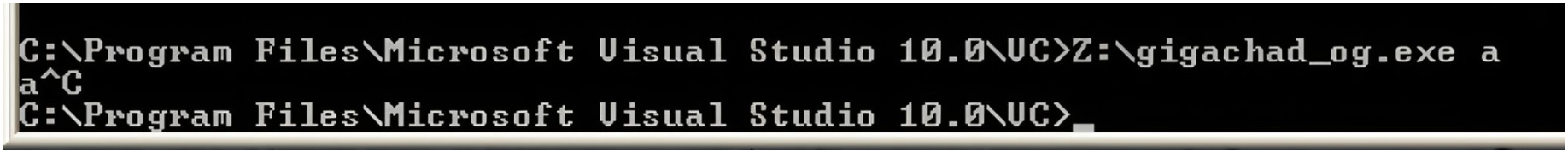
# Présentation
# de notre Attaque sur un Malware

BOUCHER, DA SILVA, SMAGGHE

# Sommaire

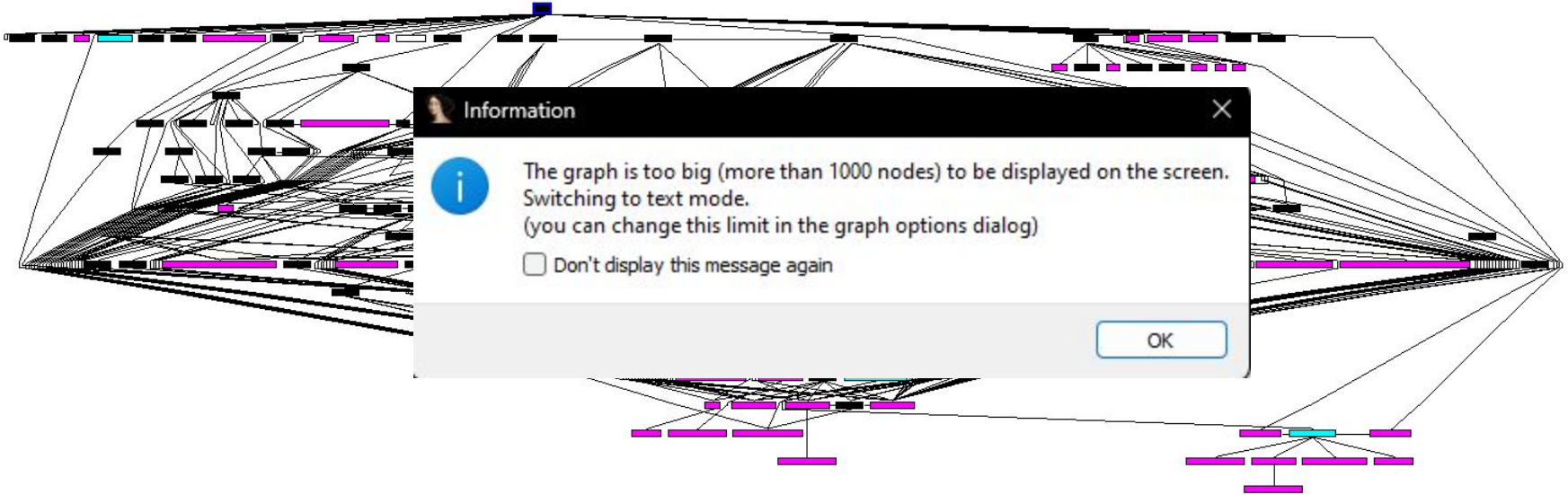
- Vue Globale
- Enigmes à résoudre
- Conclusion (Type A ou Type B)

# Vue Globale - Sanity Check



# Vue Globale - Sanity Check 2

# Vue Globale - Graphs



# Enigmes à résoudre - Anti-Debug :

Les adresses correspondantes :

IsDebuggerPresent : 00405DCE

Clock : 0040536C-00405DC2 (compteur de tick)

