

# **virse program messge Dos to Win**

차민석 책임 연구원

안철수연구소 시큐리티대응센터 분석1팀  
ASEC (AhnLab Security Emergency response Center)  
Anti-Virus Researcher

2011.7.2

[www.CodeEngn.com](http://www.CodeEngn.com)  
CodeEngn ReverseEngineering Conference

<sup>2011</sup>  
**Code**  **Engn**

 **Ah** 안철수연구소

# 시작하기 전에...

- 소개
- 3가지 특징
  - 반응 없음
  - 째려봄
  - 질문 없음
- 오탈자, 실수, 틀린 내용은 조용히 찾아오거나 메일로 ...
- **virse program messge Dos to Win**는 오타 아님
  - LBC 바이러스에서 가져온 문자열 (이후 설명)
- 목적
  - 디스크 입출력 악성코드 소개
- 감사
  - 안철수연구소 시큐리티대응센터 분석1팀 팀원

# 목 차

---

1. 디스크 입출력 이용 악성코드
2. 원도우에서 디스크 입출력
3. 추억의 **8090** 부트 바이러스
4. 원도우 부트레코드 감염
5. 주요 악성코드
6. 분석방법
7. 전망과 과제

# 1. 디스크 입출력 이용 악성코드

# 디스크 입출력 악성코드

- 디스크 입출력 악성코드 ?
  - 디스크 입출력으로 디스크 내용을 직접 변조하는 악성코드
  - 주로 주부트레코드, 파일 시스템, 특정 파일에 접근
- 악성코드 제작자 입장에서 이점
  - 기술적으로 어렵지 않음
  - 행동감시 프로그램 우회 가능성 높음
  - 자기 보호(백신 등) 프로그램 우회 변조 가능
  - MBR 변조 할 경우 MAOS (Malware OS)
- 현황
  - 폭발적인 증가세는 아직 없지만 조금씩 증가하고 있음
  - MBR 감염 형태의 악성코드도 지속 등장

# 디스크 입출력 이용 악성코드

- 디스크 입출력 악성코드 주요 사건
  - 2005년 : 블랙햇에서 eEye의 Bootroot 프로젝트 발표 (윈도우 2000/XP 전용)
  - 2007년 : NV labs의 Vbootkit (윈도우 비스타 동작)
  - 2007년 9월 : 윈도우 비스타 탑재 판매 시스템에서 Angelina 바이러스 발견
  - 2007년 11월 : MBR 루트킷 Mebroot(Sinowal) 확산 확인
  - 2008년 7월 : TDL1 발견
  - 2008년 10월: 디버깅 중이면 MBR 데이터 손상시키는 Win-Trojan/Killmbr.14848 발견
  - 2010년 2월 : TDL3와 MS10-015 충돌 (3.25 버전 이상에서 해결)
  - 2010년 5월 : MBR 변조 Win-Trojan/Torr (Yonsole)
  - 2010년 6월 : 부트 레코드를 변경하고 애드웨어 설치하는 Win-Trojan/Trup
  - 2010년 7월 : x64 윈도우 감염 징조 보이는 TDL3 3.27.3 버전 발견
  - 2010년 8월 : MBR 변조 및 userinit.exe 변조 Win-Trojan/Smitnyl

# 디스크 입출력 이용 악성코드

- 디스크 입출력 악성코드 주요 사건
  - 2010년 8월 : x64 윈도우 감염 TDL3 발견
  - 2010년 10월 : MBR 변조를 통해 돈을 요구하는 Win-Trojan/Saftad
  - 2010년 11월 : 64비트 윈도우 7 감염 TDL4

# 디스크 내용 변경 및 파괴

- 디스크 입출력으로 데이터 직접 변경 및 파괴
  - 주로 마스터 부트 레코드 내용 변경 해 부팅 불가
- 종류
  - Win-Trojan/Killmbr.14848 (2008년 10월 발견)
  - Win-Trojan/Torr.111104 (2010년 5월 발견)
  - Win-Trojan/Fakeav.103176 (2010년 6월)
  - 7.7 & 3.4 DDoS 공격 (2009년 7월 & 2011년 3월)
- 결과
  - 분석방해 -> 가상 환경이 아니라면 윈도우 재설치 !
  - 손쉬운 시스템 부팅 불가
  - 확실한 데이터 파괴

# 특정 파일 접근 혹은 변조

- FAT, NTFS 등 파일 시스템 구조를 해석해 디스크 입출력으로 대상 파일 접근
  - 드라이버 파일을 포함한 시스템 파일
  - 백신을 포함한 보안 프로그램
  - 일반 프로그램
- 결과
  - 레지스트리 변경 없이 자동 실행 가능
    - 주요 시스템 파일 변조
  - 보안 프로그램 방해
    - 패치 된 백신 프로그램은 검사 하는 듯 해도 실제 악성코드 진단 못함
    - 방화벽 우회

# 부트 레코드 변조(감염)

- 부트 레코드 변조 + 파일 변조
  - 도스 부트 바이러스와 유사한 형태
  - 다른 디스크로 직접 전파되지 않음 (바이러스는 아님)
  - Win-Trojan/Trup : 부트 레코드 감염 및 ntoskrnl.exe 변조
  - 부트 레코드와 파일 혹은 시스템을 감염시키는 부트/파일 바이러스 재등장 가능성 존재
- 부트킷 (Bootkit)
  - 부트킷 = 부트 레코드 감염 + (루트킷)
  - OS 시작 전에 악성코드가 먼저 실행
  - MAOS (Malware Operationg System) = Malware Platform
  - Mebroot, TDL(Alureon, TDSS, Tidser) 등

## 2. 윈도우에서 디스크 입출력

# 디스크 입출력

- **CreateFile – 간단한 디스크 입출력**
  - 파일이름 : \\.\PHYSICALDRIVE0, \\.\C:
  - <http://support.microsoft.com/kb/q100027>

```
HANDLE WINAPI CreateFile(
    __in      LPCTSTR lpFileName,
    __in      DWORD dwDesiredAccess,
    __in      DWORD dwShareMode,
    __in_opt   LPSECURITY_ATTRIBUTES lpSecurityAttributes,
    __in      DWORD dwCreationDisposition,
    __in      DWORD dwFlagsAndAttributes,
    __in_opt   HANDLE hTemplateFile
);
```

10002C1F	. 8D7C24 11	LEA EDI,DWORD PTR SS:[ESP+11]	hTemplateFile = NULL
10002C23	. 6A 00	PUSH 0	Attributes = 0
10002C25	. F3:A8	REP STOS DWORD PTR ES:[EDI]	Mode = OPEN_EXISTING
10002C27	. 66:AB	STOS WORD PTR ES:[EDI]	pSecurity = NULL
10002C29	. 6A 00	PUSH 0	ECX = C
10002C2B	. 6A 03	PUSH 3	ESI = 100047F0
10002C2D	. AA	STOS BYTE PTR ES:[EDI]	EDI = 0006F8A4
10002C2E	. 6A 00	PUSH 0	ShareMode = FILE_SHARE_READ FILE_SHARE_WRITE
10002C30	. B9 0C000000	MOV ECX,0C	Access = GENERIC_READ GENERIC_WRITE
10002C35	. BE F0470010	MOV ESI,WTsapnet.100047F0	FileName = "##.##PHYSICALDRIVE0"
10002C3A	. 8D7C24 20	LEA EDI,DWORD PTR SS:[ESP+20]	CreateFileA
10002C3E	. 6A 03	PUSH 3	
10002C40	. 68 000000C0	PUSH C0000000	
10002C45	. F3:A5	REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]	
10002C47	. 68 24480010	PUSH WTsapnet.10004824	
10002C4C	. C68424 2A0200	MOV BYTE PTR SS:[ESP+22A],55	
10002C54	. C68424 2B0200	MOV BYTE PTR SS:[ESP+22B],0AA	
10002C5C	. FF15 24300010	CALL DWORD PTR DS:[<&kernel32.CreateFileA>]	
10002C62	. 8BF0	MOV ESI,EAX	
10002C64	. 83FE FF	CMP ESI,-1	
10002C67	. 75 0B	JNZ SHORT WTsapnet.10002C74	

# 디스크 입출력

- Win-Trojan/Saftad.49664 물리 디스크 입출력

The screenshot shows assembly code for the `CreateFileA` function. The code is color-coded to highlight different registers and memory addresses. The assembly instructions include:

```
push    esi  
push    eax  
lea     eax, [ebp+FileName]  
push    offset a_Physicaldrive ; "wwwwww.PHYSICALDRIVE%d"  
push    eax  
call   convert_12d  
add    esp, 0Ch  
push    ebx          ; hTemplateFile  
push    ebx          ; dwFlagsAndAttributes  
push    3             ; dwCreationDisposition  
push    ebx          ; lpSecurityAttributes  
push    1             ; dwShareMode  
push    0C0000000h    ; dwDesiredAccess  
lea     ecx, [ebp+FileName]  
push    ecx          ; lpFileName  
call   ds:CreateFileA  
mov    esi, eax  
cmp    esi, 0FFFFFFFh  
jz     loc_4012C8
```

The screenshot shows assembly code for the `Check_infection` function. The assembly instructions include:

```
call   Check_infection  
test   al, al  
jnz   loc_4012C8
```

