

불법사설서버 현황 및 대응방안

서은비*, 김지흥*, 강태운*, 유창석**, 김휘강*

요약

온라인 게임 산업은 다양한 경험을 제공할 수 있는 새로운 가치를 창출하며 지속적으로 성장해왔으며, 현재 상당한 규모의 시장을 형성하고 있다. 그러나 게임회사들이 개발단계 및 서비스 운영단계에서 기술적 보호조치를 충분히 하지 못하여 게임클라이언트가 리버스엔지니어링으로 분석당하거나, 취약한 통신설계로 인하여 네트워크 단에서의 패킷 구조가 분석당하거나, 게임회사 내부 또는 IDC로 해커가 침입하여 서버프로그램 바이너리 및 소스코드를 탈취당할 수 있다. 이러한 공격이 가능할 경우 불법 사설 서버가 만들어져 운영되어 온라인게임회사의 이미지에 타격을 주거나 영업상 손실을 유발할 수 있게 된다. 각 게임회사 및 정부에서는 불법 사설 서버를 탐지하고 차단하기 위해 많은 노력을 기울이고 있지만, 점차 사설 서버가 음성적으로 운영되어 차단이 어려우며, 특히 해외에서 운영되는 경우 특별한 대안이 없는 실정이다. 본 논문에서는 현재 게임 산업을 저해하는 불법 프로그램 및 불법 사설 서버의 운영 실태를 파악하고, 이에 대한 심각성을 논의하고자 한다.

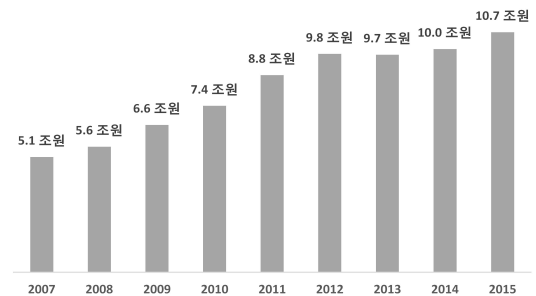
I. 서론

다양하고 극적인 재미를 경험할 수 있는 게임과 컴퓨터와의 결합은 기존에 없던 새로운 가치들을 창출하였으며, 이에 따라 게임 산업에 대한 국내외 활발한 발전이 이루어졌다. 한국 콘텐츠 진흥원에 따르면 전 세계적으로 게임은 약 1,234억 달러, 한화로는 약 130조원 규모의 시장을 형성하고 있으며, 국내 시장의 경우 2015년 기준 10조원의 규모로 전 세계에서 상당한 규모와 위치를 차지하고 있다. 그림 1과 같이, 국내 게임 시장은 2007년 5조원 수준에서 2015년 약 10조원으로까지 지속적인 성장세를 보이며 지난 10년간 빠르게 성장해왔다.

그러나 게임 시장의 성장과 함께 다양한 관련 범죄 행위도 증가하고 있다. 특히 게임 배포 및 핵심 정보의 저장지 온라인과 연계되어 진행됨에 따라, 익스플로잇(exploit), 치팅(cheating), 매크로(macro) 및 게임 봇(game bot), 어뷰징(abusing), 게임 서버 공격, 사설 서버(private server) 등 공격 형태가 다양화되며 급증하고 있다. 이에 대처하기 위해 각 게임 회사는 정보보안과 관련하여 수많은 노력을 하고 있지만, 급격히 증가하는 사용자 및 서비스 영역으로 인해 어려움을 겪고 있

는 상황이다. 또한 정부 차원의 대처도 불법 게임물에 대한 관련 자료 부족 등 실제적인 대응에 있어서 많은 어려움이 따른다. 특히 이러한 불법 사설 서버 및 불법 프로그램은 최근 기업형으로 진화하며 지속적으로 규모 및 매출액이 증가하고 있는 실정이다.

게임물 관리 위원회 내 불법 사설 서버와 관련된 인원은 2014년 1,526건 수준이었으나 2015년 2,956건으로 거의 2배 가까이 증가하였다. 이와 같은 불법 사설 서버가 제재를 당하지 않을 경우 정식 서버의 게임 유저는 굳이 유료로 정식 게임 서버를 이용할 동기를 상실하게 되며, 게임 붓과 같은 불법 프로그램을 제대로 탐지와 차단을 하지 않을 경우 게임 내 공정한 게임 플



(그림 1) 국내 게임산업규모 매출 추이

* 고려대학교 정보보호대학원 (dog722@korea.ac.kr, inside15@korea.ac.kr, ktw1332@korea.ac.kr, cenda@korea.ac.kr)

** 경희대학교 문화관광콘텐츠학과 (csyoo@khu.ac.kr)

레이가 이루어지지 않는다고 느끼게 되어 게임서비스를 이탈을 하거나 불법 사설 서버로 이동하는 현상이 발생할 수 있다. 그 결과, 게임 시장이 위축되며 온라인게임 회사에 손실을 주는 것은 물론, 해외 수출이 감소하여 국가 경제에 막대한 피해를 줄 수 있다.