CheckRemoteDebuggerPresent :004060C4

# Enigmes à résoudre - Neutralisation action en cas de mauvaise entrée

```
.text:00405212 85 C0                    test    eax, eax
.text:00405214 75 B1                    jnz     short loc_4051C7
.text:00405214
.text:00405216 68 03 00 02 80           push    80020003h               ; dwReason
.text:0040521B 6A 05                    push    5                       ; uFlags
.text:0040521D FF 15 90 A1 35 01        call    ds:ExitWindowsEx
.text:0040521D
.text:00405223 8B 4D FC                 mov     ecx, [ebp-4]
```

| | |
|---|---|
| **EWX_SHUTDOWN**<br>0x00000001 | Arrête le système à un point où il est sûr de désactiver l'alimentation. Tous les tampons de fichiers ont été vidés sur le disque et tous les processus en cours d'exécution ont été arrêtés. Le processus appelant doit avoir le privilège SE_SHUTDOWN_NAME. Pour plus d'informations, consultez la section Notes qui suit.<br><br>La spécification de cet indicateur ne désactive pas l'alimentation même si le système prend en charge la fonctionnalité de mise hors tension. Vous devez spécifier EWX_POWEROFF pour ce faire. **Windows XP avec SP1 :** Si le système prend en charge la fonctionnalité de mise hors tension, la spécification de cet indicateur désactive l'alimentation. |

| Valeur | Signification |
|---|---|
| EWX_FORCE<br>0x00000004 | Cet indicateur n'a aucun effet si les services Terminal Server sont activés. Sinon, le système n'envoie pas le message WM_QUERYENDSESSION . Cela peut entraîner la perte de données des applications. Par conséquent, vous devez utiliser cet indicateur uniquement en cas d'urgence. |

# Enigmes à résoudre - Neutralisation action en cas de mauvaise entrée

```
.text:00405195                          ; ---------------------------------------------------------------------------
.text:00405196 CC CC CC CC CC CC CC CC CC CC align 10h
.text:004051A0
.text:004051A0                          chiant:                                 ; CODE XREF: _main:loc_405E18↓p
.text:004051A0                                                                  ; _main:loc_406110↓p
.text:004051A0                                                                  ; _main+E2B↓p
.text:004051A0                                                                  ; _main+E4F↓p
.text:004051A0                                                                  ; _main:loc_406178↓p
.text:004051A0                                                                  ; _main+EAA↓p
.text:004051A0                                                                  ; _main:loc_1353A16↓p
.text:004051A0                                                                  ; DATA XREF: _main+260↓o
.text:004051A0 C3                       retn
.text:004051A0
.text:004051A1                          ; ---------------------------------------------------------------------------
.text:004051A1 8B EC                    mov     ebp, esp
.text:004051A3 83 EC 18                 sub     esp, 18h
.text:004051A6 A1 18 C0 35 01           mov     eax, ___security_cookie
.text:004051AB 33 C5                    xor     eax, ebp
.text:004051AD 89 45 FC                 mov     [ebp-4], eax
.text:004051B0 8D 45 E8                 lea     eax, [ebp-18h]
.text:004051B3 50                       push    eax                             ; TokenHandle
.text:004051B4 6A 28                    push    28h ; '('                       ; DesiredAccess
.text:004051B6 FF 15 38 A0 35 01        call    ds:GetCurrentProcess
.text:004051B6
.text:004051BC 50                       push    eax                             ; ProcessHandle
.text:004051BD FF 15 04 A0 35 01        call    ds:OpenProcessToken
.text:004051BD
```

# Auto-modification :

Les adresses correspondantes :

