

1. 온라인 게임 해킹의 패러다임 변화

이번 회에는 온라인 게임 해킹의 패러다임이 어떻게 변화되고 있으며, 현재의 온라인 게임에 주요 사용되고 있는 해킹기술들이 무엇인지 전반적으로 살펴보고자 한다.

초기 온라인 게임은 MMO RPG 형태의 게임이 주류를 이루면서 오토플레이나 매크로와 같은 해킹이 많이 이루어졌다. 또한, 이러한 툴들은 자기 과시용이나 개인 연구용으로 제작되는 경우가 많았다.

그러나, 2005년 이후 전세계적으로 온라인 게임 해킹은 일종의 비즈니스 형태를 갖추고 고도로 성장을 하고 있다. 특히, 우리나라의 경우, 중국의 영향으로 해킹툴들이 점차 상업적으로 이용되고 있으며, 이러한 툴 제작자들은 앞으로 더 조직화된 형태로 움직일 것으로 예상된다. 실제로 MMO RPG류의 게임에서의 오토플레이 툴들은 이미 상업적으로 성장해있는 것이 현실이다.

온라인 게임 해킹의 **산업화**

- 온라인 게임 산업의 급성장
- 온라인 게임 아이템 시장의 급성장
- 게임 해킹이 비즈니스로 성장

온라인 게임 해킹기술의 **고도화**

- 해킹 도구의 전문화, 상용화
- 해킹 도구의 지속적인 업그레이드
- OS 커널 기술, 악성코드 기술 등의 접목

온라인 게임 해킹의 **글로벌화**

- 온라인 게임의 글로벌화 → 해킹 도구의 글로벌화
- 인터넷을 통한 다양한 해킹기술의 공유

[온라인게임 해킹의 패러다임 변화]

온라인 게임 해킹의 산업화

온라인 게임 해킹은 기업화된 조직을 갖추고 산업의 일부로 자리잡을 것으로 예상된다. 해킹이 산업의 일부로 자리잡는 것이 의미적으로 맞지 않는 표현일지도 모르겠으나, 해킹의 개념을 좀 더 넓게 본다면 꼭 맞지 않는 표현만은 아닐 것이라고 본다.

온라인 게임 해킹을 넓은 의미로 정상적인 게임 행위가 아닌 방법으로 게임 플레이에 영향을 주는 모든 행위라고 볼 수 있다. 인터넷 상에서 가장 많이 거래되고 툴 중 하나인 오토플레이 툴들을 예로 들어보자. 오토플레이는 게임 프로그램을 조작하는 행위 - 게임 프로그램 파일을 조작하거나, 게임이 실행중인 상태에서 메모리 상의 데이터나 코드를 조작하는 행위 - 가 아니라, 인위적으로 키보드와 마우스 이벤트를 발생시켜 게임에 전달하는 방식이다. 게임 프로그램을 조작하는 행위가 아니기 때문에, 법적으로는 해킹 행위에 속하지 않을 수 있으며, 게임 업체와 게임 유저들 사이에서도 오토플레이가 해킹인지 아닌지에 대한 의견이 갈리고 있다. 만일, 이와 같은 오토플레이를 해킹으로 간주한다면, 우리나라의 온라인 게임 해킹 산업은 그야말로 급속한 성장을 이루고 있는 셈인 것이다.

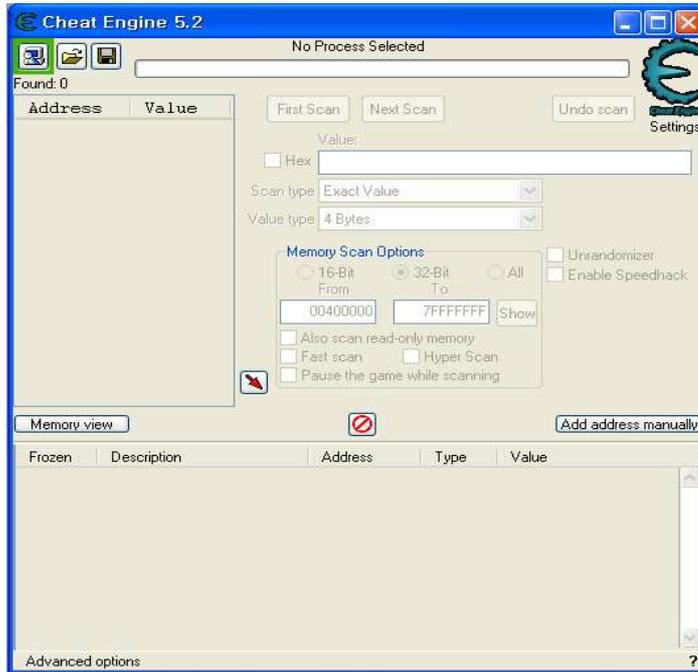
음과 양이 항상 공존하는 것이 세상의 이치라고 한다. 그런 면에서 온라인 게임 산업의 성장과 더불어 해킹 산업의 성장은 필연이라고 볼 수도 있다. 나라마다 시기와 속도의 차이는 있겠지만, 전 세계적으로 온라인 게임 해킹 산업은 계속 성장할 것이며, 문제는 그것이 음성적으로 성장하여 온라인 게임 시장에도 악영향을 미치고 사회적인 문제로 이슈화 된다는데 있다.

