게임 핵과 보안의 상관관계

지도교수 : 서 정 만
연 구 자 : 홍 정 우

< 목 차 >

요 약

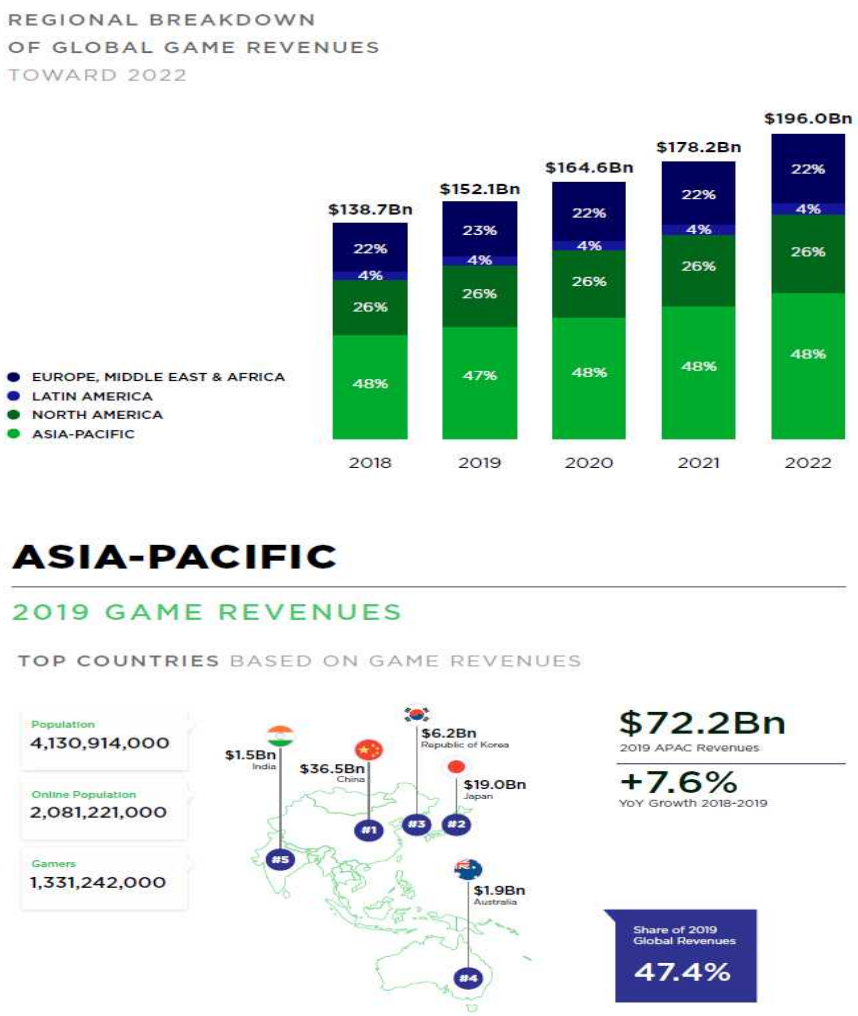
한국의 게임문화가 발전하고 PC방 문화가 발전하며 수많은 게임을 전자 소프트웨어 유통망(ESD)에 의해 쉽게 접할 수 있게 되었다. 그 과정 중에는 그만큼 게임의 위해를 가하는 게임 핵들과 게임 봇들도 같이 성장하였다. 싱글 플레이형 게임에서는 비교적 덜하여 크게 문제가 생기지 않는 경우가 있으나 온라인 기반에 멀티플레이 게임에서는 이는 게임의 인기와 서비스 문제에 직결할 정도로 큰 영향을 끼치기도 한다. 이런 게임 핵들이 어떤 것이 있고 어떤 방식으로 작동하며 사용 되는지 그리고 어떻게 막을 수 있는지 알아보도록 하겠다.

주요어 : 게임핵

1. 서론

1.1 게임의 성장

게임은 꾸준히 성장해왔고 세계적으로 지원과 관심이 주어지는 4차 산업혁명의 기술들을 적용받을 수 있는 분야 중 하나이다. 거기다 2019년 겨울부터 시작해 2020년을 강타한 SARS-CoV-2(코로나 바이러스)의 영향으로 인한 동물의 숲과 스위치 판매 대란이 일어났을 정도로 외부 활동 감소로 인해 게임이 영향과 주목을 받고 있다는 것을 짐작할 수 있으며 앞으로도 성장성이 기대되는 분야 중 하나이다.



