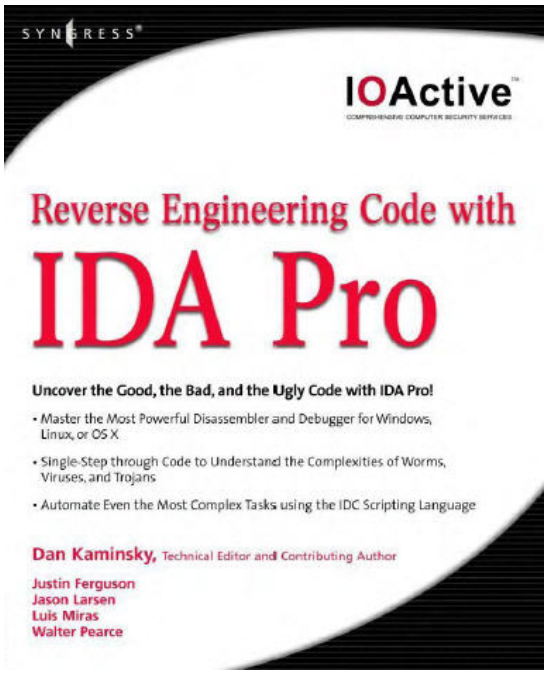
Reverse Engineering Code with IDA Pro

By Dan Kaminsky, Justin Ferguson, Jason Larsen, Luis Miras, Walter Pearce

정리: vangelis(securityproof@gmail.com)



이 글은 ***Reverse Engineering Code with IDA Pro***(2008년 출판)라는 책을 개인적으로 공부하면서 정리한 것입니다. 목적이 책 소개가 아니라 공부이므로 글의 내용은 형식에 국한되지 않고 경우에 따라 책의 내용 일부를 편역하거나 또는 철저하게 요약해서 올리고, 경우에 따라 필자가 내용을 추가할 것입니다. 내용에 오류 및 오타가 있다면 지적 부탁 드립니다.

1장

Code Debugger 개관

실행 파일(executable file)을 리버싱 엔지니어링(reversing engineering)하기 위해 우리는 다음 정보들에 대해 알고 있어야 한다.

- 호출하고 있는 정확한 메모리 주소
- 쓰고자 하는 메모리의 정확한 위치
- 읽고자 하는 메모리 위치
- 사용하고 있는 레지스터(register)

소스 코드(source code)를 가지고 있지 않은 파일을 리버싱 엔지니어링(reversing engineering)할 때 디버거(debugger)는 그 파일을 디스어셈블링(disassembling) 함으로써 우리에게 도움을 준다. 특히 디버거는 실행 파일의 소스 코드에 거의 접근할 수 없는 malware를 분석하는데 여러모로 편리하다. 이 장의 목표는 디버거들을 어떻게 사용하는지 자세하게 가르쳐주는 것이 아니라 '디버거'라는 것이 있으며, 아주 간단하게 기본 개념에 대해 알아보는 것이다. 디버거들은 전체 기능을 다 사용하는 것을 배우기에는 오랜 시간이 걸리는 아주 강력한 툴이다.

디버거들 중에서 정선된 것과 이 책에서 초점을 맞추는 것은 Interactive Disassembler Pro(IDA Pro)이며, DataRescue[1]에서 구할 수 있다. IDA Pro는 상업적인 환경에서 특히 유용하다. 이 책에서는 비싸지 않다고 하는데, 솔직히 좀 비싸다.[2]

