

SSTIC 2004:

Détections Heuristiques en environnement Win32

Nicolas Brulez – Silicon Realms



Introduction

Les différents types de virus

- Cryptés
- Oligomorphiques
- Polymorphiques
- Métamorphiques

Le Format PE

- Le MZ Header
- Le PE Header
- Le PE File Header
- Le PE optional Header
- Le Data Directory
- Les Sections Headers

Code Relogeable

Les virus doivent pouvoir être exécutable à n'importe quelle adresse mémoire. Le principe du code relogeable est un offset de référence aux données du virus.

Les données se retrouvent toujours à même distance du début du virus par exemple, ce qui permet au virus, de retrouver ses données à n'importe quelle adresse de chargement.

Delta Offset.

Présentation de quelques types d'infections Win32

Emplacement du virus

- **Dernière section:**
 - Ajout de Section

Avant:

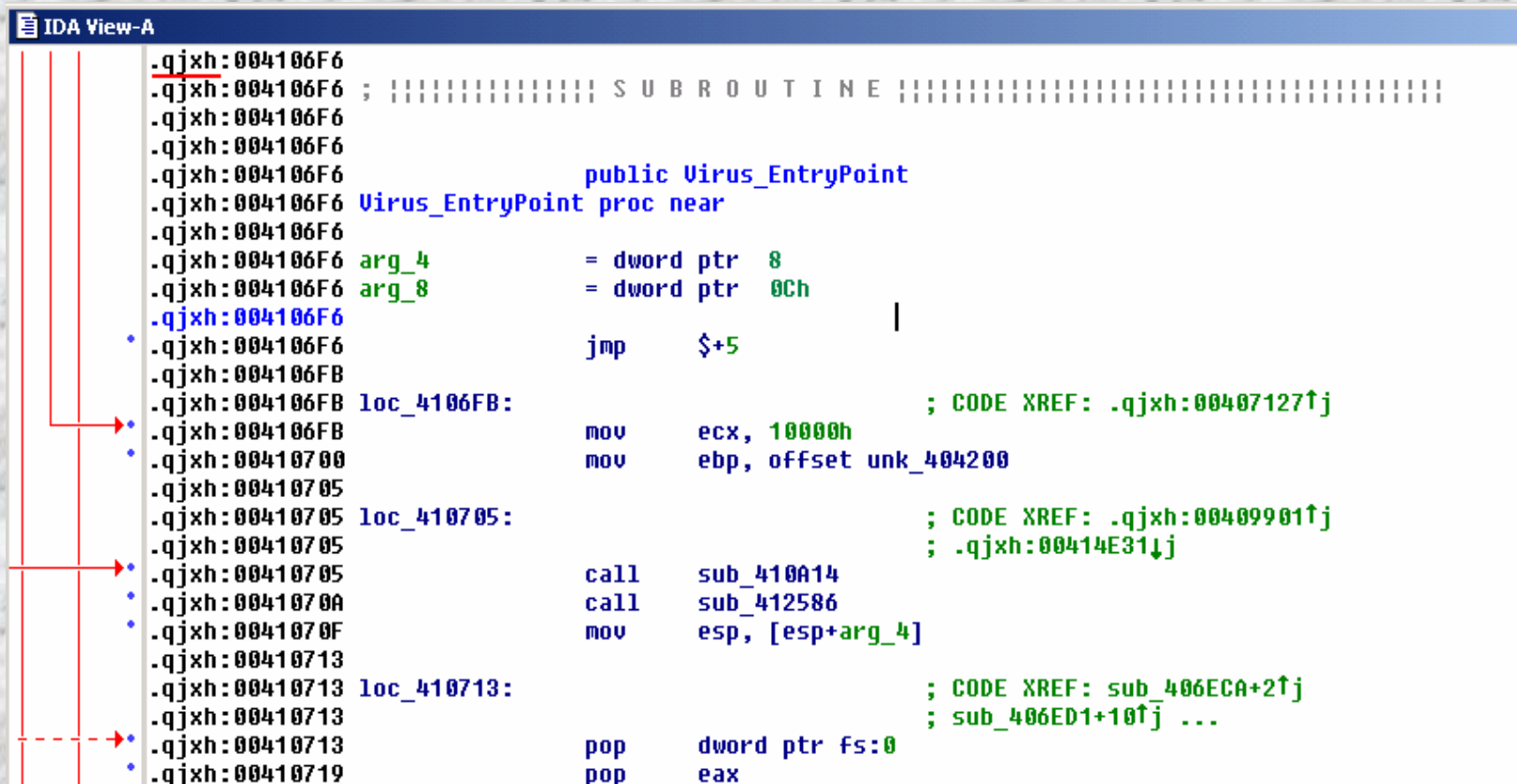
MZ Header IMAGE_DOS_HEADER
MS-DOS Stub Program
PE Header IMAGE_NT_HEADERS
Section Headers IMAGE_SECTION_HEADER
Section .text
Section .data
Section .rsrc
Section

