



Mobile Security Paradigm Shift



2018 LINE Plus Game Security

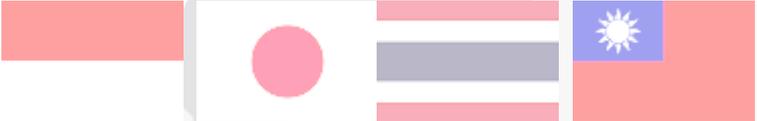
800,000,000

70,000,000

Disney tsumtsum

50,000,000

Rangers



15,000,000

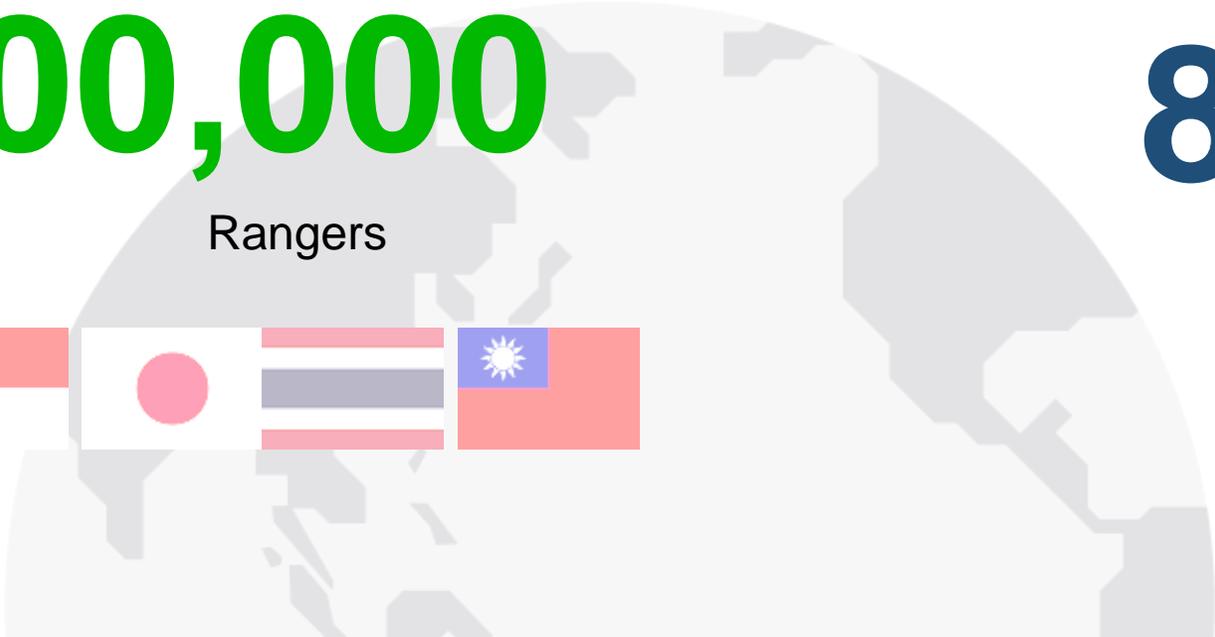
AU

200G

Security Data

84

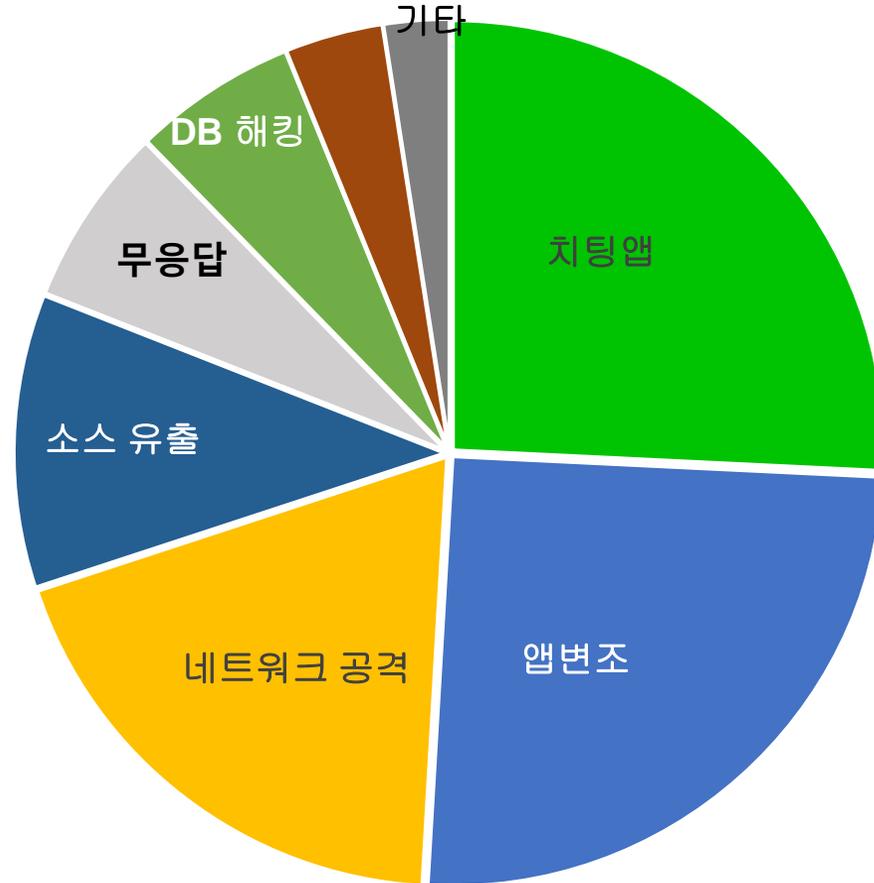
Game



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

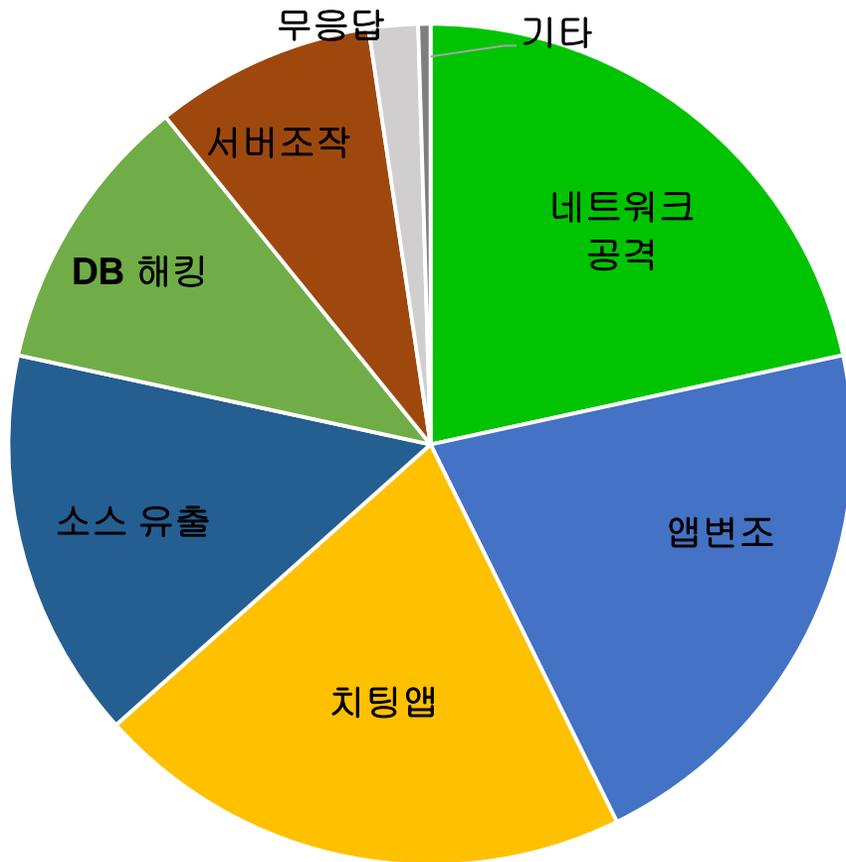


모바일 앱에서 해킹 대응 이슈가 있다면?