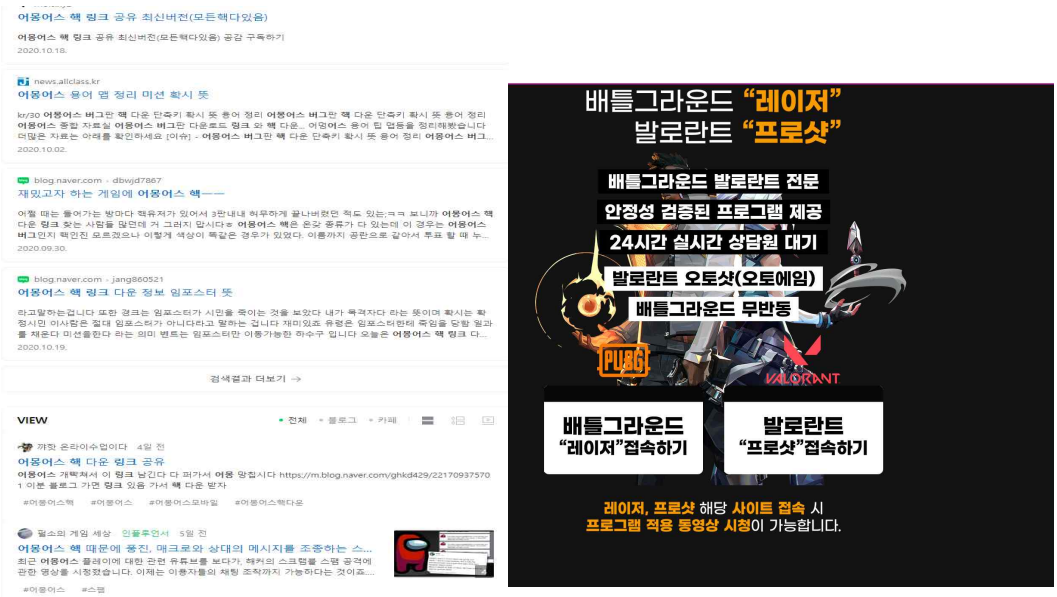
[사진 1]

2019년과 2020년에 게임의 성장 추세를 보며 커질 산업 규모를 예상한 표이며 2019년의 예상보단 낮았지만 꾸준히 성장해가는 게임의 산업 규모를 확인할 수 있다. 특히 아시아권의 지분이 굉장히 높은 수치로 나오기에 대한민국 내수시장도 중국, 일본의 수출적인 면에서도 아주 좋은 입지를 가지고 있다.

1.2 게임의 성장에 따른 게임 핵의 성장

초창기 악성코드 제작자들은 주로 자기 실력을 과시하기 위한 목적으로 악성코드를 제작하였고, 이런 의도로 만들어진 대부분의 악성 코드들은 바이러스나 웜으로 분류되는 것들이었다. 이들은 감염된 시스템의 리소스를 소모 시키거나 사용자에게 불편함을 느끼게 할지언정, 적어도 경제적인 손실과 같은 직접적인 피해를 입히진 않았다.

하지만 악성코드 제작자들의 목적이 실력 과시에서 이윤 획득으로 선회함에 따라, 마찬가지로 악성코드의 형태와 종류도 그에 맞춰 변하기 시작한다. 미국과 유럽으로 대표되는 서구권에서는 봇넷(Botnet; 많은 시스템을 자신의 Bot으로 감염시켜 조종하려는 목적의 악성코드)이나 뱅커(Banker; 은행과 관련된 인증정보 탈취를 목적으로 하는 악성코드), 랜섬웨어(RansomeWare; 감염된 PC의 자원을 사용하지 못하게 만든 후, 이를 복구해준다는 대가로 사용자에게 금전을 요구하는 악성코드)등의 악성코드가 유행하는 반면, 중국 내지 한국과 같은 동아시아권에서는 온라인 게임의 계정정보를 탈취하기 위한 목적의 악성코드인 온라인게임 핵(OnlineGameHack)이 가장 많이 만들어지고 있는 추세이다.



[사진 2]

포털 사이트에 게임의 핵 구매법이라고 검색한 결과이다. 영상이나 링크로도 쉽게 확인 가능했고 그 중에는 정상적인 사이트 마냥 판매를 하는 사이트도 존재했었다. 이제 검색만으로 상점가에서 물건을 사는 것처럼 게임 핵을 구할 수 있을 정도로 성장했다.

