주식회사 라르고소프트

Our Agenda for Today

Introduction
당신의 게임은 해킹으로부터 안전합니까?

G-Presto Solution
G-Presto는 이렇게 해결합니다.

G-Presto function
G-Presto의 혁신적인 기능을 살펴보시죠

Contact us
모바일게임 보안은 라르고소프트와 상의하세요

Introduction

당신의 게임은 해킹으로부터 안전 하십니까 ?

모바일게임 해킹 유저비율

라르고소프트 G-Presto 사용고객 2019년도 자료

4.2%

해킹위험율

2.9%

해킹시도율

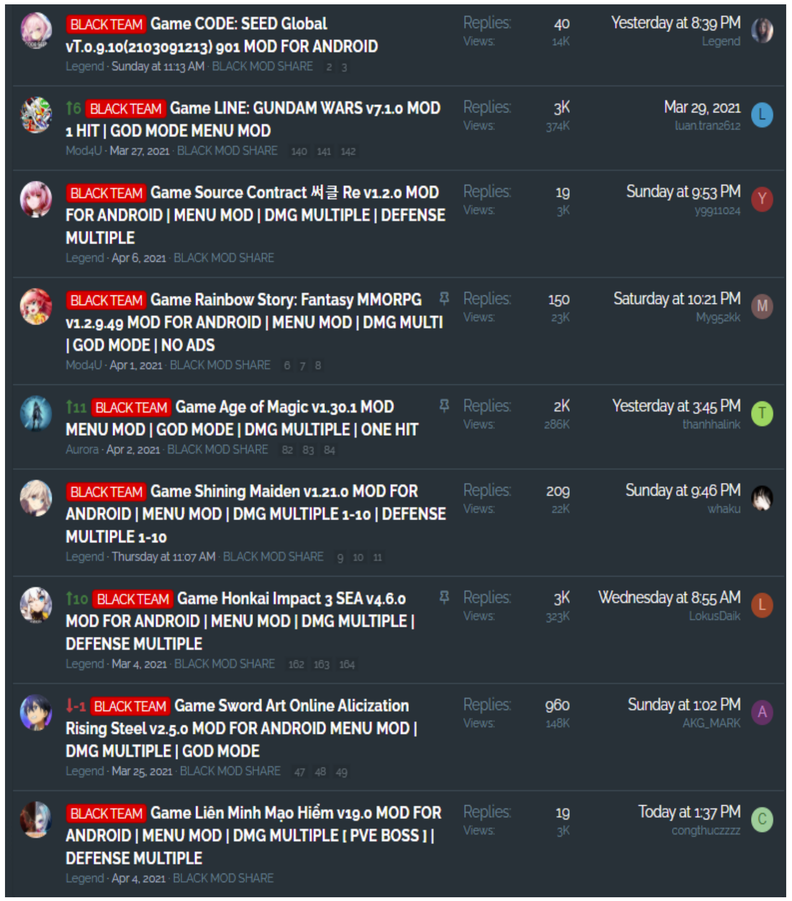
산출근거 : 해킹유저수/전체게임유저수*100

◆ 보안제품을 활용하지 않으면 위의 데이터보다 훨씬 높은 비율의 해킹유저가 유입될 가능성이 높다.

