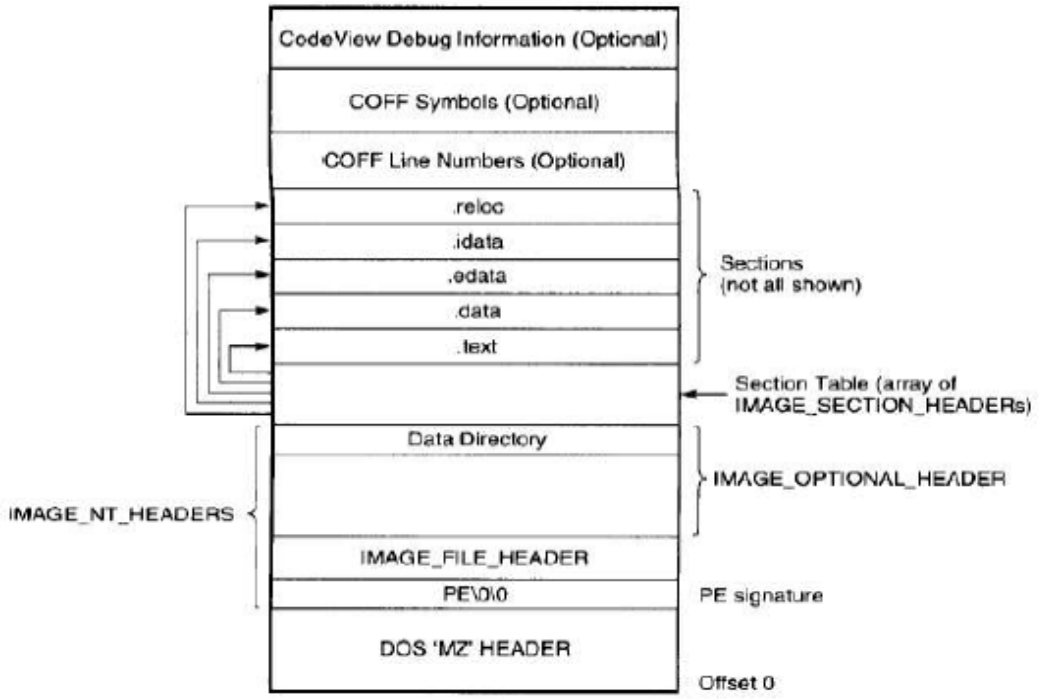
지금까지는 온라인 게임 해킹의 개념과 가장 일반적이고 널리 알려진 스피드핵과 오토마우스 해킹툴들에 대해 다루었지만, 이번에는 해킹 기술들 중에서도 고급해킹으로 통하는 실행파일 해킹과 메모리 해킹을 다루도록 하겠다.

1. 실행파일 해킹의 종류와 동작 방식

실행파일이란 윈도우에서 마우스를 클릭하였을 때 게임 프로그램이 시작되는 파일을 말하며, 파일 확장자로 exe, dll, ocx를 가진 파일을 말한다.
실행파일 해킹은 게임 클라이언트의 실행파일을 분석하여 조작하여 원하는 결과를 얻도록 하는 해킹을 말하며, 요즘에 인터넷 상에서 많이 찾아볼 수 있는 역공학(Reverse Engineering)이라는 기술을 사용하게 된다.

