Trends in dForensics, Dec/2012

pr0neer

proneer@gmail.com

http://forensic-proof.com

Kim Jinkook

Domestic Stuff

- **DailySecu** – 창과 방패, 안티포렌식 vs 안티안티포렌식
- **F-INSIGHT Forum** – 국정원 여직원 사건에 대한 기술적 논의
- **FORENSIC-PROOF** – 디지털포렌식 행사, 2013
- **CAPPLE Blog** – SSD 특성과 TRIM 기능의 이해

Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **Finding the ZeroAccess Sample**
  - In all the articles about ZeroAccess using the NTFS Extended Attributes, noticed one commonality; this technique was used in an **updated version of the Trojan.**
  - Searching sample in the Virus Shared repository, search for "zeroaccess" ➔ **6,056 results**
  - Find **Trojan.ZeroAccess.C** (Symantec's detection) ➔ **9 results**
  - Looking for ZeroAccess samples that used the NTFS EA ➔ **On the 3rd sample, hit pay dirt.**

Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **MFT Record ➔ Attributes**

Identifier		Attribute Name	Description
16	0x10	**$STANDARD_INFORMATION**	파일의 생성.접근.수정 시간, 소유자 등의 일반적인 정보
32	0x20	**$ATTRIBUTE_LIST**	추가적인 속성들의 리스트
48	0x30	**$FILE_NAME**	파일 이름(유니코드), 파일의 생성.접근.수정 시간
64	0x40	**$VOLUME_VERSION**	볼륨 정보 (Windows NT 1.2 버전에만 존재)
64	0x40	**$OBJECT_ID**	16바이트의 파일, 디렉터리의 고유 값, 3.0 이상에서만 존재
80	0x50	**$SECURITY_DESCRIPTOR**	파일의 접근 제어와 보안 속성
96	0x60	**$VOLUME_NAME**	볼륨 이름
112	0x70	**$VOLUME_INFORMATION**	파일 시스템의 버전과 다양한 플래그
128	0x80	**$DATA**	파일 내용
144	0x90	**$INDEX_ROOT**	인덱스 트리의 루트 노드
160	0xA0	**$INDEX_ALLOCATION**	인덱스 트리의 루트와 연결된 노드
176	0xB0	**$BITMAP**	$MFT와 인덱스의 할당 정보 관리
192	0xC0	**$SYMBOLIC_LINK**	심볼릭 링크 정보 (Windows 2000+)
192	0xC0	**$REPARSE_POINT**	심볼릭 링크에서 사용하는 reparse point 정보 (Windows 2000+)
208	0xD0	**$EA_INFORMATION**	OS/2 응용 프로그램과 호환성을 위해 사용 (HPFS)
224	0xE0	**$EA**	OS/2 응용 프로그램과 호환성을 위해 사용 (HPFS)
256	0x100	**$LOGGED_UTILITY_STREAM**	암호화된 속성의 정보와 키 값 (Windows 2000+)

Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **Extracting ZeroAccess from NTFS Extended Attributes**

1. mmls ₩₩.₩PHYSICALDRIVE#
2. ifind -o 2048 -n "Windows/System32/services.exe" ₩₩.₩PHYSICALDRIVE#
3. istat -o 2048 ₩₩.₩PHYSICALDRIVE3 12345
4. icat -o 2048 ₩₩.₩PHYSICALDRIVE# 12345-208-# > services_EA_INFO.bin

   icat -o 2048 ₩₩.₩PHYSICALDRIVE# 12345-224-# > services_EA.bin

Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **Clean MFT Services.exe**
  - istat -o 2048 ₩₩.₩PHYSICALDRIVE2 19211

```
... ...
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-4) Name: N/A Resident size: 90
Type: $FILE_NAME (48-2) Name: N/A Resident size: 90
Type: $DATA (128-3) Name: N/A Non-Resident size: 259072 init_size: 259072
750372 750373 750374 750375 750376 750377 750378 750379
750380 750381 750382 750383 750384 750385 750386 750387
750388 750389 750390 750391 750392 750393 750394 750395
750396 750397 750398 750399 750400 750401 750402 750403
750404 750405 750406 750407 750408 750409 750410 750411
750412 750413 750414 750415 750416 750417 750418 750419
750420 750421 750422 750423 750424 750425 750426 750427
750428 750429 750430 750431 750432 750433 750434 750435
```

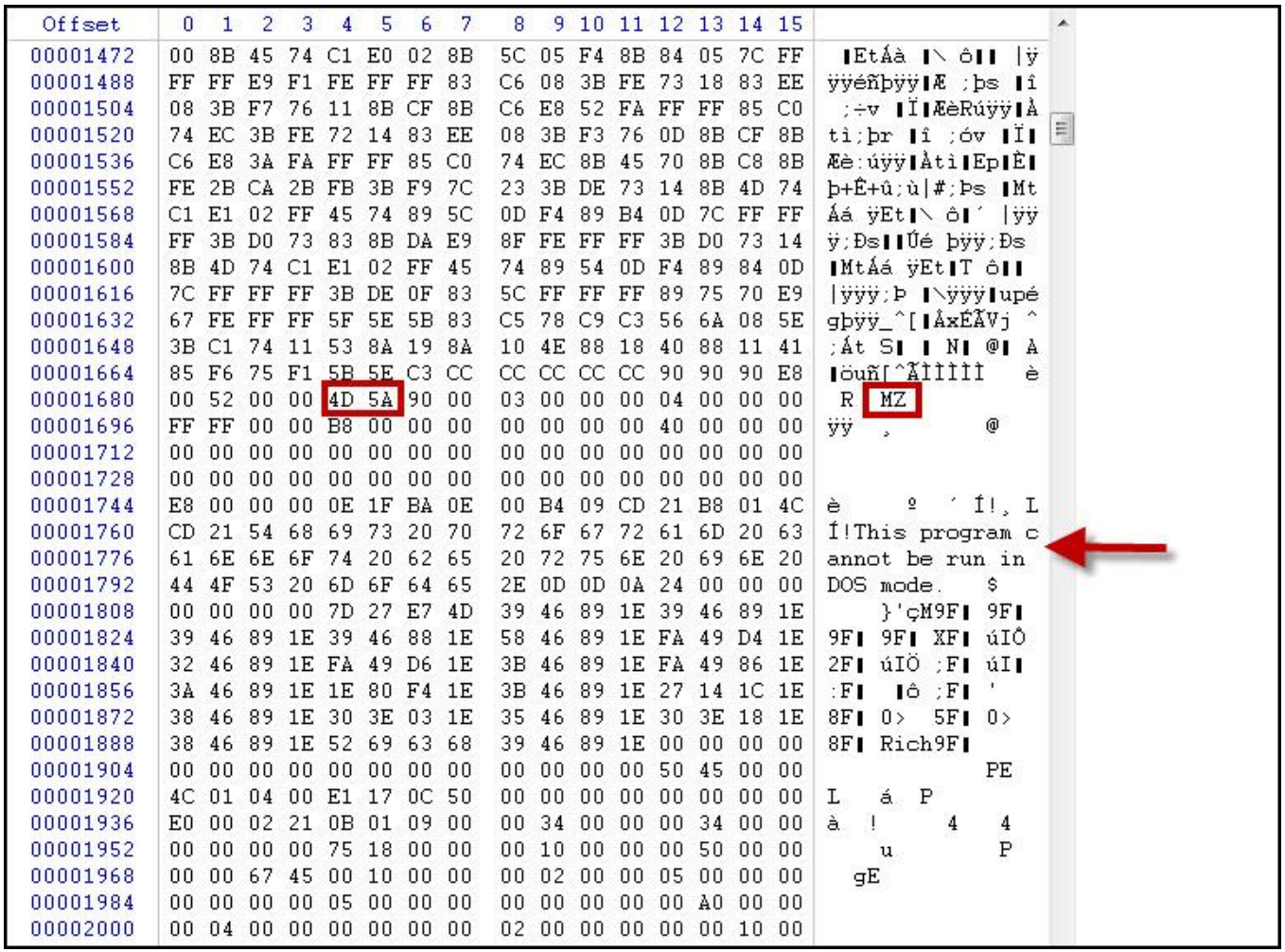
Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **Infected MFT Services.exe**
  - istat -o 2048 ₩₩.₩PHYSICALDRIVE2 19211

```
… …
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 90
Type: $DATA (128-5) Name: N/A Non-Resident size: 259072 init_size: 259072
618 619 620 621 622 623 624 625
626 627 628 629 630 631 632 633
634 635 636 637 638 639 640 641
642 643 644 645 646 647 648 649
650 651 652 653 654 655 656 657
658 659 660 661 662 663 664 665
666 667 668 669 670 671 672 673
Type: $EA_INFORMATION (208-3) Name: N/A Resident size: 8
Type: $EA (224-4) Name: N/A Non-Resident size: 23404 init_size: 23404
346 347 348 349 350 351
```

Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **Create the ZeroAccess Binary**



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00001472	00	8B	45	74	C1	E0	02	8B	5C	05	F4	8B	84	05	7C	FF	▮Et Á à ▮\ ô▮▮ |ÿ
00001488	FF	FF	E9	F1	FE	FF	FF	83	C6	08	3B	FE	73	18	83	EE	ÿÿéñþÿÿ▮Æ ;þs ▮î
00001504	08	3B	F7	76	11	8B	CF	8B	C6	E8	52	FA	FF	FF	85	C0	;÷v ▮Ï▮ÆèRúÿÿ▮À
00001520	74	EC	3B	FE	72	14	83	EE	08	3B	F3	76	0D	8B	CF	8B	tì;þr ▮î ;óv ▮Ï▮
00001536	C6	E8	3A	FA	FF	FF	85	C0	74	EC	8B	45	70	8B	C8	8B	Æè:úÿÿ▮Àti▮Ep▮È▮
00001552	FE	2B	CA	2B	FB	3B	F9	7C	23	3B	DE	73	14	8B	4D	74	þ+Ê+û;ù|#;Þs ▮Mt
00001568	C1	E1	02	FF	45	74	89	5C	0D	F4	89	B4	0D	7C	FF	FF	Áá ÿEt▮\ ô▮´ |ÿÿ
00001584	FF	3B	D0	73	83	8B	DA	E9	8F	FE	FF	FF	3B	D0	73	14	ÿ;Ðs▮▮Úé þÿÿ;Ðs
00001600	8B	4D	74	C1	E1	02	FF	45	74	89	54	0D	F4	89	84	0D	▮MtÁá ÿEt▮T ô▮▮
00001616	7C	FF	FF	FF	3B	DE	0F	83	5C	FF	FF	FF	89	75	70	E9	|ÿÿÿ;Þ ▮\ÿÿÿ▮upé
00001632	67	FE	FF	FF	5F	5E	5B	83	C5	78	C9	C3	56	6A	08	5E	gþÿÿ_^[▮ÅxÉÃVj ^
00001648	3B	C1	74	11	53	8A	19	8A	10	4E	88	18	40	88	11	41	;Át S▮ ▮ N▮ @▮ A
00001664	85	F6	75	F1	5B	5E	C3	CC	CC	CC	CC	CC	90	90	90	E8	▮öuñ[^ÃÌÌÌÌÌ è
00001680	00	52	00	00	4D	5A	90	00	03	00	00	00	04	00	00	00	R MZ
00001696	FF	FF	00	00	B8	00	00	00	00	00	00	00	40	00	00	00	ÿÿ ¸ @
00001712	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001728	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00001744	E8	00	00	00	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	è º ´ Í!¸ L
00001760	CD	21	54	68	69	73	20	70	72	6F	67	72	61	6D	20	63	Í!This program c
00001776	61	6E	6E	6F	74	20	62	65	20	72	75	6E	20	69	6E	20	annot be run in
00001792	44	4F	53	20	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	DOS mode. $
00001808	00	00	00	00	7D	27	E7	4D	39	46	89	1E	39	46	89	1E	}'çM9F▮ 9F▮
00001824	39	46	89	1E	39	46	88	1E	58	46	89	1E	FA	49	D4	1E	9F▮ 9F▮ XF▮ úIÔ
00001840	32	46	89	1E	FA	49	D6	1E	3B	46	89	1E	FA	49	86	1E	2F▮ úIÖ ;F▮ úI▮
00001856	3A	46	89	1E	1E	80	F4	1E	3B	46	89	1E	27	14	1C	1E	:F▮ ▮ô ;F▮ '
00001872	38	46	89	1E	30	3E	03	1E	35	46	89	1E	30	3E	18	1E	8F▮ 0> 5F▮ 0>
00001888	38	46	89	1E	52	69	63	68	39	46	89	1E	00	00	00	00	8F▮ Rich9F▮
00001904	00	00	00	00	00	00	00	00	00	00	00	00	50	45	00	00	PE
00001920	4C	01	04	00	E1	17	0C	50	00	00	00	00	00	00	00	00	L á P
00001936	E0	00	02	21	0B	01	09	00	00	34	00	00	00	34	00	00	à ! 4 4
00001952	00	00	00	00	75	18	00	00	00	10	00	00	00	50	00	00	u P
00001968	00	00	67	45	00	10	00	00	00	02	00	00	05	00	00	00	gE
00001984	00	00	00	00	05	00	00	00	00	00	00	00	00	A0	00	00	
00002000	00	04	00	00	00	00	00	00	02	00	00	00	00	00	10	00	

