La sécurité antivirale est un

ECHEC

Stéfan LE BERRE
Heurs

http://www.ghostsinthestack.org

s.leberre@sysdream.com
heurs@ghostsinthestack.org

Citations :

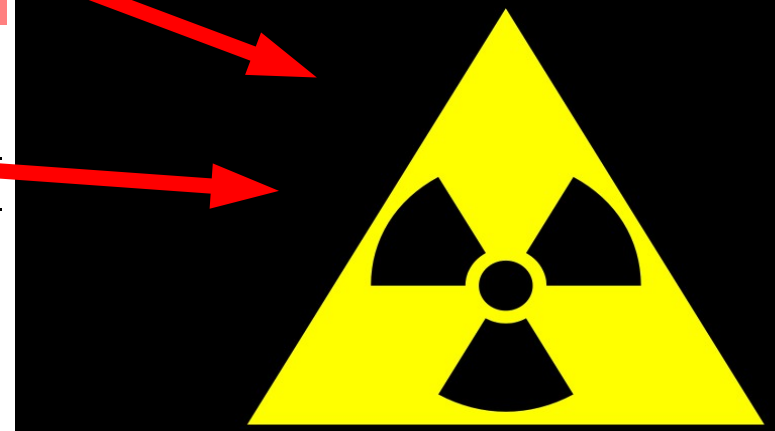
« Il vous protégera des virus, des logiciels espions, des rootkits, des pirates, de la fraude en ligne, du vol d'identité et de toutes les autres menaces Internet. »

Citations :

« Kaspersky Anti-Virus 2010 est la pierre angulaire du système de sécurité de votre PC et offre un temps réel une protection automatisée contre un grand nombre de cyber-menaces »

Protection par signature...

```
e9 02 8b fa f3 a5 8b c8 83 e1 03 f3 a4 a1 24 30
01 00 8b 4d fc 03 c3 ff 00 a1 2c 30 01 00 89 0c
18 8b 45 f8 03 d0 a1 28 30 01 00 89 14 18 a1 18
30 01 00 c7 04 18 e7 03 00 00 e9 7d 05 00 00 83
7d 1c 1a 72 19 8b 75 18 85 f6 74 12 8b 45 1c 6a
1a 33 d2 59 f7 f1 83 f8 01 89 45 10 7d 0e 8b 45
24 c7 00 06 02 00 c0 e9 63 05 00 00 e8 e5 06 00
00 50 e8 a3 fc ff ff 8b d8 85 db 75 0e 8b 45 24
c7 00 0d 00 00 c0 e9 44 05 00 00 8b 4d 1c 8b d1
c1 e9 02 33 c0 8b fe f3 ab 8b ca 83 e1 03 f3 aa
33 c0 40 39 45 10 89 5d 20 89 45 14 7c 4b 6a 1a
5f a1 20 30 01 00 ff 34 18 a1 0c 30 01 00 03 c3
50 68 00 11 01 00 8d 44 3e e6 6a 19 50 ff 15 20
20 01 00 8b 45 24 89 78 04 a1 14 30 01 00 8b 1c
18 2b d8 83 c4 14 39 5d 20 74 0e ff 45 14 8b 45
14 83 c7 1a 3b 45 10 7e b8 8b 45 24 83 20 00 e9
cb 04 00 00 83 7d 14 04 0f 82 bb 04 00 00 8b 45
10 3b c3 0f 84 b0 04 00 00 8b 00 3b c3 0f 84 00
fd ff ff 50 e8 f1 fb ff ff 3b c3 0f 84 f2 fc ff
ff 8b 0d 14 30 01 00 03 c1 8b 48 04 8b 10 89 11
```



Protection par signature...

Polymorphisme !

```
00481A54  /.  55             PUSH EBP
00481A55  |.  8BEC           MOV EBP,ESP
00481A57  |.  B9 10000000    MOV ECX,10
00481A5C  |>  6A 00          /PUSH 0
00481A5E  |.  6A 00          |PUSH 0
00481A60  |.  49             |DEC ECX
00481A61  |.^ 75 F9          \JNZ SHORT BrutusA2.00481A5C
00481A63  |.  53             PUSH EBX
00481A64  |.  8BD8           MOV EBX,EAX
00481A66  |.  33C0           XOR EAX,EAX
00481A68  |.  55             PUSH EBP
00481A69  |.  68 641E4800    PUSH BrutusA2.00481E64
00481A6E  |.  64:FF30        PUSH DWORD PTR FS:[EAX]
00481A71  |.  64:8920        MOV DWORD PTR FS:[EAX],ESP
00481A74  |.  8D55 FC        LEA EDX,DWORD PTR SS:[EBP-4]
00481A77  |.  8B83 E0020000  MOV EAX,DWORD PTR DS:[EBX+2E0]
00481A7D  |.  E8 5AE6FAFF    CALL BrutusA2.004300DC
```

Avant...

XOR

Protection par signature...

Polymorphisme !

Après !

```
00481A54  ^\78 A6           JS SHORT Packed.004819FC
00481A56    C1943D 2D2D2D47>RCL DWORD PTR SS:[EBP+EDI+472D2D2D],2D
00481A5E    47              INC EDI
00481A5F    2D 6458D47E     SUB EAX,7ED45864
00481A64    A6              CMPS BYTE PTR DS:[ESI],BYTE PTR ES:[EDI]
00481A65    F5              CMC
00481A66    1E              PUSH DS
00481A67    ED              IN EAX,DX
00481A68    78 45           JS SHORT Packed.00481AAF
00481A6A    49              DEC ECX
00481A6B    3365 2D         XOR ESP,DWORD PTR SS:[EBP+2D]
00481A6E    49              DEC ECX
00481A6F    D21D 49A40DA0   RCR BYTE PTR DS:[A00DA449],CL
00481A75  ^ 78 D1           JS SHORT Packed.00481A48
00481A77    A6              CMPS BYTE PTR DS:[ESI],BYTE PTR ES:[EDI]
00481A78    AE              SCAS BYTE PTR ES:[EDI]
00481A79    CD 2F           INT 2F
00481A7B    2D 2DC577CB     SUB EAX,CB77C52D
```

Protection par signature...

