IDEATEC
이 데 아 텍 (주)

2018.01.17

FxShield 제품 소개서

안드로이드 모바일 앱 보호 서비스

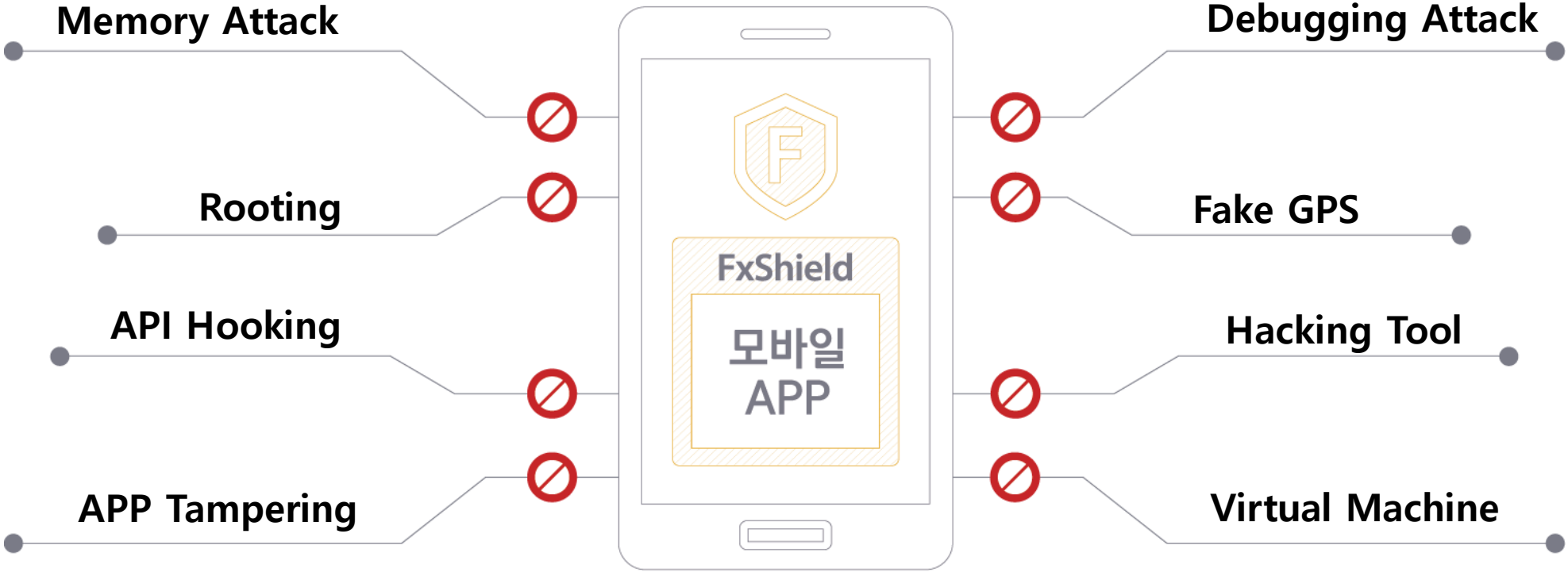
- 금융 및 일반 기업용

IDEATEC
이 데 아 텍 (주)

목 차Contents

1. 제안 배경

안드로이드 모바일앱은 다중 온라인 앱스토어 배포 방식의 개방적 구조 특성으로 인해 다양한 보안 위협에 노출되어 있는 상황이며, 지금까지 보안 취약점이 대두될 때마다 단편적 임시 방편으로 해결해왔으며, 이로 인해 새로운 서비스 개발 시에는 시간 비용과 물질적 부담이 따르며 보안 대책의 선택 적용 시 이미 노출된 취약점을 감수해야 하는 불편함이 있습니다.



2. 개발 철학

모바일앱 보안에 대해 기존의 구세대 보안 솔루션들이 제공하지 못한 전혀 새로운 개념과 접근 방식 및 개발 철학을 기반으로 차세대 안드로이드 모바일앱 보호 서비스 FxShield를 개발하였습니다.

FxShield는 3세대 모바일앱 보호 서비스로 "난독화 + 암호화 + 보안위협 탐지 " 기능을 제공하고 있습니다.

1. **ALL in One Security :**
   지금까지 축적된 모든 보안 대책을 포함하는 "능동적 앱 보호 서비스"를 구축한다.

2. **ALL New Concept :**
   메모리 해킹이나 디버거 공격 등 신규 해킹 기법에 대한 현실적인 대안을 마련한다.

3. **No Server, No Waste of Time :**
   서버 인프라의 부담 없이 적용 절차는 간단해야 한다.
   ※ 웹 빌드가 가능한 On-demand 방식 End Point Security

4. **All in One Console :**
   보안 대책들에 대한 통계 데이터를 실시간 수집하여 통계 서비스를 제공한다.

5. **Brand New Everyday**:
   새로운 공격기법의 정보를 상시로 수집하고 기능을 업데이트한다.

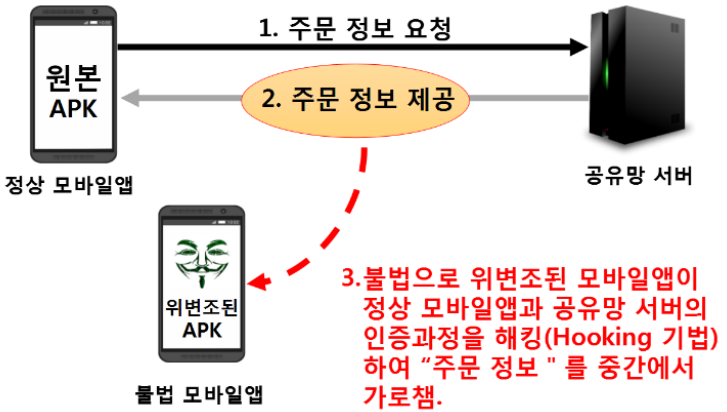
3. 적용 사례

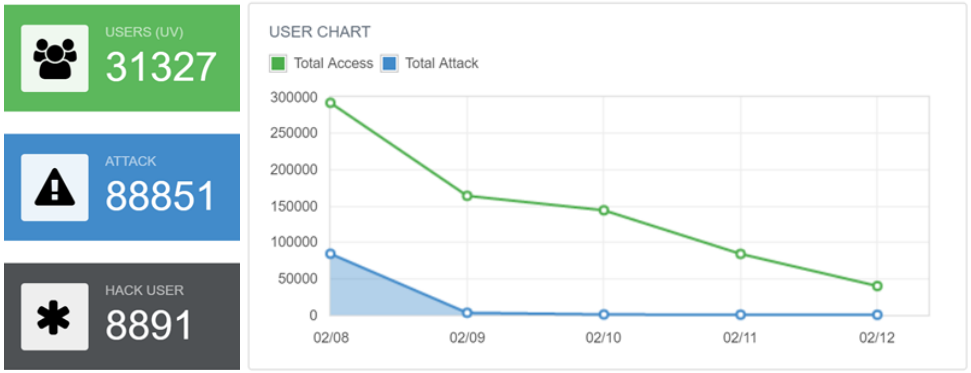
위치 기반 물류배송 모바일앱 서비스에 FxShield를 적용하여 악의적인 목적의 불법사용을 효과적으로 방지

(주)인성데이터(http://www.insungdata.com)는 **위치 기반 서비스(LBS : Location-Based Service)** 물류 배송 전문기업으로 한국의 이륜차 물류 서비스(이하 퀵서비스) 시장 규모는 2017년 현재 약 4조원 이상으로 추정되며, 인성데이터에서 개발한 퀵서비스 모바일앱은 시장 점유율 1위를 차지하고 있습니다. 퀵서비스 모바일앱 은 "중개업체"들이 "공유망"에 접수한 고객들의 배송 주문을 "배송기사"들의 위치를 GPS 기반으로 판별하여 배송 목적지까지 신속하게 배달할 수 있도록 균등하게 배정해주는 **O2O(Online to Offline)** 서비스이며 하루 평균 약 4만명의 "배송기사"들이 이용하고 있습니다.