1.3 게임(에임 봇)핵에 대한 법원의 판결

☞ 피고인은 유한회사 블리자드엔터테인먼트가 운영하는 '오버워치' 게임(이하 '이 사건 게임')에서 상대방을 자동으로 조준하는 기능을 가진 프로그램(이하 '이 사건 프로그램')을 판매함으로써 정보통신망법 제70조의2, 제48조 제2항을 위반하였다는 공소사실 등으로 기소되었음.

☞ 이 사건 프로그램은 이용자 본인의 의사에 따라 해당 이용자의 컴퓨터에 설치되어 그 컴퓨터 내에서만 실행되고, 정보통신시스템이나 게임 데이터 또는 프로그램 자체를 변경시키지 않는 점, 이 사건 프로그램은 정보통신시스템 등이 예정한 대로 작동하는 범위에서

상대방 캐릭터에 대한 조준과 사격을 더욱 쉽게 할 수 있도록 해줄 뿐이고, 이 사건 프로그램을 실행하더라도 기본적으로 일반 이용자가 직접 상대방 캐릭터를 조준하여 사격하는 것과 동일한 경로와 방법으로 작업이 수행되는 점, 이 사건 프로그램이 서버를 점거함으로써 다른 이용자들의 서버 접속 시간을 지연시키거나 서버 접속을 어렵게 만들고 서버에 대량의 네트워크 트래픽을 발생시키는 등으로 정보통신시스템 등의 기능 수행에 장애를 일으킨다고 볼 증거가 없는 점 등에 비추어, 이 사건 프로그램이 정보통신망법의 '악성 프로그램'에 해당한다고 단정하기 어렵다는 이유로, 이와 달리 판단한 원심을 파기한 사안이다.

☞ 게임의 공정성에 영향을 미칠 수 있는 프로그램이라고 하여 무조건 정보통신망법의 '악성 프로그램'에 해당하는 것이 아니고, 악성 프로그램 해당 여부는 판시와 같은 여러 요소들을 종합적으로 고려하여 판단되어야 한다는 취지를 분명히 한다.

☞ 다만 본 판결은, 이 사건 프로그램이 '정보통신망법의 악성 프로그램'에 해당하지 않는다고 판단한 것일 뿐, 온라인 게임과 관련하여 일명 '핵' 프로그램을 판매하는 등의 행위가 형사상 처벌되지 않는다고 판단한 것은 아님(이러한 행위는 정보통신망법 위반죄와 별개로 게임산업진흥에 관한 법률 위반죄 등에 해당될 수 있음) 이 결과에 의하면 형사법인 정보통신망법 위반죄로는 에임 봇 같이 게임에 수익의 직접적으로 타격을 줄 수 있는 프로그램이 아니라면 처벌을 할 수 없다는 것으로 나왔으나 게임산업진흥에 관한 법률로는 처벌이 가능할 수도 있다.

그러나 형사법에 걸리지 않기에 수익을 크게 벌고 있는 회사나 제작자들은 더더욱 핵을 거리낌 없이 만들 가능성이 높아졌다.

2. 핵의 종류

2.1 장르별 핵의 종류

핵은 게임의 정보를 조작하는 행위로 수많은 변조가 가능하지만 장르별로 많이 쓰이는 핵을 알아보도록 할 것이다. 게임마다 세부적인 조작 혹은 시스템이 각자 다르기 때문에 같은 장르에서 다른 분류의 핵이 쓰일 수도 있으며 타 장르에서 많이 사용되는 핵이 다른 장르에서 핵으로 사용될 수도 있다.

2.1.1 FPS

대부분 핵사용 이슈의 가장 민감하며 핵을 잡는데 제일 열 올리지만 생각보다 성과가 안나는 장르이다. FPS는 대부분 PVP가 중점인 게임이기에 발견 횟수가 적어도 굉장히 크게 티가 난다. 거기다 3)의 선례처럼 쉽게 법적 조치를 취하기도 쉽지가 않기 때문에 지속적이고 높은 게임회사의 관심과 제제밖에 방법이 없다. FPS는 1인칭 시점으로서 타 장르에 비해서 시야가 볼 수 있는 범위가 좁고 현실감 있게 보여지는 경우가 많다. 이 제약을 뚫어버리고 원하는 곳으로 순식간에 이동하는 스피드 핵, 벽과 같은 엄폐물 사이를 뚫고 사격이 가능하거나 적을 볼 수 있는 월 핵, 자신의 조준점을 적에게 맞춰주는 에임 핵 등이 가장 대표적인 핵들이며 이외에도 게임의 세부적인 시스템에 따라 여러 핵이 존재한다. 4)은 PLAYERUNKNOWN'S BATTLEGROUNDS라는 게임의 사용될 수 있는 핵을 모아놓은 표이다.