Polymorphisme !

Loader :

```
004AD000 >/$  B8 00104000    MOV EAX,Packed.00401000
004AD005  |.  B9 0090480     MOV ECX,Packed.00489000
004AD00A  |>  8330 2D        /XOR DWORD PTR DS:[EAX],2D
004AD00D  |.  83C0 01        |ADD EAX,1
004AD010  |.  3BC1           |CMP EAX,ECX
004AD012  |.^ 75 F6          \JNZ SHORT Packed.004AD00A
004AD014  |.  B8 0090480     MOV EAX,Packed.00489000
004AD019  |.  B9 00A24800    MOV ECX,Packed.0048A200
004AD01E  |>  8330 2D        /XOR DWORD PTR DS:[EAX],2D
004AD021  |.  83C0 01        |ADD EAX,1
004AD024  |.  3BC1           |CMP EAX,ECX
004AD026  |.^ 75 F6          \JNZ SHORT Packed.004AD01E
004AD028  |.  68 508E4800    PUSH Packed.00488E50
004AD02D  \.  C3             RETN
```

Protection par signature...

Ce que dit VirusTotal

Avant :

Fichier **BrutusA2.exe** reçu le **2010.05.17 12:44:08 (UTC)**
Situation actuelle: **terminé**
Résultat: **32/41 (78.05%)**

Formaté | Impression des résultats

Antivirus	Version	Dernière mise à jour	Résultat
a-squared	4.5.0.50	2010.05.10	-
AhnLab-V3	2010.05.16.00	2010.05.15	Win-Trojan/PWBrutus.679424
AntiVir	8.2.1.242	2010.05.17	SPR/Brutus
Antiy-AVL	2.0.3.7	2010.05.17	PSWTool/Win32.Brutus.gen
Authentium	5.2.0.5	2010.05.16	W32/Malware!lac5

http://www.virustotal.com/fr/analisis/49a3e574080a63b1a24980b3a775a82b5a9f7c269318662f5bbebcf21f8cefe4-1274100248

Protection par signature...

Ce que dit VirusTotal

Après :

Fichier **Packed.exe** reçu le **2010.05.17 13:00:11 (UTC)**
Situation actuelle: **terminé**
Résultat: **14/41 (34.15%)**

Formaté | Impression des résultats

Antivirus	Version	Dernière mise à jour	Résultat
a-squared	4.5.0.50	2010.05.10	Riskware.PSWTool.Win32.Brutus!IK
AhnLab-V3	2010.05.16.00	2010.05.15	-
AntiVir	8.2.1.242	2010.05.17	-
Antiy-AVL	2.0.3.7	2010.05.17	-
Authentium	5.2.0.5	2010.05.16	-

http://www.virustotal.com/fr/analisis/d7b47f7f1cd2837be9b7a7a8bc952620fd242ee00fb0c21c2cdc0591bb945103-1274101211

Protection par signature...

Metamorphisme

```
XOR EAX, EAX
MOV EAX, 0
SUB EAX, EAX
SHR EAX, 32
SHL EAX, 32
AND EAX, 0
```

Protection par signature...

Metamorphisme

Seul la détection comportementale peut fonctionner

et encore ...

On attaque les Anti-virus !!!

Sécurité des Antivirus

Objectif kernel !

Fuzzer les drivers des antivius

- Avantages
- Inconvénients

Sécurité des Antivirus

Objectif kernel !

Avantages :

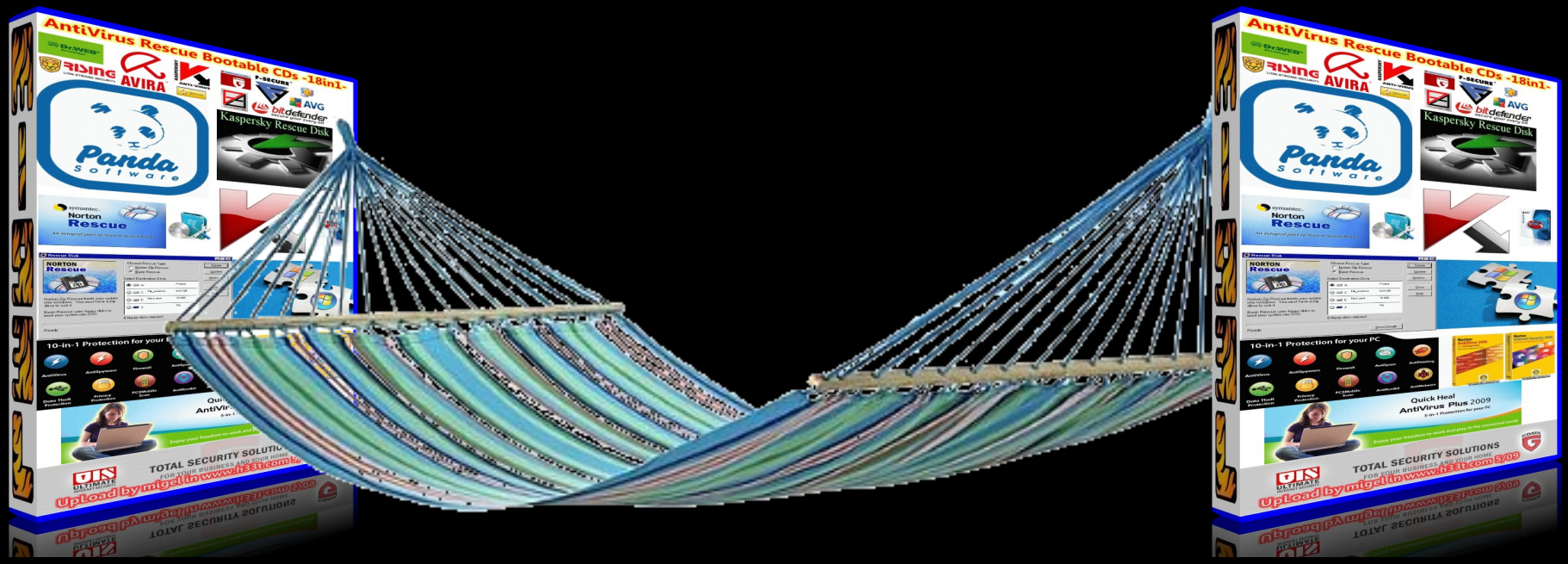
- Attaque le ring0, soit le kernel (donc élévation de privilèges)

Sécurité des Antivirus

Objectif kernel !