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)

Game Security Status



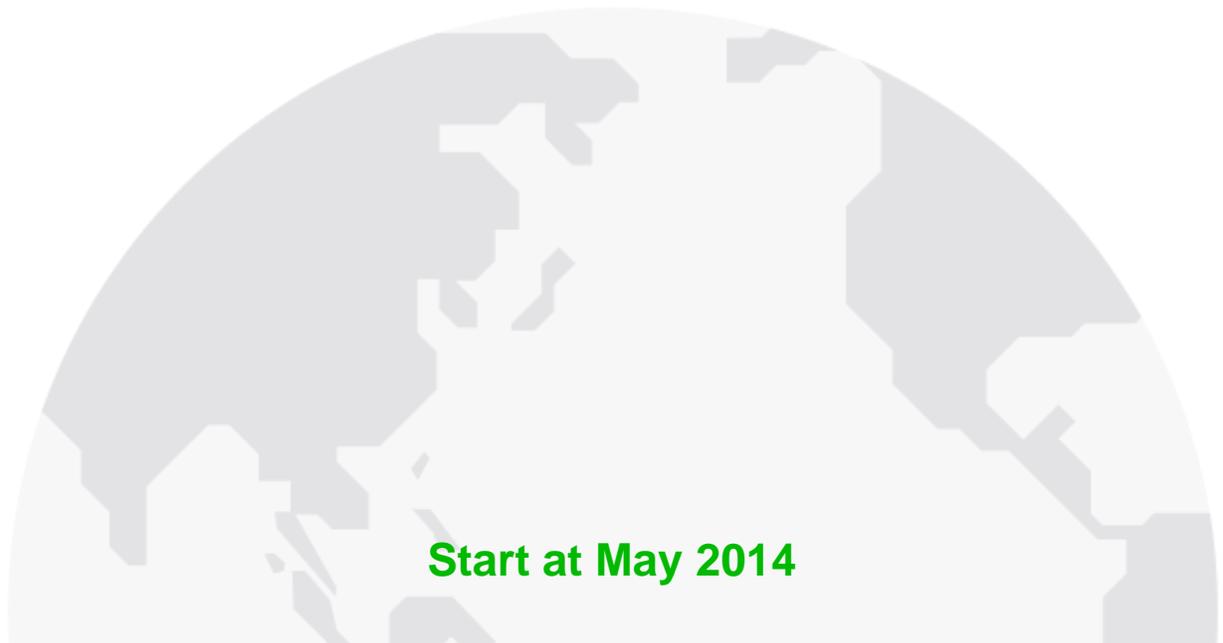
앱 개발시 가장 보안적으로 우려 되는 부분은?

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%



2014

We must build basic!



Start at May 2014

Mission

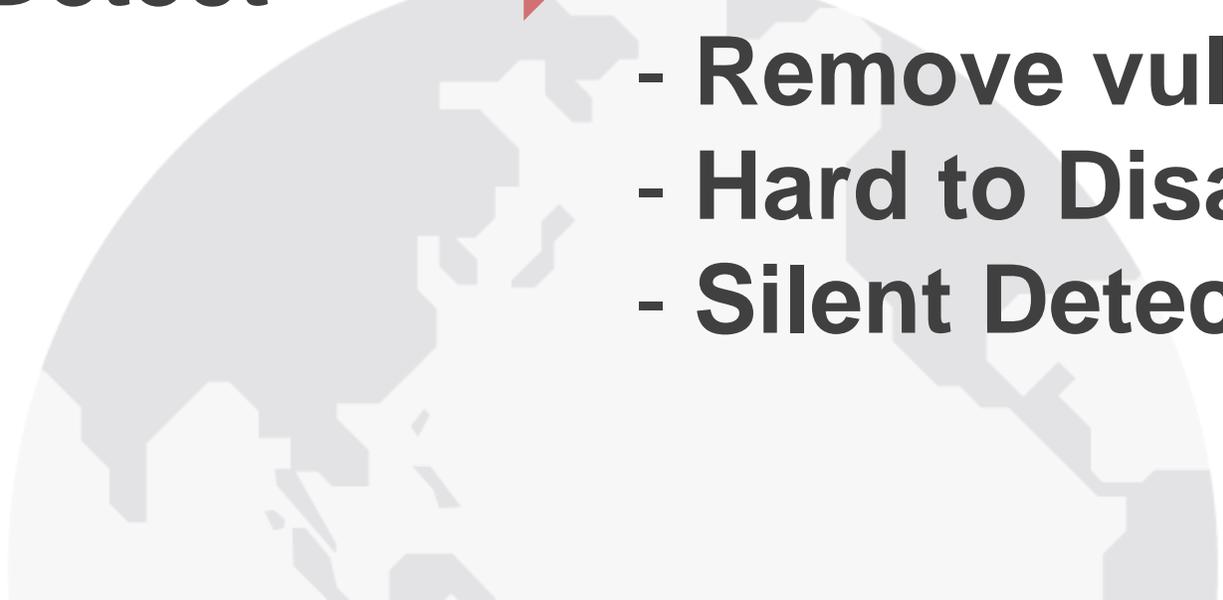
- 메모리 조작을 막을 수 있는가?
- 변조된 앱을 이용한 **Abuser**를 탐지할 수 있는가?
- 개발된 앱은 쉽게 분석되지 않도록 하며, 중요 로직은 보호한다.
- 앱 출시 이전에 근본 취약성을 제거 할 수 있을까?
(Open Source, CVE 취약성 등)
- 온라인에서 자동으로 진단하고, 보호하며, **Abuser**를 탐지하는 것이 가능할까?

Game Security Mission

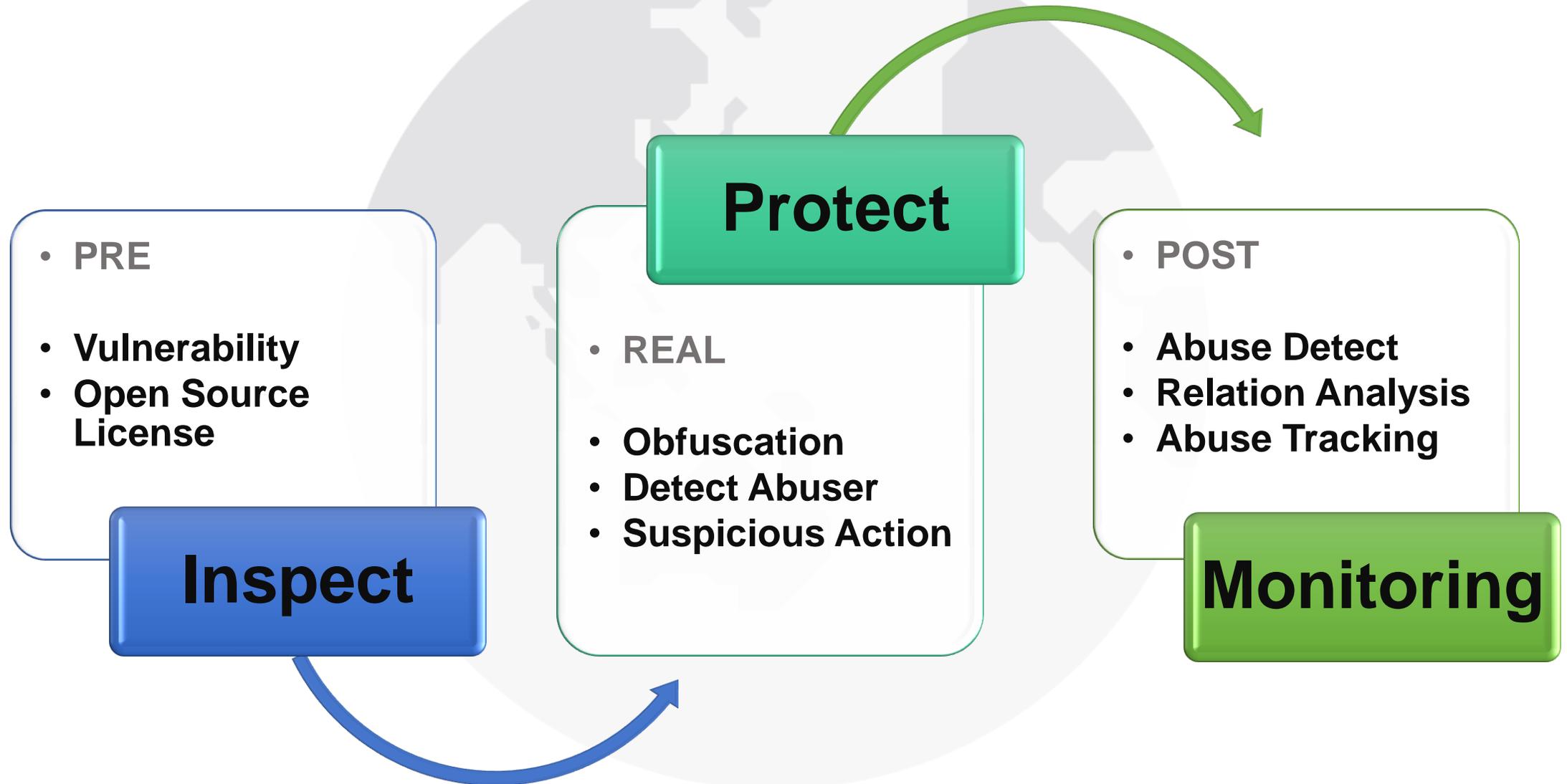
Passive Response  **Active Incident Response**