❖ FxShield 적용 전 업체의 피해 현황

해커를 고용한 불법업체에서 정상적인 퀵서비스 모바일앱을 불법적으로 리버스 엔지니어링(해킹)하여 위/변조된 모바일앱을 배송기사에게 사용료(약 100,000원/월)를 받아가며 시중에 보급하고 부당 이익을 취하였으며, 위/변조된 모바일앱을 사용하는 배송기사는 정상적인 모바일앱을 사용하는 배송기사보다 먼저 배송 주문을 중간에서 가로채거나, 모의위치앱(FakeGPS)을 사용하여 배송지에서 멀리 떨어져 있어도 배송 주문을 받을 수 있게 하는 등 퀵서비스 시장의 거래 질서를 위반하여 공유경제 생태계를 지속적으로 위협하였습니다.



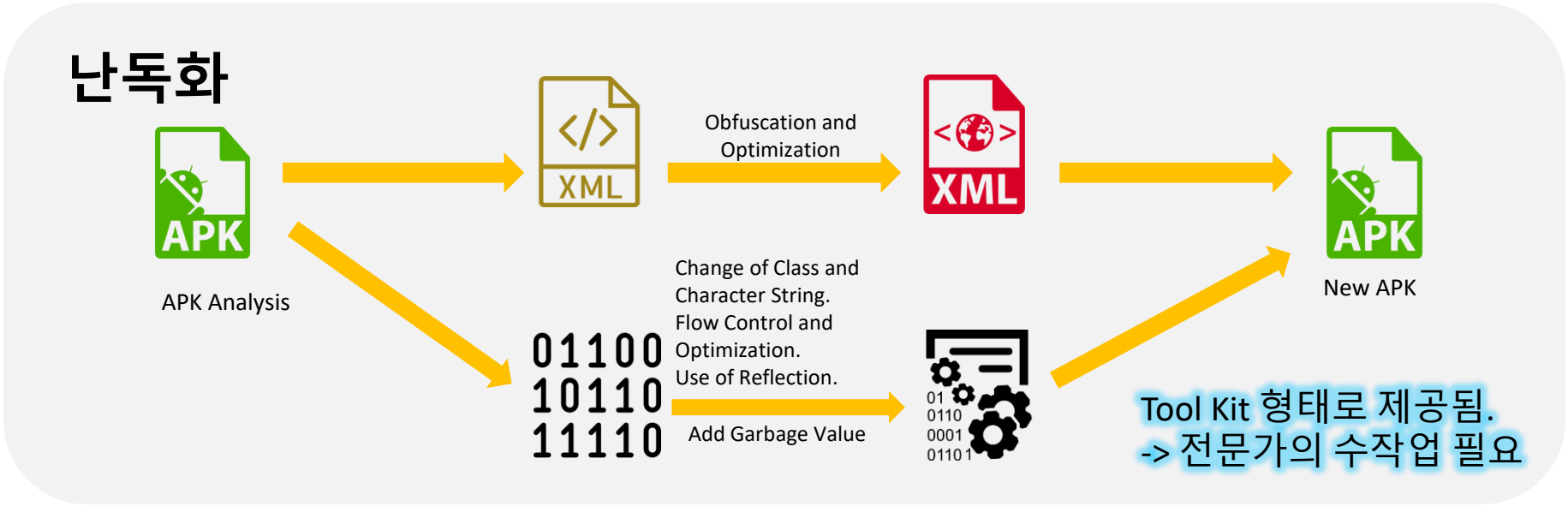


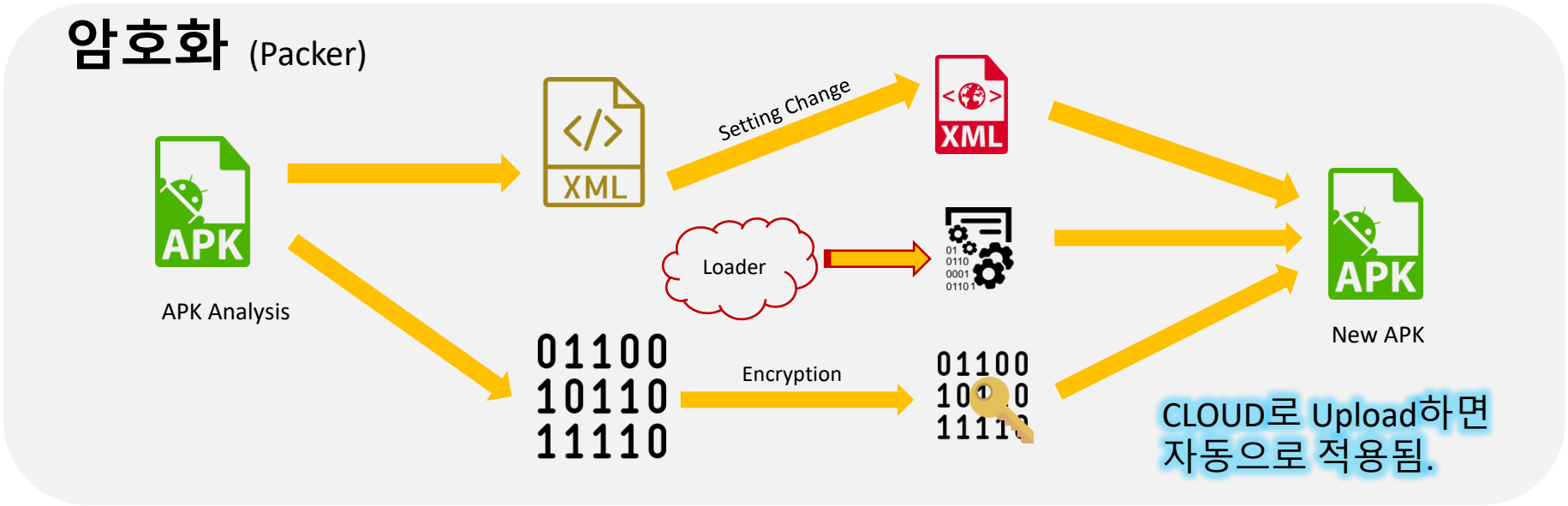
❖ FxShield 적용 후 해킹 시도 성공적 차단

적용 후 1주일 동안 다음과 같은 공격 시도를 차단하였습니다.

- 불법 행위 배송기사 색출 : 전체 31,327명 중, 8,891명(28%)
- 공격시도 차단 건 수 : 88,851건
- 연간 약 100억원 규모로 발생하던 예상 피해 금액을 방지.