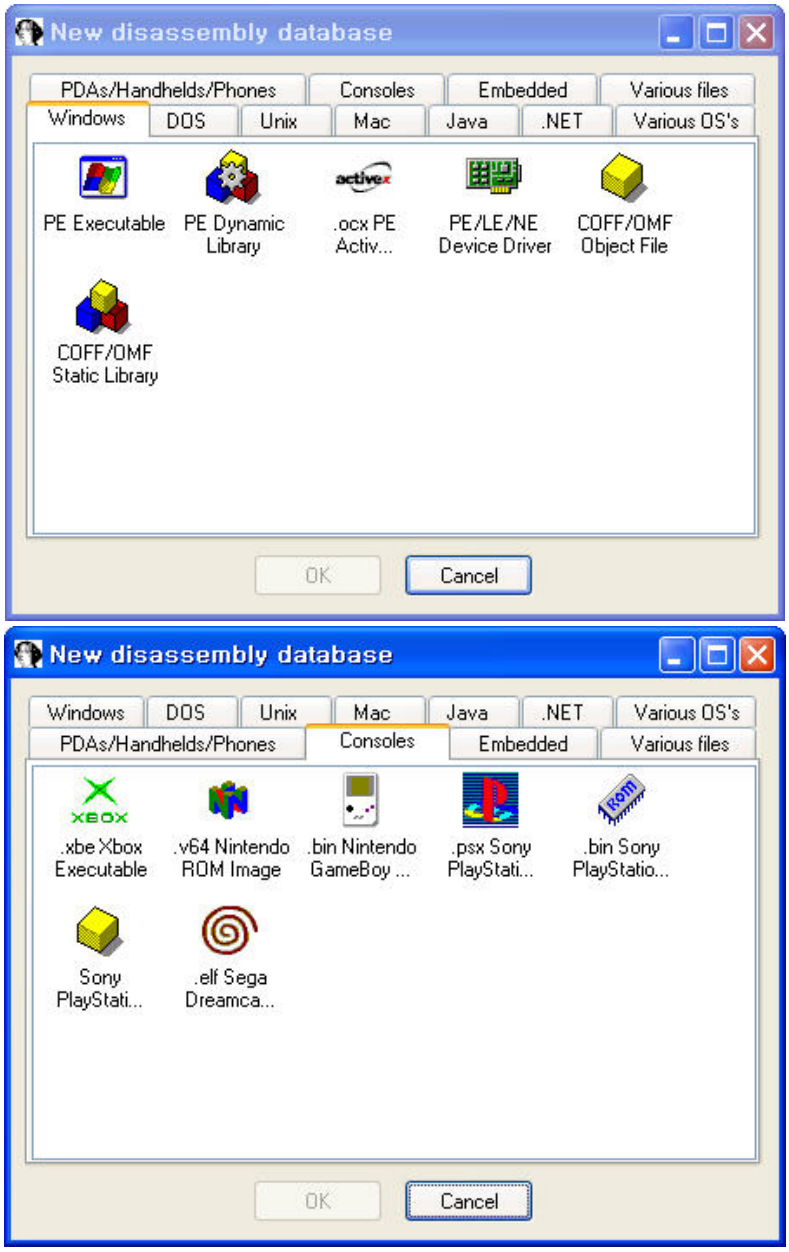
IDA Pro는 단순히 디버거 이상이다. IDA Pro는 프로그래밍이 가능하고, 대화식 디스어셈블러이자 디버거이다. IDA Pro로 현재 존재하는 어떤 타입의 실행파일이나 어플리케이션 파일도 리버스 엔

---

[1] 책에서는 datarescue 페이지로 나오지만 현재는 http://www.hex-rays.com/idapro/로 이동했다.
이 글을 쓰고 있는 현재 최신 버전은 5.2이며, http://www.hex-rays.com/idapro/idadowndemo.htm에서 데모버전을 구할 수 있다. IDA Pro 4.9(http://www.hex-rays.com/idapro/idadownfreeware.htm)는 freeware이다. 그러나 데모버전은 분석할 수 있는 파일 포맷 등에 제한이 있다.

[2] 국내에서는 100만원 이상 하고 있다. IDA Pro와 함께 사용되는 Hex-Rays Decompiler는 가격이 200만원이 넘는다. 하지만 이 툴들을 이용해 제대로 작업을 하여 최상의 결과를 거둘 수 있다면 비싸지는 않을 것이다.

지니어링을 할 수 있다. IDA Pro는 Xbox, Playstation, Nintendo와 같은 콘솔 머신에서부터 Macintosh 컴퓨터 시스템, PDA 플랫폼, Windows, UNIX, 등의 파일도 다룰 수 있다. IDA Pro를 처음 실행시켰을 때 초기 로딩 마법사[3]를 보면 디스어셈블하고자 하는 파일 타입에 대한 선택을 할 수 있도록 하는 파일 타입과 탭을 볼 수 있다.