# 디스크 입출력

- Win-Trojan/Saftad.49664 물리 디스크 입출력

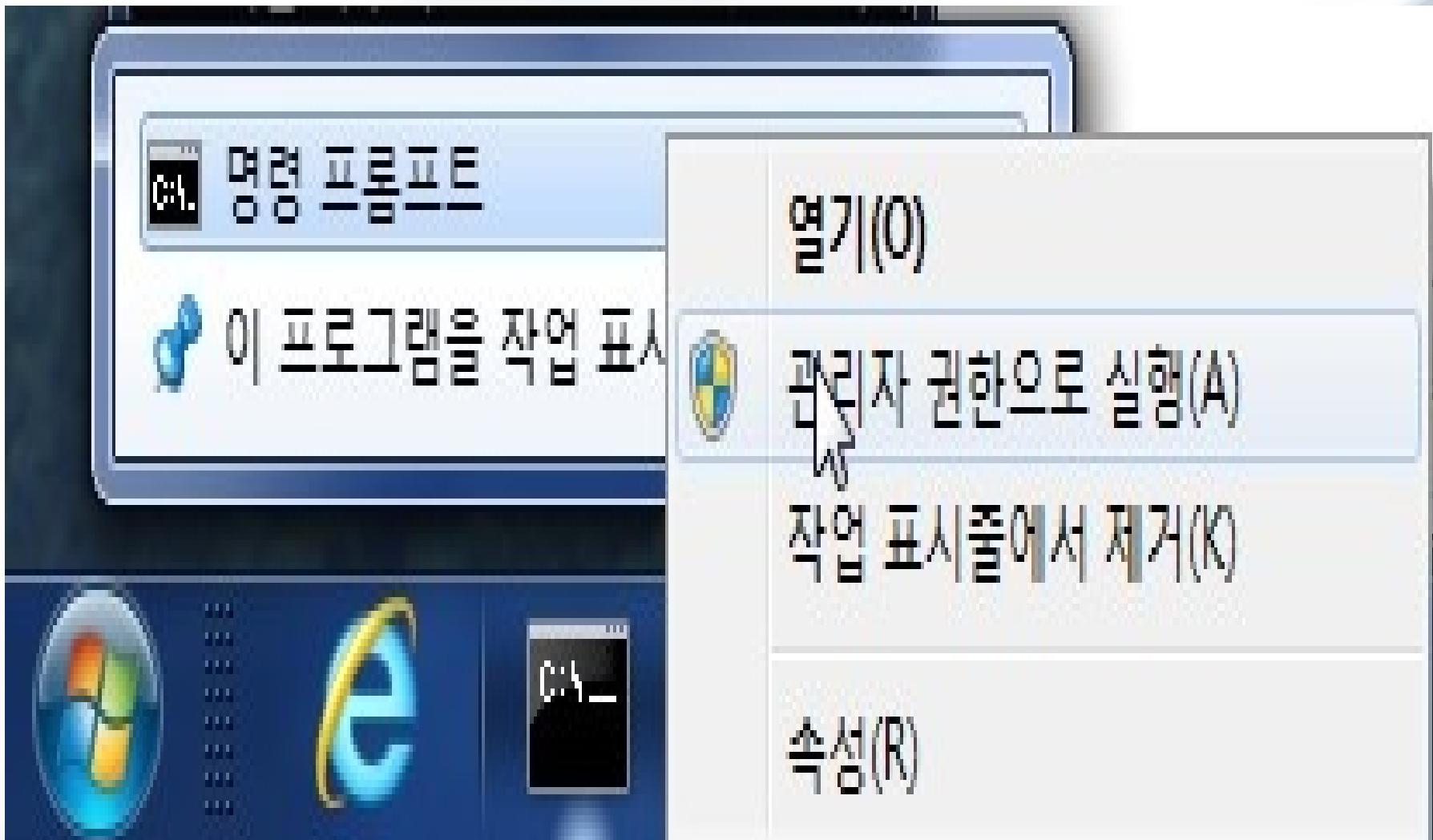
```
call    edi ; SetFilePointer
push    ebx      ; lpOverlapped
lea     edx, [ebp+NumberOfBytesRead]
push    edx      ; lpNumberOfBytesRead
push    200h    ; nNumberOfBytesToRead
lea     eax, [ebp+Buffer]
push    eax      ; lpBuffer
push    esi      ; hFile
call    ds:ReadFile
test   eax, eax
jz     short loc_4012C0
```

```
NUL
push    ebx      ; dwMoveMethod
push    ebx      ; lpDistanceToMoveHigh
push    ebx      ; lpDistanceToMove
push    esi      ; hFile
call    edi ; SetFilePointer
mov     edx, 1lpBuffer
push    ebx      ; lpOverlapped
lea     ecx, [ebp+NumberOfBytesWritten]
push    ecx      ; lpNumberOfBytesWritten
push    600h    ; nNumberOfBytesToWrite
push    edx      ; lpBuffer
mov     [ebp+NumberOfBytesWritten], ebx
mov     ebx, ds:WriteFile
push    esi      ; hFile
call    ebx ; WriteFile
test   eax, eax
jz     short loc_4012C0
```

```
NUL
push    0      ; dwMoveMethod
push    0      ; lpDistanceToMoveHigh
push    800h    ; lpDistanceToMove
mov     eax, 0AFBEh ; modify 55AA -> BEAF
push    esi      ; hFile
```

# 윈도우 Vista & 7

- 윈도우 Vista 와 7 에서는 관리자 권한으로 실행 권장

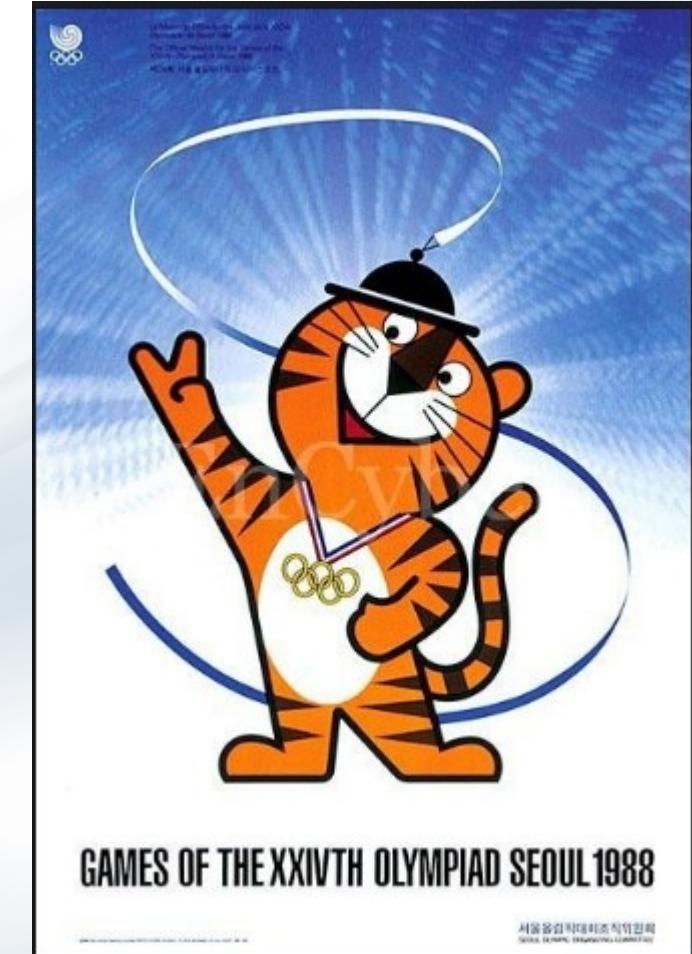


### 3. 추억의 8090 부트 바이러스

# 1988년

- 사회
  - 88 서울 올림픽
  - 필자는 컴퓨터 학원에서 애플 2 복제 컴퓨터 접함
- 브레인 바이러스 국내 유입
  - 안철수 박사 백신(Vaccine) 발표

```
1 ;  
2 ;  
3 : VACCINE.ASM    vaccine program for (c) Brain  
4 ;  
5 :                 by Ahn Cheolsoo  
6 ;  
7 : computer : IBM - PC/XT/AT  
8 : language : Microsoft Macro Assembler 5.0  
9 : creation : 1988. 6. 10.  
10;  
11;  
12 drive equ 0           ; drive A  
13 read  equ 2           ; function number of INT 13h  
14 write equ 3           ; function number of INT 13h  
15 boot  equ 1           ; boot sector  
16 FAT   equ 2           ; start of FAT  
17 dir1  equ 6           ; start of root directory  
18 dir2  equ 1           ; sector of side 1 dir  
19;  
20 Print MACRO string   ; string print function  
21     mov dx, offset string  
22     mov ah, 9  
23     int 21h  
24 ENDM  
25;  
26 Cr_Lf MACRO           ; carriage return & line feed  
27     mov ah, 2  
28     mov dl, Odh
```



# 1989년

- **사회**
  - 아시아나 항공 취항, 5공 청문회
  - 동유럽 혁명 일어나고 냉전이 끝남
  - 베를린 장벽 무너짐
  - 중국 텐안먼(천안문) 사건 발생
- **안철수 박사 LBC 바이러스로 백신 II와 예루살렘 바이러스로 백신 II 플러스 발표**
  - LBC 바이러스 등장 및 하드디스크 부팅 불가로 피해 속출
  - 새로운 컴퓨터 바이러스가 속속 국내 유입
- **필자는 Brain 바이러스와 LBC 바이러스에 감염된 디스크를 사용 못하는 줄 알고 컴퓨터 학원 친구에게 줌 -.-;;**
  - 당시 5.25 인치 플로피 디스크 약 2,000원
  - 당시 초등학생 버스비 60원 -> 버스 33회 !

# 도스 부트 바이러스 : Brain 바이러스

- 1986년 파키스탄 Amjad Farooq Alvi, Basit Farooq Alvi 형제가 제작
- 360 KB 플로피 디스크만 감염
- 감염된 디스크의 볼륨 이름 (c) Brain으로 변경
- 원형
  - 제작자 이름과 주소 포함

The image shows a screenshot of a hex editor displaying the Brain virus code. The left pane shows the hex dump, and the right pane shows the ASCII representation of the code. The ASCII text includes the virus's signature, creators' names, and their contact information.

Hex Address	Hex Value	ASCII Value	Text Content
00000000:	FA E9 4A 01 34 12 00 00 03 08 00 01 00 00 00 00 20		BJ@4† ♥♦ ⊙
00000010:	20 20 20 20.20 20 57 65.6C 63 6F 6D.65 20 74 6F		Welcome to
00000020:	20 74 68 65.20 44 75 6E.67 65 6F 6E.20 20 20 20		the Dungeon
00000030:	20 20 20 20.20 20 20 20.20 20 20 20.20 20 20 20		
00000040:	20 20 20 20.20 20 20 20.20 20 20 20.20 20 20 20		
00000050:	20 28 63 29.20 31 39 38.36 20 42 61.73 69 74 20		<c> 1986 Basit
00000060:	26 20 41 6D.6A 61 64 20.28 70 76 74.29 20 4C 74		& Amjad <put> Lt
00000070:	64 2E 20 20.20 20 20 20.20 20 20 20.20 20 20 20		d.
00000080:	20 42 52 41.49 4E 20 43.4F 4D 50 55.54 45 52 20		BRAIN COMPUTER
00000090:	53 45 52 56.49 43 45 53.2E 2E 37 33.30 20 4E 49		SERVICES..730 NI
000000A0:	5A 41 4D 20.42 4C 4F 43.4B 20 41 4C.4C 41 4D 41		ZAM BLOCK ALLAMA
000000B0:	20 49 51 42.41 4C 20 54.4F 57 4E 20.20 20 20 20		IQBAL TOWN
000000C0:	20 20 20 20.20 20 20 20.20 20 20 4C.41 48 4F 52		LAHOR
000000D0:	45 2D 50 41.4B 49 53 54.41 4E 2E 2E.50 48 4F 4E		E-PAKISTAN..PHON
000000E0:	45 20 3A 34.33 30 37 39.31 2C 34 34.33 32 34 38		E :430791,443248
000000F0:	2C 32 38 30.35 33 30 2E.20 20 20 20.20 20 20 20		.280530.
00000100:	20 20 42 65.77 61 72 65.20 6F 66 20.74 68 69 73		Beware of this
00000110:	20 56 49 52.55 53 2E 2E.2E 2E 2E 43.6F 6E 74 61		VIRUS.....Conta
00000120:	63 74 20 75.73 20 66 6F.72 20 76 61.63 63 69 6E		ct us for vaccin
00000130:	61 74 69 6F.6E 2E 2E 2E.2E 2E 2E 2E.2E 2E 2E 2E		ation....\$#0%\$0!! 길
00000140:	2E 2E 2E 2E.20 24 23 40.25 24 40 21.21 20 8C C8		