[Table 2] List of Cheating Programs in Shooter-game

Action	Cheating Program	Description
①	ESP	display information about players and items through walls and terrain
②	cool-time remover	remove cool-down
③	speed hack	increase player's moving speed
④	wall hack	make walls transparent or non-solid
⑤	sound hack	remove player's footsteps sound
⑥	ammo hack	obtain infinite ammunition
⑦	aim hack	to shoot enemies without having to aim (aiming automatically)
⑧	recoil hack	remove effects of gun recoil

[표 1]

2.1.2 RPG

RPG는 대체적으로 핵을 사용하는 목적이 게임 내 재화와 직결된 경우가 많다. 게임 내 재화를 수치를 조정하는 금전 핵이나 아이템 복사 핵, 조작을 할 때 수 십대의 컴퓨터가 같이 조작이 되는 멀티태스킹, 정해진 조작을 저장해 유저의 조작이 없이도 알아서 움직이는 오토 프로그램 등이 대표적이고 PVP까지 가능한 RPG라면 적을 쓰러트리기 쉽게 하기 위한 쿨타임 핵이나 에임 핵같은 스킬필중 핵 등 더 많은 핵이 쓰인다.

RPG는 싱글 플레이 게임이 상당히 많은데 이런 싱글 플레이형 RPG의 특이사항으로 트레이너라는 핵이 존재한다. 이 트레이너는 관리자처럼 상당수의 수치를 조정하거나 외형을 바꾸는 등의 플레이가 가능하게 해준다. 하지만 멀티 플레이 RPG와는 다르게 재화가 증가하거나 게임캐릭터가 부정하게 강해진다 하여도 이미 게임을 구입 했다면 플레이어 혼자만 상호작용이 가능하기에 대체적으로 게임회사는 크게 제제를 가하거나 하진 않는 편이며 이 트레이너가 유행하여 게임이 인기를 얻는 경우도 존재한다. 대표적으로는 The Elder Scrolls V: Skyrim이 있다.

[사진 3] Sekiro: Shadows Die Twice의 모드 적용 전과 후

2.1.3 RTS, AOS

장르의 특성상 정보전이 중요한 대결 게임이기에 적의 가려져야하는 정보를 훤히 볼 수 있는 맵 핵이 가장 많은 편이며 이 외에도 이동, 타겟팅, 마이크로 컨트롤 등을 도와주는 소위 헬퍼도 상당한 인기가 있다.

2.1.4 리듬, 격투 게임

1프레임 단위가 게임에 큰 영향을 끼치므로 타이밍을 놓치지 않게 해주는 행동을 예약시켜 주거나 가만히 있어도 노트를 눌러주거나 알아서 가드를 해주는 오토 프로그램이 대부분을 차지한다.

3. 게임 핵의 탐지와 변조 방법, 해킹 주요 프로그램 및 게임회사의 방안

3.1 탐지단의 따른 분류

게임 산업에서 사용하는 게임 봇 탐지 방법을 [표 2]에서와 같이 크게 세 가지 범주인 클라이언트 단, 네트워크 단, 서버 단에서의 탐지로 분류하였다.

클라이언트 단 탐지 방법인 보안 소프트웨어 사용은 다른 소프트웨어나 하드웨어와 자주 충돌을 일으켜서 사용자들의 불편을 야기한다. 게임 봇만 찾을 수 있는 보이지 않는 아이템을 만드는 등 게임 디자인을 통한 탐지 방법은 드러나는 순간 기능을 상실하게 된다.

네트워크 트래픽 측정이나 네트워크 프로토콜 변경과 같은 네트워크 단 탐지 방법은 네트워크 부하와 게임 플레이에 렉(lag)을 유발시킨다. 클라이언트 단과 네트워크 단 탐지 방법의 단점을 극복하기 위해 게임 회사는 게임 로그에 데이터 마이닝 기술을 적용하는 서버 단 탐지 방법을 적용하기 시작했다.