Log Base Detect  **Pre Protect**

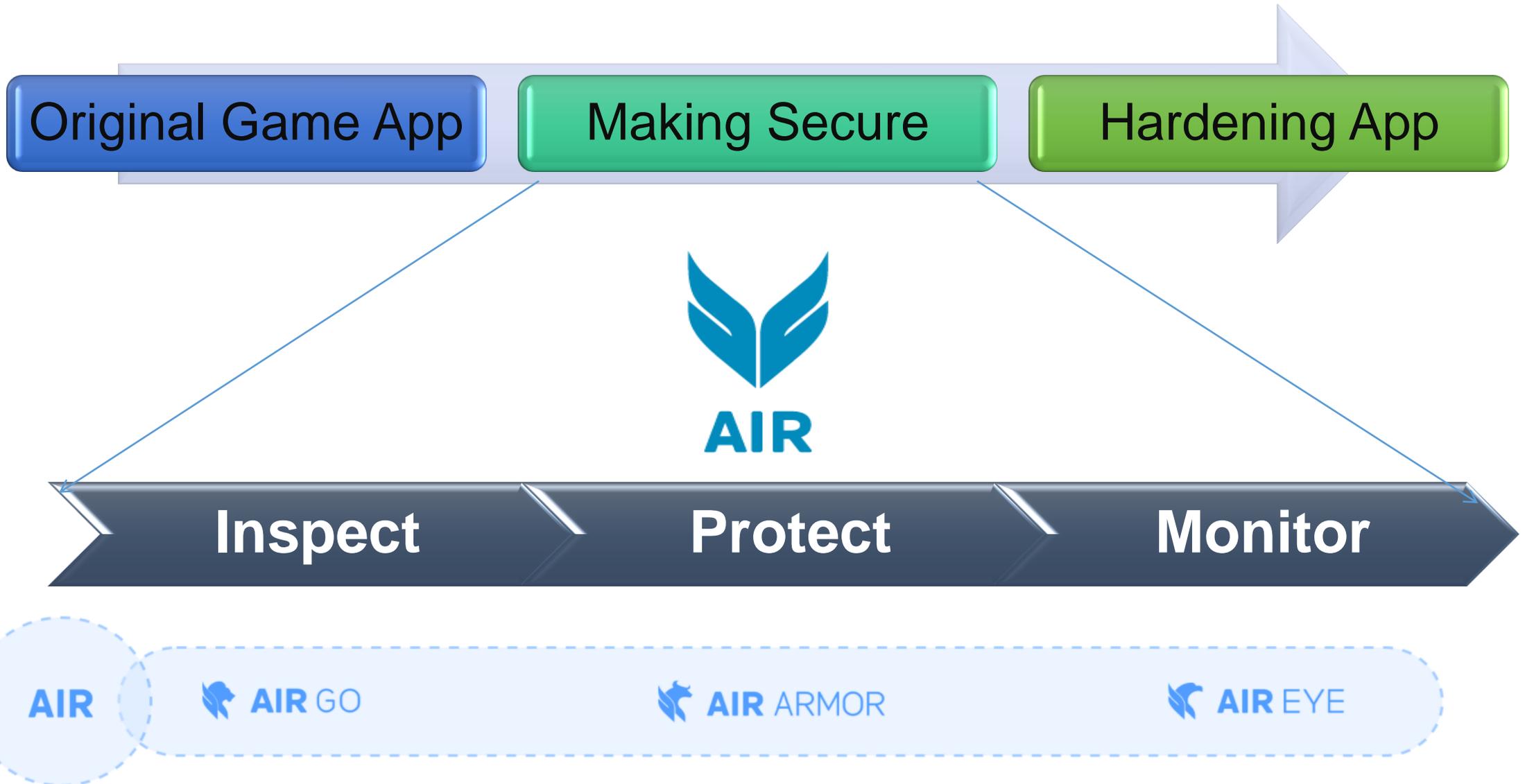
- Remove vulnerability
- Hard to Disassemble
- Silent Detect