# 도스 부트 바이러스 : Brain 바이러스

## • 국내 유입 브레인 바이러스

## 도스 부트 바이러스 : Brain 바이러스

- 브레인 바이러스 제작자와 F-Secure 연구원 만남 (2011년 2월)
  - <http://campaigns.f-secure.com/brain/index.html>



# 도스 부트 바이러스 : Stoned 바이러스

- 1987년 뉴질랜드 고등학생이 제작 (미국 아님)
  - 원래 플로피 디스크만 감염 시킬 수 있으나 누군가 하드디스크도 감염시키도록 변형
  - 대마초 합법화 주장 메시지 포함
    - Stoned는 돌이 아닌 대마초에 몽롱한 상태를 의미하는 속어
  - 전 세계적으로 가장 널리 퍼지고 변형이 많은 부트 바이러스 중 하나
    - 미켈란젤로 바이러스도 Stoned 바이러스 변형

000000130:	00	02	B1	01.BA	80	00	CD.13	72	13	0E.1F	BE	00	02	© G =!!r!!j!!F
000000140:	BF	00	00	AD.3B	05	75	11.AD	3B	45	02.75	0B	2E	C6	! ;Au4; ;EBu6. !
000000150:	06	08	00	00.2E	FF	2E	11.00	2E	C6	06.08	00	02	B8	♦ . . . . ♦
000000160:	01	03	BB	00.02	B9	07	00.BA	80	00	CD.13	72	DF	0E	0*!! !C =!!r!!J
000000170:	1F	0E	02	BE.BE	03	BF	BE.01	B9	42	02.F3	A4	B8	01	▼!!-F-F-!P@!B@!S!@!Q
000000180:	03	33	DB	FE.C1	CD	13	EB.C5	07	59	6F.75	72	20	50	*3!-+!=!6+*Your P
000000190:	43	20	69	73.20	6E	6F	72.20	53	74	6F.6E	65	64	21	C is now Stoned!
0000001A0:	07	0D	0A	0A.00	4C	45	42.41	4C	49	53.45	20	4D	41	*FOO LEGALISE MA
0000001B0:	52	49	4A	55.41	4E	41	21.00	00	00	00.00	00	00	00	RIJUANA!
0000001C0:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
0000001D0:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
0000001E0:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	

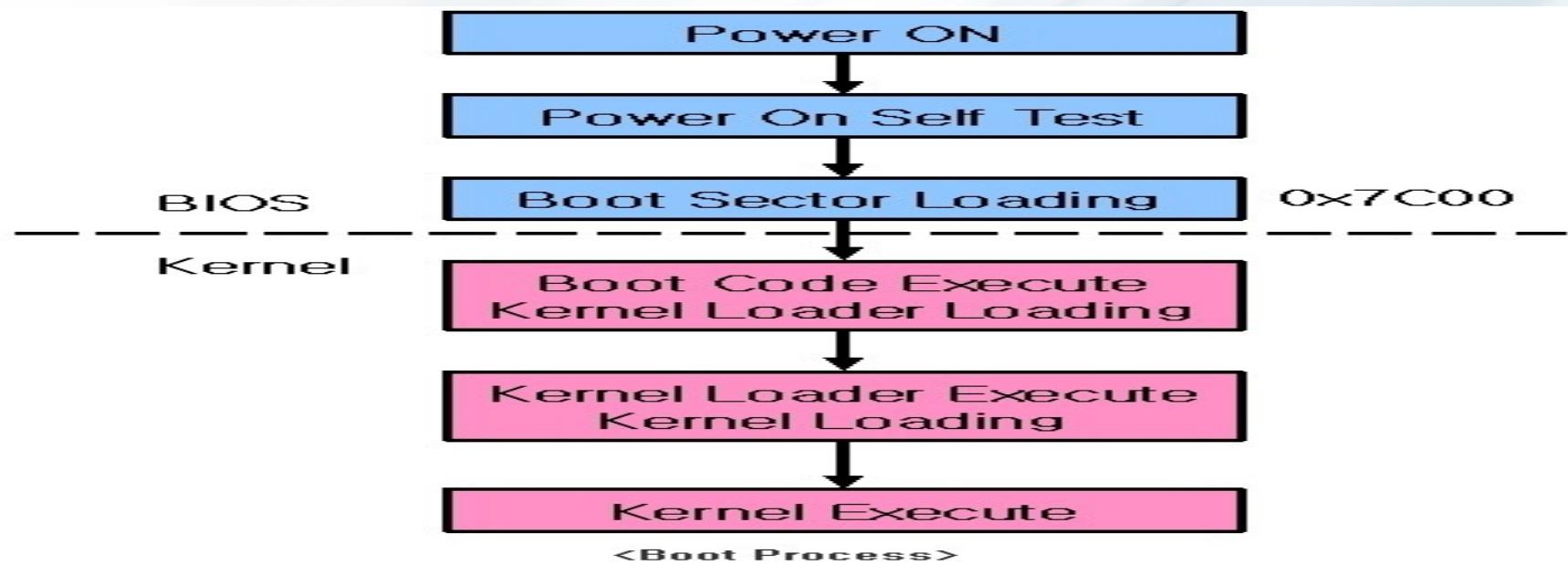
# 도스 부트 바이러스 : LBC 바이러스

- 1989년 제작된 국산 두 번째 컴퓨터 바이러스
  - Honey 바이러스가 최초
- 감염되면 하드디스크로 부팅되지 않고 인식되지 않아 포맷으로 인한 자료 손실로 많은 피해 일으킴(제작자 실수)
- 발표문서 제목은 virus program message Njh to Lbc에서 가져옴

000000100:	FF	2E	78	01.0E	07	B9	04.00	51	8A	26.7D	01	B0	01	ÿ.x0Fn•!♦ Qè&)>0
000000110:	8B	1E	82	01.8B	0E	80	01.8A	36	7F	01.8A	16	7E	01	íàéÓíñçQè64øè_~ø
000000120:	9C	FF	1E	78.01	73	0E	B4.00	9C	FF	1E.78	01	59	E2	Eyxóësñí EyxóëYñ
000000130:	D8	F9	EB	02.90	59	C3	20.76	69	72	73.65	20	70	72	½·ðæéY† virus pr
000000140:	6F	67	72	61.6D	20	20	20.6D	65	73	73.67	65	20	4E	ogram messge N
000000150:	6A	68	20	74.6F	20	4C	62.63	20	00	00.00	00	00	00	jh to Lbc
000000160:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
000000170:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
000000180:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
000000190:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
0000001A0:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
0000001B0:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	
0000001C0:	00	00	00	00.00	00	00	00.00	00	00	00.00	00	00	00	

# PC 부팅 과정

- MS-DOS, Windows를 포함한 PC 부팅 과정
  - 자기 검사 (Power-On Self-Test : POST)
  - 디스크 가장 처음에 위치한 코드(부트 레코드)를 0000:7C00에 로드 및 실행
- 운영체제와 상관없는 PC 계열의 기본 설정
  - 기본적으로 1981년 IBM PC 발표 당시 방식
  - 16비트 리얼모드로 시작 -> 보호모드로 진입



# 주부트 레코드

- **주부트레코드 (Master Boot Record)**
  - 실행 명령(부트 코드)과 디스크상에 주파티션 위치를 지정하는 4개의 항목을 가진 파티션 테이블이 있는 고정된 공간

Structure of a master boot record

Address			Description	Size in bytes
Hex	Oct	Dec		
0000	0000	0	code area	440 (max. 446)
0138	0670	440	disk signature (optional)	4
013C	0674	444	Usually nulls; 0x0000	2
013E	0676	446	Table of primary partitions (Four 16-byte entries, IBM partition table scheme)	64
01FE	0776	510	55h	2
01FF	0777	511	AAh	
MBR, total size: 446 + 64 + 2 =				512

# 주부트 레코드

- 파티션 테이블 정보
    - 1BEh 부터 시작 (80h는 부팅 가능한 영역)
    - 4개의 주파티션 포함 될 수 있음
    - 마지막 (1FE와 1FF)은 55h AAh로 종료
    - 파티션 정보가 없거나 잘못될 경우 디스크 부팅이 되지 않거나 인식이 되지 않음

**Boot Code  
446 Bytes**

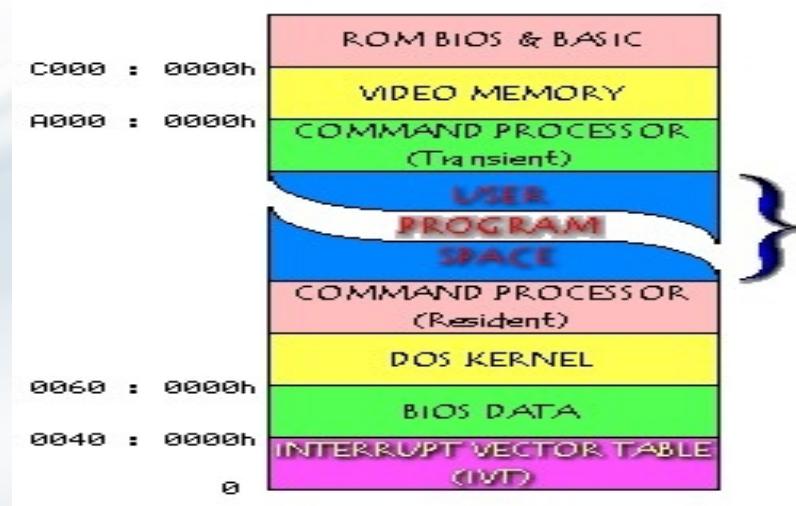
Partition 1 - 16 Bytes	
Partition 2 - 16 Bytes	
Partition 3 - 16 Bytes	
Partition 4 - 16 Bytes	55 AA

0000000A0: 00 B4 08 CD-13 72 23 8A-C1 24 3F 98-8A DE 8A FC 0=!!r#è1\$?ÿ€ à<sup>à</sup>  
0000000B0: 43 F7 E3 8B-D1 86 D6 B1-06 D2 EE 42-F7 E2 39 56 C\$¶i-àñ¶ü€B¤'9U  
0000000C0: 0A 77 23 72-05 39 46 08-73 1C B8 01-02 BB 00 7C ¶w#r#9Fos-àççñ !  
0000000D0: 88 4E 02 8B-56 00 CD 13-73 51 4F 74-4E 32 E4 8A INGiu =!sQ0tN2Èè  
0000000E0: 56 00 CD 13-EB E4 8A 56-00 60 BB AA-55 B4 41 CD U =!!δΣèU 'ù-Ü|A=  
0000000F0: 13 72 36 81-FB 55 AA 75-30 F6 C1 01-74 2B 61 60 !!r6üçÜ-üu0-1@t+a'  
00000100: 6A 00 6A 00-FF 76 0A FF-76 08 6A 00-68 00 7C 6A j. j. yvØyv¤j h !j  
00000110: 01 6A 10 B4-42 8B F4 CD-13 61 61 73-0E 4F 74 0B @j-|Bi|=!aasß0t€  
00000120: 32 E4 8A 56-00 CD 13 EB-D6 61 F9 C3-49 6E 76 61 2ΣèU =!!δηα·|Inva  
00000130: 6C 69 64 20-70 61 72 74-69 74 69 6F-6E 20 74 61 lid partition ta  
00000140: 62 6C 65 00-45 72 72 6F-72 20 6C 6F-61 64 69 6E ble Error loadin  
00000150: 67 20 6F 70-65 72 61 74-69 6E 67 20-73 79 73 74 g operating syst  
00000160: 65 6D 00 4D-69 73 73 69-6E 67 20 6F-70 65 72 61 em Missing opera  
00000170: 74 69 6E 67-20 73 79 73-74 65 6D 00-00 00 00 00 ting system  
00000180: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00  
00000190: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00  
000001A0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00  
000001B0: 00 00 00 00-00 2C 44 63-49 7A 49 7A-00 00 80 01 ,DcIzIz\_0e  
000001C0: 01 00 07 FE-FF FF 3F 00-00 00 26 B9-DF 21 00 00 00 ••yy? &|¶@  
000001D0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00  
000001E0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 00  
000001F0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 55 AA 0z