APP 보안이 필요한 이유

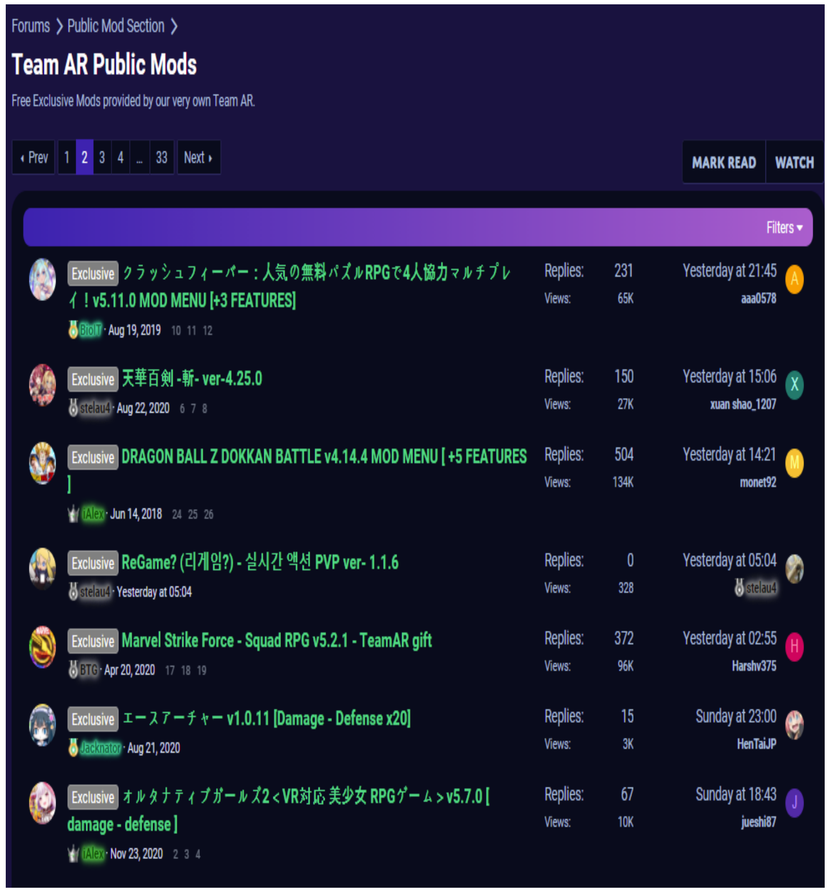
모바일게임 해킹 현황

여러나라의 해킹커뮤니티 사이트에 국내외 모바일 게임 위변조앱이 유포되어 있다



Bestapkmod 해킹사이트 유포 현황

IOSGOD 해킹사이트 유포 현황



Androidrepublic 해킹사이트 유포 현황

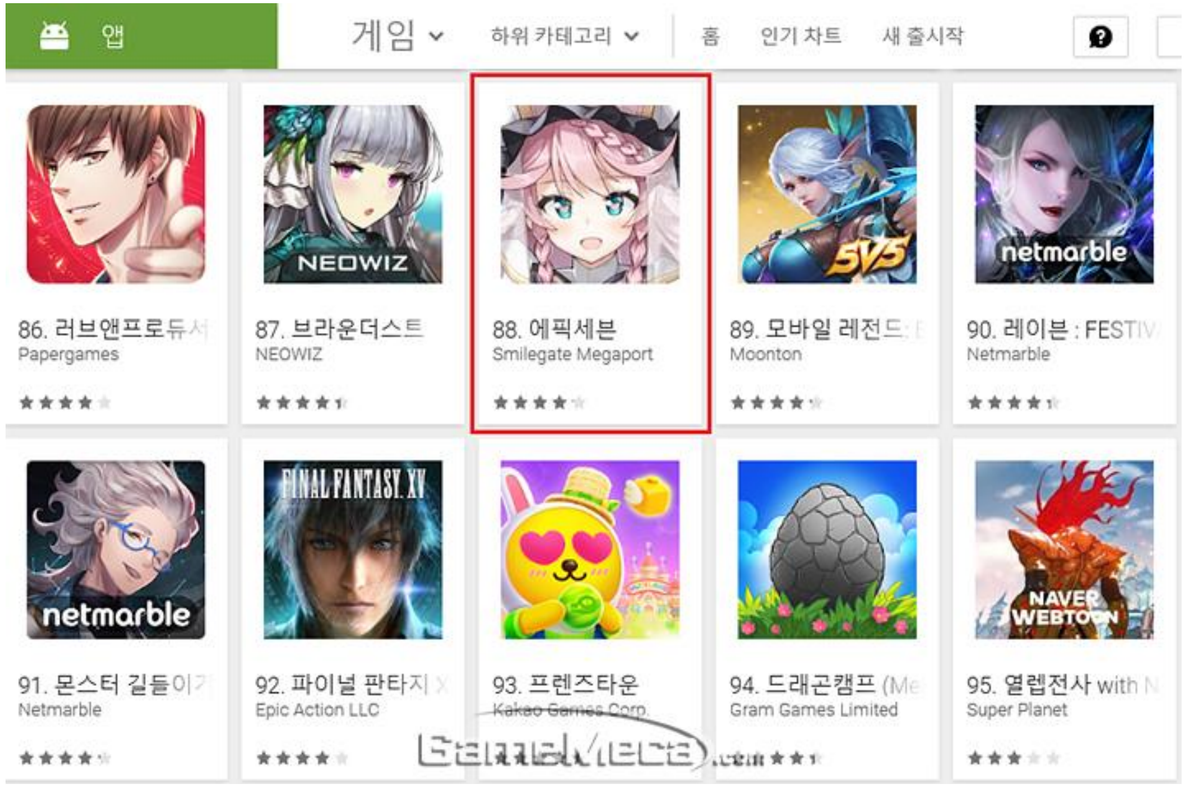
APP 보안이 필요한 이유

해킹상황의 방치는 유저들의 클레임을 유발한다.

유명 게임회사의 사례로 해킹의 지속적인 방치는 게임 운영에 악영향을 미친다는 것을 알 수 있다.

"불법 프로그램 논란 후 제재 리스트 매일 공개"

50위권에 머물던 스마일게이트 '에픽세븐' 매출 순위가 급락한 것은 지난 7월 초 불거진 보안 문제다. 오래된 치트 프로그램에 게임 보안이 뚫렸다는 이야기가 커뮤니티 등지를 통해 급속도로 확산되며 논란이 커졌고, 운영진의 불통식 대처가 겹치며 민심이 급속도로 떠났다. 그 결과 지난 15일, '에픽세븐'은 출시 이후 처음으로 구글 게임부문 매출 100위를 기록하는 등 출시 이래 최저 성적을 기록했다.