Extracting ZeroAccess from NTFS EA (Journey Into Incident Response)

- **analyzedMFT.py –f $MFT –o parsed_mft.txt**

	A	C	D	H	AU	AV
1	Record Number	Active	Record type	Filename #1	EA Information	EA
21488	21486	Active	File	/Windows/winsxs/x86_cxfalpal_ibv32.inf_31bf3856ad364e35_6.1.7600.16385_none_bd	FALSE	TRUE
21491	21489	Active	File	/Windows/winsxs/x86_cxraptor_fm1236mk5_ibv32.inf_31bf3856ad364e35_6.1.7600.16	FALSE	TRUE
21496	21494	Active	File	/Windows/winsxs/x86_cxraptor_fm1236mk5_ibv32.inf_31bf3856ad364e35_6.1.7600.16	FALSE	TRUE
21497	21495	Active	File	/Windows/winsxs/x86_cxraptor_fm1236mk5_ibv32.inf_31bf3856ad364e35_6.1.7600.16	FALSE	TRUE
21501	21499	Active	File	/Windows/winsxs/x86_cxraptor_fm1236mk5_ibv32.inf_31bf3856ad364e35_6.1.7600.16	FALSE	TRUE
21667	21665	Active	File	/Windows/winsxs/x86_mdmbr00a.inf_31bf3856ad364e35_6.1.7600.16385_none_7d002	FALSE	TRUE
21973	21971	Active	File	/Windows/winsxs/x86_ph3xibc9.inf_31bf3856ad364e35_6.1.7600.16385_none_4482afc	FALSE	TRUE
21979	21977	Active	File	/Windows/winsxs/x86_ph3xibc9.inf_31bf3856ad364e35_6.1.7600.16385_none_4482afc	FALSE	TRUE
21999	21997	Active	File	/Windows/System32/DriverStore/FileRepository/ph6xib32c1.inf_x86_neutral_569a6f9	FALSE	TRUE
25169	25167	Active	File	/Windows/winsxs/X8E68D~1.163/Brmf3wia.dll	FALSE	TRUE
25173	25171	Active	File	/Windows/winsxs/X8E68D~1.163/BrUs2Sti.dll	FALSE	TRUE
27193	27191	Active	File	/Windows/winsxs/x86_microsoft-windows-p..unterinfrastructure_31bf3856ad364e35_	FALSE	TRUE
27208	27206	Active	File	/Windows/winsxs/x86_microsoft-windows-m..-downlevelmanifests_31bf3856ad364e3	FALSE	TRUE
27216	27214	Active	File	/Windows/winsxs/x86_microsoft-windows-m..-downlevelmanifests_31bf3856ad364e3	FALSE	TRUE
27222	27220	Active	File	/Windows/winsxs/x86_microsoft-windows-m..-downlevelmanifests_31bf3856ad364e3	FALSE	TRUE
27228	27226	Active	File	/Windows/winsxs/x86_microsoft-windows-m..-downlevelmanifests_31bf3856ad364e3	FALSE	TRUE
38859	38857	Active	File	/Windows/winsxs/x86_ehome-bdatunepia_31bf3856ad364e35_6.1.7600.16385_none_e	FALSE	TRUE
38860	38858	Active	File	/Windows/winsxs/X86_EH~4.163/mcstoredb.dll	FALSE	TRUE
39952	39950	Active	File	/Windows/System32/wbem/OfflineFilesWmiProvider_Uninstall.mof	FALSE	TRUE
39990	39988	Active	File	/Program Files/DVD Maker/audiodepthconverter.ax	FALSE	TRUE
39991	39989	Active	File	/Windows/winsxs/x86_microsoft-windows-sonic-directshowtap_31bf3856ad364e35_6	FALSE	TRUE
39997	39995	Active	File	/Windows/winsxs/x86_microsoft-windows-sonic-rtstreamsink_31bf3856ad364e35_6.1	FALSE	TRUE
39999	39997	Active	File	/Windows/winsxs/x86_microsoft-windows-sonic-colorconverter_31bf3856ad364e35_6	FALSE	TRUE
41537	41535	Active	Folder	/Windows/CSC/V20~1.6	TRUE	TRUE
42748	42746	Active	Folder	/Users/lab/AppData/Local/{5da39e95-8007-4308-c6cf-bcce61795d0d}/U	TRUE	TRUE
42754	42752	Active	Folder	/Windows/Installer/{5da39e95-8007-4308-c6cf-bcce61795d0d}/U	TRUE	TRUE
42758	42756	Active	File	/Windows/System32/services.exe	TRUE	TRUE

NTOSBOOT Prefetch File (Journey Into Incident Response)

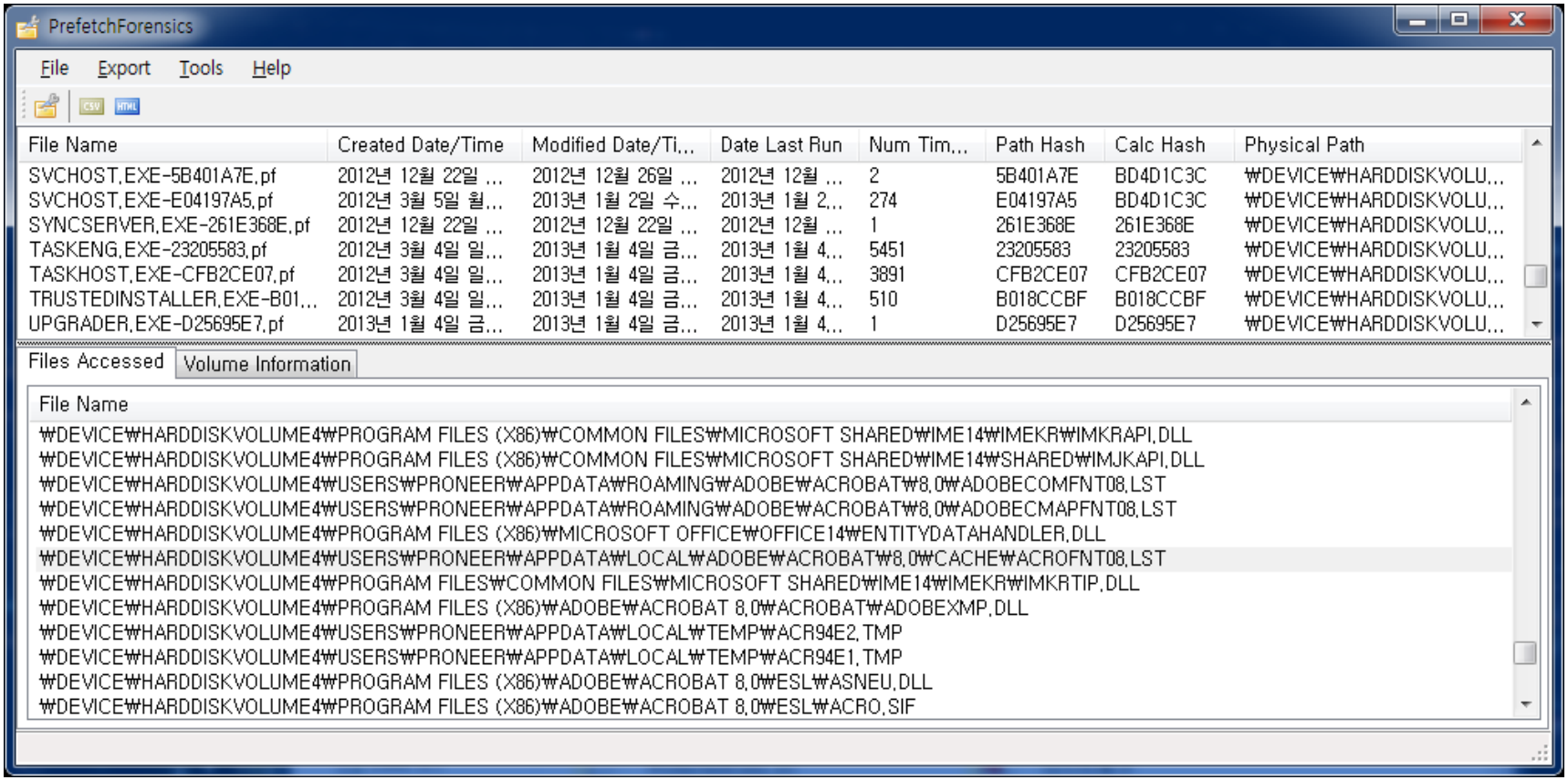
- **Prefetch**
  - To speed up the Windows OS and Application startup
  - **Types**
    - ✓ **Boot prefetching** : XP, 2003, Vista, 2008, 7
    - ✓ **Application prefetching** : XP, Vista, 7
    - ✓ **Hosting application**
  - **dForensics Value**
    - ✓ Application Name/Path + Full Path Hash Value
    - ✓ Application Number of Launches
    - ✓ Application Last Launch Time
    - ✓ Associated File List (DLL, SDB, NLS, INI, …)
    - ✓ FileSystem Timestamps (Created, Modified, Last Accessed)

NTOSBOOT Prefetch File (Journey Into Incident Response)

- **Boot Prefetching**
  - The files for booting can be fragmented or scattered on volume ➔ boot speed down
  - **Prefetching stuffs**
    - ✓ Monitoring following the start of the explorer.exe for 30 seconds
    - ✓ Monitoring following windows service initialization for 120 seconds
  - Stores information about the file accessed during boot process ➔ prefetch file
  - **Boot prefetch file**
    - ✓ %SystemRoot%₩Prefetch₩**NTOSBOOT-BOODFAAD.PF**

NTOSBOOT Prefetch File (Journey Into Incident Response)

- **PrefetchForensics (WOANWARE)**



NTOSBOOT Prefetch File (Journey Into Incident Response)

- **NTOSBOOT prefetch** in Compromised System

ticket_spam_prefetch.txt

```
389  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SHDOCLC.DLL
390  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ES.DLL
391  \DEVICE\HARDDISKVOLUME1\WINDOWS\PCHEALTH\HELPCTR\BINARIES\PCHSVC.DLL
392  \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ADMINISTRATOR\MY DOCUMENTS\DESKTOP.INI
393  \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\JAVA\JRE6\BIN\JQS.EXE
394  \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\JAVA\JRE6\BIN\MSVCR71.DLL
395  \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS\DESKTOP.INI
396  \DEVICE\HARDDISKVOLUME1\DOCUME~1\ALLUSE~1\LOCALS~1\TEMP\17F7FFF4.COM
397  \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE
398  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MAIN.CPL
399  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\PDH.DLL
```