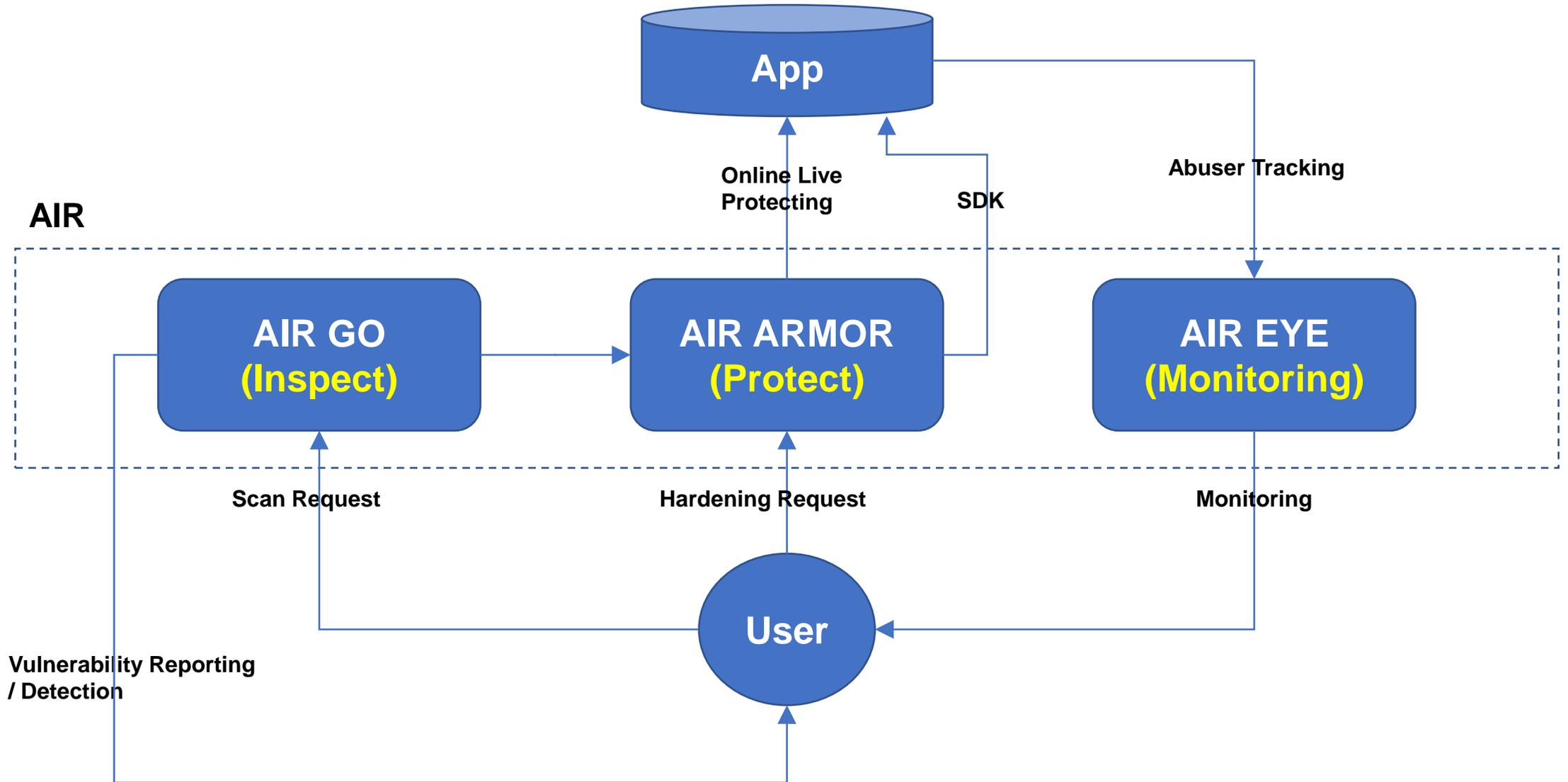
Making Security Process



Active Incident Response



AIR Flow Diagram

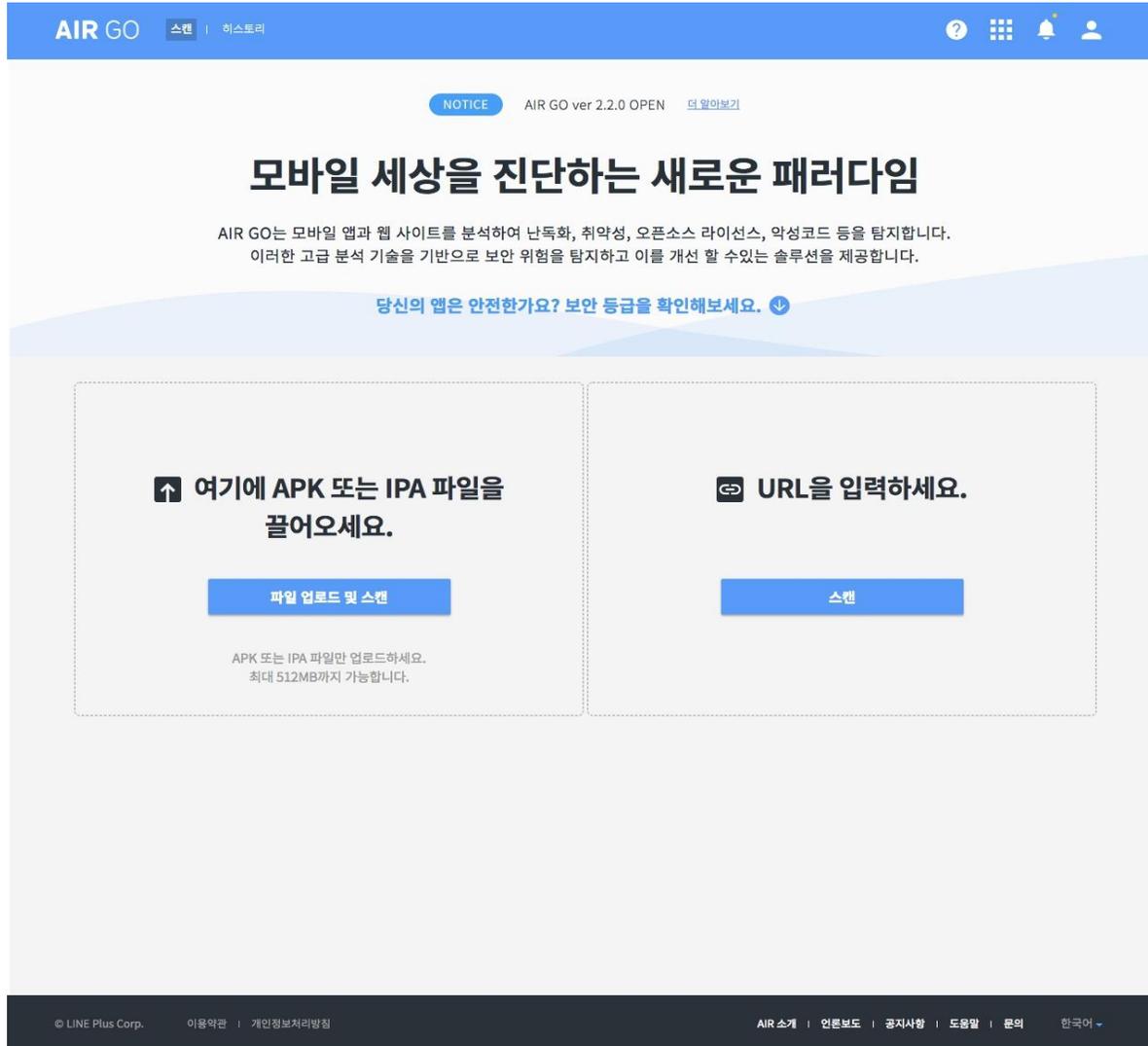


AIR GO (Inspect)

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)

AIR GO 스캔 결과 | 히스토리

보안 등급

패키지 히스토리

WARNING

2018.03.20에 스캔됨
AIR GO 버전 2.2.0
패턴 엔진 버전 2018.03.16.1

SNOW_7.2.4.apk [다운로드]

패키지 ID	388efb1527f9373c44d90cd5071c7261d2a0ea130041d9278bd0e5ee47edf19d
패키지 이름	com.campmobile.snow
앱 버전	7.2.4
플랫폼	Android
요청 IP	10.67.138.7

요약 • **난독화** • 취약점 • 라이선스 • 악성코드 • 인증 • 구조

이 정보는 법적 분쟁 발생시 법률적 해석이나 논리로 활용될 수 없습니다. [PDF 다운로드]

보안 등급 상세

난독화	취약점	오픈소스 라이선스	악성코드
18 난독화 미적용	0 1 5 CRITICAL WARNING NORMAL	4 18 반환 의무 반환 의무 불필요	발견된 악성코드 없음

솔루션 & 가이드라인

난독화

상세 보기

18개의 파일에 난독화가 적용되어 있지 않습니다.
강력한 보안을 원하신다면 AIR ARMOR를 통해 난독화하세요.

[AIR ARMOR로 가기](#)

취약점

WARNING

setWebContentsDebuggingEnabled
배포하기 전에 이 코드는 반드시 제거합니다.

참조:
<https://developers.google.com/web/tools/chrome-devtools/remote-debugging/webviews>

상세 보기

오픈소스 라이선스

상세 보기

4개의 반환 의무 오픈소스 라이선스가 발견되었습니다.
코드 공개 의무가 있습니다.

악성코드

악성코드가 발견되지 않았습니다.

© LINE Plus Corp. 이용약관 | 개인정보처리방침 | AIR 소개 | 인문보드 | 공지사항 | 도움말 | 문의 | 한국어

진단 결과

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

AIR GO (Inspect)

AIR GO
스캔 결과 | 히스토리

보안 등급
패키지 히스토리



CRITICAL

2018.04.05에 스캔됨
AIR GO 버전 2.2.0
패턴 엔진 버전 2018.03.22.0

AirRyue.apk ↓

패키지 ID: 58bf30e9953bd49bf4228655ba559c9167f0c5c4ef38cc2230b7de455361cd
 패키지 이름: com.linecorp.airgo.ndkapplication
 앱 버전: 1.0
 플랫폼: Cocos2d
 요청 IP: 10.87.138.45

요약
난독화
취약점
라이선스
악성코드
인증
구조

취약점

이 정보는 법적 분쟁 발생시 법률적 해석이나 논리로 활용될 수 없습니다.

23 CRITICAL
8 WARNING
18 NORMAL

- ApacheCordova (CVE-2014-3500)
- ApacheCordova (CVE-2014-3501)
- ApacheCordova (CVE-2014-3502)
- ApacheCordova (CVE-2015-1835)
- ApacheCordova (CVE-2015-5256)
- Fragment Injection
- GnuTLS (CVE-2014-3466)
- Insecure Hostname Verification
- LibCurl (CVE-2009-2417)
- LibCurl (CVE-2012-0036)
- Libupnp (CVE-2012-5958)
- OpenSSL (CVE-2014-0160)
- OpenSSL (CVE-2015-0204)
- OpenSSL (CVE-2015-3194, CVE-2014-0224)
- OpenSSL (CVE-2016-0701)
- OpenSSL (CVE-2016-0703)
- OpenSSL (CVE-2016-0800)
- OpenSSL (CVE-2016-2107)
- OpenSSL (CVE-2016-2108)
- OpenSSL (CVE-2016-6304)
- SSLErrorHandler
- Supersonic Ad SDK
- libpng (CVE-2015-8540)
- Application might include private keys or o...
- Developer URL Leaked Credentials
- Dynamically adding JavaScript bridge met...
- Embedded Keystore files
- Insecure Cipher
- RSA NoPadding
- ShareUserId
- setWebContentsDebuggingEnabled
- AppDebuggingEnabled
- Automatic backup is allowed (android:allo...
- Custom permission with insecure protectio...
- Debug logging in production
- Dynamic class loadname (DexClassLoader)

CRITICAL

ApacheCordova (CVE-2014-3500)

취약성

설명
Apache Cordova Android 3.5.1 이 버전에서 발견된 취약점으로, 공격자가 의도적으로 변조한 intent URL을 통해 시작 페이지를 변경할 수 있습니다.

참조:
<https://cordova.apache.org/announcements/2014/08/04/android-351.html>

솔루션 & 가이드라인
Apache Cordova 3.5.1 버전 또는 상위 버전의 라이브러리를 적용합니다.

