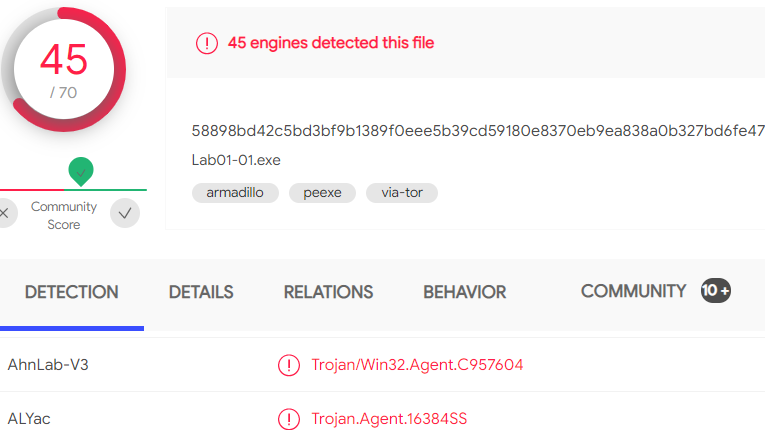
초기 분석 실습

\* test1.exe

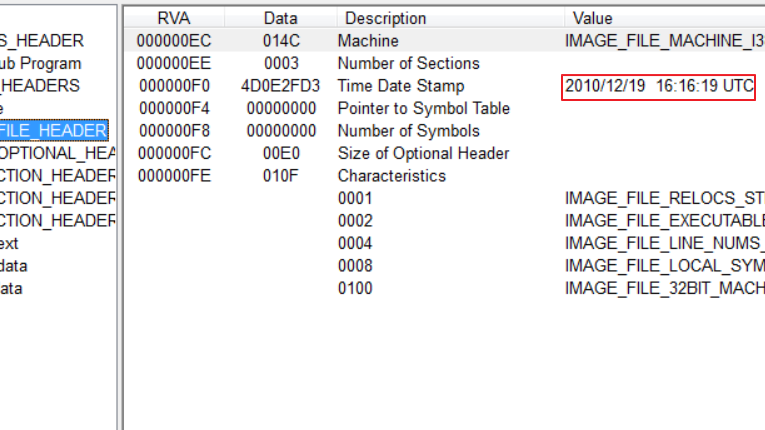
1. 알려진 바이러스 정보는?

\* 바이러스 토탈에서 Lab01-01.exe로 알려짐



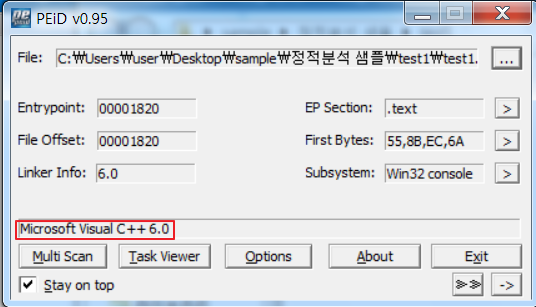
2. 컴파일 시간은?

\* 2010/12/19 16:15:19 UTC



3. 패킹 여부는?

