03. Basic Dynamic Analysis

가능한 다양한 경우의 수를 적용해 해킹툴을 동적으로 실행하는 것이 중요

**- Running Malware(DLL)**

**- Porcess Monitor**

**- Process Explorer**

**- RegShot**

**- Faking a Network**

**- Wireshark**

**- INetSim**

**1. Runnig Malware(DLL)**

- rundll32.exe DLLName, Export(name or ordinal) arguments

- wipe the IMAGE\_FILE\_DLL

- 서비스로 등록되어 동작하고, 서비스등록 API가 export 되있을 경우

rundll32.exe ipr32x.dll,InstallService ServiceName // 서비스 등록

net start ServiceName // 서비스 실행

- 서비스로 등록되어 동작하고, 서비스등록 API가 export 되있지 않을 경우

sc command or 레지스트리에 수동 등록(HKLM\SYSTEM\CurrentControlSet\Services)

net start ServiceName

**2. Process Monitor**

- registry, file system, network, process&thread

- rootkit과 Application과의 IO Control은 탐지 못한다

- Filtering : Process Name & Operation(API)

**3. Process Explorer**

- IMAGE(process, dll, driver)등을 Verify

MS에서 digital signature를 조사해 정상파일인지 확인(파일상태에서 확인)

- Process Replacement 확인

Image와 Memory 상태의 각각의 string을 비교해 확연하게 차이나는 경우

- 자식프로세스 확인

(word,pdf같은 문서파일………..;;;)

**4. Regshot**

**5. Faking a Network**

**6. Wireshark**

**7. INetSim**