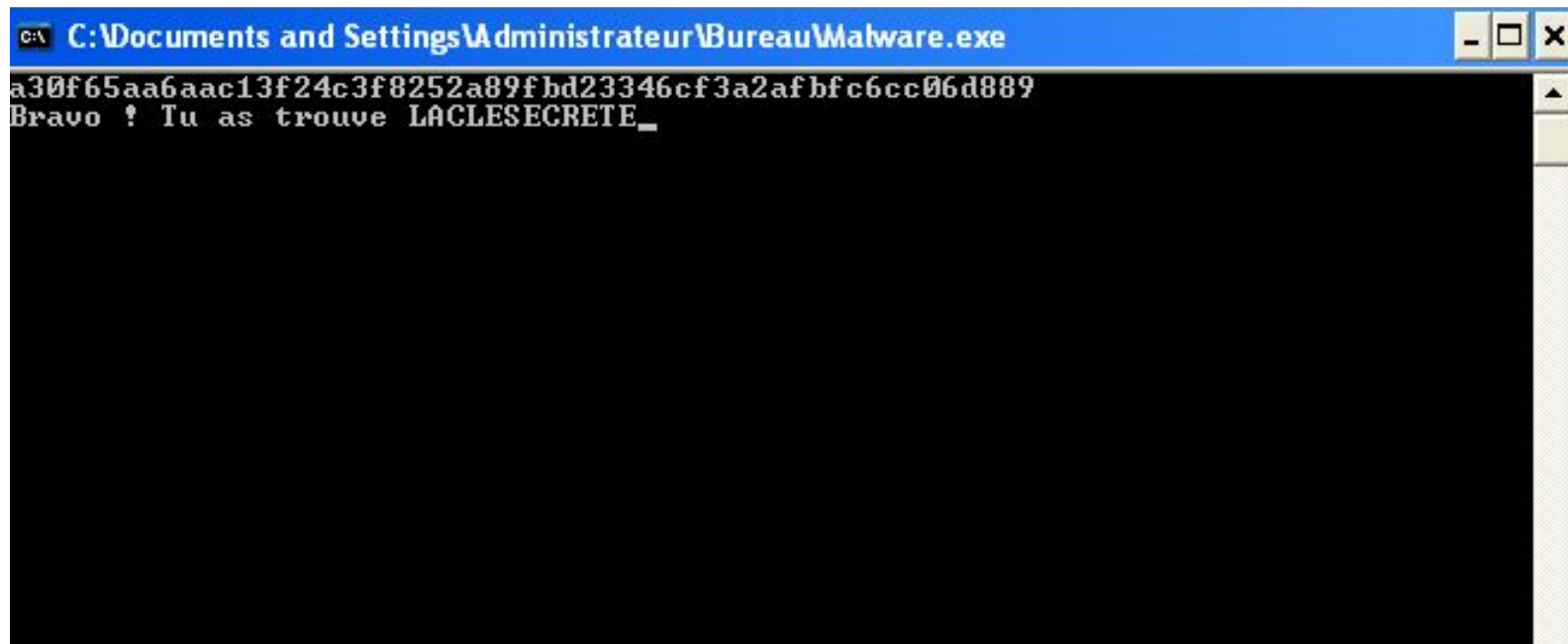
```
aJkjjkkkjjkkjj db 'jkjjkkkjjjkkjjkkjjkkjjjjjjkjjkkjkjjkkjkjjkkjkjjkkjkjjkkjkjjkkjkjjkkjkjj'
; DATA XREF: sub_403300:loc_40331B↑o
db 'jkkjkkjjkjjkkkjjkjjkkkjjkkjjjjjjkjjjjkjjkkjkjjkkjkjjkkjkjjkkjkjj'
db 'kkjkjjjkkjjjjjjkkjjkkjkjjkkjkjjkkkjjjjkkjjkjjjkkjkjjkkjkjjkkjj'
db 'jkkkjjjkkkjjjjjkkkjjkjjkkjkjjjkkjjjjjjjjkkjjkkjjkjjjkkjjkkjjkk'
db 'jjkkjjkkjkjjjjkkjkkjjkkjjjjjjkjjkkjkjjkkjkjjkkjkjjkkjjkkjjkkjjk'
db 'kkjjkjjkkjkjjjkkjjjjkjjkkjkjjkkjjjjjjkkjkkjjkkjjjjjjkkjjjjjjkkjj'
db 'jjjjkkjkjjjjjjkkjjkkkjjjjkkkjjjjkkkjjk',0
```

Déchiffre 8 caractères par 8 caractères

Obtention d'un chaîne de 54 caractères

a30f65aa6aac13f24c3f8252a89fbd23346cf3a2afbfc6cc06d889

Obtention de la clé secrète



```
C:\Documents and Settings\Administrateur\Bureau\Malware.exe  
a30f65aa6aac13f24c3f8252a89fbd23346cf3a2afbfc6cc06d889  
Bravo ! Tu as trouve LACLESECRETE_
```

FIN