Après:

MZ Header IMAGE_DOS_HEADER
MS-DOS Stub Program
PE Header IMAGE_NT_HEADERS
Section Headers IMAGE_SECTION_HEADER
Section .text
Section .data
Section .rsrc
Section <u>Virus</u>

Emplacement du virus

- Dernière section:
 - Ajout de Section



```
IDA View-A
.qjxh:004106F6
.qjxh:004106F6 ; :::::::::::::::::::: S U B R O U T I N E ::::::::::::::::::::
.qjxh:004106F6
.qjxh:004106F6
.qjxh:004106F6
.qjxh:004106F6 public Virus_EntryPoint
.qjxh:004106F6 Virus_EntryPoint proc near
.qjxh:004106F6
.qjxh:004106F6 arg_4 = dword ptr 8
.qjxh:004106F6 arg_8 = dword ptr 0Ch
.qjxh:004106F6
.qjxh:004106F6 jmp $+5
.qjxh:004106FB
.qjxh:004106FB loc_4106FB: ; CODE XREF: .qjxh:00407127↑j
.qjxh:004106FB mov ecx, 10000h
.qjxh:00410700 mov ebp, offset unk_404200
.qjxh:00410705
.qjxh:00410705 loc_410705: ; CODE XREF: .qjxh:00409901↑j
.qjxh:00410705 ; .qjxh:00414E31↓j
.qjxh:00410705 call sub_410A14
.qjxh:0041070A call sub_412586
.qjxh:0041070F mov esp, [esp+arg_4]
.qjxh:00410713
.qjxh:00410713 loc_410713: ; CODE XREF: sub_406ECA+2↑j
.qjxh:00410713 ; sub_406ED1+10↑j ...
.qjxh:00410713 pop dword ptr fs:0
.qjxh:00410719 pop eax
```


Emplacement du virus

- **Dernière section:**
 - Agrandissement de la dernière section

Avant:

Après:

MZ Header IMAGE_DOS_HEADER	MZ Header IMAGE_DOS_HEADER
MS-DOS Stub Program	MS-DOS Stub Program
PE Header IMAGE_NT_HEADERS	PE Header IMAGE_NT_HEADERS
Section Headers IMAGE_SECTION_HEADER	Section Headers IMAGE_SECTION_HEADER
Section .text	Section .text
Section .data	Section .data
Section .rsrc	Section .rsrc <u>Virus</u>

Emplacement du virus

- Dernière section:
 - Agrandissement de la dernière section

```
.rsrc:0100F7B8 aXpaddingpaddin db 'XPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD'  
.rsrc:0100F7B8                                     ; CODE XREF: .rsrc:0100F815↓j  
.rsrc:0100F7B8                                     db 'INGXXPADDINGP'  
.rsrc:0100F801 ; -----  
.rsrc:0100F801 pusha  
.rsrc:0100F802 call sub_100F951  
.rsrc:0100F807 pop edx  
.rsrc:0100F808 mov edx, 3BD5C65Bh  
.rsrc:0100F80D cdq  
.rsrc:0100F80E loc_100F80E: ; CODE XREF: .rsrc:loc_100F80E↑j  
.rsrc:0100F80E jnb short near ptr loc_100F80E+1  
.rsrc:0100F810 mov eax, 9952E35h  
.rsrc:0100F815 jnb short near ptr aXpaddingpaddin+1  
.rsrc:0100F817 leave  
.rsrc:0100F818 call far ptr 0A672h:0B98C7A6Fh  
.rsrc:0100F81F pop edi  
.rsrc:0100F820 push dword ptr [ecx+6Ah]  
.rsrc:0100F823 pop esp  
.rsrc:0100F824 cli  
.rsrc:0100F825 mov cl, 24h  
.rsrc:0100F827 dec esi  
.rsrc:0100F828 mov esi, 0A96C6E37h  
.rsrc:0100F82D xchg eax, ecx  
.rsrc:0100F82E and edi, edi  
.rsrc:0100F830 aad 0A3h  
.rsrc:0100F832 jmp far ptr 9AC6h:2FFFAB3Dh  
.rsrc:0100F832 ; -----
```