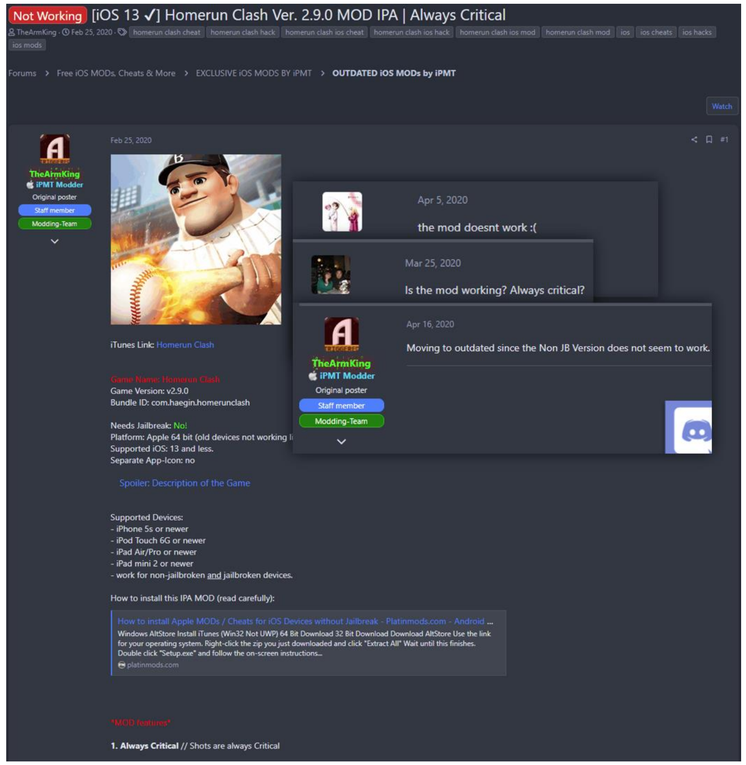


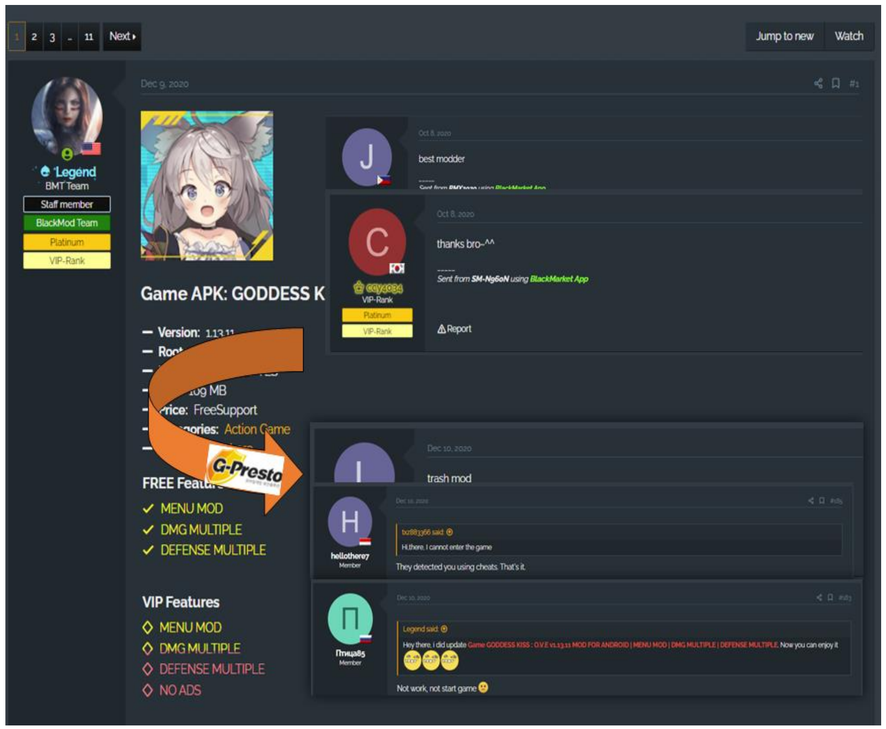
게임메카 '에픽세븐 유저간담회 1주... 매출 회복은 미미'기사내용 발췌

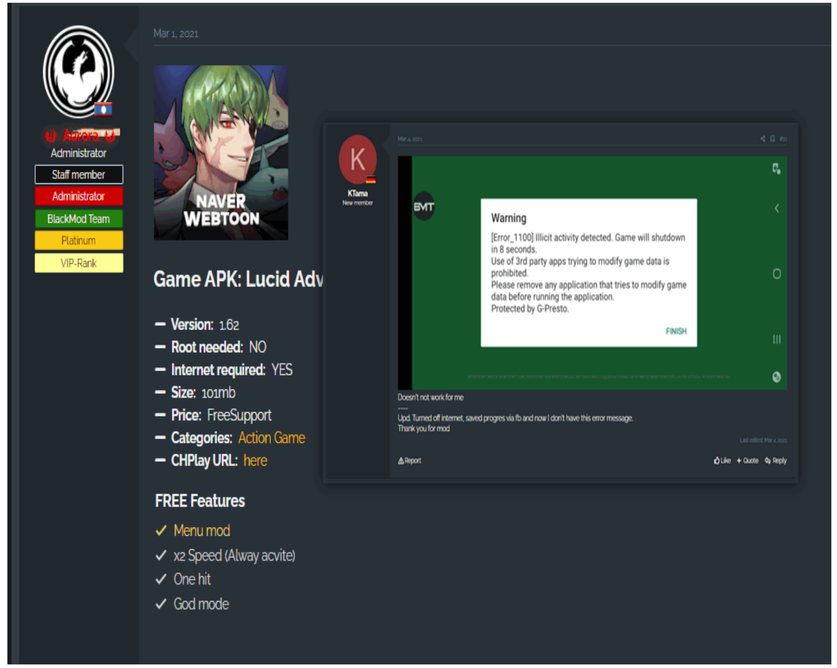
APP 보안이 필요한 이유

해킹사이트에 해킹 대응사례

라르고소프트는 기존 파트너들의 G-Presto 도입사례를 통하여 해킹 방지를 증명하였다.







- 각종 해킹커뮤니티에서 유포되었던 위변조된 모바일 게임들이 G-PRESTO 제품 적용이후 해킹 업데이트가 중단 되었다.
- 위의 그림 자료는 실제 해킹사이트에서 라르고소프트 파트너사 게임 해킹을 포기하는 사례들 이다.

How to Prevent

어떻게 해킹을 대처하고 계십니까.

서버로그분석 대응의 한계

메모리 핵, 스피드 핵, 매크로 등의 해킹유무를 개발사에서는 서버 로그 분석을 통해 로그 값의 대조로 판단하는데 한계가 있음

정확도 부족

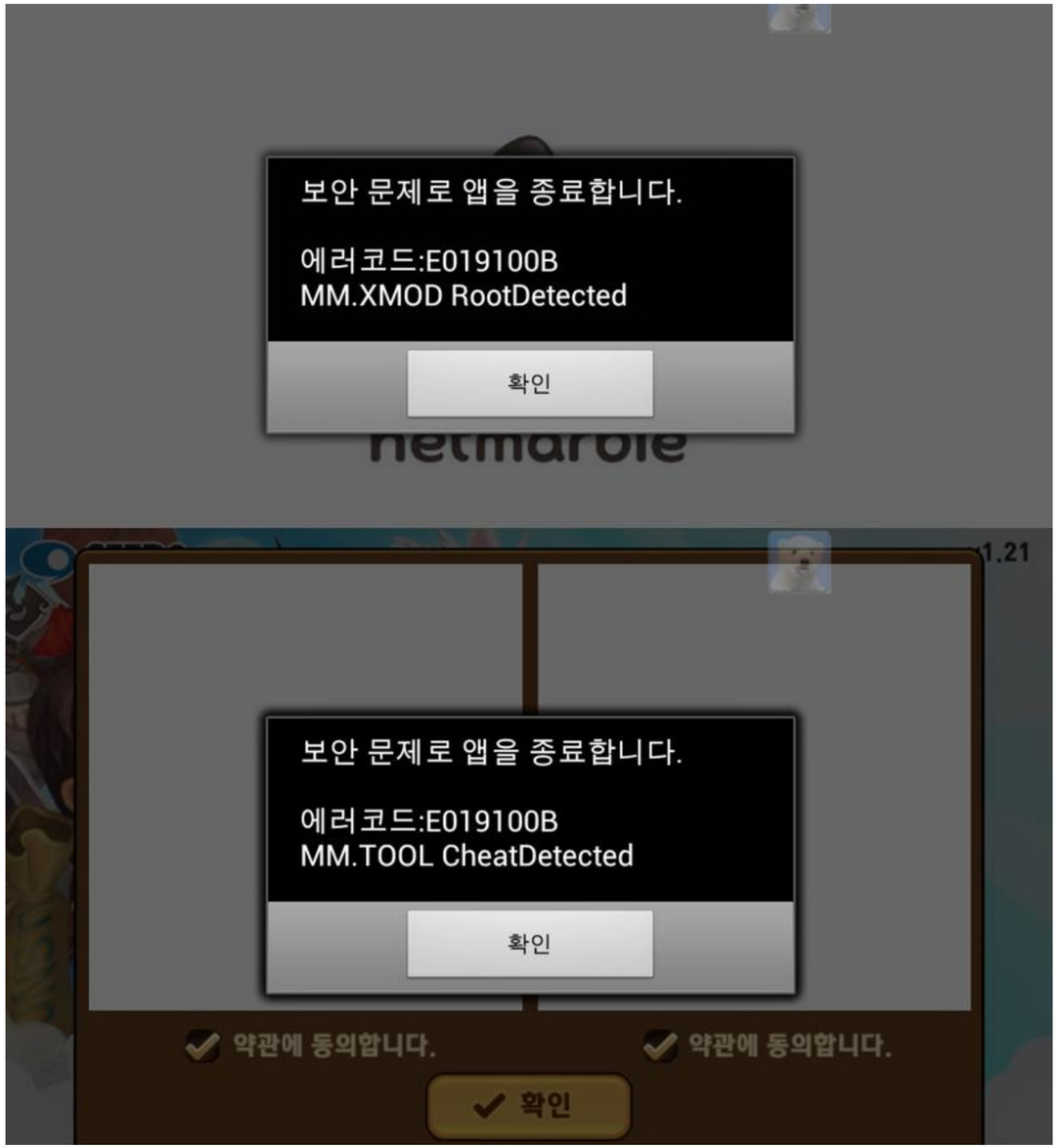
조작할 수 있는 **변수가 너무나 많기** 때문에 사전에 모든 변수를 예측하기 어려우며 또한 로그로만 해킹유무를 **정확하게 확인 할 수 없습니다.**