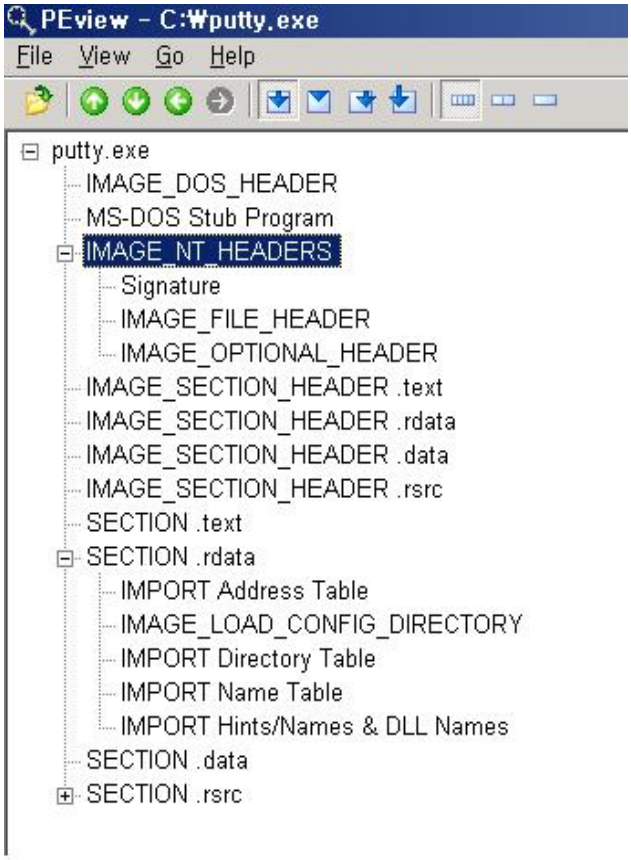
윈도우 실행파일의 구조

실행파일 해킹을 이해하기 위해서는 먼저 윈도우에서 실행되는 실행파일의 구조를 이해해야 한다. 윈도우 실행파일은 다음 그림과 같은 PE (Portable Executable)이라는 포맷을 가진다.



[그림 1] PE 포맷의 구조

PE 포맷이란 Window NT, XP, 2000 등에서 사용되는 실행가능한 코드를 포함하는 파일의 포맷을 말하며, PE 구조로 된 파일들은 플랫폼에 상관없이 Win32 운영체제가 돌아가는 시스템이면 어디서든 실행이 가능하다. (윈도우 98에서는 NE 포맷이 사용된다.)



[그림 2] PE View로 살펴본 PE 포맷의 구성

PE 포맷의 각 구성을 설명하면, 위 [그림 2]에서 볼 수 있듯이 헤더 정보와 실제 데이터로 크게 구분할 수 있다. 실제 데이터 영역의 각 Section에 대한 내용을 간단히 살펴보면 다음과 같다.

- SECTION .text : Executable Code Section
- SECTION .data, .rdata, .bss : Data Section
- SECTION .rsrc : Resource Section
- SECTION .edata : Export Data Section
- SECTION .idata : Import Data Section

윈도우 실행파일 구조에 대해 좀 더 자세한 정보를 알고싶은 분들은 관련한 정보를 찾아보기를 권장하며, 이 칼럼에서는 윈도우 실행파일 구조에 대한 개념적인 설명은 여기서 접기로 하겠다.

실행파일 해킹의 종류와 동작방식

실행파일 조작은 프로그램의 흐름이나 데이터를 영구적으로 변경할 수 있다는 장점을 가진다.

실행파일 해킹은 대게 실행코드 조작과 데이터 조작으로 이루어진다. 실행코드 조작은 PE 포맷의 Executable Code Section인 .text Section의 일부코드를 수정하는 방법을 사용한다. 가장 많이 사용되는 방법 중 하나로 보안 기능을 수행하는 함수나 게임에서 유저의 권한등을 체크하는 함수를 수행하지 않도록 하는 것이 사용된다. 예를 들어, Call SecurityFunction 이라는 실행코드가 있다고 가정할 때 이 부분은 모두 NOP(0x90)으로 수정할 경우 이 실행코드는 실행되지 않고 다음으로 넘어가게 된다.

데이터 조작은 PE 포맷의 Data Section 내에 저장된 특정 데이터를 수정하는 것이다. 예를 들어, HP INC 1 이라는 코드가 있다고 가정해보자. 이 코드는 게임 진행 중에 HP 값을 1단위로 증가시키라는 것이며, 여기서 해킹의 대상이 되는 데이터는 1이 될 수 있다. 이 값을 10으로 수정하고 게임을 실행하면, HP INC 10 이라는 코드가 실행이 되어 게임 진행 중에 HP 값을 10단위로 증가시킬 수 있게 되는 것이다.