Emplacement du virus

- Infection du Header

```
IDA View-A
HEADER:00400400 ;
HEADER:00400400 ; The code at 400000..401000 is hidden from normal disassembly
HEADER:00400400 ; and was loaded because the user ordered to load it explicitly
HEADER:00400400 ;
HEADER:00400400 ; <<<< IT MAY CONTAIN TROJAN HORSES, VIRUSES, AND DO HARMFUL THINGS >>>>
HEADER:00400400 ;
HEADER:00400400 ;
HEADER:00400400 ; :::::::::::::::::::: S U B R O U T I N E ::::::::::::::::::::
HEADER:00400400 ;
HEADER:00400400 ;
HEADER:00400400 ; public start
HEADER:00400400 start proc near
* HEADER:00400400 xchg eax, esi
* HEADER:00400401 push edi
* HEADER:00400402 sidt qword ptr [esp-2]
* HEADER:00400407 pop edi
* HEADER:00400408 fild qword ptr [edi]
* HEADER:0040040A call sub_4004B4
* HEADER:0040040F fistp qword ptr [edi-8]
* HEADER:00400412 mov ebx, 0BFF7128Ch
* HEADER:00400417 cmp byte ptr [ebx+35h], 0Fh
```

Emplacement du virus

- « Cavity »

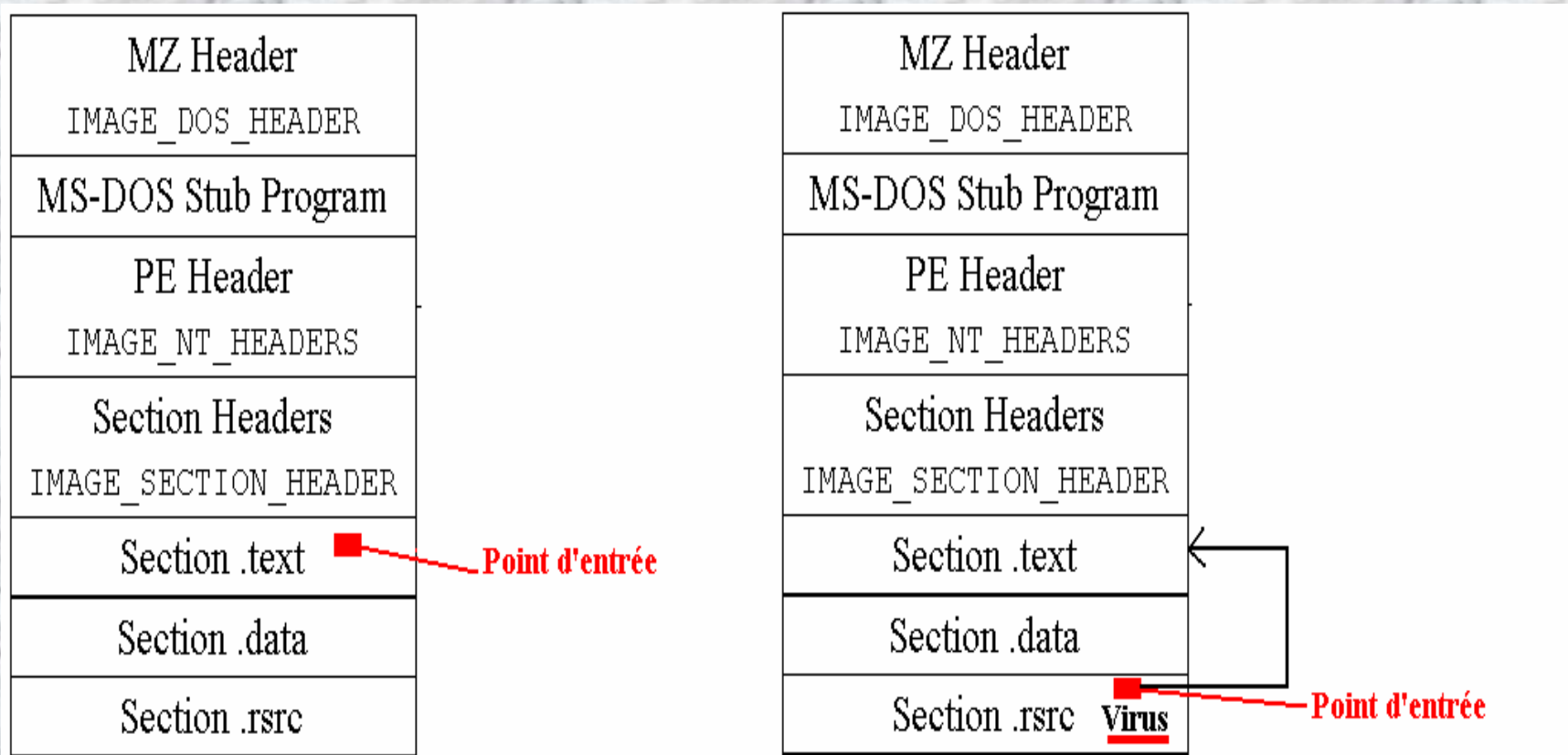
Avant:

Après:

MZ Header IMAGE_DOS_HEADER	MZ Header IMAGE_DOS_HEADER
MS-DOS Stub Program	MS-DOS Stub Program
PE Header IMAGE_NT_HEADERS	PE Header IMAGE_NT_HEADERS
Section Headers IMAGE_SECTION_HEADER	Section Headers IMAGE_SECTION_HEADER
Section .text	1 Section .text <u>Virus</u>
Section .data	3 Section .data <u>Virus</u>
Section .rsrc	2 Section .rsrc <u>Virus</u>
Section	Section

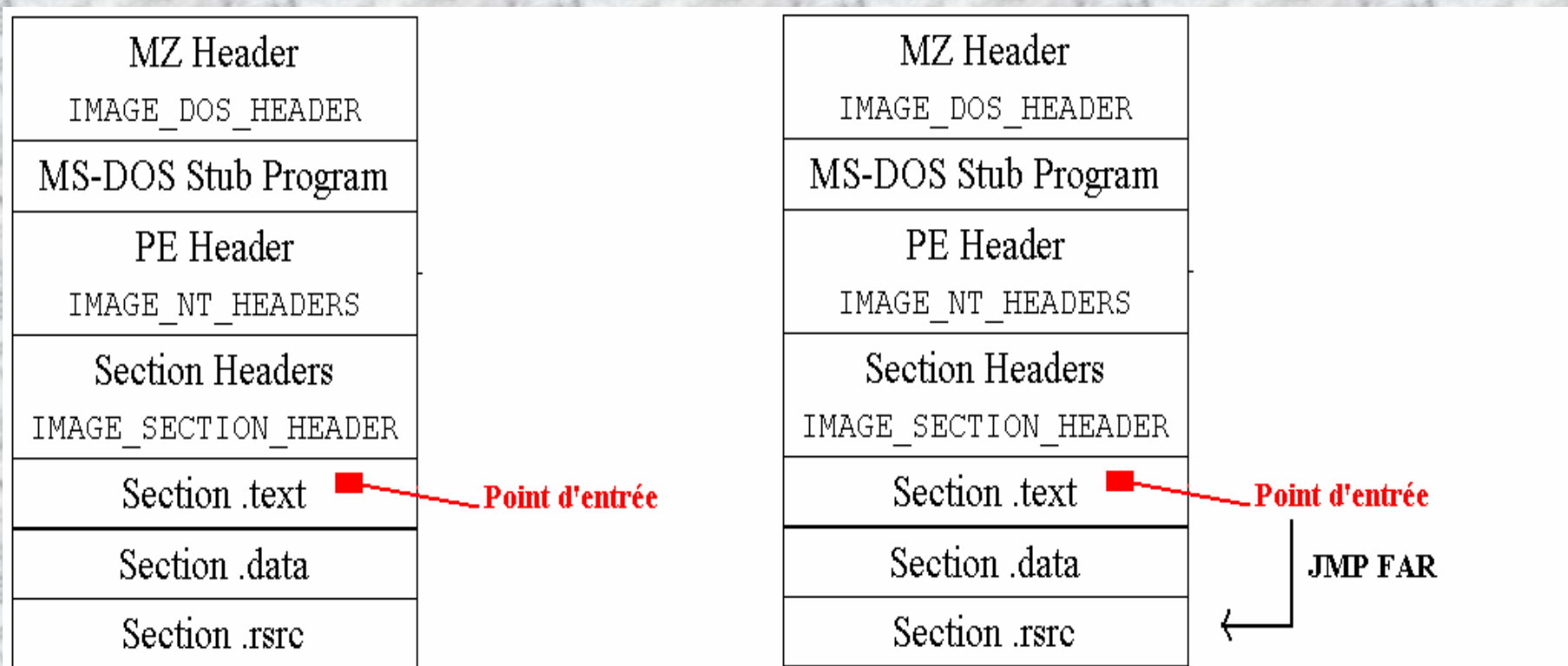
Point d'entrée

- Dans la dernière section




Point d'entrée

- **Dans la première section**




Point d'entrée

- **Avant la première section**

MZ Header IMAGE_DOS_HEADER
MS-DOS Stub Program
PE Header IMAGE_NT_HEADERS
Section Headers IMAGE_SECTION_HEADER
Section .text 
Section .data
Section .rsrc

Point d'entrée

MZ Header IMAGE_DOS_HEADER
MS-DOS Stub Program
PE Header IMAGE_NT_HEADERS
Section Headers IMAGE_SECTION_HEADER 
Section .text
Section .data
Section .rsrc

Point d'entrée

Infection par modification de e_lfanew

E_lfanew est un pointeur en MZ+3Ch qui contient l'offset du PE Header. L'infection par modification de e_lfanew consiste à ajouter le virus directement à la fin du fichier infecté, et à modifier le pointeur vers le PE Header pour que le loader de windows charge le virus à la place du binaire original.

Le PE Header se retrouve alors très loin du début du fichier.

Les détections heuristiques Win32

Analyse de la structure PE

Les détections heuristiques sont principalement basées sur l'analyse de la structure des exécutables PE Windows:

- Point d'Entrée
- Caractéristiques Sections
- Noms de sections
- Valeurs non mises à jours dans le Pe Header
- Placement du Pe Header dans le fichier...

Analyse de la structure PE

- Point d'entrée dans la dernière section
- Point d'entrée avant la première section

Analyse de la structure PE

- **Caractéristiques des sections:**