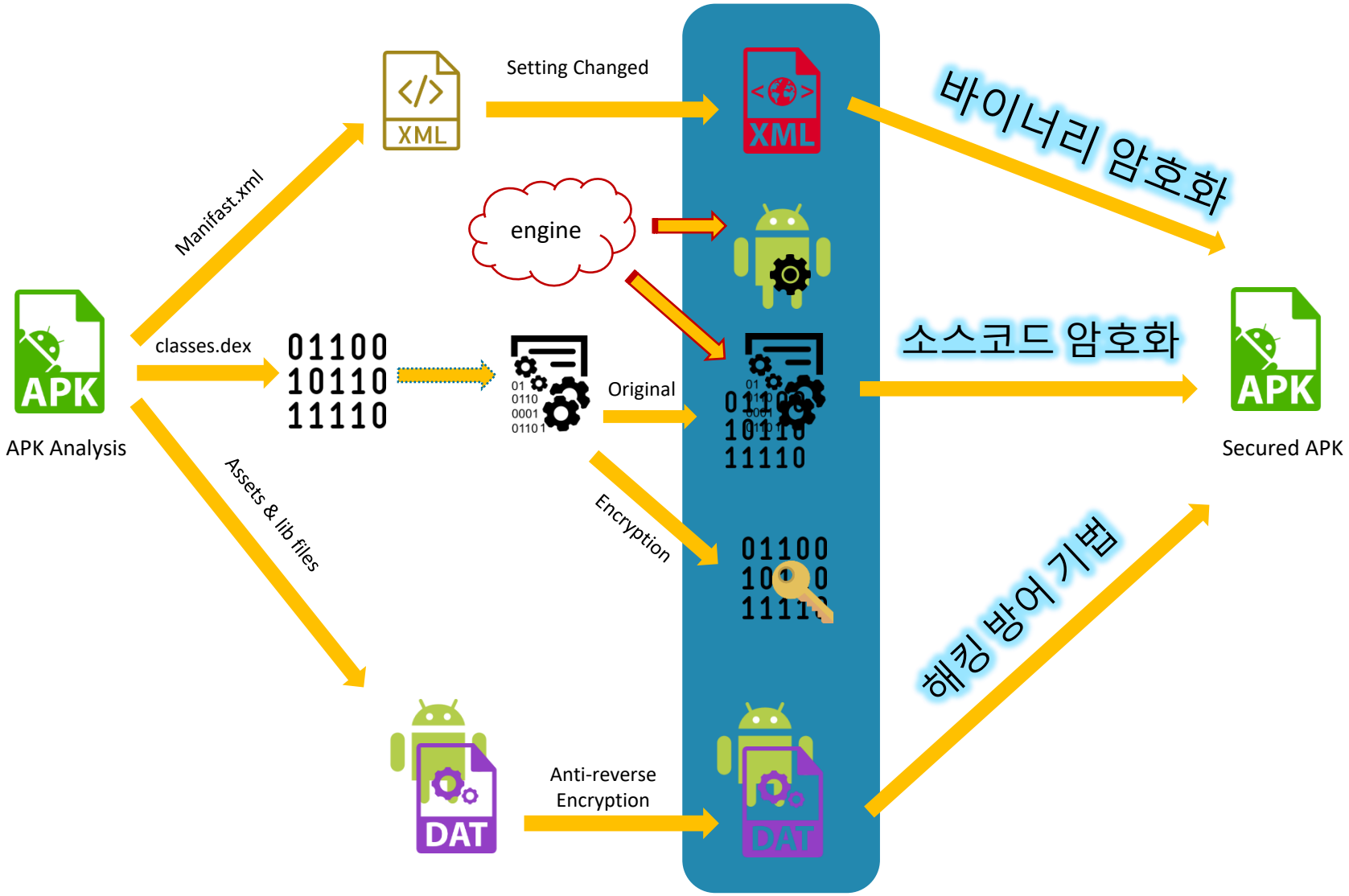
4. 난독화 vs 암호화(Packer) : 전통적인 앱 보호 기술의 종류





5. 기술적 특징

"난독화와 암호화가 다양한 해킹 방어수단과 함께 CLOUD상에서 자동으로 구현됨."



6. 주요 기능

1. **기본 보호 기능은 모바일앱을 보호하기 위한 최소한의 필수 기능을 포함하고 있습니다.**
   ('선택기능'은 모바일앱의 특성에 따라 요구되는 다양한 보안 수준을 충족하기 위한 기능입니다.)
2. **실시간 제어기능은 모바일앱 운영 정책에 따라 특정 보안영역에 대한 감시기능을 실시간 제어할 수 있도록 하는 기능입니다. ('체크박스'로 기능 선택 후 적용)**
3. **'관리자 기능'은 공격자의 시도에 대한 단말기 정보나 IP정보의 분석을 통해 관리자의 대응을 돕는 기능입니다.**
   (Web Console 사용자 환경 제공)

기본 보호 기능

- 바이너리(DEX) 암호화
- 소스코드 암호화 (리소스 ID, String, Parameter)
- 위/변조 탐지
- 메모리 공격 탐지
- 안티 디버깅
- 안티 후킹
- SO파일 안티 디컴파일
- 라이브러리 무결성 검사

실시간 제어 기능

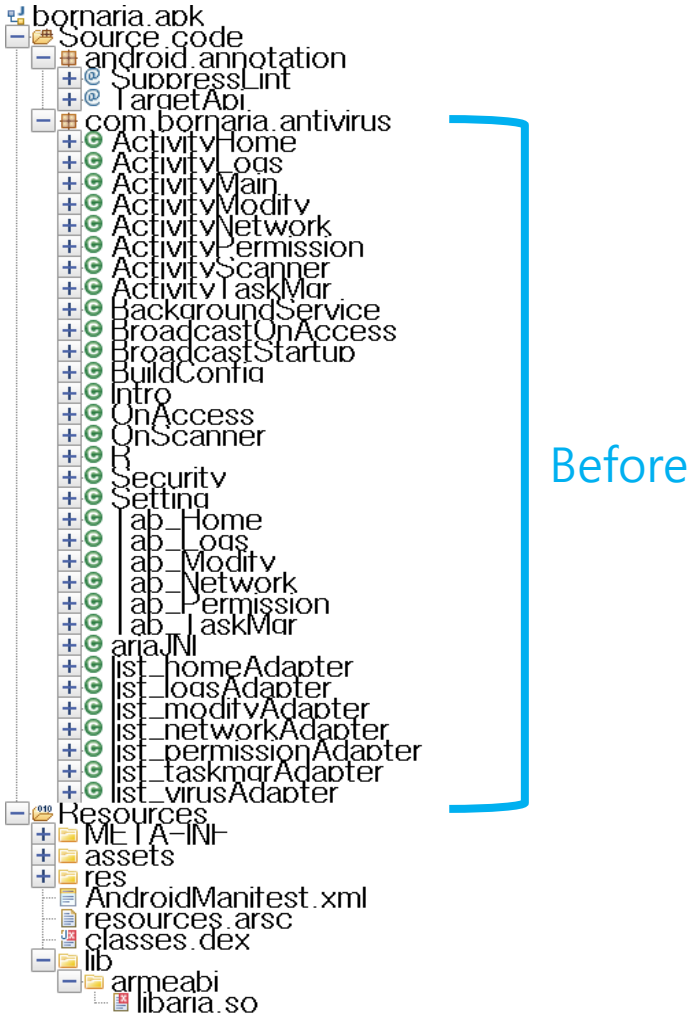
- 해킹툴 탐지
- 미러링 앱 탐지
- 모의위치앱 탐지
- 가상머신 탐지
- 루트쉘 탐지
- 루팅 탐지
- 루팅가능 탐지
- 안드로이드 오류 리포트

관리자 기능

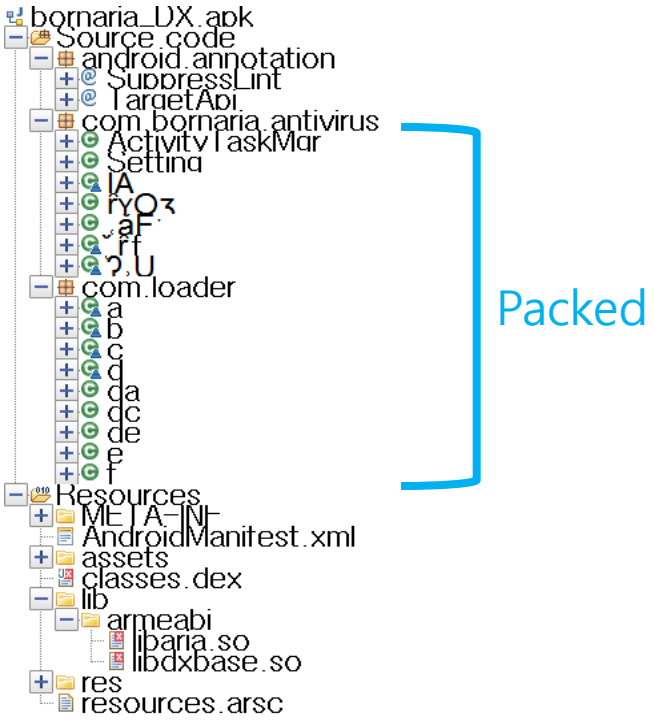
- 통계 분석 기능
  - 대시보드
  - 위협종류 통계
  - 공격자 통계
  - 지역 별 침해 시도 정보
  - DAU / MAU
- 보안 적용 화면

6. 주요 기능 : 바이너리 암호화 (Packing)