효율성 부족

지속적인 **변수를 확인**하는 작업은 **시간이 많이 소요**되어 안정적인 게임 운영을 방해합니다.

대처방안의 문제점

서버로그분석은 대부분 **해킹이 발생하고 나서 확인**이 되기 때문에 후 처리 하는 단점이 발생합니다.
또한 대부분 유저를 차단하는 방식으로 **유저를 잃게 됩니다**.



해킹툴 대응의 문제점

보안 전문 인력 부족으로 인해 변종 해킹툴 및 정보수집이 이루어지지 않고 있음

정보수집능력 부족

개발사 내의 개인 또는 팀이 사용되고 있는 많은 해킹 툴의 정보를 수집 하는 데는 한계가 있습니다.

변종해킹 툴 대응불가

원본 해킹 툴의 정보를 모두 수집하더라도 우회하는 해킹 툴을 대처하지 못하다면 대응이 불가능 합니다.

데이터 난독화

메모리 값을 찾기 어렵게 하기 위해 암호화를 사용하지만 주소를 찾는 시간을 다소 연장시킬 뿐입니다.

```
public Car(TrackPosition pos, Color drawColor,
{
  this.pos_ = pos;
  this.drawColor_ = drawColor;
  this.eraseColor_ = eraseColor;
  this.gasPedal_ = gasPedal;
  int[] xs = new int[4];
  int[] ys = new int[4];
  this.poly_ = new Polygon(xs, ys, 4);
}
```

original method

```
public a(h paramh, Color paramColor1, Color paramColor2,
{
  this.a = paramh;
  this.b = paramColor1;
  this.c = paramColor2;
  this.e = paramb;
  int[] arrayOfInt1 = new int[4];
  int[] arrayOfInt2 = new int[4];
  this.d = new Polygon(arrayOfInt1, arrayOfInt2, 4);
}
```

obfuscated method

그림 적용 전과 후의 역 컴파일 결과비교

기존 난독화 사용의 문제점

안드로이드에서 제공되어 일반적으로 사용하는 난독화 도구(ProGuard)의 사용으로는 코드 수정을 막을 수 없음

보안레벨이 낮다

흔하게 사용되는 난독화 (ProGuard 등)의 경우는 식별자명을 파악하는데 어려움이 있지만 여전히 실행코드의 제어흐름은 **쉽게 파악**이 가능합니다.(**왼쪽그림참조**)

게임엔진과의 호환이 어렵다

기존 난독화 (ProGuard 등) 는 **JAVA 난독화만 가능**하며 Unity 등의 **게임 엔진 보호 기술이** 없습니다.

난독화 만으로는 앱위변조를 방지하기 어렵다

기존의 난독화 기술은 분석 속도를 늦출 수는 있지만 코드 분석을 위해 디컴파일하여 수정 후 다시 컴파일하는 **리패키징 과정**을 차단하거나 지연 시킬 수 없습니다.

G-Presto Solution

G-Presto는 이렇게 해결합니다.

G-Presto를 활용한 해킹대처 방안

G-Presto 적용

모바일게임 출시 전후 G-Presto SDK를 적용합니다.

G-Presto 해킹통계분석

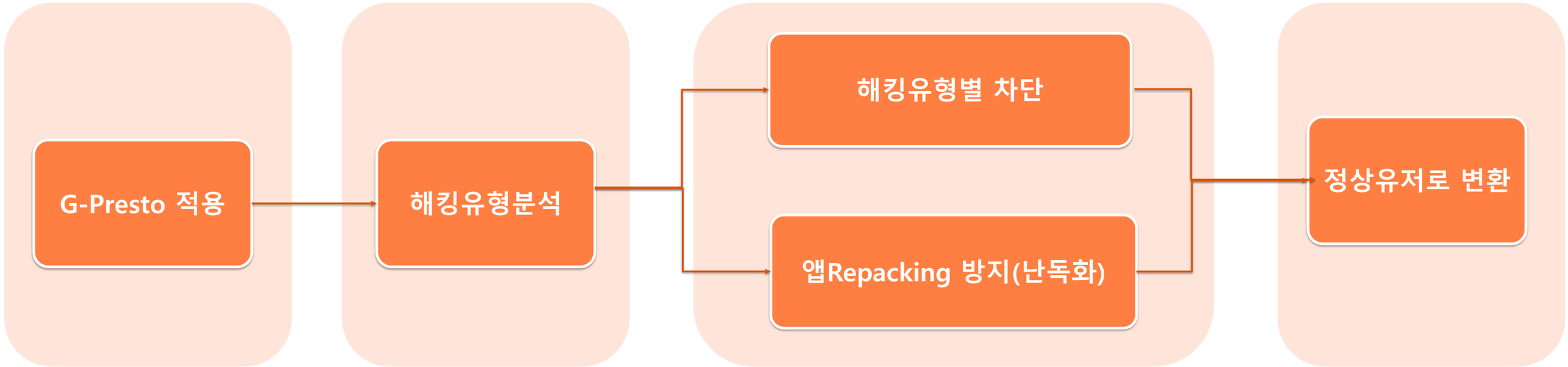
해킹통계분석툴을 이용하여 게임내 유입되는 해킹정보를 쉽게 파악합니다.