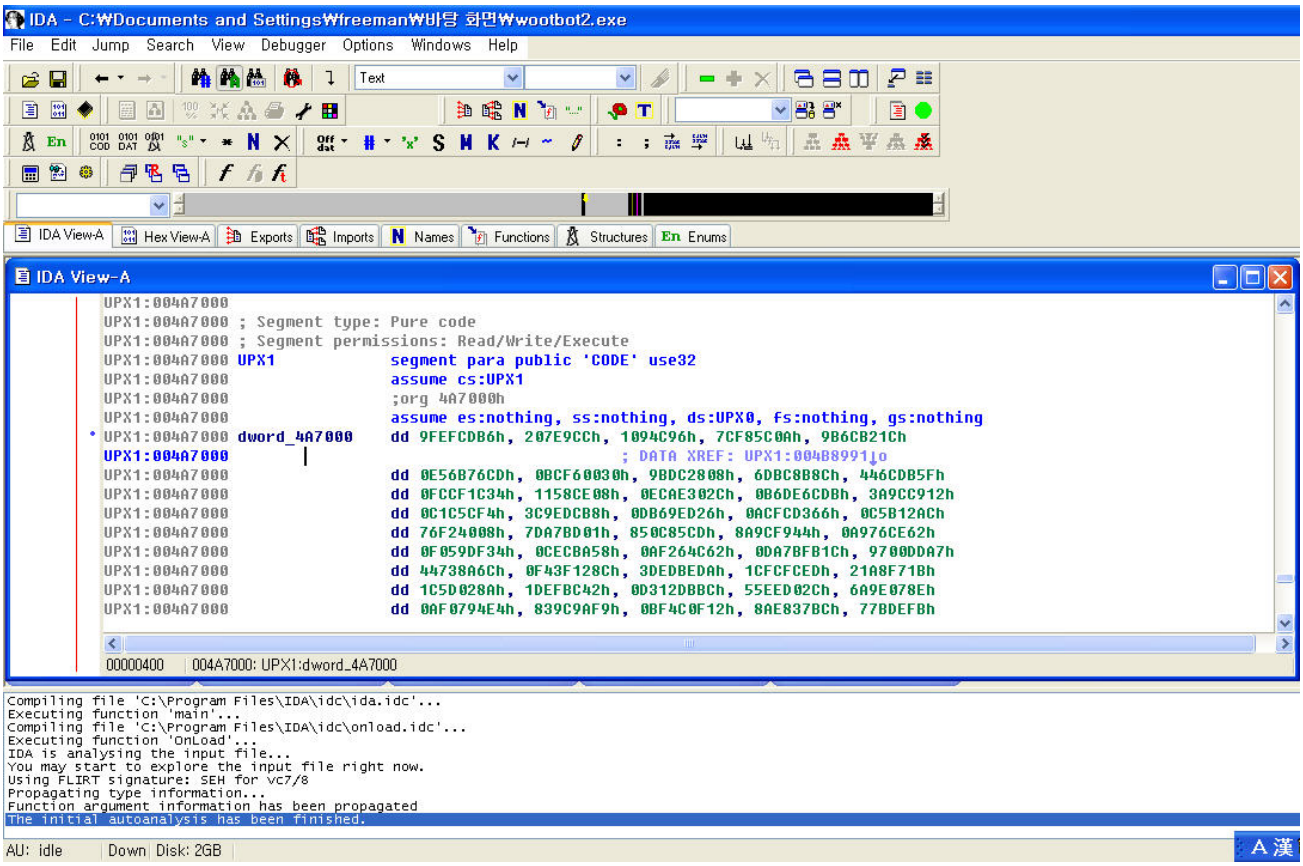


[그림1. IDA Pro의 New disassembly database]