다운로드:
<https://cordova.apache.org/docs/en/latest/guide/platforms/android/upgrade.html>

Google Play 등록 거부 사유:
<https://support.google.com/flags/answer/6325474?hl=ko>

탐지 상세

existfield	domain	Log.apache.cordova
target	path	Device.java
	field	cordovaVersion
matched value	2.4.0	

© LINE Plus Corp.
이용약관
개인정보처리방침
AIR 소개
업론보도
공지사항
도움말
문의
한국어

AIR GO
스캔 결과 | 히스토리

보안 등급
패키지 히스토리



WARNING

2018.03.20에 스캔됨
AIR GO 버전 2.2.0
패턴 엔진 버전 2018.03.16.1

SNOW_7.2.4.apk ↓

패키지 ID: 388efb1527f9373c44d90cd5071c7261d2a0ea130041d9278bd0c5ee47edf19d
 패키지 이름: com.campmobile.snow
 앱 버전: 7.2.4
 플랫폼: Android
 요청 IP: 10.87.138.7

요약
난독화
취약점
라이선스
악성코드
인증
구조

오픈소스 라이선스

이 정보는 법적 분쟁 발생시 법률적 해석이나 논리로 활용될 수 없습니다.

4 반환 의무 18 반환 의무 불필요

반환 의무	오픈소스 라이선스
OSS (모듈 경로)	오픈소스 라이선스
FFmpeg/libavcodec (lib/armeabi-v7a/libffmpegencoder.so)	GNU General Public License version 2.0 (GPLv2) GNU Library or Lesser General Public License (LGPLv2...)
FFmpeg/libavfilter (lib/armeabi-v7a/libffmpegencoder.so)	GNU General Public License version 2.0 (GPLv2) GNU Library or Lesser General Public License (LGPLv2...)
FFmpeg/libavformat (lib/armeabi-v7a/libffmpegencoder.so)	GNU General Public License version 2.0 (GPLv2) GNU Library or Lesser General Public License (LGPLv2...)
FFmpeg/libswscale (lib/armeabi-v7a/libffmpegencoder.so)	GNU General Public License version 2.0 (GPLv2) GNU Library or Lesser General Public License (LGPLv2...)
반환 의무 불필요	오픈소스 라이선스
OSS (모듈 경로)	오픈소스 라이선스
Android SDK (Lcom/google/android/gms/common/api/GoogleApiActivity; &titnit>)	Apache License 2.0
Apache Commons Lang (Lorg/apache/commons/lang3/CharSet; getInstance)	Apache License 2.0
boost (lib/armeabi-v7a/libffmpegencoder.so)	Boost Software License (BSL1.0)
conceal (lib/armeabi-v7a/libstport_shared.so)	3-clause BSD License (BSD-3-Clause)
facebook-android-sdk (Lcom/facebook/AccessToken\$2; createFromParcel)	Facebook Custom License
fmt (lib/armeabi-v7a/libffmpegencoder.so)	2-clause BSD License (BSD-2-Clause)
glyphy (lib/armeabi-v7a/libkuru.so)	Apache License 2.0

© LINE Plus Corp.
이용약관
개인정보처리방침
AIR 소개
업론보도
공지사항
도움말
문의
한국어

AIR GO (Inspect)

AIR GO
스캔 결과 | 히스토리

보안 등급

스캔 ID: 2a82a1d397e477d09f0262e26cb781b288d5dfc086281e58a414a7f5352d03

웹 사이트 URL: http://digital-imaging.co.kr

요청 IP: 10.87.138.4

지역: Republic of Korea (위도 37.5112 / 경도 126.9741)

서버 IP: 1.255.226.52

스캔 결과

78 CRITICAL 4 SAFE

- digital-imaging.co.kr/group/monster-wallpaper
- digital-imaging.co.kr/group/multi-wallpaper
- digital-imaging.co.kr/group/nargis-wallpaper
- digital-imaging.co.kr/group/philis-wallpaper
- digital-imaging.co.kr/group/pictures-for-screen-bac
- digital-imaging.co.kr/group/pro-tos-wallpaper
- digital-imaging.co.kr/group/rain-drops-wallpaper
- digital-imaging.co.kr/group/scorpion-wallpapers
- digital-imaging.co.kr/group/skull-backgrounds
- digital-imaging.co.kr/group/solar-system-background
- digital-imaging.co.kr/group/south-indian-girl-wallp
- digital-imaging.co.kr/group/spiderman-1-wallpaper
- digital-imaging.co.kr/group/the-amazing-spider-ma
- digital-imaging.co.kr/group/the-simpsons-hd-wallp
- digital-imaging.co.kr/group/to-aru-majutsu-no-inde
- digital-imaging.co.kr/group/tokyo-wallpapers
- digital-imaging.co.kr/group/volcano-eruption-wallp
- digital-imaging.co.kr/group/wallpaper-bodybuilding
- digital-imaging.co.kr/group/wallpaper-moto-cross
- digital-imaging.co.kr/group/wallpaper-under-water
- digital-imaging.co.kr/group/wallpapers-hd-for-tablet
- digital-imaging.co.kr/group/wallpapers-of-love-hearts
- digital-imaging.co.kr/group/waters-wallpapers
- digital-imaging.co.kr/group/windows-8-official-wall
- digital-imaging.co.kr/group/wmba-wallpaper
- digital-imaging.co.kr/group/zhang-ziyi-wallpapers
- digital-imaging.co.kr/style.css
- digital-imaging.co.kr/tpl/css/fonts.css
- digital-imaging.co.kr/tpl/css/imgareaselect-animate
- digital-imaging.co.kr/tpl/js/jquery.imgareaselect.pa
- digital-imaging.co.kr/www.liveinternet.ru/click
- code.jquery.com/jquery-1.11.2.min.js
- code.jquery.com/jquery-migrate-1.2.1.min.js
- fonts.googleapis.com/css?family=Tillium+Web:400
- www.zgm-org.com

CRITICAL

digital-imaging.co.kr/www.liveinternet.ru/click

탐지 상세

호출자	http://www.zgm-org.com
호출 URL	http://www.zgm-org.com
호출 방법	Safe Browsing APIs

이 정보는 업적 분쟁 발생 시 법원적 해석이나 논리로 활용될 수 있습니다.

© LINE Plus Corp. | 이용약관 | 개인정보처리방침 | AIR 소개 | 언론보도 | 공지사항 | 도움말 | 문의 | 한국어

AIR GO
스캔 | 히스토리

히스토리

최근 1년간 히스토리 조회가 가능합니다.

100개의 스캔 결과

이름	시간	난독화	취약점	라이선스	악성코드	등급
golang_sample.apk org.golang.todo.main	19시간 전	난독화	취약점	라이선스	악성코드	NORMAL
http://digital-imaging.co.kr	2018.04.09 오전 11:40	-	-	-	-	CRITICAL
AirRyue.apk com.linecorp.airgo.ndkapplication	2018.04.05 오전 09:31	난독화	취약점	라이선스	악성코드	CRITICAL
http://www.tongkooktds.net	2018.04.05 오전 09:29	-	-	-	-	CRITICAL
http://www.google.com	2018.04.04 오전 10:06	-	-	-	-	SAFE
http://www.daum.net	2018.04.03 오후 05:36	-	-	-	-	CRITICAL
http://www.naver.com	2018.04.03 오후 05:34	-	-	-	-	CRITICAL
Malware_Test.apk com.example.lineplus.ndktest2	2018.03.20 오후 05:07	난독화	취약점	라이선스	악성코드	CRITICAL
bsixonetwo-android-7.2.4-snow-norm-armAll-a...	2018.03.20 오전 11:44	난독화	취약점	라이선스	악성코드	WARNING
bsixonetwo-android-7.2.2-snow-norm-armAll-a...	2018.03.19 오후 02:17	난독화	취약점	라이선스	악성코드	WARNING
Bsixonetwo_ios_5.4.1.0.ipa com.linecorp.b612	2018.03.13 오전 11:11	난독화	취약점	라이선스	악성코드	NORMAL
Studio_644_158.ipa com.snowcorp.studio.644.beta	2018.03.13 오전 11:19	난독화	취약점	라이선스	악성코드	NORMAL
linecamera_ios_14.0.3.ipa jp.naver.linecamera	2018.03.12 오후 05:39	난독화	취약점	라이선스	악성코드	NORMAL
라-자IM_v1.0.3...apk com.ncsoft.lineagem	2018.03.08 오전 10:26	난독화	취약점	라이선스	악성코드	WARNING
LGYDS_1.0.0_staging_201803022058.apk com.linecorp.LGYDS	2018.03.07 오후 02:15	난독화	취약점	라이선스	악성코드	CRITICAL
bsixonetwo-android-7.1.3-snow-norm-armAll-a...	2018.03.07 오후 02:03	난독화	취약점	라이선스	악성코드	CRITICAL
bsixonetwo-android-5.5.1-prc-norm-release-20...	2018.03.07 오후 02:01	난독화	취약점	라이선스	악성코드	WARNING
HeroesConflict.ipa com.linecorp.inhouse.LGMR	2018.03.05 오후 04:13	난독화	취약점	라이선스	악성코드	NORMAL
LGYDS_BillingTest_1.0.0_sandbox_2018030215...	2018.03.05 오후 02:46	난독화	취약점	라이선스	악성코드	CRITICAL
lineprojectr-beta-0.0.1.apk com.linecorp.lgpjr	2018.03.05 오전 09:58	난독화	취약점	라이선스	악성코드	CRITICAL

