보안실습 8

[첫번째] 파일 시그니처 분석

- 파일 시그니처 분석의 의의
- 파일 확장자 분류의 문제점
- HxD를 통한 파일 분석
- 파일 시그니처 분석의 활용 예

보안실습 8

1. 시그니처 분석의 의의

- 파일이 담고 있는 데이터를 유용하게 사용하기 위해 소프트웨어가 필요함
- 소프트웨어들은 자신만의 고유한 파일 포맷을 사용함
- 예시 : JPEG, GIF, DOC, PPT
- 이와같은 파일들은 각각 고유한 포맷을 가지고 있으며 이를 '파일 시그니처 (File Signature)'라고 한다.

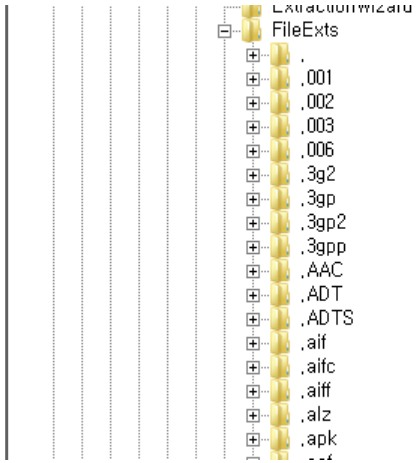
파일 포맷	시작 값	마지막 값
JPEG	FF D8 FF E0 00 10 4A 46 49 46 00 01 01	
GIF	47 49 46 38 39 61 4E 01 53 00 C4	21 00 00 3B 00
DOC	D0 CF 11 E0 A1 B1 1A E1	57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E
PPT	D0 CF 11 E0 A1 B1 1A E1	50 00 6F 00 77 00 65 00 72 00 50 00 6F 00 69 00 6E 00 74 00 20 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74

보안실습 8

2. 확장자 분류의 문제점

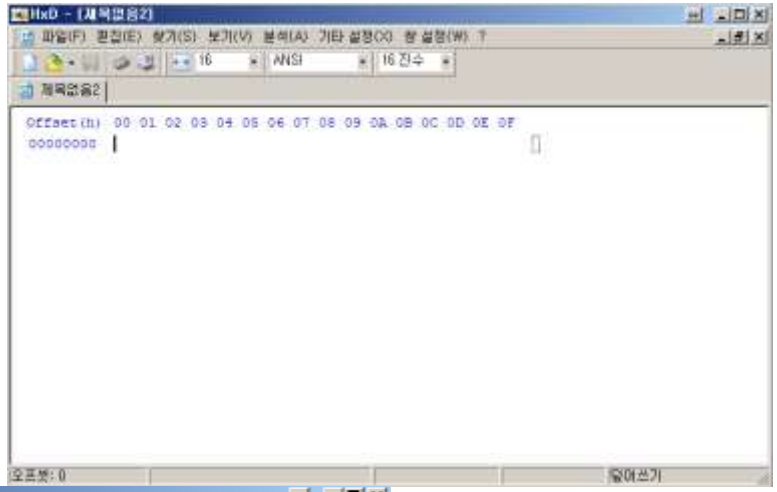
- 윈도우는 기본적으로 확장자 기반의 애플리케이션 바인딩 사용
- 파일의 이름 바꾸는 것 만으로 다른 소프트웨어에서 실행됨
- 애플리케이션 바인딩 정보는 **레지스트리**(HKEY_CURRENT_USER)**에 저장**

HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩FileExts



보안실습 8

3. HxD 설치 및 파일 시그니처 값 확인



HxD - [C:₩Users₩imhj₩Desktop₩chap00.ppt]

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?