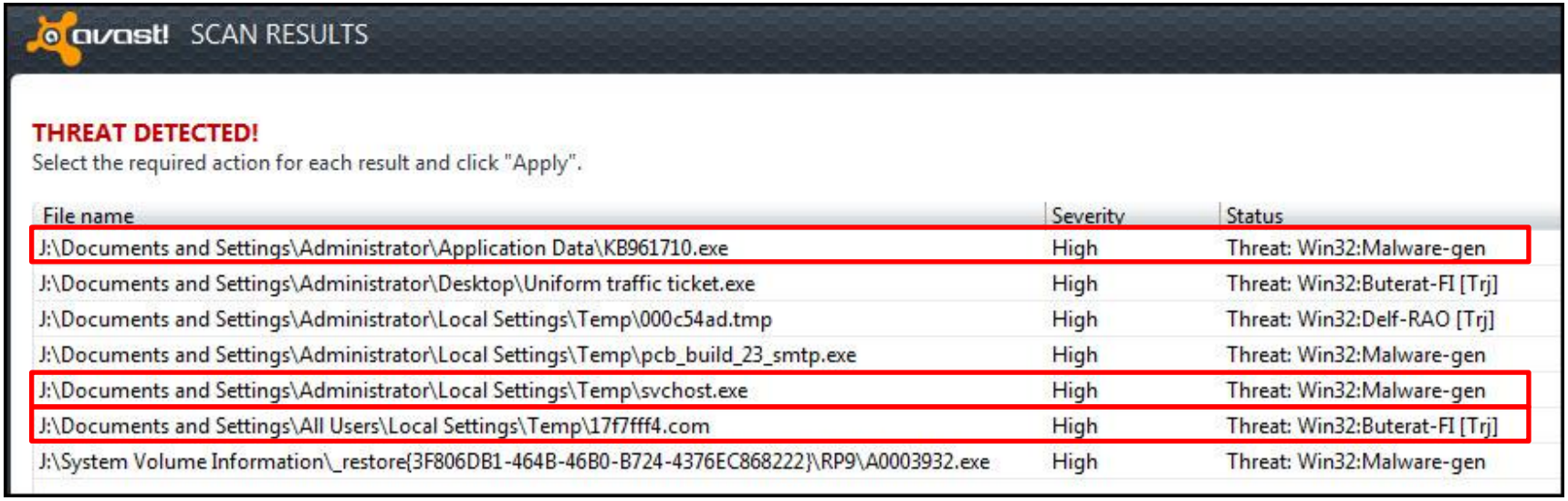
ticket_spam_prefetch.txt

```
451  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ICMP.DLL
452  \DEVICE\HARDDISKVOLUME1\SYSTEM VOLUME INFORMATION\_RESTORE{3F806DB1-464B-46B0-B724-4376EC868222}\RP9\RP.LOG
453  \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ADMINISTRATOR\APPLICATION DATA\KB961710.EXE
454  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WUAUSERV.DLL
455  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WBEM\WMISVC.DLL
456  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\VSSAPI.DLL
457  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WUAUENG.DLL
458  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVPACK.DLL
```

```
481  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WBEM\WMIPRVSD.DLL
482  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WBEM\WBEMESS.DLL
483  \DEVICE\HARDDISKVOLUME1\DOCUME~1\ADMINI~1\LOCALS~1\TEMP\SVCHOST.EXE
484  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COMSVCS.DLL
485  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COLBACT.DLL
486  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MTXCLU.DLL
487  \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\CLUSAPI.DLL
```

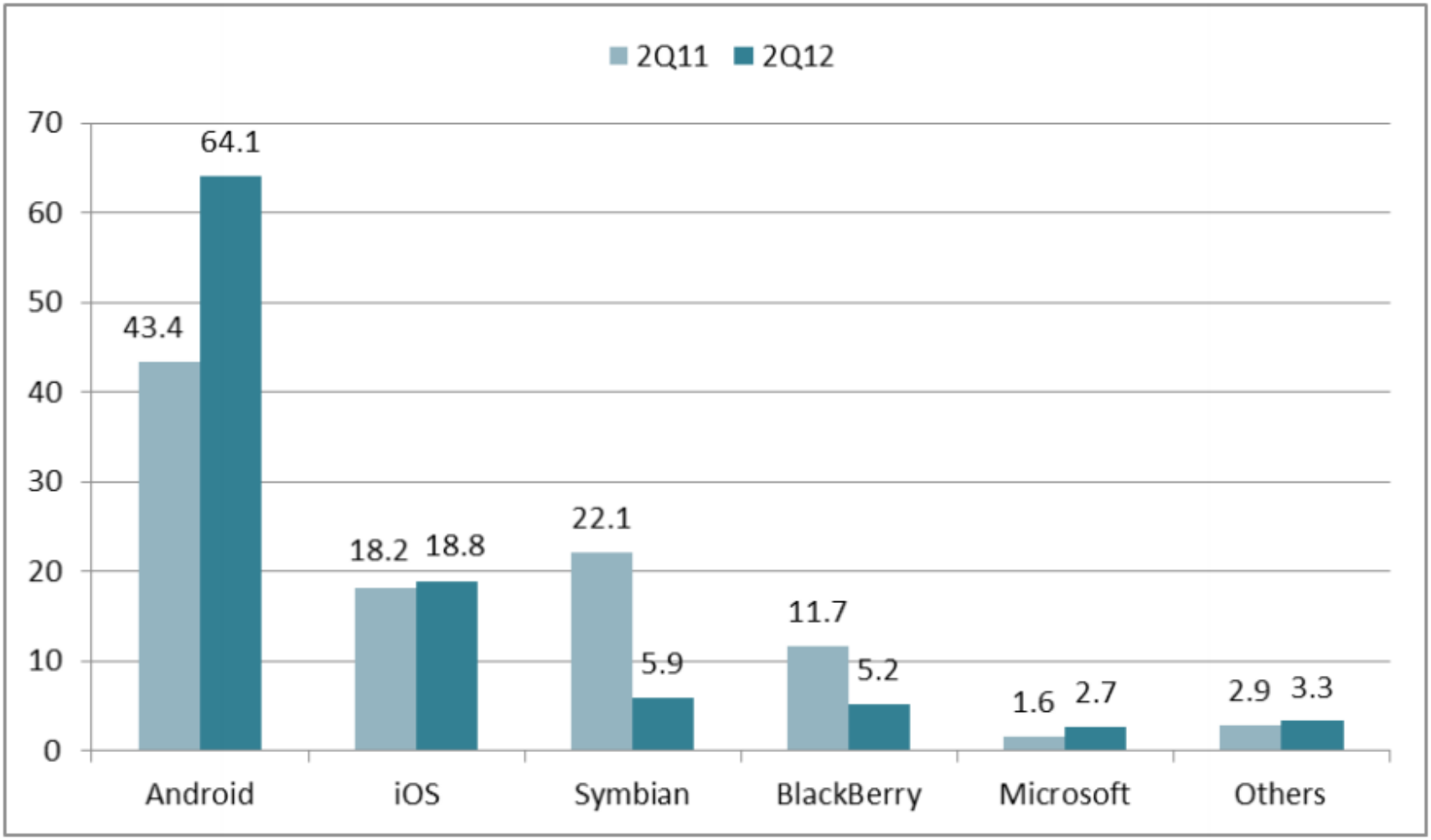
NTOSBOOT Prefetch File (Journey Into Incident Response)

- **Scan Results of AVAST!**



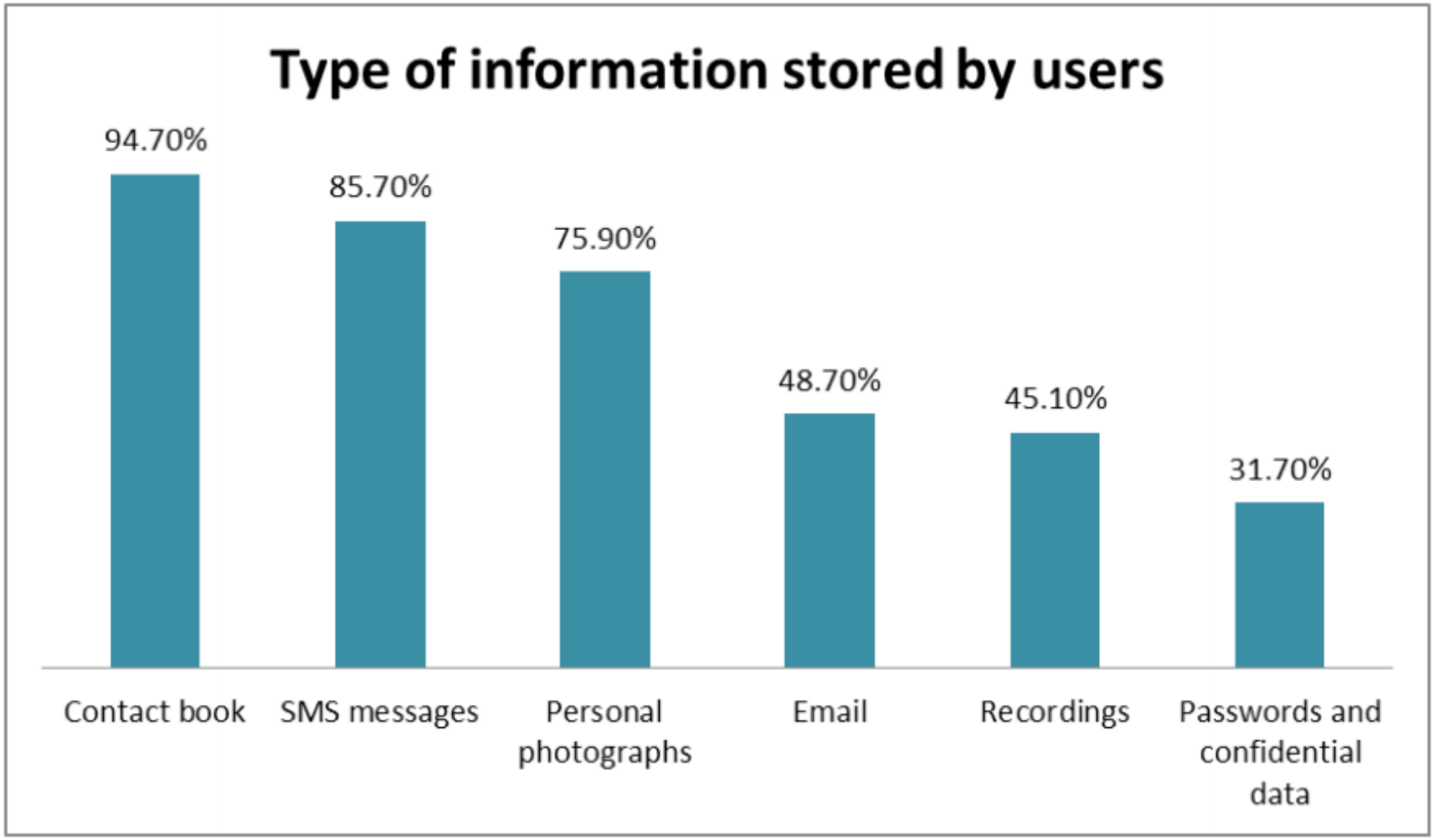
Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)