 - Dernière section « exécutable »
 - Première section « Writeable »
- **Nom des sections et leurs caractéristiques**

Analyse de la Structure PE

- « Virtual Size » incorrect dans le PE Header
- PE Header en fin de fichier
- « Size of Code » incorrect

Analyse du code

- **Instruction non standard au point d'entrée**
- **Calcul du delta offset**
- **Redirection de code Suspect:**
 - JUMP FAR
 - PUSH RET

Analyse du code

- **Recherche de fichiers PE**
- **Utilisation du PEB pour récupérer des adresses systemes**
- **Détection de code utilisant des adresses systemes
« hardcodées »**

Analyse du « code »

- **Recherche de chaînes de caractères particulières dans une section code.**
 - "*.exe"
 - API et dll windows
 - Base de Registre

Emulation

- **JMP FAR**
- **PUSH / RET**
- **Emulation des décrypteurs**

Techniques Anti Heuristiques

Structure PE

- Non Modification des caractéristiques des sections
- Ajout de plusieurs sections
- Ajout d'un bout de code du virus dans la première section (point d'entrée tjs dans la section code)
- Packing de la section code et ajout du virus dans l'espace non utilisé
- Point d'Entrée Obscure

Structure PE

- **Patch des appels aux fonctions de l'API Windows pour appeler le virus**
- **Patch du Stack Frame**
- **Calcul du Checksum du fichier PE**
- **Renommage des sections existantes**
- **« Size of Code » est corrigé**

Anti Emulation

- **SEH - Structured Exception Handling.**
- **Instructions du Co-Processeur**
- **MMX / SSE**
- **Instructions non documentées**
- **Code Anti Machine Virtuelle**
- **Couches de cryptage avec Auto brute force**
- **Threads**

Code anti heuristique

- **Le delta offset est obtenu différemment**
- **Le code pour la recherche de fichiers PE est obscurci**
- **Les fonctions de l'API Windows ne sont plus référencées directement (checksum)**

