
LINE
Mobile Security Paradigm Shift
AIR
2018 LINE Plus Game Security

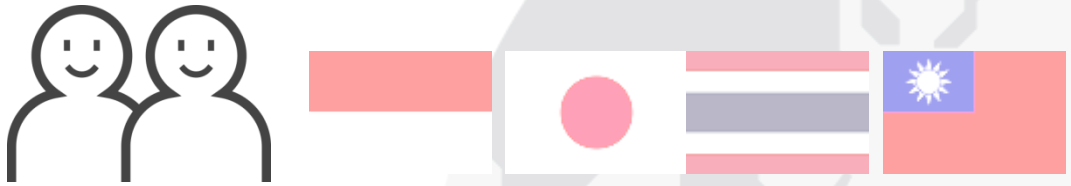
800,000,000

70,000,000

Disney tsumtsum

50,000,000

Rangers



15,000,000

AU

200G

Security Data

84

Game

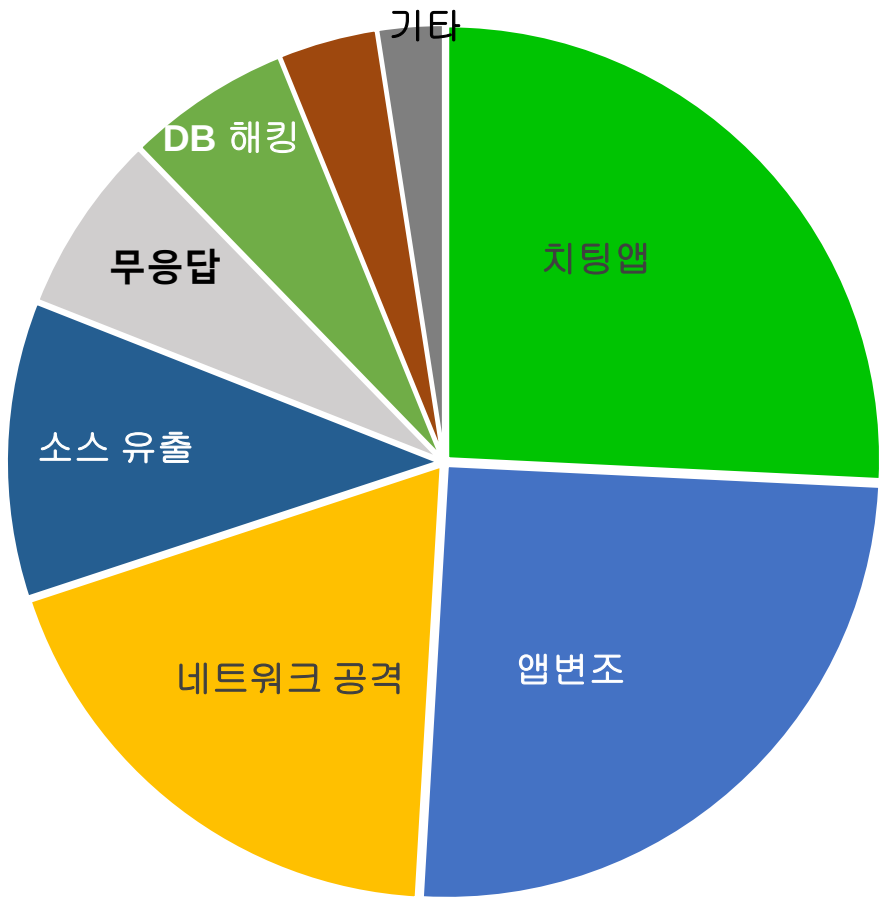
Game Security Status

- **Android -** 루팅, 메모리 조작, fake client app
- **IOS -** 루팅, 메모리 조작, fake client app (2017년 이후 관찰)

❖ 치팅앱(메모리 조작), 앱변조 (바이너리 변경)은 모든 모바일 서비스에 해당

- **Game**
  - Unity 관련 변조 (C# decompile, 로직 유출)
  - Network Attack (Packet 이용한 Auto abuse 대행)
  - 관계 서비스 Token을 이용한 치환공격 (Oauth)
  - Server 연결 조작 및 직접 해킹시도 (소규모 개발사)

Game Security Status



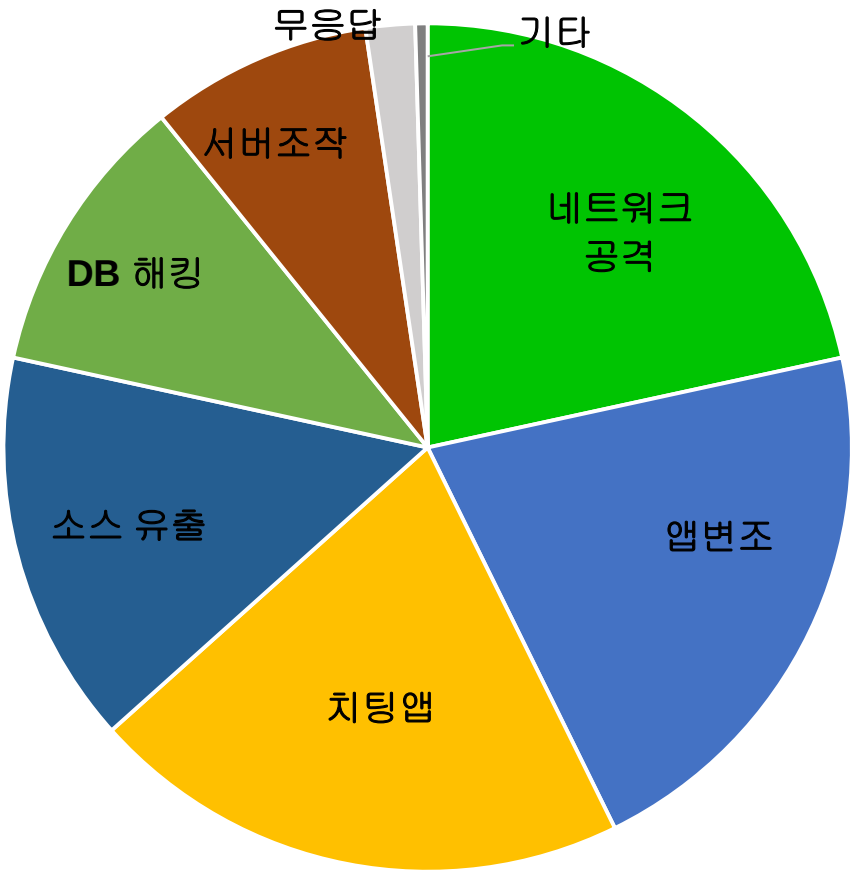
모바일 앱에서 해킹 대응 이슈가 있다면?

문항	내역	응답수	비율
1	치팅앱	42	26%
2	앱변조	41	25%
3	네트워크 공격	31	19%
4	소스 유출	18	11%
5	무응답	11	7%
6	DB 해킹	10	6%
7	서버조작	6	4%
8	기타	4	2%
Total	중복응답(42)	163	100%

기타 : 스푸핑 접근 (1)

2018. 4 개발자 대상 보안 세미나 – 주최 LINE Game Platform 설문

Game Security Status



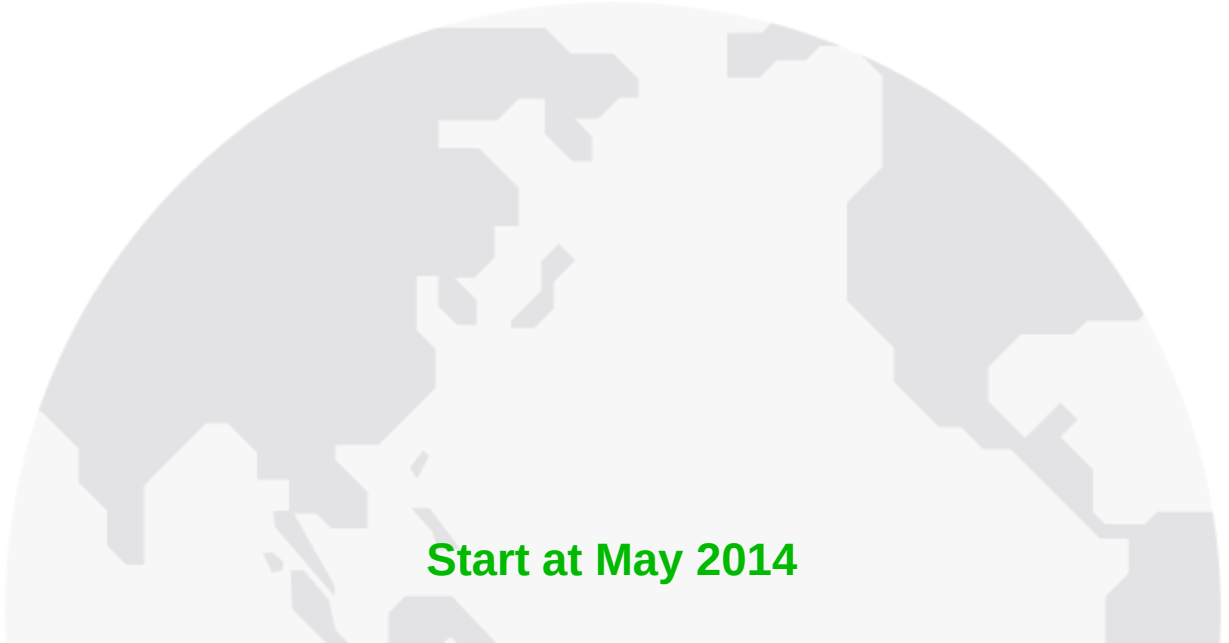
앱 개발시 가장 보안적으로 우려 되는 부분은?

문항	내역	응답수	비율
1	네트워크 공격	46	22%
2	앱변조	45	21%
3	치팅앱	44	21%
4	소스 유출	32	15%
5	DB 해킹	23	11%
6	서버조작	18	8%
7	무응답	4	2%
8	기타	1	0%
Total	중복응답(71)	213	100%

2018. 4 개발자 대상 보안 세미나 – 주최 LINE Game Platform 설문

2014

We must build basic!