Before Packing



After Packing



6. 주요 기능 : 소스코드 난독화

Before Obfuscation

```
129   public int EngineUpdate() {
130      ConnectivityManager connect_manager = (ConnectivityManager) getSystemService("connectivity");
131      NetworkInfo mobile = connect_manager.getNetworkInfo(0);
132      NetworkInfo wifi = connect_manager.getNetworkInfo(1);
134      if ((mobile == null || !mobile.isConnected()) && (wifi == null || !wifi.isConnected())) {
159         return 2;
         }
137      String server_addr = preference.getString("setting_update_address", "update.ariasecure.com");
138      String key_code = preference.getString("setting_product_key", "bornaria");
141      BackgroundService.LockJNI(12);
142      String version = new ariaJNI().UpdateEngine(this, key_code, server_addr, 80, 23);
145      if (version == null || (version.length() > 0 && version.charAt(0) == '*')) {
147         version = new ariaJNI().GetVersion(0);
148         BackgroundService.UnlockJNI();
159         return 0;
         }
151      BackgroundService.UnlockJNI();
153      Editor editor = preference.edit();
154      editor.putLong("Last_Update_Time", System.currentTimeMillis());
155      editor.commit();
155      return 1;
      }
```

After Obfuscation

```
129   public int □□□□() {
130      ConnectivityManager connect_manager = (ConnectivityManager) getSystemService(dc.sure(1458648683));
131      NetworkInfo mobile = connect_manager.getNetworkInfo(0);
132      NetworkInfo wifi = connect_manager.getNetworkInfo(1);
134      if ((mobile == null || !mobile.isConnected()) && (wifi == null || !wifi.isConnected())) {
159         return 2;
         }
137      String server_addr = □□□□.getString(dc.joint(1138506097), dc.nat(612701042));
138      String key_code = □□□□.getString(dc.kwkim(1419583255), dc.nat(612694895));
141      BackgroundService.□□□□(12);
142      String version = new ariaJNI().UpdateEngine(this, key_code, server_addr, 80, 23);
145      if (version == null || (version.length() > 0 && version.charAt(0) == '*')) {
147         version = new ariaJNI().GetVersion(0);
148         BackgroundService.□□□□();
159         return 0;
         }
151      BackgroundService.□□□□();
153      Editor editor = □□□□.edit();
154      editor.putLong(dc.joint(1138532215), System.currentTimeMillis());
155      editor.commit();
155      return 1;
      }
```

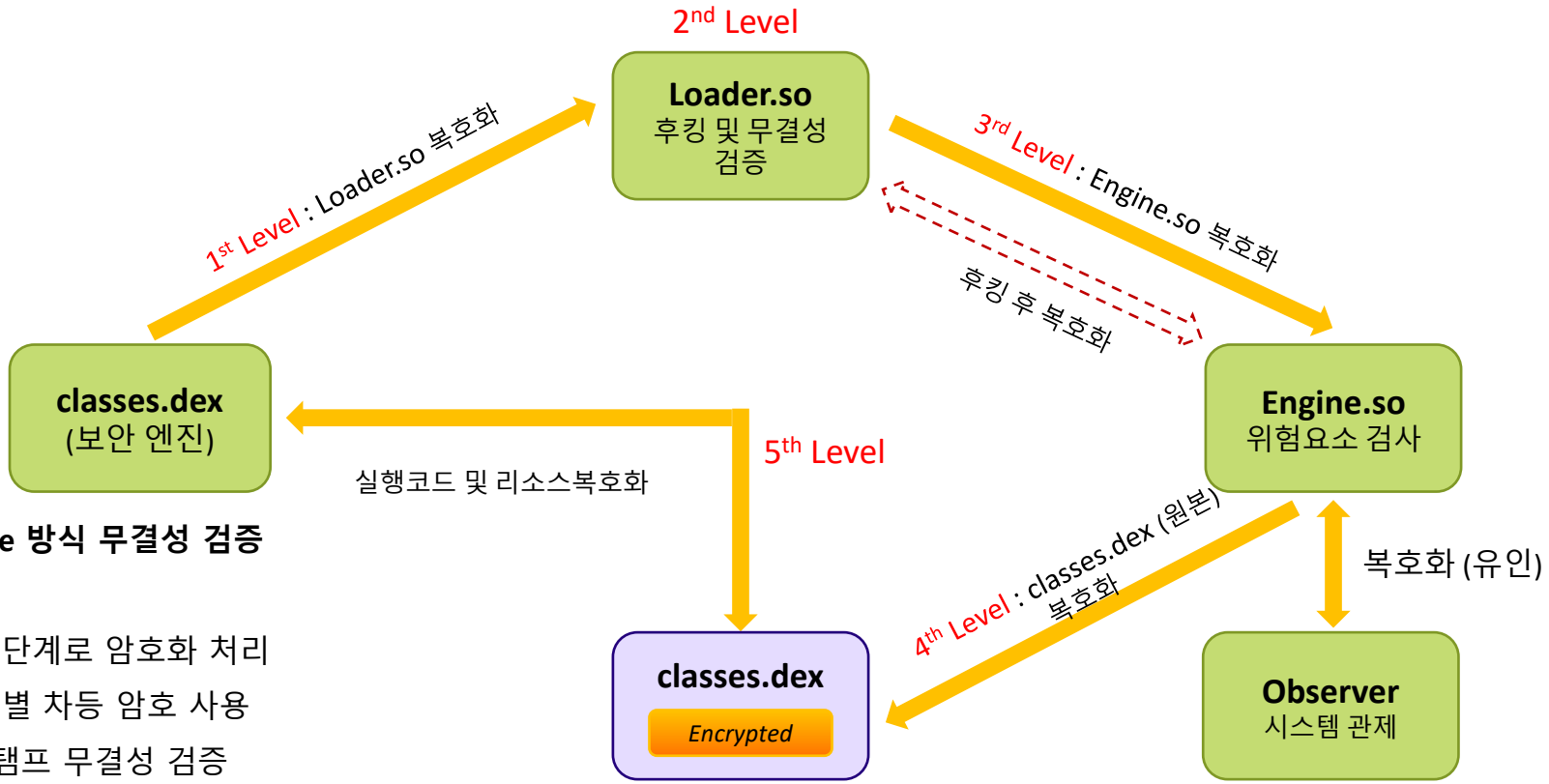
Obfuscated

Encrypted

6. 주요 기능 : #1 위변조 검증

위변조 검증을 위한 보안 솔루션은 보통 Client-Server 통신을 통한 APP 무결성을 검사하는 방식으로 구성되어 있었으나, FxShield는 Server의 역할없이 Client Side 검증이 가능합니다.

기존의 'Hash값 검증 방식' 외에 압축된 APK파일에만 존재하는 5단계 연속 개인키 알고리즘을 사용해 정적 분석으로는 해독이 불가능한 방식으로 무결성을 검증하고 있습니다.