G-Presto 보안기능의 활용

G-Presto의 사용하면 게임개발사에서 원하는 해킹유저의 해킹방법을 차단하여 일반유저로 접속할 것을 유도합니다.

결과

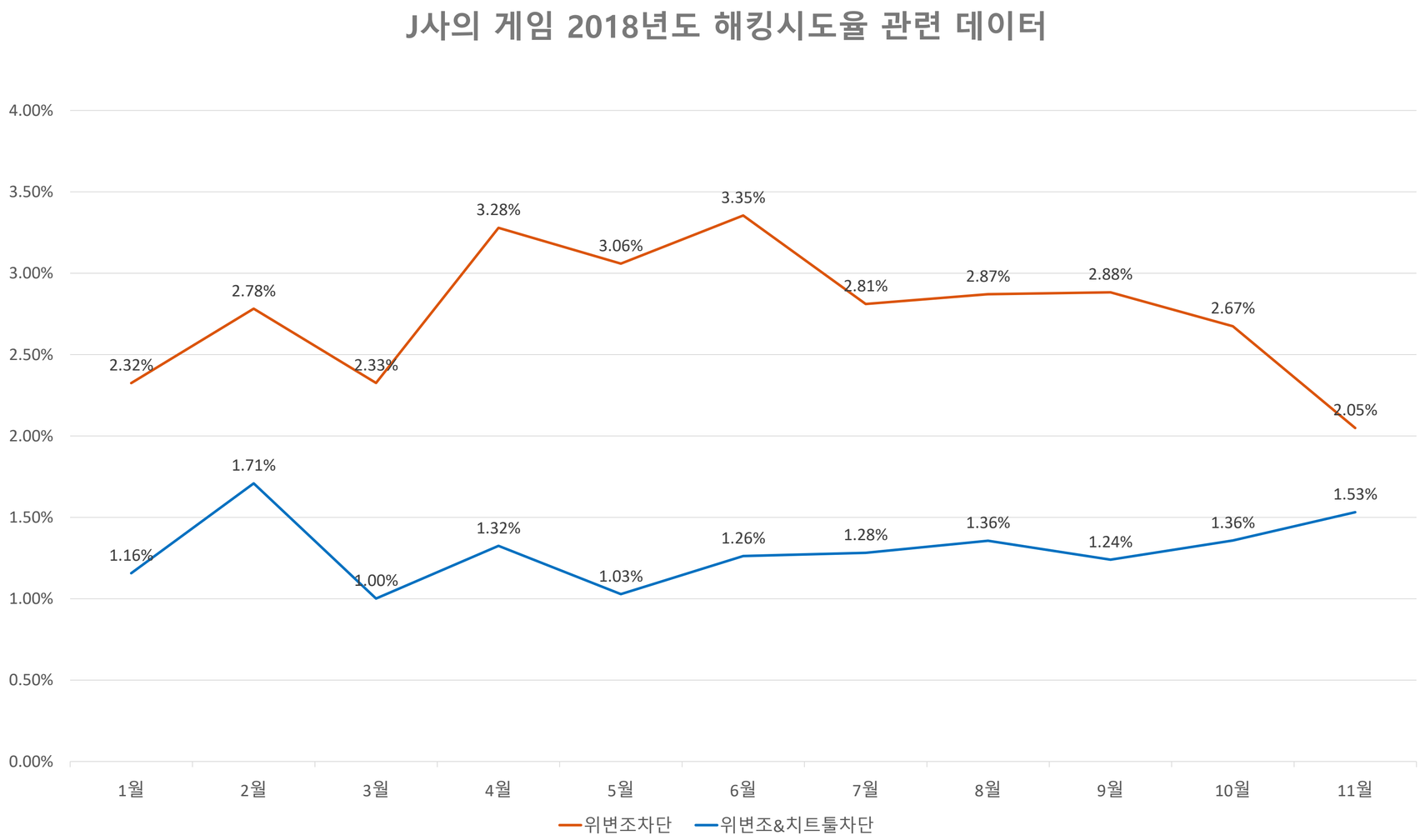
해킹유저의 비율은 낮추고 정상유저의 비율은 높여드립니다.



◆ G-Presto 사용시 해킹유저-> 일반유저 전환율 (2019년도 G-Presto 사용고객 기준)

- 하드코어 (RPG&방치형 등)게임류 : 최대 50%대
- 미들코어 (SNG&전략 등) 게임류 : 최대40%대
- 캐쥬얼 게임류(퍼즐&SNG) : 최대 30%대

보안기능 적용과 해킹시도율 상관관계



평균 2.76%

평균 1.3%

◆ 보안기능을 추가적으로 활용 할 수록 해킹시도율 평균이 줄어드는 것을 확인할 수 있다.

G-Presto function

G-Presto의 혁신적인 기능을 살펴보시죠

G-Presto 시스템구조

G-Presto Client 및 Server

G-Presto SDK

- 해킹 Tool 탐지
- APP Repacking 탐지 1
- Rooting 탐지

난독화 (App Repacking 방지)

G-Presto Ent

G-Presto Server

해킹관련 Tool Down

App Repacking 탐지 2

해킹로그 전송

MobileGame APP

* Server장애가 발생하더라도 Client가 독립적으로 실행되어 80%정도의 보안기능이 작동됨

해킹통계분석기능

APP에 유입되는 해킹유형을 수집 및 분석 합니다.

해킹유형 정보 확인

게임 내 유입되는 여러 가지 해킹방법에 대하여 확인 할 수 있습니다.

해킹유저 정보 확인

해킹을 시도하는 접속자의 다양한 정보(디바이스아이디,접속시간,UUID 등)를 확인하여 해킹유저를 찾아 낼 수 있습니다.

DAU 확인

DAU와 해킹유입의 상관관계에 대하여 한눈에 파악하여 대처 할 수 있습니다.

블랙리스트 확인

해킹시도가 많은 유저의 정보를 따로 모니터링 하여 악성 해킹유저 관리를 쉽게 하실 수 있습니다.

해킹툴탐지기능

G-Presto 엔진에서 탐지하는 주요 해킹툴 정보

Memory 해킹

GameGuadian, GameHacker
등의 메모리 해킹툴을 탐지합니다.

결제 해킹

Freedom, luckyPatcher 등의 결제
해킹툴을 탐지합니다.

Abusing

가상 머신 ,매크로 프로그램 등
오토플레이를 위한 도구를
탐지합니다.