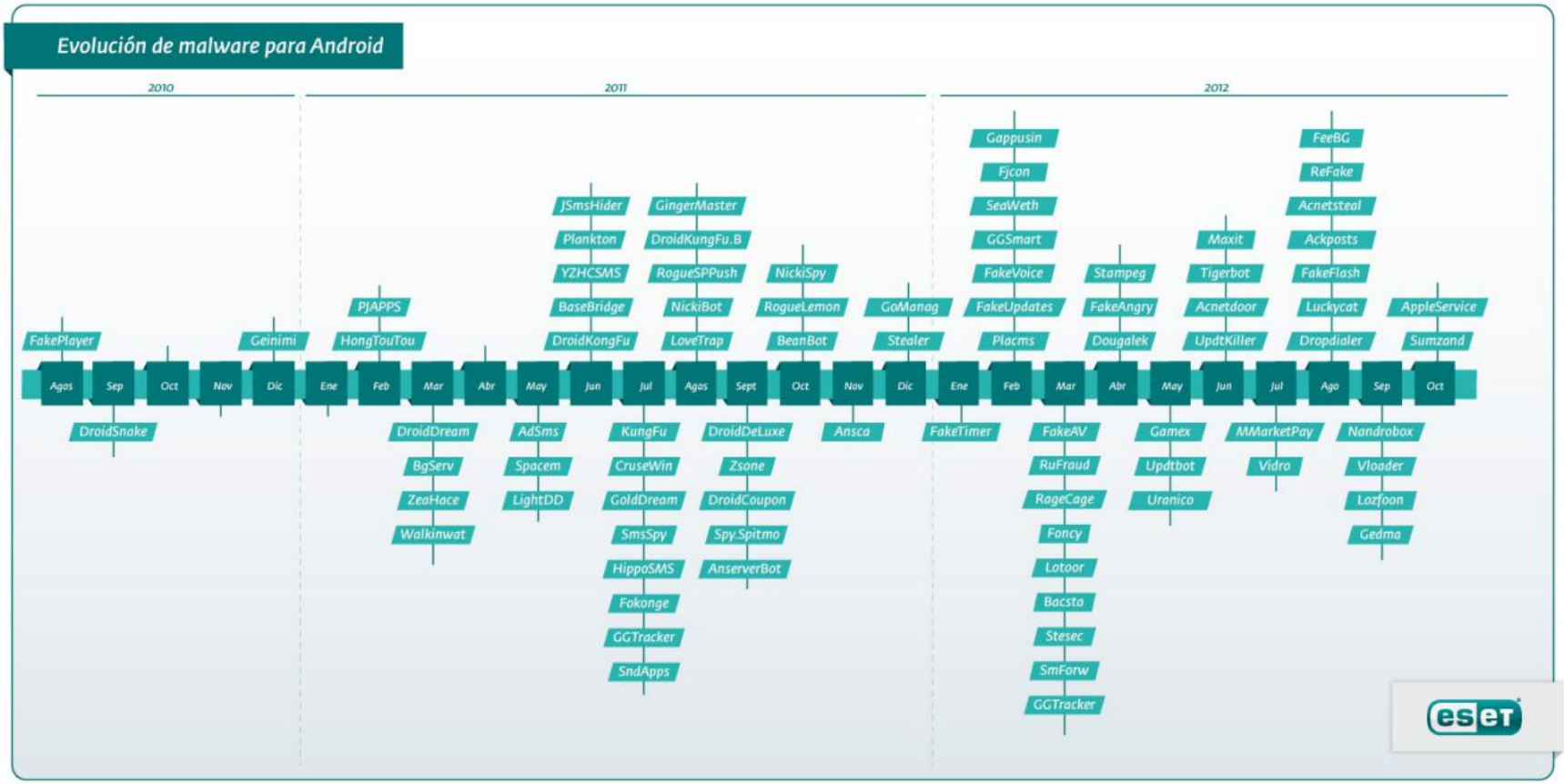
Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)



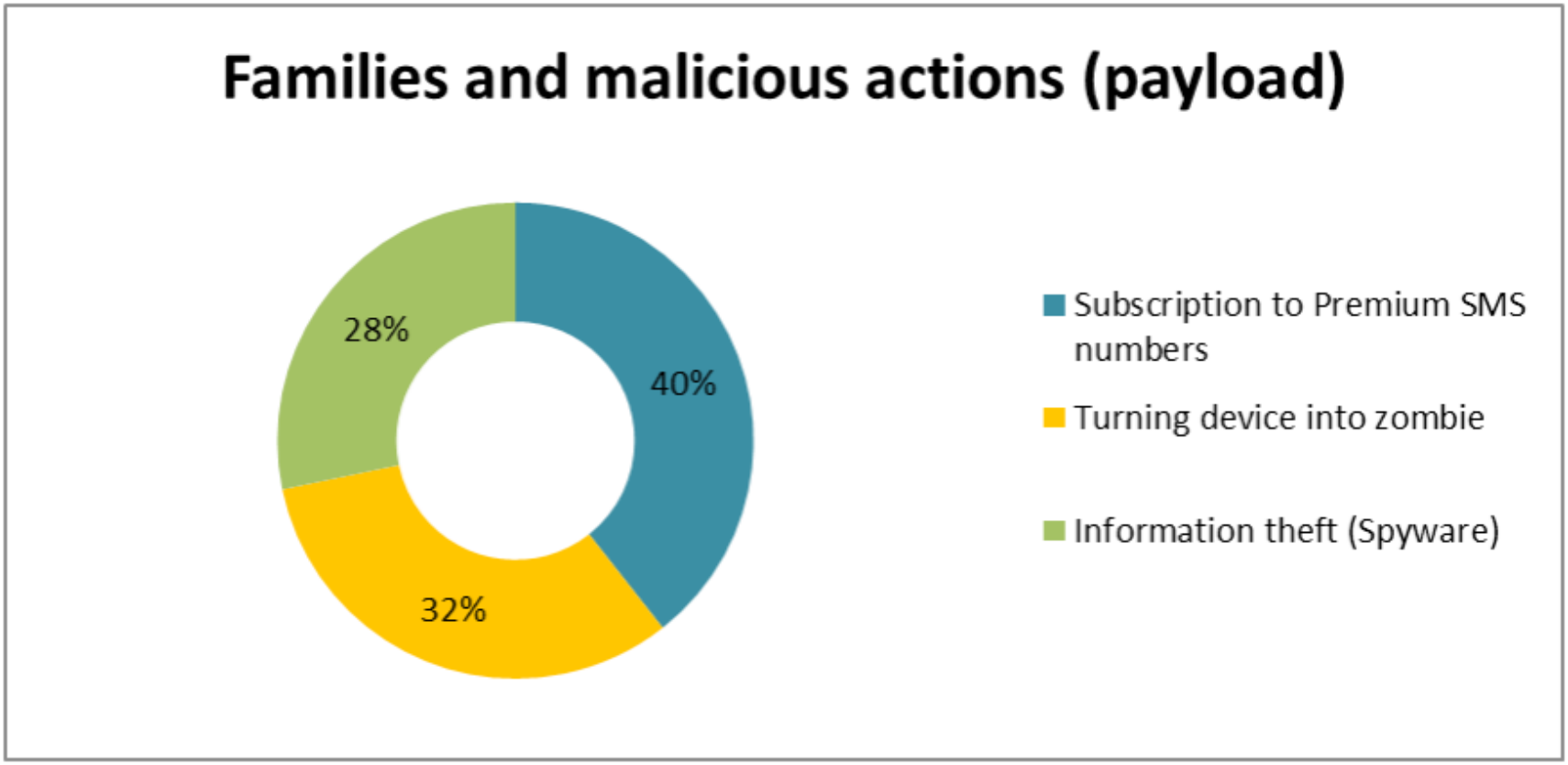
Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)



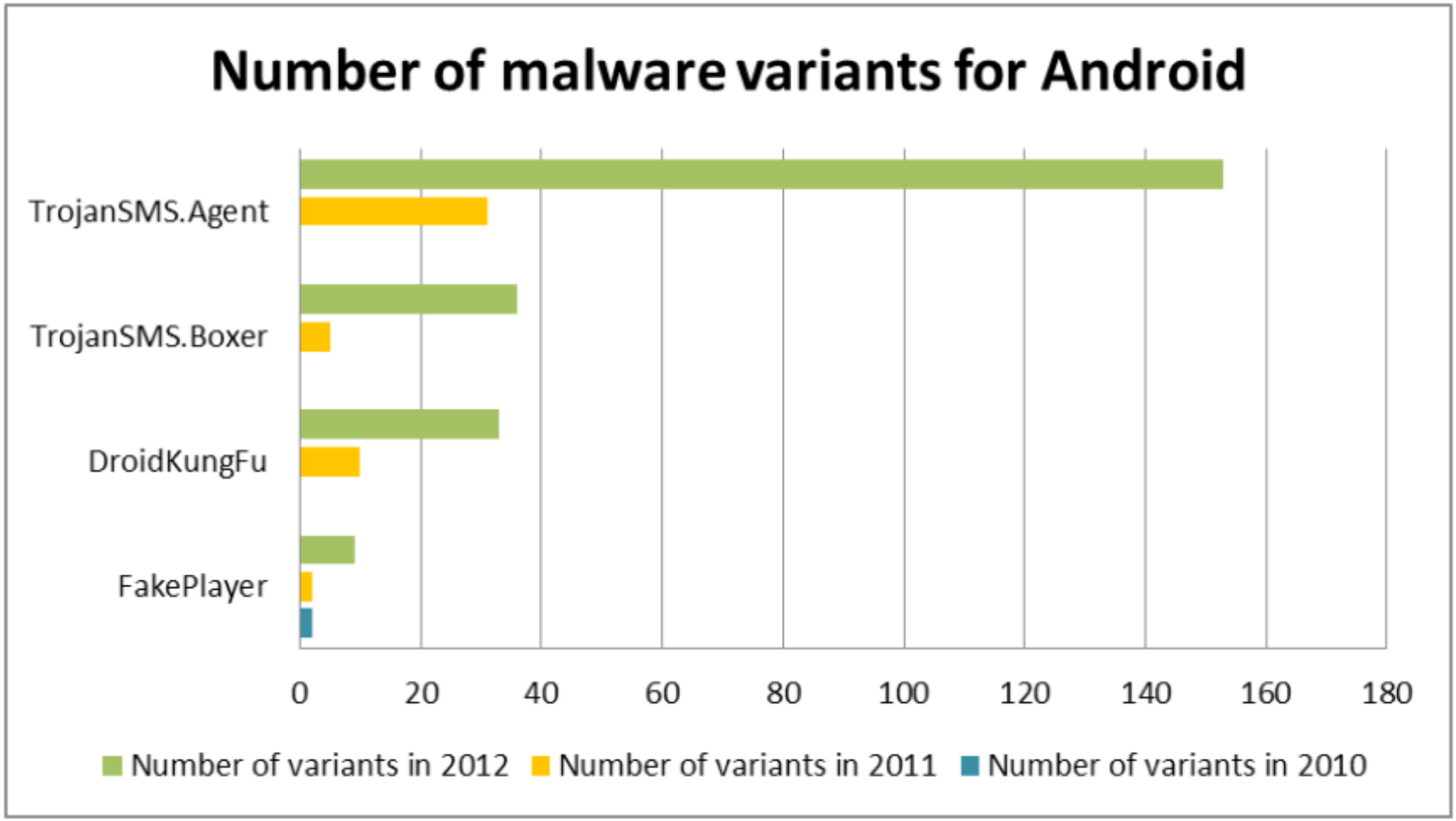
Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)



Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

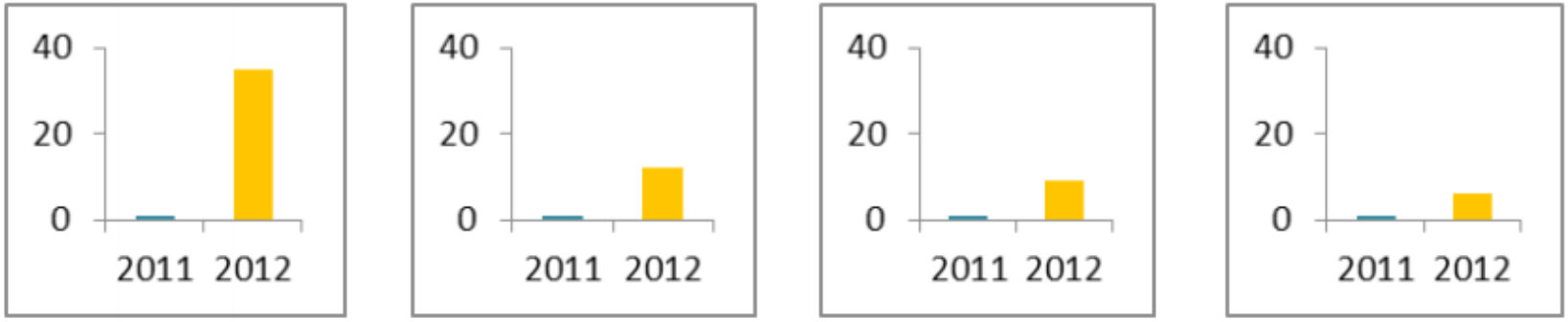
- **Trends for 2013** by ESET Latin America's Lab (PDF)



Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)

Growth of families according to the number of signatures added in 2012, compared to 2011

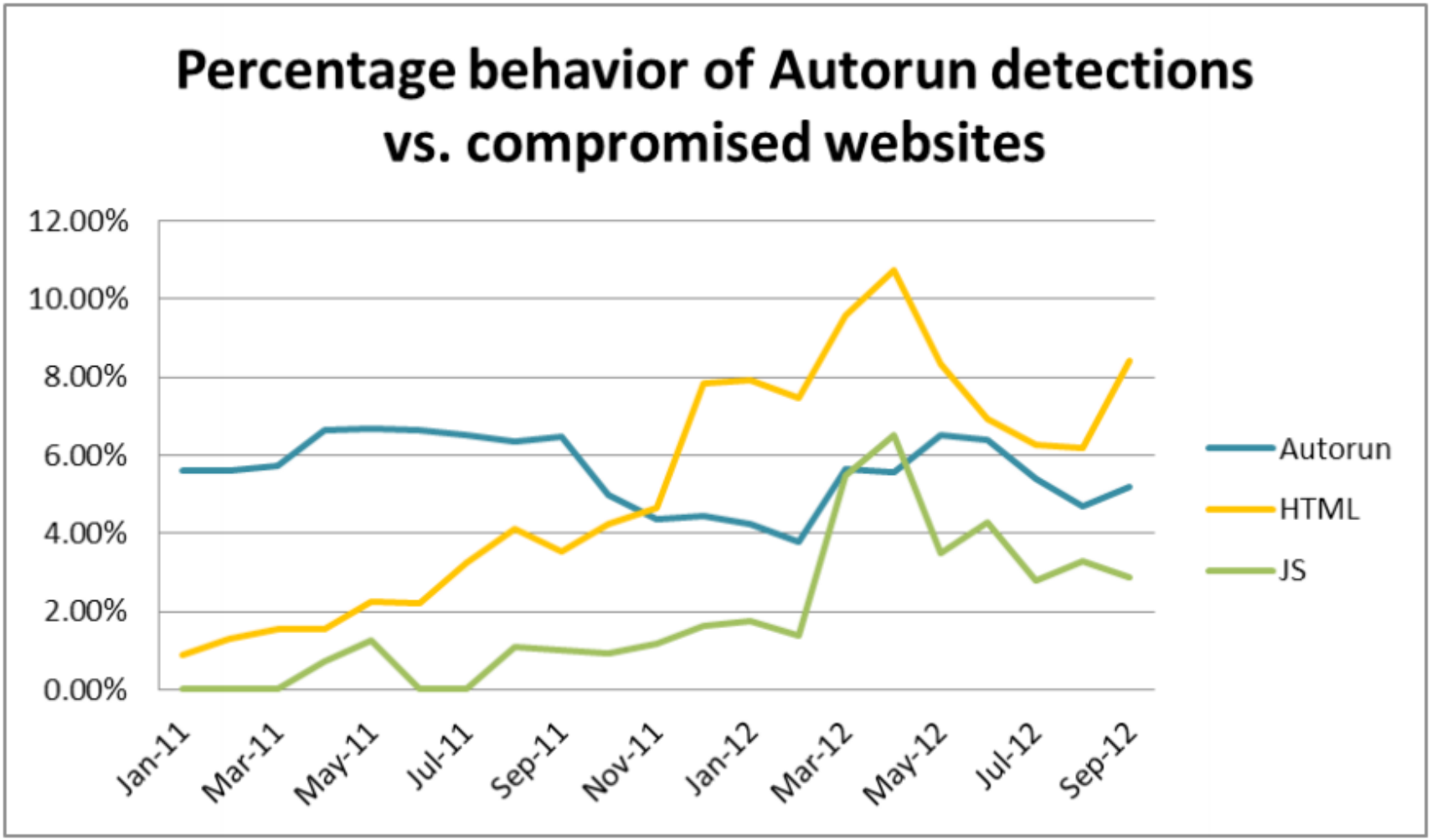


Plankton	**JSmsHider**	**DroidDream**	**DroidKungFu**
The number of signatures rose 35 times in 2012	The number of signatures rose 12 times in 2012	The number of signatures rose 9 times in 2012	The number of signatures rose 6 times in 2012

Yellow: 2012
Blue: 2011

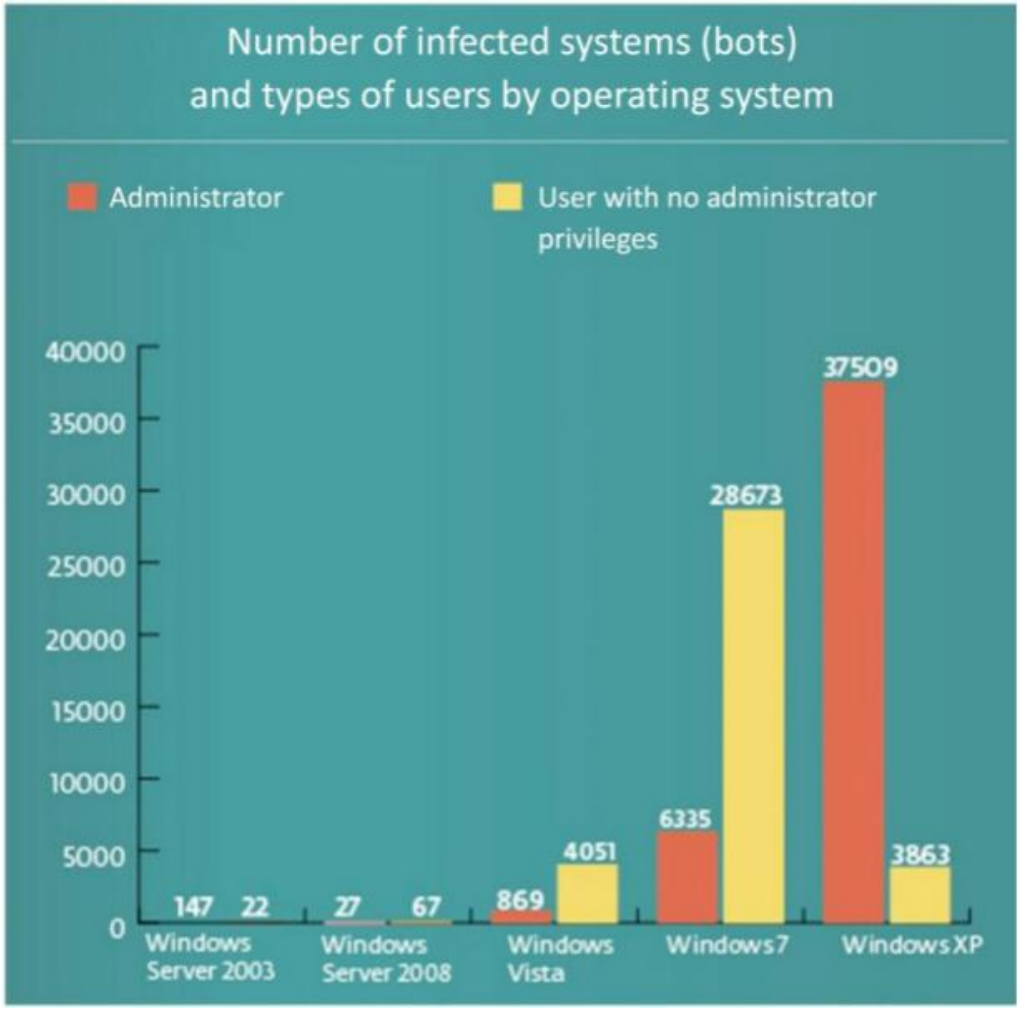
Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)



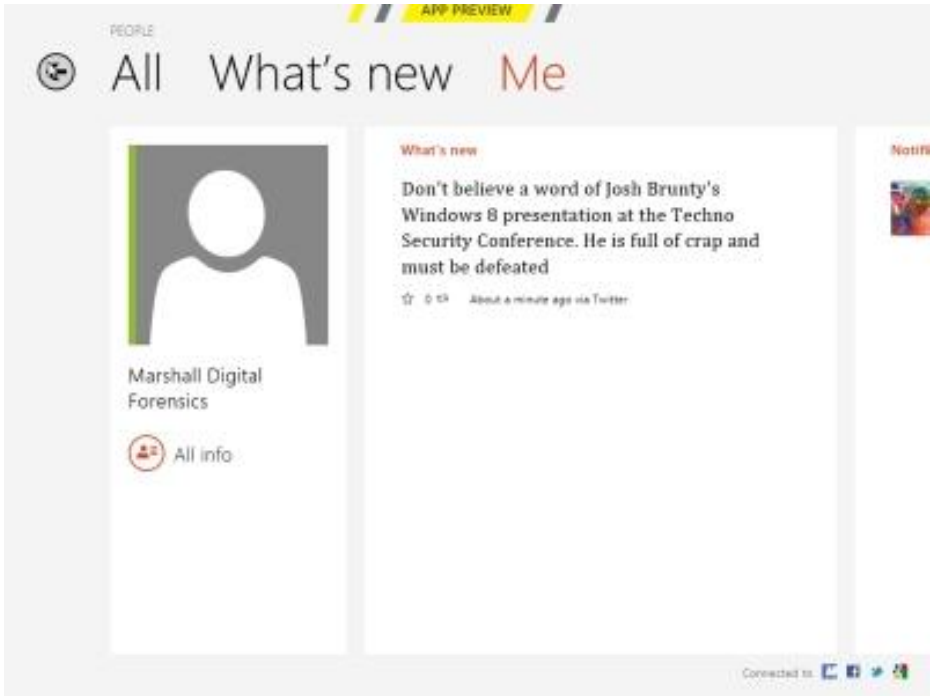
Trends for 2013: astounding growth of mobile malware (ESET Threat Blog)

- **Trends for 2013** by ESET Latin America's Lab (PDF)



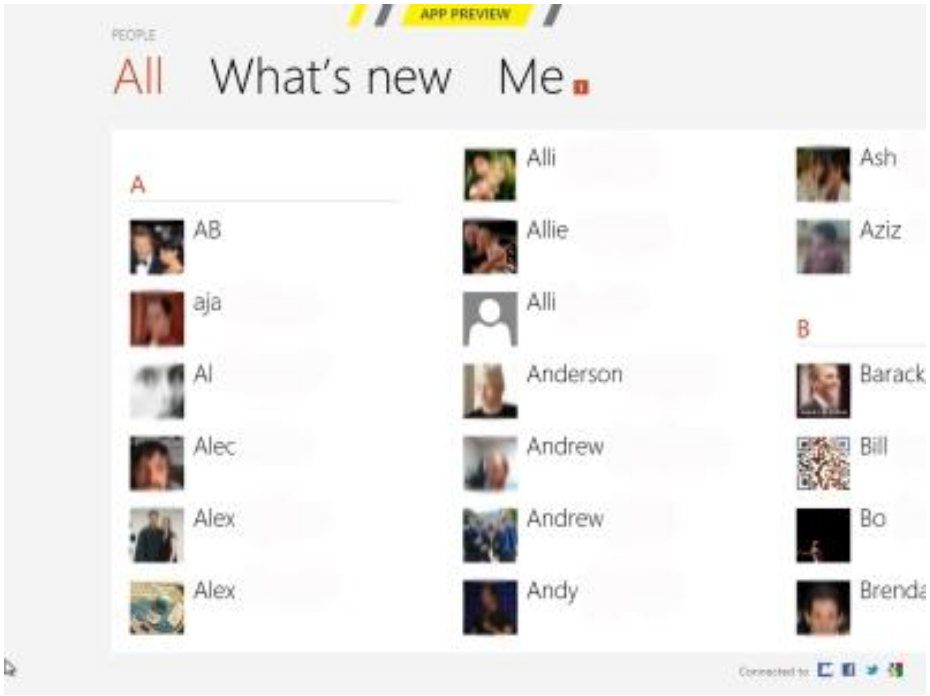
Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **DFI News** – Microsoft Windows 8 : A Forensic First Look
  - **User's Contacts from Communications Apps**
    - ✓ %Root%₩Users₩%User%₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩LocalState₩LiveComm₩%User'sWindowsLiveEmail Address%₩%App-CurrentVersion%₩DBStore₩LogFiles₩edb####.log



Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **DFI News** – Microsoft Windows 8 : A Forensic First Look
  - **User Tile Associated with Contact**
    - ✓ %Root%₩Users₩%User%₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩LocalState₩LiveComm₩%User'sWindowsLiveEmailAddress%₩%AppCurrentVersion%₩DBStore₩UserTiles



Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **Testing**
  - **Manufacturer**: Dell Latitude D430
  - **Specifications**: Intel Core 2 CPU U7600 @ 1.20GHz / 2.00GB Installed RAM /
  - **OS**: Windows 8 Release Preview / Product ID: 00137-11009-99904-AA587
  - **HARD DRIVE**: SAMSUNG HS122JC ATA Device / Capacity 114,472 MB

1. Download and Install Windows 8 RP
2. Create a single user account called "**User**" with a password of "**password**"
3. Connecting the Windows 8 laptop to web based accounts (Microsoft, Facebook, LinkdeIn, Google) and imported various info from accounts
4. Installed Applications

Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

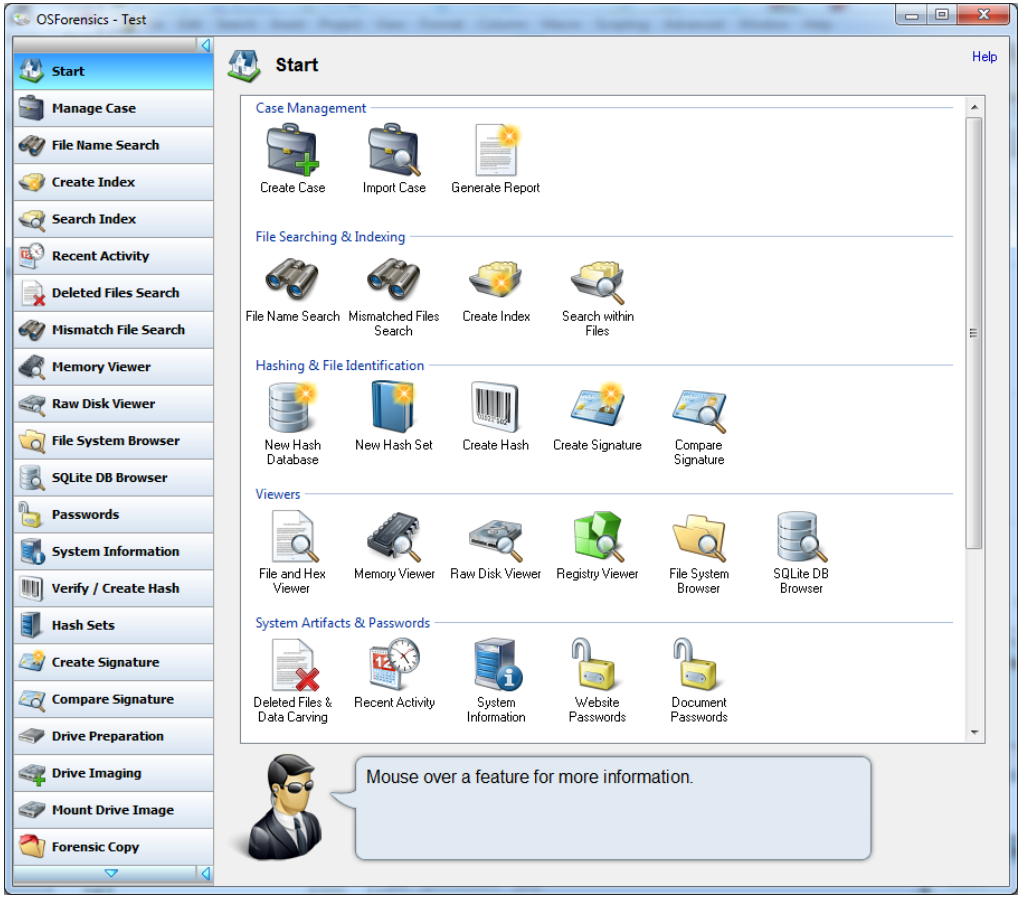
- **Programs recorded by the Control Panel**
  - **Adobe Flash Player** 11 Plugin ver. 11.4.402.287
  - **Google Chrome** ver. 23.0.1271.64
  - **Mozilla Firefox** ver. 16.0.2 (x86 en-US)
- **Programs listed under Win 8's "Store" tile**
  - **Tweetro** (I did not link to any Twitter account)
  - **Xbox Live Games** (using Microsoft account user name "larry_lieb@yahoo.com")

Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **Next**
  - Using the Chrome, logged into Google account and installed "**Gmail Offline**"
  - Then, logged in to a newly created Yahoo account (larry.lieb@yahoo.com)
  - Sent and received several emails both two and from Yahoo/Gmail Accounts
  - While logged into Yahoo.com, imported contacts from LinkedIn account
  - And Then, imaging the laptop

Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **After Imaging**
  - Indexing using Passmark's OSForensics on uFred



Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **Next**
  - Searches for common email file types
    - ✓ **2,204** items using the search string "*.eml"
    - ✓ 0 items using the search string "*.msg"
    - ✓ 0 items using the search string "*.pst"
    - ✓ 0 items using the search string "*.mbox"
  - Export a hash value and file list report for the folder "1:₩Users₩User₩AppData₩Local₩Packages₩"

Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

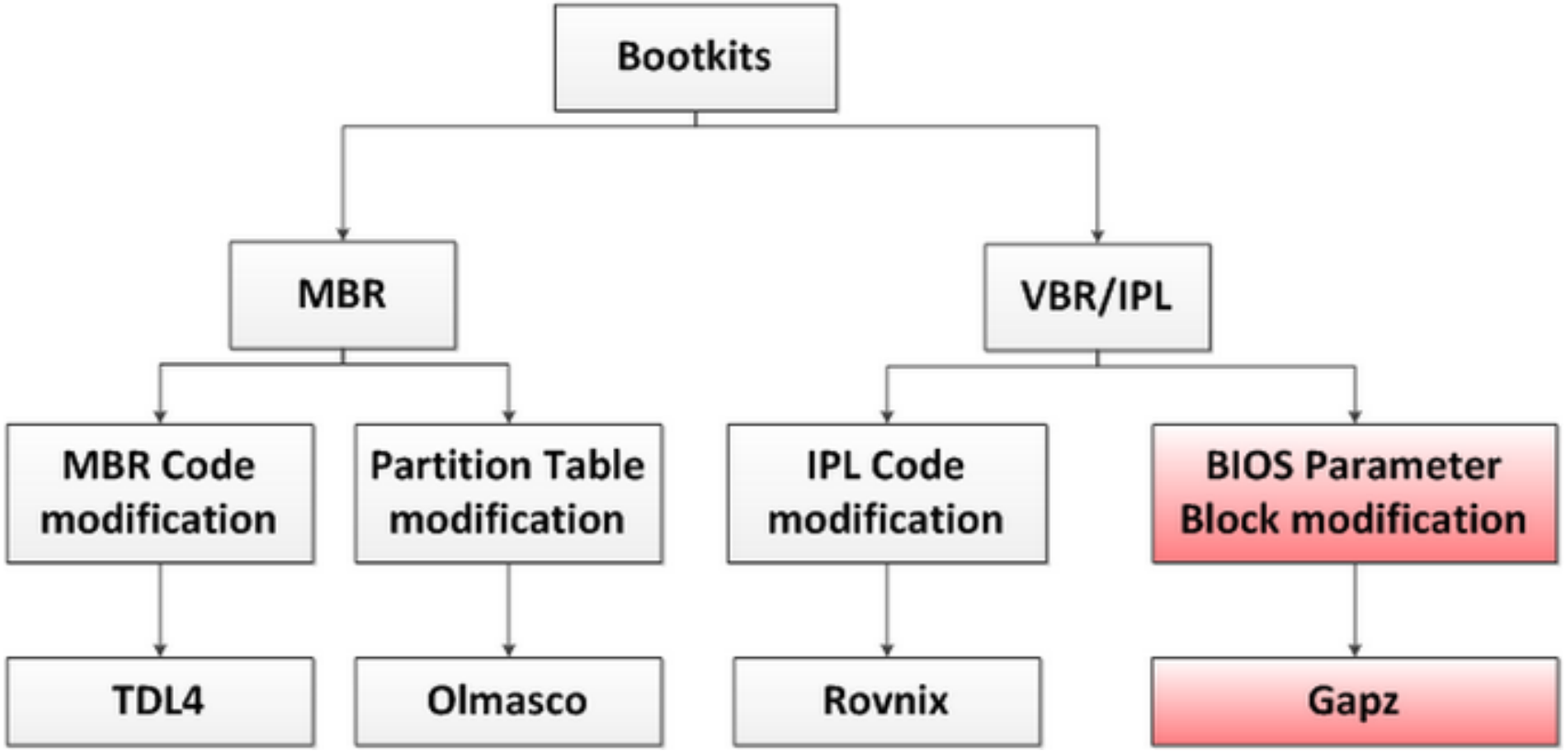
- **Next**
  - **.EML files**
    - ✓ Using FTK Imager, exported the contents of the following folder:
      - "Users₩User₩AppData₩Local₩Packages₩microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩LocalState₩Indexed₩LiveComm₩larry_lieb@yahoo.com₩".
  - **Discover Interesting Folders**
    1. Found **164 .EML** files under the "Mail" folder (containing email communications)
       - "microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩LocalState₩Indexed₩**LiveComm₩larry_lieb@yahoo.com₩120510-2203₩Mail₩**"
    - ✓ Found **1,939 .EML** files under the "People" folder (containing contacts)
      - "microsoft.windowscommunicationsapps_8wekyb3d8bbwe₩LocalState₩Indexed₩**LiveComm₩larry_lieb@yahoo.com₩120510-2203₩People₩**"
    - ✓ Found **1 .EML** file under the "People₩Me" folder ("User" .EML contact file)
      - microsoft.windowsphotos_8wekyb3d8bbwe₩LocalState₩Indexed₩**LiveComm₩larry_lieb@yahoo.com₩120510-2203₩People₩Me**"

Windows 8: Important Considerations for dForensics and eDiscovery (Forensic Focus)

- **Conclusion**
  - Often times, **further processing** such as Microsoft Word, Excel, Powerpoint, Adobe PDF, and common email file types such as .PST, .MSG., and .EML. Files found in the forensic image(s) will be exported for **further processing and review by attorneys.**
  - One of the **challenges attorneys face** in electronic discovery is reasonably **keeping costs low by avoiding human review** of obviously non-relevant files.
  - If an attorney is billing at a rate of **$200/hour**, and can review fifty documents per hour, then the **1,938 "contact" .EML** files alone would require 38.78 hours of attorney review time at a cost to the client of **$7,756.00.**
  - .EML files from the "People" folder be **excluded from processing and review.**

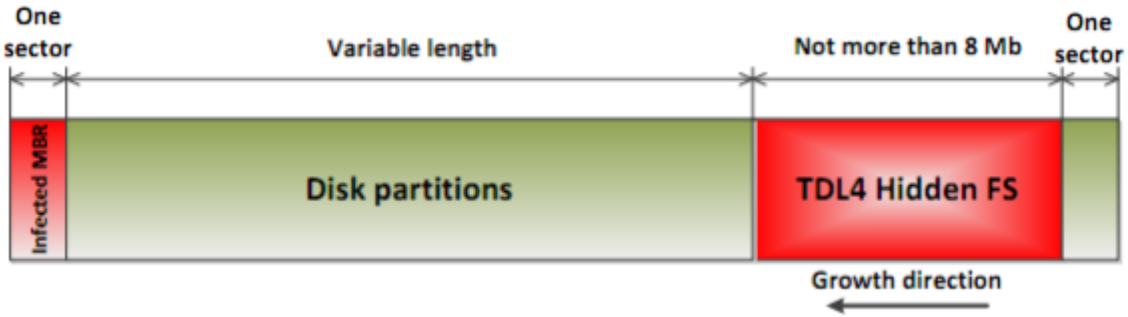
Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