Présentation d'un moteur Heuristique Perso

Présentation d'un moteur Heuristique Perso

- **Analyse de binaires standards : notepad, regedit, calc, MS Pain, WordPad etc...**

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back up\engine.EXE
Heuristic Engine v0.06
Filename: C:\WINDOWS\explorer.exe

Nb Sections: 4
Size of Code: 3D800
Entry Point: 160CC
Image Base: 1000000

.text Usize:3D78D RVA:1000 Psize:3D800 offset:400 Flags:60000020
.data Usize:1CD8 RVA:3F000 Psize:1C00 offset:3DC00 Flags:C0000040
.rsrc Usize:B3270 RVA:41000 Psize:B3400 offset:3F800 Flags:40000040
.reloc Usize:34CC RVA:F5000 Psize:3600 offset:F2C00 Flags:42000040

This file looks normal :->

Disassembly of Entry Point (or virus entry point):

push ebp
mov ebp, esp
sub esp, 44
push esi
push edi
push 10
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back up\engine.EXE
Heuristic Engine v0.06
Filename: C:\WINDOWS\notepad.exe

Nb Sections: 3
Size of Code: 6E00
Entry Point: 6AE0
Image Base: 10000000

.text Usize:6D72 RVA:1000 Psize:6E00 offset:400 Flags:60000020
.data Usize:1BA8 RVA:8000 Psize:600 offset:7200 Flags:C0000040
.rsrc Usize:8E14 RVA:A000 Psize:9000 offset:7800 Flags:40000040

This file looks normal :->

Disassembly of Entry Point (or virus entry point):

push 70
push 1001888
call 01006CA8
xor ebx, ebx
push ebx
mov edi, dword ptr ds:[100114C]
call edi
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back up\engine.EXE
Heuristic Engine v0.06
Filename: C:\WINDOWS\regedit.exe

Nb Sections: 3
Size of Code: 14C00
Entry Point: 8AC5
Image Base: 10000000

.text Usize:14B08 RVA:1000 Psize:14C00 offset:400 Flags:60000020
.data Usize:40D54 RVA:16000 Psize:200 offset:15000 Flags:C0000040
.rsrc Usize:D368 RVA:57000 Psize:D400 offset:15200 Flags:40000040

This file looks normal :->

Disassembly of Entry Point (or virus entry point):

push ebp
mov ebp, esp
sub esp, 24
push ebx
push esi
push edi
call dword ptr ds:[10011D0]
```

Présentation d'un moteur Heuristique Perso

- **Analyse de binaires Infectés : Virus polymorphes, Cryptés, Standard, EPO etc**

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX\CRYPTO.
exe

Nb Sections: 4
Size of Code: 200
Entry Point: 9FF4
Image Base: 400000

.text Usize:DD5 RVA:1000 Psize:1000 offset:1000 Flags:60000060
.idata Usize:E4 RVA:2000 Psize:1000 offset:2000 Flags:40000040
.rsrc Usize:1000 RVA:3000 Psize:1000 offset:3000 Flags:40000040
.reloc Usize:8000 RVA:4000 Psize:8000 offset:4000 Flags:E2000060

Instruction at entry point is not usually used by a compiler. ASM ? ;->
Execution starts in last section.
Last section is Writeable and Executable.
A section known not to have any code is executable! Very suspicious.

This file might be infected! :-!

Disassembly of Entry Point (or virus entry point):
and bl, 99
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX\Dream.e
xe
Nb Sections: 5
Size of Code: 4000
Entry Point: E000
Image Base: 400000

.text Usize:3E9C RVA:1000 Psize:4000 offset:1000 Flags:E0000020
.data Usize:84C RVA:5000 Psize:1000 offset:5000 Flags:C0000040
.idata Usize:DE8 RVA:6000 Psize:1000 offset:6000 Flags:C0000040
.rsrc Usize:6000 RVA:7000 Psize:6000 offset:7000 Flags:C0000040
.reloc Usize:4000 RVA:D000 Psize:4000 offset:D000 Flags:E2000060

Instruction at entry point is not usually used by a compiler. ASM ? ;->
Execution starts in last section.
Last section is Writeable and Executable.
A section known not to have any code is executable! Very suspicious.
Get Delta (Used for relative addressing) has been found at EP+0
Code section is writeable.

This file is probably infected :-/ or Packed
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX\190.exe

Nb Sections: 4
Size of Code: 200
Entry Point: 400
Image Base: 400000

.text Usize:AB RVA:1000 Psize:1000 offset:1000 Flags:60000020
.idata Usize:E4 RVA:2000 Psize:1000 offset:2000 Flags:40000040
.rsrc Usize:1000 RVA:3000 Psize:1000 offset:3000 Flags:40000040
.reloc Usize:34 RVA:4000 Psize:1000 offset:4000 Flags:42000040

Instruction at entry point is not usually used by a compiler. ASM ? ;->
Entry Point is pointing before the First section.
A JMP FAR has been found at Entry point+185. Could be Entry Point Obscuring.

This file is probably infected :-/ or Packed

Disassembly of Entry Point (or virus entry point):

xchg eax, esi
push edi
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX>Noise.exe

Nb Sections: 5
Size of Code: 4000
Entry Point: 240
Image Base: 400000

.text Usize:3E9C RVA:1000 Psize:4000 offset:1000 Flags:60000020
.data Usize:84C RVA:5000 Psize:1000 offset:5000 Flags:C0000040
.idata Usize:DE8 RVA:6000 Psize:1000 offset:6000 Flags:40000040
.rsrc Usize:6000 RVA:7000 Psize:6000 offset:7000 Flags:40000040
.reloc Usize:A9C RVA:D000 Psize:1000 offset:D000 Flags:42000040

Entry Point is pointing before the First section.
A PUSH / RET has been found. Might be used to jmp to host or virus body
Get Delta (Used for relative addressing) has been found at EP+122
Contains code searching for PE files.

This file is probably infected :-/ or Packed

Disassembly of Entry Point (or virus entry point):
```


Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX\Prizzy.exe

Nb Sections: 5
Size of Code: 4000
Entry Point: 10294
Image Base: 400000

.text Usize:3E9C RVA:1000 Psize:4000 offset:1000 Flags:60000020
.data Usize:84C RVA:5000 Psize:1000 offset:5000 Flags:C0000040
.idata Usize:DE8 RVA:6000 Psize:1000 offset:6000 Flags:40000040
.rsrc Usize:4FB8 RVA:7000 Psize:5000 offset:7000 Flags:40000040
.reloc Usize:124B0 RVA:C000 Psize:123F4 offset:C000 Flags:E2000060

Instruction at entry point is not usually used by a compiler. ASM ? ;->
Execution starts in last section.
Last section is Writeable and Executable.
A section known not to have any code is executable! Very suspicious.

This file might be infected! :-!

Disassembly of Entry Point (or virus entry point):
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX\Rain Song.exe

Nb Sections: 5
Size of Code: 4000
Entry Point: 10CC
Image Base: 400000

.text Usize:3E9C RVA:1000 Psize:4000 offset:1000 Flags:60000020
.data Usize:84C RVA:5000 Psize:1000 offset:5000 Flags:C0000040
.idata Usize:DE8 RVA:6000 Psize:1000 offset:6000 Flags:40000040
.rsrc Usize:6000 RVA:7000 Psize:6000 offset:7000 Flags:40000040
.reloc Usize:3000 RVA:D000 Psize:2000 offset:D000 Flags:E2000060

Last section is Writeable and Executable.
A section known not to have any code is executable! Very suspicious.

This file might be infected! :-!

Disassembly of Entry Point (or virus entry point):
push ebp
mov ebp, esp
```

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus\engine.exe
Heuristic Engine v0.07
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\NOUVEAUX\SAMPLES
\ZOMBIE.EX$

Nb Sections: 4
Size of Code: 1200
Entry Point: 1001
Image Base: 400000

.text Usize:10AB RVA:1000 Psize:2000 offset:1000 Flags:60000020
.idata Usize:E4 RVA:3000 Psize:1000 offset:3000 Flags:40000040
.rsrc Usize:1000 RVA:4000 Psize:1000 offset:4000 Flags:40000040
.reloc Usize:34 RVA:5000 Psize:1000 offset:5000 Flags:42000040

Instruction at entry point is not usually used by a compiler. ASM ? ;->
A JMP FAR has been found at Entry point+5. Could be Entry Point Obscuring.

This file might be infected! :-!

Disassembly of Entry Point (or virus entry point):

push ebp
mov ebp, esp
sub esp, 44
```