Start at May 2014

Mission

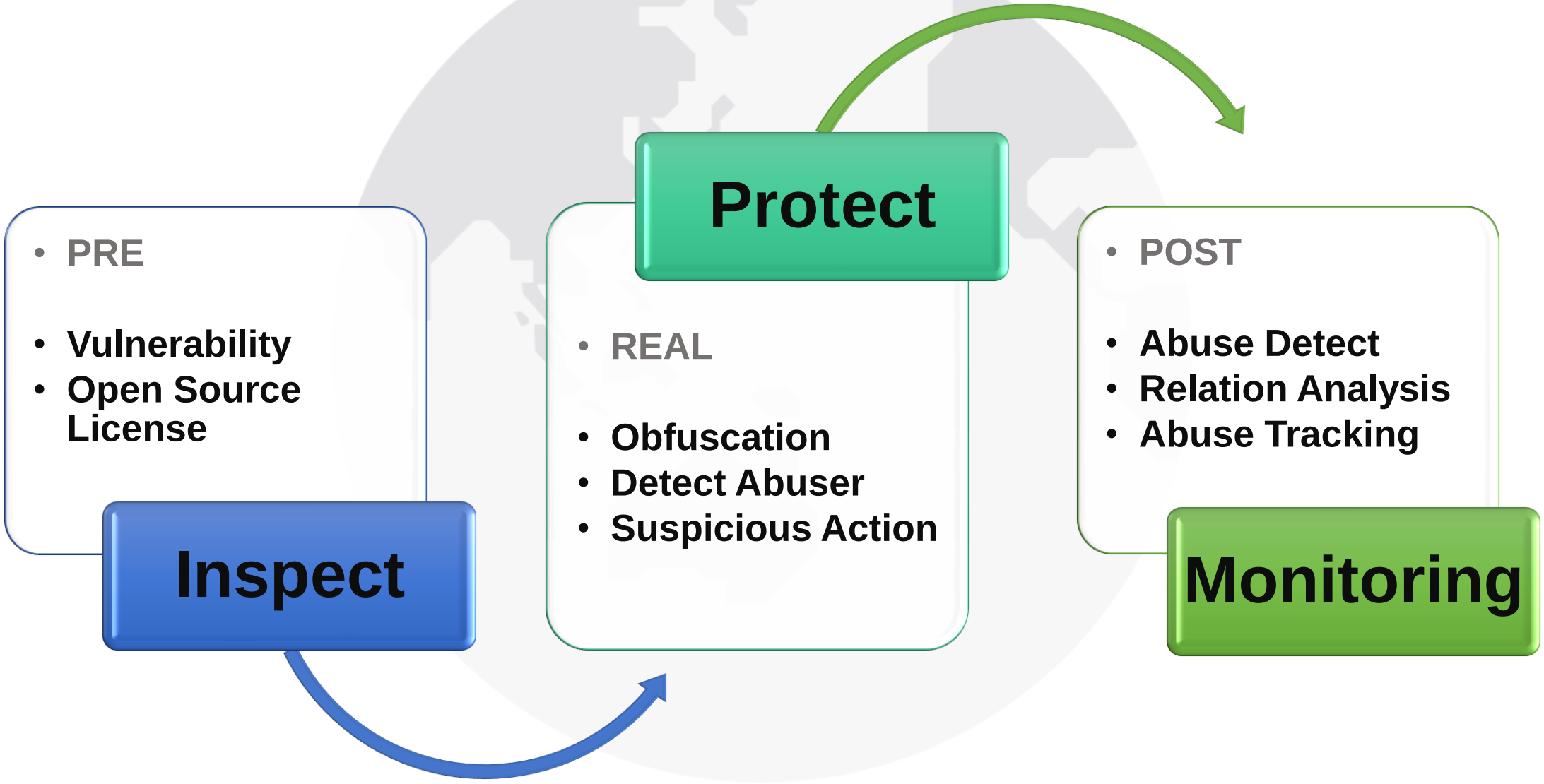
- 메모리 조작을 막을 수 있는가?
- 변조된 앱을 이용한 **Abuser**를 탐지할 수 있는가?
- 개발된 앱은 쉽게 분석되지 않도록 하며, 중요 로직은 보호한다.
- 앱 출시 이전에 근본 취약성을 제거 할 수 있을까?
  (Open Source, CVE 취약성 등**)**
- 온라인에서 자동으로 진단하고, 보호하며, **Abuser**를 탐지하는 것이 가능할까?

Game Security Mission

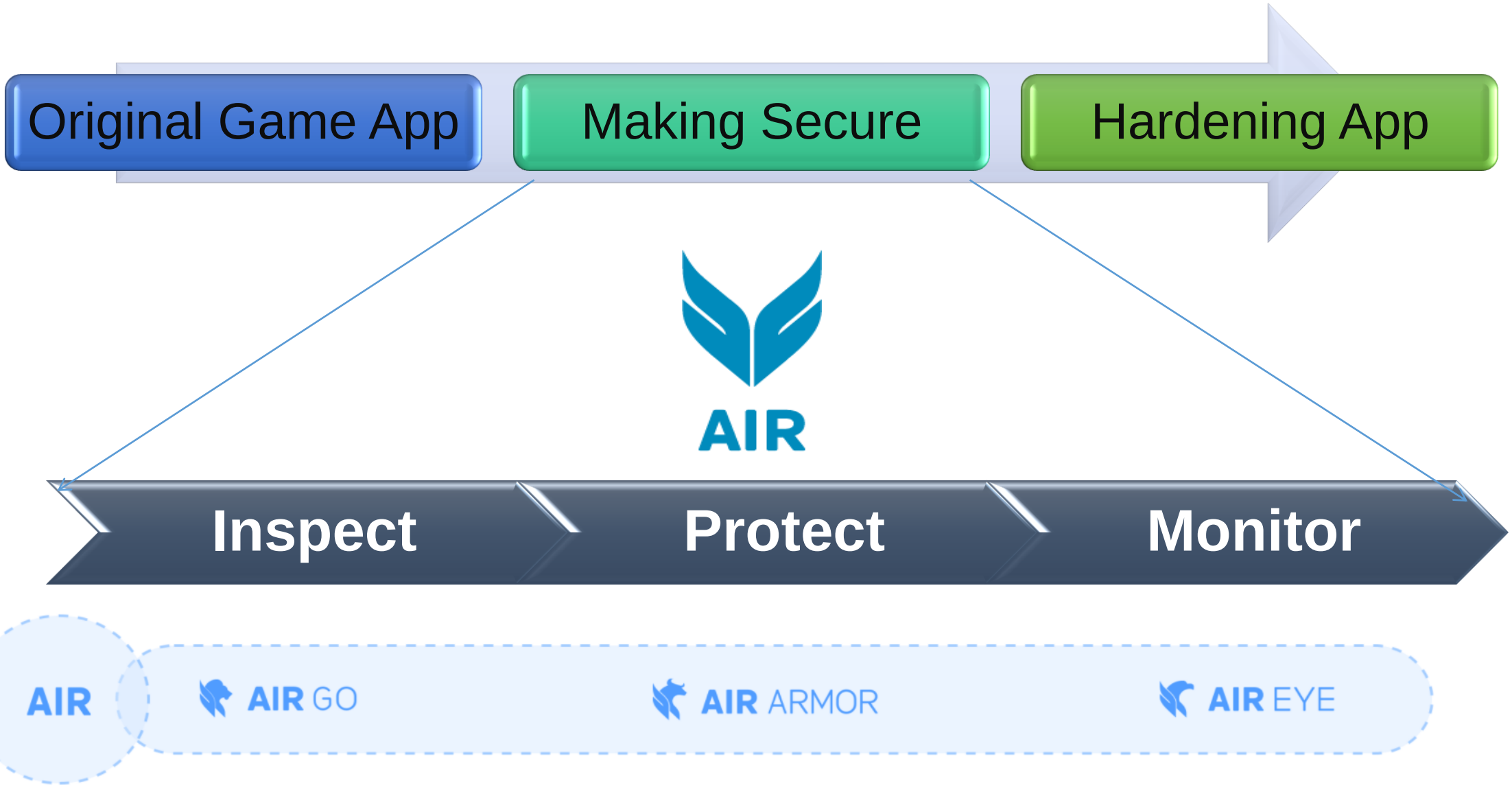
Passive Response → Active Incident Response

Log Base Detect → Pre Protect
- Remove vulnerability
- Hard to Disassemble
- Silent Detect