데이터 마이닝 방법은 높은 정확도의 탐지 규칙을 제공하고 미리 정의된 탐지 알고리즘을 사용하여 사용자와 시스템에 부작용 없는 게임 봇을 탐지할 수 있다. 서버 단에서의 이상 징후 탐지는 유저들이 온라인 게임을 플레이할 경우 플레이 로그들이 서버에 저장 되는데 이 로그의 분석을 통해서 이상 징후 발생 여부를 탐지한다.

〔표 2〕 게임 산업에서 사용되는 게임 봇 탐지 방법

범주	방법	예	특징
클라이언트 단 탐지	게임 서비스 제공사의 치팅 방지 시스템	- Blizzard 사의 World of Warcraft에 적용된 Warden system - NCsoft 사의 AION에 적용된 NC Guard - Tencent 사의 TenGuard - SNDA 사의 SNDC - NEXON 사의 Nexon Guard	- 장점: 게임 프로세스와 결합되어 동작하므로 봇 탐지가 용이하고, 게임 내부 로직과 결합하여 탐지와 차단 정책을 유연하게 적용할 수 있음 - 단점: 개발사의 개발 부담이 증가함
	보안 업체의 게임 보안 솔루션	- INCA Internet 사의 GameGuard - AhnLab 사의 Hackshield	- 단점: DRM이나 백신과 같은 다른 보안 프로그램과의 충돌이 발생함
	게임 내 디자인을 이용한 탐지	- 보이지 않는 NPC(non-player character)를 이용한 탐지: 사람은 볼 수 없는 NPC를 봇 프로그램은 감지하여 공격함 - 보이지 않는 아이템을 이용한 탐지: 사람은 볼 수 없는 아이템을 봇 프로그램은 감지하여 획득함	- 단점: 디자인이 드러나면 소용없게 되는 임시적 방법
	사용자 행동을 이용한 탐지	- Kount, iOvation	- 단점: 높은 오탐율(false positive rate)
네트워크 단 탐지	트래픽 감시: TTL(time to live) 값, RTT(round trip time) 값	- 현업에서 시행되지 않음	- 단점: 높은 오탐율, 낮은 가용성, 높은 분석 비용
	네트워크 프로토콜 변경: 키 변경 및 암호 알고리즘 변경	- NCsoft 사의 Lineage, Lineage2, AION	- 단점: 클라이언트 프로그램의 지속적인 업데이트와 네트워크 트래픽 비용이 요구됨, 실시간 암·복호화를 위해 많은 컴퓨팅 파워가 요구됨
서버 단 탐지	게임 내 로그 분석		- 장점: 높은 정확도, 게임 외 로그를 이용하여 높은 탐지율을 가짐
	게임 내 CAPTCHA 분석	- NCsoft 사의 AION	- 단점: 온라인 게임 사용자의 몰입도를 떨어뜨림, 낮은 가용성

[표 2] 게임 산업에서 사용되는 게임 봇 탐지 방법

표에서 보이듯 대부분 클라이언트 단 탐지의 많은 관심을 기울이게 된다. 네트워크 단은

그 특성상 만들기가 쉽지 않으며 설령 사용하더라도 그 특이한 렉 유발 등 증상이 보이기에 판별이 쉽고 서버단을 노리는 핵은 게임회사 최고의 보안도를 자랑하는 서버를 뚫어야 하며, 이것을 뚫어냈다면 사실상 게임회사의 데이터의 총자산 인만큼 소송도 각오해야 하기 때문이다. 그렇기에 상당수의 핵은 클라이언트 단에서 조작이 이루어진다.

3.2 변조 방법

3.2.1 패킷 변조

클라이언트-서버 모델의 온라인 게임에서 클라이언트는 대부분의 계산을 직접 처리하지 않고 서버에 요청만을 한다. 공격자 입장에서는 복잡한 보호 장치가 즐비한 클라이언트를 분석하기 전에 우선적으로 시도하는 것이 패킷 변조이다.