2007년 안철수연구소에서 발표한 온라인 게임 해킹 상반기 동향 자료를 살펴보면 실행파일 조작 해킹은 거의 등장하지 않고 있다. 이는 실행파일 조작 해킹을 방어하기 위해 많은 게임 개발사들이 업데이트/패치나 실행파일에 대한 CRC 체크 루틴을 적용하는 등 실행파일 조작을 방어하기 위한 노력의 결과로 판단하고 있다.

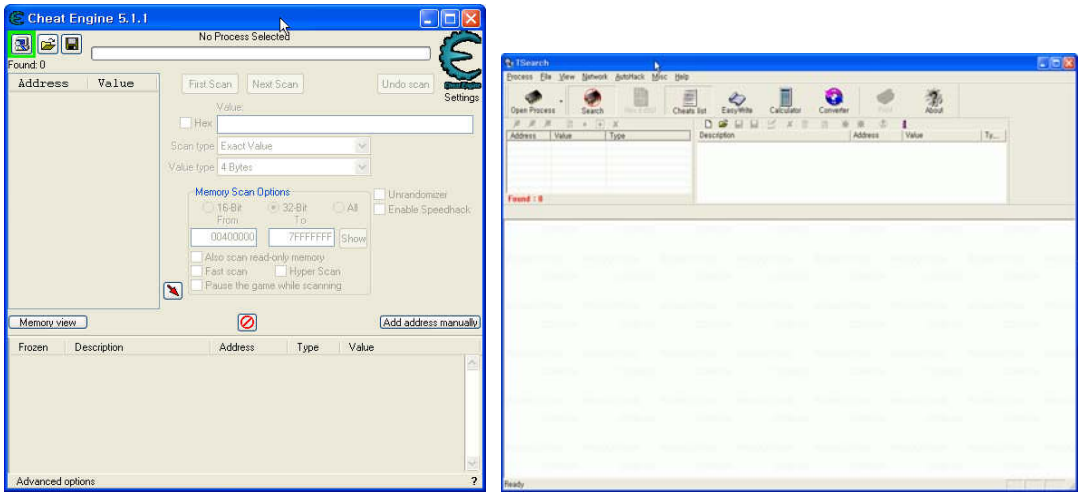
2. 메모리 조작 해킹의 종류와 동작방식

실행파일 조작에 이어 고급 해킹 기술로서 최근에도 여전히 골머리를 앓고 있는 메모리 조작 해킹에 대해 살펴보기로 하겠다. 2007년 들어서 메모리 조작 해킹은 비단 온라인 게임 뿐 아니라 다른 영역에서도 큰 문제로 등장하고 있다. 특히, 최근 모 방송사에서 인터넷 뱅킹 메모리 해킹 위협에 대한 보도 이후 메모리 해킹에 대한 관심이 매우 커졌으며, 이에 대응하는 메모리 해킹 보호 방법에 대한 많은 고민들이 진행되고 있다.

메모리 해킹의 경우 다양한 공격방법이 존재하며 모든 공격방법을 한번에 다루기는 어렵기 때문에 2번에 나눠서 설명을 하도록 하겠다.

메모리 해킹툴의 종류

해킹에 조금이라도 관심이 있는 사람이라면 인터넷 상에서 유명한 해킹툴 한두개 정도는 알고 있을 것으로 생각된다. 그 기능이 강력하다고 소문이 무성한 유명한 해킹툴들은 대부분이 메모리 해킹과 관련된 툴들이다. 메모리 해킹툴들은 기본적으로 공격 대상 프로세스에 접근하여 메모리를 서치하고 메모리 상의 데이터나 코드를 조작하고 가변적인 데이터를 고정시킬 수 있는 기능들을 제공한다. 이러한 메모리 해킹툴 들 중에서도 Cheat Engine이나 TSearch 등은 해킹에 관심있는 사람이라면 한번쯤 들어 보았음직한 메모리 조작 해킹툴이다.