이에 대처하기 위해 <게임산업진흥에 관한 법률>이 2016년 12월 통과되었으며, 이 법에는 게임물 관련사업자가 제공 또는 승인하지 아니한 게임물을 제작, 배급, 제공 또는 알선하는 행위 및 이와 같은 불법행위를 할 목적으로 컴퓨터프로그램이나 기기 또는 장치를 제작 또는 유통하는 행위를 금지하고 이를 위반한 자에 대해 5년 이하의 징역 또는 5천만원 이하의 벌금에 처할 수 있도록 할 수 있는 처벌 근거가 마련되었다.

그러나 불법 사설 서버 및 불법 프로그램의 현재 상황에 대한 객관적 지표 및 피해 규모의 연구가 부족한 실정이며, 이에 본 논문에서는 이러한 불법서버와 같은 불법게임물들의 운영 실태를 조사하려 한다.

조사 대상으로는 표 1과 같이 국내 대표 회사인 엔씨소프트, 넥슨 게임 내 불법 사설 서버를 조사하였으며, 모바일 게임 분석의 경우 불법 사설 서버가 존재하는 류 오리진, 클래시 오브 클랜을 대상으로 조사를 실시하였다. 또한 게임 장르별(스포츠 게임, 전략 시뮬레이션 등)로 불법 프로그램 조사를 수행하였다. 운영 실태 조사의 경우 구글 검색을 통한 사이트 별 노출 현황을 확인하였으며, 불법 사설 서버 접속기를 확보하여 접속기의 PE 정보를 추출하고, 이에 대한 유사도 비교를 통해 제작자 유추 방법을 분석하였다.

[표 1] 불법 사설 서버 조사 대상

게임 회사	조사 대상
엔씨소프트	리니지, 리니지2, 아이온, 블레인드앤소울
넥슨	바람의 나라, 메이플스토리
모바일 게임	클래시오브클랜, 류오리진

II. 불법 사설 서버

게임 시장을 위협하는 위협 요인으로는 대표적으로 불법 프로그램, 작업장, 불법 사설 서버, 악성 코드 등이 있다.

2.1. 불법 프로그램

불법 프로그램은 정상적 기술 운영을 조작하여 사용 허가 없이 프로그램을 운영하거나, 정상적인 이용자가 할 수 없는 행위를 하게 만드는 프로그램 등을 의미한다. 게임 붓은 게임 플레이어를 대신하여 사냥을 하거나 특정 아이템을 복사하는 등 불법적인 행위를 수행한다. 또한 게임 핵은 정상적인 게임의 메모리 변조 등을 통해 자신에게 유리하도록 게임 조작을 가능하게 한다. 이들은 게임 내 특정 활동을 무한히 반복할 수 있으므로, 다른 게임 플레이어에게 불쾌감을 줄 뿐만 아니라 궁극적으로 게임 산업을 위축시킬 수 있다.

2.2. 작업장

작업장은 주로 MMORPG와 같은 온라인 게임을 대상으로 운영되며, 엔씨소프트사의 대표 RPG 게임인 리니지를 시작으로 게임 아이템의 현금화와 함께 발전되어 왔다. 작업장에서는 수십 및 수백 대의 컴퓨터를 통해 오토 프로그램 등 불법 프로그램을 수행하여 대량의 게임 머니, 게임 아이템 등을 수집하는 등 부당 이득을 취하고 있다. 2015년 8월 playforum의 기사에 따르면, 작업장은 월 평균 1,000만원부터 1억원까지의 수익을 내는 것으로 확인되고 있다. 이처럼 작업장의 규모가 커지고 활발해짐에 따라 정상적인 게임 이용자의 이탈 및 게임사의 수익 감소가 발생할 수 있다.

2.3. 불법 사설 서버

불법 사설 서버는 게임에 대한 저작권 및 권리를 소유하지 않은 운영자가 게임 업체의 동의 없이 게임 서버를 제작 및 운영하는 행위 또는 서버를 말하며, Free Server, Mirror Server, Private Server의 명칭으로도 불린다. 정상적인 게임과는 달리 쉬운 레벨 업 및 희귀 아이템을 얻을 수 있으며, 사행성 콘텐츠를 포함하기도 한다. 대규모의 특정 불법 사설 서버로 인한 게임 운영사의 피해액은 연간 약 1,500억 원대로 추정되며, 이는 게임 시장의 매출을 감소시키기 때문에 정부 차원의 단속 강화가 이루어져야 한다.