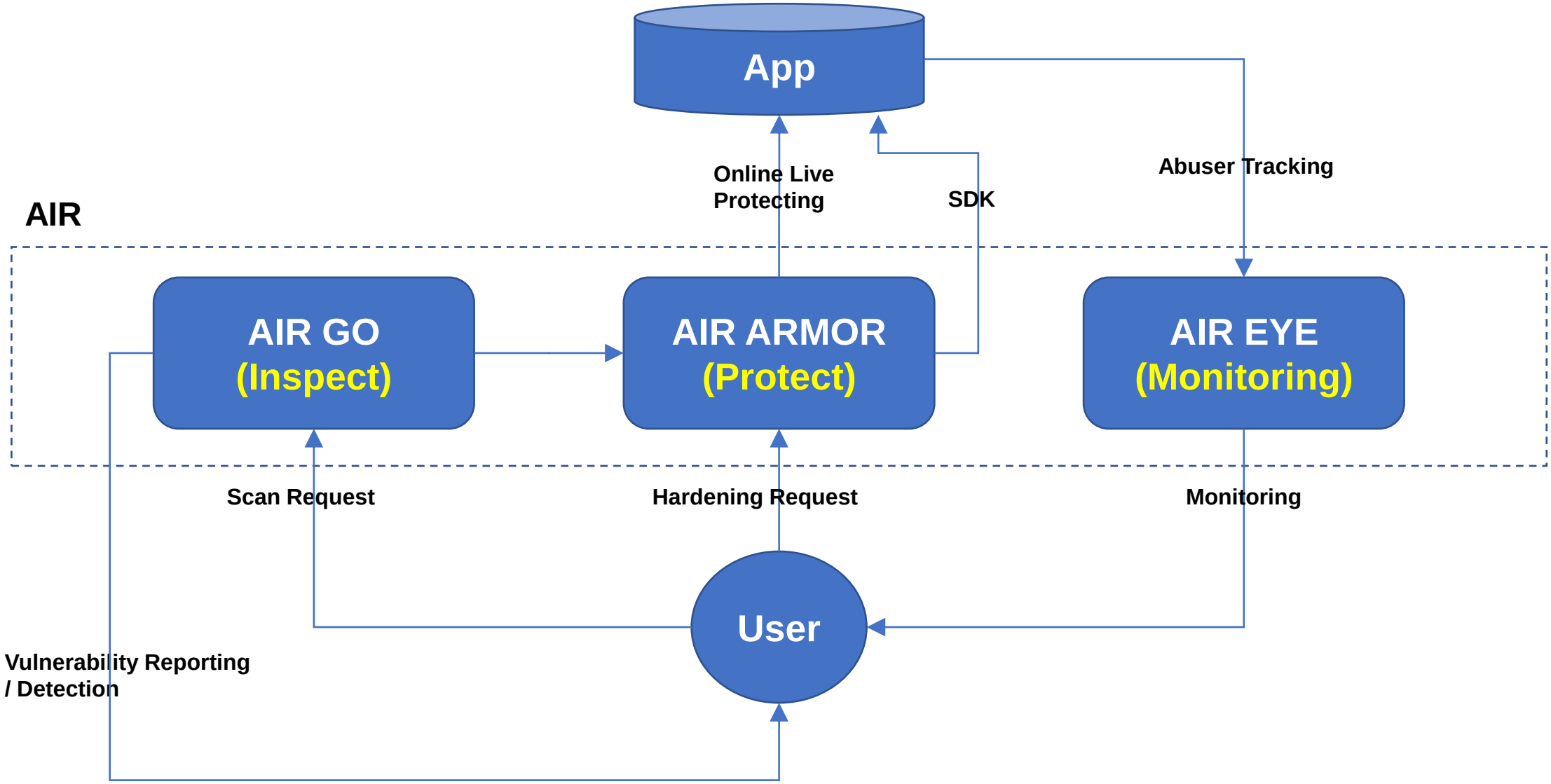
Making Security Process



Active Incident Response



AIR Flow Diagram

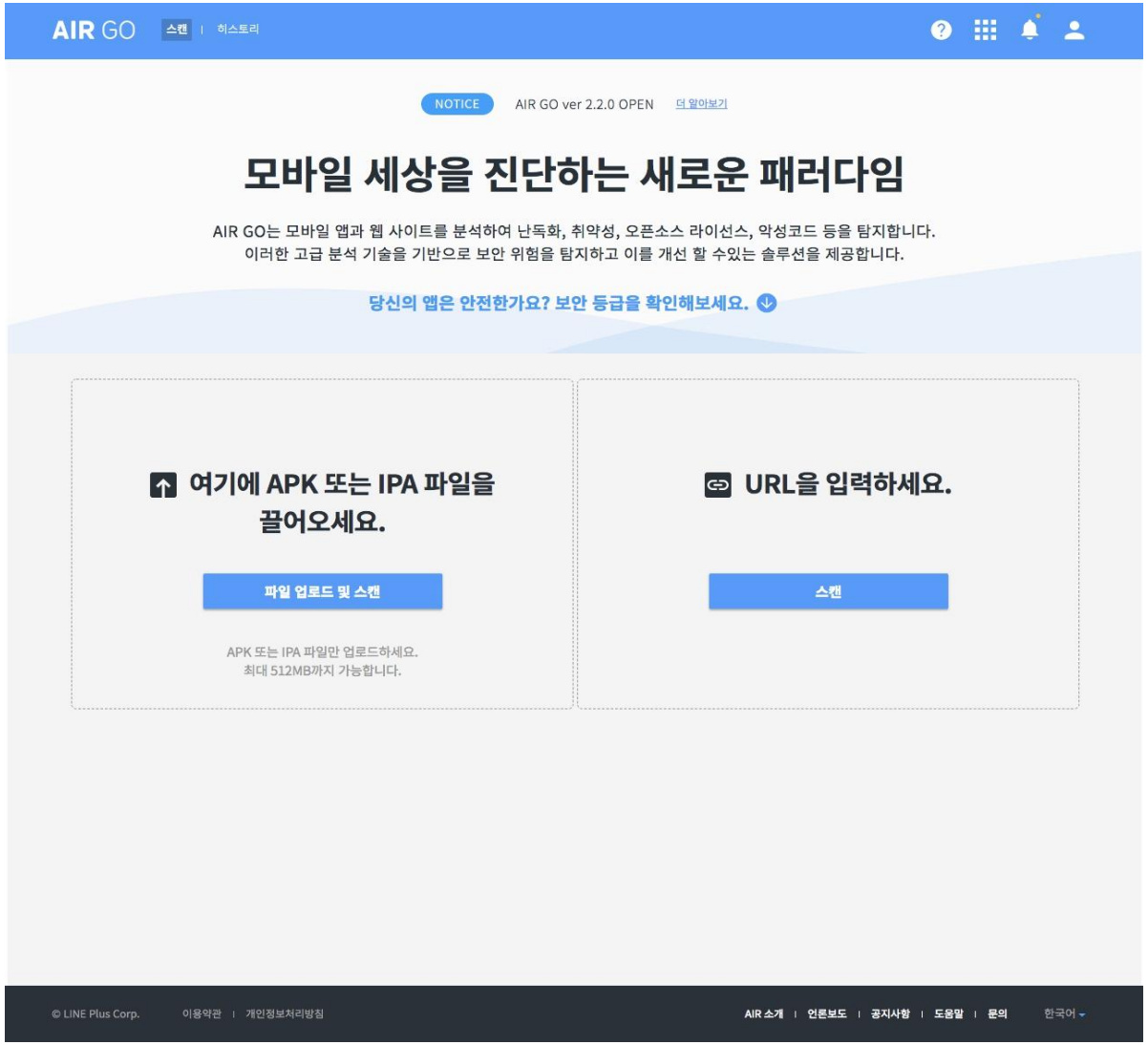


AIR GO (Inspect)

obfuscation, vulnerability, open source license, malicious URLs

https://air.line.me/airgo

AIR GO (Inspect)



- APK, IPA 파일 업로드 이후 자동분석
1. 취약성 (모바일 관련 CVE)
2. Open Source License
3. Google Secure App Guide 취약성
4. 난독화 여부

- URL 입력 시 악성 진단
1. URL 내에 악성 URL 포함 여부

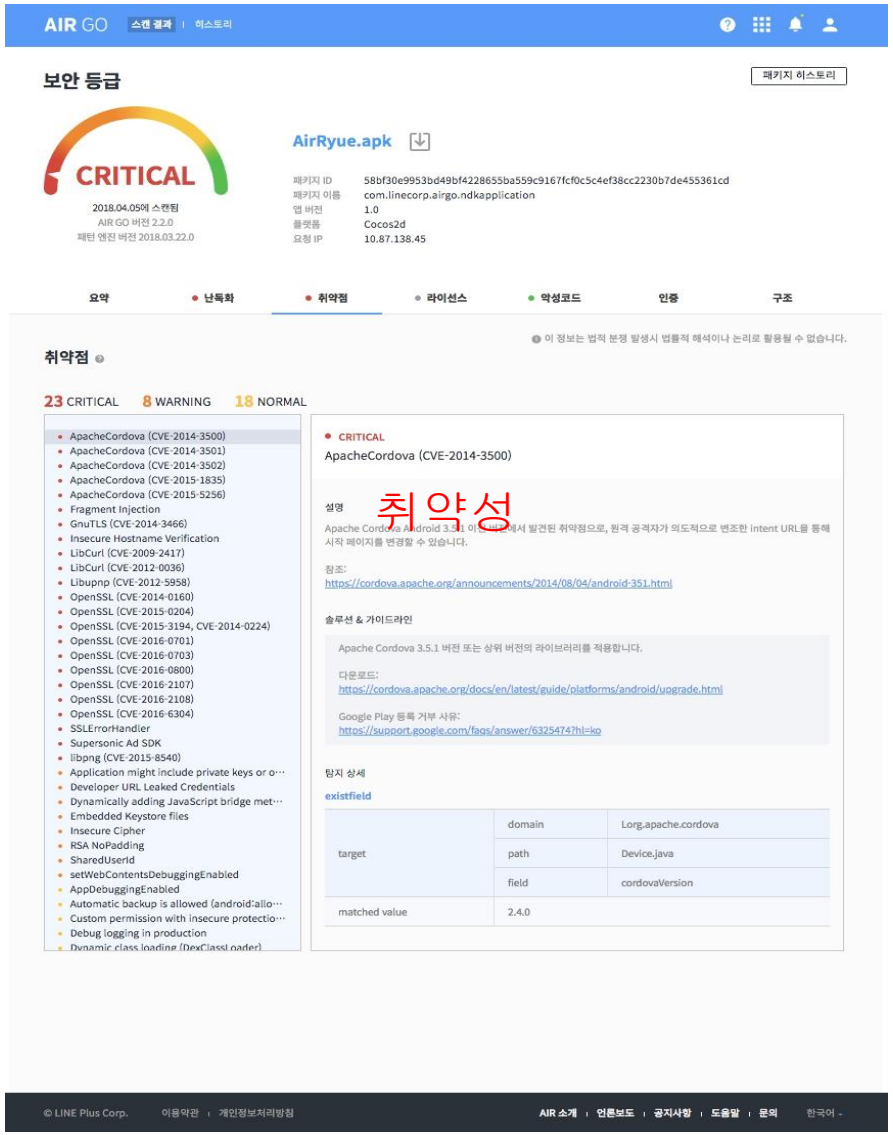
* Rest API 서비스 내부운영 (라인, 네이버)
* Google App Security
https://developer.android.com/google/play/asi.html