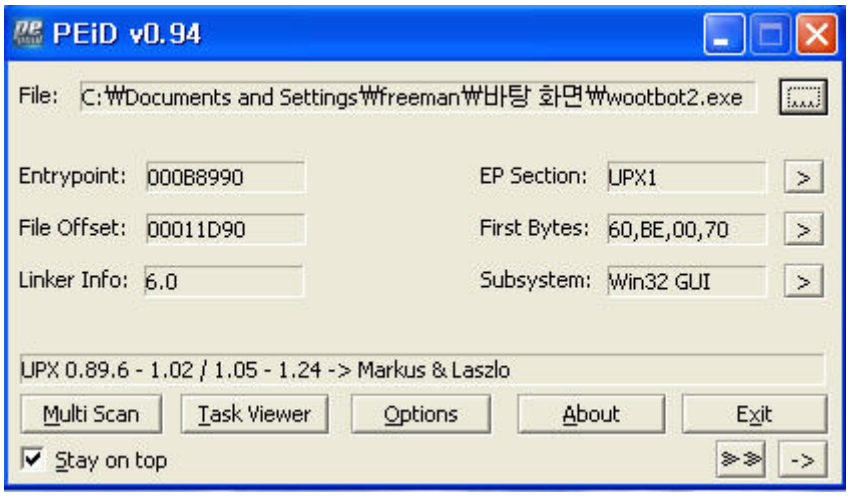
책에서는 IDA Pro는 instantmsgrs.exe라는 이름을 가진 WootBot 변종을 로딩하여 디스어셈블링하

[3] IDA Pro를 위한 플러그인 Hex-Rays를 설치하게 되면 "New disassembly database"창이 바로 띄지 않는 경우가 있는데, 굳이 "New disassembly database"창에서 지정하지 않아도 되기 때문이다. 이때 File -> New 를 클릭하면 "New disassembly database"창이 뜬다.

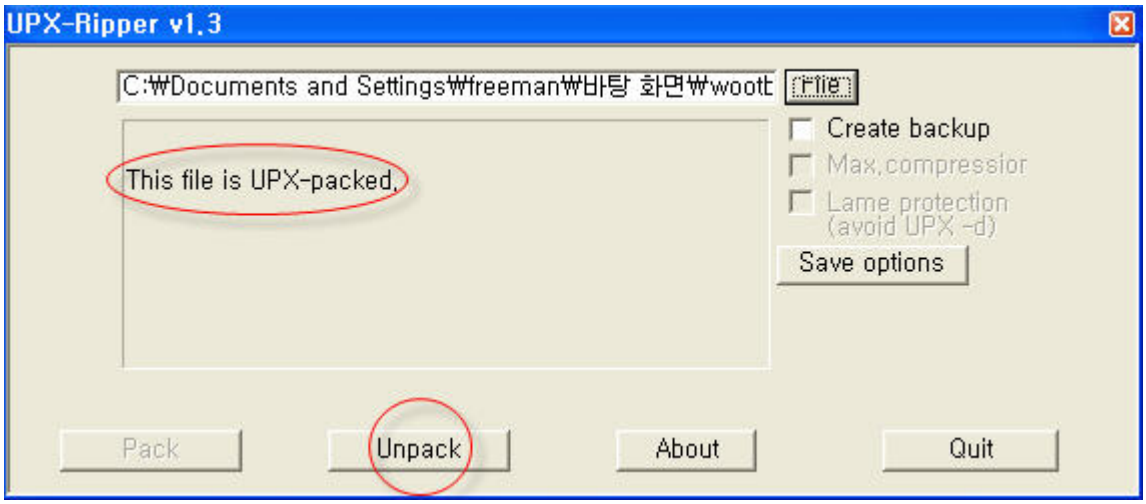
고 있다. instantmsgrs.exe는 Molebox라는 packer를 이용해 패킹되어 있다. 테스트를 위해 instantmsgrs.exe 파일을 구하려고 했으나 쉽게 구할 수 없었다. 그래서 필자는 국내 백신 업계 친구에게 wootbot 변종 하나를 구하여 IDA로 분석을 시도했다. 그러나 아래 그림에서 보듯 UPX로 패킹이 되어 있었다. UPX로 패킹되어 있어 바로 분석이 힘들다.