1
2
3
4
5

© LINE Plus Corp. | 이용약관 | 개인정보처리방침 | AIR 소개 | 언론보도 | 공지사항 | 도움말 | 문의 | 한국어

진단 - History

AIR GO (Inspect-ref)

Google Play Top 100 앱 보안 등급

2018. 03

US: 66, Korea: 41, Japan: 56

Google Play Store Top 100 앱의 취약성

취약점	등급	진단된 앱의 개수
TrustManager Verification	CRITICAL	29
Insecure Hostname Verification	CRITICAL	9
SSLErrorHandler	CRITICAL	7
Embedded Keystore files	WARNING	3
OpenSSL (CVE-2015-3194, CVE-2014-0224)	CRITICAL	1

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)

The screenshot shows the AIR ARMOR web interface. At the top, there is a blue navigation bar with the AIR ARMOR logo, links for '난독화', '히스토리', and 'SDK', and utility icons for help, grid, notifications, and a user profile with '10/10' status. Below the navigation bar, a 'NOTICE' banner for 'AIR ARMOR ver 3.0.0 OPEN' is visible. The main content area features a large heading '모바일 환경 보호' (Mobile Environment Protection) with a sub-heading '모바일 환경에서의 악위적인 공격으로부터 앱을 보호하고 대응할 수 있는 강력한 보안 체계를 제공합니다.' (We provide a powerful security system to protect and respond to malicious attacks in mobile environments). A call-to-action button says '더 강력한 보안을 원하시나요? 지금 시작하세요!' (Do you want stronger security? Start now!). Below this, there are two tabs: '파일 업로드' (File Upload) and 'AIR GO 스캔 파일 중 선택' (Select from AIR GO scan files). The '파일 업로드' tab is active, showing instructions: '사용자 식별을 위한 Java 코드를 추가하신 후 APK를 업로드 해주세요. AIR ARMOR 적용 후 사용자 식별자(UserID 등)의 로그를 AIR EYE에서 확인하실 수 있습니다. 이미 다른 보안 제품으로 난독화가 적용되어 있다면, 이중 난독화로 정상 작동하지 않을 수 있습니다.' (After adding Java code for user identification, upload the APK. After applying AIR ARMOR, you can check the logs of the user identifier (UserID, etc.) in AIR EYE. If the APK is already obfuscated by another security product, it may not work normally due to double obfuscation). A large dashed box contains the instruction '여기에 APK 파일을 끌어오세요.' (Drag and drop your APK file here.) with an 'APK 파일 업로드' (APK File Upload) button. Below the box, it says 'APK 파일만 업로드하세요. 최대 512MB까지 가능합니다.' (Upload only APK files. Up to 512MB is possible). The footer contains copyright information for LINE Plus Corp., privacy and security policies, and navigation links for AIR 소개, 언론보도, 공지사항, 도움말, 문의, and language selection (한국어).

- 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)

AIR ARMOR | 난독화 | 히스토리 | SDK

파일 업로드 > 강화 진행 > 다운로드

당신의 앱은 강화되었습니다.

강화 전과 후를 비교해 보세요.

원본 코드 미리보기

```
6e 76 00 73 74 72 6e 63 70 79 00 5f 5a
4e 37 5f 4a 4e 49 45 6e 76 31 31 47 65
74 49 6e 74 46 69 65 6c 64 45 50 38 5f
6a 6f 62 6a 65 63 74 50 39 5f 6a 66 69
65 6c 64 49 44 00 5f 5a 4e 37 5f 4a 4e
49 45 6e 76 31 37 47 65 74 53 74 72 69
6e 67 55 54 46 43 68 61 72 73 45 50 38
5f 6a 73 74 72 69 6e 67 50 68 00 5f 5a
```

nv.strncpy..._ZNT_JN Env
11GetIntFieldEP8_obj_e
ctP9_jfieldD..._ZNT_JN
Env17GetStringUTFChars
EP8_stringPh..._ZNT_JN
Env21ReleaseString

강화된 코드 미리보기

```
9h 76 04 73 07 06 1e 0d 13 0a 70 0d 5e
4e 37 5f 4a 4e 49 45 6e 76 31 31 47 65
74 49 6e 74 46 69 65 6c 64 45 50 38 5f
6a 6f 62 6a 65 63 74 50 39 5f 6a 66 69
65 6c 64 49 44 00 5f 5a 4e 37 5f 4a 4e
49 45 6e 76 31 37 47 65 74 53 74 72 69
6e 67 55 54 46 43 68 61 72 73 45 50 38
5f 6a 73 74 72 69 6e 67 50 68 00 5f 5a
```

강화로 인하여 APK 파일이 변경되었습니다. 서명을 다시 하세요.

[APK 서명 직접 하는 방법 -](#)

[강화된 파일 다운로드](#)

다음 단계

- 1 앱의 정상 동작 여부를 확인 해주세요.
- 2 AIR ARMOR에서 강화된 파일의 난독화 상태를 AIR GO에서 확인해보세요. [AIR GO로 가기](#)
- 3 강화된 파일을 배포하시면, 조작 시도나 변조 행위를 AIR EYE에서 모니터링 할 수 있습니다. [AIR EYE로 가기](#)

난독화 완료 -이전/이후 비교

© LINE Plus Corp. | 이용약관 | 개인정보처리방침 | AIR 소개 | 언론보도 | 공지사항 | 도움말 | 문의 | 한국어

AIR ARMOR | 난독화 | 히스토리 | SDK

SDK

AIR ARMOR SDK를 이용하여 Android와 iOS 앱을 빌드할 수 있습니다. 시작 방법은 [API 문서](#) 에서 확인할 수 있습니다.

SDK 다운로드 | 문서

당신의 라이선스 키: U

Version 2018.01.16 오후 06:53

LATEST RELEASE

- armor-sdk-android
- armor-sdk-ios
- armor-sdk-unity

AIR SDK는 여러 오픈소스 소프트웨어를 포함하고 있습니다. 오픈소스 라이선스를 준수하기 위해 공지사항에서 별도의 고지를 하고 있습니다.