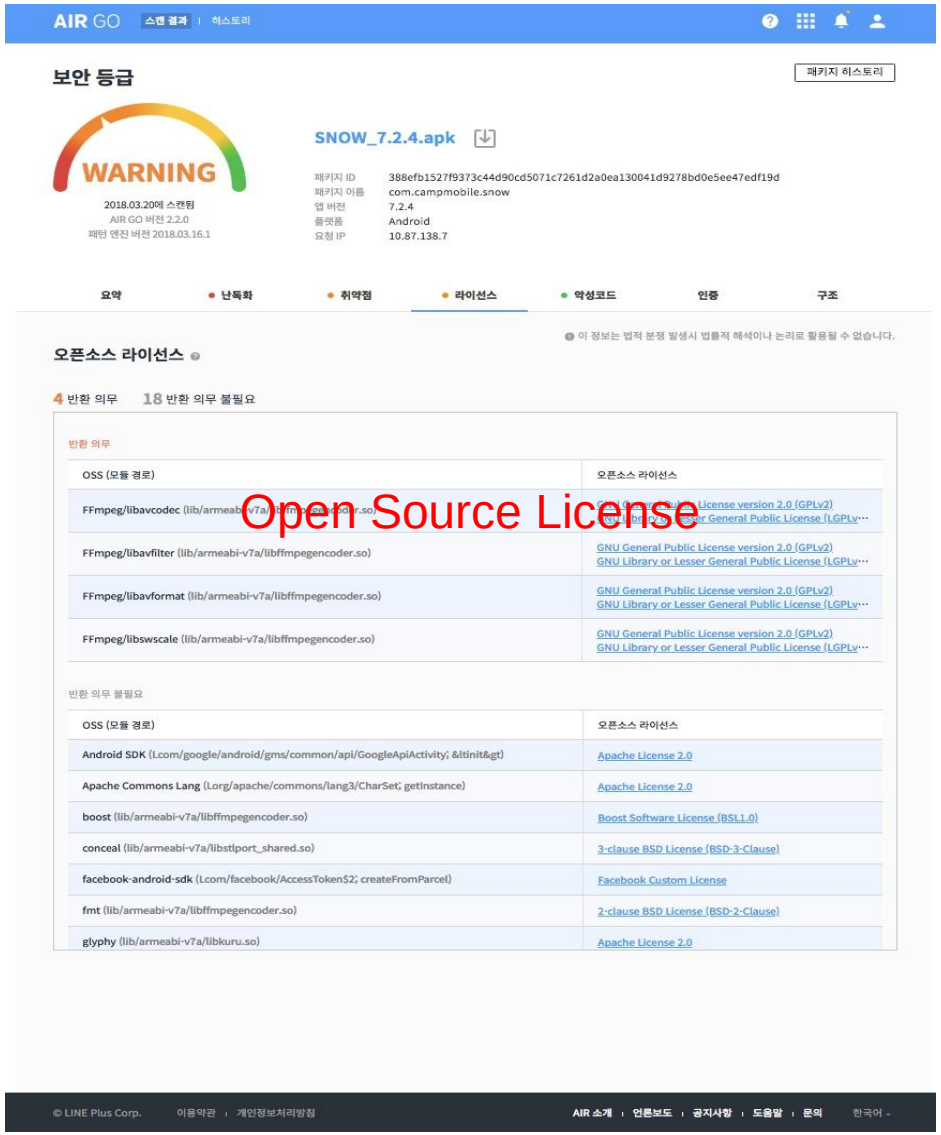
AIR GO (Inspect)

진단 결과

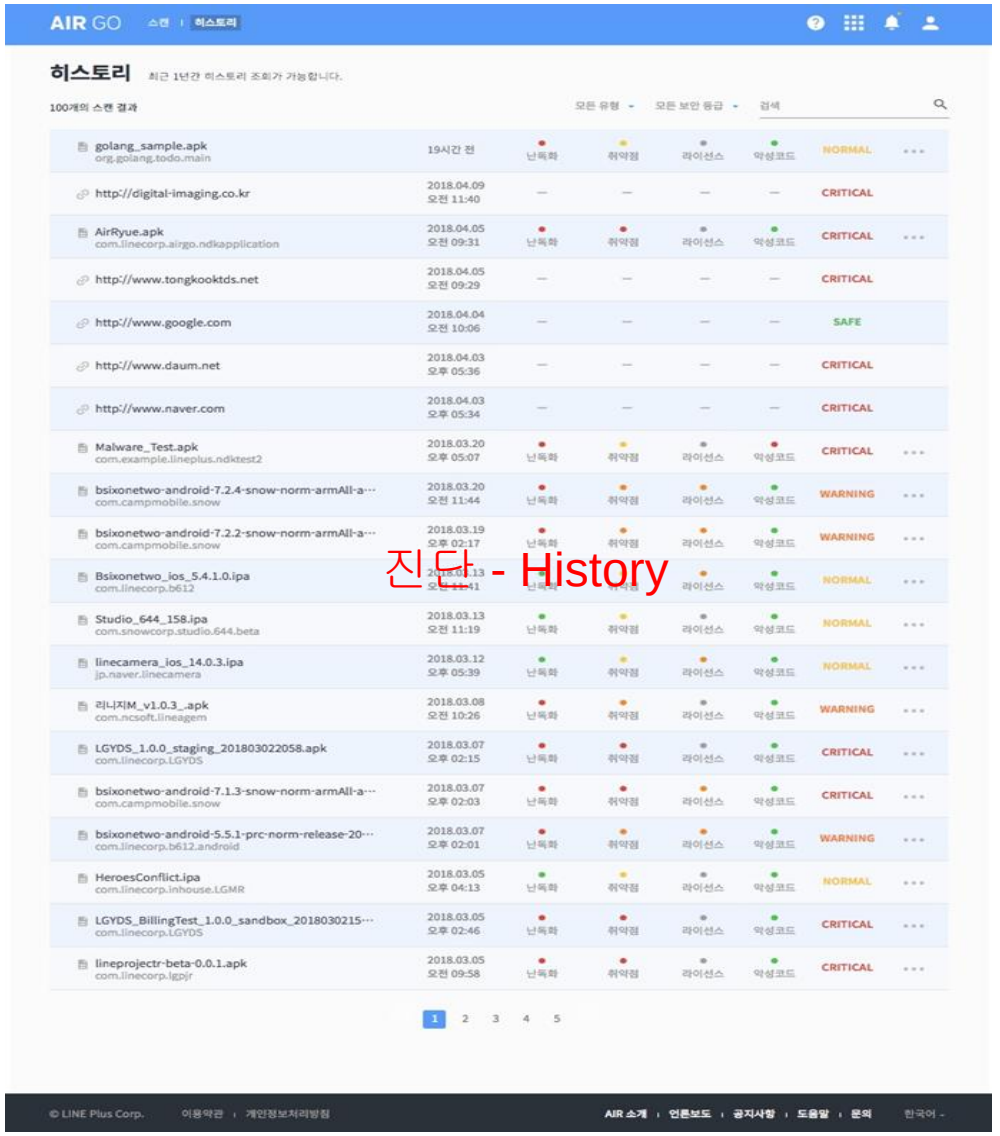
- 평가 등급
- 앱내 중요 파일의 난독화 여부
- 취약성 통계
- 앱내의 오픈소스 라이선스
- 악성 **URL** 및 악성코드 포함여부

AIR GO (Inspect)





AIR GO (Inspect)



AIR GO (Inspect-ref)

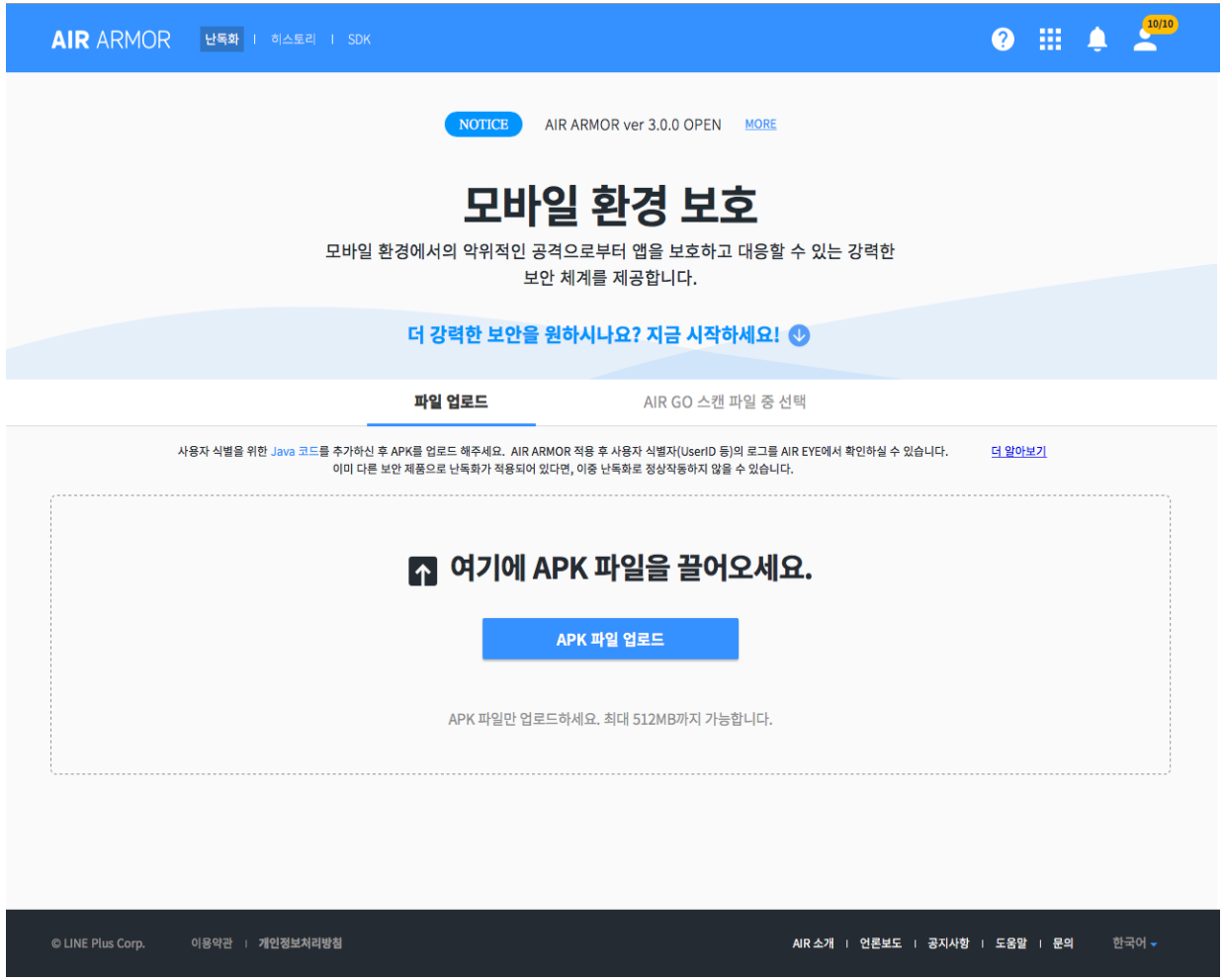
Campaign
Path Traversal
Insecure Hostname Verification
Fragment Injection
Supersonic Ad SDK
Libpng
Libjpeg-turbo
Vpon Ad SDK
Airpush Ad SDK
MoPub Ad SDK
OpenSSL (“logjam” and CVE-2015-3194, CVE-2014-0224)
TrustManager
AdMarvel
Libupup (CVE-2015-8540)
Apache Cordova (CVE-2015-5256, CVE-2015-1835)
Vitamio Ad SDK
GnuTLS
Webview SSLErrorHandler
Vungle Ad SDK
Apache Cordova (CVE-2014-3500, CVE-2014-3501, CVE-2014-3502)

App 등록 시 향후 취약성 포함된 앱에 대한 점검 강화 예상됨

AIR ARMOR (Protect)

Protection, Obfuscation

AIR ARMOR (Protect)

