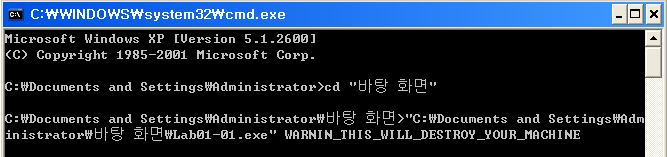
실습보고서4 2016111566 이나경

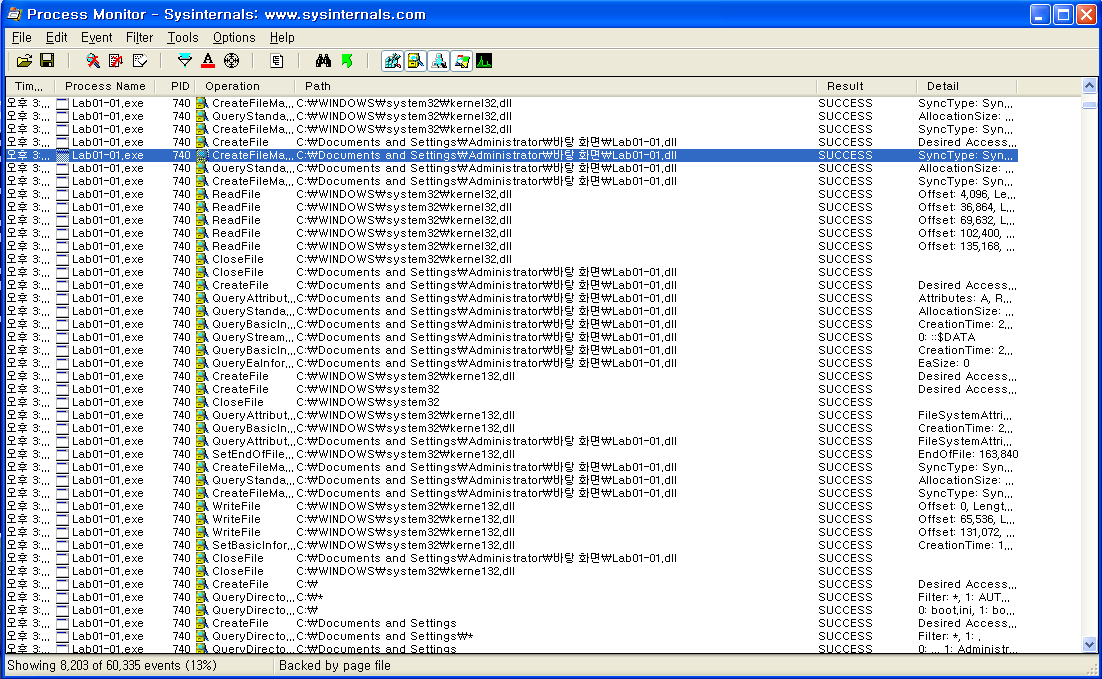
실습환경 : Windows XP(VMware 가상머신)

Tool : Process Monitor, Process Explorer, WinMD5free 등

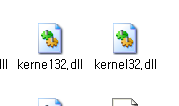
먼저 Lab01-01.exe과 함께 Lab01-01.dll을 실행시키기 위해 cmd를 사용한다.



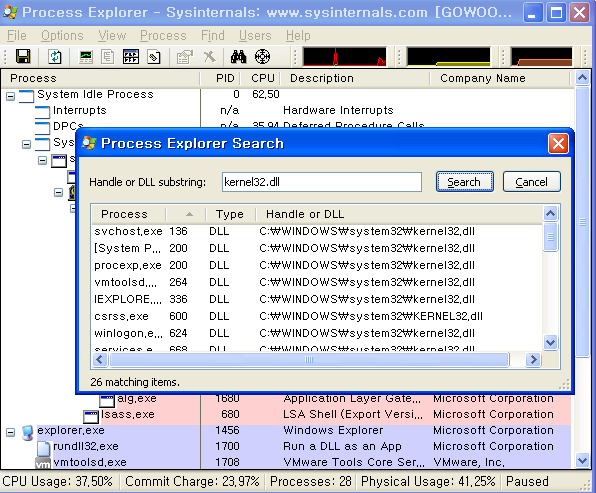
먼저 Lab01-01.exe와 Lab01-01.dll을 같은 폴더에 놓는다. 저번 Strings를 통한 정적분석 실습에서Lab01-01.exe가 WARNING\_THIS\_WILL\_DESTROY\_YOUR\_MACHINE라는 특정 인자 값과 함께 실행되는 것을 확인하였는데 이를 이용하여 Lab01-01.exe를 실행시킨다.

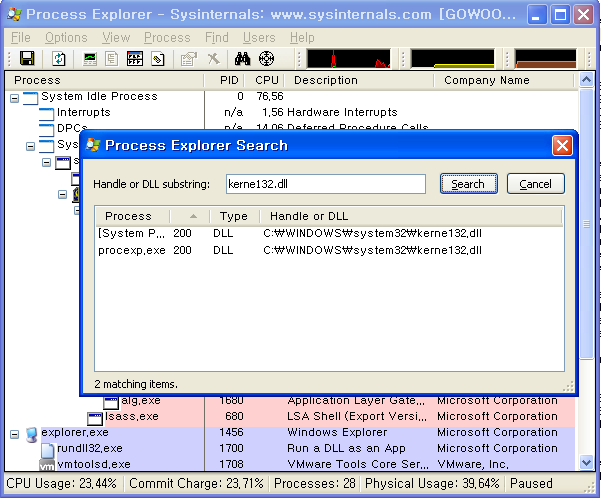


Process Monitor를 통해 확인하면 Lab01-01.exe가 실행되면서 Lab01-01.dll을 이용해 system32 폴더에 kerne132.dll을 생성하는 것을 알 수 있다.



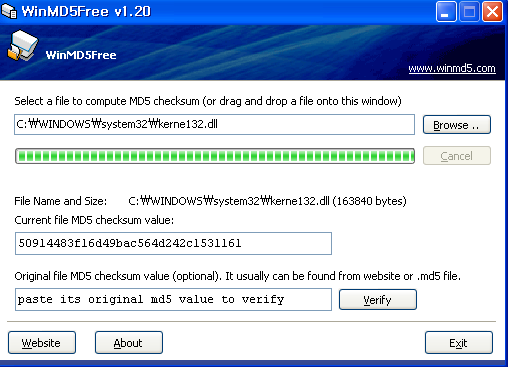
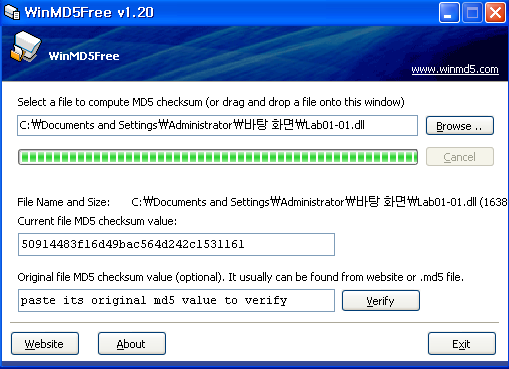
Windows/system32 폴더에 kernel32.dll과 kerne132.dll이 존재하는 것을 직접 확인해볼 수 있었다.



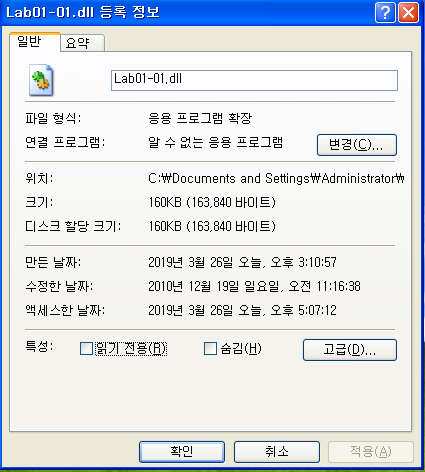
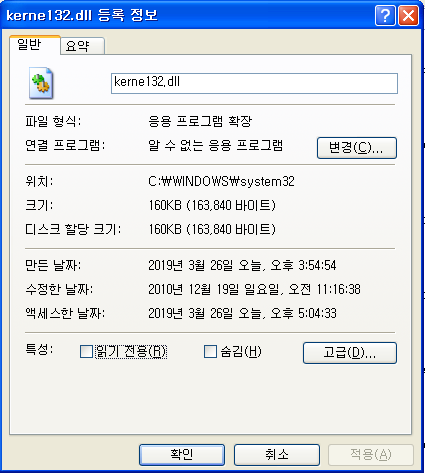


Kerne132.dll이 생성되면 kernel32.dll이 인젝션되고 시스템이 오작동을 일으키는데 악성코드 실행후 프로그램을 실행시켜보면 kerne132.dll를 링크한다. 이는 Process Explorer에서 kerne132.dll을 서치해보면 확인할 수 있다.

Lab01-01.dll은 Lab01-01.exe 실행 후 변경되고 kerne132.dll로 복제되기 때문에 두 파일은 동일하다고 유추해볼 수 있다.



WinMD5free로 확인한 결과 두 파일의 해시값이 같고

또한 두 파일의 크기가 같아

두 파일이 동일한 것임을 확인할 수 있다.