Avantages :

- Fuzzing en local, donc possibilité de s'adapter à l'environnement



Sécurité des Antivirus

Objectif kernel !

Inconvénients :

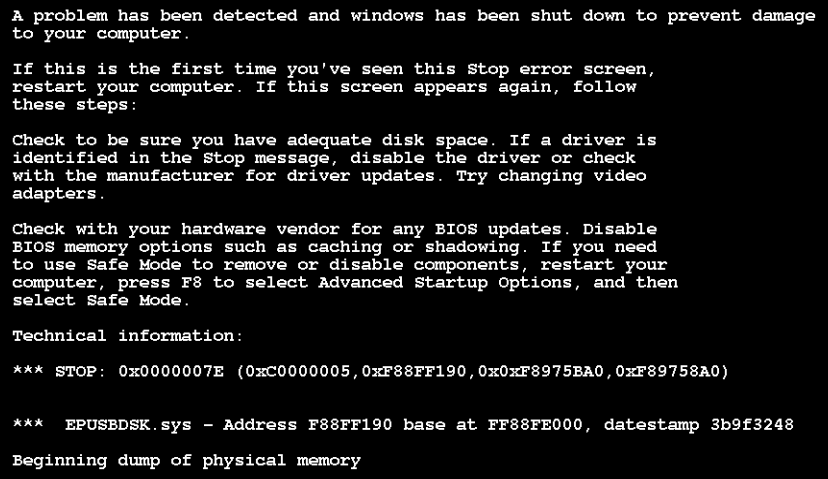
- Pas de remote :'(

Sécurité des Antivirus

Objectif kernel !

Inconvénients :