온라인 게임 해킹의 고도화

온라인 게임 해킹이 상업성을 띄면서 그 기술조차 매우 고도화되어 가고 있다. 또한, 과거 악성코드 제작자들이 금전적인 이득을 취할 수 있는 온라인 게임 쪽으로 눈을 돌리게 되면서, 그 기술은 더욱 발전하고 있다.

최근에는 악성코드 기술과 온라인 게임 해킹기술이 서로 교류하면서 발전하는 경향마저 보이고 있다.

과거에 자기 과시용으로 많이 배포되던 공용 해킹툴들-메모리 조작, 매크로류-도 그 기술이 날로 발전하여 다양한 고급 기능과 편리한 사용자 인터페이스를 제공함으로써 누구나 쉽게 해킹을 접할 수 있도록 하고 있다.



[메모리 조작 해킹툴로 유명한 Cheat Engine]

온라인 게임 해킹의 글로벌화

인터넷 시대에 걸맞게 다양한 해킹기술에 대한 정보를 손쉽게 인터넷 상에서 얻을 수 있다. 이러한 해킹기술에 대한 정보를 게시하는 사이트는 2006년 이후 많이 늘어난 것으로 파악된다.

실제로 2005년까지 우리나라의 온라인 게임 해킹기술은 매크로와 오토플레이가 주류를 이루었으며, 메모리 조작이나 실행파일 조작과 같은 고급 기술들은 많이 등장하지 않았다. 또한, 해킹기술의 전파 흐름을 볼 때도 2005년 이전까지는 중국에서 동남아를 거쳐 우리나라로 유입되는 현상을 볼 수 있었다. 예를 들어, 중국에서 발견된 해킹툴이나 해킹기법이 5-6개월 정도 후에 우리나라에서 발견되는 경우가 대부분이었다.

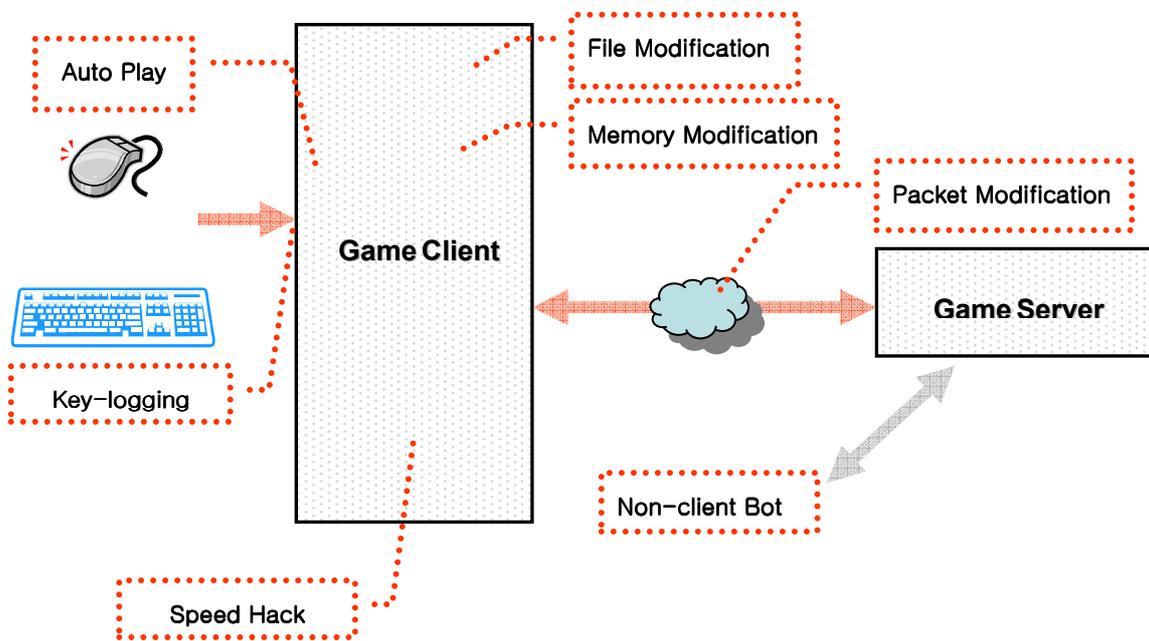
그러나, 2006년 이후 해킹기술의 전파속도가 매우 빠르고 그 기술 또한 다양해졌으며, 많은 커뮤니티가 생기면서 기술공유의 글로벌화를 이루고 있다. 앞으로 이러한 해킹기술은 국가적 특성이나 환경에 구애 받지 않고 자유롭게 공유되고 연구되어 그 발전 속도가 더 빨라질 것으로 예상하고 있다.

