CoRIIN 2017

Lille - 23/01/2017

Détection *post-mortem* de « bootkits »

Intervenants

- Sébastien CHAPIRON sebastien.chapiron@ssi.gouv.fr
- Thierry GUIGNARD thierry.guignard@ssi.gouv.fr

- Spécialistes en investigation numérique - Bureau Réponse aux Incidents de l'ANSSI (Pôle Analyse Système)

Plan

1/ Besoins métier
2/ Bootkits
3/ Objectifs
4/ Chaîne de démarrage Windows
5/ Vérifications
6/ Outillage

Besoins métier

- Analyse de matériels potentiellement compromis.
- Mise en place de procédures d'analyse :
  - applicables pour une analyse unitaire et sur un parc ;
  - permettant d'identifier les malwares connus, inconnus et atypiques.

Bootkits

- **« Bootkit » = « Boot » + « Rootkit »**

- Aucun fichier sur le système de fichiers :
  - Secteurs de démarrage et espaces non partitionnés ;
  - Echappe plus facilement aux analyses.

- Code malveillant utilisant les mécanismes de démarrage pour :
  - Garantir son exécution ;
  - Assurer sa persistance.

Bootkits

- Contournement des mécanismes de sécurité :
  - *Code Integrity* ;
  - *PatchGuard* ;
  - Etc…
- Chargement du *rootkit* :
  - Dissimule sa présence et les activités malveillantes ;
  - Contrôle complet du poste compromis.

Objectifs

- Présentation d'une méthodologie de détection des « bootkits ».
- Mise à disposition d'un outil facilitant les recherches.

Périmètre

- Analyse « *post-mortem* ».
- Architecture s'appuyant sur un« BIOS » et un « MBR » classiques.
- Méthodologie applicable aux mécanismes de démarrage de Windows et partiellement applicable à tous les OS (MBR).

Chaîne de démarrage
BIOS

1. Alimentation électrique
2. POST – Power On Self Test
3. Identification du disque de démarrage
4. Chargement du code du MBR

Chaîne de démarrage Windows

Boot Sector (VBR) + IPL

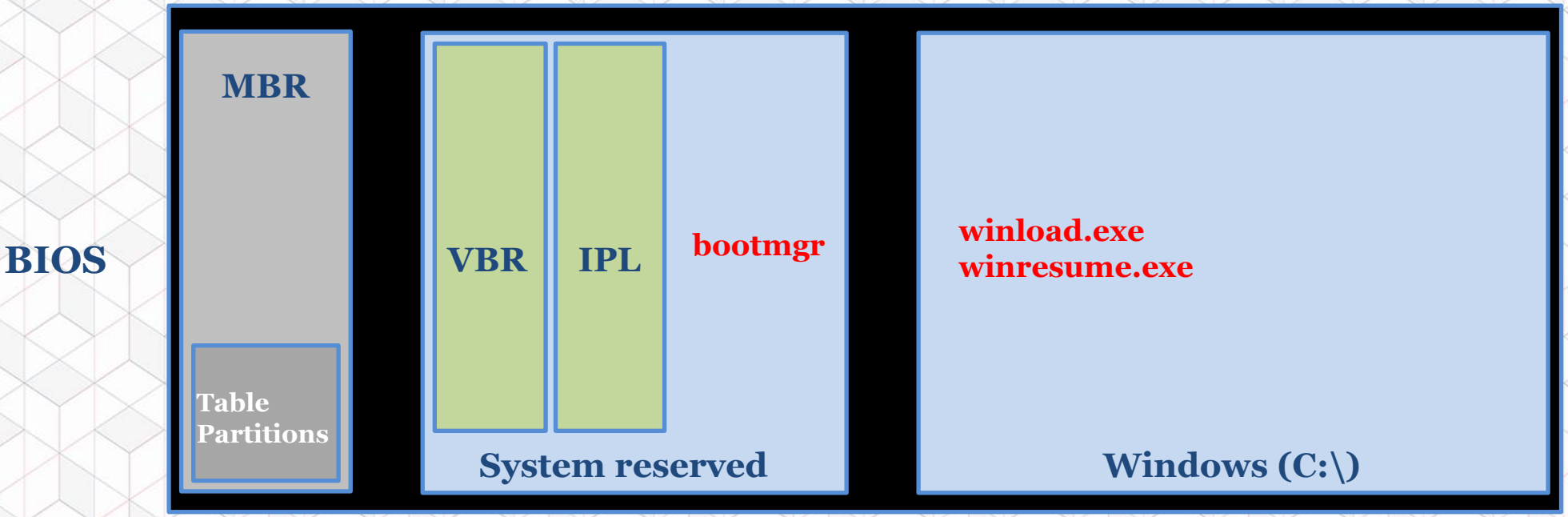
5
- Parcours de la table des partitions
- Identification de la partition active (0x80)

6
- Chargement du code du VBR
- Identification de l'IPL

7
- Chargement du code de l'IPL
- Lancement du *bootloader* (« ntldr » ou « bootmgr »)

8
- Démarrage de Windows (winload.exe, pilotes, noyau…)

Chaîne de démarrage Windows



DISQUE DUR DE DEMARRAGE (Win7 et suiv.)