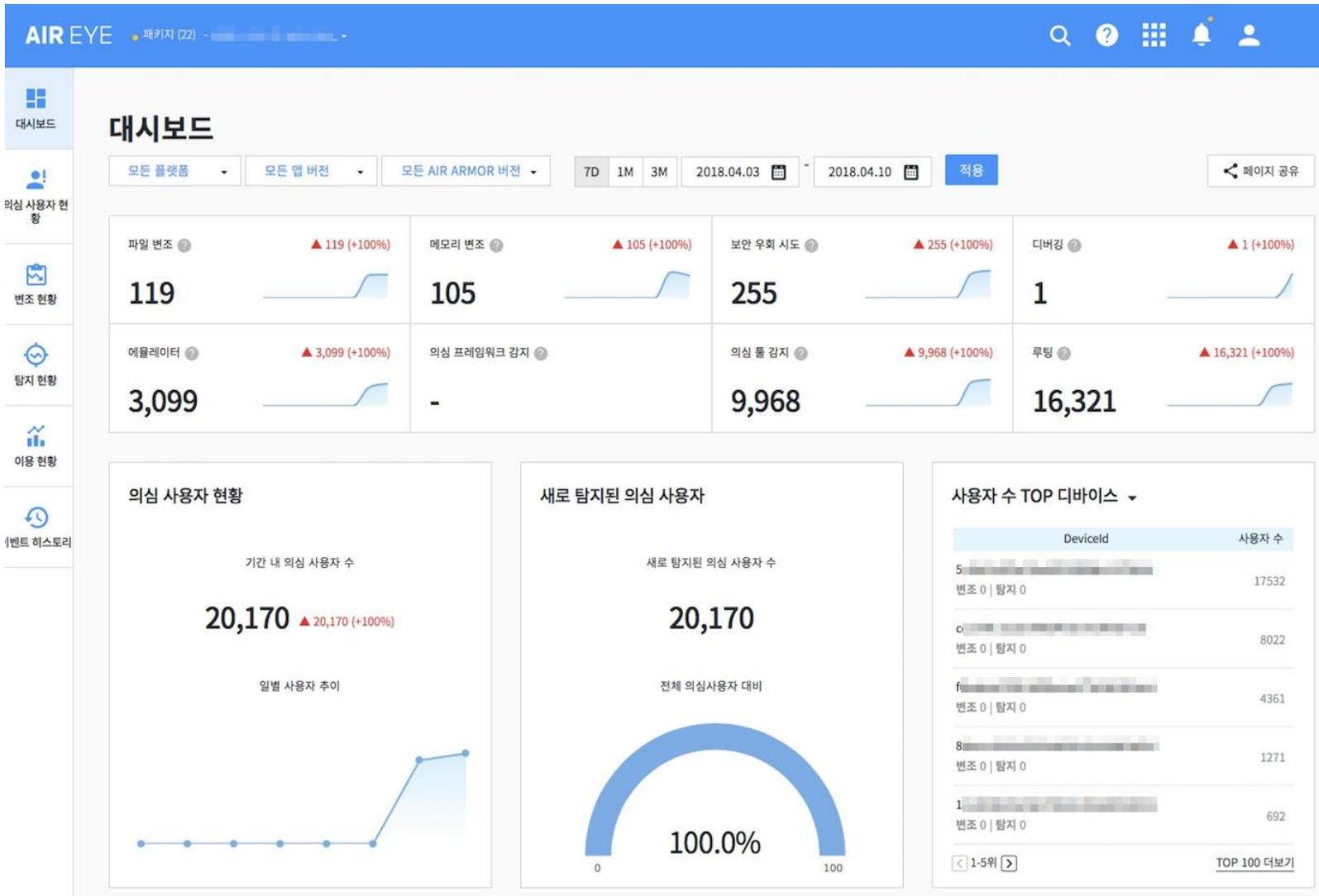
IOS/Android SDK 제공

© LINE Plus Corp. | 이용약관 | 개인정보처리방침 | AIR 소개 | 언론보도 | 공지사항 | 도움말 | 문의 | 한국어

AIR EYE (Monitoring)

Abuser Monitoring , Relation Analysis , Abusing Detect

AIR EYE (Monitoring)

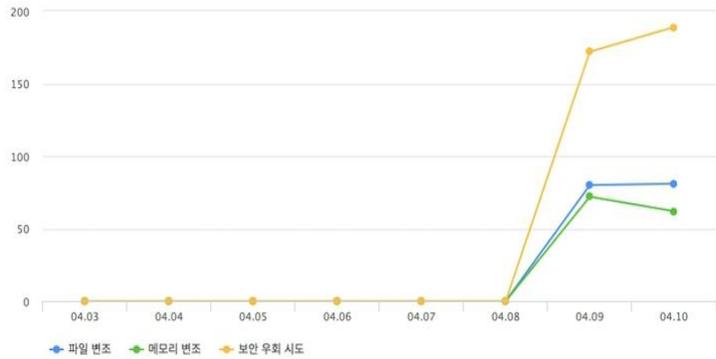


패키지별 대쉬보드

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

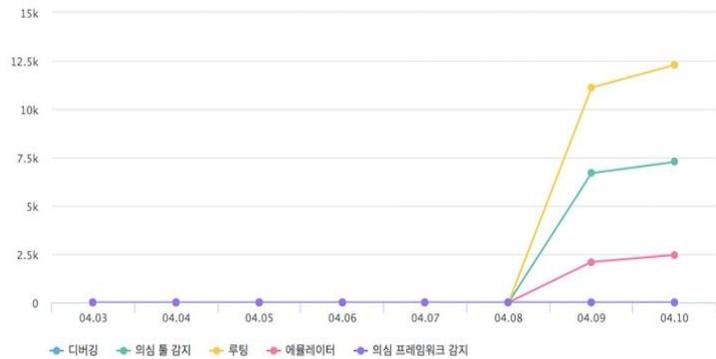
AIR EYE (Monitoring)

변조 추이
일별 변조 사용자 수를 확인하는 차트입니다.



변조 탐지 추세

탐지 추이
일별 탐지 사용자 수를 확인하는 차트입니다.



변조 현황

모든 변조

변조 시도 대상	변조 추이
signature	[Line Chart]
signature	[Line Chart]
YDS	[Line Chart]
com.linecorp. [redacted]	[Line Chart]
lib. [redacted] unity.so	[Line Chart]
com.linecorp. [redacted]	[Line Chart]
lib. [redacted] unity.so memory	[Line Chart]
com.linecorp. [redacted]	[Line Chart]

전체보기

이벤트 히스토리

모든 이벤트

1.56.0 android	com.linecorp. [redacted]	2018.04.08
9 ios	com.linecorp. [redacted]	2018.04.08
2.6.0 android	com.linecorp. [redacted]	2018.04.08
1.56.0 ios	com.linecorp. [redacted]	2018.04.08
2.0.0.31 ios	com.linecorp. [redacted]	2018.04.08

전체보기

의심 사용자 현황

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

의심 사용자 현황

20,170
▲ 20,170 (+100%)

시간 내 의심 사용자 수

일별 사용자 추이

새로 탐지된 의심 사용자

20,170

100.0%

0 | 100

전체 의심 사용자 대비

의심 사용자 탐지 추이

파일 변조 119 |
 메모리 변조 105 |
 보안 우회 시도 255 |
 디버깅 1 |
 에뮬레이터 3,099 |
 의심 프레임워크 감지 - |
 의심 톨 감지 9,968 |
 루팅 16,321

의심 사용자 탐지 추세

의심 사용자 리스트 (결과는 1000개로 제한됩니다.)

사용자 ID	파일 변조	메모리 변조	보안 우회 시도	디버깅	의심 톨 감지	루팅	에뮬레이터	의심 프레임워크 감지
[redacted]	0	0	0	0	2	2	0	0
[redacted]	0	0	0	0	0	0	2	0
[redacted]	0	0	0	0	0	2	0	0
[redacted]	0	0	0	0	1	2	1	0
[redacted]	0	0	0	0	1	1	1	0
[redacted]	0	0	0	0	0	1	0	0
[redacted]	0	0	0	0	0	0	2	0

AIR EYE (Monitoring)

변조 현황

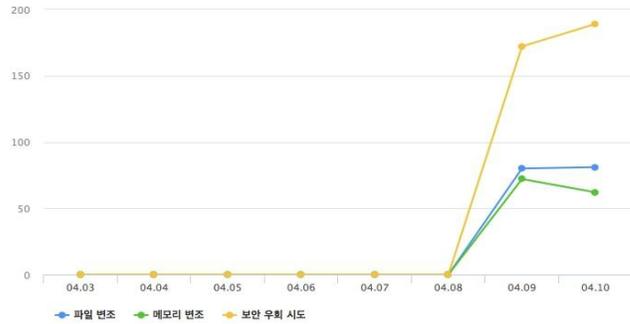
모든 플랫폼 | 모든 앱 버전 | 모든 AIR ARMOR 버전 | 7D | 1M | 3M | 2018.04.03 | 2018.04.10 | 적용 | < 페이지

변조 현황 | 일반 변조 사용자 수를 확인하는 차트입니다.

파일 변조 **119** ▲119(+100%)

메모리 변조 **105** ▲105(+100%)

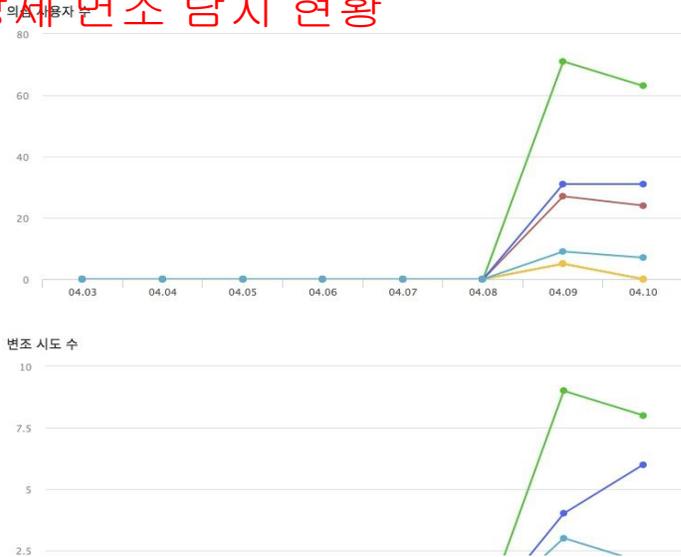
보안 우회 시도 **255** ▲255(+100%)



변조 시도 대상별 추이

- 파일 변조
- libunity.so
 - signature
 - libunity.so
 - VDS
- 메모리 변조
- lib.so memory
 - libgame.so memory
 - VDS memory
 - libunity.so memory

상세 변조 탐지 현황



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	libunity.so memory	33
Android	2.6.0	2.2.3	libunity.so	33
Android	5.2.3	2.2.2.158	signature	19
iOS	1.0.4	2.2.4	memory	17
iOS	1.0.4	2.2.4	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	libunity.so memory	5
Android	1.0.4	2.2.4	libunity.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	memory	1
Android	5.2.1	2.2.2.158	signature	1

패키지별 변조 탐지 현황
- 무엇을 공격 대상으로 하였는가?