2. 온라인게임의 다양한 해킹기법

과거의 게임 해킹은 PC게임을 중심으로 이루어졌으며, 스크립트를 조작하거나 Cheat Key 형태의 장난스러운 게임 조작이 주를 이루었다. 예를 들어,

축구 게임에서 캐릭터의 모습을 변형한다거나 스타크래프트와 같은 전략시뮬레이션 게임에서 미네랄과 가스의 양을 순식간에 늘려준다든가 하는 것이 그것이다. 이러한 치트키들은 해킹이라고 보기 보다는 개발사에서 게임을 테스트하는 용도로 사용되거나 유저들에게 보다 재미있게 게임을 즐기도록 제공하는 것이 대부분이었다. 또한 이러한 Cheat Key나 스크립트 조작 등은 온라인상에서 자기 과시용으로 많이 활용되기도 하였다.

앞서 언급한 온라인 게임 해킹의 패러다임 변화로 인해 온라인 게임 해킹의 접근 경로가 다양화되고 있다.



[온라인 게임 해킹의 종류]

오토플레이 (Auto Play)

오토플레이는 오토마우스와 매크로류의 툴들을 통칭하는 의미이다. 사용자가 직접 게임 플레이를 하지 않더라도 다른 프로그램 또는 H/W를 통해 자동으로 키보드와 마우스 이벤트를 게임에 전달하여 자동으로 게임 플레이를 하도록 하는 툴을 말한다. 주로 MMO RPG 게임에서 많이 등장하고 있다.

키로거 (Key-logging)

최근 사회적으로 가장 문제가 되고 있는 해킹툴로 트로이목마성 악성코드로 분류된다. 주로 사용자의 계정과 개인정보를 훔쳐내기 위한 용도로 사용된다.

스피드 핵 (Speed Hack)

가장 많이 사용되는 해킹툴 중의 하나로 PC 시간을 인위적으로 조작하여 게임 플레이 속도를 자유롭게 조작하도록 하는 툴이다. 최근에는 게임개발 시점에 스피드 핵을 보완하는 설계를 하고 있어서 조금씩 사라지는 경향을 보이고 있다.

파일 조작 (File Modification)

게임 클라이언트 파일의 코드나 데이터에 인위적으로 조작을 가하여 제작된 해킹툴이다. 주로 온라인 게임 보안제품을 호출하는 부분이나 게임 내부의 주요 함수를 조작한다. 온라인 게임 보안제품을 호출하는 부분을 건너뛰거나 실행하지 않도록 함으로써 보안기능을 무력화시키는데 주로 활용된다.

메모리 조작 (Memory Modification)

파일 조작과 동일한 목적으로 사용되며, 게임이 실행 중인 상태에서 메모리 상에 있는 데이터와 코드를 조작하는 해킹툴을 말한다. 게임의 결과치를 수정하거나 경험치, 능력치를 인위적으로 조작하는데 사용된다.

네트워크 패킷 조작 (Packet Modification)

게임 클라이언트와 서버간의 네트워크 패킷을 조작하는 해킹툴을 말한다. 대부분의 게임이 네트워크 패킷을 암호화하여 전달하지만, 다양한 방법으로 이를 무력화시켜 인위적으로 패킷을 조작한다. 주로 클라이언트에서 서버로 전달하는 패킷을 가로챈 후 이를 조작하여 전달하는 방식이다.

논클라이언트 봇 (Non-Client Bot)

해킹툴 중 가장 악명높은 해킹툴로 게임 클라이언트 없이 해킹툴만으로 실제 게임을 한 것과 동일한 결과를 얻을 수 있도록 해준다. 논 클라이언트 봇은 게임 클라이언트와 패킷 등 게임의 모든 부분이 다 분석이 되었다는 것을 의미하며 보안 상 치명적인 문제를 발생시킨다.

3. 마치며

이번 회는 온라인 게임 해킹의 패러다임의 흐름과 온라인 게임 해킹의 종류에 대해서 전반적으로 살펴보았다. 다음 회에는 온라인 게임 해킹의 종류별로 좀 더 깊이 있는 분석을 진행하고자 한다.