2.4. 악성 코드

악성코드는 사용자의 컴퓨터에 해를 끼칠 수 있는 모

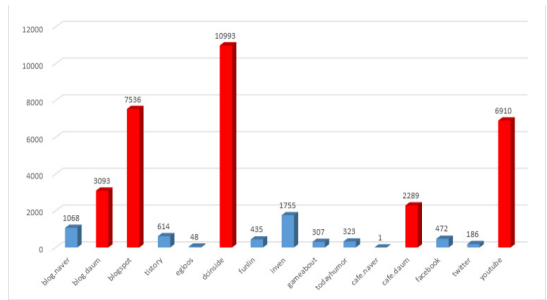
든 코드를 의미하며, 최근 네트워크의 발달로 감염 방법과 증상이 다양해지고 있다. 악성코드의 종류로는 워, 트로이 목마, 스파이웨어, 랜섬웨어 등이 있다. 불법 사설 서버의 설치 및 유해 사이트 접속으로 인해 PC내 악성코드가 침투될 수 있으며, 불법 사설 서버 실행기를 빙자 하여 웹 하드에 악성코드를 삽입 후 개인 정보를 탈취하는 사례가 증가하고 있다. 따라서 저작권 침해 뿐만이 아닌 사용자의 개인 정보 보호를 위해 불법 사설 서버의 근절이 강화되어야 한다.

III. 불법 사설 서버

3.1. 불법 사설 서버 운영 현황

그림 2에서 볼 수 있듯이, 조사 결과 확인된 불법 사설 서버의 수는 285개이며 그 중 리니지 게임이 242개로 가장 많은 불법 사설 서버를 보유한 것으로 확인되었다. 발견된 불법 사설 서버 285개 중, 194개(약 68%)의 사이트가 현재 운영 중에 있었으며, 그림 3과 같이 리니지 게임 수집기의 수가 146개로 가장 많이 제작된 것을 확인할 수 있다.

불법 사설 서버 관련 운영 페이지는 구글 검색 내 검색 결과가 약 733,000개가 있을 만큼 포털 내 불법 사설 서버의 차단이 미비하며 검색 및 조회가 쉽게 가능하다. 그림 4는 구글 검색 결과 확인된 사이트 별 불법 사설 서버 관련 게시물 수를 보여준다. 국내 가장 큰 규모의 커뮤니티 사이트인 디지인사이트 내 게시물들은



(그림 4) 사이트 별 불법 사설 관련 게시물 수

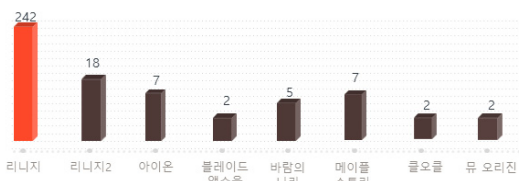
불법 사설 관련 홍보 내용을 담고 있다. 또한 구글에서 서비스하는 블로그스팟은 회원가입 시 개인정보를 요구하지 않으므로, 도박 등 불법 콘텐츠 및 불법 사설 서버의 운영 페이지로 사용되고 있다. 불법 콘텐츠 적발 시 페이지 삭제 및 계정 차단이 이루어지지만, 운영자는 여러 계정을 보유하여 사이트 주소의 넘버링을 통해 비슷한 사이트 주소로 쉽게 이전할 수 있으므로, 완전한 차단이 어려운 실정이다.

3.2. 불법 사설 서버 운영 방식

불법 사설 서버의 운영자는 웹 호스팅 업체나 포털 사이트의 카페를 이용하여 불법 사설 서버의 서비스를 제공하는 웹페이지를 제작한다. 대다수의 운영자들은 별도의 서버 호스팅을 받거나, IDC의 서버를 구입하여 서버 프로그램을 실행한다. 그 후, 해당 서버에 접속할 수 있도록 변조된 클라이언트 및 서버 파일을 웹페이지를 통해 배포하게 된다.

불법 사설 서버의 운영자는 전문적 기술을 가진 접속기 개발자와 서버 개발자, 보안 전문가 등의 조직적인 형태로 운영된다. 또한 사설 토토 등 불법 광고를 통해 수익을 얻기도 한다. 또한 경우에 따라서는 경쟁관계에 있는 또 다른 불법 사설 서비스에 DDoS 등 해킹을 시도하여 경쟁관계에 있는 불법 사설 서버의 운영을 방해하기도 한다.