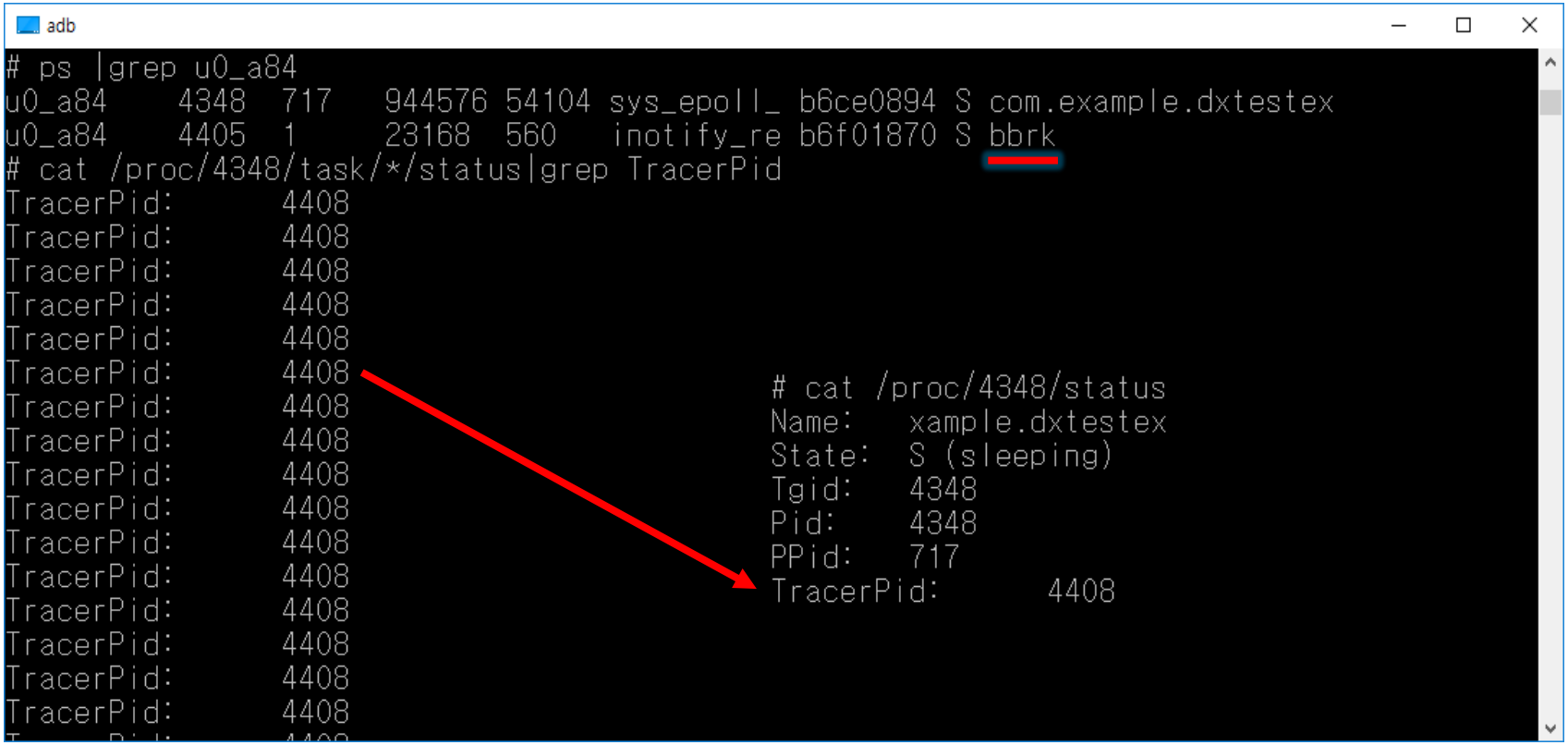
Standalone 방식 무결성 검증

- 총 다섯 단계로 암호화 처리
- 각 단계 별 차등 암호 사용
- 타임 스탬프 무결성 검증
- 마지막 단계로 실행 시 복호화

5단계 다이나믹 암호화를 통한 위변조 검증 (특허출원)

6. 주요 기능 : #2 Anti-Debugging

'Debugger 공격'의 경우 Program 수정작업을 위해 개발된 Debugger를 통해 Process를 Tracking 하여 해킹을 하는 방법으로 FxShield는 Process 실행 후 APK 와 Observer가 서로 ptrace를 선점해 이후 모든 디버깅 시도를 차단합니다.



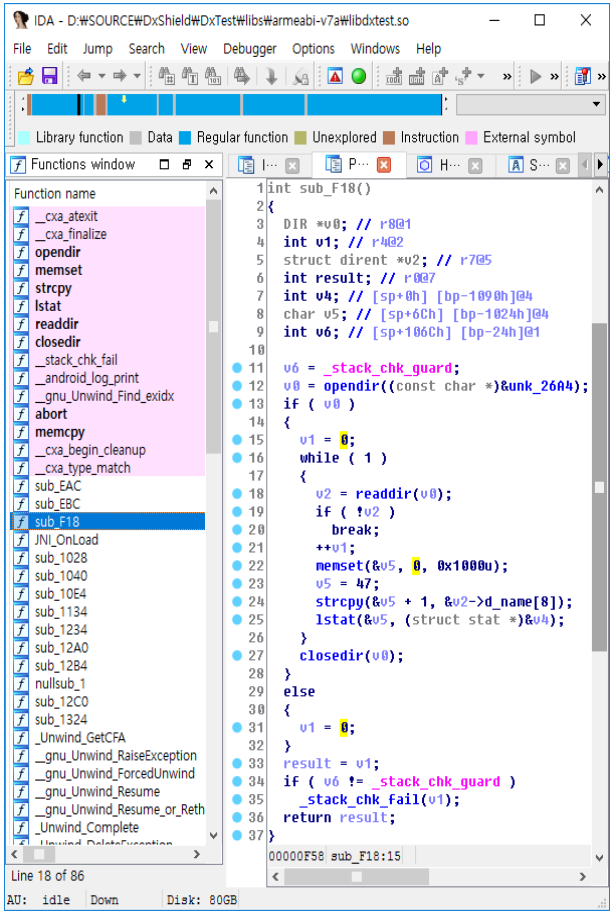
Anti-Debugging – 메모리 해킹 방지 (특허출원)

6. 주요 기능 : #3 Anti-Reverse

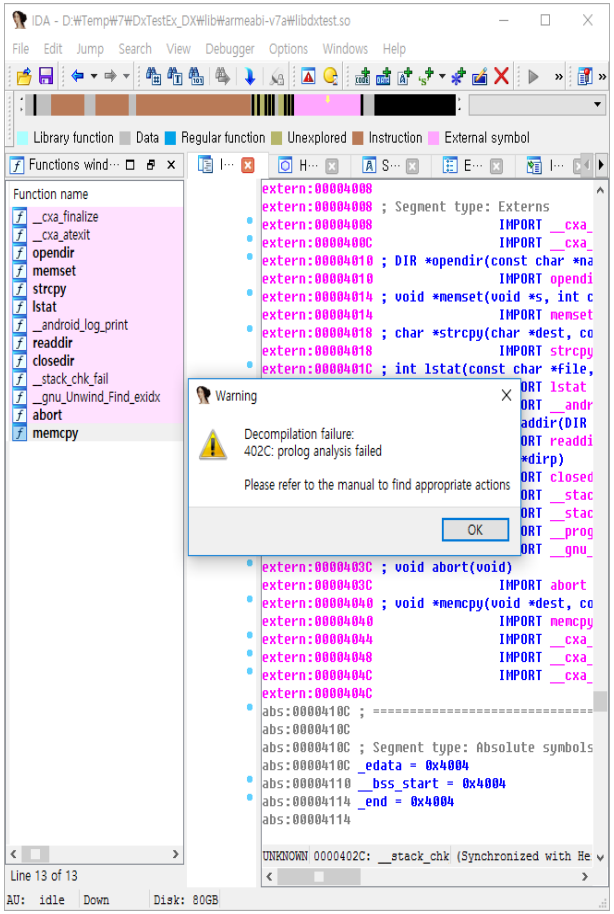
Anti-Reverse 기능은 Decompile을 막아주는 기능으로서 라이브러리(so) 파일을 변경하여 모바일앱 실행에 영향을 주지 않는 일부 section header를 제거하여 결과적으로 Debugging을 불가능하게 합니다.

```
static
int testApi(char *dirPath)
{
    int result = 0;

    DIR *dir_info;

    struct dirent *dir_entry;

    dir_info = opendir(dirPath);

    if(NULL != dir_info)
    {
        while(dir_entry = readdir(dir_info))
        {
            struct stat fstat;

            char pathName[PATH_MAX] = {0};

            strcpy(pathName, dirPath);
            strcat(pathName, dir_entry->d_name);

            lstat(pathName, &fstat);

            result++;
        }
        closedir(dir_info);
    }

    return
        result;
}
```

원본 소스코드



디컴파일 된 소스코드



FxShield를 적용한 이후 디컴파일 시도

6. 주요 기능 : #4 Anti-Hooking

5가지 방법으로 'JAVA Hooking'과 'NDK Hooking'을 구분하여 감지합니다. (국내유일 기능)