# MS-DOS 메모리 구조

- **MS-DOS 메모리 구조**
  - 기본 메모리는 최대 640 킬로바이트 (KB)
  - 당시 640 KB 이하 메모리 용량도 많아 000:0413h에 메모리 용량 정보 보관
  - 0000:0413h-0000:0414h memory size: normally accessed via interrupt 12h
- **참조**
  - <http://www.osdata.com/system/physical/lowmem.htm>

Memory Type	Total	=	Used	+	Free
Conventional	640 KB		122K		518K
Upper	155K		41K		144K
Reserved	128K		128K		0K
Extended (XMS)	7,269K		2,486K		4,783K
Total Memory	81,259K		21,777K		5,415K
Total under 1 MB	795K		163K		632K
Largest executable program size			518K (530,096 bytes)		
Largest free upper memory block			114K (116,352 bytes)		



# 부트 바이러스 원리

- 보통 최상위 영역의 메모리에 자기 복사하고 기억장소 줄임
  - 기본메모리 용량을 보관하는 0000:0413h 번지 값 줄임
  - 도스가 사용하지 않아 바이러스 코드 보호
- 인터럽트 벡터 주소 가로챔
  - 보통 디스크 입출력 담당하는 인터럽트 13h 가로챔
  - 인터럽트 13h 주소는 000:004Ch 에 존재
- 보관한 정상 부트 레코드나 자체 기능으로 재 부팅
  - 다른 부트 바이러스에 감염된 경우 2가지 부트 바이러스가 동시 활동
- 사용되는 플로피 디스크 혹은 하드 디스크 감염
  - 보통 정상 부트 레코드로 재 부팅 전 하드디스크 감염
  - DIR 등 명령 때 다수의 인터럽트 13h 수행 -> 디스크 입출력 속도 저하
- 기타 의도된 증상
  - 디스크 볼륨 이름 변경, 메시지 출력, 디스크 데이터 파괴 등

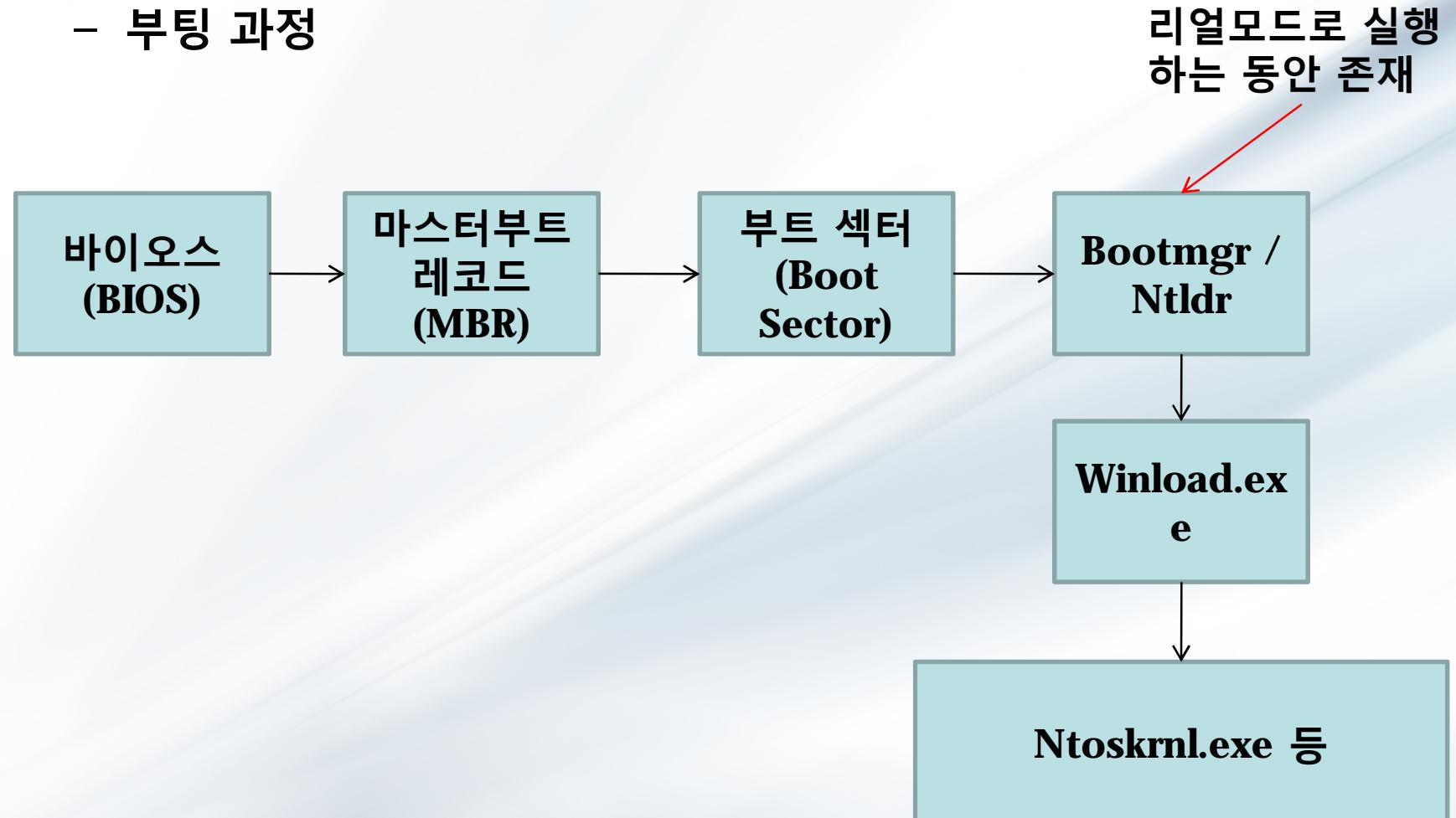
# 윈도우 95 등장과 부트 바이러스

- 32비트 디스크 입출력으로 인터럽트 13h가 더 이상 이용하지 않음
  - 인터럽트 13h를 가로채는 부트 바이러스는 다른 디스크를 감염 시킬 수 없음
  - 루마니아 RP가 제작한 Dodgy 바이러스는 system\iosubsys\hsflop.pdr 파일 삭제하는 우회 기법 이용
- 다수의 부트 바이러스는 윈도우 95 이상 시스템에서 오동작 일으킴
- 플로피 디스크 사용이 급격히 줄어듦
  - 더 이상 부트 바이러스 확산이 어려움
- 윈도우 NT 기반의 윈도우 2000과 윈도우 XP 이후 부트 바이러스는 거의 멸종됨
- 2011년 현재도 부트 바이러스는 종종 보고 !
  - V3에서 부트 바이러스 치료 기능 제외
  - 치료 요청 올 경우 전용 백신 제공 -> 종종 접수