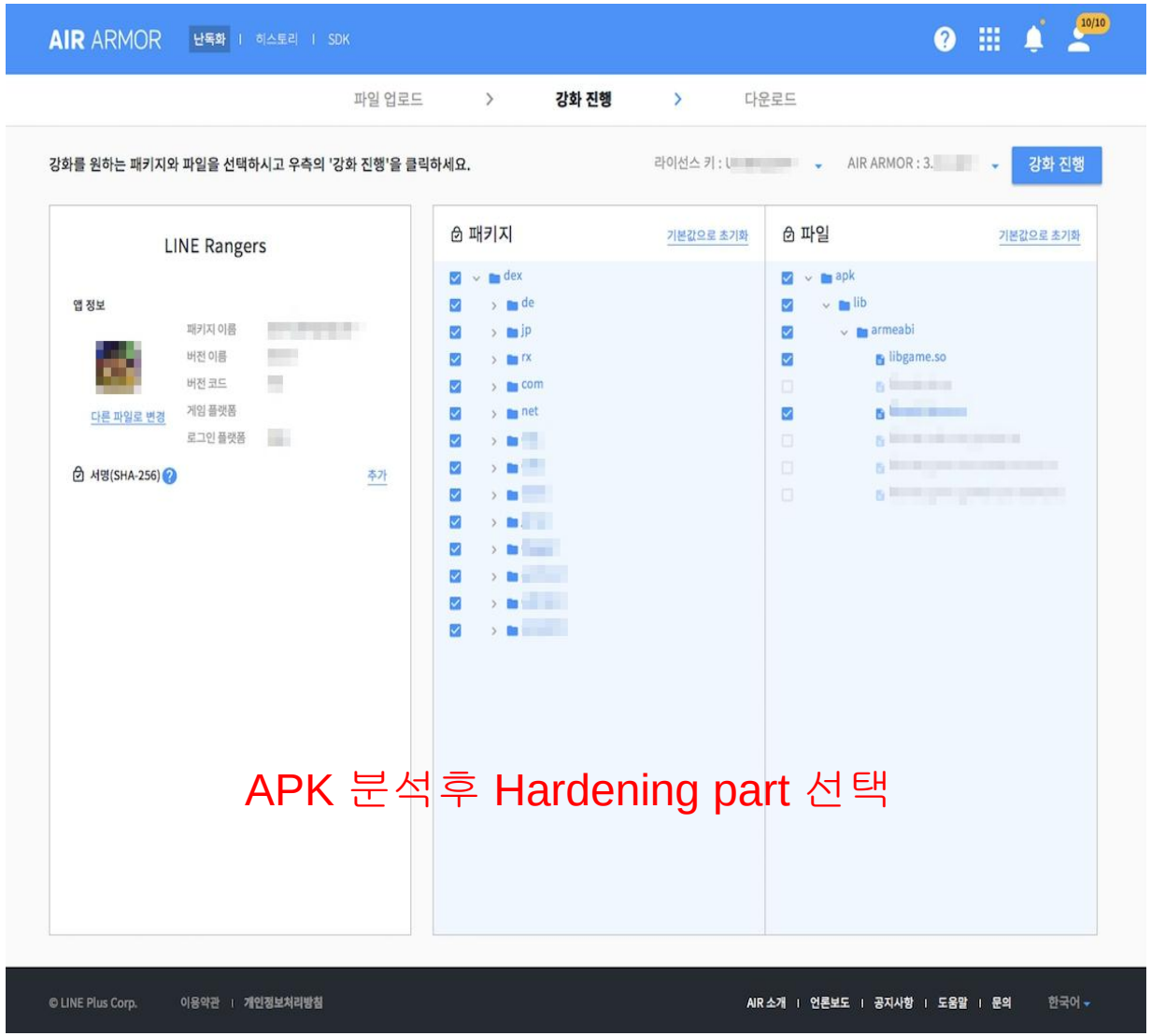


- APK (Android) 대상 Live Protect

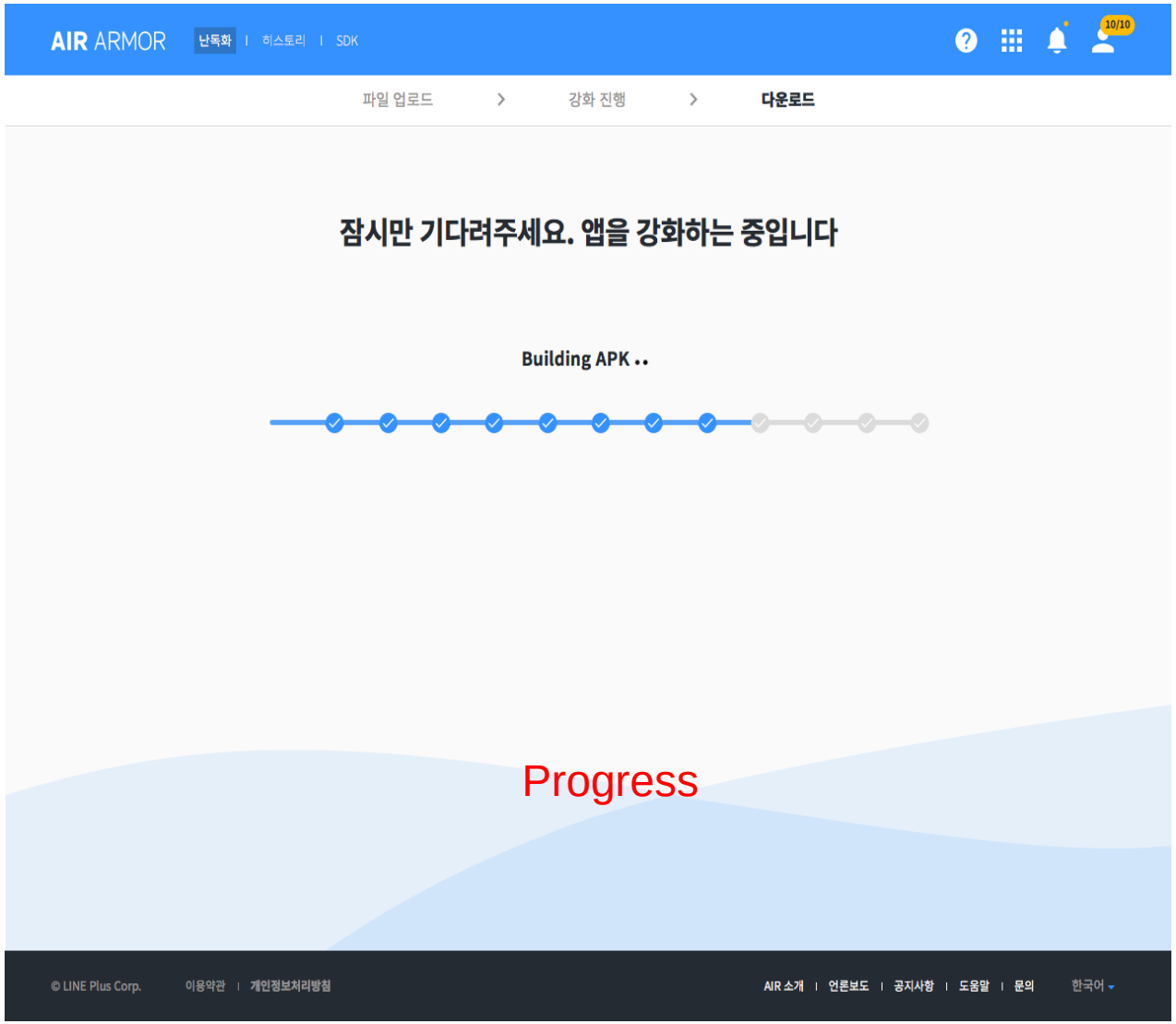
1. APK Upload
2. Structure Analysis
3. Hardening List 추출 및 식별
4. Hardening 진행
   - Dex, So, Dll 난독화
   - Detection Module 삽입
   - Reassemble

- APP 빌드시 자동적용 (라인게임)
- IOS - SDK 제공, AOS – SDK or Live

AIR ARMOR (Protect)