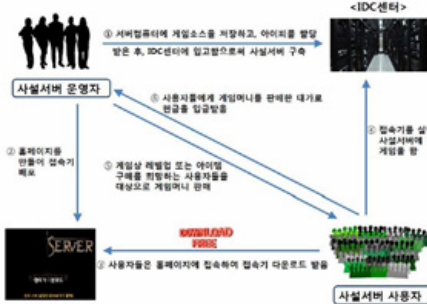
불법 사설 서버 프로그램에 접속하기 위한 절차는 그림 5와 같이 매우 간단하다. 운영자는 홈페이지를 통해 접속기를 배포하며, 사용자는 해당 홈페이지에서 다운 받은 접속기를 실행하여 불법 사설 서버에 접속할 수 있다. 불법 사설 서버의 운영자는 게임 유저로부터 문화 상품권이나 패키지(아이템 판매)를 통한 금전적인 거래를 통해 서버 호스팅 비와 운영비를 얻는다. 또한 사용



(그림 2) 확인된 불법 사설 서버 수



(그림 3) 다운로드 가능한 불법 사설 서버 접속기 수



[그림 5] 불법 사설 운영 방법(출처 : 플레이포럼㈜)

자와의 소통을 위해 SNS, 게시판 등 다양한 방법을 이용하기도 한다.

앞서 언급한 바와 같이 블로그 및 커뮤니티를 통해 불법 사설 서버의 홍보가 이루어지고 있지만, 전문적으로 불법 사이트를 홍보할 수 있는 사이트도 존재한다. 대표 홍보 사이트인 ‘팍리니지’의 홍보비용은 24시간 기준 50~200만원에 달하며, 이를 통해 많은 게임 유저들이 불법 사설 서버를 이용하는 것을 알 수 있다.

3.3. 불법 사설 서버 제작 과정

온라인 게임은 유저가 어떠한 액션을 수행 시 정해진 규칙에 의해 서버로 패킷을 전송하며, 서버는 규칙을 해석하고 결과를 다시 패킷으로 응답하게 된다. 불법 사설 서버의 제작자는 정식 게임 서버와 클라이언트의 통신 내용을 스니핑하여 정보를 수집한 후, 암호화된 수집 정보를 해석하기 위해 리버스 엔지니어링(Reverse Engineering)을 수행한다. 이는 게임 소스 코드 복원 및 어셈블리어 조작을 통한 게임 수정을 가능하게 한다. 리버스 엔지니어링은 기술적 난이도가 높으며 분석 결과에 따라 불법 사설 서버의 성능 차이가 발생하므로, 미흡한 불법 사설 서버는 잦은 시스템 장애를 일으키기도 한다.

정상적인 게임 클라이언트는 IP주소, 포트 번호 등 서버의 중요한 정보를 포함하고 있다. 불법 사설 서버 개발자들은 임의로 제작한 사설 서버로 접속하도록 정상 게임의 클라이언트 접속 정보를 변조한다. 최근 온라인 게임은 이러한 클라이언트 변조를 막기 위해 암호화를 하거나 중요 정보를 클라이언트에 저장하지 않고 서버로 전송하고 있다.

3.4. 불법 사설 서버 접속기 분석

불법 사설 서버의 운영자는 접속기는 다르지만 유사한 여러 개의 불법 사설 서버를 운영할 수 있다. 본문에서는 불법 사설 서버의 제작자 추적을 목표로 접속기의 유사도 분석을 수행하였다. 먼저 수집한 불법 사설 서버 접속기의 PE 분석을 통해 파일 해시값, DLL 라이브러리 사용, 파일 사이즈, 패커 정보, 코드 섹션 정보, API 정보, 파일 내 URL등을 추출하였다.

해시값은 파일의 고유 값이기 때문에 두 파일의 해시값이 같다는 것은 제작자 및 실행파일이 동일함을 의미한다. 그림 6은 해시 값이 동일한 리니지의 불법 사설 접속기를 보여주며, 이와 같이 운영자는 서버 명만을 변경하여 동시에 여러 서버를 운영하게 된다.

그림 7과 같이, 접속기 내부의 URL 정보 분석 결과, 특정 사이트 및 블로그 주소를 확인할 수 있었다. 이는 사설 서버 운영자나 개발자의 개인 정보가 포함되어 있을 가능성이 높으며, 이를 통해 동일한 개발자가 해당 서버를 제작했음을 추정할 수 있다.

game	server	sha256
리니지	동일동장비포박서버	2dd069a725c2965008feb0490c4fb1251642b50e3e64489fe41a6b5c72cee612
리니지	신화서버	2dd069a725c2965008feb0490c4fb1251642b50e3e64489fe41a6b5c72cee612

[그림 6] 해시값이 동일한 불법 사설 서버 접속기

game	server	sha256
리니지	동일동장비포박서버	2dd069a725c2965008feb0490c4fb1251642b50e3e64489fe41a6b5c72cee612
리니지	신화서버	2dd069a725c2965008feb0490c4fb1251642b50e3e64489fe41a6b5c72cee612

[그림 7] PE 분석 URL 정보

3.5. 불법 사설 서버 사행성 콘텐츠 운영 실태

2004년 6월 출시된 엔씨소프트사 리니지 게임의 미니 게임인 ‘리틀 버그베어 경주’는 가상 화폐인 ‘아테나’를 걸고 경주를 하는 콘텐츠로 특정 연령들만 이용할 수 있도록 제한된 콘텐츠이다. 그러나 불법 사설 서버에서는 버그 베어 경주 서비스가 불법 사설 서버에 접속한 모든 연령층들이 제한 없이 이용할 수 있도록 되어 있어 이용자 보호 측면에서도 문제를 야기할 수 있다.