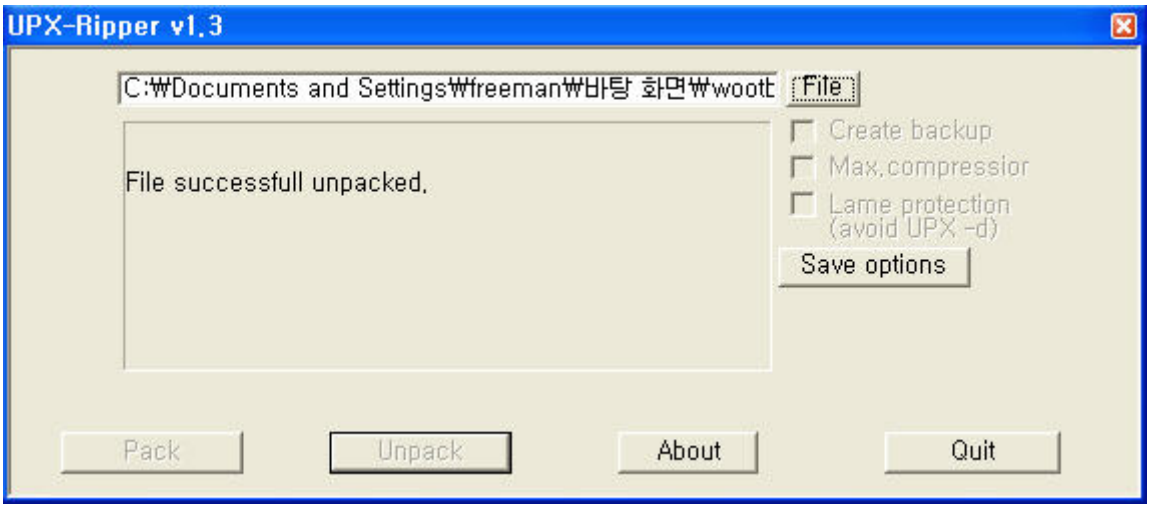


일반적으로 무엇으로 패킹되어 있는지 확인할 때 PEiD를 많이 사용한다. 여기서도 PEiD를 이용해 wootbot.exe라는 파일이 무엇으로 패킹되어 있는지 다시 확인해보았다. 요즘 악성코드 대부분이 패킹되어 나오기 때문에 먼저 packer가 무엇인지 확인해보는 것이 좋을 것이다.

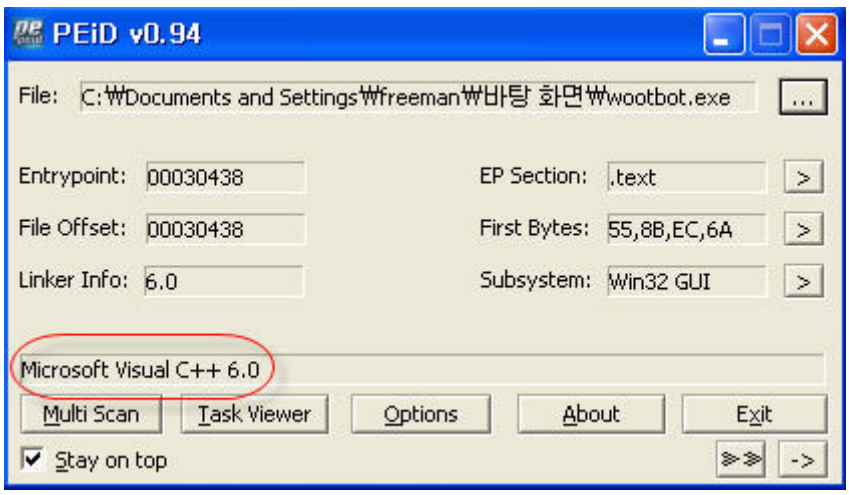


결과를 보니 UPX 0.89.6을 사용했다. 이 파일을 언패킹 하기 위해 UPX-Ripper라를 unpacker를 이용했다.