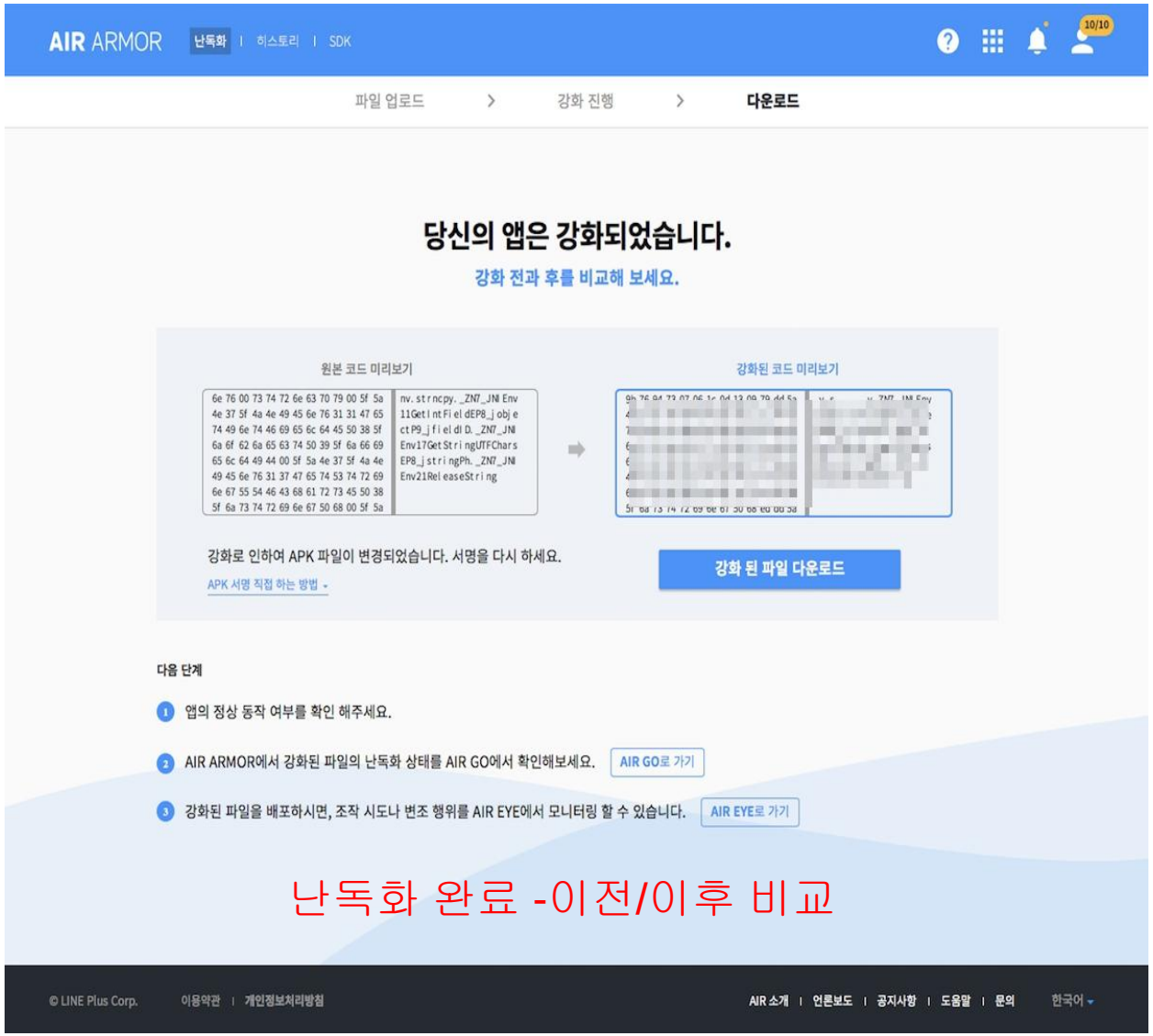


APK 분석후 Hardening part 선택

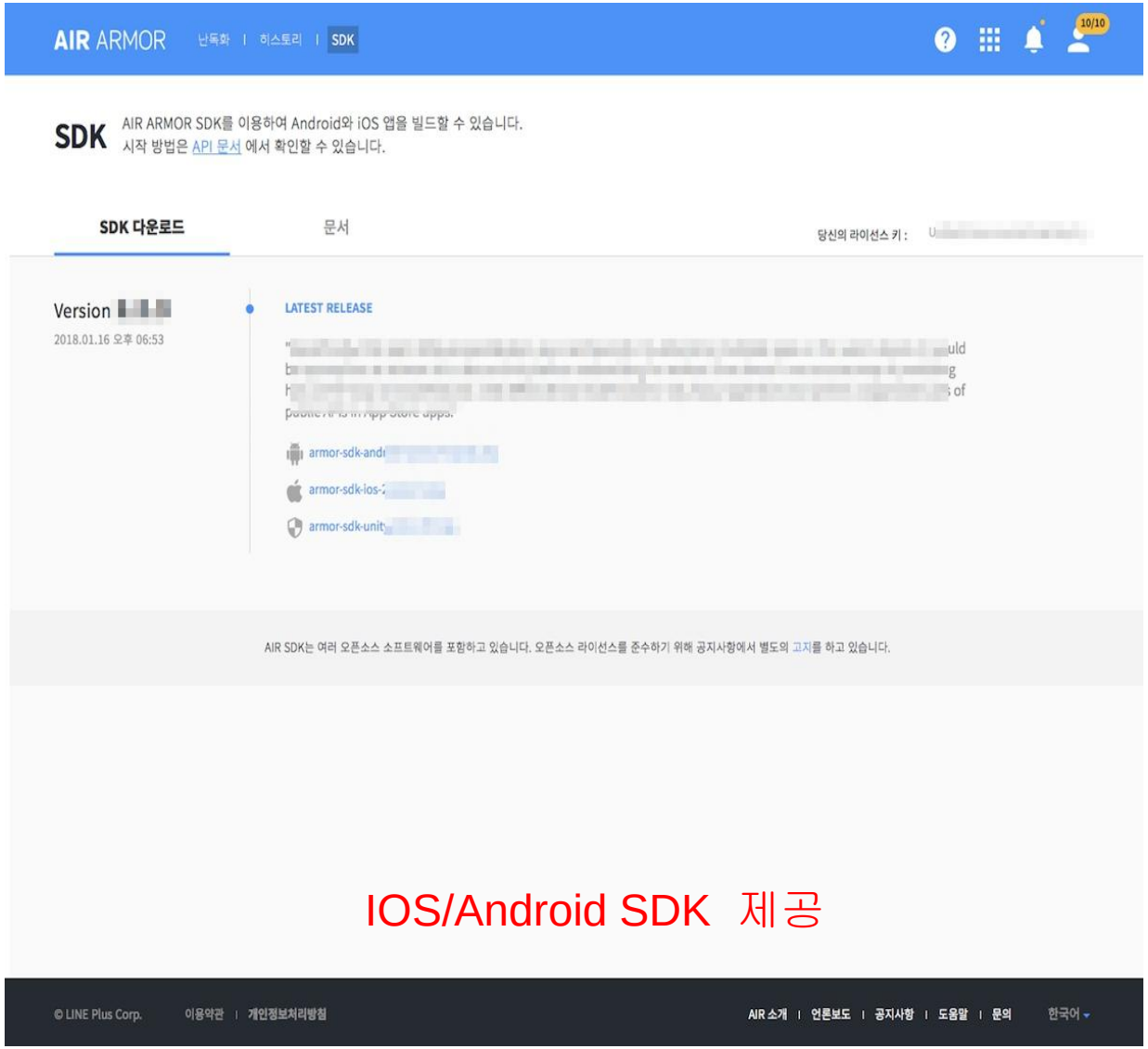


Progress

AIR ARMOR (Protect)



난독화 완료 -이전/이후 비교

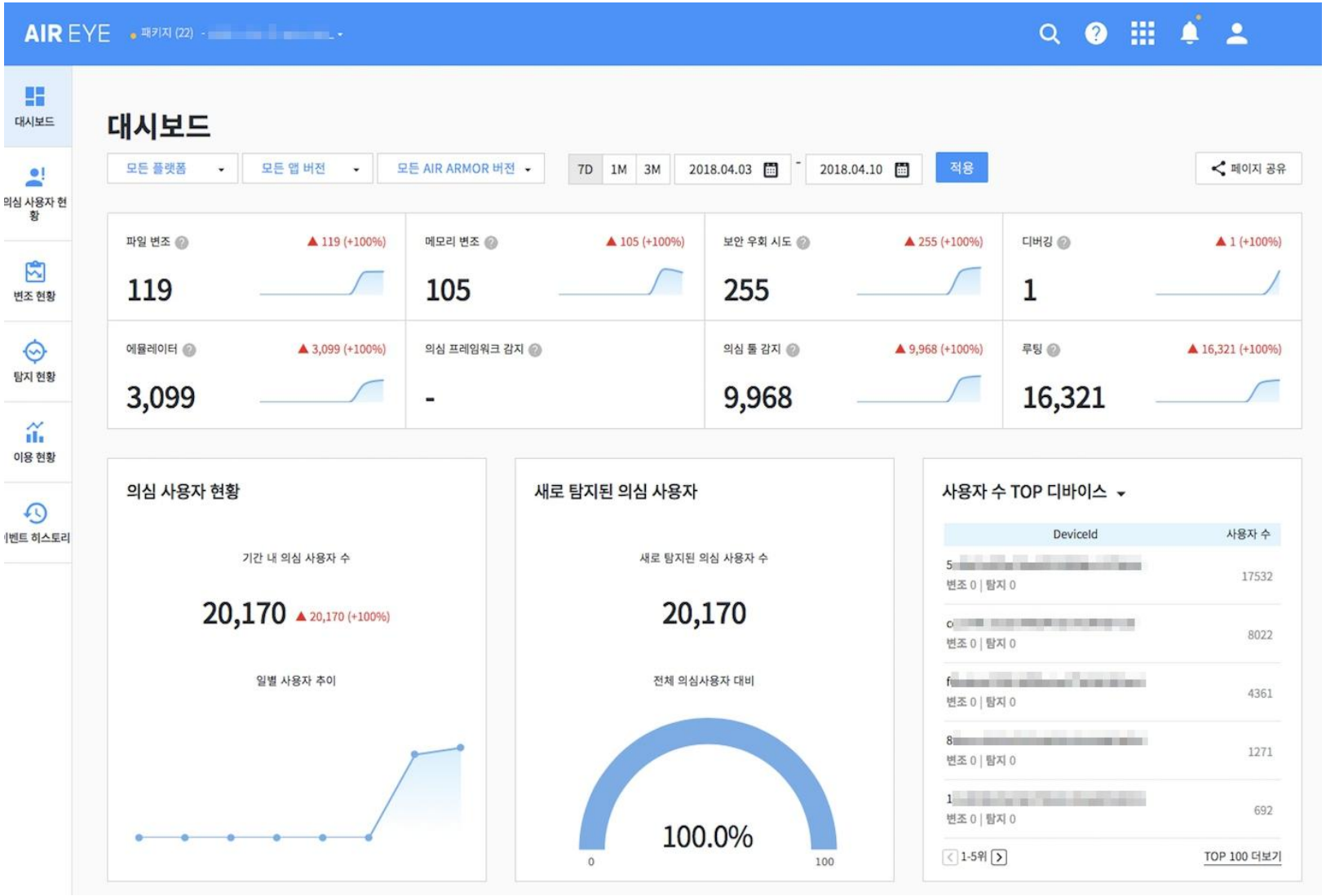


IOS/Android SDK 제공

AIR EYE (Monitoring)