## 4. 윈도우 부트레코드 감염

# 윈도우 부팅 과정

- 윈도우 부팅 과정
  - 초반부는 MS-DOS와 동일
  - 부팅 과정



# 보호모드로 전환시키는 Bootmgr

- Windows 7 bootmgr과 Windows XP ntldr

Offset:	0h, 0	Sector:	0:0	Dec [2]:	54761
0:	E9 D5 01 EB 04 90 00 00 00 52 8B C3 0E 07 66 33			8 F06♦E Ri Jn-f3	
10:	DB BA 01 00 E8 34 00 E9 51 01 2E 88 16 06 00 50			■ @ 04 8Q0.é-♦ P	
20:	66 0F B6 54 02 66 0F B7 04 66 F7 E2 66 C1 E8 04			f+ Tf*f* [♦f*Gf-♦♦	
30:	2E A3 07 00 8C C1 03 C8 8E C1 58 E8 30 00 0F 82			.ú. i-♦Lá Xg0 xé	
40:	05 00 E8 06 00 EB F4 5A E9 8D 01 8B CA 8B D0 52			♦ ♦ ♦ ♦ fZ0i@i"i"R	
50:	51 06 66 53 8A 44 02 FF 1D 66 5B 07 8C C1 2E 03			Q♦fSèDøy+f[•i-♦	
60:	0E 07 00 8E C1 59 5A 42 E2 E5 4A 8B C2 C3 66 53			R. àYZBfGJiTfS	
70:	66 53 50 E8 CA 00 E8 3A 00 66 8B C8 58 66 8B DA			fSPø" ♦: filXfir	
80:	E8 80 00 66 5B 83 FA FF 0F 85 05 00 33 D2 F9 EB			øC fIâ·y*à·3n·ô	
90:	1F 8B C2 50 E8 A9 00 66 3B C8 0F 84 03 00 E8 12			▼iTfØ- f;lxaw ♦	
[1] File: Z:\WORK\NTLDR Size: 259,776					
Offset:	0h, 0	Sector:	0:0	Dec [2]:	54761
0:	E9 D5 01 EB 04 90 00 00 00 52 8B C3 0E 07 66 33			8 F06♦E Ri Jn-f3	
10:	DB BA 01 00 E8 34 00 E9 51 01 2E 88 16 06 00 50			■ @ 04 8Q0.é-♦ P	
20:	66 0F B6 54 02 66 0F B7 04 66 F7 E2 66 C1 E8 04			f+ Tf*f* [♦f*Gf-♦♦	
30:	2E A3 07 00 8C C1 03 C8 8E C1 58 E8 30 00 0F 82			.ú. i-♦Lá Xg0 xé	
40:	05 00 E8 06 00 EB F4 5A E9 8D 01 8B CA 8B D0 52			♦ ♦ ♦ ♦ fZ0i@i"i"R	
50:	51 06 66 53 8A 44 02 FF 1D 66 5B 07 8C C1 2E 03			Q♦fSèDøy+f[•i-♦	
60:	0E 07 00 8E C1 59 5A 42 E2 E5 4A 8B C2 C3 66 53			R. àYZBfGJiTfS	
70:	66 53 50 E8 CA 00 E8 3A 00 66 8B C8 58 66 8B DA			fSPø" ♦: filXfir	
80:	E8 80 00 66 5B 83 FA FF 0F 85 05 00 33 D2 F9 EB			øC fIâ·y*à·3n·ô	
90:	1F 8B C2 50 E8 A9 00 66 3B C8 0F 84 03 00 E8 12			▼iTfØ- f;lxaw ♦	
[1] File: Z:\WORK\BOOTMGR Size: 383,786					
Offset:	190h, 400	Sector:	0:400	Dec [2]:	3942
190:	66 0F B7 44 06 66 C1 E0 05 66 0F B7 1C 66 03 C3			f*øDøf-♦f*ø-f*†	
1A0:	66 48 66 33 D2 66 F7 F3 66 2B C8 66 0F B7 44 03			fHf3øf≈f+4f*øDø	
1B0:	66 2B C8 66 8B C1 66 0F B6 4C 02 66 33 D2 66 F7			f+4f i-♦f* [Løf3øf≈	
1C0:	F1 32 D2 66 3D F5 0F 00 00 0F 83 02 00 FE C2 66			±2øf=J* øøø IJf	
1D0:	59 66 5B 66 58 E9 42 FE BB E0 3D C1 EB 04 8C C8			Yf lfXøBøø=±δ♦iL	
1E0:	03 C3 8E D0 BC 80 0C 52 8E D8 8E C0 66 33 ED 66			ø HwøCøRa†øf3øf	
1F0:	0F B7 E4 8C 1E 34 15 8C 0E 36 15 E8 6E 03 00 00			*øøø 14481ø6øøøø	
200:	66 55 66 53 66 56 66 57 66 8B DC B8 60 00 0E D8			fUfSfUfWfiføøøøø	
210:	8E D0 BC 80 14 66 33 ED 66 0F B7 E4 66 53 66 B9			øøøøf3øf*øøøøøø	
220:	02 00 00 00 66 8B F3 66 03 C6 14 6A 30 1F 16 07			ø fiøføøjøøøøø	
[1] File: Z:\WORK\NTLDR Size: 259,776					
Offset:	190h, 400	Sector:	0:400	Dec [2]:	3942
190:	66 0F B7 44 06 66 C1 E0 05 66 0F B7 1C 66 03 C3			f*øDøf-♦f*ø-f*†	
1A0:	66 48 66 33 D2 66 F7 F3 66 2B C8 66 0F B7 44 03			fHf3øf≈f+4f*øDø	
1B0:	66 2B C8 66 8B C1 66 0F B6 4C 02 66 33 D2 66 F7			f+4f i-♦f* [Løf3øf≈	
1C0:	F1 32 D2 66 3D F5 0F 00 00 0F 83 02 00 FE C2 66			±2øf=J* øøø IJf	
1D0:	59 66 5B 66 58 E9 42 FE BB 40 2F C1 EB 04 8C C8			Yf lfXøBøø=±δ♦iL	
1E0:	03 C3 8E D0 BC 28 15 52 8E D8 8E C0 66 0F B7 D0			ø HwøCøRa†øf3øf	
1F0:	66 C1 E2 04 66 81 C2 80 1D 00 00 66 89 16 BE 0C			f+Γ♦fUfC+ø f-øøø	
200:	33 ED 66 0F B7 ED 66 0F B7 E4 8C 1E BC 15 E8 0F			3øf*øøf*øøøøøøø	
210:	17 66 68 00 00 00 00 66 9D 8B DC 8B 57 02 33 C0			øøøøøøøøøøøøøøø	
220:	8E E8 8E C0 6A 30 0F A1 FA 0F 01 16 A8 15 0F 01			øøøøøøøøøøøøøøø	

# 도스 부트 바이러스 원리 응용

- 디스크 입출력 인터럽트 (Int 13h) 후킹 후 윈도우 부팅 과정에서 코드 변조

## eEye BootRootKit – OSLOADER Patch

32

- We patch 6 bytes executed after boot driver load:

```
0031ADF1 BB F0      MOV    ESI, EAX
0031ADF3 85 F6      TEST   ESI, ESI
0031ADF5 74 21      JZ    $+23h
0031ADF7 80 ...     ; not modified, only used as part of signature
```

- Hook must be absolute – we don't know where code will load
  - "CALL seg:ofs32" is 7 bytes
  - "CALL DWORD PTR [ ofs32 ] " is 6 bytes – perfect for this patch site
- We use "CALL DWORD PTR [ addr1 ] ", where [ addr1 ] = addr2, and both addr1 and addr2 are addresses in our resident code
- Paging is not a concern – OSLOADER will map low 16MB virtual memory to low 16MB physical memory

## 5 주요 악성코드

# Win-Trojan/Killmbr.14848

- World of Warcraft 게임 사용자 계정과 암호 유출 악성코드
  - 2008년 10월 발견
  - 디버깅 중이면 MBR 내용을 변경해 부팅 되지 않게 함

.10004760:	66 6D 74 2E.6C 6F 67 00.6B 72 2E 6C.6F 67 6F 6E	fmt.log kr.logon
.10004770:	2E 77 6F 72.6C 64 6F 66.77 61 72 63.72 61 66 74	.worldofwarcraft
.10004780:	2E 63 6F 6D.3A 33 37 32.34 00 00 00.66 6D 74 74	.com:3724 fmtt
.10004790:	65 6D 70 2E.6C 6F 67 00.53 4F 46 54.57 41 52 45	emp.log SOFTWARE
.100047A0:	5C 42 6C 69.7A 7A 61 72.64 20 45 6E.74 65 72 74	\Blizzard Entert
.100047B0:	61 69 6E 6D.65 6E 74 5C.57 6F 72 6C.64 20 6F 66	ainment\World of
.100047C0:	20 57 61 72.63 72 61 66.74 00 00 00.49 6E 73 74	Warcraft Inst
.100047D0:	61 6C 6C 50.61 74 68 00.52 45 47 5F.53 5A 00 00	allPath REG_SZ
.100047E0:	57 54 46 5C.41 63 63 6F.75 6E 74 5C.00 00 00 00	WTF\Account\
.100047F0:	B8 12 00 CD.10 BD 18 7C.B9 18 00 B8.01 13 BB 9C	↑ ↑ ↑! ↑ 0!! ♀
.10004800:	00 BA 1D 0E.CD 10 E2 FE.49 20 61 6D.20 76 69 72	↑ I am vir
.10004810:	75 73 21 20.46 75 63 6B.20 79 6F 75.20 3A 2D 29	us! Fuck you :-(
.10004820:	30 00 00 00.5C 5C 2E 5C.50 48 59 53.49 43 41 4C	\\.\PHYSICAL
.10004830:	44 52 49 56.45 30 00 00.00 00 00 00.00 00 00 00	DRIVE0

# Win-Trojan/Torr (Yonsole)

- 2010년 5월 발견
  - <http://blogs.technet.com/b/mmpc/archive/2010/06/18/your-pc-has-been-stoned-again.aspx>
- 원격 명령 중 MBR 변조해 부팅 불가 기능 존재

```
case 0x36: —
    result = sub_12405FB0(0);
    break;
case 0x37:
    result = (int)write_MBR();
    break;
case 0x38:
    result = sub_124068E0(this);
    break;
case 0x39:
```

- MBR 변경

```
result = CreateFileA("WWW.WWPHYSICALDRIVE0", 0xC0000000u, 3u, 0, 3u, 0, 0);
v1 = result;
if ( result != (HANDLE)-1 )
{
    dword_1241951C(0, &v4, 260);
    DeviceIoControl(v1, 0x90018u, 0, 0, 0, 0, &BytesReturned, 0);
    dword_12419518(&v4, &v4, 260);
    WriteFile(v1, &Buffer, 0x200u, &NumberOfBytesWritten, 0);
    dword_1241951C(0, &v4, 260);
    DeviceIoControl(v1, 0x9001Cu, 0, 0, 0, 0, &BytesReturned, 0);
    dword_12419518(&v4, &v4, 260);
    CloseHandle(v1);
```

# Win-Trojan/Torr (Yonsole)

- 변경되는 코드는 메시지 출력 후 중지(무한 루프)

```

.12417090: 6C 6A 3B 6F-6C 6A 68 6F-52 4B 55 6A-42 4B 55 68 1j;oljh0RKUjBKUh
.124170A0: 64 51 5B 55-6B 42 00 00-60 42 41 12-00 00 00 00 dQIUKB `BA‡
.124170B0: 2E 50 41 58-00 00 00 00-60 42 41 12-00 00 00 00 .PAX `BA‡
.124170C0: 2E 50 41 44-00 00 00 00-54 79 70 65-00 00 00 00 .PAD Type
.124170D0: 53 59 53 54-45 4D 5C 43-75 72 72 65-6E 74 43 6F SYSTEM\CurrentCo
.124170E0: 6E 74 72 6F-6C 53 65 74-5C 53 65 72-76 69 63 65 ntrolSet\Service
.124170F0: 73 5C 00 00-31 30 2E 31-30 2E 31 30-2E 31 30 00 s\ 10.10.10.10
.12417100: 00 00 00-00-00 00 00 00-00 00 00 00-00 00 00 00
.12417110: 00 00 ►00 0-50 00 00 00-B8 12 00 CD-10 BD 18 7C P ↗↑ →U↑
.12417120: B9 18 00 8-01 13 BB 0C-00 BA 1D 0E-CD 10 E2 FE █↑ ↗Θ!!Γ♀ █↑→Γ█
.12417130: 3D 3D 3D 3D-3D 3D 3D 3D-3D 3D 3D 3D-3D 3D 3D =====
.12417140: 3D 3D 3D 3D-3D 3D 3D 3D-3D 00 00 00-5C 64 65 73 =====■ \des
.12417150: 6B 74 6F 70-2E 69 6E 66-00 00 00 00-47 51 6C 4B ktop.inf GQ1K
.12417160: 6A 59 2E 42-3A 55 54 59-65 52 6A 00-6E 31 70 35 jY.B:UTYeRj n1p5
.12417170: 64 34 61 31-74 65 00 00-39 6E 6E 52-51 5B 59 6A d4aite 9nnRQlYj
.12417180: 51 6F 6C 6B-42 51 55 66-6E 52 6F 68-55 2C 55 66 Qo1kBQUFnRohU_Uf
.12417190: 55 42 6B 56-55 52 52 42-6F 6E 55 6C-42 5B 6F 6D UBkUURRBonUlBlom
.124171A0: 6D 59 6C 5A-00 00 00 00-4B 61 6B 6A-55 6D 00 00 mY1Z KakJUm
.124171B0: 4B 55 5B 65-68 51 6A 61-00 00 00 00-39 6E 6E 52 KULehQja 9nnR
.124171C0: 51 5B 59 6A-51 6F 6C 00-48 6F 73 74-00 00 00 00 QIYjQo1 Host
.124171D0: 50 6C 75 67-69 6E 46 75-6E 63 00 00-53 65 44 65 PluginFunc SeDe
.124171E0: 62 75 67 50-72 69 76 69-6C 65 67 65-00 00 00 00 bugPrivilege