패킷 변조란 서버와의 통신에 주고받는 프로토콜을 분석하여 원하는 정보가 전송되게 하는 공격 방법이다. 이를 일차적으로 예방하기 위해서는 검증된 알고리즘으로 패킷을 암호화하고 주기적으로 프로토콜을 바꾸는 방법이 이용된다. 몹에게 히트를 한 방 먹이면 1이라는 패킷이 전달된다고 가정하고, 이 때 전송되는 이 1값이 포함된 패킷을 가로채 100이라고 바꾸면 백배의 공격력으로 바뀌어 전달되어 어떤 몹 이라도 한 번에 잡을 수 있게 된다.

여기서 패킷을 암호화하거나 서버에서 패킷 체크를 함으로써 네트워크상에서 값을 조작하여 전달하는 것이 불가능할 경우, 그냥 캡처한 값을 보내지 않고 보내되, 같은 값을 계속적으로 여러 번 보내는 작업을 한다면 한 방 먹였을 때 수 십방 먹인 것과 같은 효과가 발생되어 역시 같은 효과를 낼 수 있다. 이것이 곧 한방에 적을 물리칠 수 있는 한방 핵의 원리이다.

3.2.2 메모리 변조

공격자는 자신이 조작하고자 하는 변수가 저장된 메모리에 접근하여 원하는 수치로 조작을 하고, 이후 클라이언트가 정상적으로 실행되면서 조작된 데이터를 서버로 전송하게 된다. 이 때, 조작하고자 하는 변수가 저장된 메모리를 찾는 방법은 메모리 스캐닝과 리버싱 기법들이 주로 이용된다.

메모리 스캐닝은 현재 수치와 일치하는 값을 가진 메모리들을 지속적으로 추려내면서 메모리의 위치를 찾아가는 방식이고 Cheat Engine 등의 오픈소스 도구들로 인해 별도의 지식이 없어도 쉽게 시도할 수 있다.

리버싱은 보다 숙련된 공격자들이 이용하는 방식으로 바이너리 상태에서 역으로 코드의 흐름을 분석하고 원리를 알아낸 후, 코드 자체를 조작하거나 원하는 변수가 메모리에 저장되는 시점을 알아낼 수 있다. 더불어 후킹이나 Dll Injection을 이용해 소프트웨어 구성 요소 사이에 발생하는 함수 호출, 메시지 등을 바꾸거나 가로채는 방식도 자주 이용된다.

메모리 해킹 및 코드 변조는 핵심적인 변수에 대한 은닉, 소스코드 난독화, 패킹 등 전통적인 안티 리버싱 기술로 대응을 한다. 메모리 해킹의 경우 민감한 정보가 저장된 변수의 주소를 노출하지 않는 것이 핵심이며 부하가 적고 구현이 용이한 XOR 암호화를 통해 평문을 은닉하고 ASLR을 통해 메모리 주소를 임의적으로 만드는 방법을 고려할 수 있다. 또한 숙련된 공격자들은 바이너리 상태의 파일도 리버싱을 통해 손쉽게 분석할 수 있으므로 Themida와 같은 난독화 도구들을 이용해 핵심적인 코드를 숨기는 것이 중요하다.

3.3 게임핵 프로그램

3.3.1 Cheat 'O Matic

프로그램 내부의 수치를 찾아서 변경할 수 있게 해주는데 게임에서 체력치를 고정하거나 돈을 늘리는 등 이름대로 치트에 주로 쓰인다. 간단한 저용량 프로그램으로서 이용 방법도 매우 간단하다.

1.게임 내에서 내가 10골드를 가지고 있는데 이걸 바꾸고 싶다.
2.오매틱을 켜고 프로그램을 설정한 다음 10을 입력한다.
3.게임으로 돌아와서 골드를 조금씩 얻거나 줄여서 숫자를 변경한다.
4.오매틱에 변경한 값을 입력한다.
5.오매틱이 값을 찾아낼 때까지 여러 번 이 행동을 반복한다.
6.최종적으로 값을 찾아내면 원하는 값으로 변경하고 게임을 즐긴다.

10이라는 수치는 골드가 아니더라도 게임 내부에 많이 존재하기 때문에 정확히 이 숫자 중 골드에 해당하는 것을 찾기 위해 골드 값을 변경시켜가며 해당 수치를 찾는 것이다. 1997년에 만들어진 프로그램임에도 불구하고 원리 자체는 여전히 사용 가능하다. 단, 워낙 단순한 프로그램이다 보니 0~10 정도의 매우 흔한 숫자를 검색할 경우 검색 결과가 너무 많아 과부하가 걸려서 프로그램이 멈추기도 한다. 또 정확한 숫자를 입력해서 검색하는 방식이다 보니 체력 게이지처럼 숫자로 표시되지 않는 값은 찾을 수 없다.