\* not

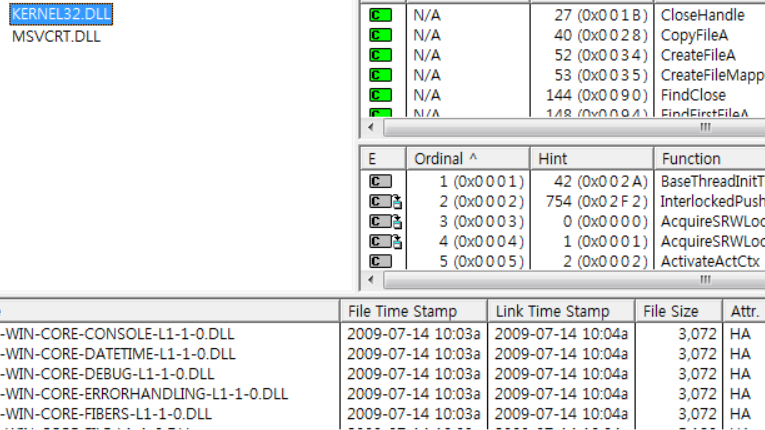


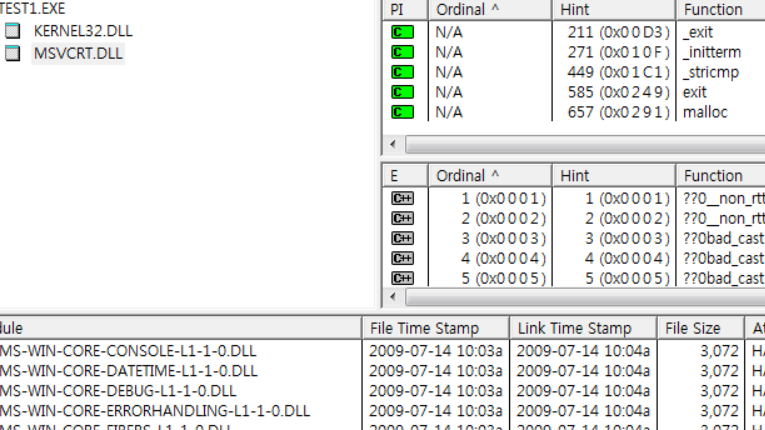
4. import 된 정보를 통해 얻을 수 있는 부분은?

\* KERNEL32.dll과 MSVCRT.dll 사용하고 있음

\* MSVCRT.dll : 마이크로소프트 비주얼 C 런타임 라이브러리

\* 파일을 힙공간을 사용하며, 찾고, 복사하고, 비교하고, 생성하는 일을 하는 것으로 추측됨

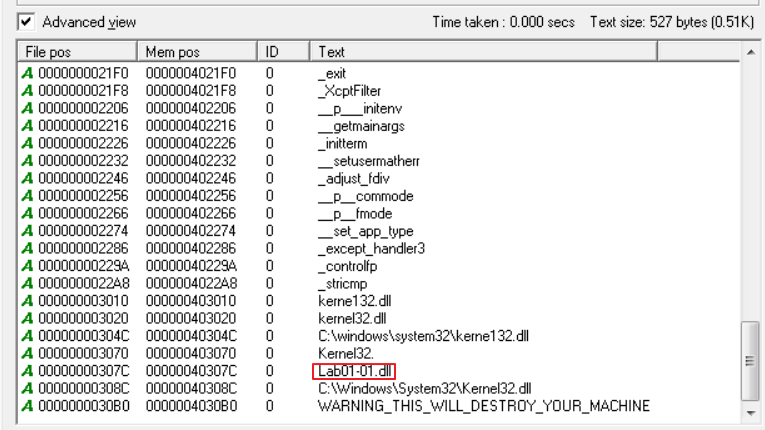




5. strings 나 bintext 를 이용해서 얻을 수 있는 정보는 ?

\* 4번 정보와 더불어, 추가적으로 ‘Lab01-01.dll’을 사용한다고 추측이 가능

\* kerne132.dll이라는 kernel32.dll과 비슷한 dll을 사용함



6. 실습파일의 목적?