```

000000000:	B81200	mov	ax, 000012
000000003:	CD10	int	010
000000005:	BD187C	mov	bp, 07C18 ;'↑'
000000008:	B91800	mov	cx, 000018
00000000B:	B80113	mov	ax, 01301
00000000E:	BB0C00	mov	bx, 00000C
000000011:	B81D0E	mov	dx, 00E1D
000000014:	CD10	int	010
000000016:	E2FE	1 loop	0000000016 --↑1
000000018:	3D3D3D	cmp	ax, 03D3D ;'=='
00000001B:	3D3D3D	cmp	ax, 03D3D ;'=='
00000001E:	3D3D3D	cmp	ax, 03D3D ;'=='
000000021:	3D3D3D	cmp	ax, 03D3D ;'=='
000000024:	3D3D3D	cmp	ax, 03D3D ;'=='
000000027:	3D3D3D	cmp	ax, 03D3D ;'=='
00000002A:	3D3D3D	cmp	ax, 03D3D ;'=='
00000002D:	3D3D3D	cmp	ax, 03D3D ;'=='

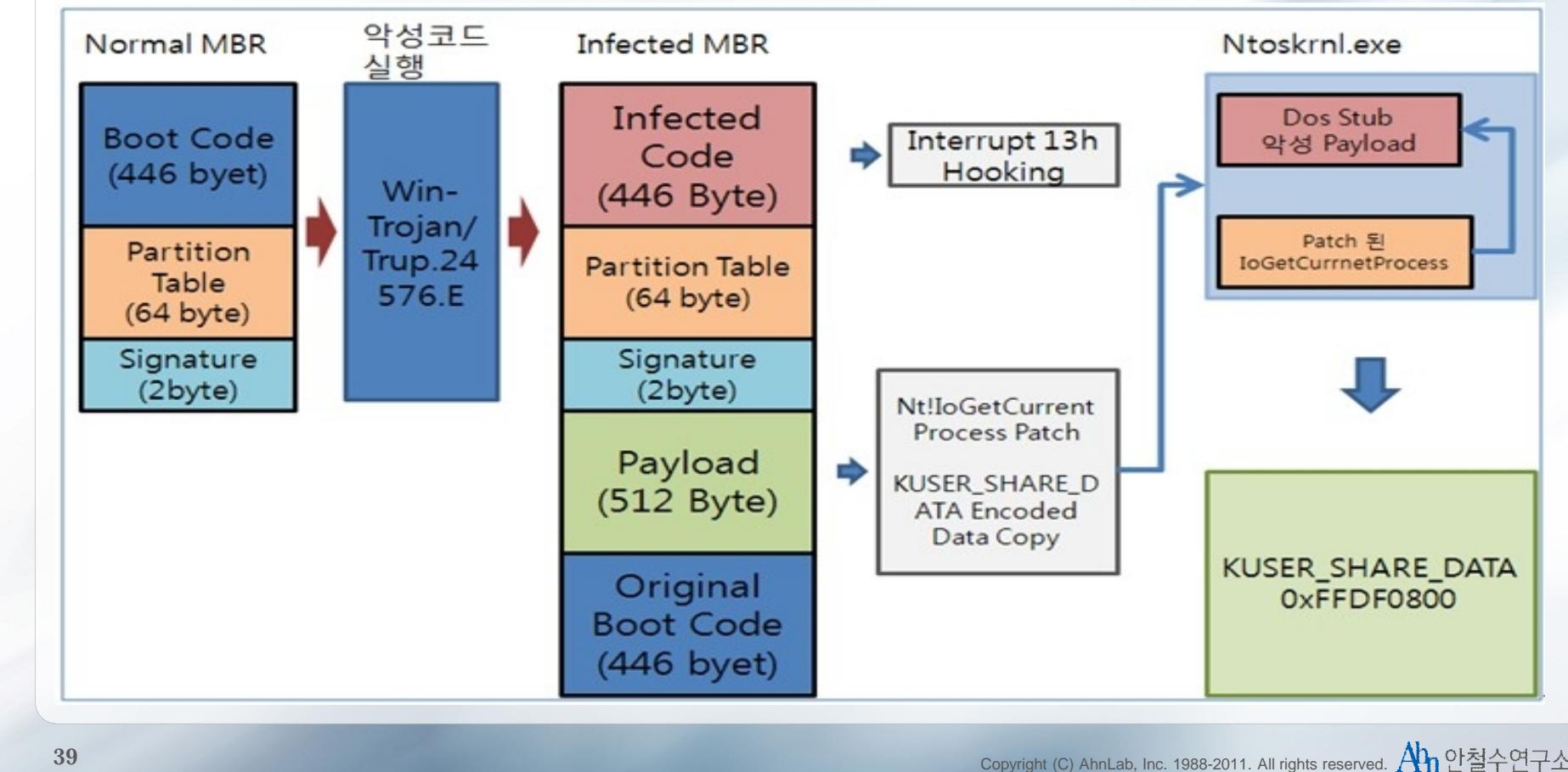
# Win-Trojan/Saftad.49664

## • 변조된 부트 레코드

00000490:	3C	6C	20	74-68	65	20	68-61	72	64	20-64	72	69	76	11	the hard driv
000004A0:	65	73	20	77-65	72	65	20-65	6E	63	72-79	70	74	65	es were encrypte	
000004B0:	64	2E	0D	0A-42	72	6F	77-73	65	20	77-77	77	2E	73	d.JBrowse www.s	
000004C0:	61	66	65	2D-64	61	74	61-2E	72	75	20-74	6F	20	67	afe-data.ru to g	
000004D0:	65	74	20	61-6E	20	61	63-63	65	73	73-20	74	6F	20	et an access to	
000004E0:	79	6F	75	72-20	73	79	73-74	65	6D	20-61	6E	64	20	your system and	
000004F0:	66	69	6C	65-73	2E	0D	0A-41	6E	79	20-61	74	74	65	files.JAny atte	
00000500:	6D	70	74	20-74	6F	20	72-65	73	74	6F-72	65	20	74	mpt to restore t	
00000510:	68	65	20	64-72	69	76	65-73	20	75	73-69	6E	67	20	he drives using	
00000520:	6F	74	68	65-72	20	77	61-79	20	77	69-6C	6C	20	0D	other way will J	
00000530:	0A	6C	65	61-64	20	74	6F-20	69	6E	65-76	69	74	61	Clead to inevita	
00000540:	62	6C	65	20-64	61	74	61-20	6C	6F	73-73	20	21	21	ble data loss !!	
00000550:	21	0D	0A	50-6C	65	61	73-65	20	72	65-6D	65	6D	62	?JPleas rememb	
00000560:	65	72	20	59-6F	75	72	20-49	44	3A	20-37	37	33	39	er Your ID: 7739	
00000570:	32	31	2C	20-0D	0A	77	69-74	68	20	69-74	73	20	68	21, Jwith its h	
00000580:	65	6C	70	20-79	6F	75	72-20	73	69	67-6E	2D	6F	6E	elp your sign-on	
00000590:	20	70	61	73-73	77	6F	72-64	20	77	69-6C	6C	20	62	password will b	
000005A0:	65	20	67	65-6E	65	72	61-74	65	64	2E-00	00	00	00	e generated.	
000005B0:	00	00	00	00-00	00	00	00-00	00	45	6E-74	65	72	20	Enter	
000005C0:	70	61	73	73-77	6F	72	64-3A	00	00	00-00	00	00	00	password:	
000005D0:	00	00	00	00-00	00	00	00-00	00	57	72-6F	6E	67	20	Wrong	
000005E0:	70	61	73	73-77	6F	72	64-00	00	00	00-00	00	00	00	password	
000005F0:	00	00	00	00-00	00	00	00-00	00	01	3C-68	6A	6D	63	0Kjhjmc	

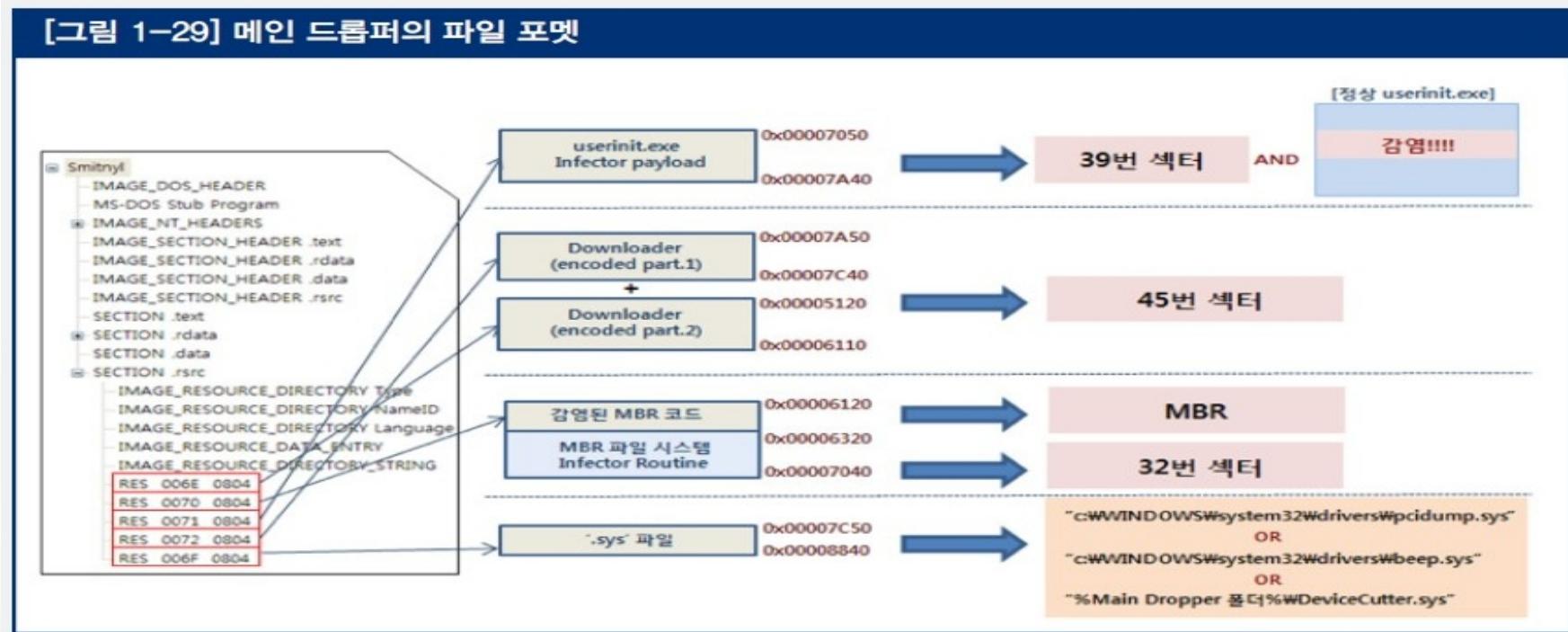
# Win-Trojan/Trup

- 부트 레코드 변형 및 애드웨어 다운로드
  - 2010년 6월 발견
  - Ntoskrnl.exe 의 IoGetCurrentProcess() 함수 패치
  - 개념도 (by 안철수연구소 시큐리티대응센터 분석1팀 이도한 연구원)