불법개조폰

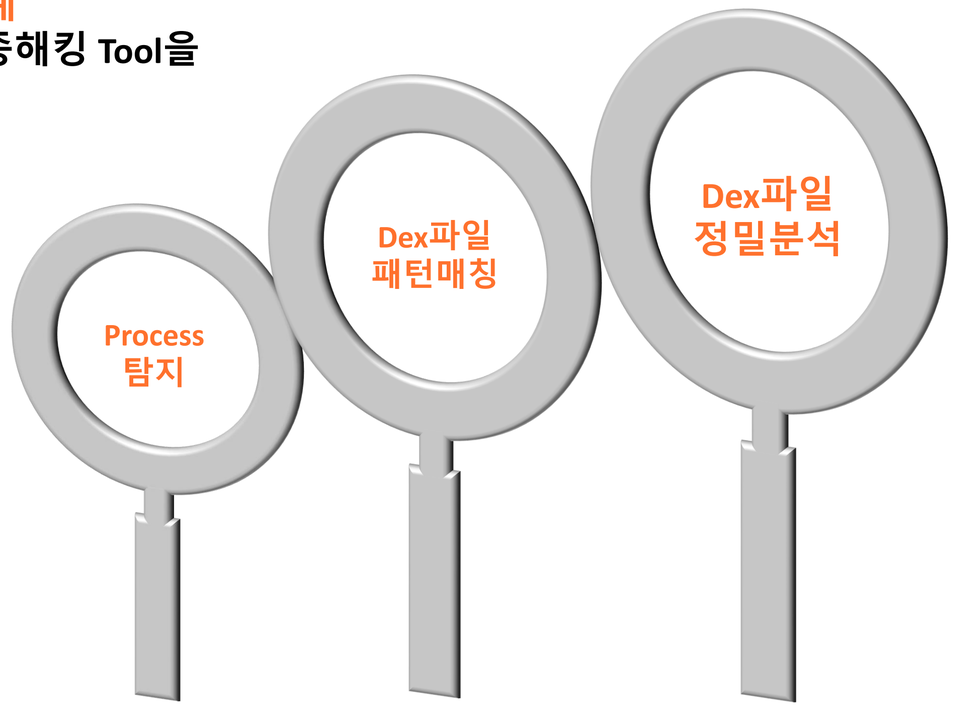
Android 루팅폰, iOS 탈옥폰 등
불법개조폰을 탐지합니다.

해킹툴탐지기능

G-Presto 해킹툴탐지기능 특장점

변종해킹 툴 차단기능

G-Presto만의 3단계 탐지방식으로 변종해킹 Tool을 원천 차단합니다.



*Dex : Dalvik Executable Format

메모리 핵 차단 기능

◆ 변수 암호화

- 유니티 게임 코드의 상수, 변수의 값을 암호화하고 변조를 감지하는 기능

◆ 프로세스 접근 방지

【Anti-Dump】

메모리상에 올라간 앱에 대해 메모리 덤프 기능을 차단

【Anti-Ptrace】

Ptrace, Strace 등의 차단으로 후킹 등의 행위를 차단

【Anti-Debugging】

GDB 등의 디버깅 툴의 접근을 차단

해킹툴탐지기능

G-Presto 해킹툴탐지기능 특장점

PC (에뮬레이터)환경에서도 해킹 감지 가능

◆ **보안에 취약한 PC 환경에서의 해킹시도가 빈번해짐**

- 현재 라르고소프트에서는 가장 문제가 되고 있는 PC 환경에서의 메모리 해킹 및 스피드핵관련 부분을 대응하고 있음 (유니티 환경에서 가능)

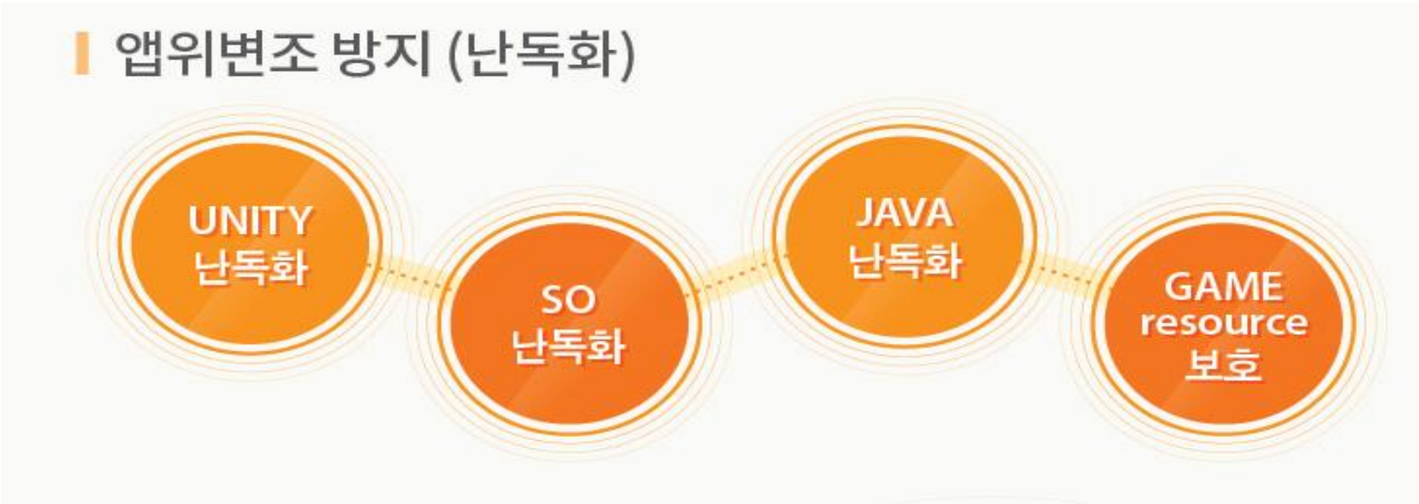
모바일 환경에서 보안강화로 해킹이 어려워짐

상대적으로 취약한
NOX,MOMO등과 같은 앱플레이어 환경에서 해킹시도

G-Presto는 PC 환경에서도 주요 해킹 대응가능

앱Repacking 방지 및 탐지

2가지 방식으로 Repacking앱을 방어합니다.