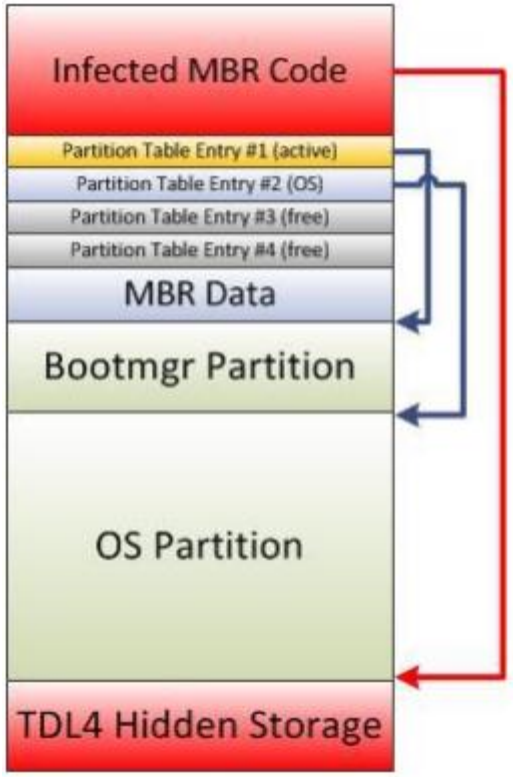
- **Types of Bootkit**



Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **TDL4**
  - By the late 2010 – TDL4(Win32/Olmarik)
  - The first widely spread bootkit targeting 64-bit systems ➔ building botnets
  - Self-protection with hooking and encryption
  - **Concealing Techniques**
    - ✓ Overwritten MBR Code
    - ✓ Using unpartitioned area (reserved for dynamic disk)

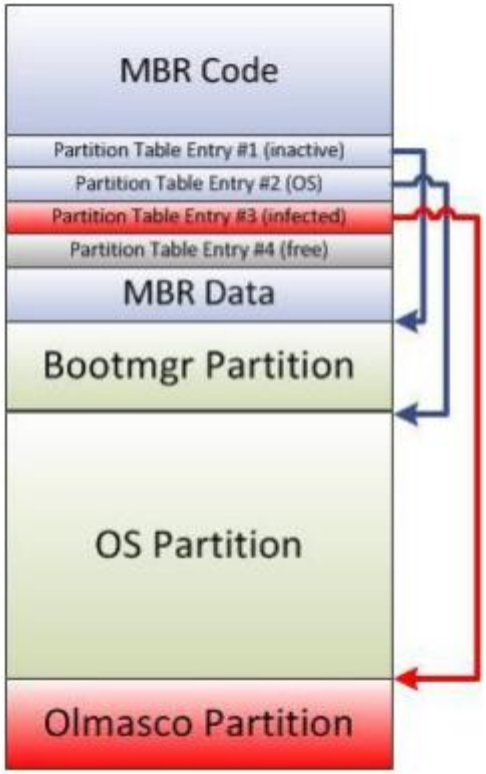




Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

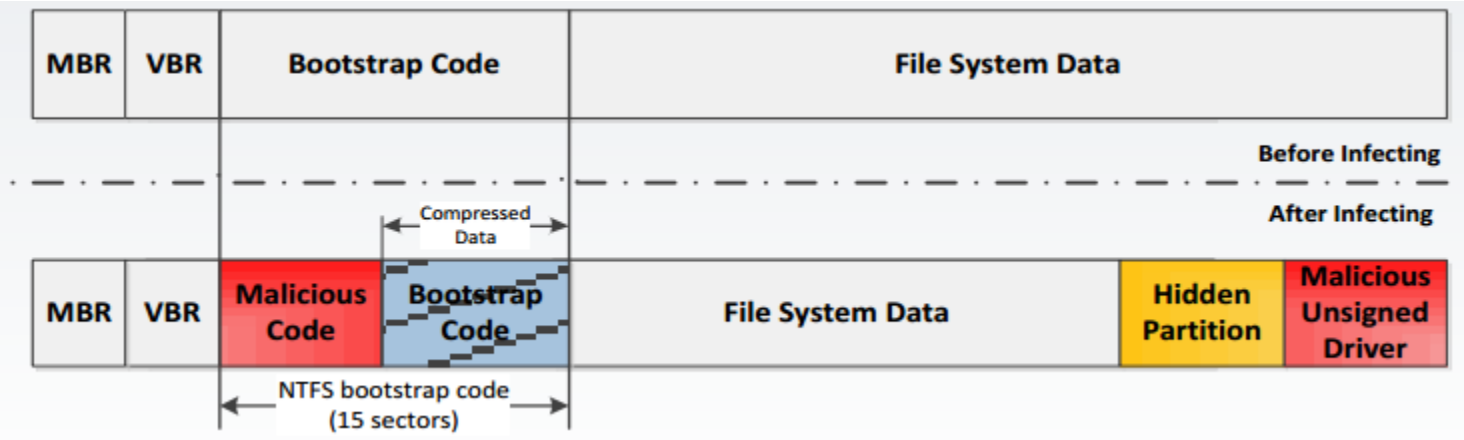
- **Olmasco**
  - At the beginning of 2011 a brand new bootkit
  - Enhanced techniques developed and evolved within the TDL4
  - Aim for building botnets
  - Error Report ➔ patching
  - **Concealing Techniques**
    - ✓ Modify partition table ➔ create a new partition
    - ✓ Create unique volume/filesystem (like NTFS) ➔ Run a payload

```
0000  EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00  ыRPNTFS    .....
0010  00 00 00 00 00 F8 00 00  3F 00 FF 00 53 AC FF 00  .....°..?. .Sм .
0020  00 00 00 00 80 00 80 00  9C 53 00 00 00 00 00 00  ....А.А.ьS......
0030  39 05 00 00 00 00 00 00  00 02 00 00 00 00 00 00  9...............
0040  F6 00 00 00 01 00 00 00  8B 62 C8 E9 B8 4B 28 D5  ў.......ЛbLщ¬K(-
0050  00 00 00 00 FA 31 C0 8E  D0 BC 00 7C FB 0E 1F 0E  ....·1LO¦-.|v...
0060  07 66 60 88 16 00 7E C6  06 04 7E 1E B4 48 BE 04  .f`И..~¦..~.+H-.
0070  7E CD 13 B0 50 0F 82 71  01 83 2E 13 04 14 A1 13  ~=.-P.Bq.Г....б.
```



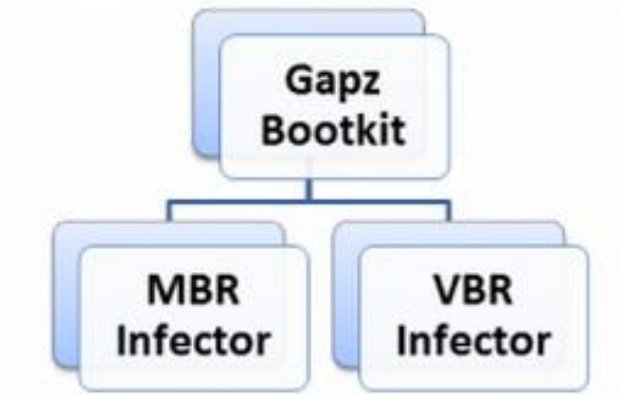
Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **Rovnix**
  - Early in 2011 (Win32/Rovnix, Win32/Carberp)
  - Modifying the VBR and Bootstrap code
  - for-sale bootkit builder



Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

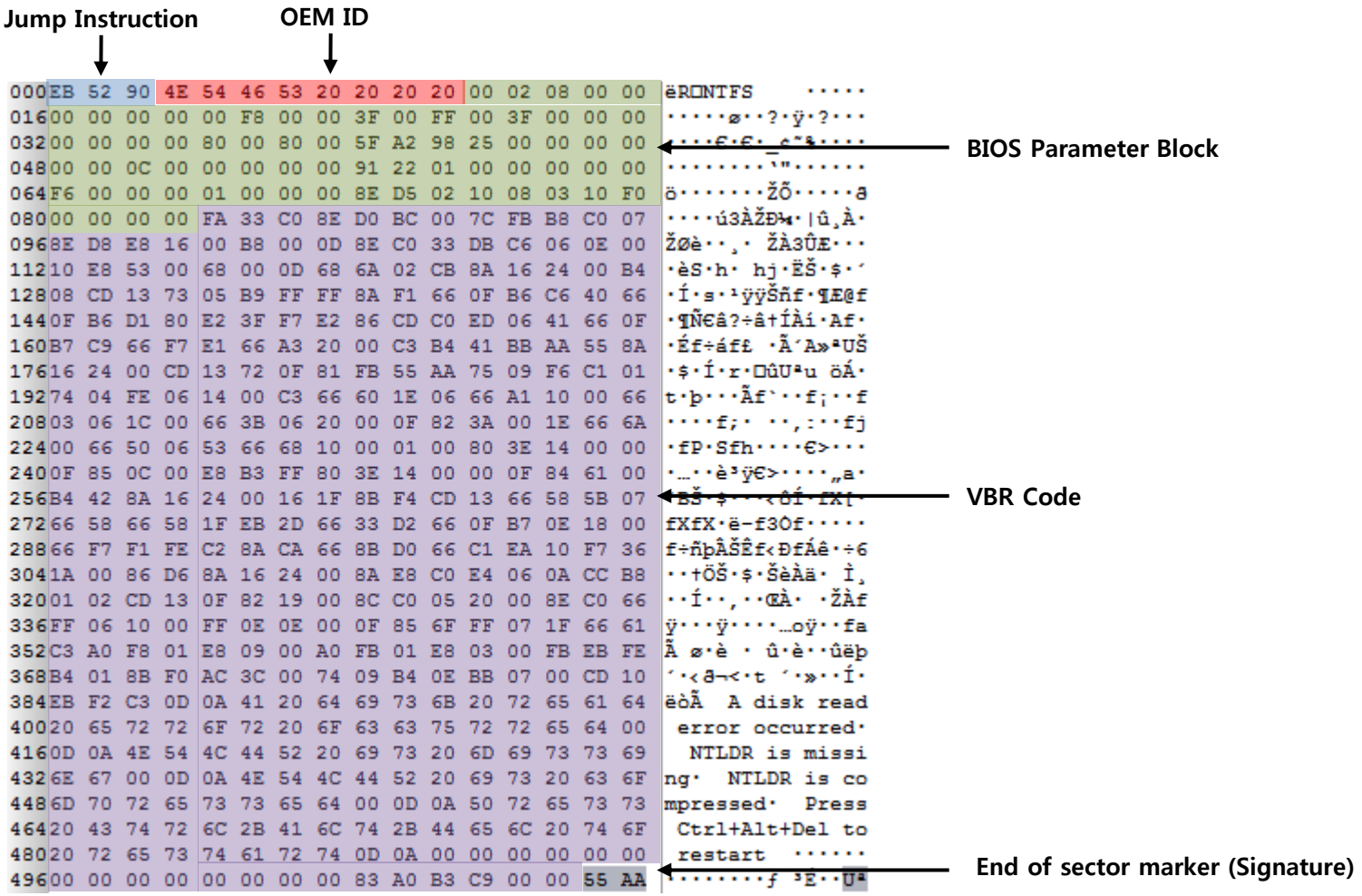
- **Win32/Gapz**



- 2012, summer : **MBR Infector**
  - ✓ malicious MBR
  - ✓ kernel-mode code and payload injected into user-mode process
  - ✓ code & payload was written either ahead or after on the volume
- 2012, autumn : **VBR Infector**