아이템 중개 사이트에서는 불법 사설 서버 내 거래가 금지되어 있지만, 각 서버의 은어를 통해 하루 80~120 페이지에 걸쳐 불법 거래 내용이 등록되고 있다. 리니지

종류	등급	물품명	단위금액	거래금액	등록시간
아이템	[110001]	갈순	-	57,000원	11-20
아이템	[11091]	타니치	-	12,000원	15-16
아이템	[11091]	타니치	-	50,000원	15-30
아이템	[11091-001]	쿠루레노	1억당 5,000원	최소 5,000원	11-20
아이템	[11091-001]	쿠루레노	1억당 5,000원	최소 5,000원	11-20
아이템	[11091-001]	쿠루레노	-	8,000,000원	11-20
아이템	[021-9901]	배리버나	1만당 10,000원	최소 21,000원	15-11
아이템	[021-9901]	배리버나	1만당 11,000원	최소 22,000원	15-25
아이템	[021-9901]	배리버나	1만당 11,000원	최소 22,000원	14-21
아이템	[02-990]	배리버나	1만 11,000원	최소 22,400원	16-45
아이템	[11-999]	배리버나	1만 13,000원	최소 13,000원	16-41
아이템	[01]	배리버나	-	8,000,000원	11-20

(그림 8) 아이템 매니아 불법 사설서버 거래 목록

게임의 아데나는 그림 8과 같이 아이템 중개 사이트를 통해 현금화가 가능하다. 한 매체에 따르면 불법 사설 서버 및 사행성 콘텐츠 운영으로 인해 2010년 8월부터 약 5년간 약 120억원 규모의 게임 머니가 거래된 것을 확인할 수 있었다.

3.6. 불법 사설 서버 사용이 청소년에 끼치는 영향

사행성 콘텐츠를 포함한 불법 사설 서버는 게임 산업의 성장을 저해할 뿐만 아니라 불법 행동으로 인한 사회적 비용을 증가시키기도 한다. 그 중 가장 대표적인 사례는 청소년에게 끼치는 영향이다.

『게임산업진흥에 관한 법률』 제16조는 청소년을 보호하기 위해 청소년 유해성 확인 및 게임물 등급 분류를 시행하고 있다. 불법 사설 서버가 존재하는 게임은 폭력적이고 잔인한 콘텐츠로 인해 대부분 청소년이용불가 등급을 갖고 있다. 그러나 불법 사설 서버는 본인 인증 절차가 없으며, 이로 인해 청소년들은 게임의 폭력적 요소, 범죄 및 약물 내용 등을 포함한 청소년 이용 불가 게임에 무분별하게 노출되고 있다.

청소년 일탈 행동 이론인 “사회학습이론”에 따르면, 법을 어기는 잦은 경험은 궁극적으로 청소년 비행 및 범죄 행위까지 이어질 수 있다. [1] 또한 온라인 게임 내에서 각 구성원들이 서로의 행위를 보고 배우며 답습하는 것과 같이, [2] 불법 사설 서버 및 프로그램의 사용은 청소년에게 있어 전염성을 가진다. 불법 사설 서버의 사용은 청소년에게 불법 다운로드와 같은 행위보다 더 심각한 범죄 행위를 유발할 수 있으므로 이에 대한 경각성을 높여야 한다.

IV. 불법 프로그램

4.1. 불법 프로그램 종류

불법 프로그램은 게임의 종류에 따라 다양하며, 자동 플레이를 지원하는 오토 프로그램, 게임 내 능력치를 극대화할 수 있는 핵 프로그램 등으로 분류된다. 표 2는 대표적인 게임 장르의 불법 프로그램을 보여준다.

