01. Basic Static Techniques

**- Antivirus Scanning**

**- Hashing**

**- Packing**

**- Strings**

**- PE Format, Imports functions**

**- PE Format, Headers and Sections**

**- PE Format, Resource Section**

**1. Antivirus Scanning**

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

**2. Hashing**

MD5 or SHA-1

tool)md5deep, WinMD5를 이용해 md5추출

**3. Packing and Obfuscated Malware**

패킹된 프로그램은 strings, imports 등의 데이터가 보이지 않는다

tool) PEiD : 패킹,컴파일러 확인

PEiD 0.92는 버퍼오버플로우 취약점을 가지고 있다.

**4. Strings**

올바른 문자열과 cpu명령어, 데이터, 메모리어드레스 등이 문자열로 출력된 경우를 구분

tool) strings

**5. Imports Functions**

Static Linking - 코드가 실행파일에 복사됨, 프로그램의 코드와 링킹된 코드의 구분이 어렵다

Runtime Linking - LoadLibrary&GetProcAddres, LdrGetProcAddress&LdrLoadDll

Dynamic Linking - PE Format의 imports에 목록이 저장, 프로그램의 로드타임에 로딩

tool) Depends(Dependency Walker) - import dll확인

PEView

advapi32.dll - core Windows components such as the Service Manager and Registry

ntdll.dll - kenel32.dll에 의해 간접적으로 로드됨

Native API사용을 위해 Dynamic Linking할 경우 import테이블에 존재

Wininet.dll - networking protocols such as FTP, HTTP, and NTP

**6. Header & Sections**

IMAGE\_FILE\_HEADER.Time Date Stamp : 컴파일 타임, 델파이는 June 19, 1992로 고정

IMAGE\_OPTIONAL\_HEADER.Section Header의 Virtual Size & Size of Raw Data :

사이즈 크기로 패킹 유무 판별(.text, .data, .rdata…..)

**7. Resource Section**

embedded program or driver를 숨겨 놓을 수 있다

tool) Resource Hacker