# Win-Trojan/Smitnyl

- MBR 감염 및 userinit.exe 변조
  - 2010년 8월 발견
  - 원본 MBR은 섹터 5에 백업
  - 파일 시스템 확인 해 FAT과 NTFS에 따라 파일 위치 계산해 userinit.exe 변조
- Smitnyl 개념도 (by ASEC 분석1팀)



# Win-Trojan/Saftad.49664

- 마스터 부트 레코드 변조 후 돈 요구
  - 2010년 10월 발견된 랜섬웨어
  - 하드디스크 데이터가 암호화 되었다고 알림 (실제로는 MBR만 변조)
  - [www.safe-data.ru](http://www.safe-data.ru)로 접속 유도 -> 50 유로 요구
  - **aaaaadabia**를 입력하면 정상 부팅 됨 (자체 치료)

Your PC is blocked.  
All the hard drives were encrypted.  
Browse [www.safe-data.ru](http://www.safe-data.ru) to get an access to your system and files.  
Any attempt to restore the drives using other way will  
lead to inevitable data loss !!!  
Please remember Your ID: 773921,  
with its help your sign-on password will be generated. Enter password: \_

# Win-Trojan/Saftad.49664

- 우크라이나 소재 홈페이지
  - 50 유로 요구



# Win-Trojan/Saftad.49664

## • 변조된 MBR 내용

- 악성코드 뒷부분 읽기
- 메시지 출력 및 키 값 입력
- 옳은 키이면 정상 MBR 복구 -> 정상 부팅

```
; 0000:7C1B . . . .  
0B07:011B B80202      MOV     AX,0202          ↪  
0B07:011E BB007C      MOV     BX,7C00          ↪  
0B07:0121 B90200      MOV     CX,0002          ↪  
0B07:0124 BA8000      MOV     DX,0080          ↪  
0B07:0127 CD13        INT    13               ; 뒷부분 코드 읽기 ↪  
0B07:0129 721B        JB     0146             ↪  
0B07:012B 66817F02686A CMP    DWORD PTR [BX+02],636D6A68 ; 제대로된 감염된 MBR 인  
가 ? ↪  
0B07:0133 7516        JNZ    014B             ↪  
0B07:0135 81C3FC03    ADD    BX,03FC          ↪  
0B07:0139 66813F686A    CMP   WORD PTR [BX],636D6A68 ↪  
0B07:0140 7509        JNZ    014B             ↪  
↪  
0B07:0142 68007C      PUSH   07C00          ; 뒷부분 0000:7C00으로 로드  
해 다시 시작 (part - II로 이동) ↪  
0B07:0146 C3          RET               ↪  
↪  
0B07:0146 BE5C06      MOV    SI,065C          ; 읽기 실패 에러 메시지  
출력 ↪  
0B07:0149 EB03        JMP    014E             ↪  
↪  
0B07:014B BE7106      MOV    SI,0671          ; 뒷부분 없음 ↪
```

# Demo

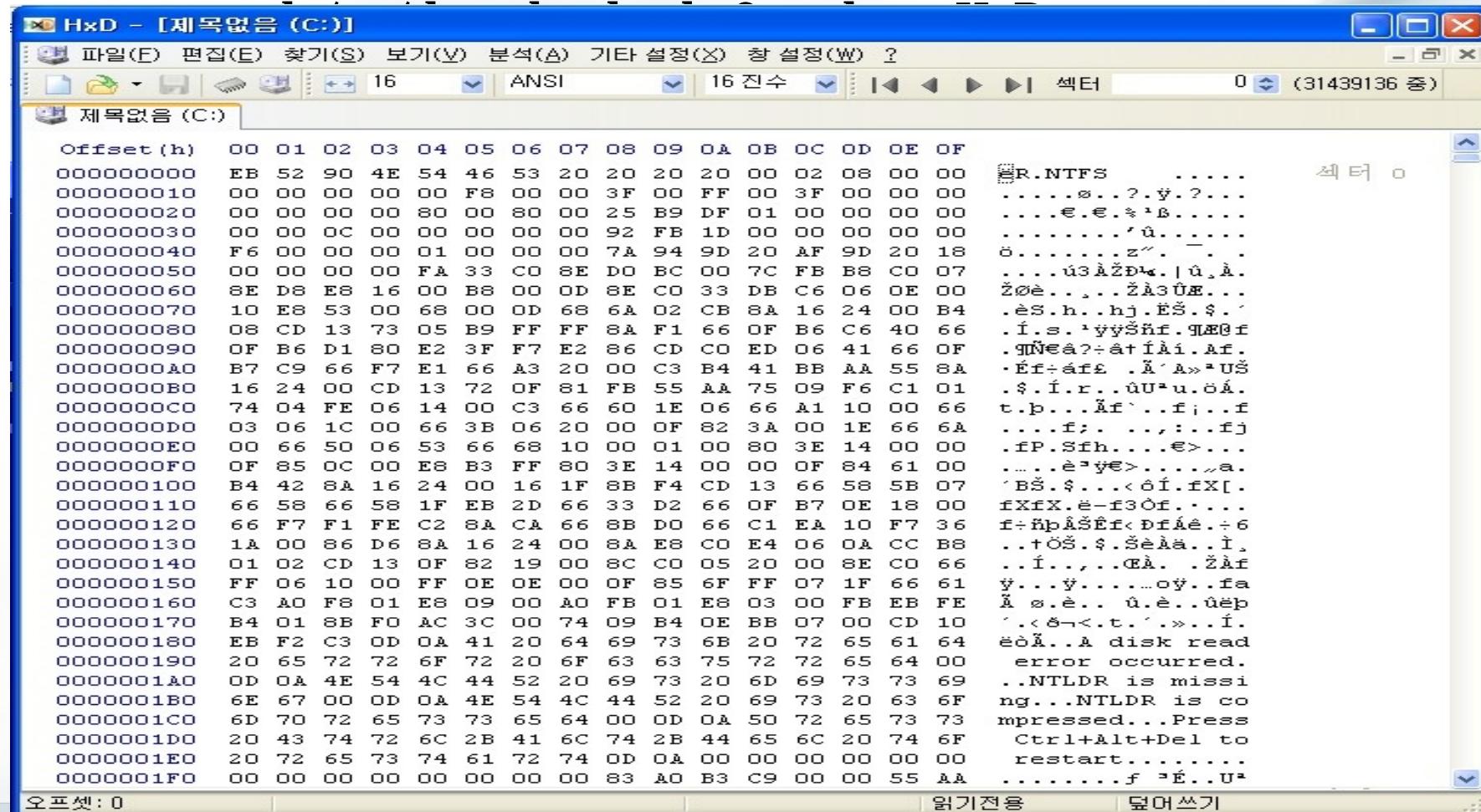
## 6. 분석 방법

# 디스크 섹터 뷰어/편집기

- **HxD**

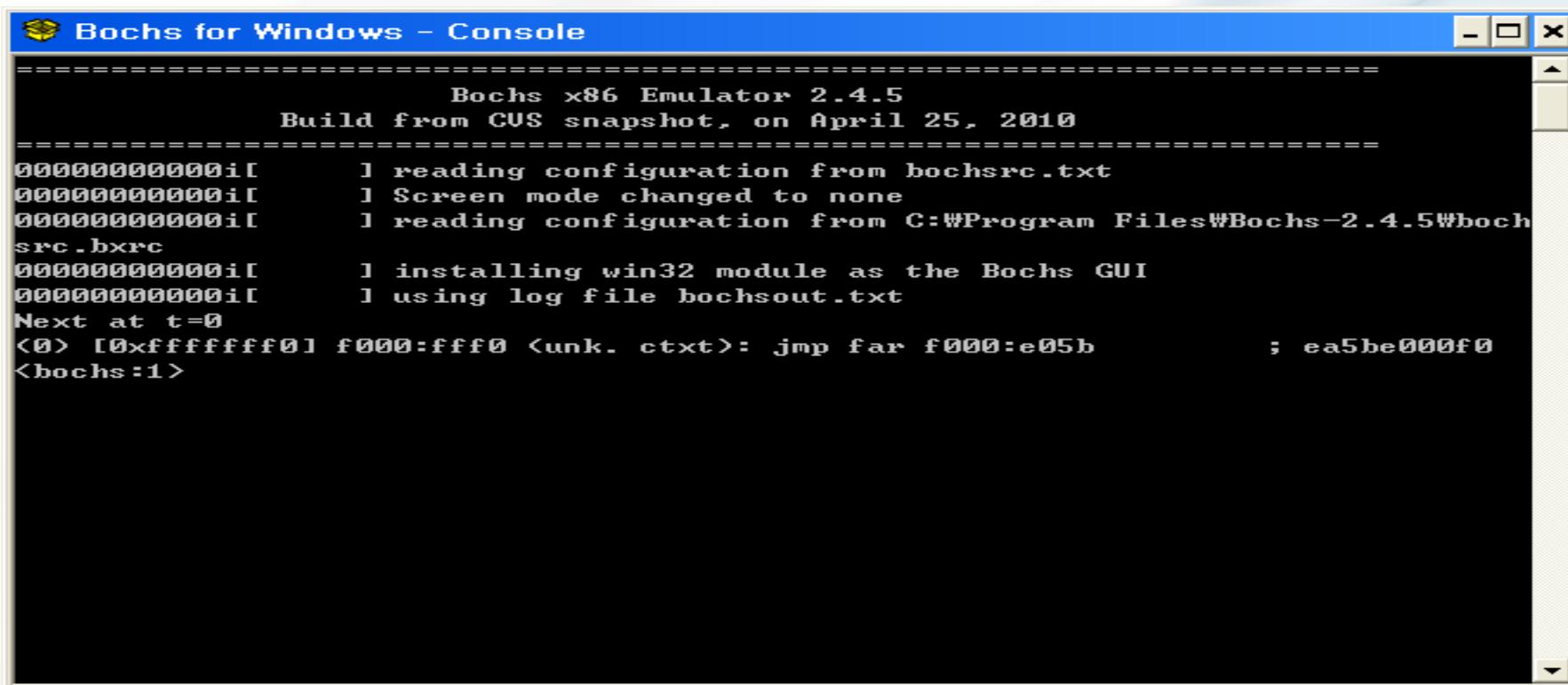
- <http://mh-nexus.de/en/hxd/>

- 다운로드 : <http://mh->



# 부트 레코드 디버깅

- 디버깅 방법
  - Debug, 소프트아이스 2.8, Windbg (?)
  - Bochs
- Bochs
  - <http://bochs.sourceforge.net/>



The screenshot shows a Windows console window titled "Bochs for Windows - Console". The window contains the following text:

```
=====
Bochs x86 Emulator 2.4.5
Build from CVS snapshot, on April 25, 2010
=====
000000000000il ] reading configuration from bochssrc.txt
000000000000il ] Screen mode changed to none
000000000000il ] reading configuration from C:\Program Files\Bochs-2.4.5\bochs
src.bxrc
000000000000il ] installing win32 module as the Bochs GUI
000000000000il ] using log file bochsout.txt
Next at t=0
<0> [0xfffffffff0] f000:ffff0 <unk. ctxt>: jmp far f000:e05b ; ea5be000f0
<bochs:1>
```