MMORPG의 대표 불법 프로그램은 오토 프로그램이다. 오토 프로그램은 매크로 프로그램 또는 자동 프로그램이라 불리며, 채집, 사냥 등의 반복적 행위를 자동으로 가능하게 해주는 프로그램을 의미한다. 에컨대 리니지에서는 사냥터의 위치 및 사냥 방법을 선택하여 자동 플레이를 수행 할 수 있다. FPS의 경우 대표적으로 오토 에임, 모드 윌렉 등의 프로그램이 사용되고 있다. 오토 에임 프로그램은 마우스를 움직이지도 않아도 총구가 상대 캐릭터를 향하게 하는 기능을 제공한다. 모드 윌렉은 벽 뒤의 적군 캐릭터 위치를 표시하는 프로그램으로, 총알이 벽을 통과해 적군을 사살하도록 ‘관통’ 기능을 제공한다. RTS에서는 지도에서 보이지 않는 부분

(표 2) 게임 장르에 따른 불법 프로그램 종류

게임 종류	프로그램 종류
MMORPG	스피드 핵, 다중 클라이언트 핵, 오토 프로그램, 버그 핵, 순간이동 핵, 투명 핵,
FPS	모드 윌렉, 바디샷, 스피드 핵, 오토에임, norecoll, 오토샷, 락 에임, almhltbox,
RTS	맵핵, 강퇴핵, 상태핵, 네임핵, 멀티캐릭터
SPORTS	복사 핵, 스피드 핵, 오토 장사 프로그램



(그림 9) 스타크래프트 맵 핵 실행 화면

의 시야를 보이게 해주는 맵핵이 성행하고 있다. 그림 9는 핵감지기인 wDetector가 실행됨에도 불구하고 불법 프로그램인 맵핵이 실행되는 것을 보여준다. 마지막으로 SPORTS에서는 게임 머니를 복사하는 복사 핵 등이 사용되고 있으며, 사용자는 이를 통해 손쉽게 게임 머니를 벌 수 있다.

4.2. 불법 프로그램 거래 방식 및 비용

불법 프로그램은 블로그나 카페 등 거래 사이트 또는 개인 연락처를 통해 판매된다. 불법 거래 사이트를 이용한 거래 방식의 경우, 그림 10과 같이 구매자들이 운영자에게 돈을 입금한 후 운영자로부터 받은 계정으로 판매 사이트에 접속하여 프로그램을 다운받는다. 그밖에 유튜브 등의 동영상 사이트에 불법 프로그램 사용법 및 실행 화면을 홍보한 후, 개인 SNS등의 연락처를 통해 프로그램을 판매하기도 한다.

불법 프로그램은 사용 기간에 따라 가격을 다르게 책정하여 판매되며, 구입하는 프로그램의 수가 증가할수록 월 별 지불 가격이 낮아진다. 또한 문화 상품권

또는 특정 거래 사이트를 통해 구입 시 가격이 추가될 수 있다. 표 3은 RPG 오토 프로그램 판매 사이트인 ‘오토싸다’의 대표 불법 프로그램의 거래 비용을 정리한 표이다.



(그림 10) 불법 프로그램 판매 사이트

(표 3) 대표 RPG 게임의 불법 프로그램 거래 비용

프로그램 종류	가격(/월)	비고
리니지 패신 프로그램	20,000원	27,000원(10개 이상 시) 25,000원(30개 이상 시) 23,000원(50개 이상 시)
리니지2 애플 프로그램	10,000원	9,500원(10개 이상 시)
아이온 환복 프로그램	20,000원	12,000원(10개 이상 시) 20개 이상은 메신저 문의

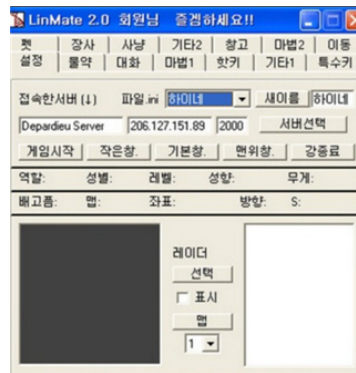
4.3. 불법 프로그램 제작 방법

불법 프로그램 제작은 크게 이미지 인식 기반, 메모리 기반, 패킷 기반, 하드웨어 기반 등으로 구분된다.

이미지 인식 기반은 이미지에 대한 정보를 프로그램에 저장하여 이미지 변화에 따른 행동을 정의하는 방법으로, 제작하기 쉽다는 장점이 있다. 모바일 게임에서는 오토핫키라는 오픈 소스 소프트웨어를 사용하여 매크로를 제작한다. 오토핫키는 사용자가 매크로 기능을 쉽게 제작할 수 있도록 도와주는 소프트웨어로, 전공자가 아니더라도 쉽게 제작이 가능하다. 그러나 이러한 방법은 고도화에 한계가 있고, CAPTCHA, 데이터 마이닝 등의 보안 기술이 적용된 게임에는 사용하기 어렵다는 단점이 있다.

메모리 기반 제작 방법은 이미지 인식 기반 제작 방법과 비교하여 보다 강력한 기능을 만들 수 있다. 모든 프로그램은 메모리 공간에 적재된 후 작동한다. 게임 프로그램 또한 특정 메모리 공간에 올라가며, 현재 실행 중인 데이터는 메모리에 담겨져 있기 때문에 해당 메모리 값을 분석하여 오토 프로그램을 제작할 수 있다. 이때 현재 캐릭터의 체력 정보에 해당하는 메모리의 데이터 위치만을 모니터링하여 제작하게 된다. 그러나 많은 양의 데이터 위치를 탐색해야 하며, 많은 시간과 높은 분석 실력 등이 요구된다.