점프주소 검사
- API 시작 주소가 정상인지 검사

근거리 주소 비교
- 인접한 시스템 API의 주소 비교

콜 스텍 검사
- 특정 함수까지의 호출자 검사

직접 Hooking 시도
- 주요 API를 미리 Hooking

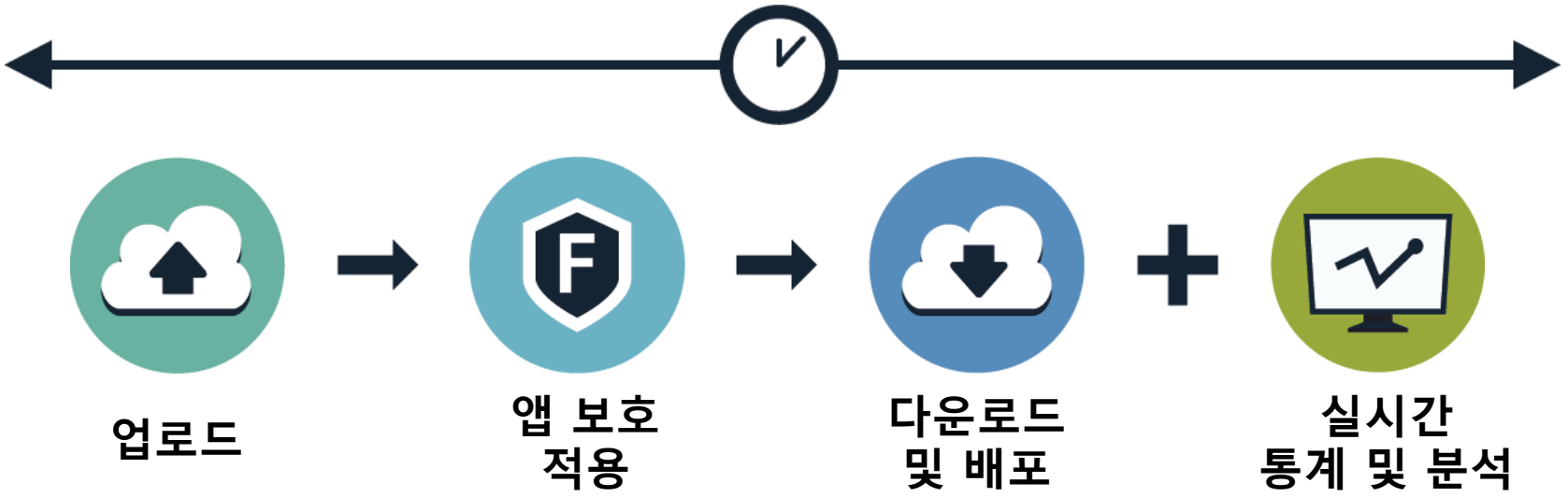
함수 숨기기
- 주요 함수를 직접 로드 함.

```
(00) com.loader.da
(01) com.loader.da
(02) android.app.Application
(03) android.app.Instrumentation
(04) android.app.Instrumentation
(05) android.app.LoadedApk
(06) android.app.ActivityThread
(07) de.robv.android.xposed.XposedBridge
(08) de.robv.android.xposed.XposedBridge
(09) android.app.ActivityThread
(10) android.app.ActivityThread
(11) android.app.ActivityThread$H
(12) android.os.Handler
(13) android.os.Looper
(14) android.app.ActivityThread
(15) java.lang.reflect.Method
(16) java.lang.reflect.Method
(17) com.android.internal.os.ZygoteInit$MethodAndArgsCaller
(18) com.android.internal.os.ZygoteInit
(19) de.robv.android.xposed.XposedBridge
(20) dalvik.system.NativeStart
```

adjacent addresses

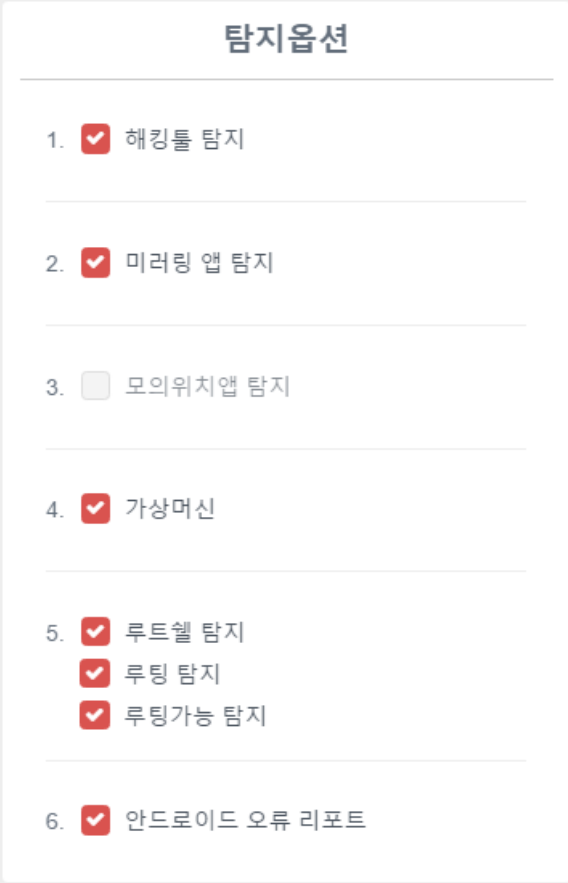
모바일앱을 안전하게 보호하기 위한 짧은 투자.

단, 10분!



6. 주요 기능 – 보안 기능 적용 옵션

- **보호패킹 옵션 및 탐지옵션**
  - **보호패킹 옵션 : FxShield 적용 시 필수로 적용되는 옵션 및 선택 가능 옵션**
  - **탐지옵션 : FxShield 적용 후 대시보드에서 On/Off 제어가 가능한 옵션**



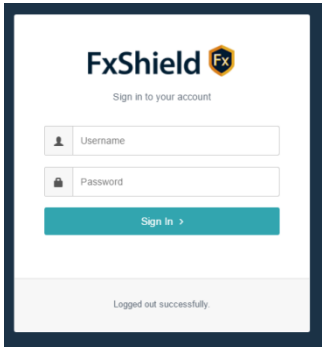
- **보안 정책 On/Off 기능**
  - **FxShield는 보안 정책 On/Off 기능을 제공하여 모바일앱의 효율적인 운영이 가능합니다.**
  - **보안기능 On/Off는 패키지 단위로 제어가 가능하며 적용 시점은 FxShield가 적용된 단말기에서 모바일앱이 재시작 할 때 적용됩니다.**

주요기능	기능 설명
해킹툴 탐지	메모리에 접근하는 해킹툴 탐지 및 차단
미러링 앱 탐지	모비즌, 팀뷰어 등의 미러링 앱 탐지 및 차단
모의위치앱 탐지	단말기에 내장된 GPS에서 감지한 위치를 조작하는 모의위치앱 탐지 및 차단
가상 머신 탐지	가상머신(VM)이 사용하는 공통적인 프로세스를 탐지
루팅 탐지	루트 쉘 탐지 : 아직 알려지지 않은 쉘 루트 권한을 가진 프로세스를 탐지 루팅 탐지 : 이미 알려진 루팅 방법 및 아직 알려지지 않은 잠재적인 루팅 방법을 모두 탐지 루팅 가능 탐지 : 루팅 된 단말과 정상 단말을 번갈아 사용하는 '좀비 단말기' 탐지
안드로이드 오류 리포트	안드로이드 앱 구동 시 발생하는 오류 리포트를 FxShield 대쉬보드에서 확인 가능