Présentation d'un moteur Heuristique Perso

```
.text:00401001
.text:00401001 ; :::::::::::::::::::: S U B R O U T I N E ::::::::::::::::::::
.text:00401001
.text:00401001
.text:00401001 public start
.text:00401001 start proc near
.text:00401001 call sub_40100C
.text:00401006 jmp loc_40200C
.text:00401006 start endp
.text:00401006
.text:0040100B ; -----
.text:0040100B ; retn
.text:0040100C
.text:0040100C ; :::::::::::::::::::: S U B R O U T I N E ::::::::::::::::::::
.text:0040100C
...

.text:0040200C
.text:0040200C loc_40200C: ; CODE XREF: start+51j
* .text:0040200C push ebp
* .text:0040200D mov ebp, esp
* .text:0040200F sub esp, 44h
* .text:00402012 push esi
* .text:00402013 call ds:GetCommandLineA
* .text:00402019 mov esi, eax
```

Présentation d'un moteur Heuristique Perso

A Noter:

Un outil de génération de virus a été publié récemment par un des groupes de création de virus les plus connus.

Tout les virus générés sont détectés heuristiquement par le moteur.

Présentation d'un moteur Heuristique Perso

- **Analyse de fichiers PE packés : PE protect, PESHield etc...**

Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back up\engine.EXE
Heuristic Engine v0.06
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back
up\packers\done\PCPEC.EXE

Nb Sections: 6
Size of Code: 1600
Entry Point: B000
Image Base: 400000

CODE Usize:2000 RVA:1000 Psize:1600 offset:600 Flags:E0000020
DATA Usize:2000 RVA:3000 Psize:1400 offset:1C00 Flags:C0000040
.idata Usize:1000 RVA:5000 Psize:400 offset:3000 Flags:C0000040
.reloc Usize:1000 RVA:6000 Psize:600 offset:3400 Flags:D0000040
.rsrc Usize:3000 RVA:7000 Psize:2200 offset:3A00 Flags:D0000040
.PCPEC Usize:1000 RVA:B000 Psize:789 offset:5E00 Flags:F0000020

This file is protected by PCPEC "alpha - preview"
-
```

Présentation d'un moteur Heuristique Perso

```
C:\> D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back up\engine.EXE
Heuristic Engine v0.06
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back
up\packers\done\PESHIELD.EXE

Nb Sections: 6
Size of Code: 1E00
Entry Point: B000
Image Base: 400000

PESHIELD  Usize:2000  RVA:1000  Psize:1E00  offset:400  Flags:C0000040
PESHIELD  Usize:3000  RVA:3000  Psize:2200  offset:2200  Flags:C0000040
PESHIELD  Usize:1000  RVA:6000  Psize:400   offset:4400  Flags:C0000040
PESHIELD  Usize:1000  RVA:7000  Psize:400   offset:4800  Flags:C0000040
PESHIELD  Usize:3000  RVA:8000  Psize:1600  offset:4C00  Flags:C0000040
ANAKIN2K  Usize:3000  RVA:B000  Psize:1600  offset:6200  Flags:C0000040

This file is protected by PE Shield 0.25
```


Présentation d'un moteur Heuristique Perso

```
C:\D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back up\engine.EXE
Heuristic Engine v0.06
Filename: D:\Documents and Settings\Administrateur\Bureau\sstic\anti virus back
up\packers\done\UGCRYPT.EXE

Nb Sections: 8
Size of Code: 800
Entry Point: 8000
Image Base: 400000

CODE Vsize:1000 RVA:1000 Psize:800 offset:400 Flags:E0000020
DATA Vsize:1000 RVA:2000 Psize:800 offset:C00 Flags:C0000040
.idata Vsize:1000 RVA:3000 Psize:400 offset:1400 Flags:C0000040
.reloc Vsize:1000 RVA:4000 Psize:200 offset:1800 Flags:50000040
.vgc Vsize:158 RVA:5000 Psize:200 offset:1A00 Flags:E0000060
.vgc Vsize:158 RVA:6000 Psize:200 offset:1C00 Flags:E0000060
.vgc Vsize:158 RVA:7000 Psize:200 offset:1E00 Flags:E0000060
.vgc Vsize:158 RVA:8000 Psize:200 offset:2000 Flags:E0000060

This file is protected by UGCrypt
```

Conclusion

Questions?