VirtualProtect : 004053B5

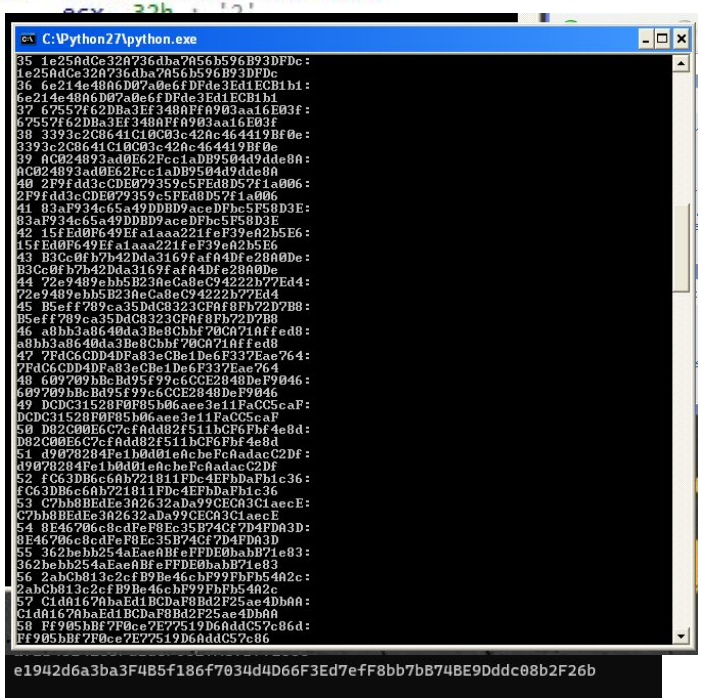
```
.text:00405372 89 85 C8 FE FF FF          mov     [ebp+var_138], eax
.text:00405378 C6 85 04 FF FF FF 46       mov     [ebp+var_FC], 46h ; 'F'
.text:0040537F C6 85 05 FF FF FF 20       mov     [ebp+var_FB], 20h ; ' '
.text:00405386 C6 85 06 FF FF FF 44       mov     [ebp+var_FA], 44h ; 'D'
.text:0040538D C6 85 07 FF FF FF 4C       mov     [ebp+var_F9], 4Ch ; 'L'
.text:00405394 C6 85 08 FF FF FF 7B       mov     [ebp+var_F8], 7Bh ; '{'
.text:0040539B A1 04 D2 35 01             mov     eax, off_135D204
.text:004053A0 89 85 64 FF FF FF          mov     [ebp+lpAddress], eax
.text:004053A6 8D 4D B8                   lea     ecx, [ebp+flOldProtect]
.text:004053A9 51                         push    ecx                             ; lpflOldProtect
.text:004053AA 6A 40                      push    40h ; '@'                       ; flNewProtect
.text:004053AC 6A 06                      push    6                               ; dwSize
.text:004053AE 8B 95 64 FF FF FF          mov     edx, [ebp+lpAddress]
.text:004053B4 52                         push    edx                             ; lpAddress
.text:004053B5 FF 15 30 A0 35 01          call    ds:VirtualProtect
.text:004053B5
.text:004053BB C7 85 88 FE FF FF 00 00 00 00 mov  [ebp+var_178], 0
.text:004053C5 EB 0F                      jmp     short loc_4053D6
.text:004053C5
.text:004053C7                            ; ---------------------------------------------------------------------------
.text:004053C7
.text:004053C7                            loc_4053C7:                             ; CODE XREF: _main+EA↓j
.text:004053C7 8B 85 88 FE FF FF          mov     eax, [ebp+var_178]
.text:004053CD 83 C0 01                   add     eax, 1
.text:004053D0 89 85 88 FE FF FF          mov     [ebp+var_178], eax
.text:004053D0
.text:004053D6
.text:004053D6                            loc_4053D6:                             ; CODE XREF: _main+B5↑j
.text:004053D6 83 BD 88 FE FF FF 06       cmp     [ebp+var_178], 6
.text:004053DD 7D 1D                      jge     short loc_4053FC
```

# Clés

Environ 13 000 clés qui suivent un pattern :

```
.text:00427A73 8B 55 0C          mov     edx, [ebp+argv]
.text:00427A76 8B 42 04          mov     eax, [edx+4]
.text:00427A79 0F BE 48 1B       movsx   ecx, byte ptr [eax+1Bh]
.text:00427A7D 83 F9 32          cmp     ecx, 32h ; '2'
.text:00427A80 0F 85 5B 02 00 00 jnz
```

Extraction des clés selon le pattern



# Clés

Environ 13 000 clés générées d'environ cette manière :

```
void main() {
    if (input[0] == '9' && input[1] == 'F' && input[2] == '6' ) {
        printf("%c", '9');
        printf("%c", 'F');
        printf("%c", '6');
    }
}
```

Sauf une...

```
void main() {
    if (input[0] == 'A' && input[1] == 'B' && input[2] == 'C' ) {
        printf("%c", 'B');
        printf("%c", 'o');
        printf("%c", 'n');
        printf("%c", 'n');
        printf("%c", 'e');
        printf("%c", ' ');
        printf("%c", 'p');
        ...
    }
}
```

# Conclusion

Malware de type A