16 | ANSI | 16 진수

제목없음2 | chap00.ppt

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	ĐÏ.à¡±.á........
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00	........>...þÿ..
00000020	06	00	00	00	00	00	00	00	00	00	00	00	2B	00	00	00	............+...
00000030	1B	15	00	00	00	00	00	00	00	10	00	00	FE	FF	FF	FF	............þÿÿÿ
00000040	00	00	00	00	FE	FF	FF	FF	00	00	00	00	F0	14	00	00	....þÿÿÿ....ð...
00000050	F1	14	00	00	F2	14	00	00	F3	14	00	00	F4	14	00	00	ñ...ò...ó...ô...
00000060	F5	14	00	00	F6	14	00	00	F7	14	00	00	F8	14	00	00	õ...ö...÷...ø...
00000070	F9	14	00	00	FA	14	00	00	FB	14	00	00	FC	14	00	00	ù...ú...û...ü...
00000080	FD	14	00	00	FE	14	00	00	FF	14	00	00	00	15	00	00	ý...þ...ÿ.......
00000090	01	15	00	00	02	15	00	00	03	15	00	00	04	15	00	00	....
000000A0	05	15	00	00	06	15	00	00	07	15	00	00	08	15	00	00	....
000000B0	09	15	00	00	0A	15	00	00	0B	15	00	00	0C	15	00	00	....
000000C0	0D	15	00	00	0E	15	00	00	0F	15	00	00	10	15	00	00	....
000000D0	11	15	00	00	12	15	00	00	13	15	00	00	14	15	00	00	....
000000E0	15	15	00	00	16	15	00	00	17	15	00	00	18	15	00	00	..........□....
000000F0	19	15	00	00	1A	15	00	00	FF	FF	FF	FF	FF	FF	FF	FF	........ÿÿÿÿÿÿÿÿ
00000100	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000110	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000120	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