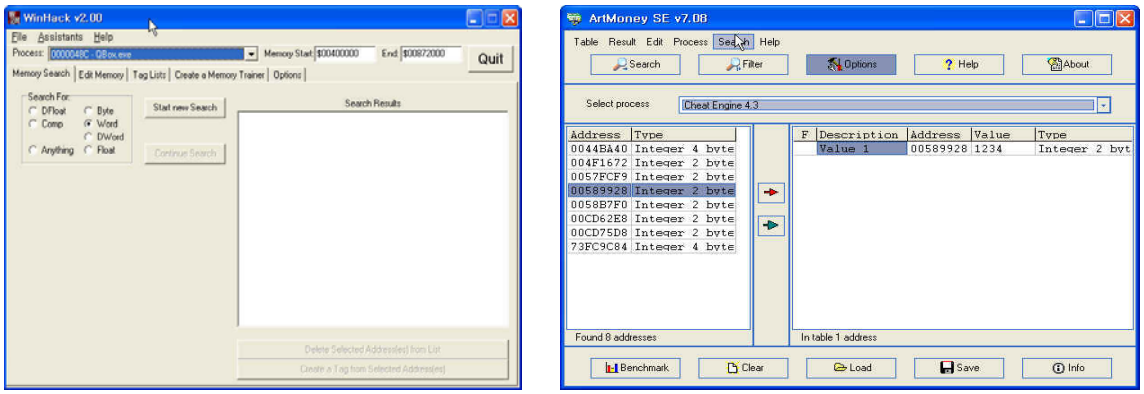


[그림 3] Cheat Engine과 TSearch

Cheat Engine은 게임 상의 특정 데이터를 지정하면 그 데이터를 조작하는 실행코드를 찾아주는 기능을 제공하여 보다 쉽게 메모리 상의 코드조작을 할 수 있도록 도와준다. 또한, Cheat Engine Trainer Builder라는 것을 제공하여 Cheat Engine 없이 독립적으로 실행가능한 해킹툴을 제작할 수 있도록 함으로써 누구나 쉽게 해킹툴을 제작하고 사용할 수 있다. 또한 은폐기능을 제공하여 스스로를 숨기는 기능을 가지고 있어서 일반적인 프로세스 감지 기술로는 발견하기 어려운 해킹툴이다.

TSearch의 경우 기본적인 메모리 조작 기능외에 간단히 Debugger 역할을 수행할 수 있는 기능을 제공하며, 네트웍을 통한 접근을 허용한다는 특징을 가지고 있다.

그 외에도 WinHack, ArtMoney와 같은 해킹툴 세계에선 고전적인 해킹툴들도 여전히 사용되고 있으며, Game Master, Game Hack, Game Wizard와 같은 게임 전용 메모리 해킹툴들도 사용되고 있다.



[그림 4] WinHack과 ArtMoney

3. 마치며

이번에는 실행파일 조작과 메모리 조작 해킹에 사용되는 해킹툴들에 대해서 살펴보았다. 메모리 조작과 같은 고급 해킹은 아직은 우리나라에서 심각하게 대두되고 있는 것은 아니며, 현재는 중국과 일본, 동남아 등지에서 많이 발생하고 있다. 국내의 경우 CheatEngine Trainer를 이용한 해킹툴들은 간간히 발견되고는 있으나, 특정 게임을 대상으로 직접적인 메모리 해킹을 시도하는 해킹툴은 오토플레이에 비하면 매우 미약한 수준이다. 메모리 조작 해킹은 다음 호에서도 이어서 다룰 예정이며, 다음 호에서는 실행파일(PE구조)의 메모리 로딩 방식과 메모리 조작의 다양한 방법에 대해서 살펴보도록 하겠다.