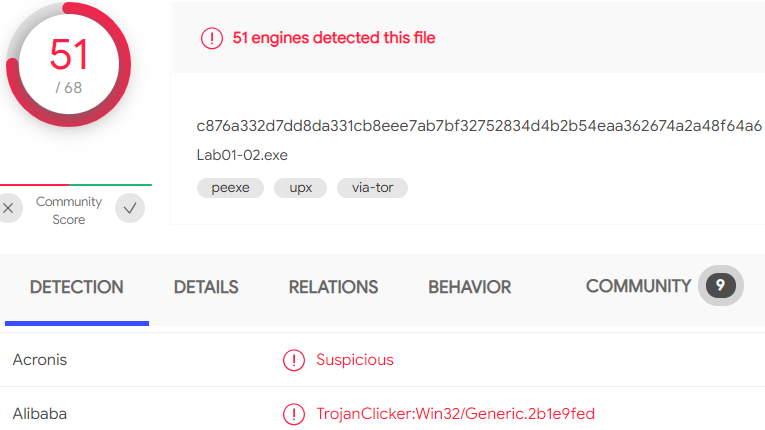
\* 특정 파일을 찾아서 복사, 생성하는 목적을 가짐

\* test1.dll

\* test2.exe

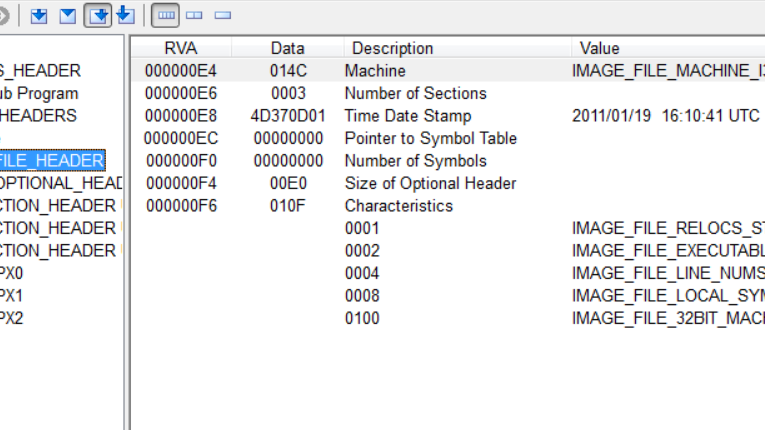
1. 알려진 바이러스 정보는?

\* 바이러스 토탈에서 Lab01-02.exe로 알려짐



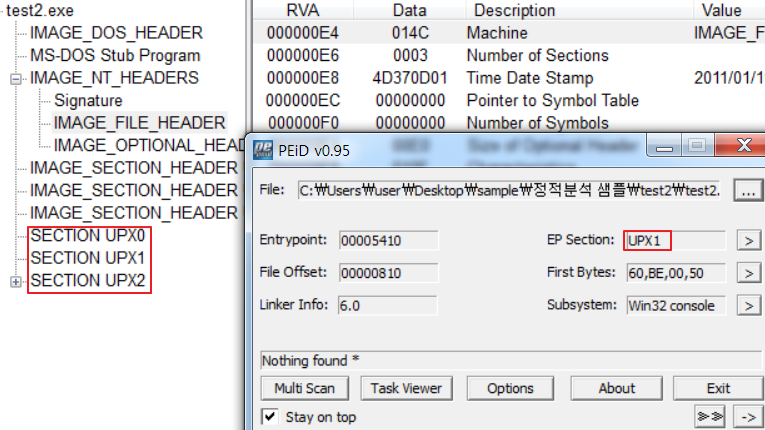
2. 컴파일 시간은?

2011/01/19 16:10:41 UTC

****

3. 난독화, 패킹 여부는?

\* UPX라는 패킹 프로그램으로 패킹됨

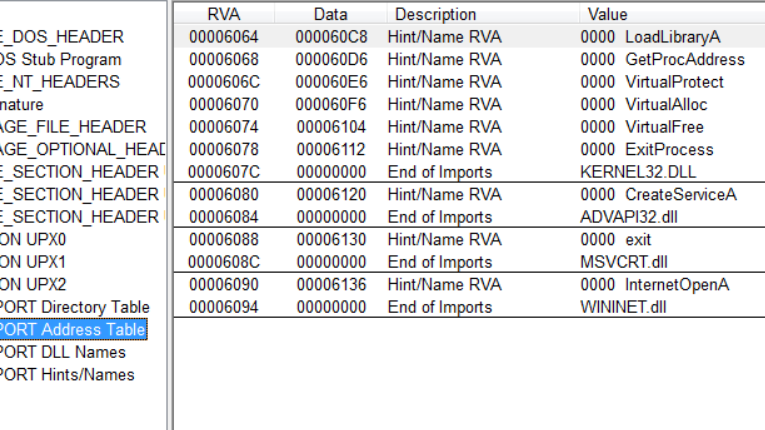


4. import 된 정보를 통해 얻을 수 있는 부분은?