패킷 기반의 제작 방법은 네트워크상의 패킷을 송수신 하는 온라인 게임 특성을 이용한다. 예컨대 패킷 수신 시 자신의 게임 정보를 전달하고, 수신 시 서버 정보 또는 주변의 다른 유저 정보를 받아 게임 콘텐츠를 조작한다. 이는 패킷을 임의로 제작할 수 있기 때문에 보다 강력한 오토 프로그램을 만들 수 있다. 그림 11은 패



(그림 11) 패킷 기반 오토 프로그램

킷 기반으로 제작된 오토 프로그램의 예로, 클라이언트를 실행하지 않아도 캐릭터의 정보 및 실제 게임 플레이를 할 수 있는 것을 볼 수 있다.

V. 피해 사례

5.1. 불법 사설 서버 폐쇄 사례

2016년 게임물관리위원회와 부산지방경찰청이 함께 공모하여 약 30억원 규모의 리니지 불법 사설 서버 운영자를 검거하였다. 해당 불법 사설 서버의 운영자는 ‘기르타스 서버’를 운영하였으며, 4년 간 회원 4,700여 명에게 총 28억원 상당의 부당 이득을 취하였다. 검거된 운영자는 중국 불법 사설 서버 광고 업체 등을 통해 아이템, 게임 머니 등을 판매하고 사행성 경마 게임을 운영하였다. 게임물관리위원회와 부산지방 경찰청은 지속적인 협업을 통해 사행성 콘텐츠 및 불법 사설 서버 근절을 목표로 지속적인 단속 활동을 펼치고 있다.

또한 2006년, 엔씨소프트와 미국연방수사국(FBI)이 함께 공조하여 북미 최대 리니지 서버를 검거하였다. 엔씨소프트의 북미 사업부는 ‘L2 Extreme’이라는 대형 프리서버를 폐쇄시키고, 해당 운영자를 검거하는 데에 성공하였다. 이 서버는 평균 5만 명의 유저가 접속하였던 서버로, 등록 유저 중 50만 명이 월정액 유저로 지속적으로 활동 해왔던 것으로 알려져 있다. 그림 12는 FBI에 의해 차단된 북미 사설 서버 홈페이지의 화면이다.



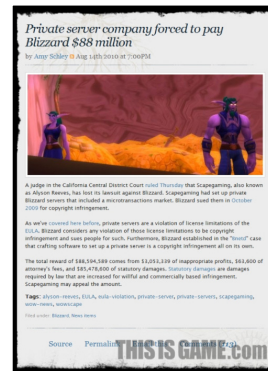
(그림 12) FBI에 의해 차단된 북미 사설 서버 홈페이지 화면

5.2. 불법 사설 서버 소송 및 판례 사례

스케이프게이밍은 ‘엘리슨 리브스’라는 월드 오브 워크래프트(WoW)의 불법 사설 서버를 운영하는 회사이

다. 해당 운영자인 스케이프게이밍은 불법 사설 서버 내 부분 유료화 모델을 적용하고, 유저와의 현금 거래를 통해 부당 이익을 취하였다. 블리자드 엔터테인먼트는 저작권 침해로 스케이프 게이밍을 고소하였으며, 해당 불법 사설 서버의 수익금인 305만달러(약 35 억원)과 법적 손해 배상금 8,500만 달러(약 1,020억원), 변호사 비용 6만 3,600달러(약 7,500만원)등을 포함한 약 8,859만 달러(약 1,020억원)을 배상하라는 판결이 내려졌다. 그림 13은 WoW 북미 사이트에 올라온 공지문이다.

반면 온라인 게임인 ‘뮤’ 서버를 개조한 국내 판례 사례에서는 무죄로 판결된 사례가 존재한다. 해당 운영자는 온라인 게임 ‘뮤’의 정식 배포 프로그램을 임의로 개조하여 불법 사설 서버를 운영한 것으로 『게임산업진흥에관한법률』 제32조 제1항 제8호가 금지하고 있는 “게임물의 정상적 운영 방해할 목적으로 게임물 관련 사업자가 승인하지 아니한 컴퓨터 프로그램을 배포하는 행위”에 위반하였다. 그러나 피고인은 배포 사실은 인정되지만, 게임 내용 자체에 부정적인 영향을 줄 목적으로 배포하였다고 단정하기 어려워 무죄 판결을 받았다.