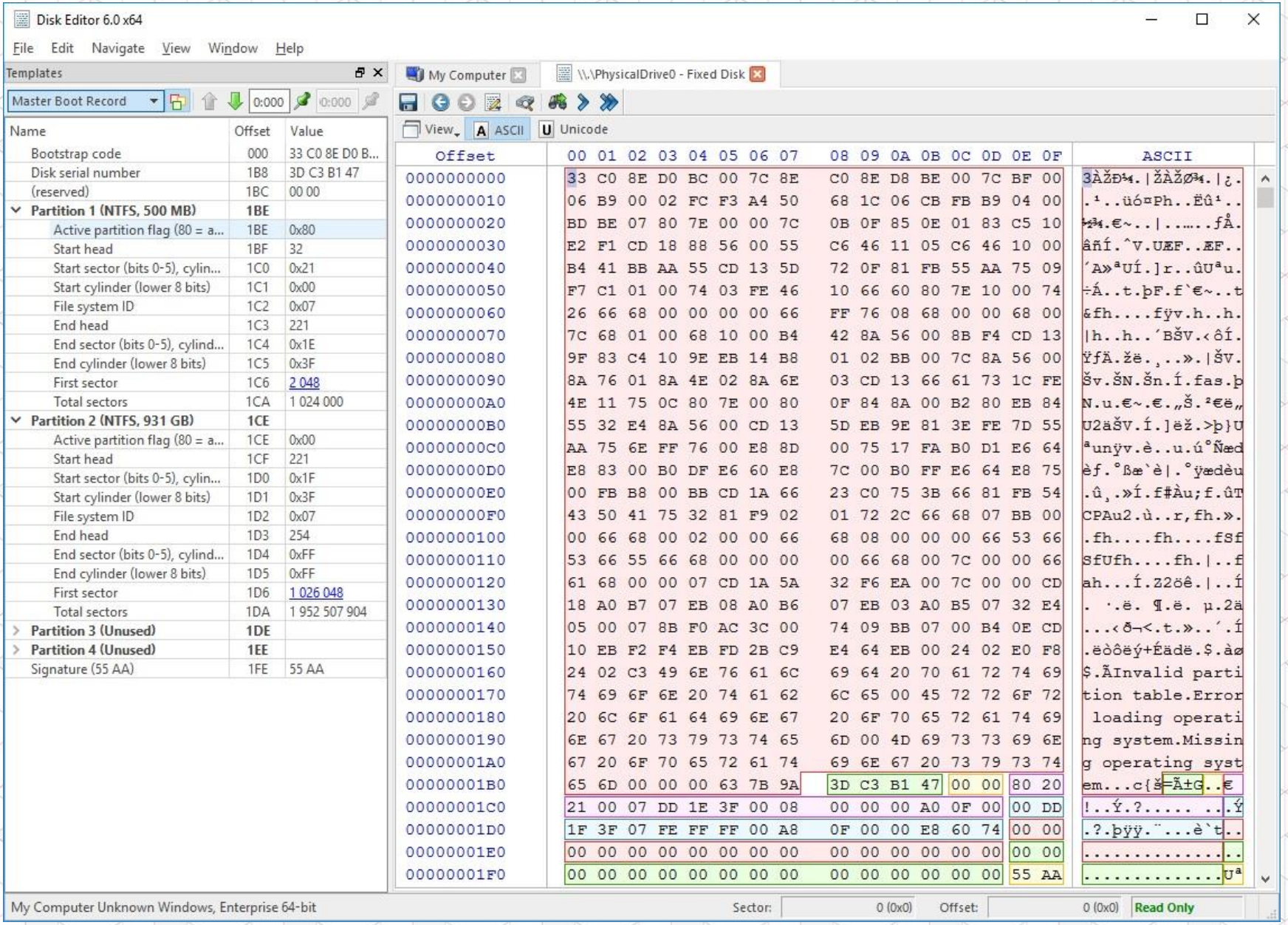
Analyses

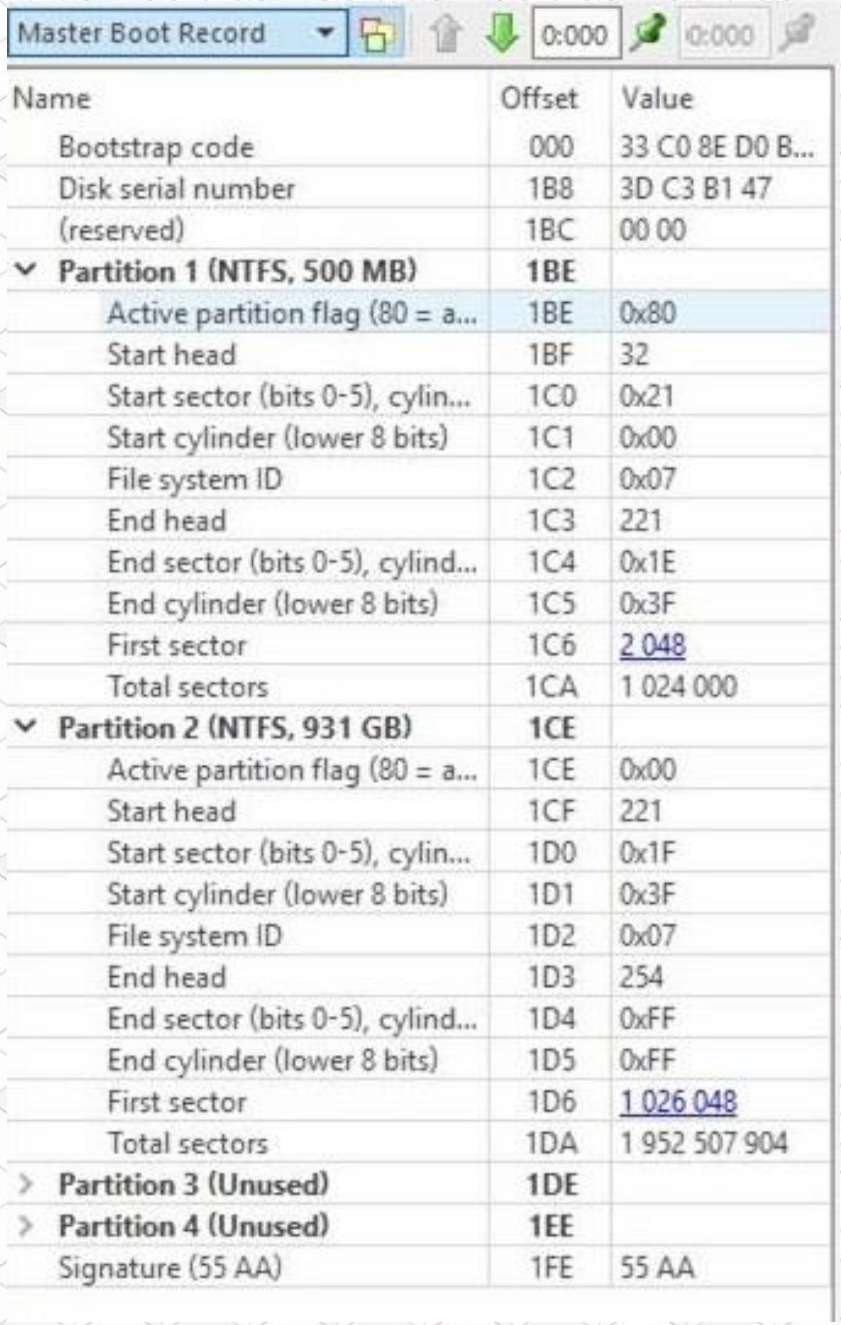
- MBR
  - Structure
  - Vérifications
- VBR
  - Structure
  - Vérifications
- IPL
  - Structure
  - Vérifications

MBR - Structure

Master Boot Record - 1er secteur du disque dur de démarrage

Offset (décimal)	Taille (octets)	Valeur
0 -> 439	440	Code du MBR
440 -> 443	4	Identifiant du disque
444 -> 445	2	Réservé
446 -> 509	64	Table des partitions
510 -> 511	2	Signature « 55 AA »


Disk Editor 6.0 x64
File Edit Navigate View Window Help
Templates
Master Boot Record
0:000
0:000
Name Offset Value
Bootstrap code 000 33 C0 8E D0 B...
Disk serial number 1B8 3D C3 B1 47
(reserved) 1BC 00 00
Partition 1 (NTFS, 500 MB) 1BE
Active partition flag (80 = a... 1BE 0x80
Start head 1BF 32
Start sector (bits 0-5), cylin... 1C0 0x21
Start cylinder (lower 8 bits) 1C1 0x00
File system ID 1C2 0x07
End head 1C3 221
End sector (bits 0-5), cylind... 1C4 0x1E
End cylinder (lower 8 bits) 1C5 0x3F
First sector 1C6 2 048
Total sectors 1CA 1 024 000
Partition 2 (NTFS, 931 GB) 1CE
Active partition flag (80 = a... 1CE 0x00
Start head 1CF 221
Start sector (bits 0-5), cylin... 1D0 0x1F
Start cylinder (lower 8 bits) 1D1 0x3F
File system ID 1D2 0x07
End head 1D3 254
End sector (bits 0-5), cylind... 1D4 0xFF
End cylinder (lower 8 bits) 1D5 0xFF
First sector 1D6 1 026 048
Total sectors 1DA 1 952 507 904
Partition 3 (Unused) 1DE
Partition 4 (Unused) 1EE
Signature (55 AA) 1FE 55 AA
My Computer
\\.\PhysicalDrive0 - Fixed Disk
View
ASCII
Unicode
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
0000000000 33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00 3ÀŽÐ¼.|ŽÀŽØ¾.|¿.
0000000010 06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00 .¹..üó¤Ph..Ëû¹..
0000000020 BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10 ½¾.€~..|..…..ƒÅ.
0000000030 E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00 âñÍ.ˆV.UÆF..ÆF..
0000000040 B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09 ´A»ªUÍ.]r..ûUªu.
0000000050 F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74 ÷Á..t.þF.f`€~..t