Abuser Monitoring , Relation Analysis , Abusing Detect

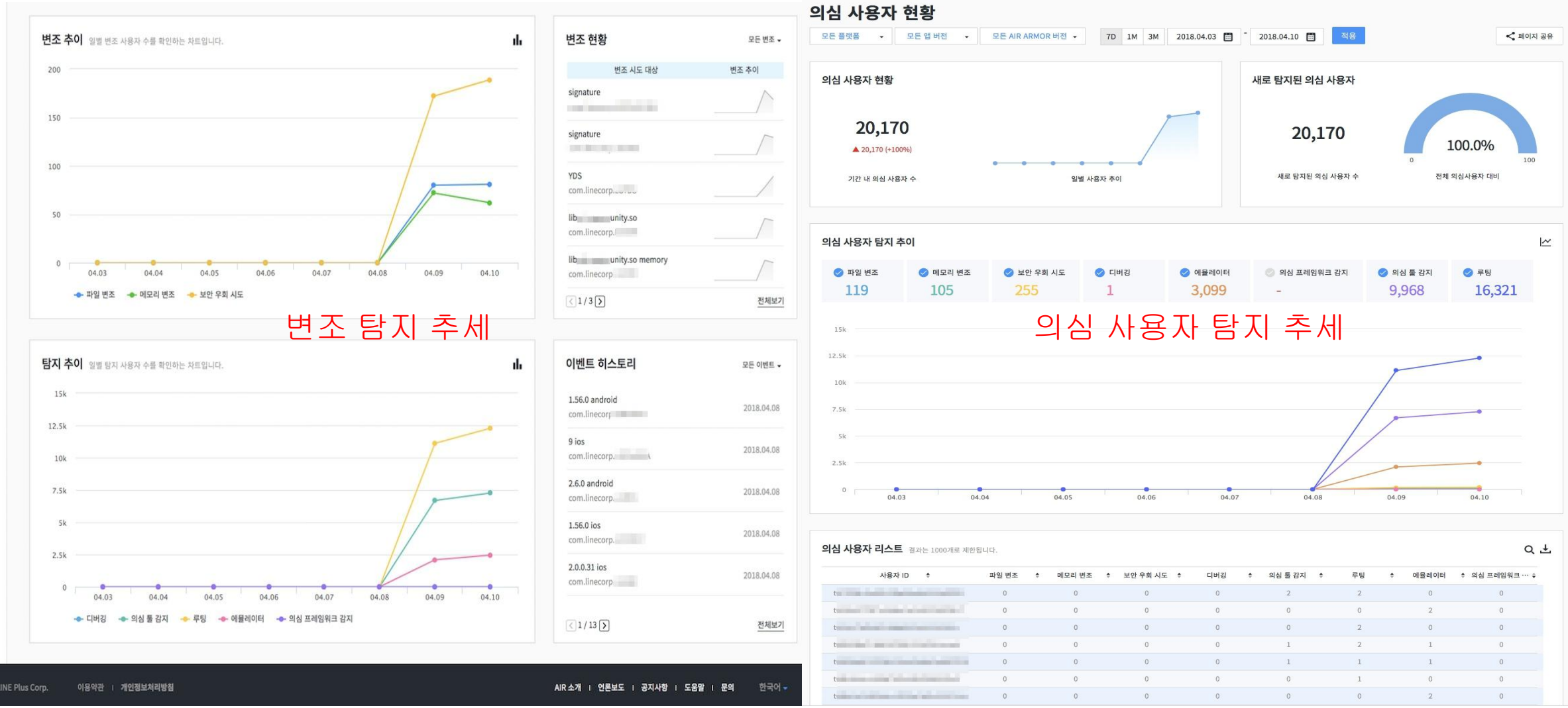
AIR EYE (Monitoring)



패키지별 대쉬보드

- 전체현황
- 의심사용자
- 변조 현황 (파일, 메모리)
- 탐지현황
- 루팅,치팅앱, 에뮬레이터, 디버깅 탐지

AIR EYE (Monitoring)



AIR EYE (Monitoring)

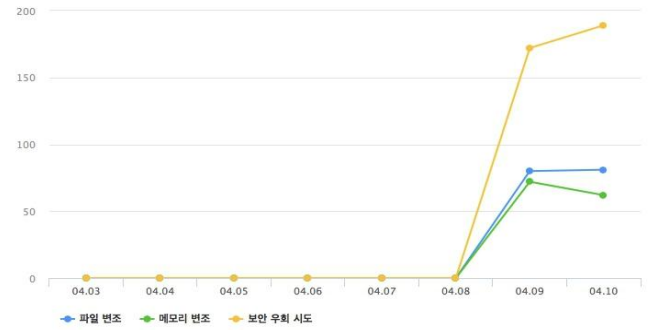
변조 현황

모든 플랫폼 | 모든 앱 버전 | 모든 AIR ARMOR 버전 | 7D | 1M | 3M | 2018.04.03 - 2018.04.10 | 적용

변조 현황

일별 변조 사용자 수를 확인하는 차트입니다.

파일 변조	119	▲119(+100%)
메모리 변조	105	▲105(+100%)
보안 우회 시도	255	▲255(+100%)

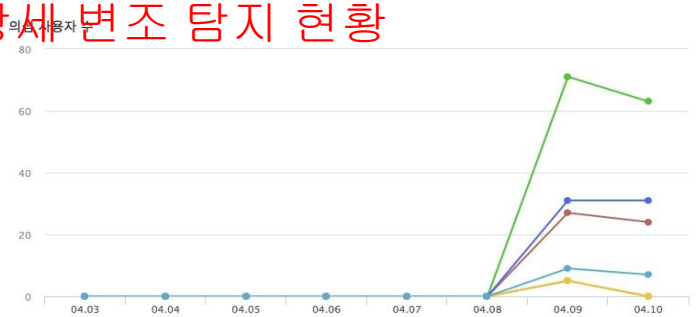


변조 시도 대상별 추이

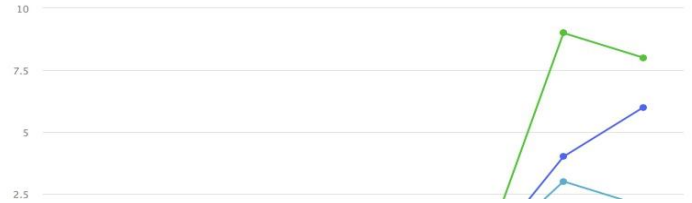
파일 변조
- lib[redacted]unity.so
- signature
- lib[redacted].so
- YDS

메모리 변조
- lib[redacted].so memory
- libgame.so memory
- YDS memory
- lib[redacted]unity.so memory