(그림 13) WoW 북미 홈페이지 공지 사항

VI. 결 론

불법 사설 서버의 근절을 위해서는 검찰, 저작권 협회 등 기관과의 적극적인 협력이 필요하다. 또한 주요 홍보 수단인 블로그, 카페, 페이스북, 유튜브 등에서 불법 사설 서버에 대한 검색 결과에 노출되지 않도록, 홍보 수단의 제재 방안 또한 마련되어야 한다. 불법 사설 서버는 해킹 및 내부자에 의한 소스코드 유출로 인해서도 구축이 가능하다. 따라서 해킹 및 정보 유출 예방

을 위해, 정품 개발 툴, 소프트웨어 업데이트, 망 분리 시스템 구축, DLP 솔루션 등을 통한 내부 시스템 보안 강화를 할 필요가 있다.

온라인게임 서비스는 다년간 우리나라의 효자 수출 상품, 서비스로 자리잡고 있는데, 불법 사설 서버에 대한 차단과 예방활동을 하여 서비스 경쟁력을 다시 재고할 필요가 있다. 요컨대, 게임 산업의 기술적 성장과 경제적 성장을 위해 정부 및 관련 기관들의 적극적인 규제 완화 및 협조가 요구된다. 또한 불법 사설 서버 및 프로그램을 예방할 수 있도록 불법 사설 서버 제작자 및 운영자에 대한 강력한 처벌 규정규제 또한 필요할 것으로 판단된다.

참 고 문 헌

- [1] 이성식, “청소년의 온라인 저작물 불법다운로드 행위에 있어 낮은 자기통제력과 사회학습요인들의 영향 및 상호작용효과”, 청소년학연구 제18권 제10호, 2011
- [2] Ah Reum Kang, Hana Kim, Jiyoung Woo, Juyong Park, Huy Kang Kim, “Altruism in games: Helping others help themselves”, Network and Systems Support for Games (NetGames), 2014
- [3] 한국콘텐츠진흥원 (2016) “2016년 콘텐츠산업 전망,” 한국콘텐츠진흥원
- [4] 임영택 (2014) “정부, 연간 1633억원 피해 ‘불법 게임사설서버’ 강력 단속,” 매일경제(<http://game.mk.co.kr>)
- [5] 황태영 (2014) “[단독]리니지, 작업장 6개월 수익이 무려 5억원 ‘충격’,” 플레이 포럼(<http://playforum.net>)
- [6] 임광빈 (2015) “‘리니지’ 불법서버 운영...120억대 사행성 게임까지,” 연합뉴스TV
- [7] 이재진 (2006) “엔씨와 FBI, 복미 최대 리니지II 프리서버 폐쇄,” 디스이즈게임(<http://www.thisisgame.com>)
- [8] 플레이포럼 (2015) “엔씨소프트, 정부와 공조로 불법사설서버에 철퇴,” 플레이포럼(<http://lineage.playforum.net>)
- [9] 게임물관리위원회 “불법게임물 신고 안내,” (<http://www.grac.or.kr>)

www.grac.or.kr

<저자 소개>



서 은 비 (Eunbi Seo)

2016년 8월 : 숙명여자대학교 IT공학과 학사

2016년 8월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정
관심분야 : 데이터마이닝, 자동차 보안, AI



김 지 홍 (Ji Hong Kim)

2011년 8월 : 숭실대학교 수학과 학사

2014년 2월 : 고려대학교 정보보호대학원 정보보호학과 석사

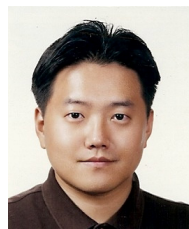
2016년 9월~현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정
관심분야 : 시스템 보안, 네트워크 보안, 디지털포렌식



강 태 운 (Tae Un Kang)

2016년 8월 : 충북대학교 컴퓨터공학과 학사

2016년 9월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정
관심분야 : 시스템 보안, 웹 보안, AI



유 창 석 (Changsok Yoo)

정회원

1999년 2월 : 서울대학교 자원공학과 졸업

2001년 2월 : 서울대학교 지구환경시스템공학부 (공학석사)

2011년 8월 : 서울대학교 지구환경시스템공학부 (공학박사)

2006년 7월~2012년 6월 : 엔씨소프트 과장

2013년 3월~현재 : 경희대학교 문화관광콘텐츠학과 조교수
관심분야 : 경제학, 게임보안, 사용자 행동



김 휘 강 (Huy Kang Kim)

종신회원

1998년 2월 : KAIST 산업경영학과
학사

2000년 2월 : KAIST 산업공학과 석사

2009년 2월 : KAIST 산업및시스템
공학과 박사

2004년 5월~2010년 2월 : 엔씨소

프트 정보보안실장, Technical Director

2010년 3월~2015년 2월 : 고려대학교 정보보호대학원 조
교수

2015년 3월~현재 : 고려대학교 정보보호대학원 부교수

관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌직