모바일 APP 취약점 점검 솔루션

제안 목차

제안 개요

제조사 소개

제조사인 ㈜라온시큐리티는 기술과 고객과의 신뢰를 최우선으로 생각하며 운영하고 있는 회사입니다.
기존의 많은 모의해킹 수행 이력과 연구 성과, 해킹대회 입상 경력 등 최고의 기술력을 확보하기 위해 최선을 다하고 있습니다.

1. 다수의 모의 해킹 수행 경험 보유

- 다수 모의 해킹 수행 인력 보유
- 일반/금융/기관 등 다양한 환경에서 모의해킹 수행
- 웹/데이터베이스/단말 등 다양한대상에 대한 모의 해킹 수행

2. 세계해킹대회 입상 경력자 보유

- KISA 해킹방어대회 8년 연속 출제 / 운영
- 세계 최고 수준의 DEFCON 본선 진출 4위
- 국내에서 주최한 국제해킹대회 우승

Raon Security

3. 최신 해킹기법 보유

- 금융권 메모리 해킹 최초 발견 및 보유
- Mobile 해킹 기법 보유
- APT 공격 해킹 기법 보유
- 취약점 Exploit 제작 기술 보유
- Mobile Zero Day 보유 (구글에 보고/버그 채택)

4. 보안 솔루션 개발 기술 보유

- 웹 애플리케이션 취약점 점검 솔루션 개발 기술 보유
- Smart Phone Monitoring 시스템 개발
- 모의해킹 시 필요 도구 개발 기술 보유
- 다양한 개발 언어 숙련승

주요 사업

제조사인 ㈜라온시큐리티는 모바일 앱 취약점 점검 솔루션으로 삼성전자, KT, KISA 등에 레퍼런스를 가지고 있으며 , 다수의 모의해킹 컨설팅 경험뿐 아니라 Andorid 및 IOS 취약점과 관련하여 지속적으로 연구해 오고 있습니다.

솔루션	• Android Application 점검 도구 (Zyroid SE, iOS, DE) - KB국민은행, KB손해보험, SKTelecom, SKPlanet, 동서발전, 해군 등 • Android 악성행위 모니터링 시스템 (Zyroid Enterprise) - 삼성전자, KT • KISA Android 악성행위 모니터링 시스템 개발
컨설팅	• SK Planet 모의해킹 • 삼성전자 갤럭시S4 모의해킹 (2회 수행, NDA체결) • 온라인게임 모의해킹 (다수) • EBAY(옥션, 지마켓) 모의해킹 • LG U+ Fuzzing • 대검찰청 모의 해킹 • 카카오 앱 모의 해킹 • 삼성SDS 화이트해커 해킹대회 문제출제 및 운영 • KISA 해킹방어대회 문제출제 및 운영 (06년 3회 ~ 13년 10회) 총 8번 운영
연구	• Google Android 취약점 발견 (2013) • Android 악성행위 모니터링 시스템 구축 - Hooking 기법 연구 • iPhone Hooking 기법 연구 - Kernel Hooking, Library Hooking, Application Hooking 기법 연구

도입 필요성

앱의 보안성 확보를 위해 진단 인력을 통한 취약점 점검을 수행하고 있지만 인력, 비용, 시간 등의 부족으로 효율적인 취약점 진단이 어렵습니다. Zyroid를 도입하면 효율적인 취약점 진단과 컴플라이언스 대응이 가능합니다.

- 악성코드의 증가, 고도화
- 모바일 앱 보안사고의 증가
- 운영 앱에 대한 취약점 제거와 관리 필요

모바일 보안사고 증가

모바일 금융서비스 고객 증가

- 스마트폰 이용자의 증가
- 다양한 금융앱의 출시
- 스마트폰 전자금융 서비스 이용고객 증가

효과적인 취약점 진단, 컴플라이언스 대응 필요

- 모바일 전자정부 서비스 관리 지침
  - 제25조(취약점 점검)
- 금보원
  - 스마트폰 전자금융서비스 보안 가이드

컴플라이언스 [공공 / 금융]

취약점 점검 이슈

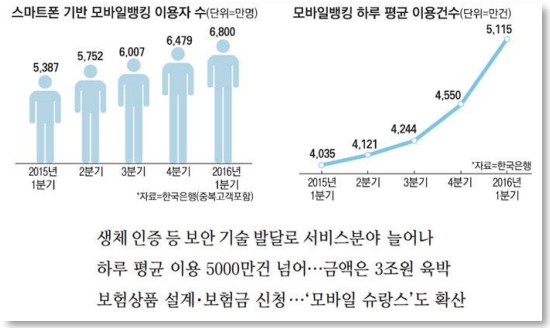
- 난독화 적용으로 인한 분석 난이도 향상
- 모바일 APP 점검을 위한 전문 인력 부족
- **인력 투입에 따른 비용, 시간 소요**

[스마트폰 전자금융서비스 안전대책 체크리스트]
- 앱 무결성 검증 포함-

영역	점검항목	세부내용
스마트폰 금융 보안대책	백신프로그램 적용	① 앱 실행 시 백신프로그램 구동 여부 (안드로이드 운영체제를 탑재한 스마트폰의 경우 해당)
		② 백신프로그램 최신버전 업데이트 여부 (안드로이드 운영체제를 탑재한 스마트폰의 경우 해당)
	입력정보 보호 대책 적용 여부	③ 주요정보 입력시 입력정보 보호 대책 적용 여부 (가상 보안키패드 등)
	금융정보 종단간 암호화 적용 여부	④ 스마트폰 앱과 금융회사 전자금융 서버간의 종단간 암호화(End-to-End) 적용 여부
	거래전문 무결성 검증기법 적용	⑤ 거래정보 무결성 정보생성 및 검증 여부
		⑥ 표준 통신규약 적용 여부
앱 위·변조 방지대책	폰 임의개조 탐지 및 차단 적용	⑦ 스마트폰 앱 실행시 폰 임의개조 탐지 및 차단 여부

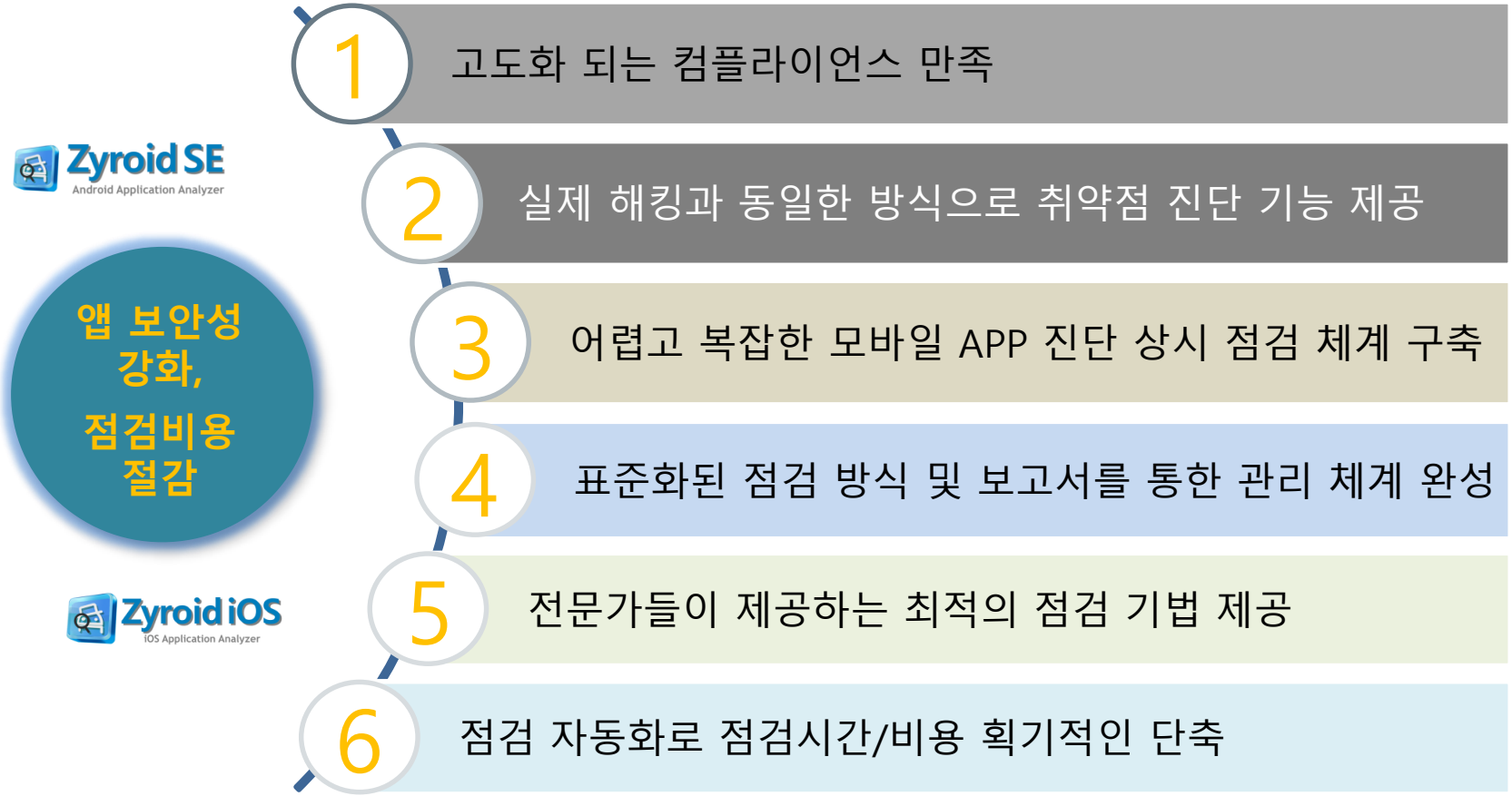
별표 1 모바일 서비스 앱 대상 보안취약점 점검기준

번호	점검 항목	설명	비고
1	반복 설치 시 오류 발생	앱 반복 설치 시 주요 설정 파일 변경 등의 문제가 발생할 수 있는 취약점	설치
2	앱 설치 전후 비정상적인 파일 및 디렉토리 설치	앱 설치 전후로 비정상적인 파일 및 디렉토리가 생성될 수 있는 취약점	설치
3	불필요하거나 과도한 권한 설정	불필요하거나 과도한 설정으로 앱 서비스 목적과 상이한 임의 기능 동작이 가능한 취약점	설치
4	앱 삭제 후 안전성	앱 삭제 시 관련(설치된) 디렉토리 및 파일 이외 파일이 삭제될 수 있는 취약점	삭제
5	기능의 정상동작	각 기능이 오동작할 수 있는 취약점 * 단, 인터페이스 관련 사항은 "모바일 애플리케이션 접근성 지침" 준수여부 등을 고려하여 판단할 수 있음	동작
6	임의기능 등 악성행위 기능 존재	앱 서비스 목적과 상이한 임의기능, 백그라운드에서 구동되는 악성행위 기능(프로세스 등)이 존재할 수 있는 취약점	동작
7	정보 외부 유출	허가된 주소 이외의 주소로 정보 전송이 가능한 취약점	동작
8	자원고갈	정상기능 오동작 또는 취약점을 통해 과도한 트래픽 사용 및 배터리를 고갈 시키는 취약점	동작
9	루팅 및 탈옥 기기에서의 정상 동작	루팅 및 탈옥된 기기에서 앱 설치·동작되어 보안메커니즘 우회 등이 발생할 수 있는 취약점	플랫폼
10	ID 값의 변경	안드로이드 플랫폼에 설치되는 앱에 부여되는 app_### 과 같은 일반 권한의 UID, GID 등 ID가 임의로 변경될 수 있는 취약점	플랫폼 (Android)



기대 효과

모바일 APP 취약점점검 솔루션 Zyroid의 다양한 기능을 통해 앱의 보안성이 향상되며 취약점 점검을 위한 인력, 비용, 시간이 절감됩니다.



제품 구성

본 제안의 세부 내역은 "모바일 APP 취약점 점검용 노트북(Windows, Mac)" 2식과 "Zyroid SE, iOS 소프트웨어" 2식, 그리고 "Nexus 단말기" 1식과 "아이폰 단말기" 1식으로 구성되어 있습니다.

제품 구성도

제안 세부 내역

구 분	항 목	수 량
모바일 APP 취약점 점검 솔루션 (Zyroid SE, iOS)	취약점 점검용 노트북	2식
	Zyroid SE, iOS소프트웨어	2식
	Nexus 단말기 (USIM 미지원)	1식
	아이폰 단말기 (USIM 미지원)	1식
	제품 매뉴얼	2식

유지보수 및 기술지원		횟수
교 육	사용자 기본 교육 (Zyroid 사용법 및 기본점검)	분기별 1회 (또는 요청시)
	사용자 심화 교육 (취약점의 이해와 조치 방법)	분기별 1회 (또는 요청시)

제품 특장점

모바일 환경에서의 해킹 기술은 진화하고 있으나 인적(전문가), 물적 자원의 부족으로 인한 대응 능력의 한계와 다양한 보안 요구사항의 수용능력의 제한 등은 점검 기준 및 절차의 표준화가 요구되고 있으며 Zyroid는 기술적, 관리적(컴플라이언스) 측면에서 향상된 보안 점검을 수행합니다.

실제 단말기 사용	안드로이드 가상 에뮬레이터가 아닌 실제 단말기를 사용
동적 Hooking 사용	단말기 독립적 동적 Hooking 을 통한 소스 및 바이너리를 수정 없이 분석 가능
Proxy / Debugger 기능	호출되는 API의 입/출력 값 실시간 분석/수정 가능 진단 APP의 전반적인 API 호출 흐름 파악 가능
표준화된 점검 가능	표준화된 점검 기준 적용을 통한 분석 결과의 신뢰성 향상
악성앱 분석 기능	사용자 정보 유출 및 권한 상승 등 악의적인 행동을 하는 악성앱 분석 가능
형상관리 기능	점검 후 수정 된 코드에 대한 형상관리로 수정 이력 확인 가능

타사 대비 장점

컴플라이언스 충족
스마트폰 전자금융 서비스 보안가이드
정보통신망법

난독화 된 앱 분석
난독화 적용 앱에 대한 분석 및 해제 기능 제공

수준 높은 점검환경
정밀분석을 위한 다양한 정보 제공, 시스템이 판단하기 힘든 항목 점검 가능

자동 패킷 분석
발생된 네트워크 패킷 자동분석 및 rePlay 기능

메모리 중요정보 분석
앱 동작 중 메모리를 분석하여 중요정보 노출 분석

Zyroid

실시간 API 분석
점검자 PC에서 APP API의 실시간 분석 및 조작

편리한 자동점검
점검을 위한 기본 정보 입력 후 자동점검

악성앱 탐지 가능
행위기반 판단을 통해 악성앱 검증 가능

콜 다이어그램
강력한 코드 분석을 위한 콜다이어 그램 지원

쉬운 사용자 입력
스마트폰과 PC 동기화 후 키보드와 마우스로 스마트폰 조작

주요 사업 실적

제조사 ㈜라온시큐리티 동종 및 유사 분야 사업 실적입니다.

	사 업 명	계약처	사업 기간	동종/유사
1	모바일 App 취약점 점검 솔루션 구축(Zyroid SE, iOS)	KB국민은행	2018.06	동종
2	모바일 App 취약점 점검 솔루션 구축(Zyroid SE)	해군	2018.05	동종
3	모바일 App 취약점 점검 솔루션 구축(Zyroid SE, iOS)	동서발전	2018.01	동종
4	모바일 App 취약점 점검 솔루션 구축(Zyroid iOS)	SK텔레콤	2017.11	동종
5	모바일 App 취약점 점검 솔루션 구축(Zyroid DE)	LG유플러스	2017.08	동종
6	모바일 App 취약점 점검 솔루션 구축(Zyroid SE)	CJ올리브넷	2016.02	동종
7	모바일 App 취약점 점검 솔루션 구축(Zyroid SE)	KB손해보험	2015.12~2016.03	동종
8	앱 취약점 점검 솔루션 구축(Zyroid SE)	SKP	2015.10~2015.11	동종
9	앱 취약점 점검 솔루션 구축(Zyroid SE 개발자버전)	SKT	2015.08~2015.11	동종
10	악성행위 탐지 솔루션 구축(Zyroid Enterprise)	삼성전자	2014.01~2014.03	유사
11	악성행위 탐지 솔루션 구축(Zyroid)	KT	2013.12~2014.01	유사

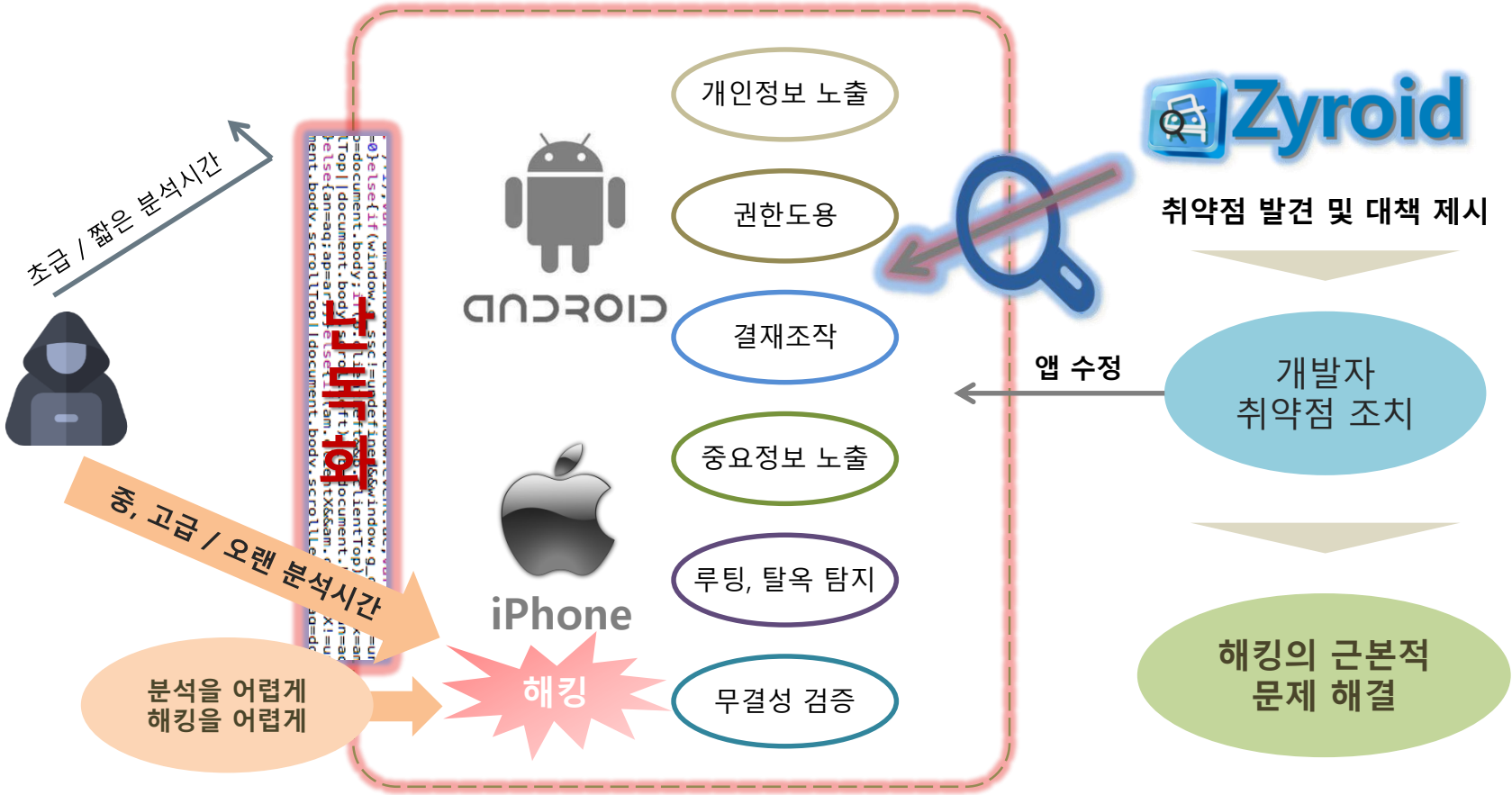
유사 제품 비교

현재 공개되어 있는 유사제품 중 컴플라이언스, API Hooking, 취약점 관리 등에서 최고의 성능을 보여주고 있습니다.

경쟁사		Raonsecurity	A사	B사
구성		단말기 <-> PC	단말기 <-> PC	Cloud
점검 난이도		쉬움	어려움	쉬움
정적 점검	소스코드	O	O	O
	난독화 여부	O	-	-
	디버그 버전	O	-	-
	하드코딩 중요정보	O	O	-
동적 점검	개조 폰 탐지	O	-	-
	위변조 탐지	O	-	-
	메모리 검사	O	O	-
	난독화 해제	O	-	-
	네트워크 분석	O	O	O
	storage 분석	O	O	-
	Database 분석	O	O	-
실시간 점검	API Hooking	O	-	-
	API Trap	O	-	-
	API Modify	O	-	-
보고서 포멧	PDF, HTML, CVS	O	△	△
취약점 화면 스크린 샷		O	O	O
점검결과 형상관리		O	-	-

난독화 솔루션과의 차이점

난독화 솔루션은 앱에 존재하는 취약점을 수정하지 않고 분석을 어렵게 하는 솔루션입니다. 그러므로, 오랜 분석과 고급 해킹 기술에 의해 우회될 수 있습니다.
Zyroid 솔루션은 앱에 존재하는 취약점을 스캔하여 개발자가 문제를 해결하도록 도와주므로 근본적인 문제점을 해결할 수 있습니다.



제안 내용 II

II-1. 장비 소개
II-2. 장비 기능

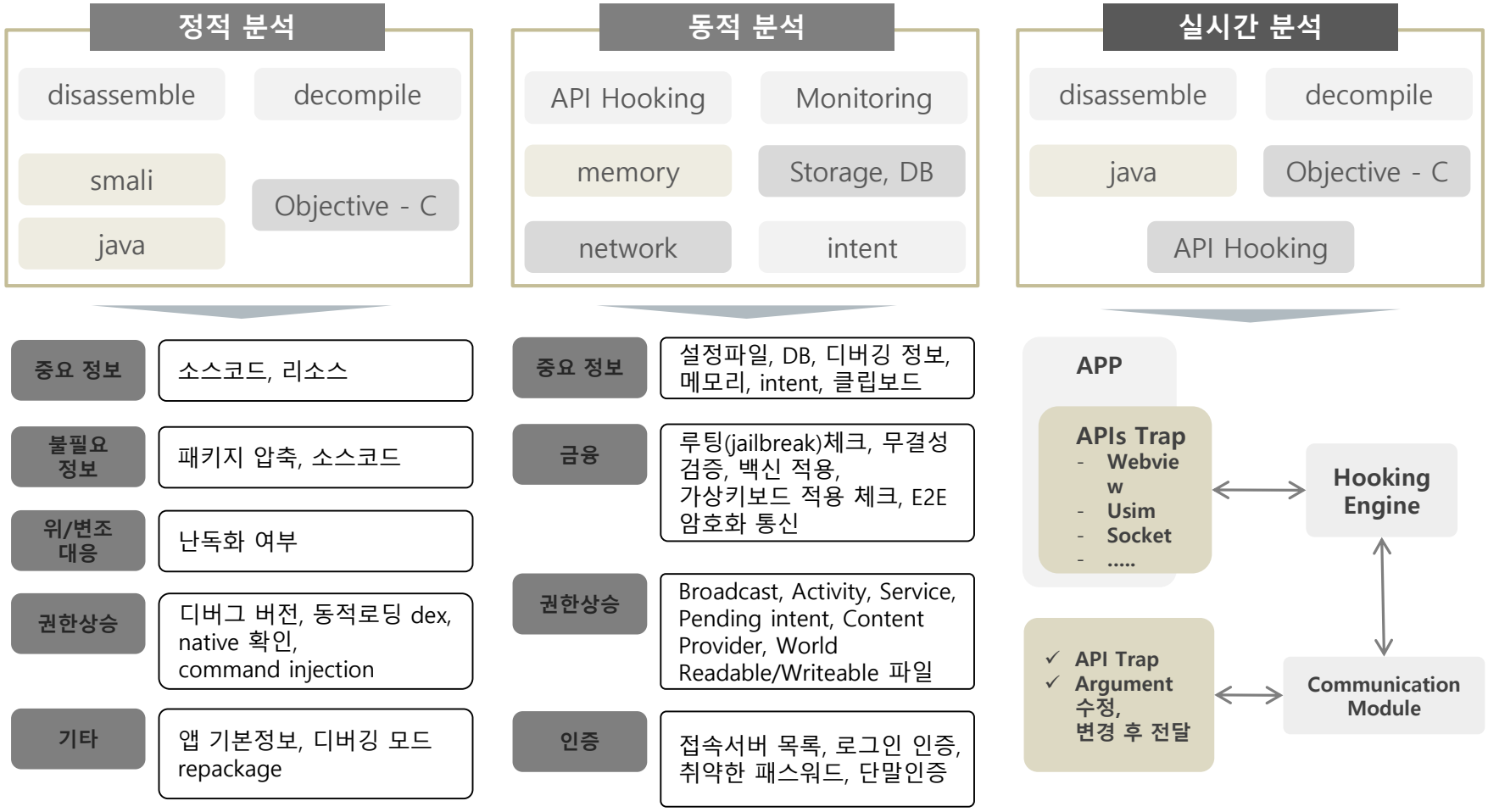
장비 소개

II-1.1 제품 구성

제품의 구성은 점검용 노트북, Zyroid SE, Zyroid iOS, Nexus 단말기, iOS 진단 단말, USB Cable로 구성되어 있습니다.
PC와 동기화 후 PC 스크린상에서 키보드와 마우스를 이용해 단말기 조작 및 데이터 입력이 가능합니다.

II-1.2 Zyroid 취약점 분석

정적분석 : 앱 파일을 Disassemble, Decompile을 통해 소스코드, disassemble code 에서 보안취약점을 점검 합니다.
동적분석 : 앱 동작 중에 네트워크, log, memory, files, API 의 변화를 모니터링 하여 보안취약점을 점검 합니다.
실시간분석 : 소스코드 분석 후 특정 API에 Trap을 걸어 동작을 멈춘 상황에서 변수를 조작하여 앱 취약점을 점검할 수 있습니다.



장비 기능

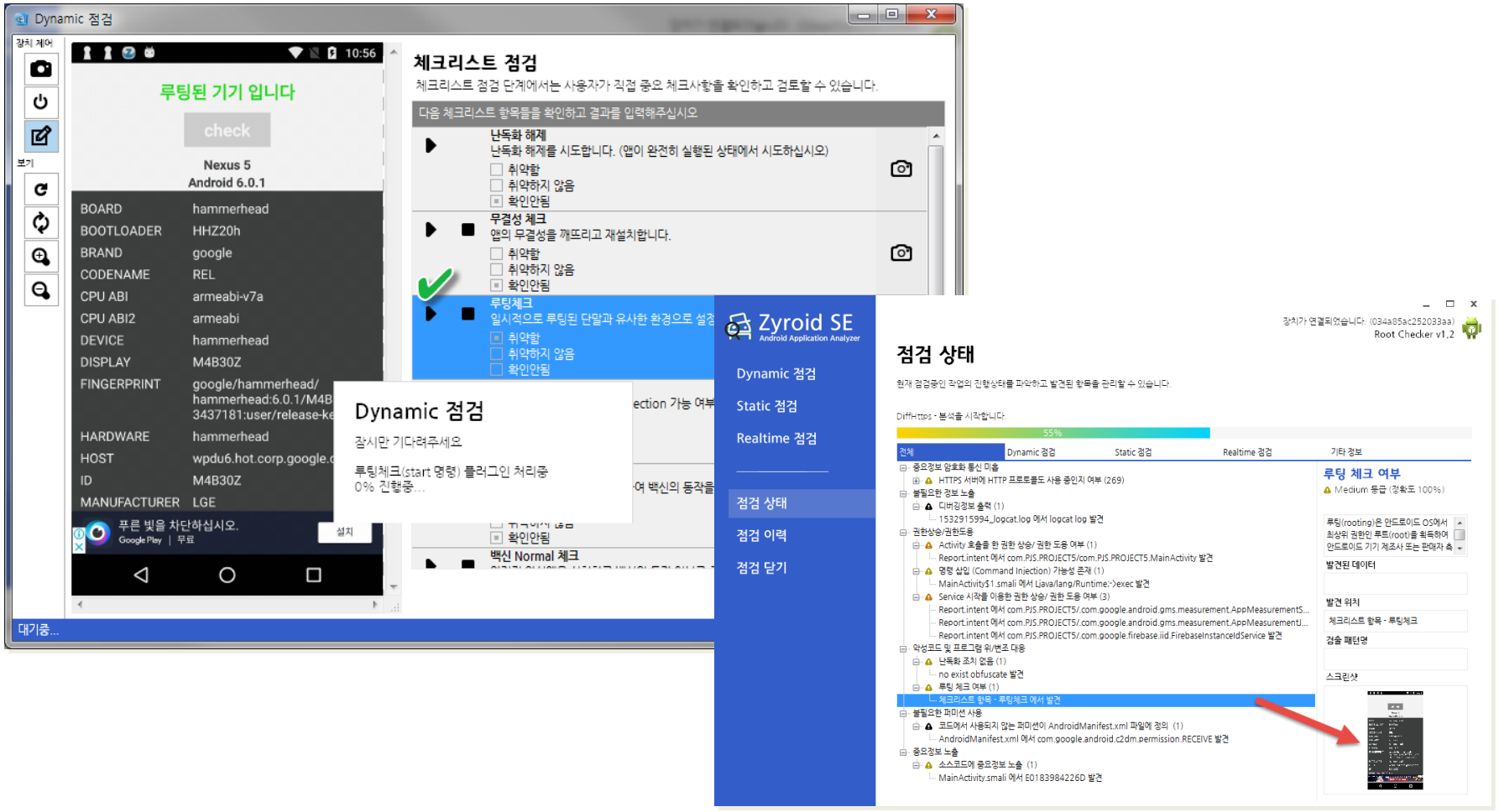
Zyroid는 앱 자체 취약점은 물론 컴프라이언스 항목 점검을 위한 기능을 포함하고 있으며 해당 취약점에 대한 설명과 보안대책을 제시하고 신규 취약점 업데이트를 지원하고 있습니다.

No.		비고	No.		비고
1	PC, Device의 APP 분석 기능		**11**	**지정된 프로세스가 호출하는 시스템 콜 추적 기능**	
2	실제 물리디바이스를 대상검사 기능		12	입력 값 검증(SQL injection, 경로조작, XSS)에 대한 자동/수동 진단 기능	
3	**실시간 점검화면을 PC에서 제공**		13	취약점 내용 스크린샷 및 설명기능	
4	루팅(jailbreak)폰 탐지 기능		14	분석결과 오탐 제외 기능	
5	앱 무결성 검증 기능		**15**	**취약점 별 위험도 변경 기능**	
6	메모리 중요정보 평문 노출 분석 기능		**16**	**분석결과 형상관리**	
7	**패킷 수준의 네트워크 분석 기능**		17	보안권고안 및 조치 방안 제공	
8	**중요정보 평문 저장 분석 기능**		18	다양한 보고서 유형 지원	
9	시스템 로그 추출 및 저장 기능		19	보고서 한글 지원	
10	**난독화 앱 분석 기능**		20	보안 위협 식별을 위한 지속적인 업데이트 지원	

장비 기능

II-2.1 rooting & jailbreak 단말기 탐지 기능

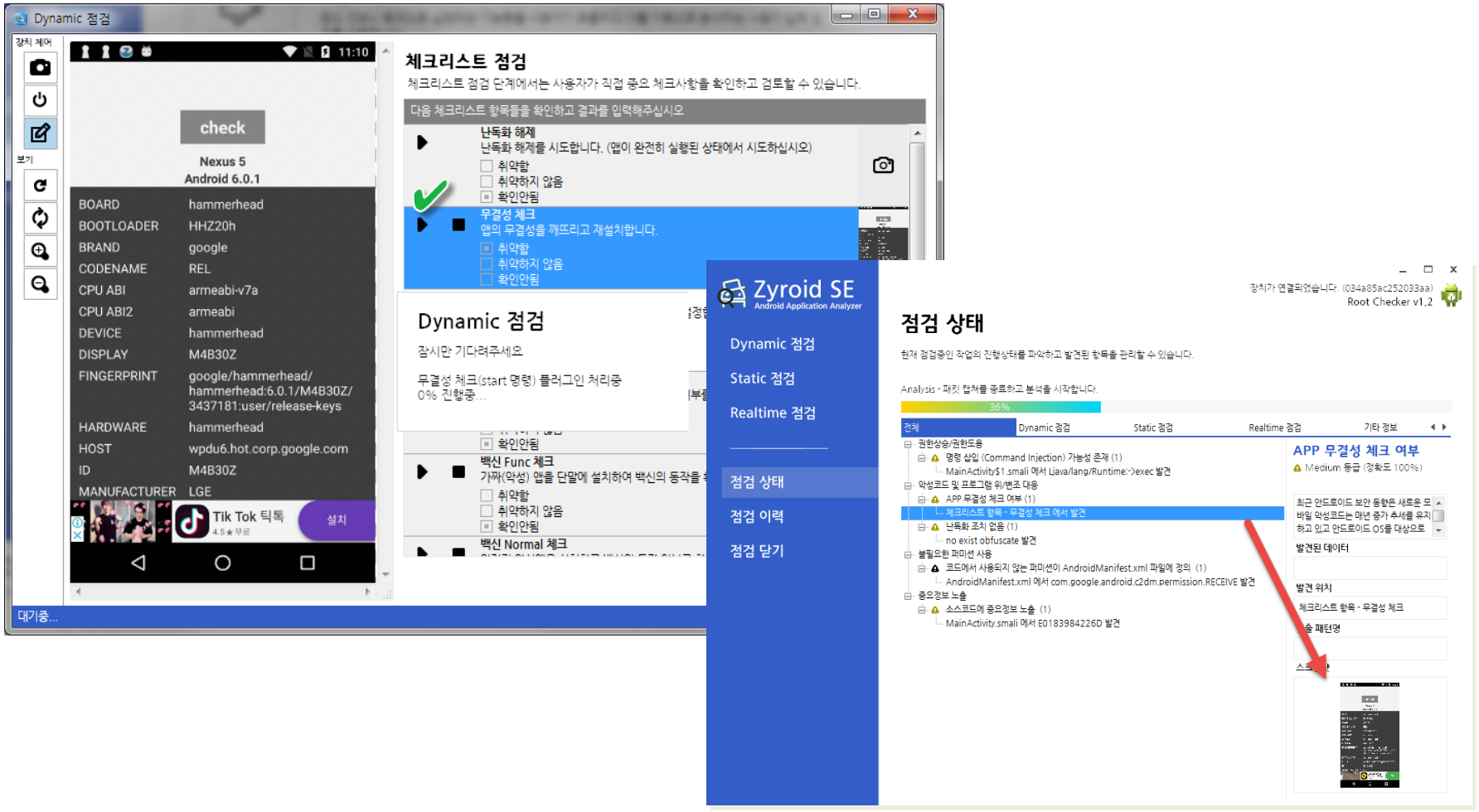
금융 앱의 안전한 동작을 위해 변조된 단말기에서 실행을 금지하고 있습니다.
Zyroid는 앱 동작 중 단말기의 루팅(jailbreak) 상태를 체크하고 있는지 버튼 한번의 동작으로 확인하고 보고서에 반영합니다.



장비 기능

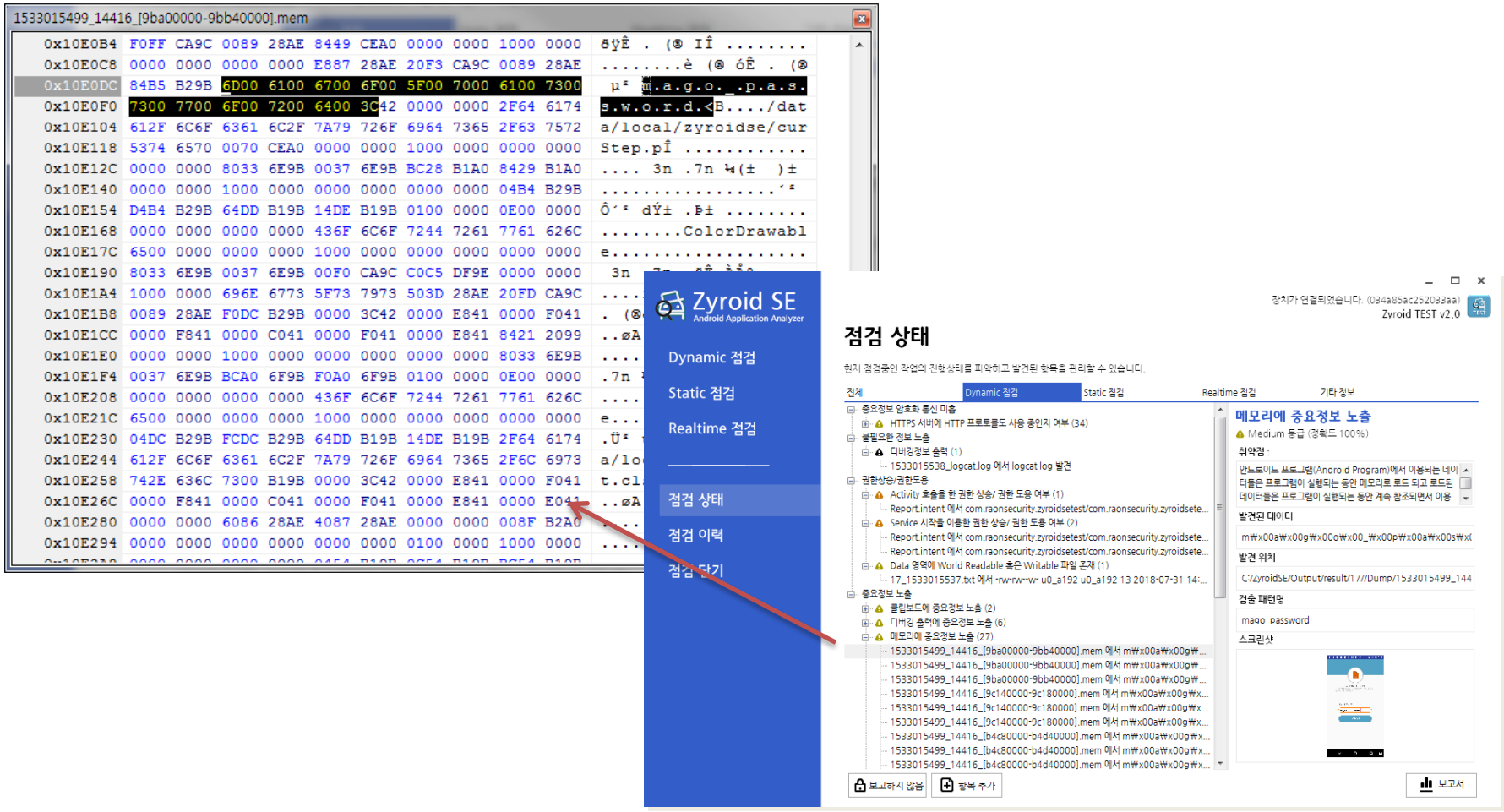
II-2.2 앱 무결성 검증 기능

금융 앱으로 위장해 정보를 유출하는 악성앱의 실행을 금지하기 위해 위·변조 방지 솔루션이 작동되고 있는 상황에서 Zyroid는 버튼 하나로 변조된 앱을 체크하고 있는지 판단하고 결과에 반영합니다.



II-2.3 메모리 중요정보 평문 노출 분석 기능

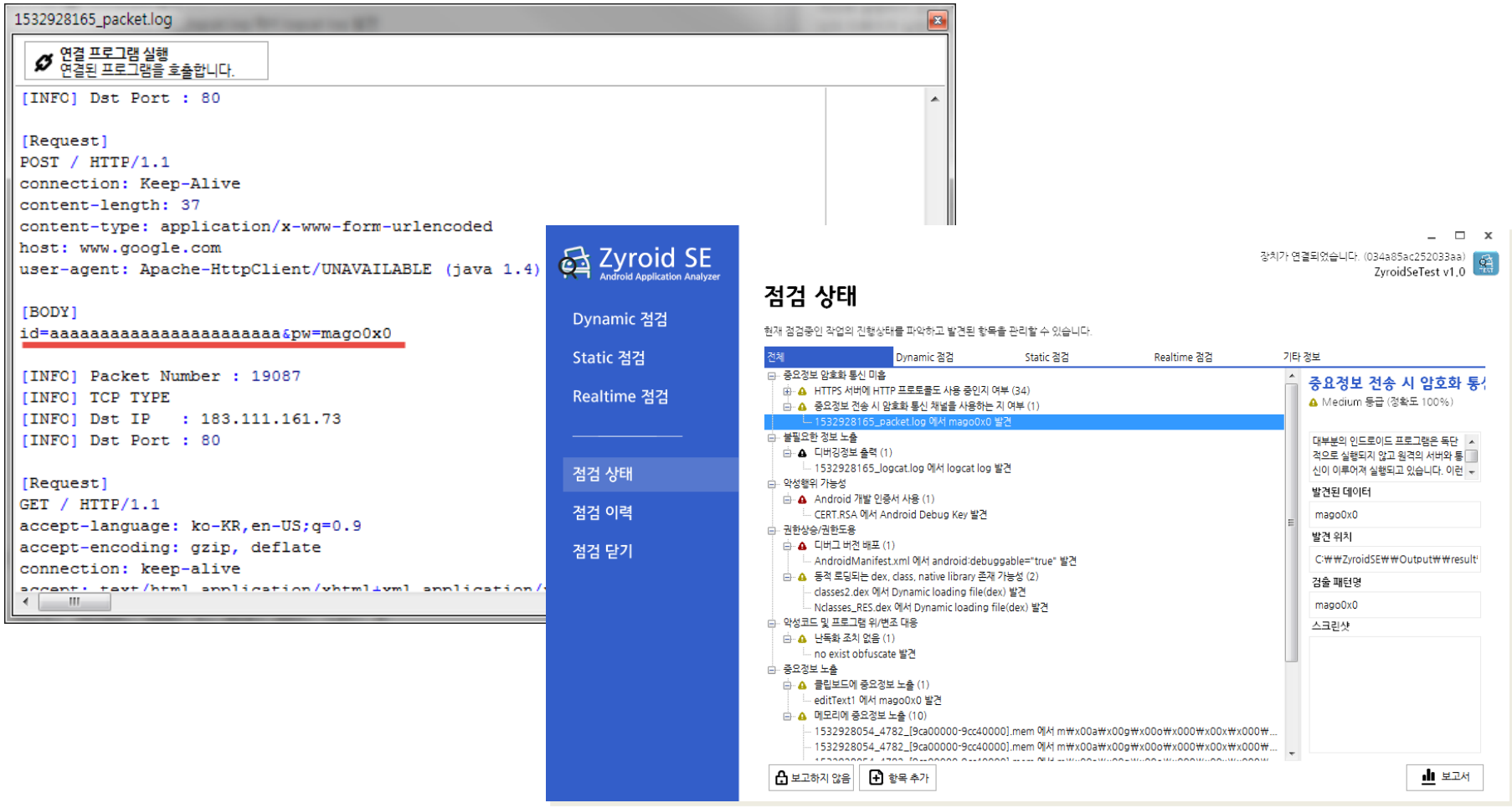
앱 동작 중 메모리에 중요정보(password, 주민번호, 계좌번호)가 평문으로 노출되어 있는지 또 노출되어 있다면 어떤 화면에서 노출되었는지 한번의 실행으로 점검이 가능하며 이를 보고서에 반영합니다.



장비 기능

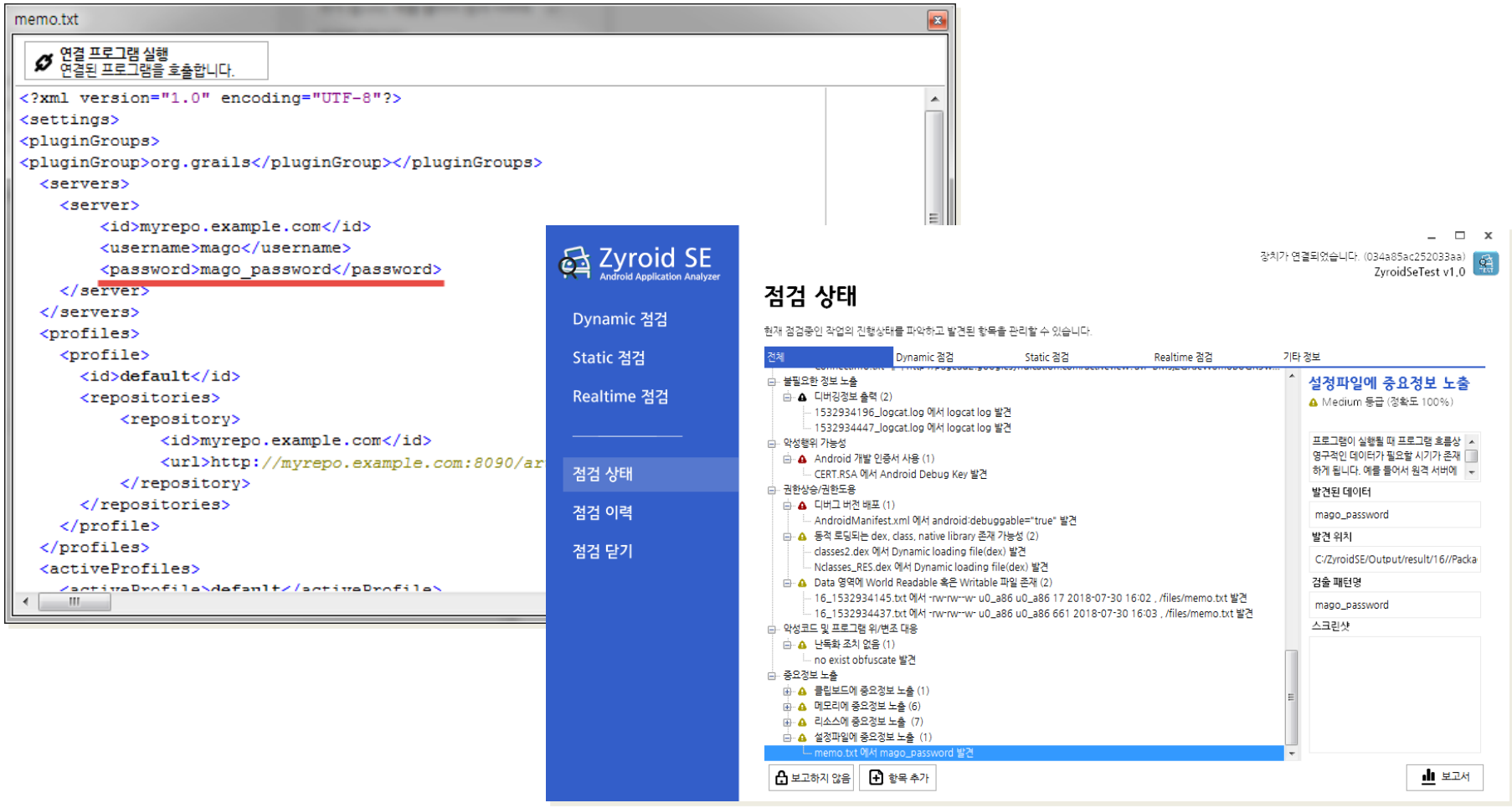
II-2.4 패킷 수준의 네트워크 분석 기능

Zyroid의 패킷 분석 기능은 모든 네트워크를 동시에 모니터링하고 패킷 데이터를 텍스트 수준으로 분석하여 사용자에 제공하고 중요정보가 평문으로 전송되는지를 한번 실행으로 점검하고 분석된 패킷을 재전송할 수 있는 강력한 기능을 제공합니다.



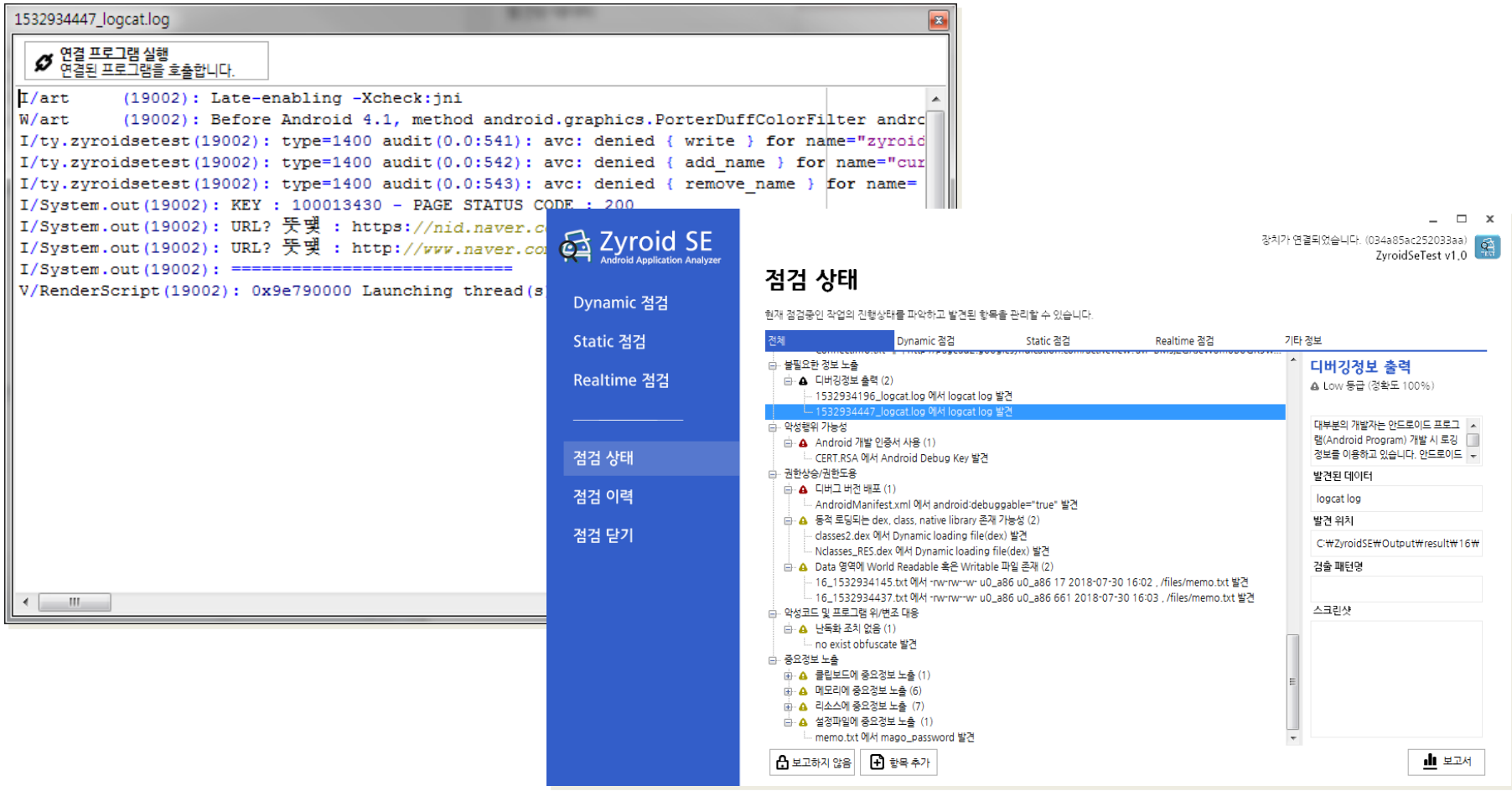
II-2.5 중요정보 평문 저장 분석 기능

Zyroid는 앱이 동작하는 동안 Setting, Cache, DB, Sdcard, Clip board 에 변화를 모니터링 하여 평문으로 저장되는 데이터를 감지하여 점검하는 강력한 기능을 제공합니다.



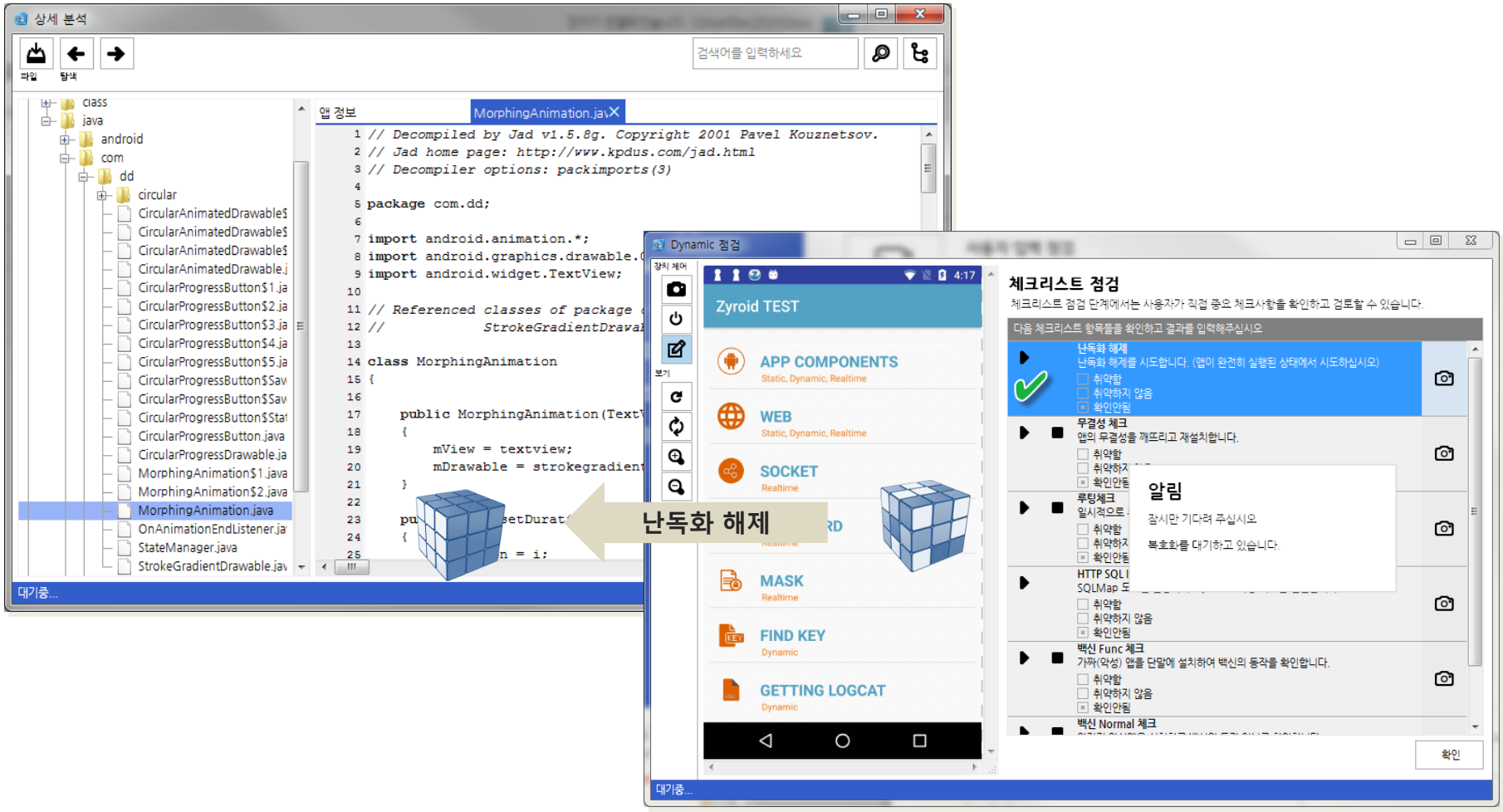
II-2.6 시스템 로그 추출 및 저장 기능

Zyroid는 시스템 로그는 물론 해당 앱이 발생하는 모든 로그를 기록하고 분류하여 중요한 정보가 유출되는지를 점검자에게 전송하고 해당 중요정보가 로그에 포함되는지를 점검합니다.



II-2.7 난독화 앱 분석 기능

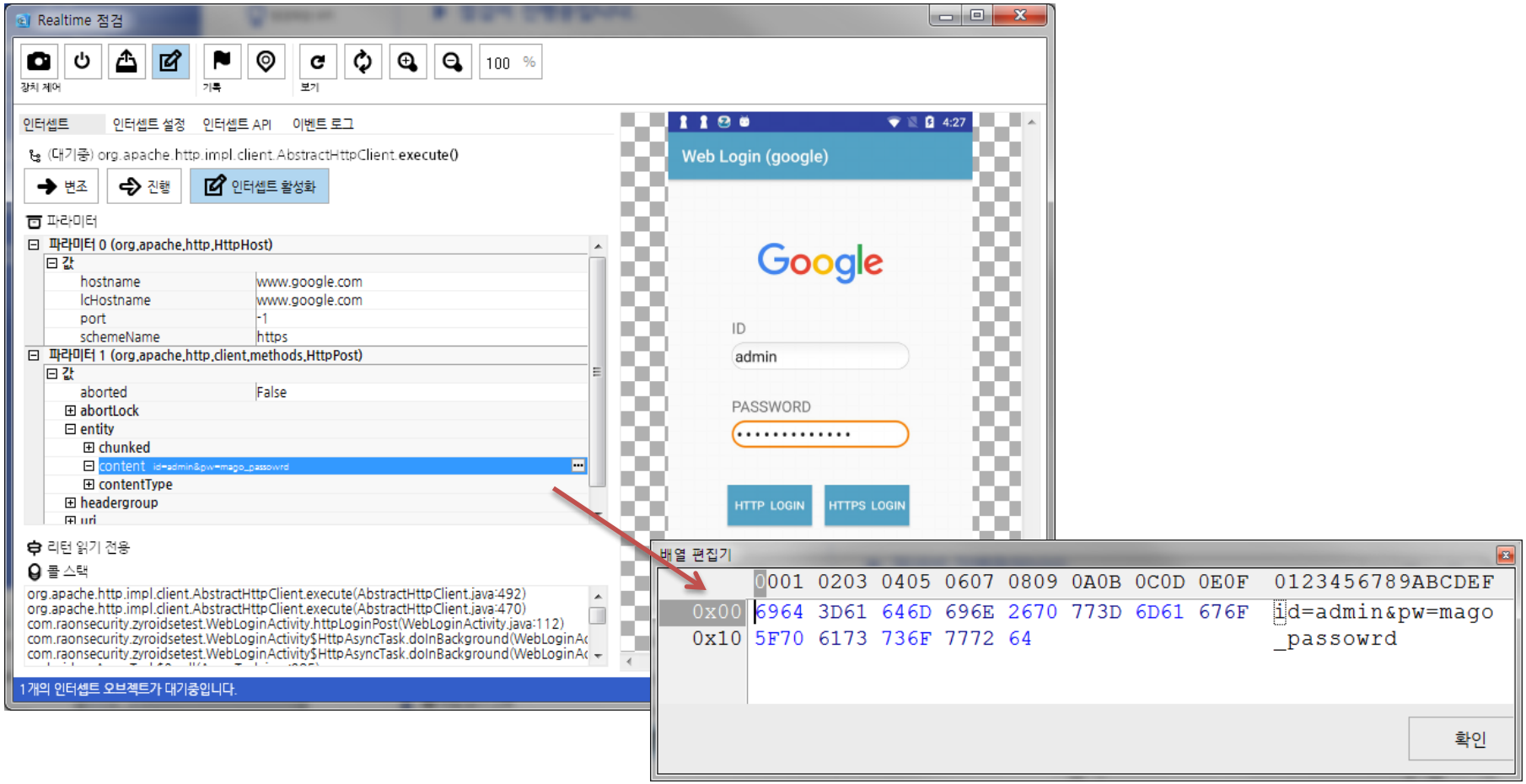
난독화된 앱인 경우 사용자의 소스코드 분석을 돕기 위해 강력한 난독화 해제(암호해제, 문자열 치환) 기능을 지원하고 있습니다.



장비 기능

II-2.8 개별 API(JAVA, C) 실시간 조작 기능

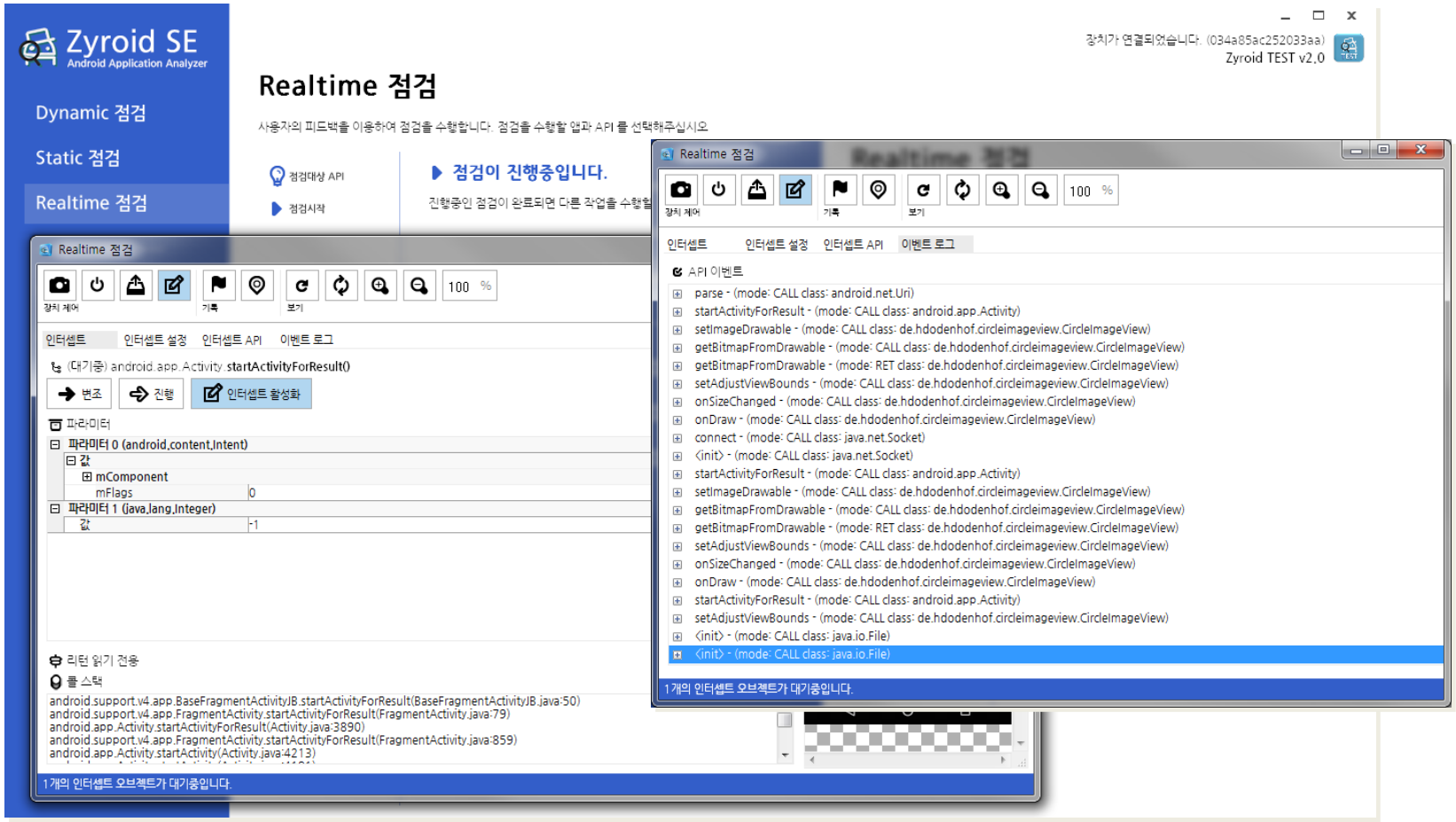
실시간 분석은 단말기내에 설치된 Hooking engine을 통해 앱 동작시 사용되는 API를 hooking하고 변조, 추적할 수 있는 기능을 내장하고 있고 이를 이용해 네트워크(Wifi, 4G), API 관계없이 Trap을 걸어 변조할 수 있는 강력한 기능을 지원합니다.



장비 기능

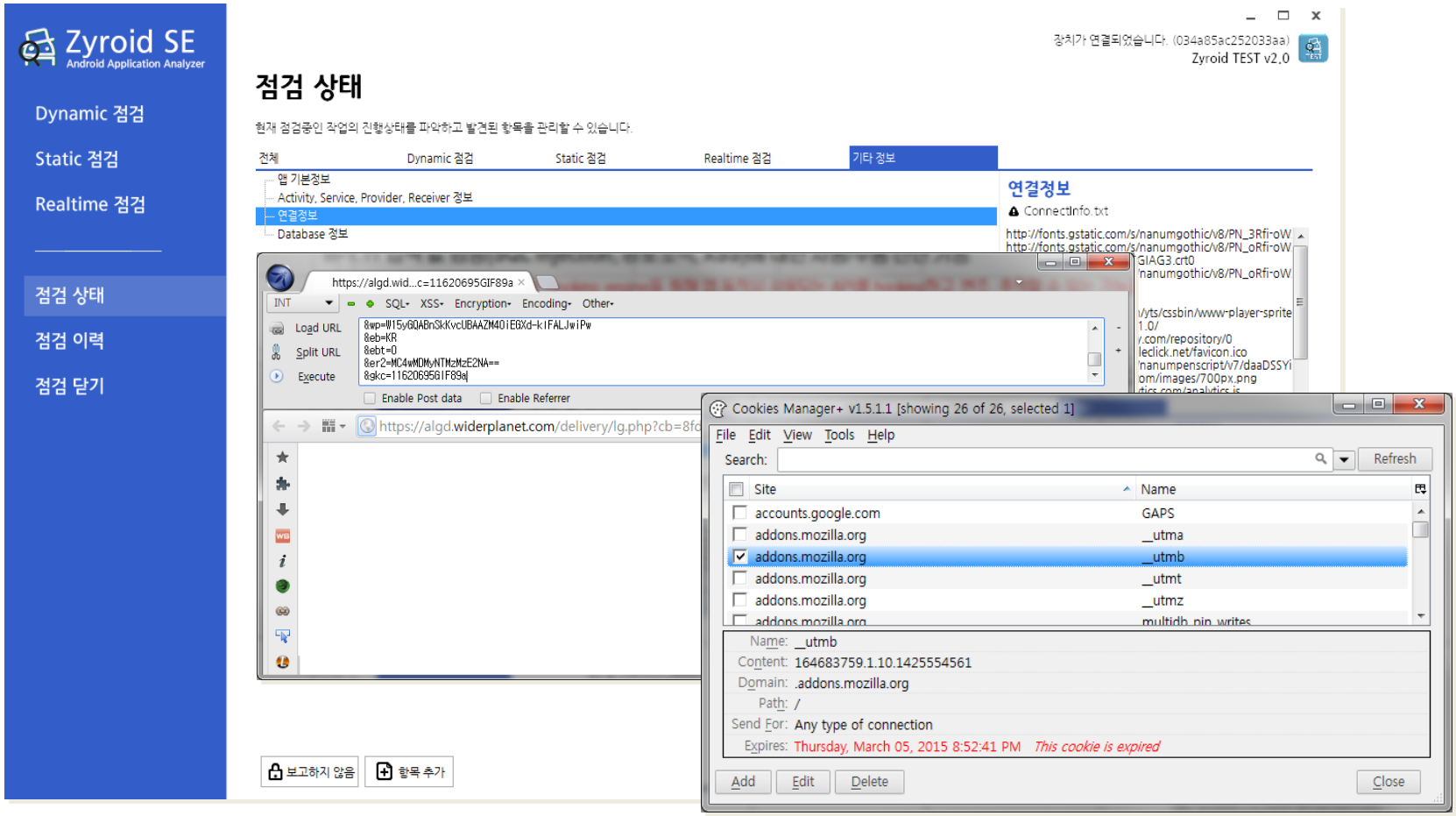
II-2.9 지정된 프로세스가 호출하는 시스템 콜 추적 기능

앱이 실행되는 동안 단말기내에 설치된 Hooking engine을 통해 앱 동작 시 호출되는 API 이벤트를 모두 기록하고 분류하여 사용자에게 제공하여 강력한 API 추적기능을 제공합니다.



II-2.10 입력 값 검증(SQL injection, 경로조작, XSS)에 대한 자동/수동 진단 기능

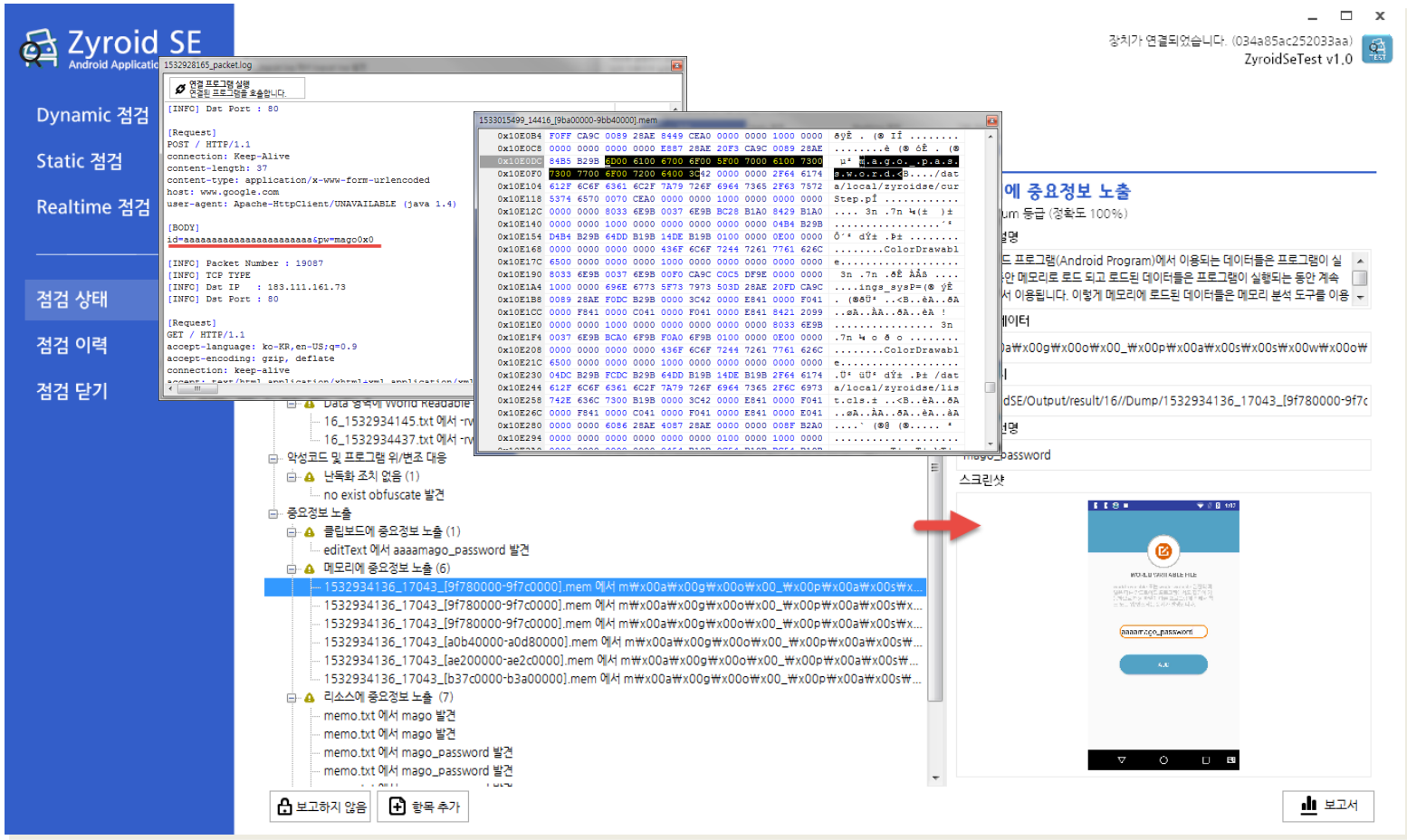
Zyroid는 앱 동작 중 발생되는 모든 통신을 모니터링하고 저장하고 있고 이를 이용하여 외부 프로그램(Sql injection tool, Hack Browser)을 연동할 수 있는 추가 기능을 지원하고 있습니다.



장비 기능

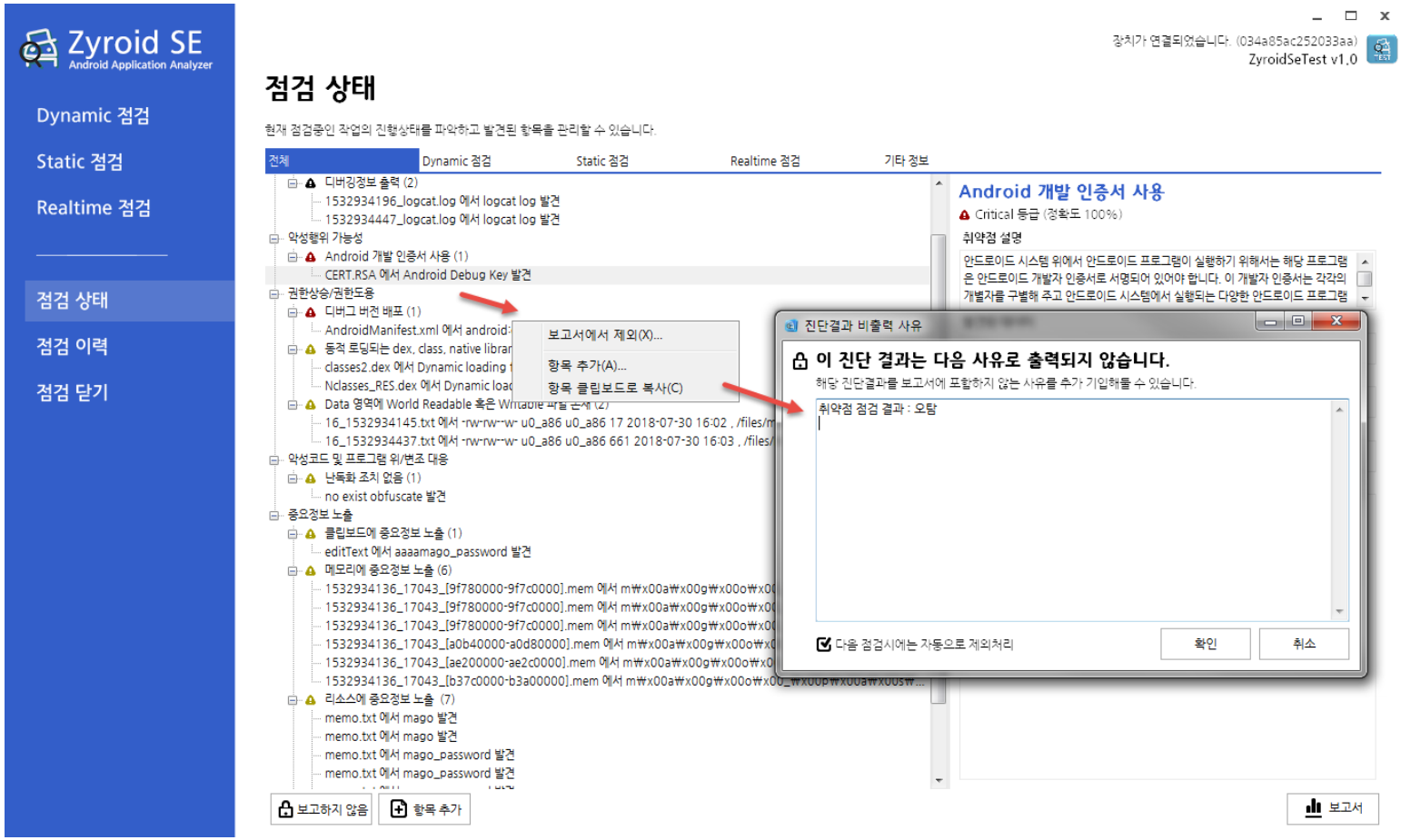
II-2.11 취약점 내용 스크린샷 및 설명기능

발견된 취약점 화면 스크린샷은 물론 네트워크, 메모리, 파일 등위 취약한 결과(파일, 메모리, DB)를 보고서에 추가 함으로써 취약점 이해도를 극대화 하고 있습니다.



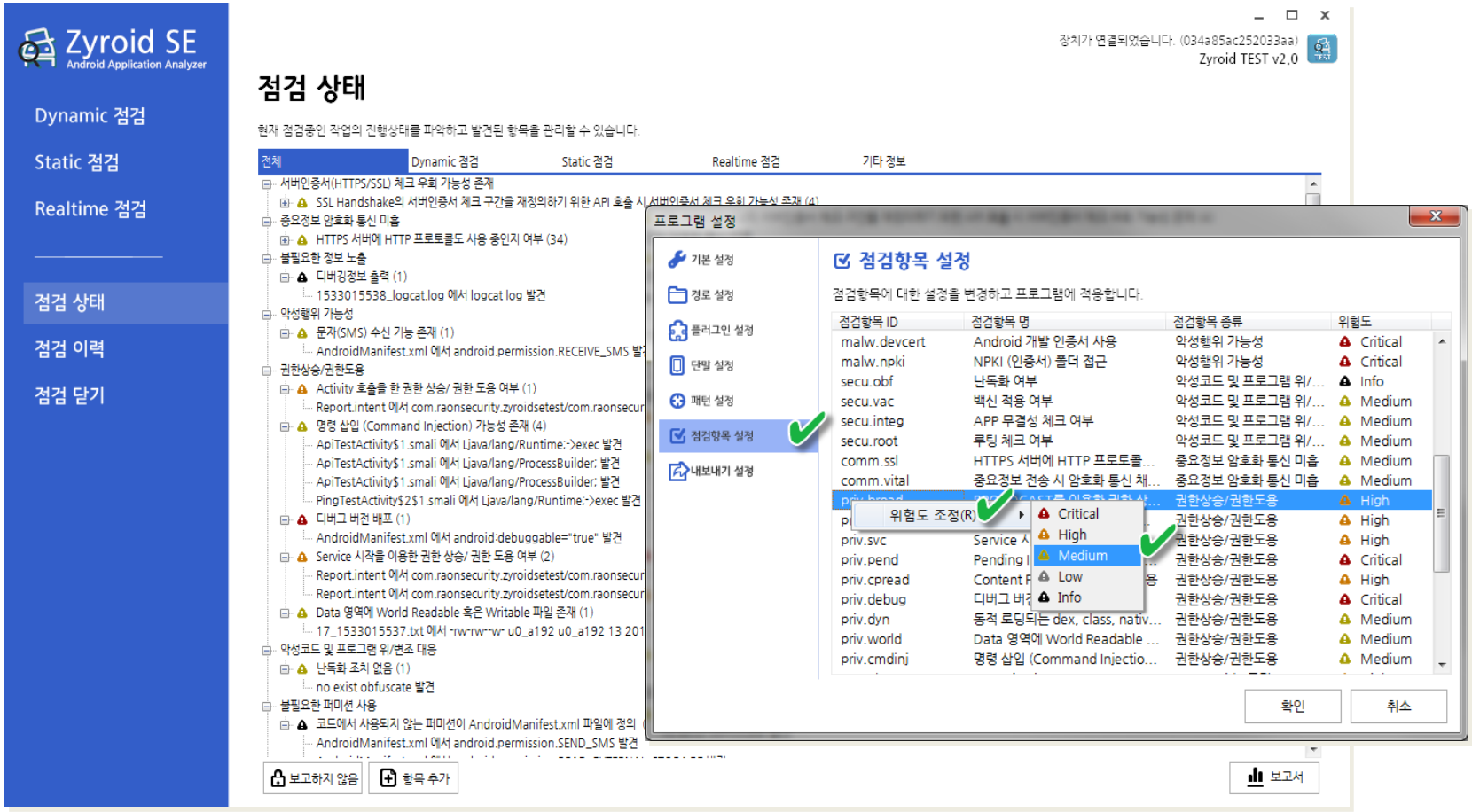
II-2.12 분석결과 오탐 제외 기능

자동으로 취약점 진단을 진행하는 동안 발생할 수 있는 오탐을 제거하기 위해 점검결과 화면에서 간단한 클릭으로 오탐 된 취약점을 보고서에서 제거하는 기능을 제공합니다.



II-2.14 취약점 별 위험도 변경 기능

고객사 실정에 맞는 결과를 도출하기 위해 점검자가 각각의 점검항목의 위험도를 조정하거나 제외 할 수 있는 메뉴를 제공하고 있습니다.



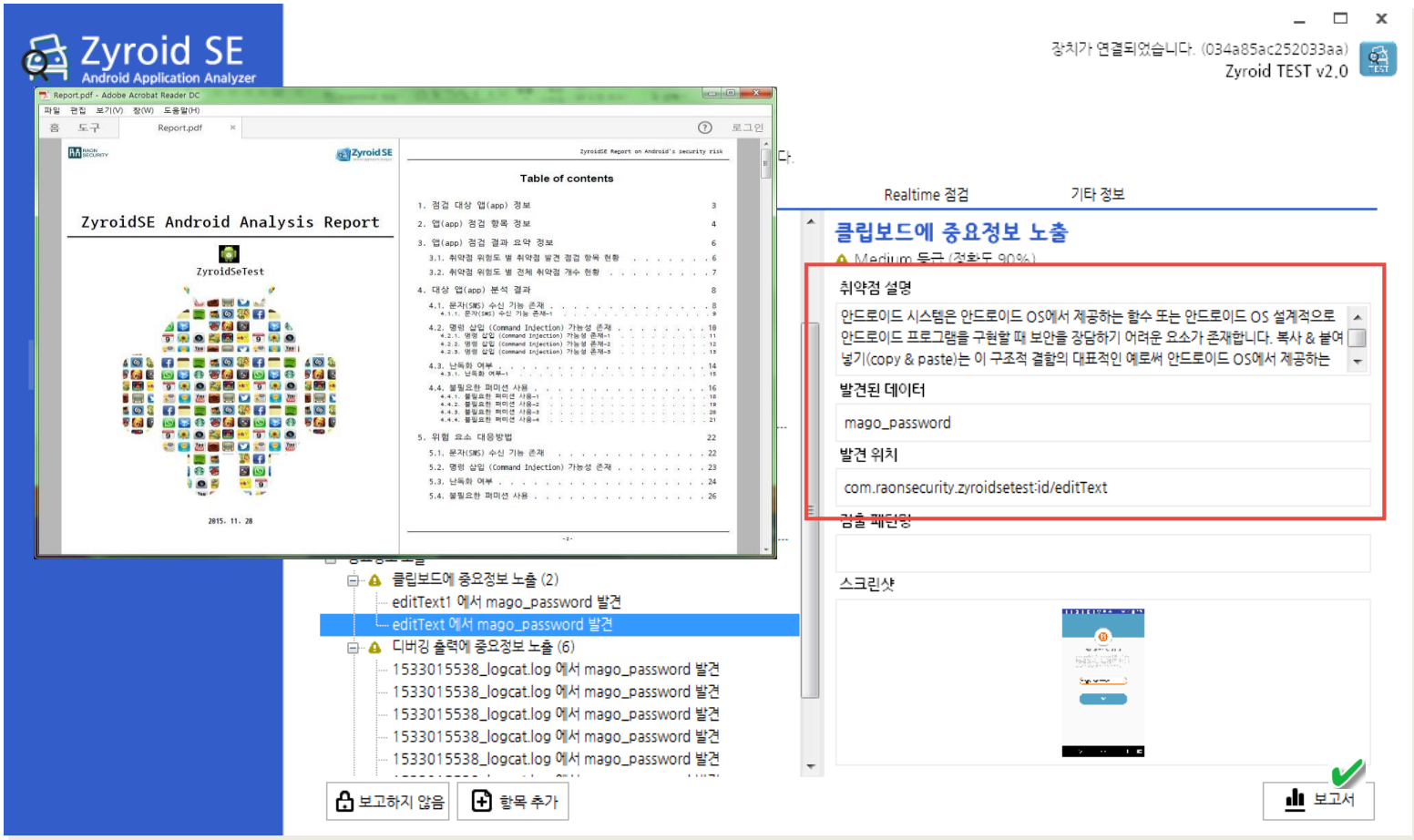
II-2.15 분석결과 형상관리

대상 앱 버전 별 취약점 결과를 비교하고 차이를 분석할 수 있는 기능을 제공하여 버전에 따른 형상관리 기능을 제공합니다.

장비 기능

II-2.16 보안권고안 및 조치 방안 제공

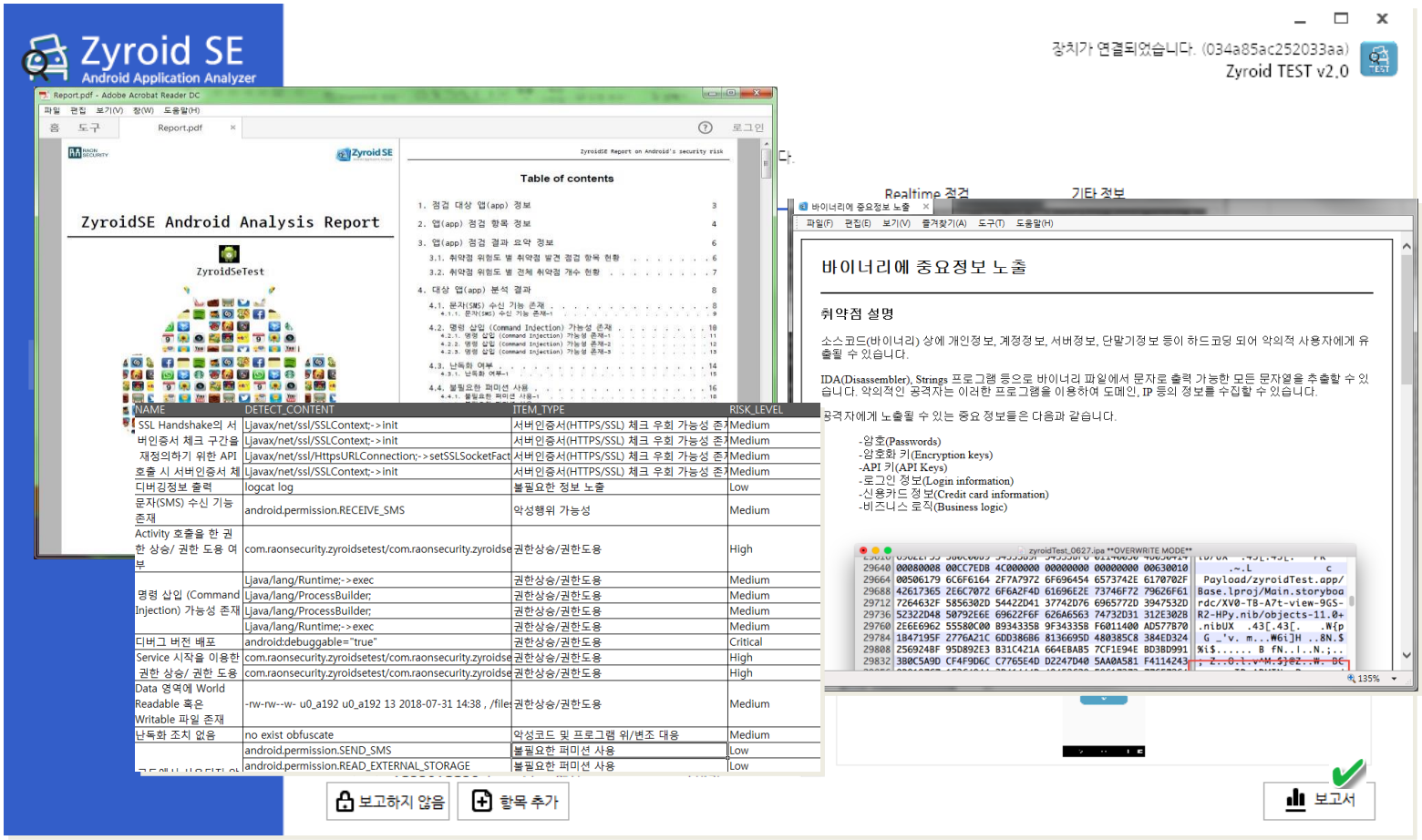
모든 점검이 완료되고 오탐을 제거하면 컨설턴트 수준의 취약점 설명, 결과, 조치방안을 보고서와 점검결과에서 확인할 수 있습니다.



장비 기능

II-2.17 다양한 보고서 유형 지원

고객사 환경을 지원하기 위해 Zyroid는 다양한(PDF, WEB, CVS, Word) 문서 포멧을 지원합니다.



관리 계획 III

III-1. 유지보수 방안
III-2. 유지보수 내용 및 범위
III-3. 교육지원

관리 계획

III-1 유지보수 방안

모바일 APP 취약점 점검 솔루션 구축 후 유지보수 체계를 수립하고 절차에 따라 유지보수 활동을 수행하며, 제품에 문제가 발생할 경우 장애처리 절차에 의거하여 신속하게 조치하겠습니다.