난독화 기능 설명 보안

G-Presto의 난독화는 다양한 모바일게임 APP의 환경에 **호환**되는 난독화를 **자체 개발**하여 제공합니다. **(IOS 난독화 기술도 보유함)**

Repacking 앱

Repacking 앱 접속시도

G-Presto Client

Step1. 엔진(SDK)에서 무결성 검사

&

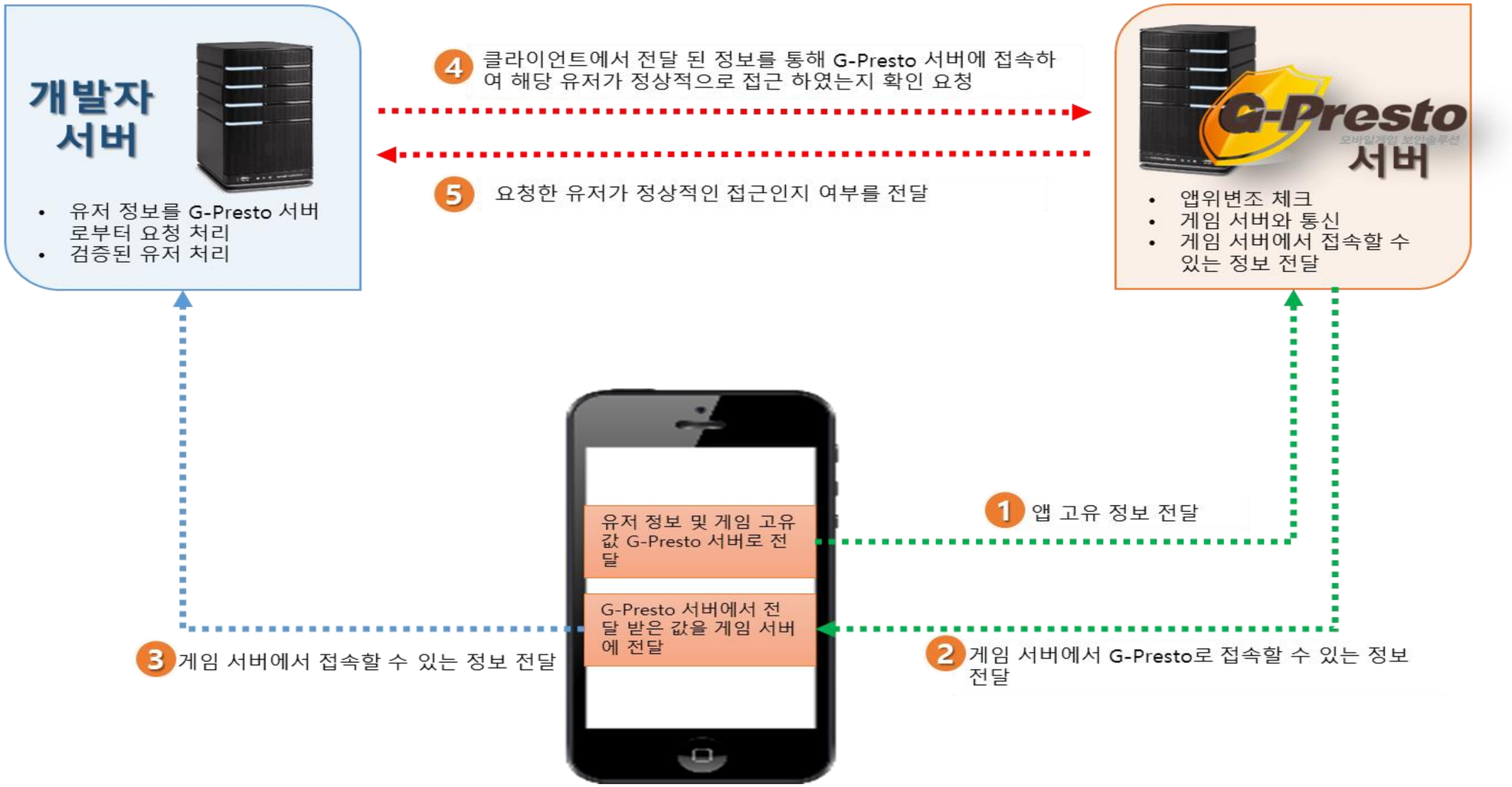
G-Presto Server

Step2. Server에서 무결성 검사

G-Presto만의 **2가지 방식의** 검사기능으로 **Repacking APP의** 접근을 **차단**합니다.

앱Repacking 크로스체크 탐지 (G-Presto Premium 모델기능)

기존 Repacking 탐지기능에 비해 엔진해킹에 대한 보안성 강화된 기술



해킹커뮤니티 사용자로그분석

G-Presto 적용되어 해킹커뮤니티 사이트 등록된 경우 유저확인 가능

보안프로그램해킹

보안프로그램 적용된

게임을 우회하여 해킹하는

경우가 발생 될 수 있다.

보안공백기간발생

보안프로그램 해킹에

대처하는 동안 해킹유저가

유입되어 보안 운영에

문제가 발생 할 수 있다.

1. 보안회사에서 이를 대처하기 위한 분석과 개발에 시간

+

2. 업데이트된 보안프로그램이 게임에 적용되어 스토어에 업데이트 되는 시간

=

보안공백기간

해킹커뮤니티 유저 정보 수집

라르고소프트는 보안제품을 우회하는 유저들의 정보를 역
해킹하여 해당 해킹유저 정보를 수집 할 수 있어서
보안운영에 허점이 생기는 기간 동안에 대응이 가능하다.

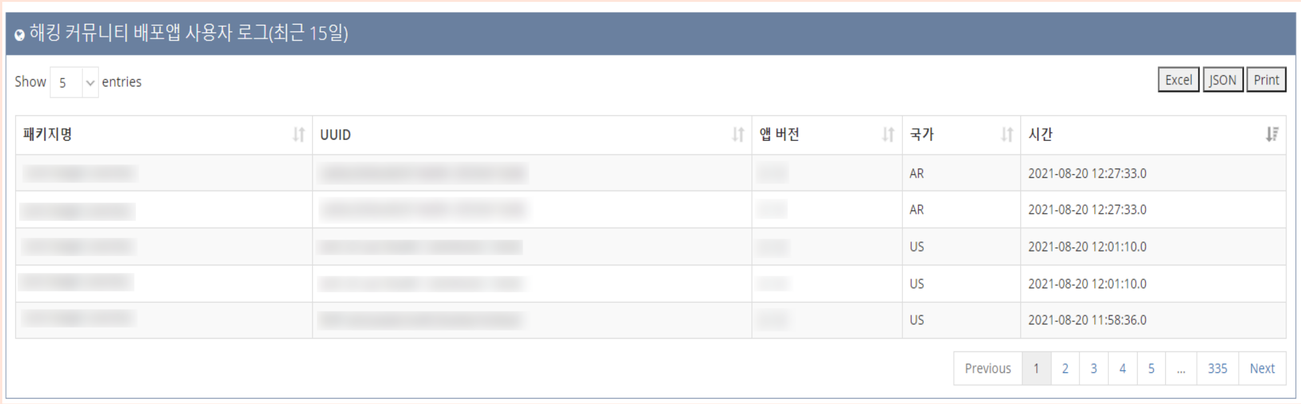


그림. 라르고소프트 관리자 페이지 화면(고객사 관리툴에 api연동가능)

실시간 정책 적용 기능

G-Presto 패키지 설정 기능 특장점

원하는 유형의 해킹정보를 관리자페이지에서 패키지별로 실시간 정책기능을 사용하여 차단이 가능합니다.

