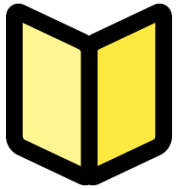
‘총칼 없는 전쟁’
모바일 게임 내의
보안 위협 요소

곽병완(Kwak Byung Wan)
byungwan@kakao.com

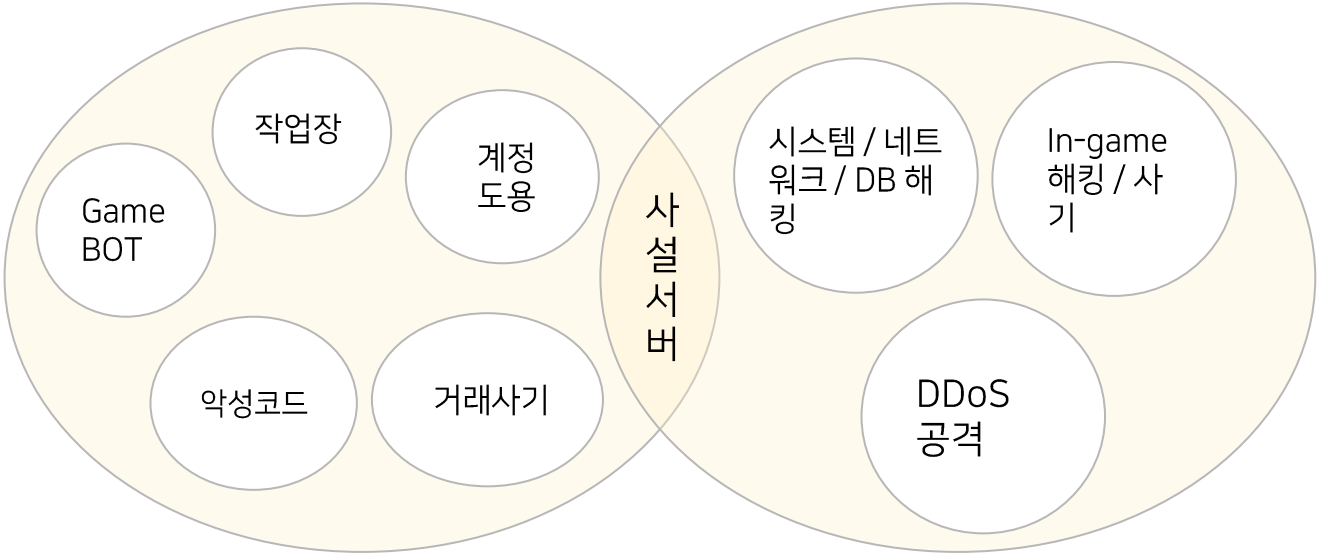


Contents

나날이 증가하는 게임 시장

1. COVID-19 이후 국내 게임 시장 규모 확대
    - 2020년 게임 시장 규모: 약 17조 (모바일: 9조)
    - 19년 대비 9.2% 상승 (출처: 2020 대한민국 게임백서)
2. BM 고도화로 인한 유료 거래량 증가
3. 돈의 흐름이 증가하여 범죄 발생률 또한 증가
    - 게임 계정 및 아이템 거래 사기 사건 매년 증가
    - 모바일 게임 보안 서비스 상담 급증 (출처: SK 인포섹 공식 블로그)

보안 위협의 종류


작업장
Game BOT
계정 도용
악성코드
거래사기
사설서버
시스템 / 네트워크 / DB 해킹
In-game 해킹 / 사기
DDoS 공격
외부적 위협 요소
내부 시스템 피해 요소

외부적 위험요소

1. 게임 봇(Game Bot) & 핵
    - 사람을 대신해서 자동으로 플레이를 해주는 프로그램
2. 작업장
    - PC 기반 작업장 -> 모바일 기반 작업장으로 진화
    - 대가를 받고 전문적으로 육성을 하는 것은 불법
3. 악성 코드
    - PC용 앱 플레이어 내 악성코드를 심어 고객 정보 및 결제 정보 탈취
    - PC용 앱 플레이어 악용한 공급망 공격 발견... 게임 업계 노린 표적 공격 추정 (출처 : 보안뉴스)
4. 계정 도용
5. 거래 사기

내부 시스템 피해 요소 사례

1. 시스템 해킹
    - 2011년 PSN 해킹 사건 : 총 1억 명의 개인정보 유출
2. DDoS 공격
    - **DDoS**, Distributed Denial of Service – 분산 서비스 거부
    - 2018년 유비소프트, 스퀘어에닉스 DDos 공격으로 인한 시스템 마비 발생
3. 사설 서버
    - 개발사의 동의 없이 게임을 복제하여 개인이 운영하는 서버에서 별도로 운영하는 행위
    - '리니지' 불법 서버 운영한 일당 검거 "19억 수익 올려 " (출처 : 아시아경제)

보안 위협의 영향

1. 정상적으로 플레이 하는 유저들에게 상대적 박탈감 발생
2. 게임 내 밸런스 붕괴로 유저들의 불만, 이탈률 증가
3. 유저 감소로 인한 수익 저하로 게임 서비스 지원 축소 및 조기 종료
4. 해킹을 통해 유저들의 개인정보 유출 및 금전적인 손실이 발생 우려
5. 장기적인 측면에서, 회사의 평판 및 신뢰도 하락

불법 프로그램 사용 예시 1

"쿠키런 킹덤 - 자동 매크로"

그림1) 쿠키런 : 킹덤 메인화면

다운로드 : 쿠키런킹덤 매크로 v1.13
녹스 앱플레이어 7.0.0.9 버전 32bit 가능
메뉴얼

녹스 버전 7.0.0.9 버전에서 작동 가능합니다.