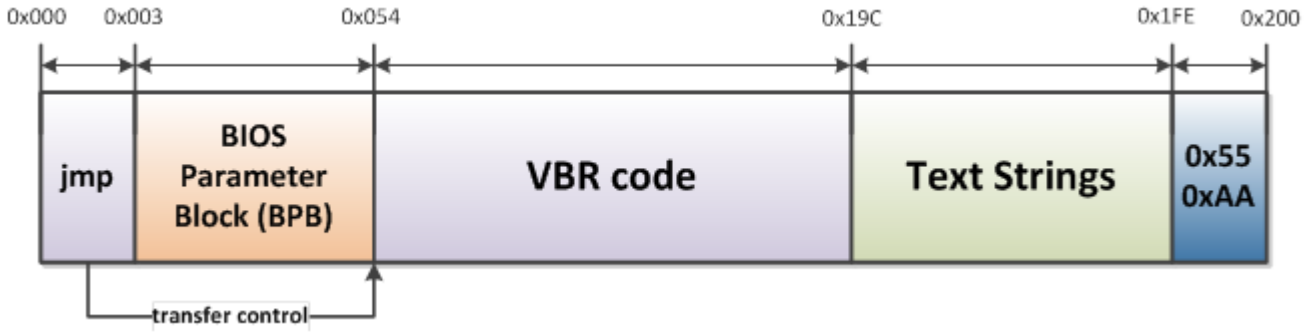
Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **Win32/Gapz: VBR Infector**



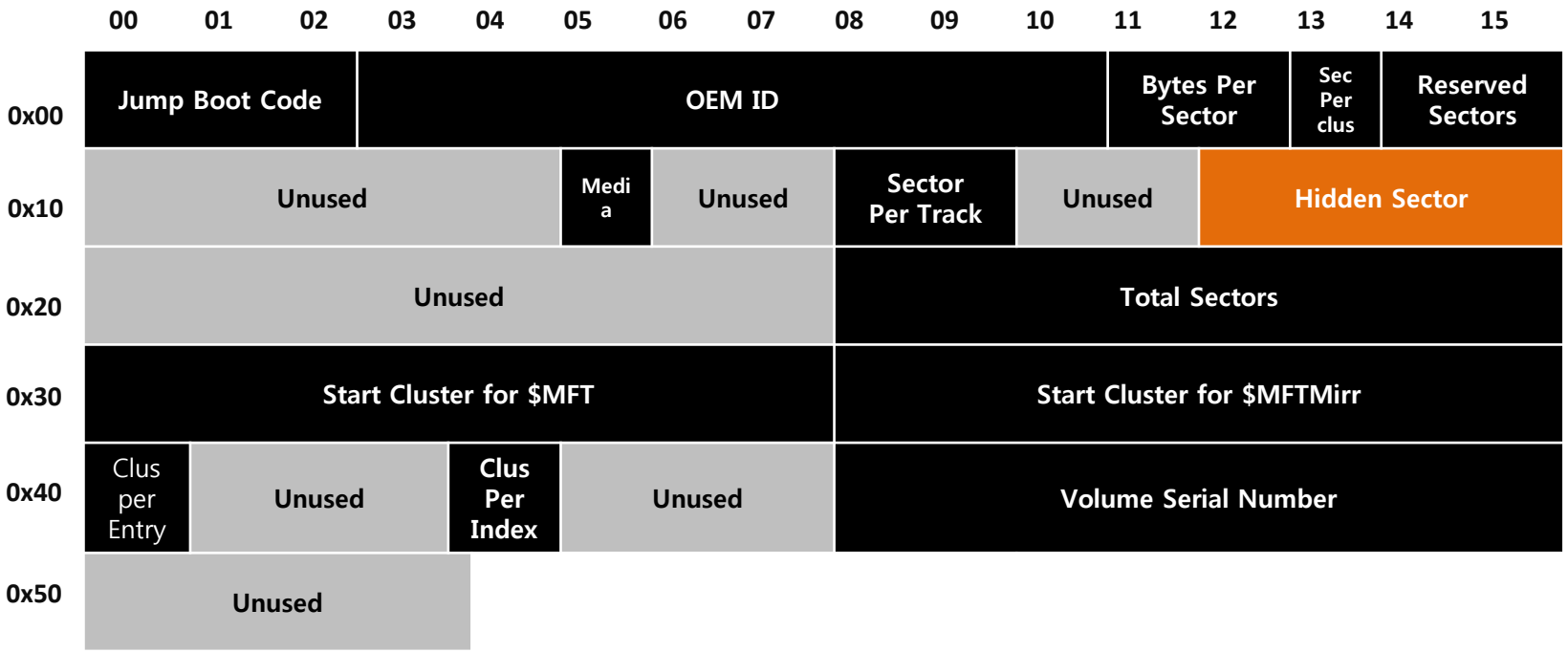
Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **Win32/Gapz: VBR Infector**



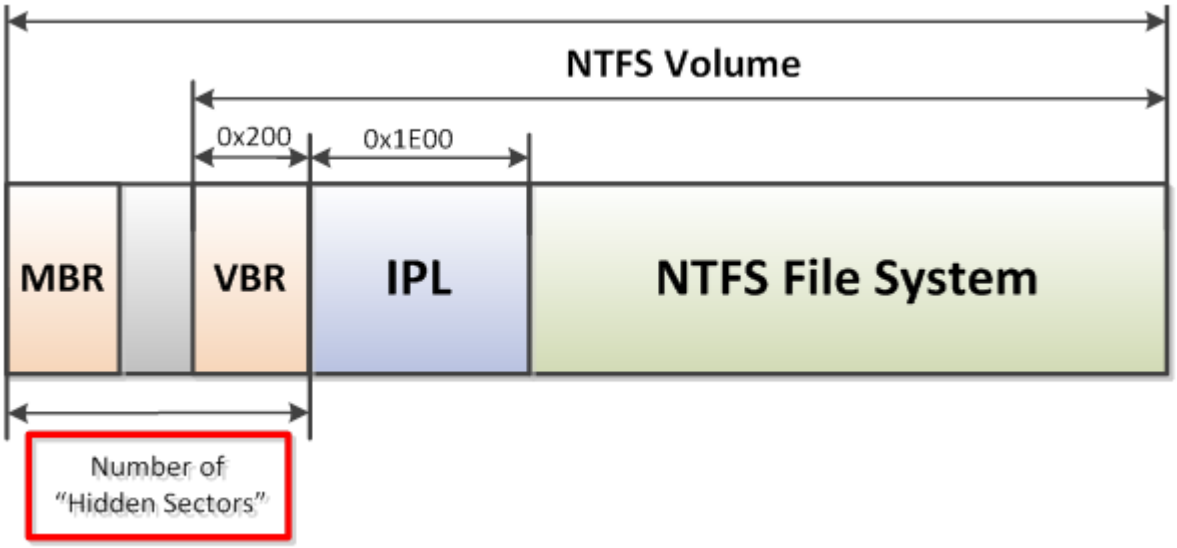
Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **Win32/Gapz: VBR Infector**
  - NTFS **BPB** (BIOS Parameter Block)



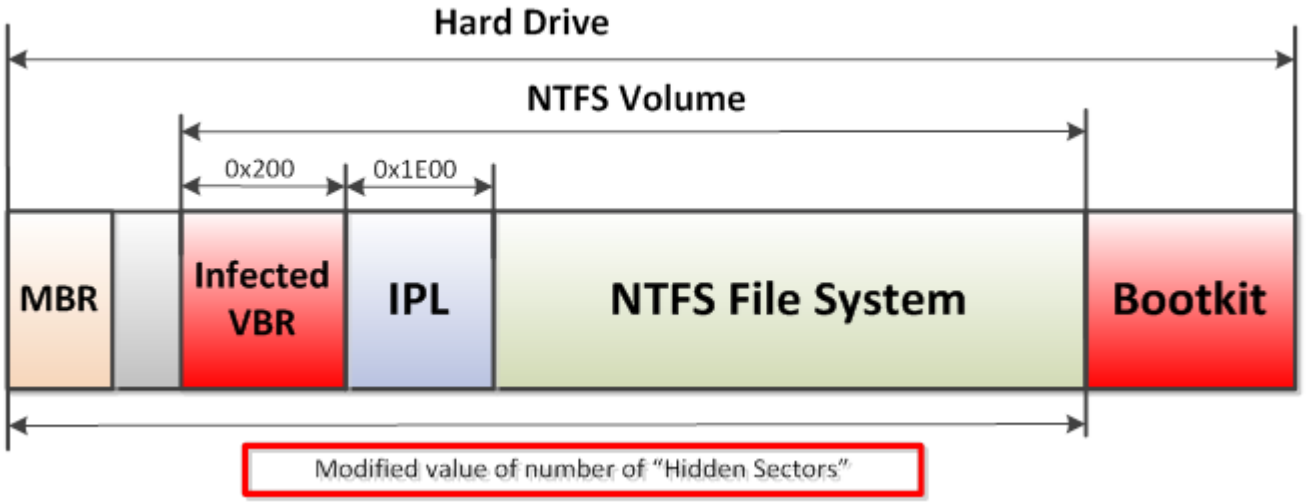
Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **Win32/Gapz: VBR Infector**
  - **Hidden Sector** : specifies IPL (Initial Program Loader) / MBR + MBR Slack (?)
    - ✓ Hidden Sector is generally **63**(0x3F, until windows vista). Hidden Sector of Win7 is **2048**(0x800)



Win32/Gapz: New Bootkit Technique (ESET Threat Blog)

- **Win32/Gapz: VBR Infector**
  - **Modified** "Hidden Sector" value
  - Run **Bootkit**



Protecting Privileged Domain Accounts: PsExec Deep-Dive (SANS Blog)

- **After further tests, It will be presented.**

Others

- **Android and iOS Forensics**: PIN Cracking, Backup Recovery, and More (**slide**)
- **NIST** updates, expands glossary of security terms
- 2013 **SC Magazine US Awards** Finalists
- **Windows 8 ASLR Internals**
- **OSX**/Dockster.A, Win32/Trojan.Agent.AXMO Samples, **OSX malware analysis tools**
- **Automatic Malware Analysis**: An Emulator Based Approach (**book**)
- **Current Android Malware**
- DFI News: **Mozilla Firefox Forensics Part I, II, III**
- **HTC Fuze Forensics**
- New **NIST** Document Offers **Guidance in Cryptographic Key Generation**

dForensics Challenges

- **DC3 2013 Forensic Challenge**
  - **Level 100**(5), **Level 200**(5), **Level 300**(5), **Level 400**(5), **Level 500**(5, require develpment of dForensics Tools)
  - **2013-04-02**: 20% Bonus Round Ends
  - **2013-07-02**: 10% Bonus Round Ends
  - **2013-10-02**: 5% Bonus Round Ends
  - **2013-10-16**: Registration Closes
  - **2013-11-01**: Solutions Due
  - **2013-12-02**: Winners Announced

- **Honeynet Forensic Challenge 13 – 'A Message in a Picture'**
  - **Hidden Channel (steganography)**
  - **Skill Level**: Intermediate
  - **Deadline**: 2013, Feb 15th

dForensics News

- **LawTimes** – '디지털 포렌식 전문가' 자격증 국가 공인으로
- **Chosun** – [궁금하다, 이 직업 | 디지털포렌식전문가] 범죄 단서 될 '디지털 자료' 분석… IT·법 지식 필요
- **BOAN News** – [정보보호법바로알기 18] 사례로 풀어보는 디지털 포렌식 절차 길라잡이
- **InformationWeek Security** – Guatemala Arrests Rogue AV Founder McAfee
- **CHANNELNOMICS** – Bitdefender Breaks Into Mobile Forensics

dForensics Tools

- **Autopsy** – v3.0.2 updated (windows only)
- **Windows Memory Reader** – CLI memory dump utility (32/64 bit, freely)
- **Dexter** – Static Android Application Analysis Tool
- **IOC Editor** – v2.2 updated
- **Support for the IP country/city database of MaxMind**
  - **NirSoft** – CurrPorts, SmartSniff, NetworkTrafficView, CountryTraceRoute
- Guidance Software announced the **Tableau T35u USB 3.0 forensic SATA/IDE bridge**
- **Redline** – v1.7 updated
- **iParser** – v1.0.0.20 updated

Question and Answer