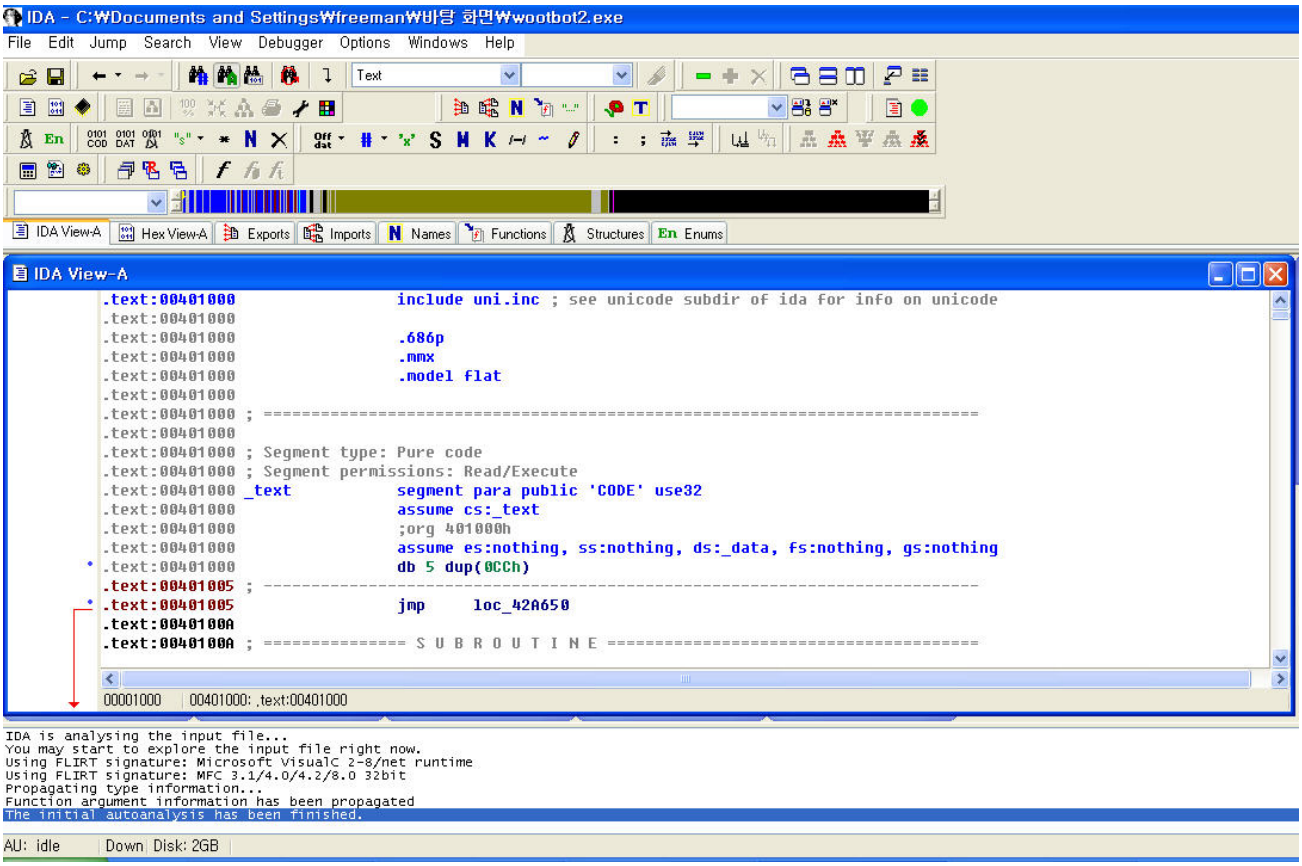




성공적으로 언패킹이 되었다. 다시 PEiD를 이용해 확인해보니 wootbot..exe라는 파일은 Microsoft Visual C++6.0으로 코딩되었다는 것을 알 수 있다.



이제 언패킹도 되었으므로 IDA로 분석이 가능해졌다. 언패킹 하기 전에 분석이 힘들었지만 아래 그림을 보듯 언패킹 후 메모리의 데이터를 확인할 수 있게 되었다. .



참고로 이런 악성코드 분석 작업은 vmware 같은 가상 시스템에서 실시하는 것이 보안을 위해서도 필수적이다.

요약

IDA는 가장 유명한 Windows용 디버깅 툴들 중의 하나이다. 먼저, IDA Pro는 바이너리(실행파일 또는 DLL(dynamic link library)의 어셈블리어 코드를 보여주는 **disassembler**이다. IDA는 어셈블리어 코드를 가능한 쉽게 이해할 수 있도록 하는 발전된 기능들을 가지고 있다. 두 번째, IDA는 바이너리 파일의 실제 명령(instruction) 분석과 그 명령이 연속적으로 실행되는 과정을 하나하나 분석할 수 있게 하는 **debugger**이다.