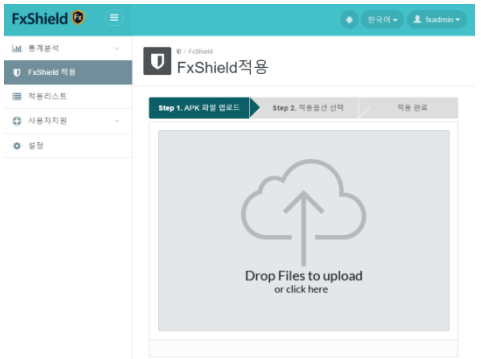
6. 주요 기능 – 간편한 보안 기능 적용

- **웹 콘솔 사용자 환경**

1. 서비스 웹사이트 로그인



2. 보안 기능을 적용할 APK파일 업로드



3. 업로드 완료 후 “Start” 버튼 Click

4. 보안 기능 적용이 완료 된 APK를 다운로드

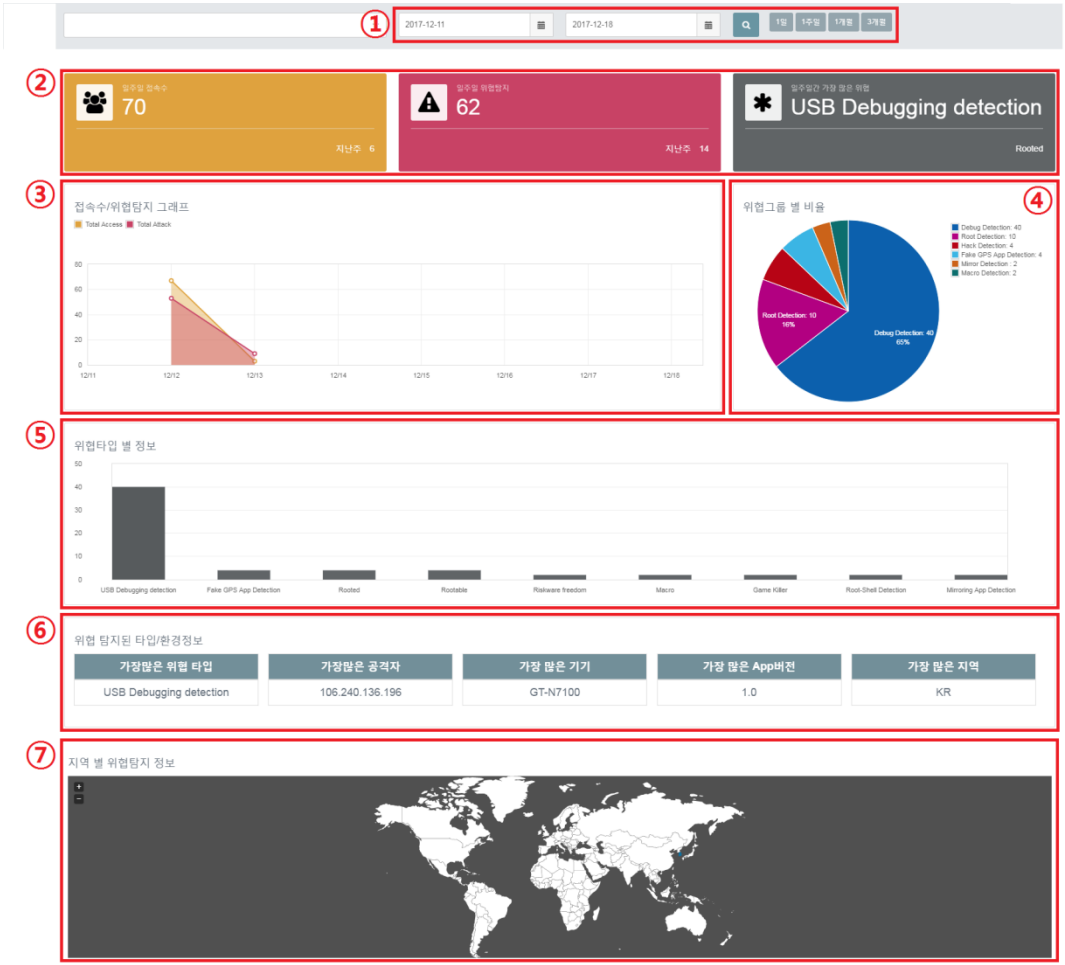
(FxShield 적용 후 실행 및 마켓 등록 시 다시 Signing 필요)

- **웹 콘솔 메뉴 구성**

메뉴	기능설명	비고
대시보드	FxShield가 적용된 모바일앱의 이벤트(접속자, 위협탐지 등) 현황을 확인 가능합니다.	
위협종류통계	FxShield가 적용된 모바일앱에 발생된 공격 로그를 유형별로 분리하여 정보를 제공합니다.	
	공격 유형별 및 Top10 공격 유형에 대한 정보를 제공합니다.	
공격자 통계	공격자의 IP주소를 기반으로 지역(Region) 식별 및 공격횟수, 공격유형에 대한 정보를 제공합니다.	
원시로그	FxShield의 실시간 로그를 표시합니다.	
사용자 통계	Daily Unique한 사용자수 (DAU), Monthly Unique한 사용자수 (MAU) 통계를 표시합니다.	
FxShield 적용	APK파일을 업로드하여 FxShield를 적용 할 수 있습니다.	
적용 리스트	현재 로그인 사용자의 FxShield 적용 이력을 확인할 수 있습니다. APK에 적용된 보안기능, 파일관리(다운로드, 삭제)등을 수행할 수 있습니다.	
사용자 지원	FxShield 서비스에 필요한 사용자 지원 사항을 제공합니다. 릴리즈노트, 유틸리티 및 서비스 가이드(매뉴얼)가 제공 됩니다.	
설정	모니터링 패키지 변경 및 FxShield 보안 기능 On/Off등을 설정할 수 있습니다 .	

6. 주요 기능 – 대시보드

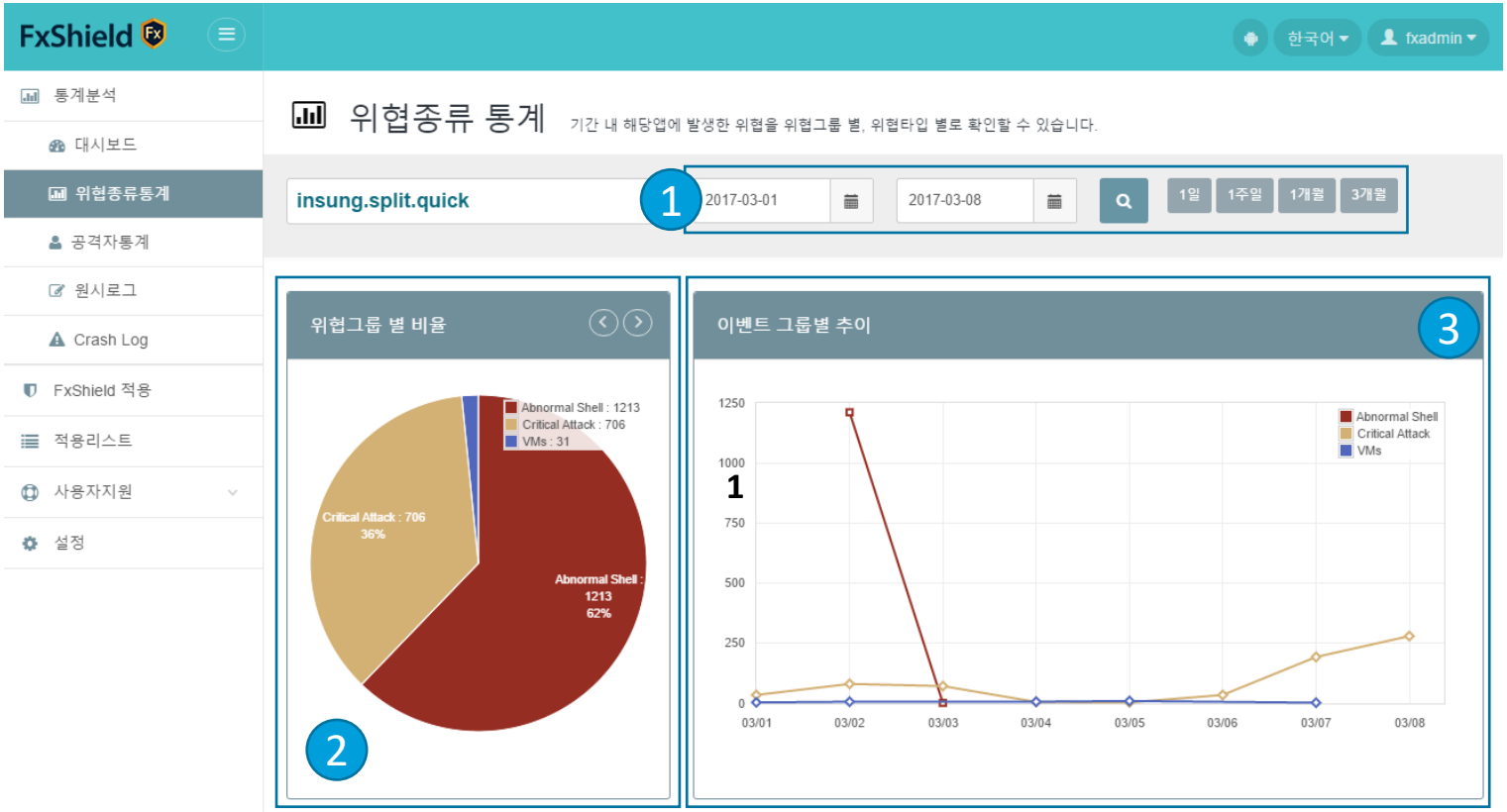
- 웹 콘솔 - 대시보드



1. 조회기간 설정
2. 전체 접속수 / 위협탐지 횟수 / 가장 많은 위협 유형
3. 접속 수 및 위협탐지 그래프
4. 위협타입 별 비율 PIE CHART
5. 위협 탐지 별 정보 그래프
6. 위협 탐지된 타입 / 환경정보
7. 지역 별 위협탐지 정보