- Exploit pas stable == BSOD

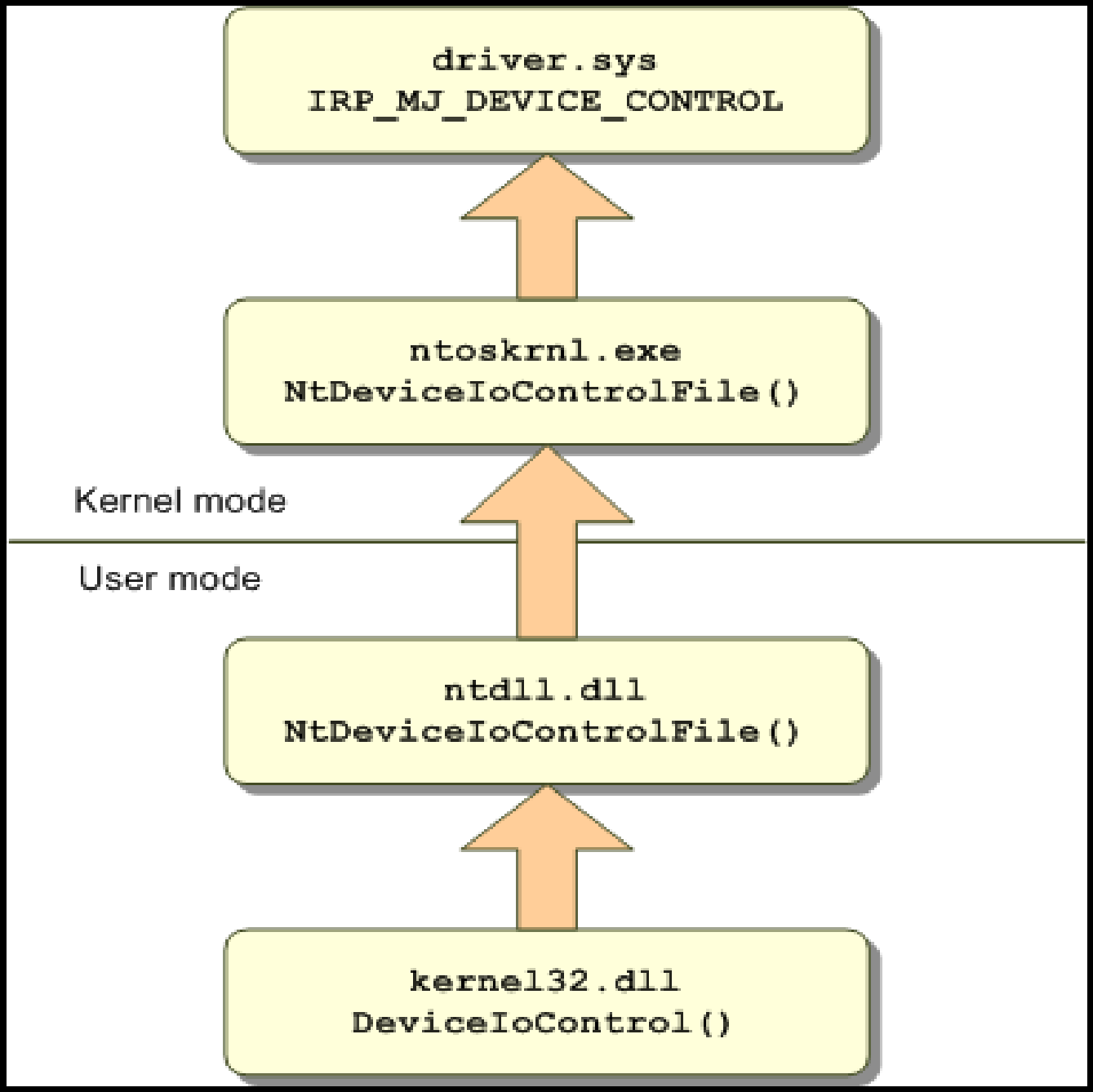


IOCTL_FUZZER

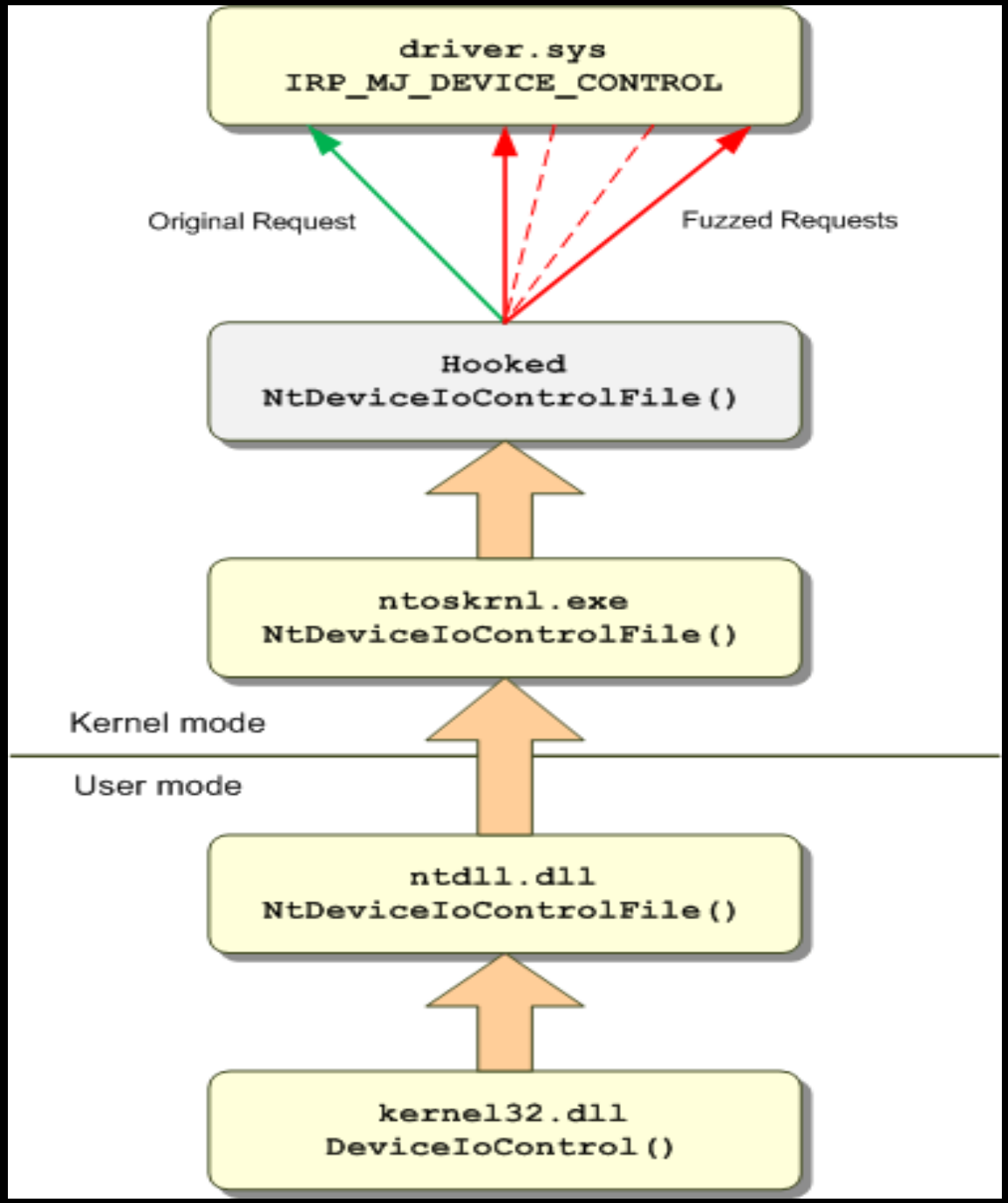
=> IOCT_FUZZER (créé par Oleksyuk Dmitry)

Fuzz les communications entre les programmes et les drivers

IOCTL_FUZZER



IOCTL_FUZZER



IOCTL_FUZZER

Actuellement (v1.1)

Fonctionnalités :

- Déréférence les pointeurs INPUT et OUTPUT

- Augmente la taille totale des buffers

- Fuzz 20 fois les buffers de facon aléatoire

IOCTL_FUZZER

Actuellement (v1.1)

Fuzzing (origine) :

```
0267b600 : 00000001 00000001 00000001 00000007
0267b610 : 00000001 00000001 00000001 004d4f43
0267b620 : 00455845 004c4c44 00535953 00524353
0267b630 : 004c5043 003f564f 00445856 00363833
0267b640 : 004e4942 00544142 00444d43 003f4f44
0267b650 : 003f4c58 003f5050 002a5448 0054484d
0267b660 : 00504c48 003f4843 007d2a7b 00505341
0267b670 : 2a414c43 53534300 464e4900 2a534a00
0267b680 : 4b4e4c00 3f534d00 58434f00 46445000
0267b690 : 46495000 3f4f5000 43525000 46545200
```

IOCTL_FUZZER

Actuellement (v1.1)

Fuzzing (random, 20x) :

```
0267b600 : 73d1dde9 24135758 cd62b301 35a96b72
0267b610 : 45c3745d cfae802b ed77fbb8 ecc2f16d
0267b620 : a6409255 5b608056 7b2e40db c250e10c
0267b630 : 284fc4b1 bab9b00d 2fce932c 42d9380b
0267b640 : 72b21bd3 4646eb4c dfcc6996 4060e991
0267b650 : ce1fa555 eda7ae0b 4f918340 90059feb
0267b660 : f4cf7bb7 8b0c9a64 9b99f867 d673970a
0267b670 : 591dbc4c 2d54989b ddb9c19d 8121eaac
0267b680 : 199b21f5 c30a1e03 7c618cb1 eb3e06f0
0267b690 : 7cebbd74 aef8a969 25cdcda9 f47297c9
```

IOCTL_FUZZER

Actuellement (v1.1)

Problèmes :

- Peu de chance d'appeler des sous routines (faible couverture de code)

- Pas de gestion des chaines de caractères

- Pas de reconnaissance des pointeurs (pas de fuzzing des sous structures)

IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des DWORD :

```
0267b600 : 00000001 00000001 00000001 00000007
0267b610 : 00000001 00000001 00000001 004d4f43
0267b620 : 00455845 004c4c44 00535953 00524353
0267b630 : 004c5043 003f564f 00445856 00363833
0267b640 : 004e4942 00544142 00444d43 003f4f44
0267b650 : 003f4c58 003f5050 002a5448 0054484d
0267b660 : 00504c48 003f4843 007d2a7b 00505341
0267b670 : 2a414c43 53534300 464e4900 2a534a00
0267b680 : 4b4e4c00 3f534d00 58434f00 46445000
0267b690 : 46495000 3f4f5000 43525000 46545200
```

IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des DWORD :

```
0267b600 : 73d1dde9 00000001 00000001 00000007
0267b610 : 00000001 00000001 00000001 004d4f43
0267b620 : 00455845 004c4c44 00535953 00524353
0267b630 : 004c5043 003f564f 00445856 00363833
0267b640 : 004e4942 00544142 00444d43 003f4f44
0267b650 : 003f4c58 003f5050 002a5448 0054484d
0267b660 : 00504c48 003f4843 007d2a7b 00505341
0267b670 : 2a414c43 53534300 464e4900 2a534a00
0267b680 : 4b4e4c00 3f534d00 58434f00 46445000
0267b690 : 46495000 3f4f5000 43525000 46545200
```

IOCTL_FUZZER

En dev... (v1.2)

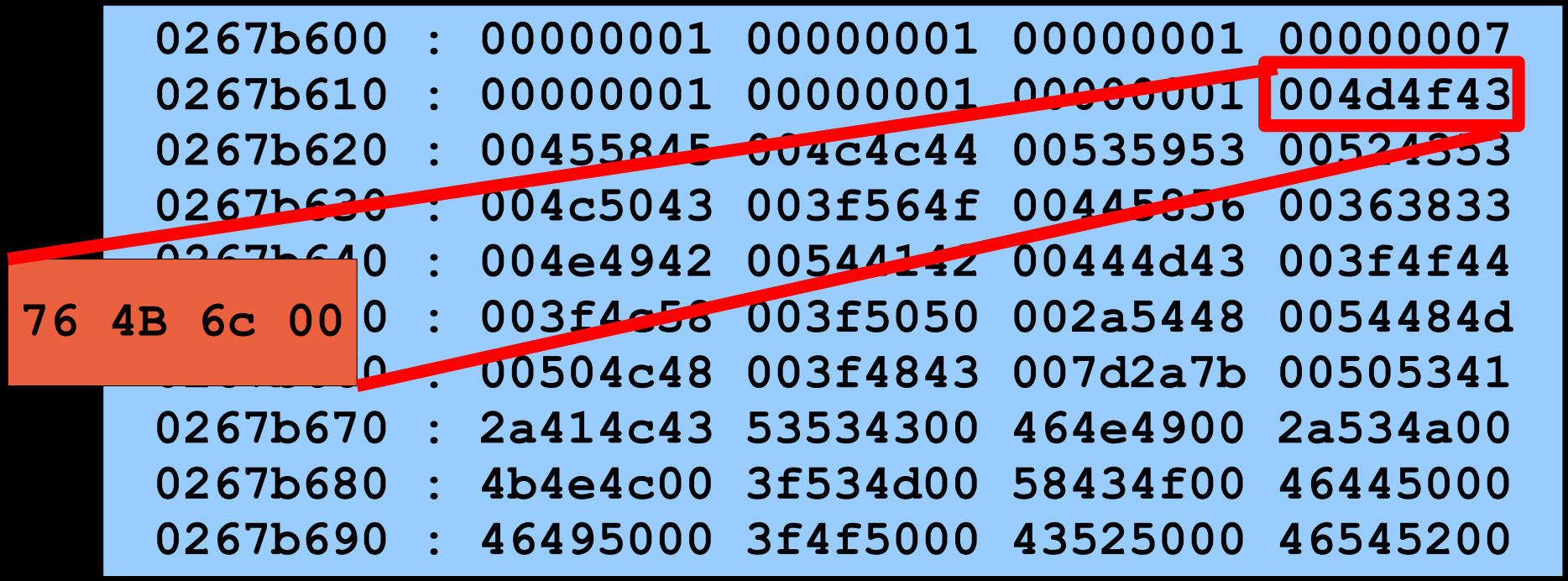
Fuzzing des DWORD :

```
0267b600 : 00000001 24135758 00000001 00000007
0267b610 : 00000001 00000001 00000001 004d4f43
0267b620 : 00455845 004c4c44 00535953 00524353
0267b630 : 004c5043 003f564f 00445856 00363833
0267b640 : 004e4942 00544142 00444d43 003f4f44
0267b650 : 003f4c58 003f5050 002a5448 0054484d
0267b660 : 00504c48 003f4843 007d2a7b 00505341
0267b670 : 2a414c43 53534300 464e4900 2a534a00
0267b680 : 4b4e4c00 3f534d00 58434f00 46445000
0267b690 : 46495000 3f4f5000 43525000 46545200
```

IOCTL_FUZZER

En dev... (v1.2)

