PE Header Custom Packing

onesider@gmail.com

2008.3.17

1. 들어가며

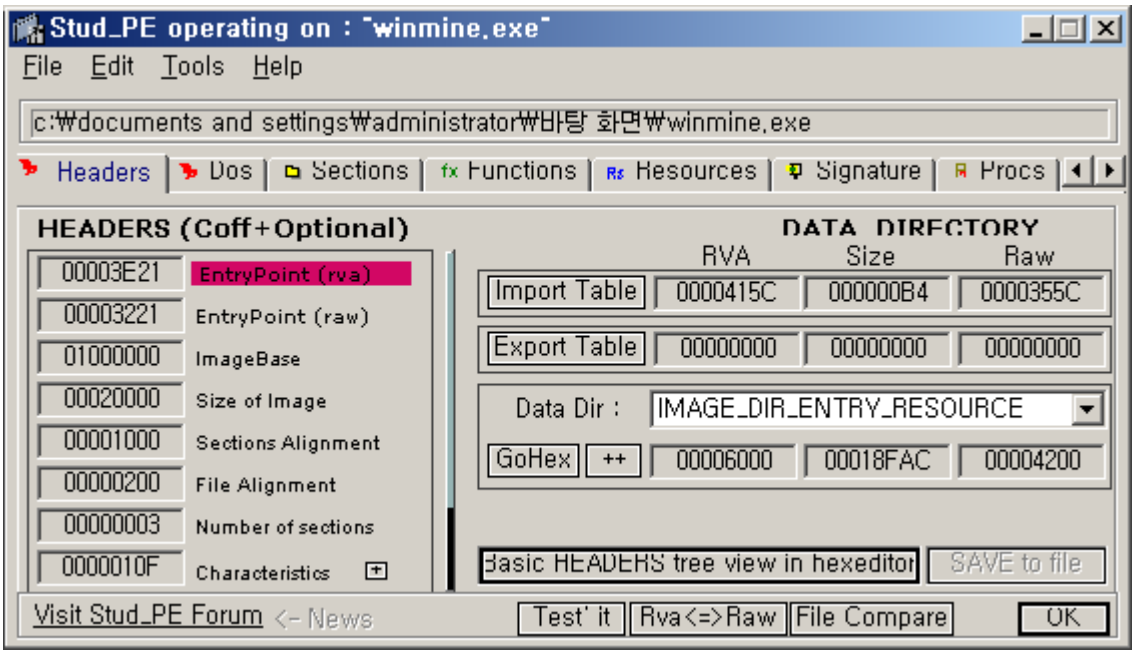
제목을 PE Header Custom Packing 라고 붙였지만 사실 이기법(?)의 정확한 명칭을몰라 이렇게 붙였습니다.(참조한 곳에서 이렇게 이름을 붙여놓아서 그냥 이름을 이렇게 붙였습니다.) 이글은 누구나 재배포 및 수정이 가능합니다. (출처만 붙여주셨음하는 소망이 있습니다.)
또한 질은문은 받지 않습니다. 개인적으로 공부한 것을 문서로 만든것 만든 것 일뿐입니다. 내용상의 오류나 오타는 적극 환영합니다.
이 문서는 PE구조의 기본적인 골격은 이해하고 있다는 가정하에 기술하도록 하겠습니다.

이글의 목적은 address of entry point를 00 로 변경하여 ollydbg에서 디버깅을 방해(?)하고 한때 악성코드들이 av를 피하기위하여 사용되었던 방법입니다.(요즘은 대부분 av가 다 잡아줍니다.)