AIR EYE (Monitoring)

탐지 현황

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

모든 앱 버전 | 모든 AIR ARMOR 버전 | 7D | 1M | 3M | 2018.04.03 | 2018.04.10 | 적용 | 페이지 공유

디버깅 1 ▲ 1 (+100%)	에뮬레이터 3,099 ▲ 3,099 (+100%)	의심 프레임워크 감지 -	의심 툴 감지 9,968 ▲ 9,968 (+100%)	루팅 16,321 ▲ 16,321 (+100%)
----------------------	--------------------------------	------------------	----------------------------------	-------------------------------

루팅 3	디버깅 -	의심 툴 감지 3	의심 프레임워크 감지 -
에뮬레이터 -	메모리 변조 -	파일 변조 -	보안 우회 시도 -



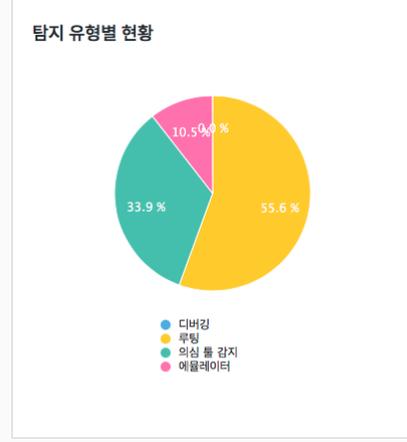
프로필 정보

5료 후 재실행

최근 탐지 일자
2018.04.10 23:21:11

GBB2

특정 사용자(어뷰저)별 탐지 상황



상세 로그 | 모두 펼치기 | 모두 접기

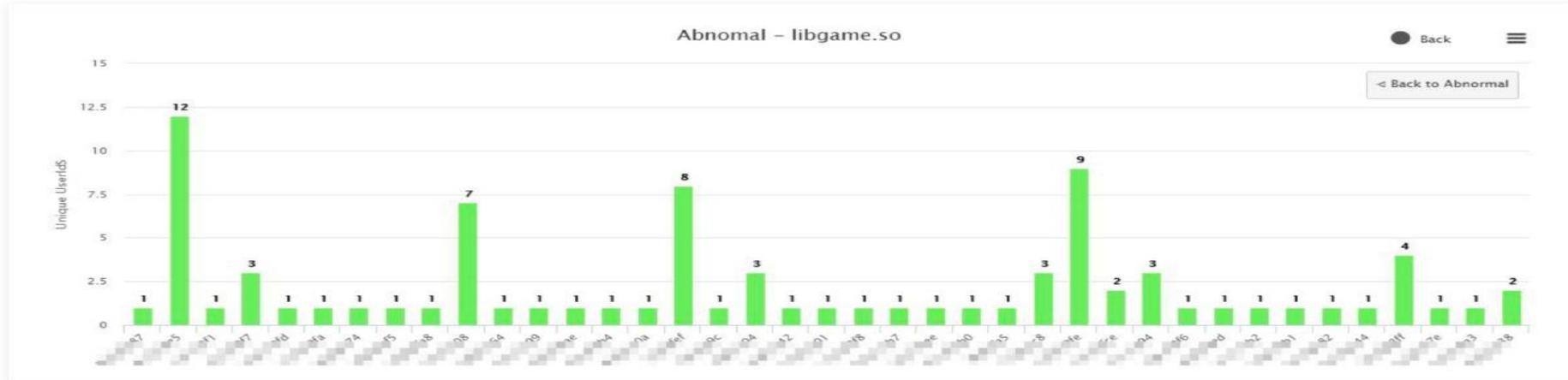
2018.04 (9)

2018.04.09 21:57:26	루팅	com.linecorp
DeviceId: 39cc47a388b8eaf3dc2702509e24f21f AppId: 4db8361d474a67c80a67d098b87cc0d App Version: 2.0.0.33 AIR ARMOR version: 2.2.5.172 Target: roo Ip: 124.218.47.82 Country: TW		
2018.04.09 22:01:36	의심 툴 감지	com.linecorp

AIR (Active Incident Response)



AIR (사례)

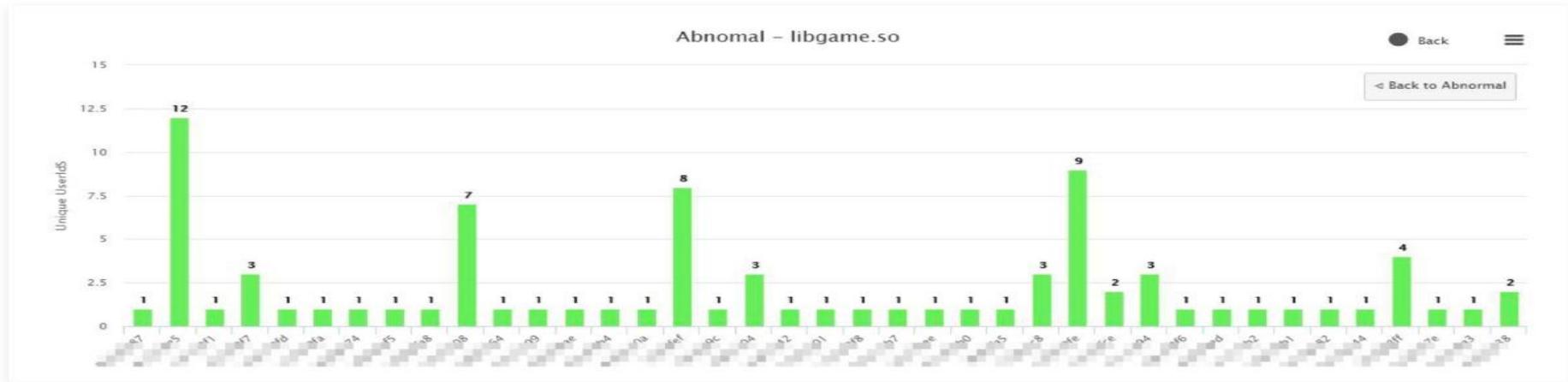


게임 로직이 들어 있는 SO 파일의 해쉬 탐지 (다양한 변조)

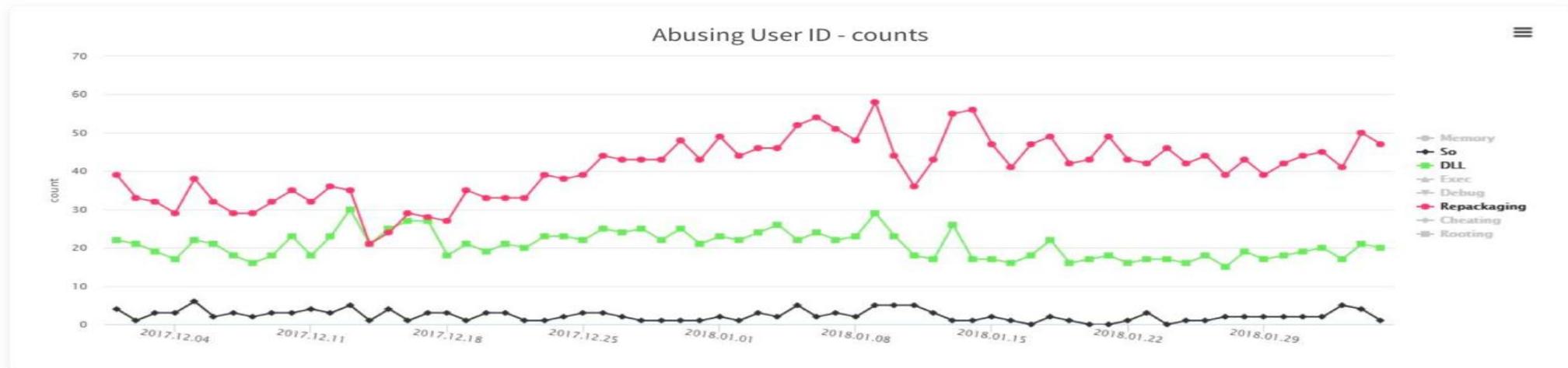


게임개발 엔진인 Unity의 각 구성요소별 변조 탐지 통계 - so, dll 변조 및 리패키징

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