# Demo

## 7. 전망 및 과제

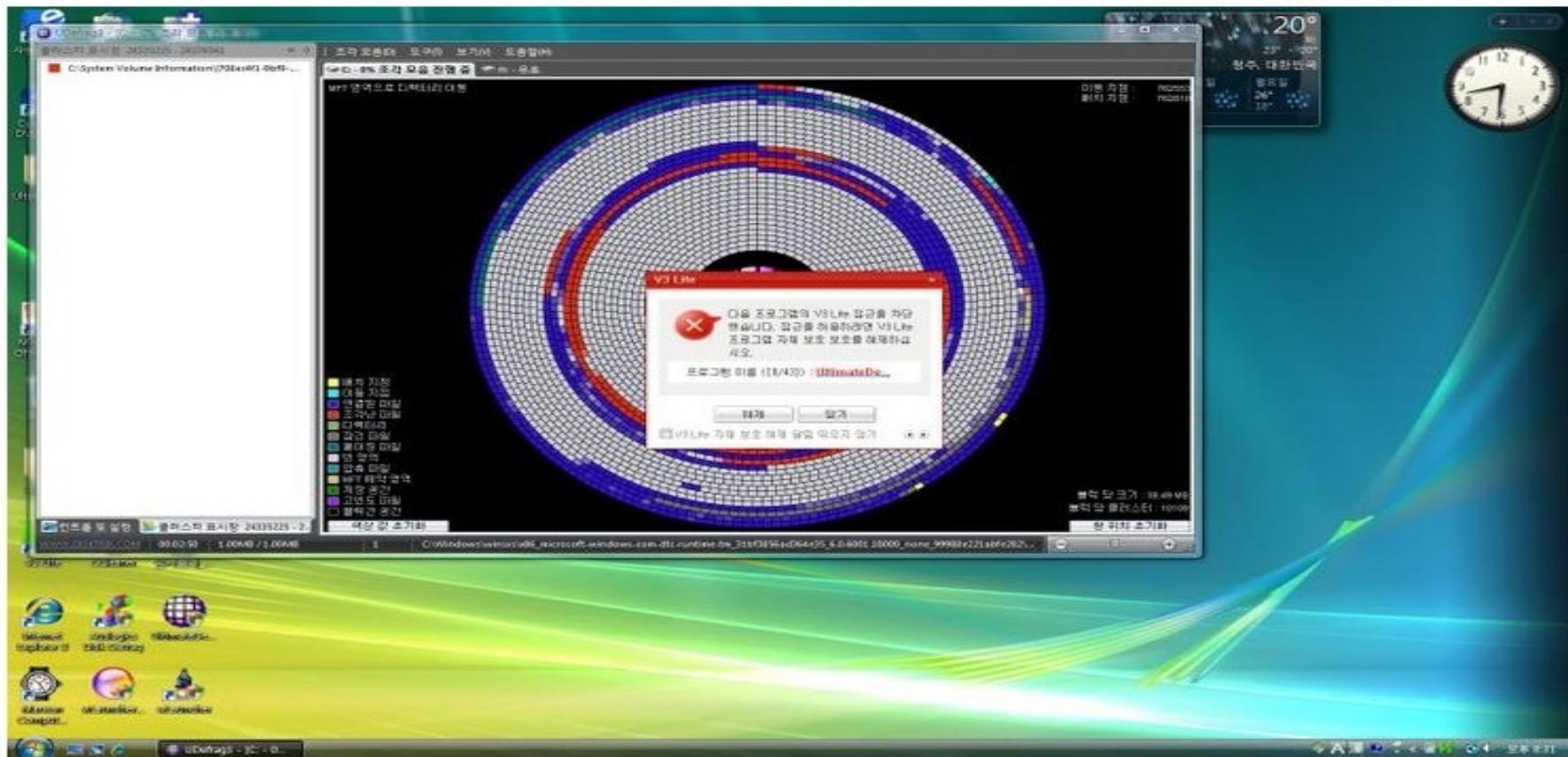
# 간단한 디스크 입출력

- 간단한 방식이라 쉽게 악성코드에 적용 가능
- 윈도우 버전별 차이
  - 윈도우 XP까지는 큰 어려움 없음
  - 윈도우 비스타 및 7 이상에서 우회 방안 필요
- 보안프로그램에서 디스크 입출력 차단 기능
  - 윈도우 7 서비스팩1, 단편화 제거 프로그램 등의 정상 프로그램에서도 디스크 입출력 이용
  - 윈도우 7에서 파티션 변경 지원
  - 해결 방안
    - 화이트리스트 ?
    - 사용자 선택 ?

# 안철수연구소의 디스크 입출력 차단 기능

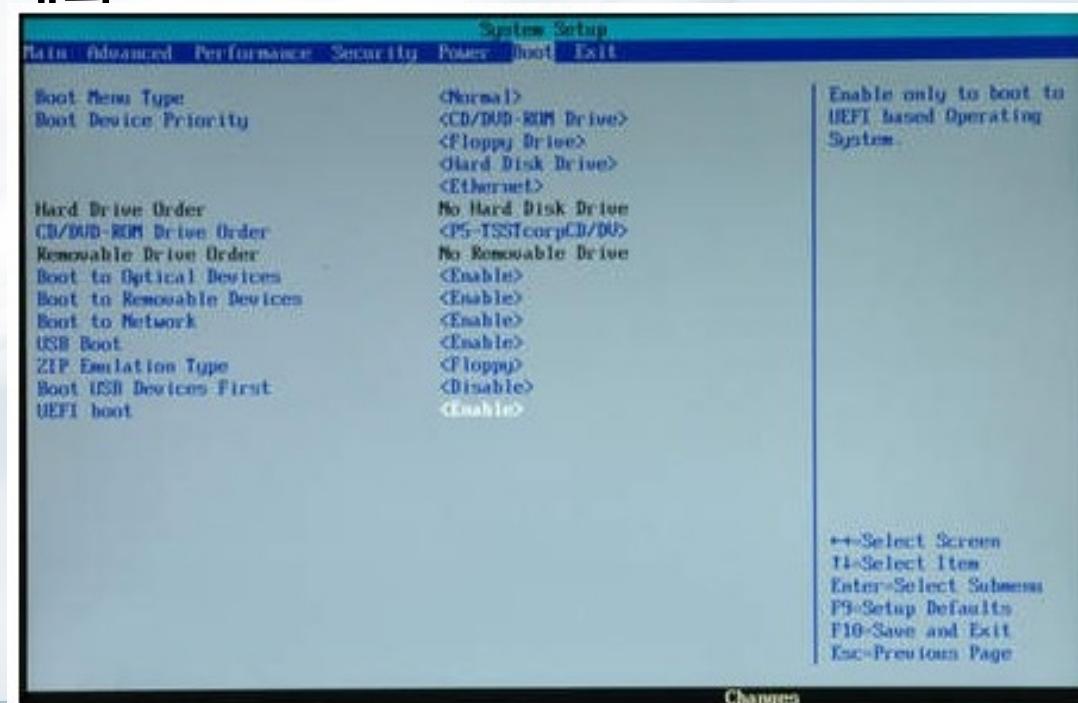
- **V3 Lite 디스크 입출력 차단 기능**

- 조각 모음 등에서도 뜰 수 있음
- 출처 : 네이버 바이러스제로 카페  
[\(http://cafe.naver.com/malzero/72209\)](http://cafe.naver.com/malzero/72209)



# 새로운 부팅 방식

- **EFI, UEFI (EFI 2.0)**
  - <http://www.uefi.org/home/>
  - 현재 BIOS 시스템이 사용하는 레거시 16비트 코드를 대체하는 최신 표준안
    - 사전 부트 프로그램(preboot program) 로딩과 운영체제 로딩 과정을 지원하는 드라이버 허용
    - 부팅 시간 10-20초 내외
- EFI는 OS 환경과 비슷
- 맥 등에서 사용



# 새로운 부팅 방식

- **EFI**
  - 스크립트 (NSH)
  - EFI shell로 부팅 가능
  - EFI shell startup video
    - <http://www.youtube.com/watch?v=wrybDw9UL5E>
  - EFI shell startup video and HEXEDIT.EFI demo
    - <http://www.youtube.com/watch?v=kiRsaaS1mbM>
- **가능한 시나리오**
  - EFI 내에 악성코드 보관
  - 다른 이미지로 부팅
  - 악성코드가 제어권을 가진 후 부팅
    - 진정한 MAOS !

## 향후 과제

- 부트 루트킷(부트킷) 분석과 진단/치료
  - Mebroot, TDL
  - 64비트 TDL 분석
- 새로운 부팅 방식을 이용한 악성코드 등장 가능성 연구
  - EFI, UEFI 백신 필요 ?!

## 퀴즈

- 발표자료 제목인 **virse program messge Dos to Win**는 LBC 바이러스에서 가져왔다. 이 바이러스의 원래 메시지는?
- 0번 헤드, 0번 트랙, 1번 섹터에서 0번 헤드, 0번 트랙, 7번 섹터의 내용을 파일로 저장하려면 몇 바이트가 필요한가?
- LBC 바이러스에 감염된 하드디스크로는 부팅되지 않고 인식도 되지 않는다. 그 이유는 각각 무엇인가 ?

## 퀴즈 정답

- 발표자료 제목인 **virse program messge Dos to Win**는 LBC 바이러스에서 가져왔다. 이 바이러스의 원래 메시지는?
  - **virse program messge Njh to Lbc**
- 0번 헤드, 0번 트랙, 1번 섹터에서 0번 헤드, 0번 트랙, 7번 섹터의 내용을 파일로 저장하려면 몇 바이트가 필요한가?
  - **3,584 바이트**
  - **7개 섹터 \* 512 = 3,584 바이트**
- LBC 바이러스에 감염된 하드디스크로는 부팅되지 않고 인식도 되지 않는다. 그 이유는 각각 무엇인가 ?
  - 부팅시 A 드라이브라고 가정해서 하드 디스크 부팅되지 않음
  - 감염된 부트레코드에는 파티션 정보가 존재하지 않음

# 질문

- 메일주소 : [jackycha@ahnlab.com](mailto:jackycha@ahnlab.com)



## 참고자료

- **Windows Internals 제 5 판**
- **Ralf Brown's Interrupt list**  
(<http://www.cs.cmu.edu/~ralf/files.html>)
- **Your computer is now stoned (... again) (F-Secure)**
- **ASEC Report Vol. 16 중 MBR infection : Smitnyl 분석 정보 (안철수연구소)**
- **TDL3 : The Rootkit of All Evil? (Eset)**
- **The Case of Trojan Downloader “TDL3” (F-Secure)**
- **안철수연구소 ASEC 분석1팀 내부 분석 자료**

# 감사합니다

세상에서 가장 안전한 이름

Ahn안철수연구소

ASEC Threat Research

<http://blog.ahnlab.com/asec/>  
<http://core.ahnlab.com>

<sup>2011</sup>  
**CodeEngn**

[www.CodeEngn.com](http://www.CodeEngn.com)

CodeEngn ReverseEngineering Conference