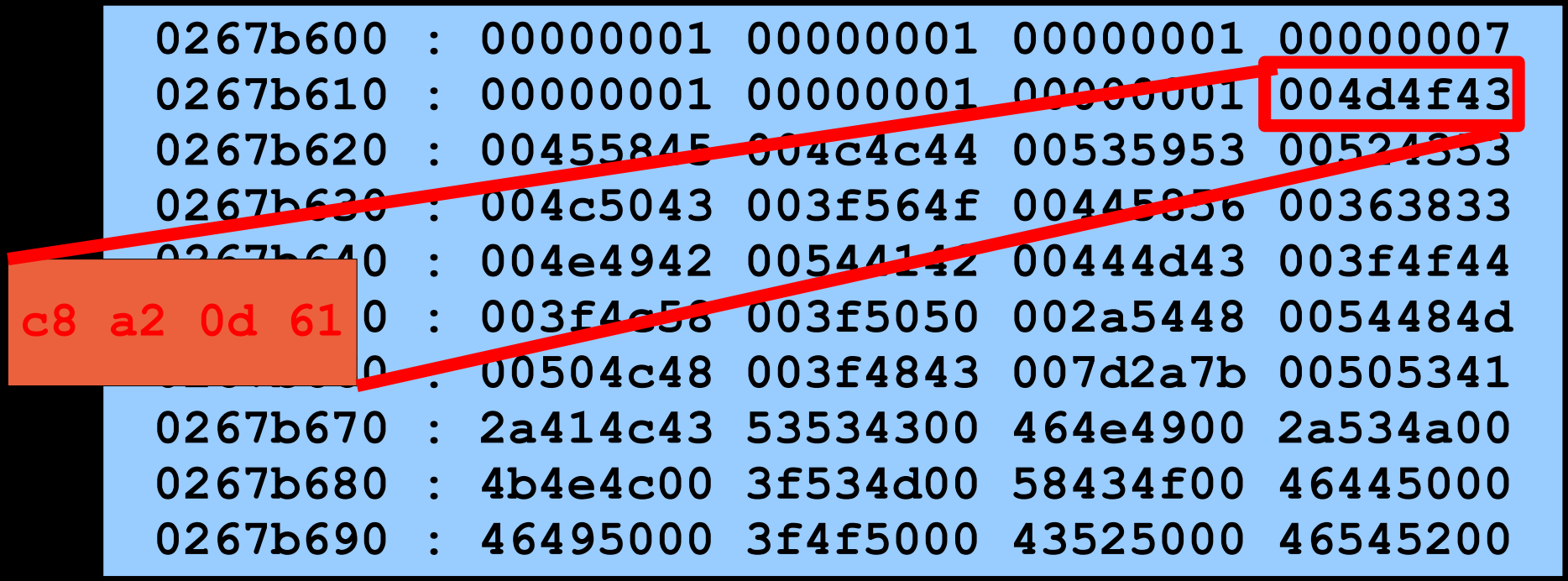
Fuzzing des datas pointées :



IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des datas pointées :



IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des strings :

```
00ee38d0 : 465d1683 d53ebbbe 783d71c8 059fa0ea
00ee38e0 : c022650c 918a2664 d706918c 8d8aea14
00ee38f0 : b4a91048 c8956809 5972356e c277c79e
00ee3900 : 216d9a59 61776c41 61207379 776f6c6c
00ee3910 : 6d6f6320 206e6f6d 6c707061 74616369
00ee3920 : 736e6f69 63636120 20737365 74206f74
00ee3930 : 6e206568 6f777465 00006b72 00000000
00ee3940 : 00000000 00000000 00000000 00000000
00ee3950 : 00000000 00000000 00000000 00000000
00ee3960 : 00000000 00000000 00000000 00000000
```

IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des strings :

```
00ee38d0 : 465d1683 d53ebbbe 783d71c8 059fa0ea
00ee38e0 : c022650c 918a2664 d706918c 8d8aea14
00ee38f0 : b4a91048 c8956809 5972356e c277c79e
00ee3900 : 216d9a59 41414141 41414141 41414141
00ee3910 : 41414141 41414141 41414141 41414141
00ee3920 : 41414141 41414141 41414141 41414141
00ee3930 : 41414141 41414141 41414141 41414141
00ee3940 : 41414141 41414141 41414141 41414141
00ee3950 : 41414141 41414141 41414141 41414141
00ee3960 : 41414141 41414141 41414141 41414141
```

IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des strings unicode :

```
4f 00 00 00 03 00 92 00  40 00 00 00 00 00 00 00
00 00 04 00 00 2a 00 00  00 5c 00 44 00 65 00 76
00 69 00 63 00 65 00 5c  00 48 00 61 00 72 00 64
00 64 00 69 00 73 00 6b  00 30 00 5c 00 44 00 52
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

IOCTL_FUZZER

En dev... (v1.2)

Fuzzing des strings unicode :

```
4f 00 00 00 03 00 92 00  40 00 00 00 00 00 00 00
00 00 04 00 00 2a 00 00  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
00 41 00 41 00 41 00 41  00 41 00 41 00 41 00 41
```

IOCTL_FUZZER

En dev... (v1.2)

Ajouts :

- Fuzz chaque DWORD séparément
- Fuzz les Datas pointées
- Agrandit les strings (unicode compris)

IOCTL_FUZZER

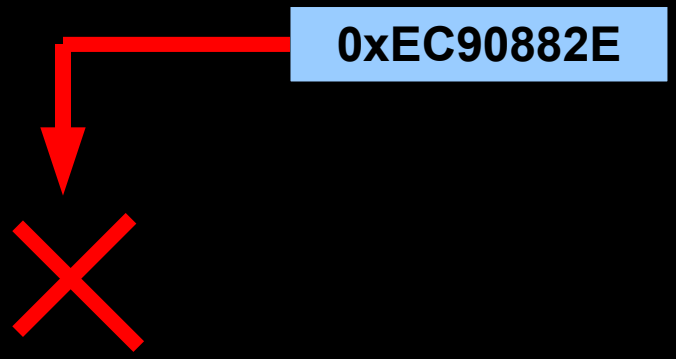
Et sur les Anti-virus / Firewalls ?

On attaque donc les drivers propriétaires

IOCTL_FUZZER

En action !

Vulnérabilité dans GMER :

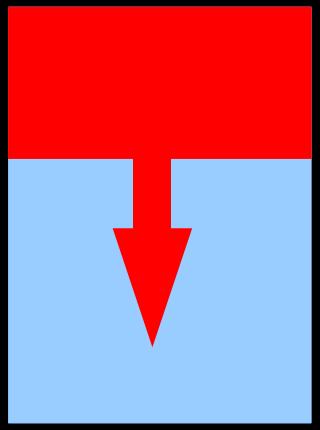


Kernel pointer dereferencement

IOCTL_FUZZER

En action !

Vulnérabilité dans avast! :

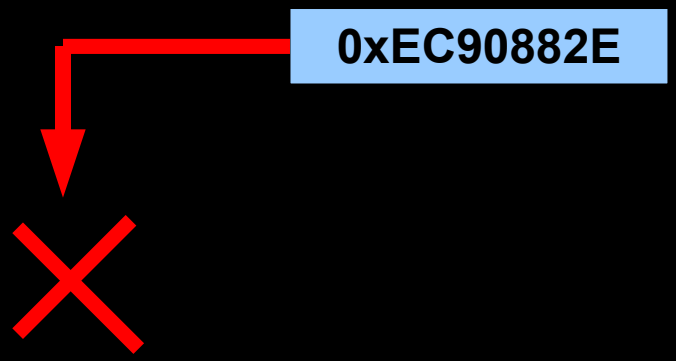


Buffer Overflow
Local privilege escalation

IOCTL_FUZZER

En action !

Vulnérabilité dans kaspersky :

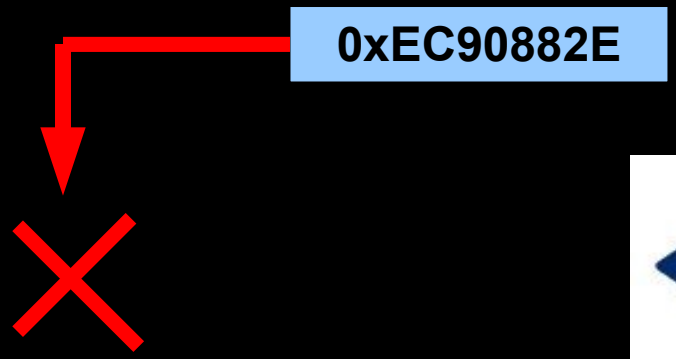


Kernel pointer dereferencement

IOCTL_FUZZER

En action !

Vulnérabilité dans kerio :

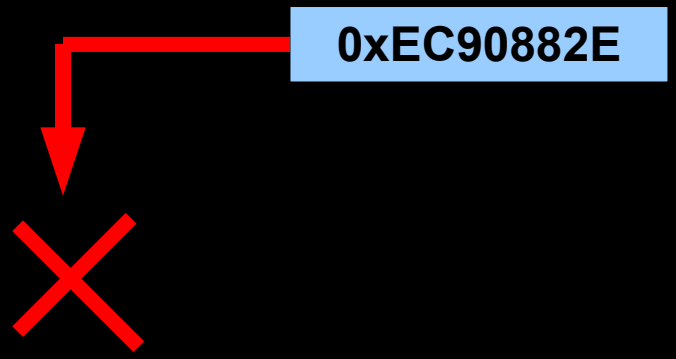


Kernel pointer dereferencement

IOCTL_FUZZER

En action !

Vulnérabilité dans Look 'n' Stop :

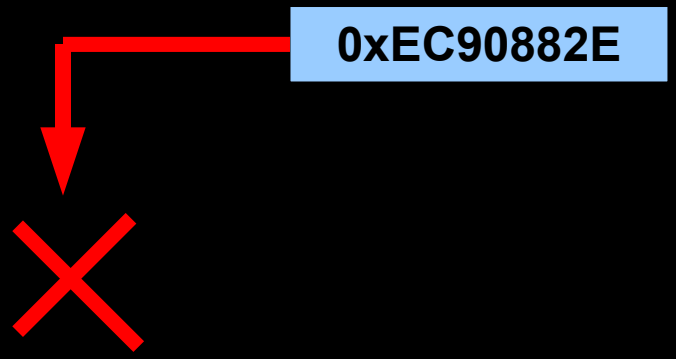


Kernel pointer dereferencement

IOCTL_FUZZER

En action !

Vulnérabilité dans BifDefender :

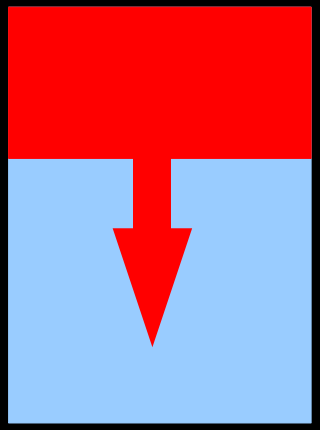


Kernel pointer dereferencement

IOCTL_FUZZER

En action !

Vulnérabilité dans Panda :

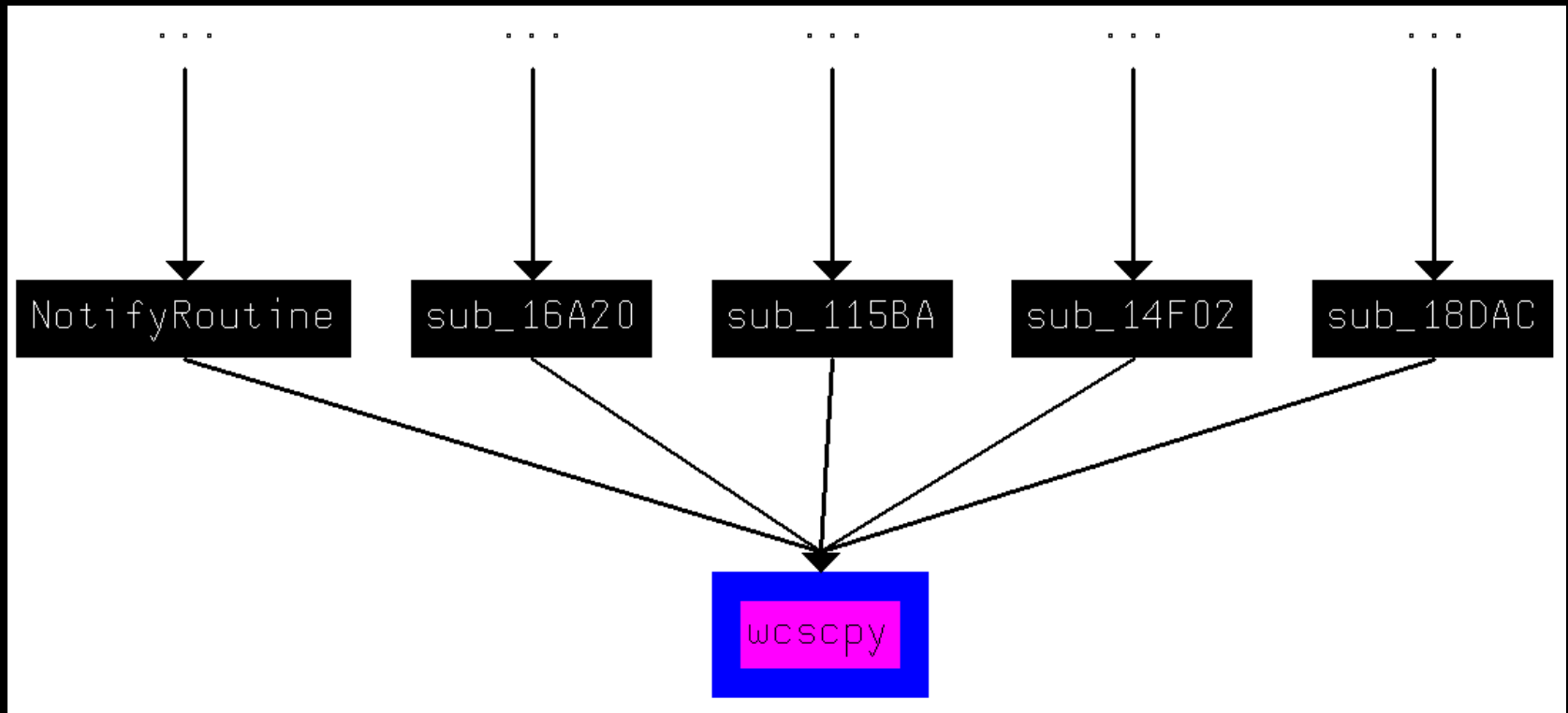


Kernel heap overflow

IOCTL_FUZZER

Toujours Panda !

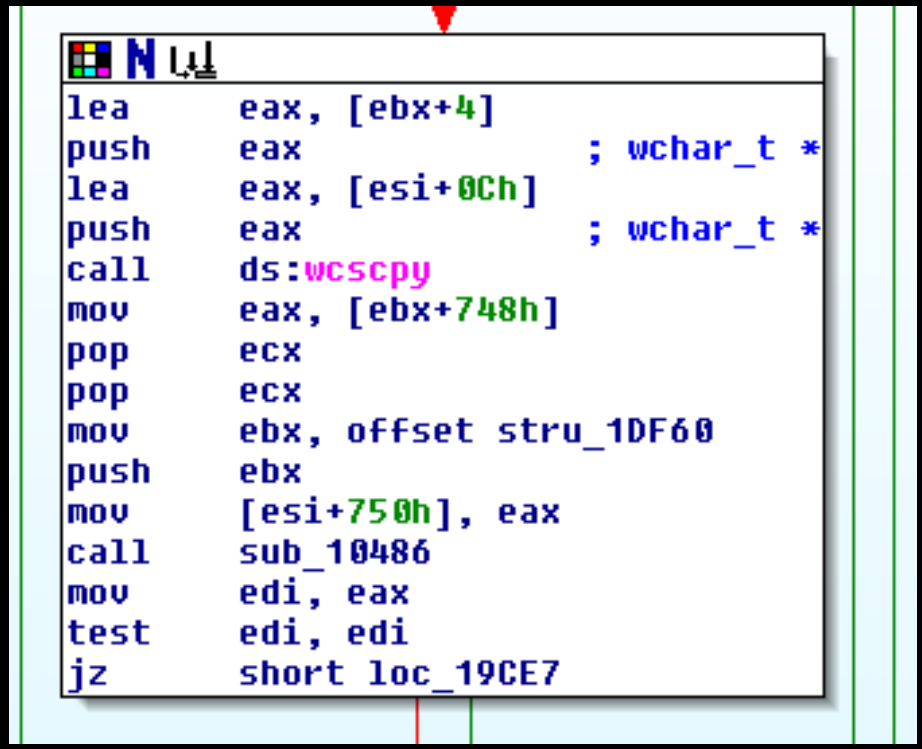
En cherchant un peu plus on trouve :



IOCTL_FUZZER

Toujours Panda !

Dans la fonction de gestion IOCTL :