녹스 해상도 800 * 600 에 240 DPI입니다

감사합니다.

그림2) 매크로 사용방법 안내 영상

- 아이템 자동 생산 및 클릭 매크로 사용
- 풍요의 분수, 곰젤리 열기구 등의 아이템 획득을 매크로를 사용하여 주기적으로 자동 획득

불법 프로그램 사용 예시 2

“메모리 변조를 통한 해킹”

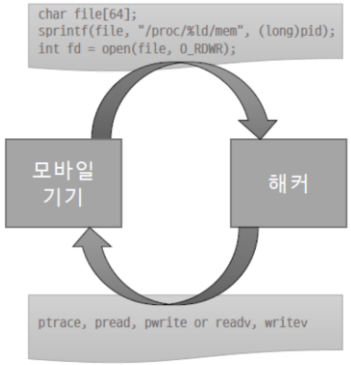


그림3) 시스템API를 이용한 메모리 변조

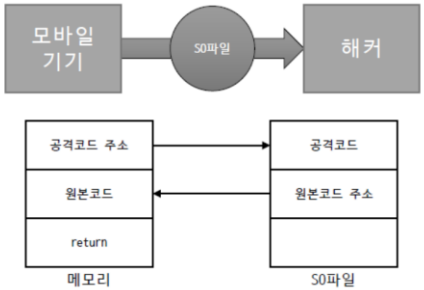


그림4) 후킹을 이용한 메모리 변조

- 메모리 변조를 통해 게임 프로세스 메모리 조작
- 게임 내 데이터(재화, 체력, 공격력 등)을 변조하거나 허용되지 않는 방법으로 게임 플레이를 진행

불법 프로그램 사용으로 인한 결과

해커 그룹, NoxPlayer 안드로이드 에뮬레이터에 악성코드 삽입해

국내외 보안동향 · by 알약4 · 2021. 2. 2. 09:00

♡ 2 💬 0

(출처 : EST security 알약 블로그)

중국발 앱플레이어의 문제점이 무엇이냐하면

보안(ADB)에 취약할 뿐더러, 한창 가상화폐가 유행할 시절 사용자 몰래 채굴프로그램을 실행하였다는 점 입니다.

심지어 몇몇 프로그램들은 백도어에 악성코드까지 심어져 논란이 되었던 적이 있습니다.

대부분의 앱플레이어들이 보안에 취약한 안드로이드 구버전을 고집하는 것도 이러한 이유가 있어서가 아닐까 싶습니다.

이런 문제점때문에 최근 몇몇 게임사들은 스스로가 개발한 앱플레이어나,

pc에서 모바일 구동가능하도록 별도의 프로그램을 제작하기도 합니다.

(출처 : 넥슨 카운터 사이드 유저 게시판)

보안 위협 대응 방안 - 1

1. 최신 게임 변조 기법 및 방어 기술에 대한 지속적인 연구와 개선 등의 고도화 작업 필요
2. 게임 내 중요 함수 및 우선순위가 높은 변수는 암호화로 사용
3. 자동 플레이 매크로 모듈에 대해 실시간 패턴 업데이트로 즉각적인 대응 필요
    - 정상 유저의 클릭 패턴을 활용하여 매크로 유저들을 발견 한다.
    - 해커들이 현재 사용하고 있는 해킹툴, 프로그램을 직접 사용해보면서 분석
4. 안드로이드 및 게임 엔진 등을 보안 이슈를 확인하고 최신 버전으로 유지
5. 보안 체크리스트를 작성하여 주기적으로 성능 및 안정성 검증

보안 위협 대응 제안 – 자체 매크로 개발

1. 게임성을 저해시키지 않는 선에서 단순 반복 생산 작업의 경우 유료 매크로 기능 판매 제안
2. 기대효과
    - 보안이 강화되어 유저들이 안전하게 매크로를 이용 가능
    - 해당 프로그램 사용 유저의 플레이 패턴 파악 가능
    - 자사 프로그램 플레이 패턴과 불법 프로그램 사용 플레이 패턴을 손쉽게 비교 가능
    - 유저도 납득 할 수 있는 합리적인 가격 책정으로 추가적인 부수입 기대

보안 위협 대응 제안 – 보안 캠페인 시행

1. 유저 간 자발적인 신고 기능을 통해 불법 이용자들을 색출
2. 기술적으로 탐지가 어려운 부분을 신고 & 포상 제도를 이용하여 보충
3. 불법 행위 근절 주제로 유명 게임 유튜버에게 영상 의뢰
4. 보안 센터에 접속을 하여 로그인 기록을 확인 하면 보상 아이템 제공 이벤트 제안
5. 간과하기 쉬운 보안 문제를 지속적인 보상을 통해 유저 스스로 보안 의식을 고취시키는 것이 목표

참고자료

1. “데이터 분석 기반 게임봇과 작업장 탐지.” 김휘강 고려대학교
http://ndcreplay.nexon.com/NDC2017/sessions/NDC2017_0013.html#p=8

2. “쿠키런 킹덤 매크로 소개 및 다운로드” https://onmacro.com/board_fTzG94/11072

3. “코로나19에 모바일 게임 이용률 급증, ‘해킹’도 급증?” https://blog.naver.com/skinfosec2000/221960060071

4. “PC용 앱 플레이어 악용한 공급망 공격 발견” https://m.boannews.com/html/detail.html?idx=94867

5. "게임 보안은 끊임없이 확인하고 개선을 거듭하는 전쟁" 김성준 NHN 응용보안팀장
https://www.donga.com/news/It/article/all/20191114/98366238/1

6. “에뮬레이터 메모리 변조를 통한 해킹” https://appguard.toast.com/blog/5

End Of Document