0000000060 26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00 &fh....fÿv.h..h.
0000000070 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13 |h..h..´BŠV.‹ôÍ.
0000000080 9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00 ŸƒÄ.žë.¸..».|ŠV.
0000000090 8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE Šv.ŠN.Šn.Í.fas.þ
00000000A0 4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84 N.u.€~.€.„Š.²€ë„
00000000B0 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55 U2äŠV.Í.]ëž.>þ}U
00000000C0 AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64 ªunÿv.è..u.ú°Ñæd
00000000D0 E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75 èf.°ßæ`è|.°ÿædèu
00000000E0 00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54 .û¸.»Í.f#Àu;f.ûT
00000000F0 43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00 CPAu2.ù..r,fh.».
0000000100 00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66 .fh....fh....fSf
0000000110 53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66 SfUfh....fh.|..f
0000000120 61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD ah...Í.Z2öê.|..Í
0000000130 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4 . ·.ë. ¶.ë. µ.2ä
0000000140 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD ...‹ð¬<.t.»..´.Í
0000000150 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8 .ëòôëý+Éädë.$.àø
0000000160 24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69 $.ÃInvalid parti
0000000170 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72 tion table.Error
0000000180 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69 loading operati
0000000190 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E ng system.Missin
00000001A0 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 g operating syst
00000001B0 65 6D 00 00 00 63 7B 9A 3D C3 B1 47 00 00 80 20 em...c{š=Ã±G..€
00000001C0 21 00 07 DD 1E 3F 00 08 00 00 00 A0 0F 00 00 DD !..Ý.?..... ...Ý
00000001D0 1F 3F 07 FE FF FF 00 A8 0F 00 00 E8 60 74 00 00 .?.þÿÿ.¨...è`t..
00000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA ....Uª
My Computer Unknown Windows, Enterprise 64-bit
Sector: 0 (0x0)
Offset: 0 (0x0)
Read Only