```
lea     eax, [ebx+4]
push    eax             ; wchar_t *
lea     eax, [esi+0Ch]
push    eax             ; wchar_t *
call    ds:wcscpy
mov     eax, [ebx+748h]
pop     ecx
pop     ecx
mov     ebx, offset stru_1DF60
push    ebx
mov     [esi+750h], eax
call    sub_10486
mov     edi, eax
test    edi, edi
jz      short loc_19CE7
```

IOCTL_FUZZER

Toujours Panda !

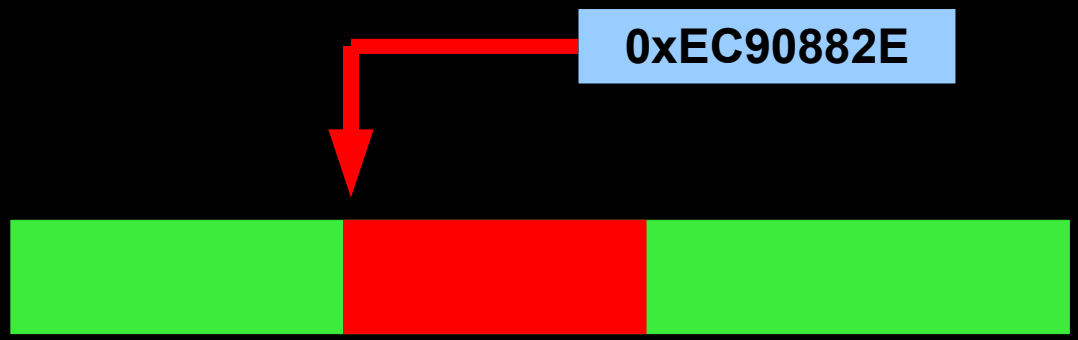
Et on contrôle les datas ainsi que le pointeur de destination !

Donc bon....

IOCTL_FUZZER

2ème édition !

Vulnérabilité dans Panda :



Kernel pointer dereferencement
Privilège escalation

Bilan

Encore une victoire de cannard !

Trop peu de contrôle sur la sécurité des anti-virus

Questions ?

Merci pour votre attention

RDV au bar

Et surtout, passez un agréable soirée

Greetz to : Virtualabs, cde, CrashFR, Trance, Mysterie, Sh4ka et tous les autres !