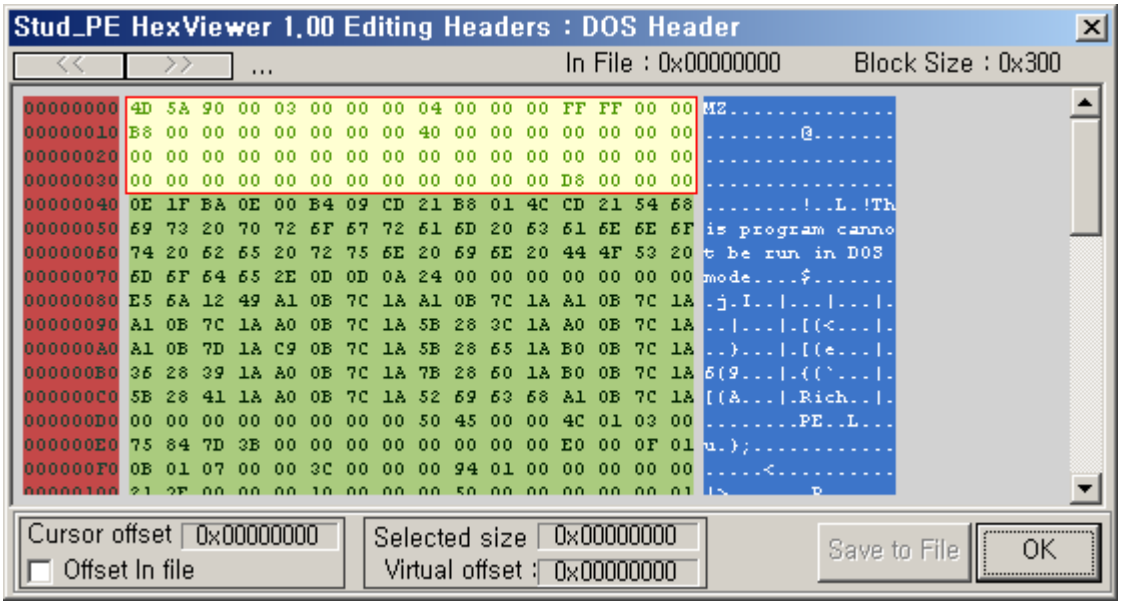
2. 준비물

Stud_PE (다를 툴을 사용해도 됩니다.)
PE 파일 (본문서에서는 winmine.exe를 사용함)
Ollydbg (없어도 됨)

3. 시작

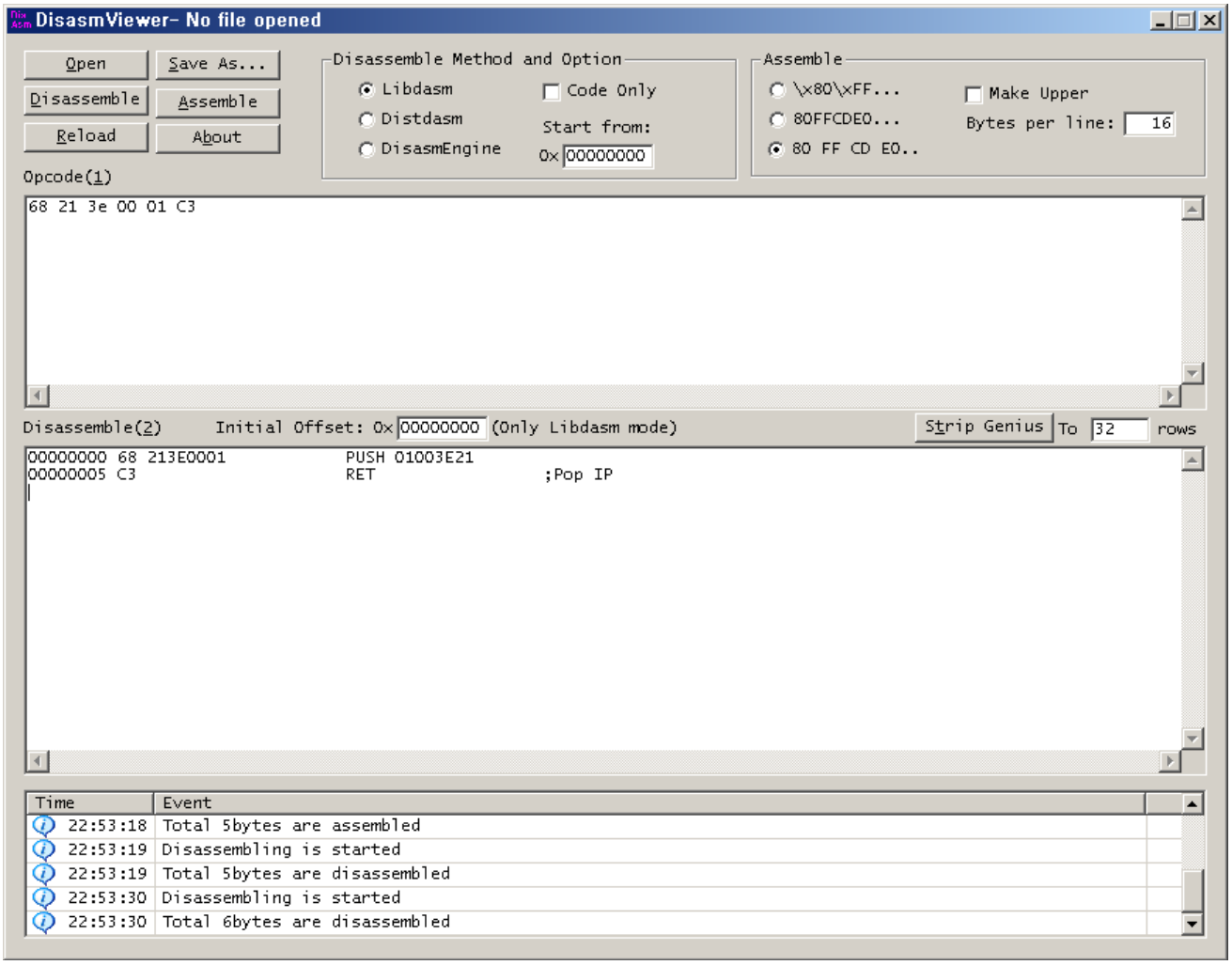


위 의 그림은 stud_pe 툴로 winmine.exe(지뢰찾기)를 오픈 한 화면 입니다. 잘보시면 ep 는 00003E21이고 imagebase는 01000000 이죠? Basic HEADERS tree view in hexeditor를 누르면 pe 파일구조가 헥사 값으로 보입니다.



위와 같이 dos header 가 보입니다. 당연히 MZ(4D 5A)값으로 PE는 시작을 합니다.

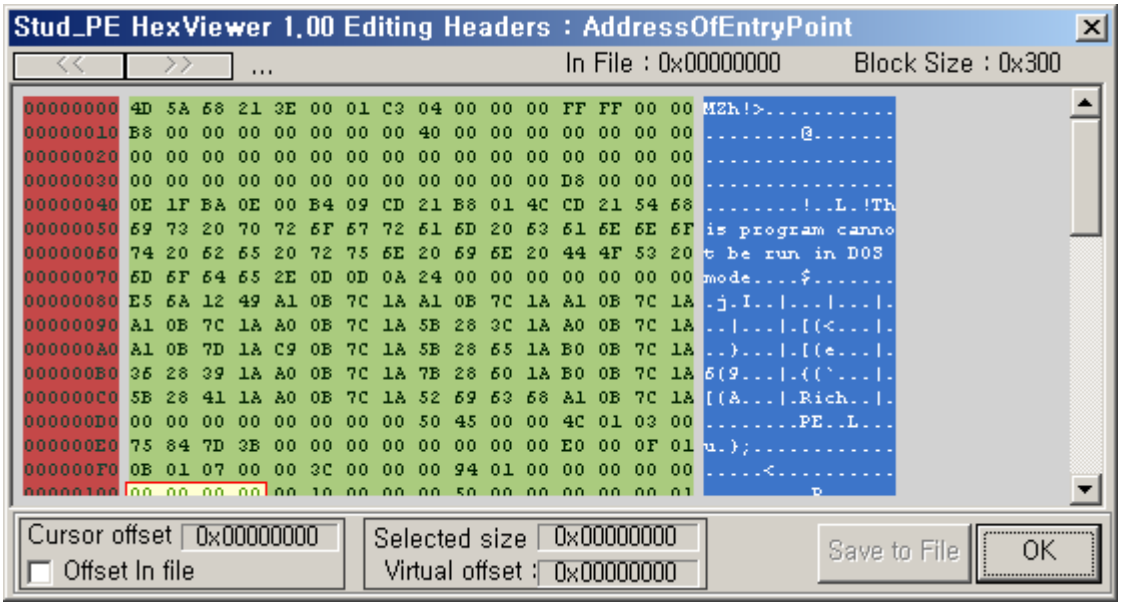
DOS HEADER의 시작값을 Address Of Entry Point + ImageBase 하여 Push 하고 ret 하는 헥사 값을 넣습니다.



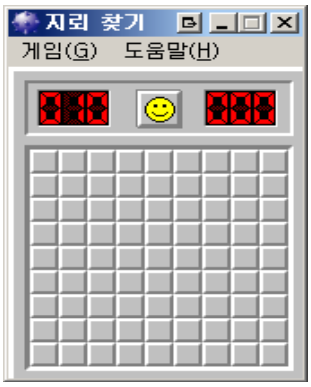
Hex 값으로 68 21 3e 00 01 C3 입니다.

그리고 Address Of Entry Point 포인트를 00 00 00 00 로 수정하고 저장합니다. (이때 hex edit 툴을 사용하면 좀더 편리할수도 있습니다.) Stud_pe가 저장이 잘 안될때가 있습니다.

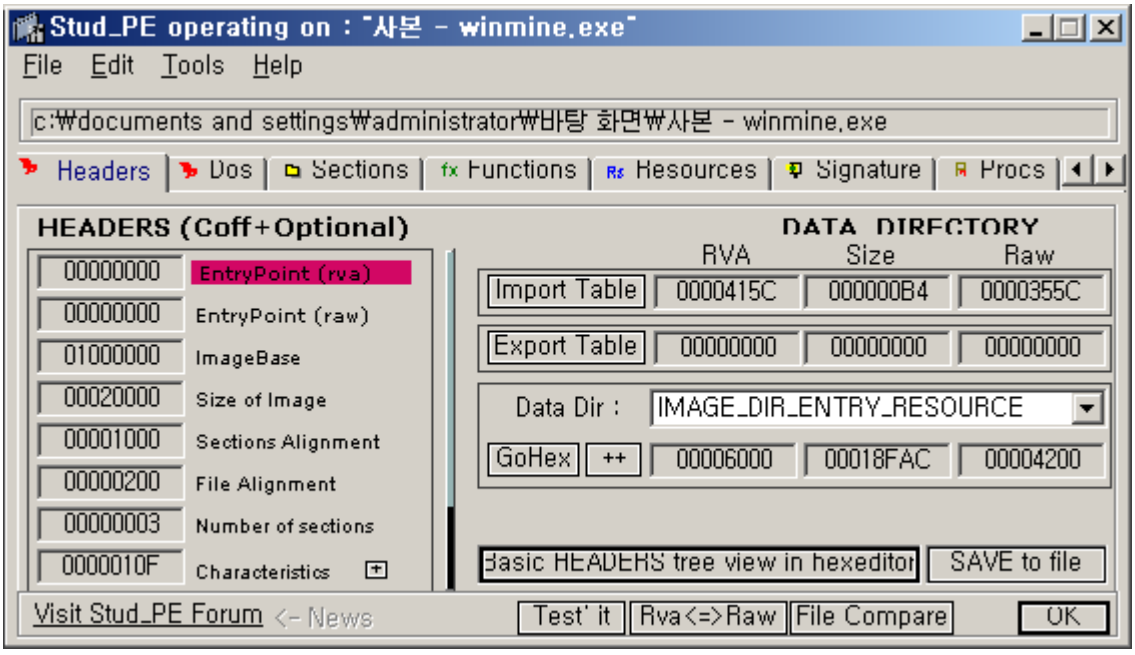
그리고 저장한후에 수정한 파일이 실행되는지 확인합니다.



수정된 화면입니다.



지뢰 찾기가 위와같이 잘 실행되면 성공적으로 수정이 된겁니다.



이제 이것을 ollydbg에 올리고 실행을 해보면 ollydbg가 제대로 ep를 찾지 못합니다. (일종의 안티리버싱 효과를 냅니다.)

물론 pe구조를 아는사람이라면 한번에 고치겠지만이요 ^^
악성코드들이 사용하는 방법이라고 하지만 요즘 av들은 자동으로
Ep를 수정하여 잘 잡는다고 하더군요
이상으로 PE Header Custom Packing를 마치겠습니다.

3. 마지막으로

처음 만들어본 문서라 참.. -_-문서형식이 없군요 죄송합니다;
Pe 골격을 알고계신분이라면 이방법을 알고 계실수도 있지만 혹시 모르시더라도 바로 알수있을만큼 쉬운 내용이라 부연설명은 제외하고 그냥 테크닉위주로 문서를 작성하였습니다. 아래는 참고한 곳입니다.

http://www.icrack.co.kr/viewthread.php?tid=169&extra=page%3D1
http://viruslab.tistory.com/362