- 패킹 상태

\* kernel32.dll, advapi32.dll, msvcrt.dll, winnet.dll 사용을 확인

\* InternetOpenA 함수를 통해 인터넷 연결을 함



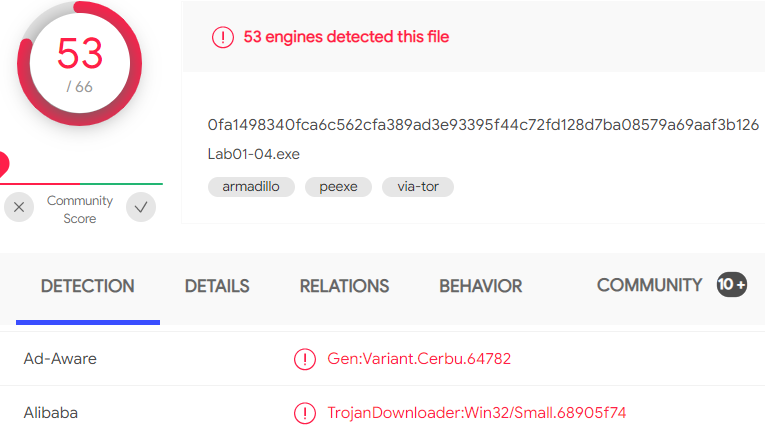
5. strings 나 bintext 를 이용해서 얻을 수 있는 정보는 ?

\* 언패킹을 할 수가 없어 스킵하기로 함

\* test3.exe

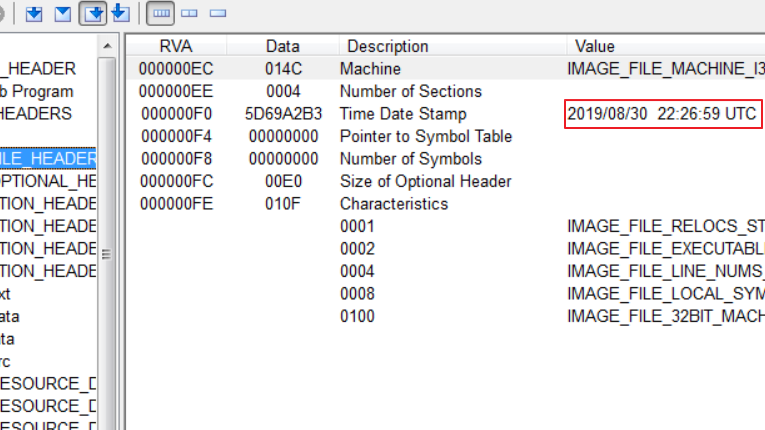
1. 알려진 바이러스 정보는?

\* 바이러스 토탈에서 Lab01-04.exe로 알려짐



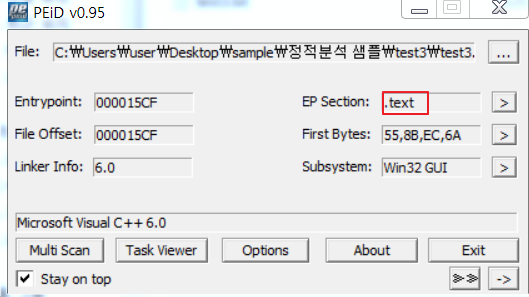
2. 컴파일 시간은?

\* 2019/08/30 22:26:59 UTC



3. 패킹 여부는?

\* not



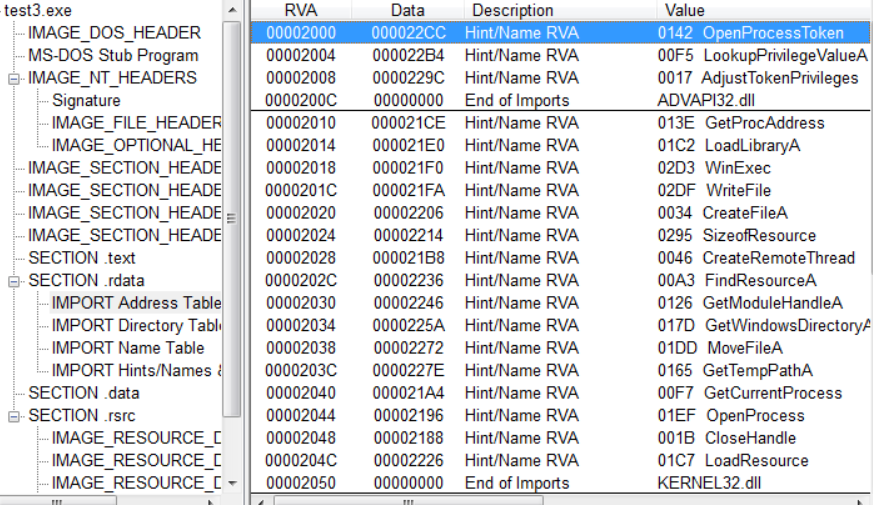
4. import 된 정보를 통해 얻을 수 있는 부분은?

\* kerner32.dll, advapi32.dll, msvcrt.dll 사용

\* WinExec : 이 함수는 다른 프로그램을 실행하는데 사용된다. ShellExecute와 유사함

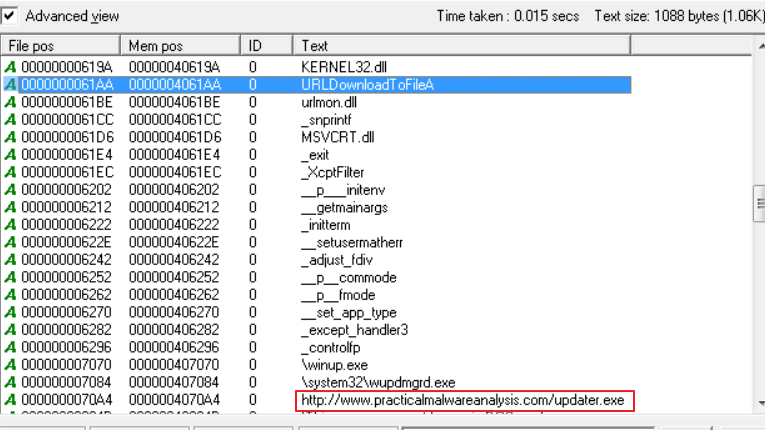
\* CreateRemoteThread : 이 함수는 원격 프로세스에서 스레드를 시작하는데 사용함, dll Injecion에 많이 사용함

\* 기타 다른 함수들을 보아, 현 상태에선 dll Injecion 공격을하는 프로그램으로 추측됨



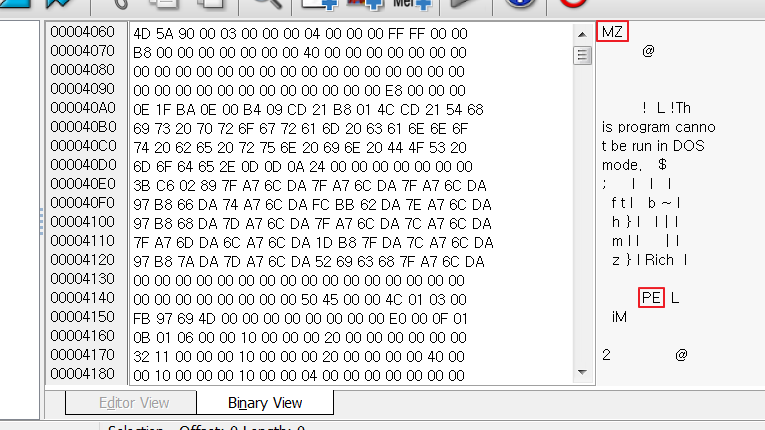
5. strings 나 bintext 를 이용해서 얻을 수 있는 정보는 ?

\* 4번 정보에 추가해, 위험한 파일을 다운로드하는 것을 추측할 수 있음



6. 리소스 섹션 분석을 통해 얻을 수 있는 정보는?

\* dos\_header와 nt\_header의 시그니처를 확인하여, pe구조를 가진 데이터가 리소스 섹션에 있다는 것을 확인 가능



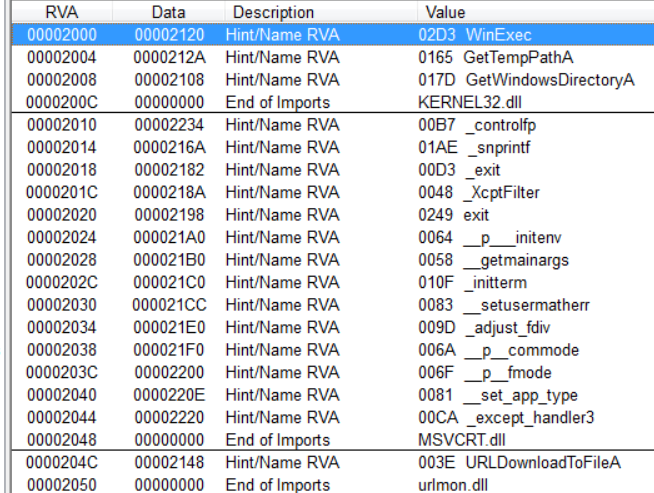
\* 리소스 세션에 있는 데이터를 .bin 파일로 만들어 확인하면, 'winEexc' 등 파일을 임시폴더에 다운로드하고 실행하는 프로그램으로 추측할 수 있음

- GetTempPathA

- GetWindowsDirectoryA

- WinExec

- URLDownloadToFileA

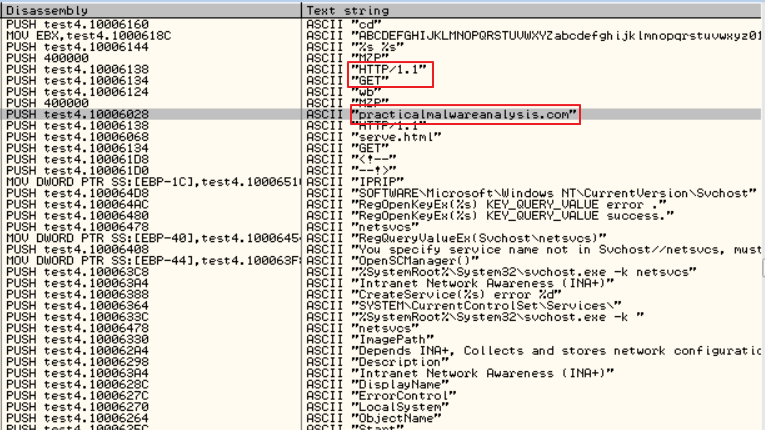


동적 분석 실습

\* test4.exe

1. 악성코드는 어떻게 설치되는가? 설치 후 변화도 포함

\* http GET 요청을 통해 'practicalmalwareanalysis.com'에서 악성코드들 다운 받는 것으로 보임



2. 악성코드가 사용하는 서비스는?

3. process explorer 로 실행된 DLL 파일을 찾고 해당 PID 정보의 흔적을 찾아 보자.

4. process monitor 를 이용하여 위 PID 를 통해 확인 된 정보를 분석 하자.

5. 리스너를 통해 나오는 도메인 정보는?