뒤에 소수점이 있는데 게임에서 생략되어 나오는 경우나, 출력되는 값과 실제 저장되는 값이 다른 경우도 찾기 어렵다. 또 만약 한 수치를 같은 값으로 2개 이상 메모리에 저장하는 방식일 경우도 있는데, 해당 값을 1개만 찾을 때까지 계속 검색해야 하는 치트오매틱의 특성상 수정할 수 없게 된다.

3.3.2 Cheat Engine

가장 유명한 메모리 에디트 툴 및 헥스 에디터 프로그램이다. 주로 게임 관련 해킹이나 핵을 만드는 데에 사용되기에 게임 해킹의 필수품으로 여겨진다. 오픈소스이며 대부분의 핵들이 치트 엔진을 통해 얻은 정보로 제작된다고 해도 될 정도다.

강력한 헥스에디팅/메모리에디팅 툴로, 다른 프로그램에 비해 스캔 속도가 매우 빠른 편이다. 'cheat engine assembler'를 지원하는데, 이를 통해 코드 인젝션을 손쉽게 할 수 있다. 레지스터까지 변경할 수 있고 특정 주소에 무슨 opcode가 접근하거나 쓰고 있는지도 찾을 수 있는 등 디버깅 기능도 많이 포함하고 있다.

1~8 바이트, Float, Double, String, Binary 등 다양한 형식을 스캔할 수 있어 매우 유용하다. 또한 Lua 스크립트도 지원하고 5.8 버전부터는 DBVM(가상머신)까지 자체적으로 지원한다.

치트 엔진은 그 훌륭한 기능도 기능이지만, 아무래도 가장 큰 심각성은 소스가 오픈되어 있다는 것에 있다. 오픈소스로 인해 수백 종 이상의 게임 보안 솔루션 바이패스 버전이 등장했으며 게임 보안 솔루션의 패치 속도보다 더 빠른 업그레이드 속도를 보여주고 있다.

이 때문에 게임 보안 솔루션 개발업체에서는 이 치트 엔진 때문에 골머리를 앓고 있을 정도이다. 보안솔루션 개발자 몇 명이서 막고 있는데, 전세계 게임 해커들은 이를 우회하는 방법을 찾고 있기 때문이다. 특히 치트 엔진은 주로 로컬 메모리에 대한 의존도가 높은 게임에 많이 악용되고 있다.

3.4 핵에 대응하는 게임회사의 방안

3.4.1 전문 보안회사 기용

이런 핵을 전문으로 차단하는 보안 회사들이 존재한다. 이들이 모든 핵을 잡을 수 있는 건 아니지만 엄청난 개발비용과 연구를 한 것이 아닌 이상 금액 면에서도 성능 면에서도 뛰어나기에 이들의 보안 프로그램을 사용하는 경우가 많다.

대표적으로는 BattlEye, EasyAntiCheat, Denuvo Anti-Tamper 등이 있다.

3.4.2 모니터링

보안 솔루션 들이 존재한다고 핵이 사용되지 않는 것이 아니다. 그렇기에 자본에 여유가 되는 회사들은 모니터링 요원들을 배치하여 핵을 사용하는 유저들을 확인하며 유저들로 하여금 신고를 받아 신고 받은 핵 유저들을 주시하여 핵 유저가 맞는지 판별하고 맞을시 계정 정지, 삭제, 하드웨어 밴, 저 우선도 매칭 등의 조치를 취하여 핵 유저들에게 제제를 가한다.

3.4.3 소송

게임회사 최후의 방안으로 이미 당한 핵은 어쩔 수 없지만 법적 공방으로 넘어가 핵을 사용하는 것의 대한 해커들에게 경각심을 부각 시키는 방법이다. 다만 승소를 무조건 할 수 있는 것이 아니고 엄청난 비용과 시간이 들기에 대형 게임회사가 아니면 취하지 않는 방안이다. 실제로 나름 효과가 있었는지 Fortnite는 핵사용자의 일부를 본보기로 소송을 하려는 움직임을 보여주었고 그 결과 타 인기 FPS게임에 비해서 현저하게 핵의 적발과 신고가 적어졌다.