웹페이지 콘솔 기능 화면

치트툴차단	앱위변조차단	가상머신차단	매크로차단	dex난독화	Res암호화	unity암호화	루팅차단
ON	ON	OFF	OFF	ON	OFF	ON	OFF
ON	OFF	OFF	ON	ON	ON	ON	OFF
OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF
ON	OFF	ON	ON	OFF	ON	ON	OFF
OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF

보안 운영 시스템(G-Presto Premium 모델기능)

추가적으로 발생될 수 있는 해킹위협에 빠르게 대응

빠른 CS 대응

메신저 방을 개설하여 365일 고객의 문의사항에 대하여 대응합니다.

해킹관련 사이트 모니터링

각국의 모바일 게임 해킹관련 사이트 및 게임커뮤니티 사이트를 항시 모니터링 함.

보안 취약점 분석

모바일 게임의 보안 취약점 분석 및 보안 가이드를 제공 합니다.

자동적용 시스템

APP 업로드만 하면 3분이내 G-Presto 적용가능

자동적용 홈페이지에서 쉽고 빠르게 G-Presto의 보안기술 적용 가능

G-Presto 주요기능

OS	기능	상세기능	주요특징
AOS	해킹툴탐지	결제해킹,메모리해킹,어뷰징,루팅단말기 등을 차단	변종해킹툴 탐지가능 메모리 변조 분석 방지기능
	Repacking앱 탐지	Repacking된 앱으로 게임서버에 접근하는 것을 차단	당사 모바일 보안엔진 해킹에 대응 하여 보안성을 높이는 보안기능
	Repacking앱 방지	게임APP의 소스를 분석 및 수정하는 행위을 방지	유니티 암호화 ,SO난독화,JAVA난독화 등을제공
	자동적용시스템	G-Presto의 SDK 및 난독화 기능을 자동으로 적용	웹페이지를 이용하여 3~5분이내 적용가능
IOS	해킹툴탐지	결제해킹,메모리해킹,어뷰징,탈옥단말기 등을 차단	메모리 변조 분석 방지기능
	Repacking앱 탐지	Repacking된 앱으로 게임서버에 접근하는 것을 차단	당사 모바일 보안엔진 해킹에 대응 가능한 고도의 앱Repacking 기술을 사용
공통	호환성	Android 2.3 이상 IOS 6.X 이상	모든 모바일게임엔진 호환가능
	통계분석	게임 내 접근하는 다양한 해킹유형 정보를 파악	DAU,블랙리스트유저,해킹유형분석등
	실시간 정책적용	당사가 제공하는 여러 보안기능별로 실시간 정책이 가능	웹콘솔(웹페이지)에서 적용 가능
	자동업데이트	재적용을 하지 않더라도 자동으로 당사엔진 업데이트가능	새로운 기능 업그레이드 외 SDK 재적용 불필요

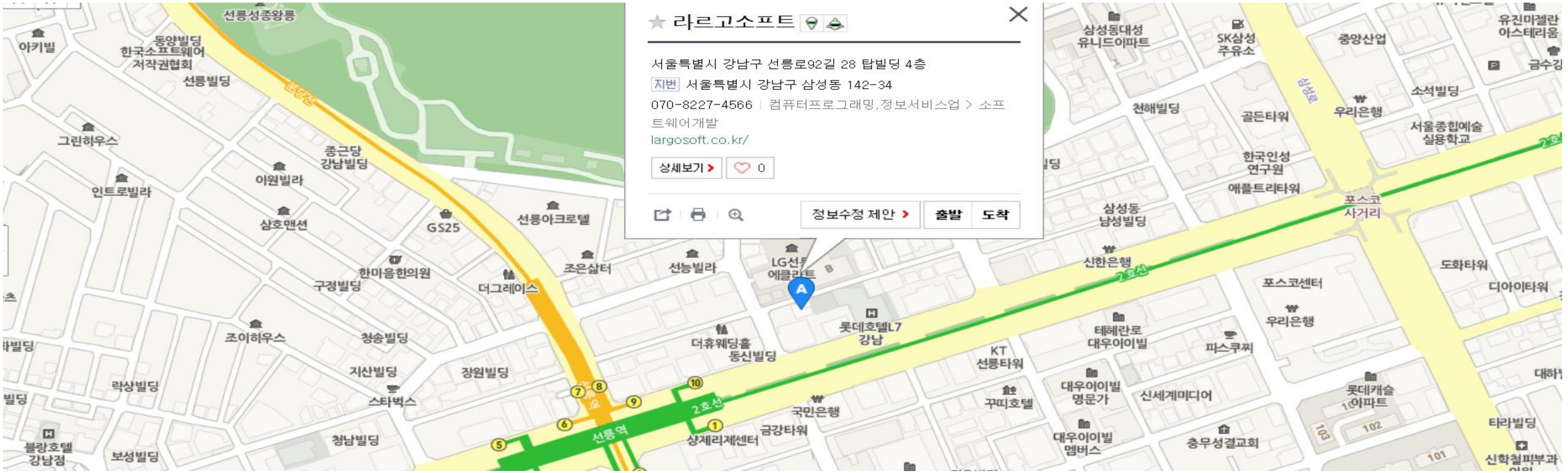
라르고소프트 주요고객사

Contact us

모바일 게임 보안은 라르고소프트와 상의하세요

찾아오시는 길

위치



Our Location

28, Seolleung-ro 92-gil,
Gangnam-gu, Seoul, Republic of Korea

Our Phone

(+82)70 8227 4566

Email / Website

help@largosoft.co.kr
www.largosoft.co.kr