6. 주요 기능 – 이벤트 통계

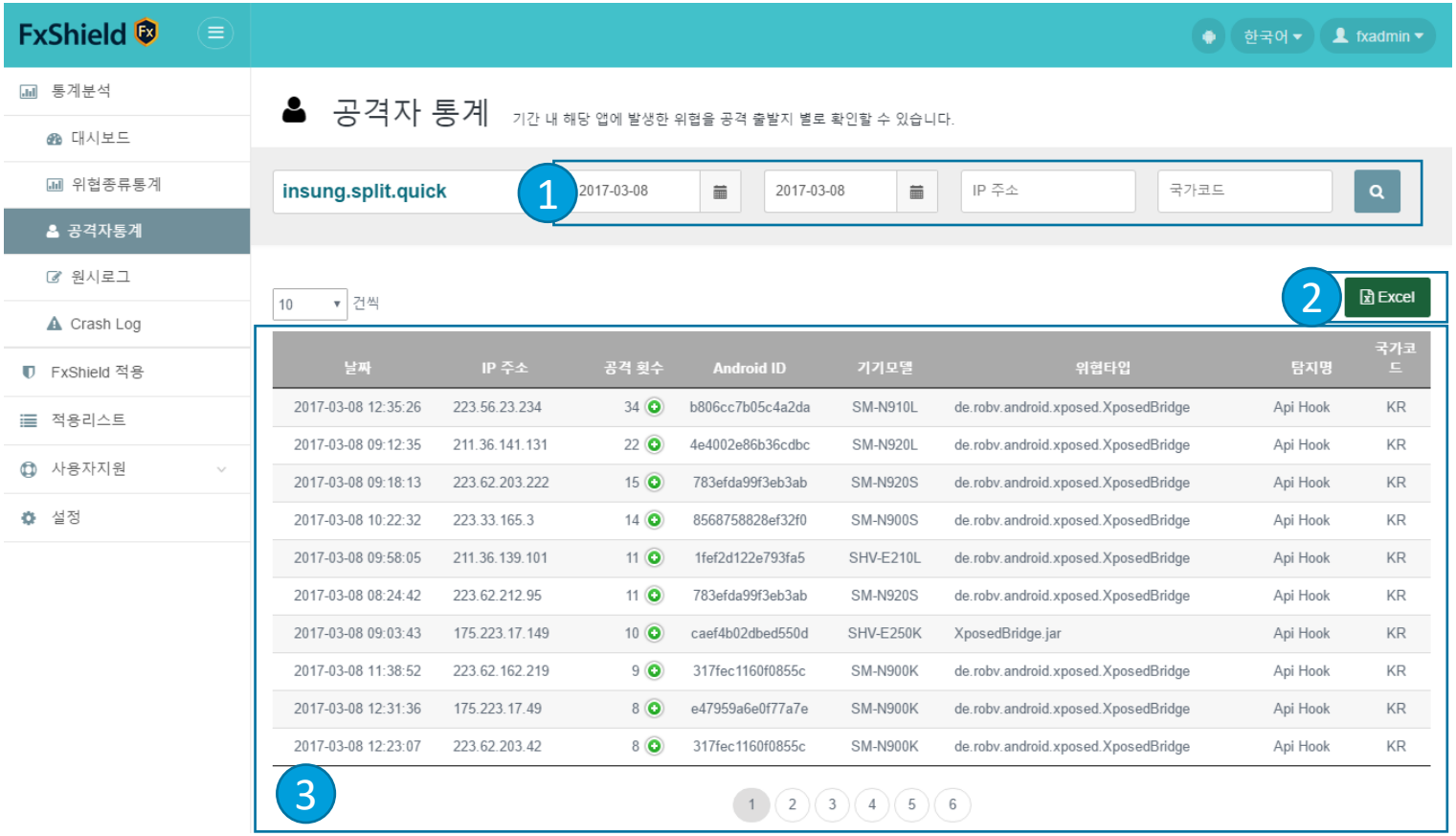
- **웹 콘솔 – 이벤트 통계**



1. **조회 기간 설정(기간통계) : 조회 기간 설정 시 조회 기간은 최대 3개월까지 설정 가능합니다.**
2. **위협그룹 별 비율**
3. **이벤트 그룹별 추이**

6. 주요 기능 – 공격자 통계

- **웹 콘솔 – 공격자 통계**



1. 기간 및 검색 조건(IP, 국가코드) 설정(최대 3개월)
2. 화면상 조회 결과를 Excel 파일로 내보내기
3. 조회 기간 설정에 따른 조회 결과가 표시됩니다.

7. 품질 인증

- **Good Software (GS인증)**

소프트웨어품질인증서

Certificate of Software Quality

상호또는성명 Trade Name or Applicant : (주)엔에스에이치씨(123-86-15737) NSHC Co., Ltd.

소프트웨어의명칭 Name of Software : 에프엑스쉴드 V2.0 FxShield V2.0

인증번호 Certification No. : 15-0433

제조자및제조국가 Manufacturer and Nation : (주)엔에스에이치씨/대한민국 NSHC Co., Ltd./Republic of Korea

인증년월일 Date of Certification : 2015년(Year) 11월(Month) 30일(Day)

기타 Others :

위 소프트웨어는 소프트웨어산업진흥법 제13조에 의하여 품질이 인증되었음을 증명합니다.

We testify that the quality of foregoing software has been certified under the Software Industry Promotion Act.

2015 년(Year) 11 월(Month) 30 일(Day)

TTA 한국정보통신기술협회장 CEO & President Telecommunications Technology Association

Certificate of Software Quality

Trade Name or Applicant : NSHC Co., Ltd.(123-86-15737)

Name of Software : FxShield V2.0

Certification No. : 150433

Manufacturer and Nation : NSHC Co., Ltd./Republic of Korea

Date of Certification : 2015. 11. 30

Others :

We testify that the quality of foregoing software has been certified under the Software Industry Promotion Act.

2015. 11. 30

TTA CEO & President Telecommunications Technology Association

1. 소프트웨어진흥법 제13조에 의거한 소프트웨어 품질 인증 취득.
2. 전문 소프트웨어 품질인증기관에서 공인된 제품으로 높은 신뢰도를 확보

8. 주요사업 소개

- 주요 사업 내용

보안기술 우위에 기반한 차별화 전략으로, 정보보호 컨설팅, 정보보호 솔루션, 보안 취약점 정보 제공 등 정보보호와 관련한 모든 분야에 사업 영역을 가지고 있으며, 지속적인 유지보수 지원 서비스를 제공하고 있습니다.

CONSULTING	SOLUTION	INFORMATION
정보 보호 컨설팅	**정보 보안 솔루션**	**Red Alert**
• 취약점 진단 및 분석 • 모의해킹 • 개인정보보호 컨설팅 • 정보보호 인증 지원 • 모바일 APP 진단 • IoT 및 핀테크 진단	• 스마트 입력 보안 키패드 • 모바일 더블 난독화 솔루션 • 앱 위·변조 방지 솔루션 • 모바일 전용 안티 바이러스 • 게임용 / 핀테크 통합보안 솔루션 • 암호화 라이브러리 • Smart OTP 솔루션	• 모바일, IoT, 핀테크 취약점 분석 보고서 • 악성코드, 제로데이 정보 제공 • 국내·외 보안 동향 정보 제공 • 사이버테러, 고객 정보 유출 등 긴급 보고서

IDEATEC
이 데 아 텍 (주)

감사합니다.

Contact Us

영업문의: jspark@ideatec.co.kr
H.P : 010-9334-7182
전화번호: +82 2-6952-9160
팩스: +82 2-6952-9161
주소: 서울시 강남구 논현로 63길 51 미림빌딩 2층