Name	Offset	Value
Bootstrap code	000	33 C0 8E D0 B...
Disk serial number	1B8	3D C3 B1 47
(reserved)	1BC	00 00
Partition 1 (NTFS, 500 MB)	**1BE**	
Active partition flag (80 = a...	1BE	0x80
Start head	1BF	32
Start sector (bits 0-5), cylin...	1C0	0x21
Start cylinder (lower 8 bits)	1C1	0x00
File system ID	1C2	0x07
End head	1C3	221
End sector (bits 0-5), cylind...	1C4	0x1E
End cylinder (lower 8 bits)	1C5	0x3F
First sector	1C6	2 048
Total sectors	1CA	1 024 000
Partition 2 (NTFS, 931 GB)	**1CE**	
Active partition flag (80 = a...	1CE	0x00
Start head	1CF	221
Start sector (bits 0-5), cylin...	1D0	0x1F
Start cylinder (lower 8 bits)	1D1	0x3F
File system ID	1D2	0x07
End head	1D3	254
End sector (bits 0-5), cylind...	1D4	0xFF
End cylinder (lower 8 bits)	1D5	0xFF
First sector	1D6	1 026 048
Total sectors	1DA	1 952 507 904
Partition 3 (Unused)	**1DE**	
Partition 4 (Unused)	**1EE**	
Signature (55 AA)	1FE	55 AA

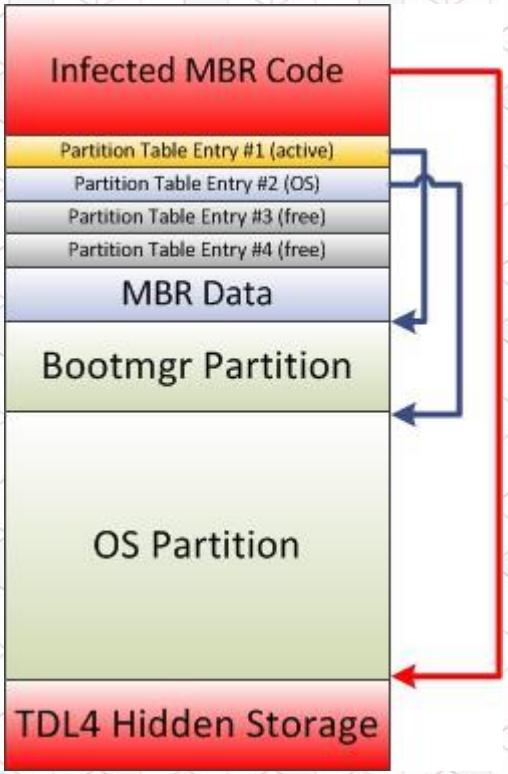
Analyses

- MBR
  - Structure
  - Vérifications
- VBR
  - Structure
  - Vérifications
- IPL
  - Structure
  - Vérifications

MBR – Vérifications du code

- Condensat
  - MBR complet (512 octets) => Echec
  - Section de code (440 octets) => Exploitable
    - Localisation linguistique des messages d'erreurs ;
    - Versions de Windows, solutions de chiffrement, etc.
- Heuristiques :
  - Interruptions suspectes ;
  - Saut en dehors du premier secteur.

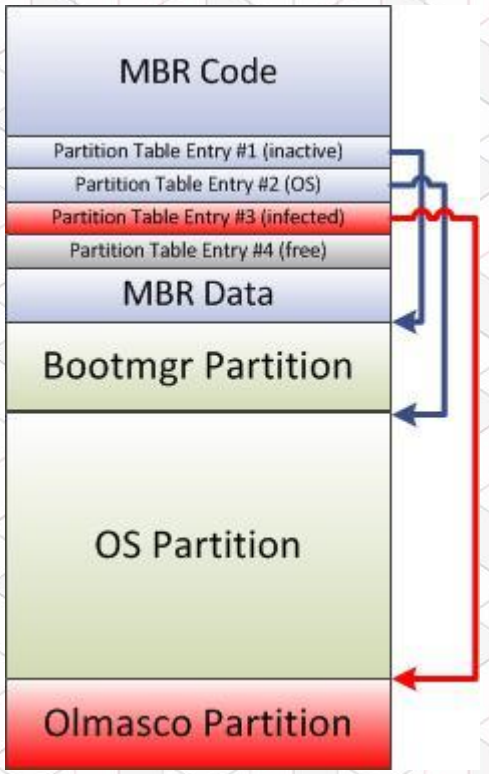
Exemple : TDL4



MBR – Vérifications de la table des partitions

- Rappel :
  - NT5 : une seule partition ;
  - NT6.1 : « *system reserved* » + OS.
- Partition active :
  - NT5 : secteur 63 ;
  - NT6 : secteur 2048 ;
  - Vérification du VBR.

Exemple : Olmasco



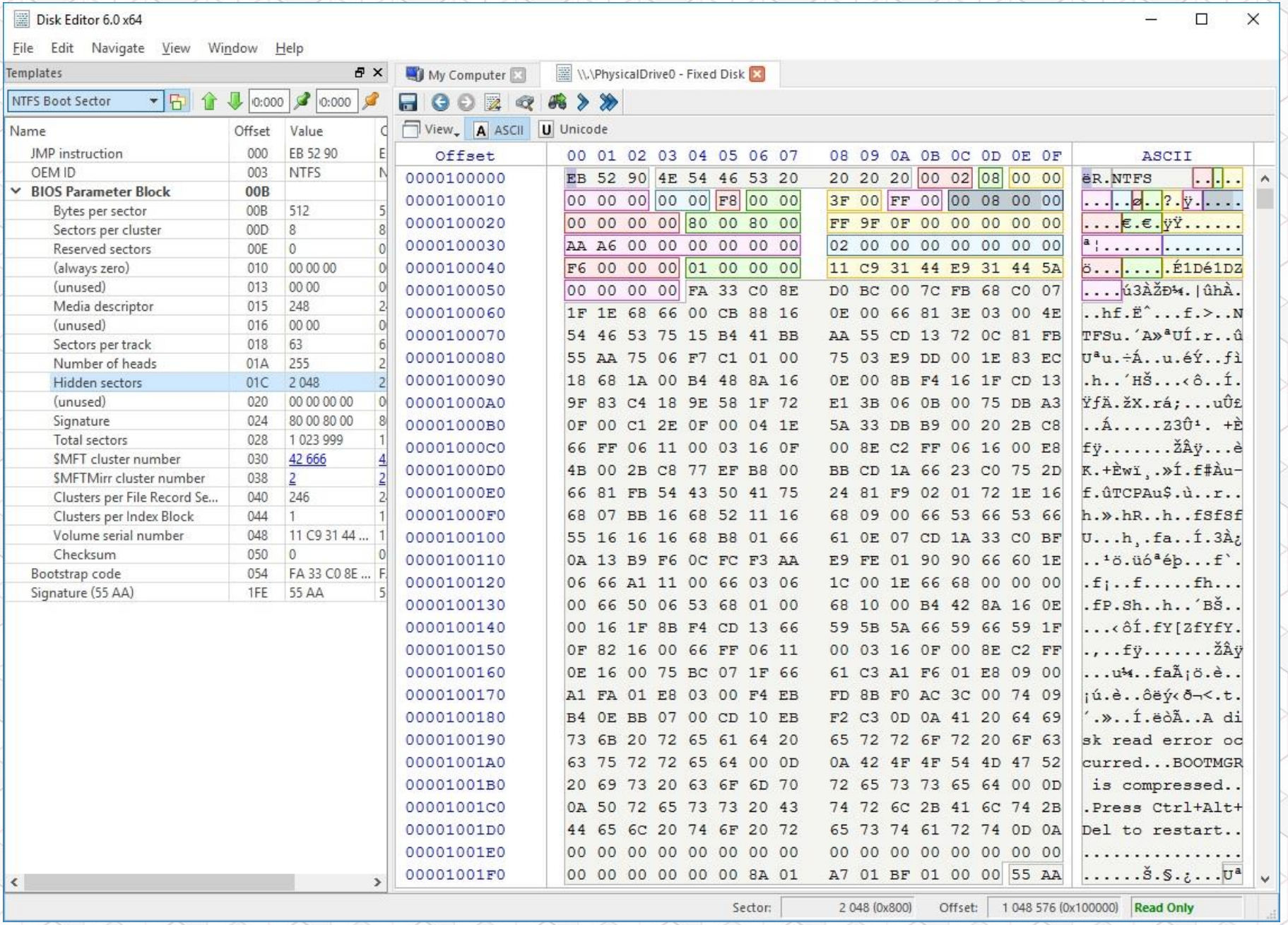
Analyses

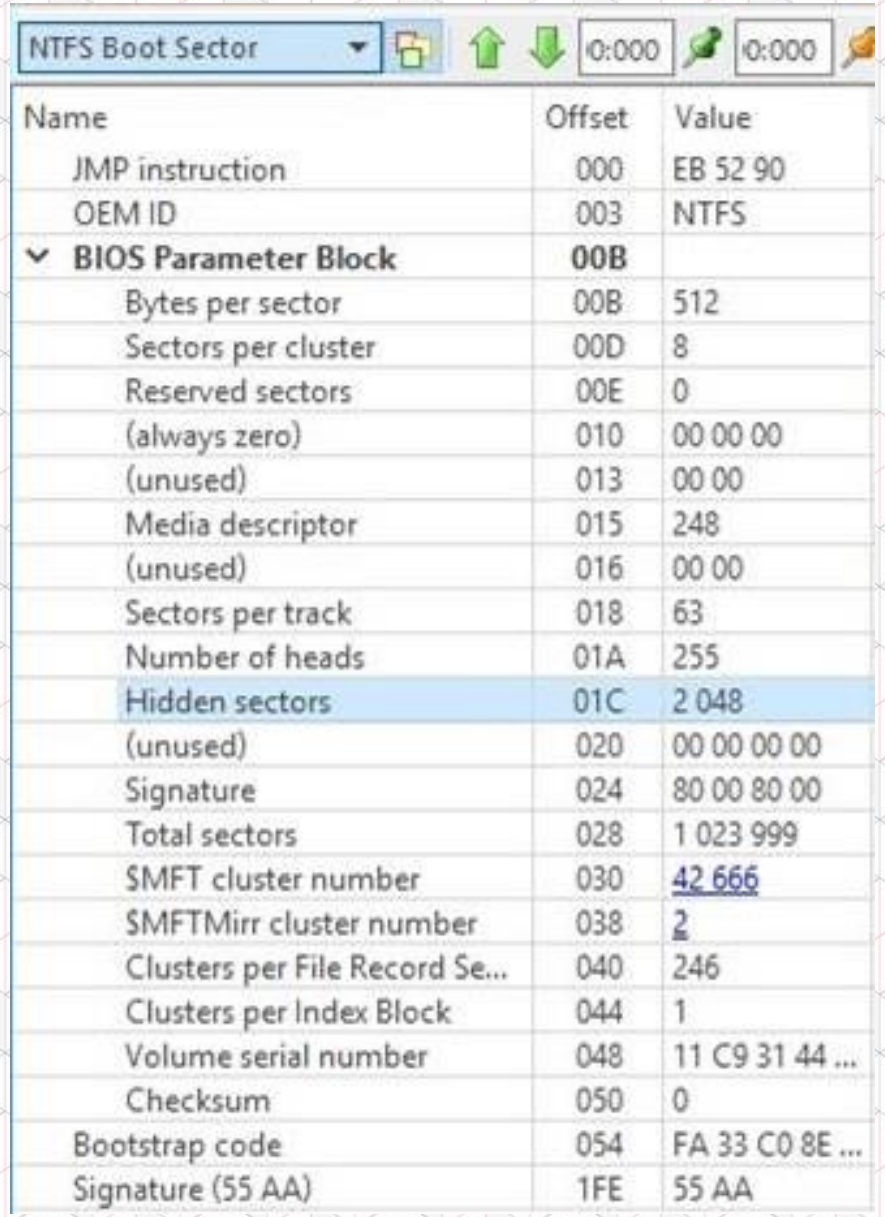
- MBR
  - Structure
  - Vérifications
- VBR
  - Structure
  - Vérifications
- IPL
  - Structure
  - Vérifications

VBR - Structure

Volume Boot Record (Boot Sector) - 1er secteur d'une partition NTFS.

Offset (décimal)	Taille (octets)	Valeur
0 -> 02	03	Instruction « Jmp »
03 -> 10	08	« NTFS »
11 -> 83	73	Bios Parameter Block
84 -> 509	426	Code du VBR
510 -> 511	02	Signature « 55 AA »


Disk Editor 6.0 x64
File Edit Navigate View Window Help
Templates
NTFS Boot Sector
0:000
0:000
Name Offset Value
JMP instruction 000 EB 52 90
OEM ID 003 NTFS
BIOS Parameter Block 00B
Bytes per sector 00B 512
Sectors per cluster 00D 8
Reserved sectors 00E 0
(always zero) 010 00 00 00
(unused) 013 00 00
Media descriptor 015 248
(unused) 016 00 00
Sectors per track 018 63
Number of heads 01A 255
Hidden sectors 01C 2 048
(unused) 020 00 00 00 00
Signature 024 80 00 80 00
Total sectors 028 1 023 999
$MFT cluster number 030 42 666
$MFTMirr cluster number 038 2
Clusters per File Record Se... 040 246
Clusters per Index Block 044 1
Volume serial number 048 11 C9 31 44 ...
Checksum 050 0
Bootstrap code 054 FA 33 C0 8E ...
Signature (55 AA) 1FE 55 AA
My Computer
\\.\PhysicalDrive0 - Fixed Disk
View
ASCII
Unicode
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII
0000100000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 ëR.NTFS ....
0000100010 00 00 00 00 00 F8 00 00 3F 00 FF 00 00 08 00 00 ....ø..?.ÿ.....
0000100020 00 00 00 00 80 00 80 00 FF 9F 0F 00 00 00 00 00 ....€.€.ÿŸ......
0000100030 AA A6 00 00 00 00 00 00 02 00 00 00 00 00 00 00 ª¦..... ....
0000100040 F6 00 00 00 01 00 00 00 11 C9 31 44 E9 31 44 5A ö....... .É1Dé1DZ
0000100050 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 ....ú3ÀŽÐ¼.|ûhÀ.
0000100060 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E ..hf.Ëˆ...f.>..N
0000100070 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB TFSu.´A»ªUÍ.r..û
0000100080 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC Uªu.÷Á..u.éÝ..ƒì
0000100090 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13 .h..´HŠ...‹ô..Í.
00001000A0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3 ŸƒÄ.žX.rá;...uÛ£
00001000B0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8 ..Á.....Z3Û¹. +È
00001000C0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8 fÿ.......ŽÂÿ...è
00001000D0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D K.+Èwï¸.»Í.f#Àu-
00001000E0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16 f.ûTCPAu$.ù..r..
00001000F0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66 h.».hR..h..fSfSf
0000100100 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF U...h¸.fa..Í.3À¿
0000100110 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E ..¹ö.üóªéþ...f`.
0000100120 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00 .f¡..f.....fh...
0000100130 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E .fP.Sh..h..´BŠ..
0000100140 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F ...‹ôÍ.fY[ZfYfY.
0000100150 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF .‚..fÿ.......ŽÂÿ
0000100160 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00 ...u¼..faÃ¡ö.è..
0000100170 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09 ¡ú.è..ôëý‹ð¬<.t.
0000100180 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69 ´.»..Í.ëòÃ..A di
0000100190 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63 sk read error oc
00001001A0 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52 curred...BOOTMGR
00001001B0 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D is compressed..
00001001C0 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B .Press Ctrl+Alt+
00001001D0 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A Del to restart..
00001001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00001001F0 00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA ......Š.§.¿...Uª
Sector: 2 048 (0x800) Offset: 1 048 576 (0x100000) Read Only



Name	Offset	Value
JMP instruction	000	EB 52 90
OEM ID	003	NTFS
BIOS Parameter Block	**00B**	
Bytes per sector	00B	512
Sectors per cluster	00D	8
Reserved sectors	00E	0
(always zero)	010	00 00 00
(unused)	013	00 00
Media descriptor	015	248
(unused)	016	00 00
Sectors per track	018	63
Number of heads	01A	255
Hidden sectors	01C	2 048
(unused)	020	00 00 00 00
Signature	024	80 00 80 00
Total sectors	028	1 023 999
$MFT cluster number	030	42 666
$MFTMirr cluster number	038	2
Clusters per File Record Se...	040	246
Clusters per Index Block	044	1
Volume serial number	048	11 C9 31 44 ...
Checksum	050	0
Bootstrap code	054	FA 33 C0 8E ...
Signature (55 AA)	1FE	55 AA

Analyses

- MBR
  - Structure
  - Vérifications
- VBR
  - Structure
  - Vérifications
- IPL
  - Structure
  - Vérifications

VBR – Vérification de la copie

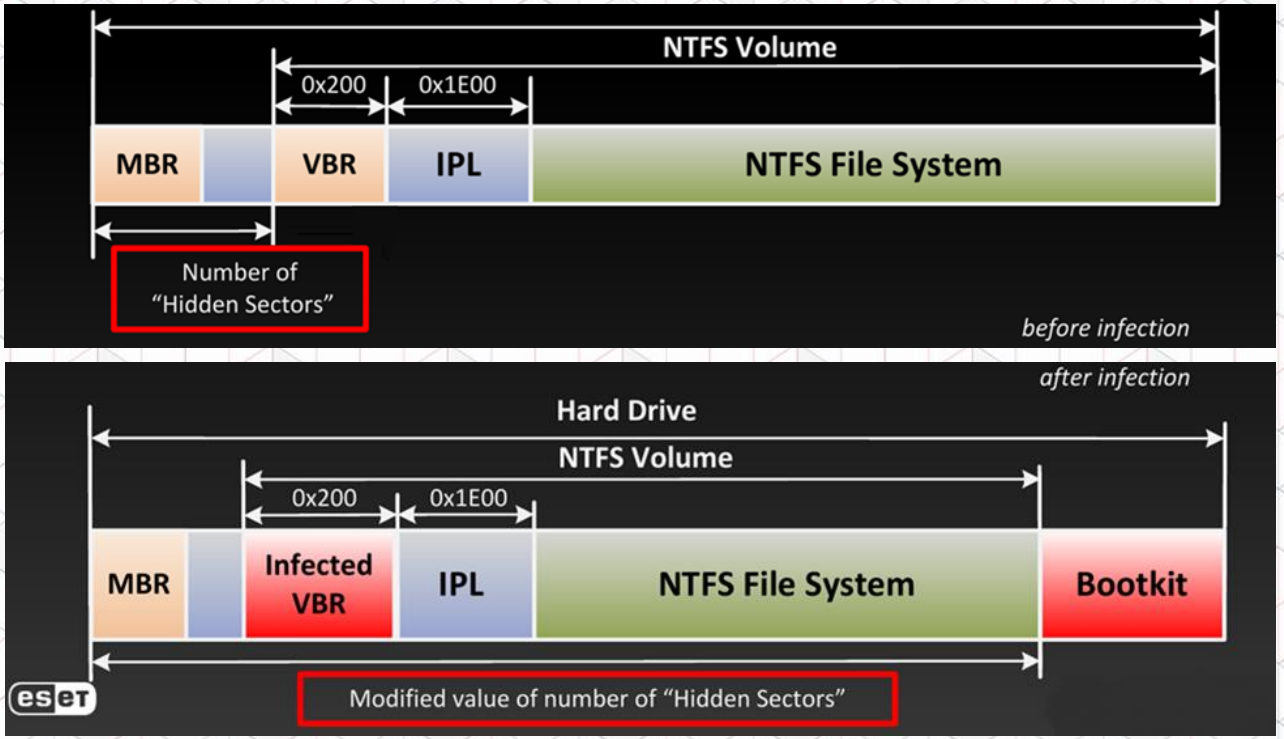
- Sauvegarde complète à la fin du volume NTFS (depuis NT4).

- Condensats identiques en théorie :
  - Pas de bootkit identifié qui modifie cette copie ;
  - Limites :
    - Mise à jour de version de Windows,
    - Bitlocker ou autre solution FVE.

VBR – Vérification du BPB

- Bios Parameter Block :
  - Métadonnées sur le volume NTFS ;
  - Valeur d'intérêt : « *hidden sectors* » (nombre de secteurs avant le Boot Sector).

Exemple : Gapz



VBR – Vérifications du code

- Condensat :
  - VBR complet (512 octets) => Echec
  - Section de code (426 octets) => Exploitable
    - Localisation linguistique des messages d'erreurs ;
    - Versions de Windows, solutions de chiffrement, etc.
- Intégrité du code du VBR :
  - JMP initial ;
  - Interruptions suspectes.

Analyses

- MBR
  - Structure
  - Vérifications
- VBR
  - Structure
  - Vérifications
- IPL
  - Structure
  - Vérifications

IPL – Structure

Initial Program Loader - 15 secteurs (7680 octets) situés à la suite du VBR.

Secteurs	Valeur
1 à 9	Code exécutable (taille variable)
10 et suivants	« Zéro »

Suivi par la première entrée de la MFT (« FILE » pour $MFT).

Analyses

- MBR
  - Structure
  - Vérifications
- VBR
  - Structure
  - Vérifications
- IPL
  - Structure
  - Vérifications

IPL – Vérifications

- Condensat :
  - 15 secteurs : Echec
    - Le dernier secteur peut être utilisé pour stocker des données (VSS).
  - Code seulement : Exploitable
    - Code de taille variable suivant les versions ;
    - Depuis NT6.2 : message d'erreur localisé.

Outillage

- Nombreux outils :
  - www.disk-editor.org : Active@ Disk Editor ;
  - www.garykessler.net : mbrparser, bsparser, gptparser, etc ;
  - www.hex-rays.com : IDA.

Outillage – bootcode_parser.py

https://github.com/ANSSI-FR

- Parser MBR/VBR/IPL
- Validation sommaire des structures
- Condensat des sections de code critiques
- Comparaison par liste blanche
- Heuristiques basiques

Outillage – bootcode_parser.py

- Contenu de la liste blanche :

```
"Type","SHA256","Comment"
"MBR","b5ed343494f0326a08aa6abf7cc9aa4d96207532cf0d2b39453c6eb7bede19e3","NT5.1/5.2 MBR"
"MBR","4799e8c92d32bca8e5103110a322523adb7a3909324132bd9abab8f3345e094a","NT6.0 MBR"
"MBR","088995559ab317af9b3291408da689651e8353f62e0a478d92eb0b5a947063fd","NT6.1+ MBR"
"MBR","955ff28fdffd869e617dfc1d44a6a40b45005c5d76491069e06ad48817499fea","GRUB2 MBR"
"MBR","e6e6605c48665800786de4651ade2893970aafb1237a06db0943a8603dd4fce1","TrueCrypt MBR"
"MBR","8a029cf94efd555b34d5564cc5c8e290a6ba5a52b6cdf9f02253f0d939f4dcec","Safeboot MBR"
"MBR","eedc57fa55ab1c71aa2fd511ff121e7d635b1e4bf7e7aeaa2a860360442790e1","Safeboot MBR"
"VBR","5cb5aa385e0ada266690a2821e3a36ad372720d2ff47c0b1cd9d6ebcab25bf4e","NT5.1/NT5.2 VBR"
"VBR","a1932aaba7d6d3adb1637e2ee0c8355706842ba825ea811728165420c518c0b1","NT6.0 VBR"
"VBR","96d38c1be37b9124fb71d1d0f5c52969f0074687fe17aef0e1bafc54428674f6","NT6.1 VBR"
"VBR","51643dcce7e93d795b08e1f19e38374ae4deaf3b1217527561a44aa9913ded23","NT6.2+ VBR"
"VBR","47138cbe995a20483209270ef55693c8c8e85ca870f28789229ce421aded92b4","NT6.1+ Bitlocker VBR"
"IPL","525788a688cfbe9e416122f0bc3cfb32ce9699fd12356b6ccaa173444c7d8f3f","NT5.1/NT5.2 IPL"
"IPL","ff1aae04bac3e29f062a7fa17320d7d26363256a69f96840718d45301da71291","NT6.0 IPL"
"IPL","462afe2322bad3d1c2747d7437d5f6c157e00ca37e5d38ebedd25346b3b488ce","NT6.1 IPL"
"IPL","c09d496a1f24086c333468d58256d5db9c73fee945fca74603bdab05f19a6d57","NT6.2+ IPL"
```

Outillage – Démo

- Système sain.
- Chaîne de démarrage compromise.

Et après ?

- UEFI
- Microgiciel de la carte mère :
  - Collecte
  - Analyse

Questions ?

Merci

Crédits illustrations : ESET – welivesecurity.com