오프셋: F8 덮어쓰기

보안실습 8

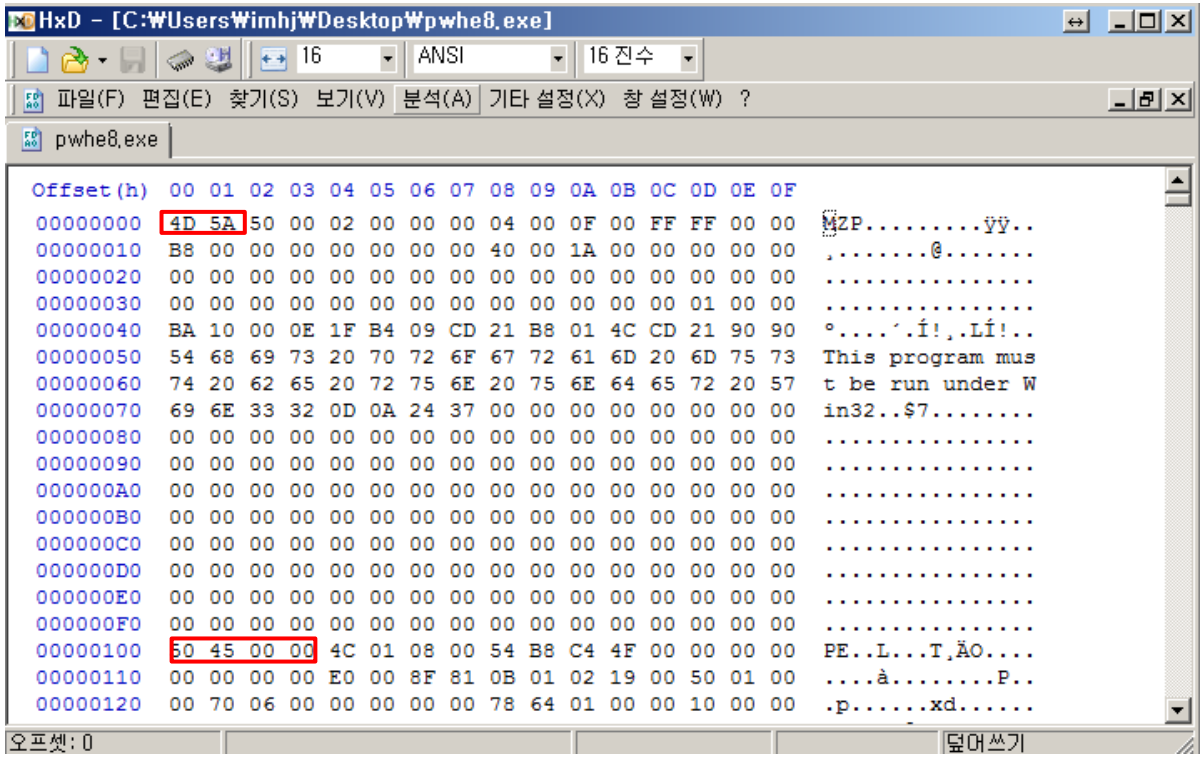
4. PE파일의 의미

PE (Portable Executable) 포맷

유닉스 COFF(Common Object File Format)을 기반으로 윈도우 3.1 부터 지원된 실행 파일 형식

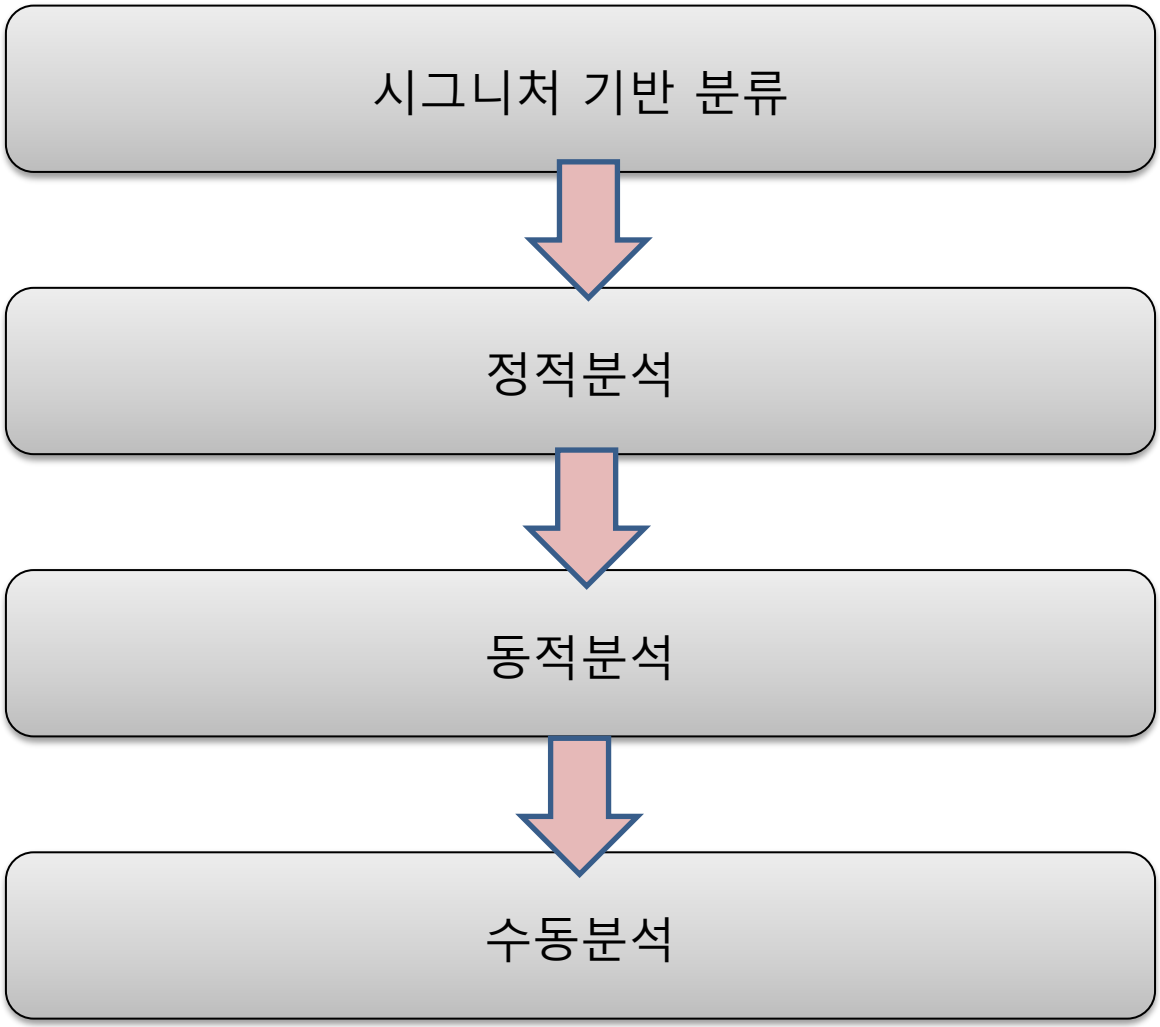
PE 파일 종류

실행계열 : EXE , SCR, 드라이버 계열 : SYS , VXD
라이브러리 계열 : DLL,OCX,CPL,DRV , 오브젝트 파일 계열 OBJ



보안실습 8

5. 시그니처 분석의 활용 예 (악성코드 분석, 1/2)



보안실습 8

5. 시그니처 분석의 활용 예 (악성코드 분석, 2/2)

1. **동영상 다운로드**
   웹하드, 토렌트 등을 통한 동영상 다운로드

2. **확장자 변경**
   야구동영상.(exe).avi
   정상 동영상 파일 앞 부분에 악성파일 삽입, 리소스 변경을 이용해 아이콘 변경

3. **자체 압축 풀림 (Self-Extracting Archive, SFX)**
   야구동영상.avi

4. **동영상 플레이어 취약점**
   플레이어의 취약점을 이용해 동영상 포맷 구성