3.4.4 클라우드 게임 서비스

클라우드 게임은 직접 구축한 클라우드 컴퓨팅 서버에서 동작하는 게임을 정해진 게임들을 스마트폰 / PC / 콘솔 등 다양한 개인소유의 플랫폼에서 스트리밍을 통해 플레이하는 것이다. 클라우드 게임 서비스는 보안만을 위해 개발된 것은 아니나 보안면에서도 영향을 주는데 핵과 관련된 면에서는 모든 정보를 서버에서 처리하는 방식이기에 서버의 보안이 안전하다는 가정하에 대부분의 클라이언트를 기반으로 하는 메모리 핵 등을 사용하는 게 불가능해진다.

상당수의 핵이 클라이언트 기반 핵이 많기에 클라우드 게임 서비스의 범위가 넓어질수록 더더욱 핵으로부터 쾌적한 게임이 가능할 것이다.

4. 결론

게임은 꾸준히 성장하고 있으며 직접적이진 않아도 간접적으로 4차 산업혁명의 지원을 조금씩 받고 있기에 그 전망도 나쁘지 않다. 거기다 SARS-CoV-2(코로나 바이러스)의 영향으로 외출을 자제 하게 된 현 상황에서 사람들과 같이 즐길 수 있는 몇 없는 취미이기도 하다.

하지만 이런 같이 즐기기 위한 게임을 자신의 승부욕으로 인해 부정행위로 기만을 하는 핵 사용자들과 이런 사람들의 심리를 이용해 돈을 버는 핵 제작자들도 같이 성장하고 있다. 거기다 법원도 이런 핵은 게임사와 유저간의 문제로 생각하여 처벌을 내리지 않는 경우도 많다.

장르를 가리지 않고 핵이 있으며 핵이 주는 영향력도 다양하며 공격 방법마저도 다양하다. 자신만이 게임을 재밌게 즐기기 위한 트레이너 같은 형태의 핵이 있는가하면 일부러 PVP에 사용이 가능하게 만드는 핵들도 있다.

특히 치트 엔진은 오픈소스로서 상당수의 핵 제작의 기반이 되지만 막기도 힘든 게 사실이다. 하지만 그렇다고 게임회사도 보안회사도 핵에 당하기만 해서는 안 될 것이며 실제로 핵을 위한 전문 프로그램과 보안회사 설립, 모니터링과 클라우드 게임 서비스의 적극적인 협조하는 방식의 조치를 취하고 있다. 4차 산업혁명으로 인해 보안회사는 앞으로 더욱 성장할 것이며 향후 추가적인 연구와 조사로 핵에 탐지와 분별 방식도 성장해갈 것이다.

참고문헌

1) Newzoo, “2019,2020 Global games Market Report”
2) 유동영, 서동남, 김휘강, 최진영, “온라인게임 서비스 분야에 정보보호 사전진단 적용시 효과성에 관한 연구” 한국IT서비스학회지, 제10권, 제2호, pp.293~308, 2011
3) 온라인 슈팅게임의 자동조준 프로그램이 정보통신망법의 ‘악성프로그램’에 해당하는지 여부가 문제된 사건[대법원 2020. 10. 15. 선고 중요판결]
4) 안진경. (2020). 온라인 게임의 치팅 프로그램에 나타난 플레이어의 욕망 - 슈팅 장르를 중심으로. 한국게임학회 논문지, 20(4), 89-99.
5) 강아름. "온라인 게임 봇 탐지를 위한 사용자 행위 분석." 국내석사학위논문 高麗大學校 情報保護大學院, 2012. 서울
6) 곽병일, 김휘강 “온라인 게임에서의 이상 징후 탐지 기법 조사 및 분류” 1097~1114
7) 김정환. "상호 감시 기반의 온라인 게임 치팅 탐지 방법." 국내석사학위논문 고려대학교 정보보호대학원, 2016. 서울
8) Lee, Jin-Tae·Lim, Jong-In ‘MMORPG게임의 오토프로그램과 저작권’ 275-296
9) Ki Sung Lee, Huy Kang Kim, “Android Game Repackaging Detection Technique using Shortened Instruction Sequence”, Korea Game Society, Vol. 13, No.6, pp.85-94, 2013.
10) 김정환. "상호 감시 기반의 온라인 게임 치팅 탐지 방법." 국내석사학위논문 고려대학교 정보보호대학원, 2016. 서울