상세변조 탐지 현황



변조 시도 수



변조 시도 이력

1-17건 조회 중 | 전체 17건

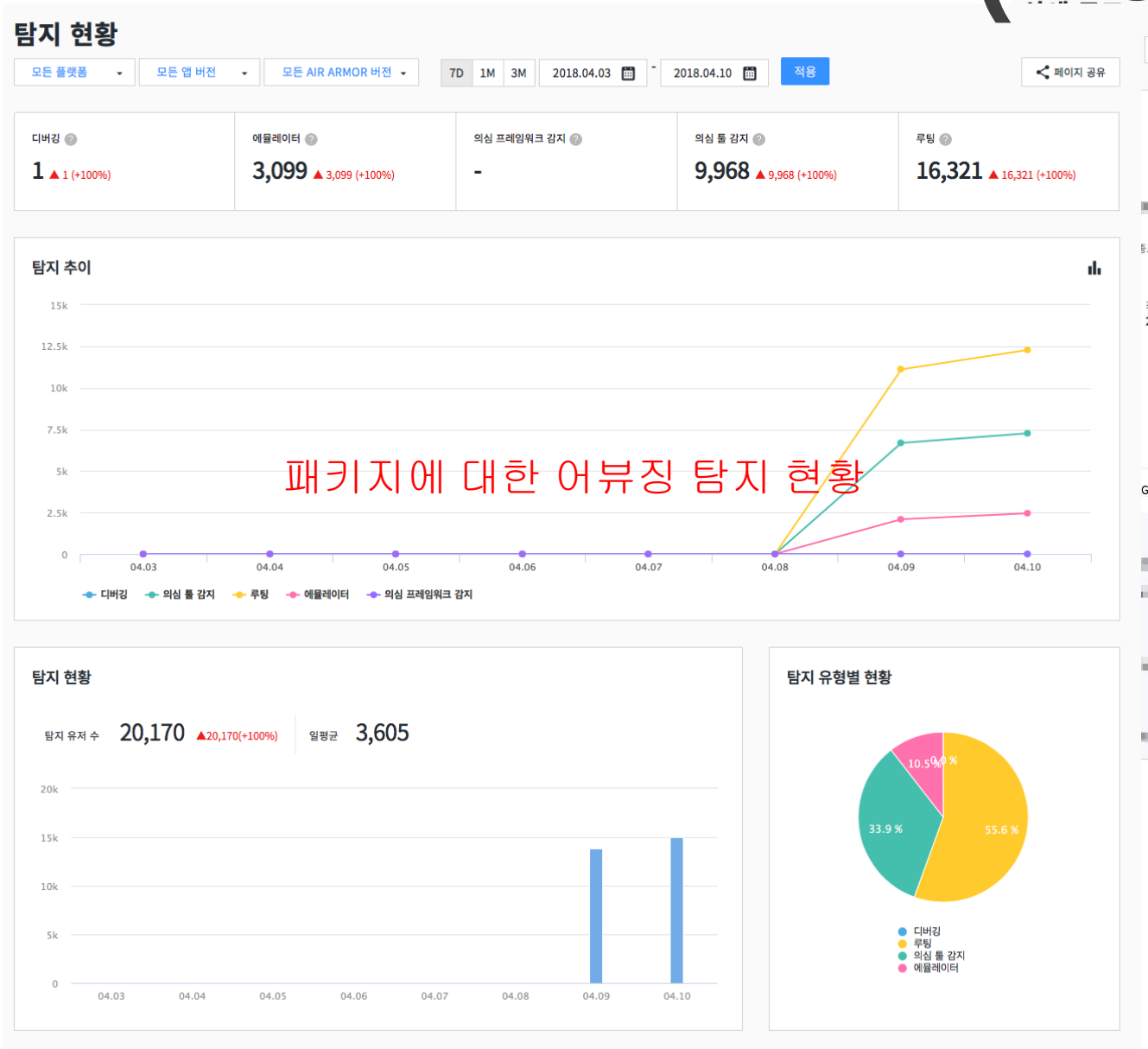
50개씩 보기

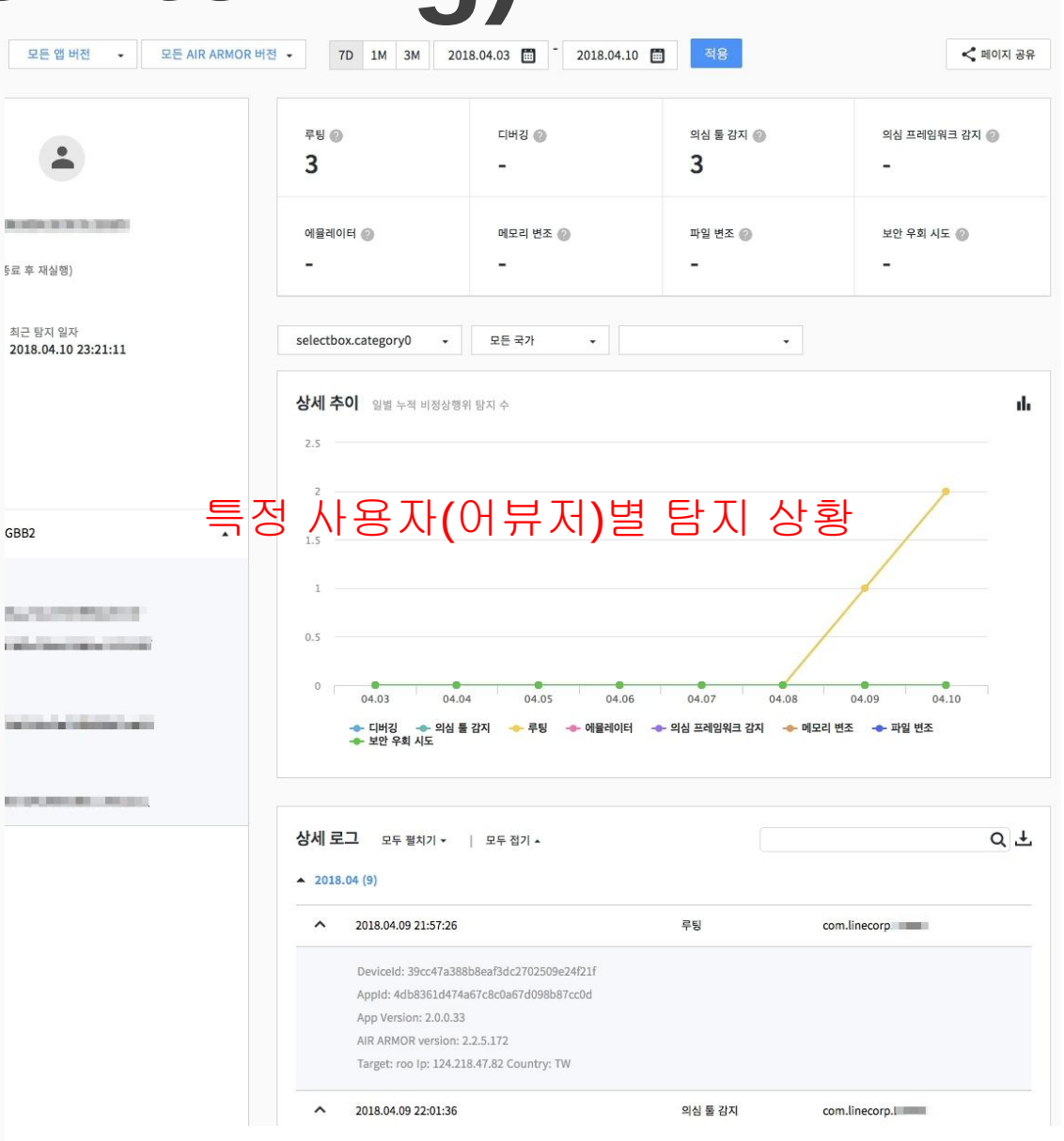
플랫폼	앱 버전	AIR ARMOR 버전	변조 시도 대상	변조 시도 사용자 수
Android	6.1.3	2.1.0	libgame.so memory	53
Android	2.6.0	2.2.3	signature	49
Android	2.6.0	2.2.3	lib[redacted]unity.so memory	33
Android	2.6.0	2.2.3	lib[redacted]unity.so	33
Android	5.2.3	2.2.2.158	signature	19
iOS	1.0.4	2.2.4	[redacted]	17
iOS	1.0.4	2.2.4	[redacted] memory	13
Android	6.1.3	2.2.4	signature	8
Android	1.0.4	2.2.4	signature	6
Android	1.0.5	2.2.4	signature	5
Android	1.0.4	2.2.4	lib[redacted].so memory	5
Android	1.0.4	2.2.4	lib[redacted].so	5
Android	5.2.2	2.2.2.158	signature	4
Android	1.56.0	2.2.2	signature	4
Android	1.1.0	2.2.5	signature	4
iOS	1.0.3	2.2.4	[redacted] memory	1
Android	5.2.1	2.2.2.158	signature	1

1 / 1

패키지별 변조 탐지 현황
- 무엇을 공격 대상으로 하였는가?

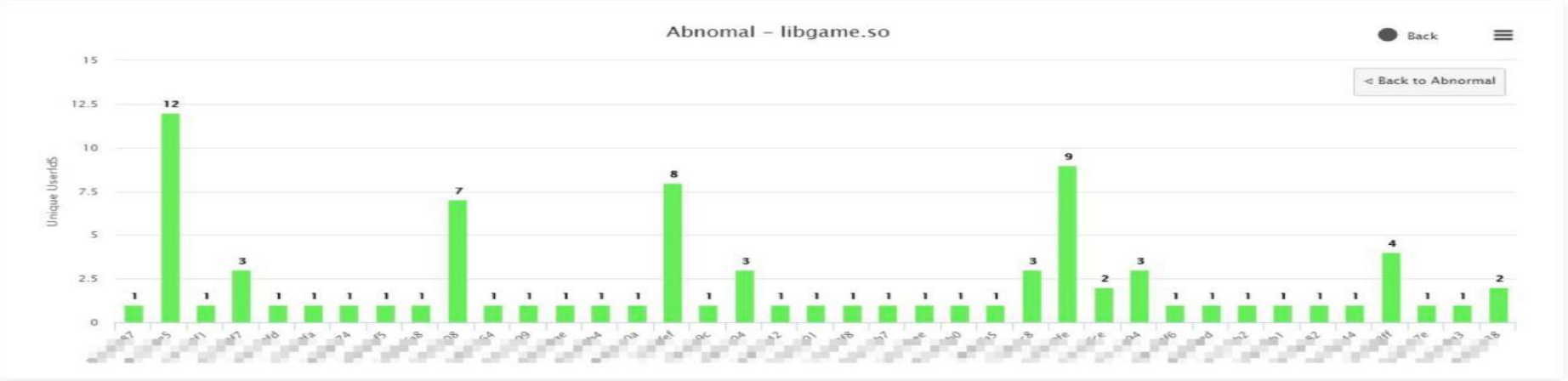
AIR EYE (Monitoring)





AIR (Active Incident Response)

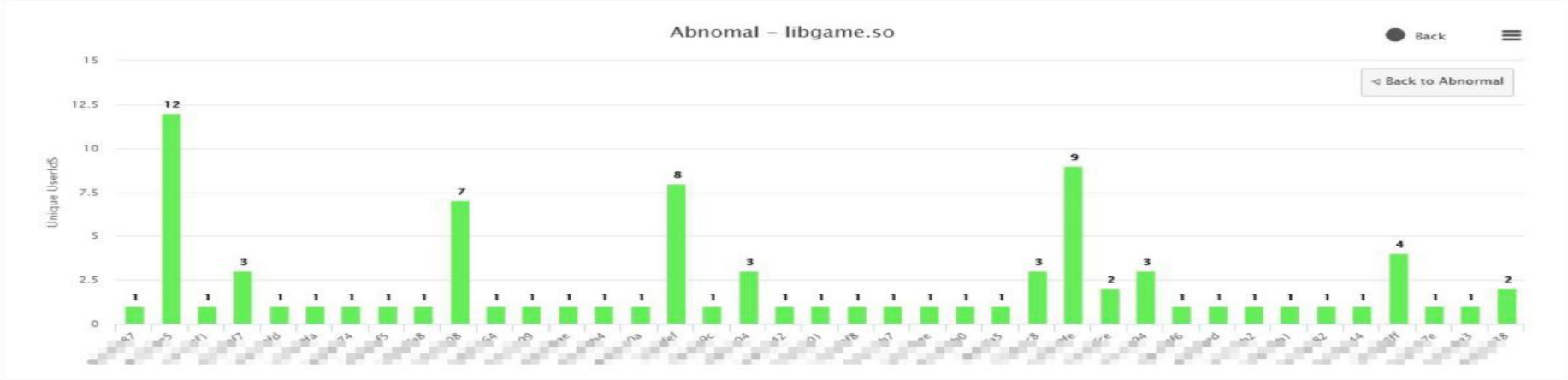
AIR (사례)



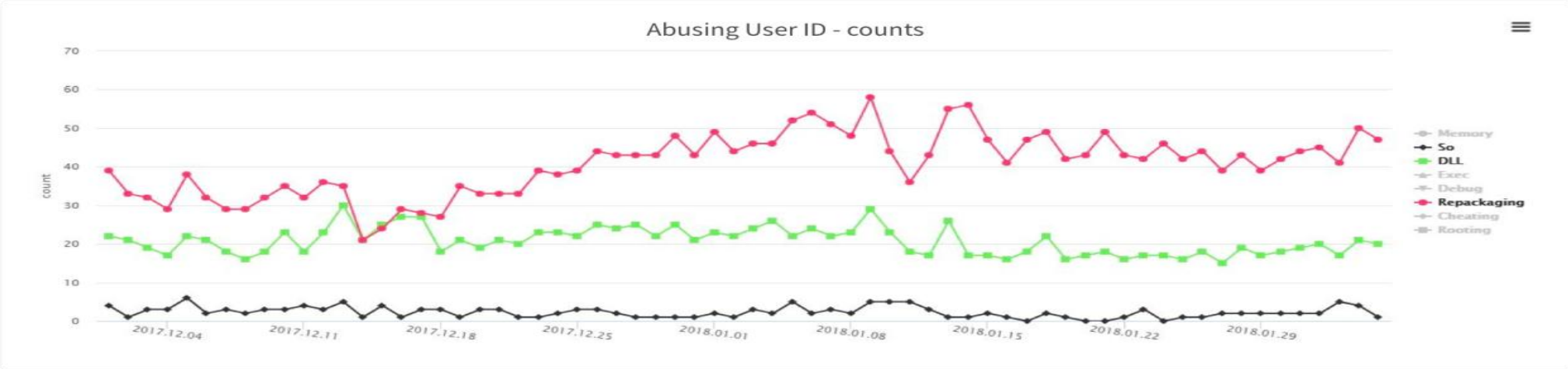
게임 로직이 들어 있는 SO 파일의 해쉬 탐지 (다양한 변조)

게임개발 엔진인 Unity의 각 구성요소별 변조 탐지 통계 - so, dll 변조 및 리패키징

AIR (사례)



게임 로직이 들어 있는 SO 파일의 변형 탐지 (다양한 비정상 버전 존재)



게임개발 엔진인 Unity의 각 구성요소별 변조 탐지 통계 - so, dll 변조 및 리패키징

AIR (사례)

IOS 에 대한 파일 변조도 2017년부터 탐지. 현재 많이 증가됨 (루팅 이후)

Last

Passive -> Active

http://apk.tw
https://androidrepublic.org
https://www.androidthaimod.com/
http://appzzang.ca/

주요 치팅앱 유통 커뮤니티 사이트.
…

모바일에서도 이미 유료화, 비즈니스 모델, 해킹툴 및 아이템 판매는 일상적

모바일 기술적 보호 대응 -> OS 의 기능 제한 으로 어려움.

문제를 사전에 제거하고, 분석하기 어렵게 만들며, 어뷰저를 모니터링 해야...

Active Incident Response (AIR) https://air.line.me

THANK YOU