유지보수 활동

- 무상 유지보수 계획서 제출(인력, 조직, 방안)
- 무상 유지보수(검수완료일로부터 12개월)
- 24시간 x 365일 지원 및 정기점검활동, 비상시 긴급 정비활동
- S/W 버전 및 패턴 업그레이드, 정기적 적용
- 운영매뉴얼 버전관리 및 제공

기술지원 활동

- 유지보수 엔지니어를 통한 기술지원활동
- 시스템 운영자 및 업무 담당자를 위한 기술지원 활동
- 문제점 및 개선요구사항 지원

서비스 범위

- 솔루션 구축 후 안정화 기간 동안 체계적인 인수 테스트 진행
- 구축 솔루션에 대한 정기 유지보수
- 장애 상황 진단 및 처리

유지보수 방안

- 업무별 세분화된 지원
- 24시간 장애접수
- 비상연락망 구축 (2선 지원체계 수립)
- 모니터링과 정기점검, 예방점검으로 장애 예방
- 필요 시 시스템에 대한 특별점검

장애 복구

- 장애발생시 최단시간 내 조치, 복구 및 사후관리(이력관리)
- 장애발생시 장애원인, 조치결과, 원인분석 및 재발 방지책 마련
- H/W 주요 예비 부품 비치
- 장애처리 결과 보고서 제출

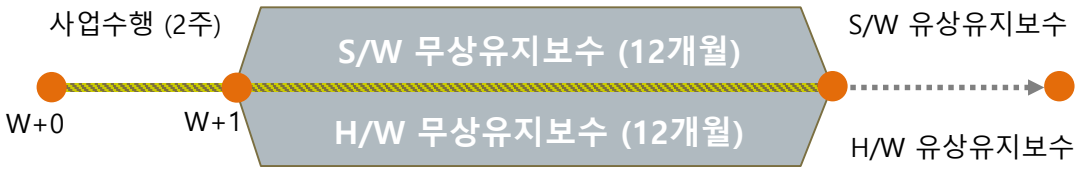
기술 지원

- 시스템의 효율적 운영과 보안기술 향상을 위한 기술자문 및 지원
- 조직변경이나 담당자 변경 시 요청에 의한 교육
- 고객의사 소통채널 확보
- 업그레이드 및 신규 버전에 대한 최신 보안 동향에 대한 자료 및 기술 제공

관리 계획

III-2 유지보수 내용 및 범위

유지보수는 유상유지보수와 무상유지보수로 구분되며, 무상유지보수 기간은 최종 검수 완료 후 1년으로 하여 시스템 설치 및 관리 전문 기술인력 지원을 통해 시스템 안정화 및 운영지원 활동을 수행합니다.



- 납품장비에 대한 하자보수, 재설치 또는 패치
- 장애신고 접수 최단시간내 장애처리, 정기/비정기 예방점검
- 시스템 운영자를 위한 기술지원
- 장애, 운영상태, 운영자 Q&A에 대한 Help Desk 운영

구 분	무상 유지보수 범위	유상 유지보수 범위
수행기간	▪ H/W , S/W 검수 후 1년	▪ 무상 유지보수 이후 별도 유지보수 계약에 의거
일반 사항	▪ 정기점검, Trouble Shooting 및 원활한 운영을 위한 기술 지원 일반 ▪ 유지보수 계획 및 유지보수 인력명단, 유지보수 방법 등의 변경 시 고객사와 사전 협의하여 변경	▪ 유상 유지보수는 무상 유지보수 기간이 경과한 이후 별도의 유지보수 계약 후 시작 ▪ 무상유지보수 기간 중 사용자의 과실 또는 천재지변에 의한 손상은 유상 유지보수
인력 운영	▪ 전문 유지보수 인력 (정/부)	▪ 제조사 전문가는 비상주 지원
H/W	▪ 부품파손, 교체(순정품) 및 불량장비 보수 ▪ Config. 설정 변경 및 최적화	▪ 부품파손, 교체(순정품) 및 불량장비 보수 ▪ Config. 설정 변경 및 최적화
S/W	▪ S/W 업그레이드 및 패치, 신규 패턴 업그레이드 무상 제공 ▪ 시스템 기능 및 오류 테스트, 수정 ▪ 장애에 대한 Trouble Shooting ▪ 로그 분석 요청 시 지원	▪ 무상유지보수 범위 포함 ▪ 시스템 확장 및 기능개선 (협의)

관리 계획

III-3 교육지원

Zyroid 의 단계별 교육을 통해 앱 점검의 완전한 이해와 심도 깊은 점검이 가능하도록 지원하고 수시로 발생되는 이슈에 대한 교육을 병행 지원할 것입니다.

교육목적

- 모바일 APP 진단 환경 구축 방법 습득
- Zyroid 사용법 및 기본점검 방법 습득
- 단계별 APP 진단 방법 습득 및 활용

교육내용

- Zyroid 개요 및 모바일 APP 취약점
- 진단 환경 구축 및 취약점 점검
- 점검 결과 분석 및 보고서 작성

구 분		내용	대상	인원	방 법	회수	장소
Zyroid	점검 및 조치	▪ Zyroid 개요 ▪ 모바일 APP 취약점의 종류 및 특징 ▪ 진단 환경 구축 방법 ▪ 모바일 APP 취약점 점검 ▪ 취약점 점검 결과 분석 ▪ 점검 결과 보고서 작성	사용자	협의	이론 및 실습	구축기간 1회 (또는 요청 시)	고객사 지정 장소
	관리	▪ 최신 보안 트렌드 소개 ▪ 발견된 취약점에 대한 상세 가이드 확인 및 조치방법 ▪ 신규 취약점에 대한 대응 방법 (업데이트 방법)	사용자	협의	이론 및 실습	구축기간 1회 (또는 요청 시)	고객사 지정 장소

레퍼런스

coupang
VERTIGO GAMES
Tales Runner
ASIANA AIRLINES
농협
Gmarket
KB 국민은행
SK telecom
HYUNDAI
KB 국민카드
KISA 한국인터넷진흥원
AUCTION. KOREA
한국전자인증 국가공인인증기관
kt olleh
전자경비감시구역 NSOK
kct
ETRI 한국전자통신연구원
SK planet
HYUNDAI MnSOFT
kt ds

라온시큐리티

쇼핑 통신 금융 전자 자동차 정부

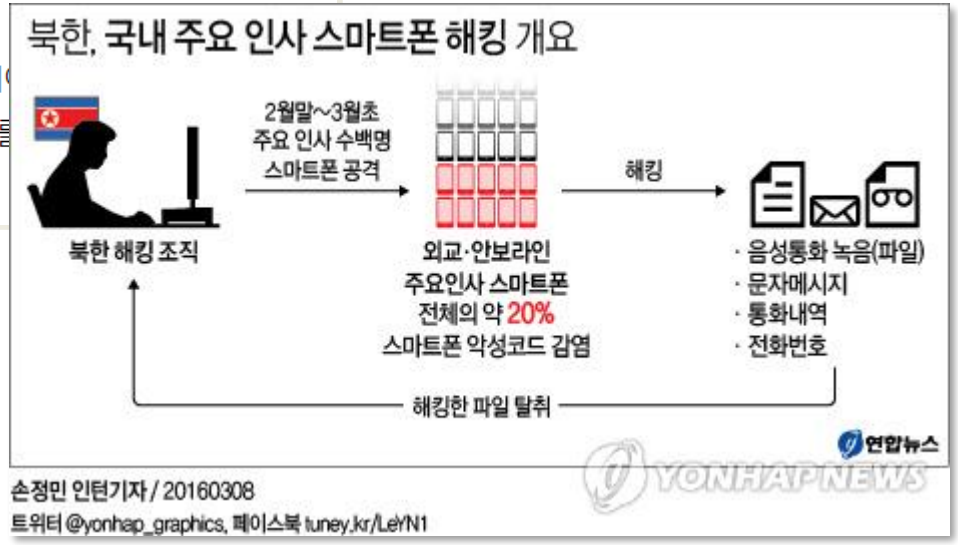
Daum 게임
11번가
SK telink
한국도서보급(주)
SAMSUNG 삼성전자
LG전자
Paytok
롯데홈쇼핑
나눔 Lotto
SAMSUNG 삼성SDS
검찰
NSRI 국가보안기술연구소
금융위원회
LOTTE.com 롯데닷컴
신협
KIA MOTORS
법무부
한국수력원자력
정부24

"北, 정부인사 수십명 스마트폰 해킹…문자·통화 탈취"

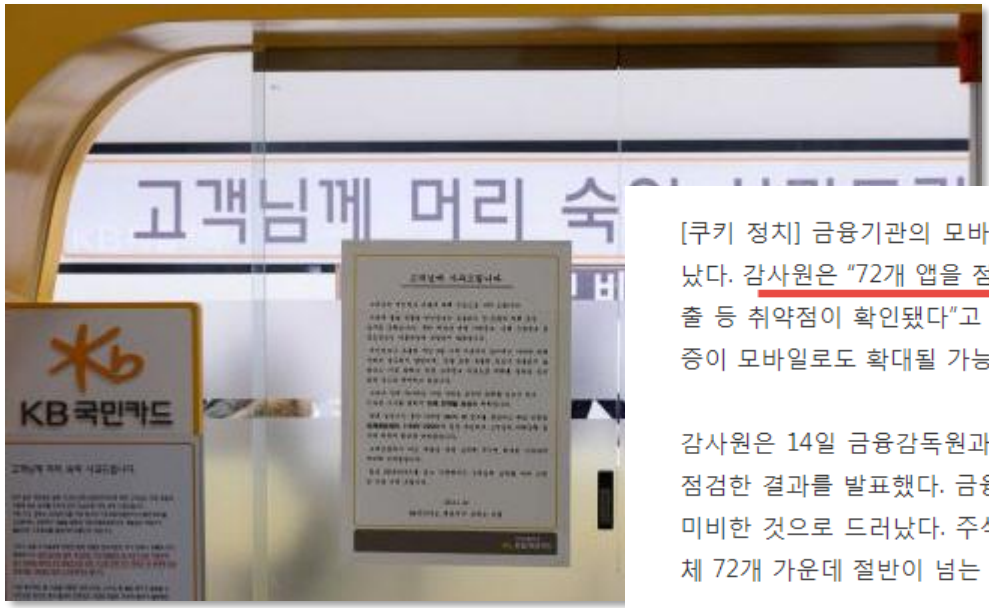
국정원 "악성코드 심는 방식 공격…20% 감염돼 전화번호도 유출"
"인터넷 뱅킹 등 보안 SW 업체 전산망 장악…전자인증서도 탈취"
철도운영기관 직원 대상으로 메일 계정·패스워드 탈취 시도
긴급 국가 사이버안전 대책회의 개최

(서울=연합뉴스) 이광빈 강병철 기자 = 북한이 최근 우리 정부의 주요 인사 수십명의 스마트폰을 해킹해 문자 메시지와 음성통화 내용을 탈취한 것으로 나타났다.

또 인터넷뱅킹이나 인터넷 카드결제 시 사용하는 보안소프트웨
전산망을 장악하고 금융권 보안솔루션 공급업체의 전자인증서를
위적으로 사이버 공격을 하고 있는 것으로 드러났다.



‘이러니 털리지’ 감사원 “금융권 모바일 앱 해킹에 취약…5곳 중 1개 꼴 금융보안 검사 전무”



[쿠키 정치] 금융기관의 모바일 애플리케이션이 해킹에 매우 취약한 것으로 감사원 감사결과 드러났다. 감사원은 “72개 앱을 점검한 결과, 38개에서 위조 및 변조 가능 또는 소스코드 내 주요정보 노출 등 취약점이 확인됐다”고 밝혔다. 사실상 전국민의 개인정보를 털리게 한 금융기관의 보안 불감증이 모바일로도 확대될 가능성이 높은 현실이다.

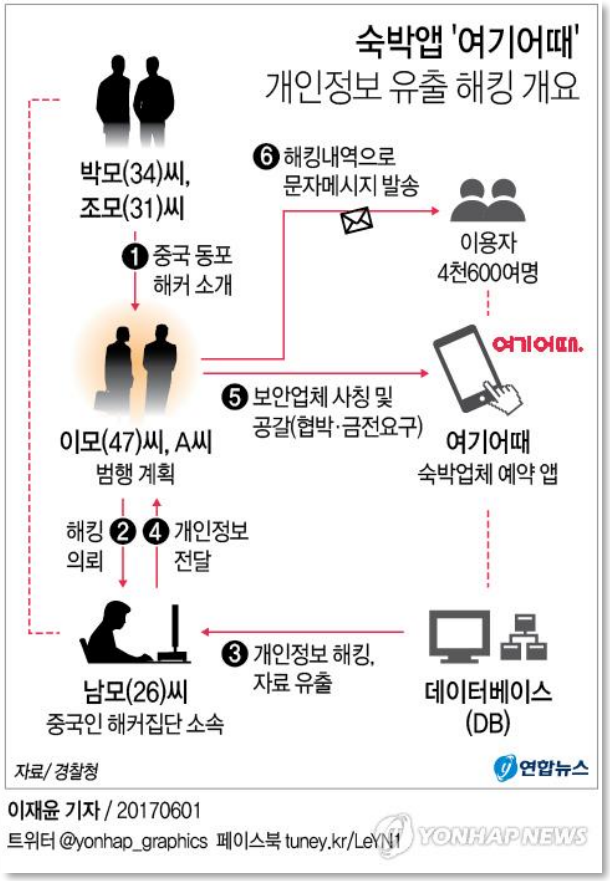
감사원은 14일 금융감독원과 금융위원회를 중심으로 금융권 사이버 안전관리 및 감독실태를 집중 점검한 결과를 발표했다. 금융위 소관인 금융기관 모바일 앱에 대한 보안성 검증 관련 규정 자체가 미비한 것으로 드러났다. 주식거래나 은행거래를 모바일로 할 때 이용하는 앱 말이다. 감사원은 전체 72개 가운데 절반이 넘는 38개가 해킹에 취약하다고 판정했다.

감사원은 또 금융감독원 소관인 금융기관 보안관련 사항을 점검했는데, 주요 검사 대상 144개 금융기관 가운데 26개는 5년간 검사한 실적이 전혀 없었다고 했다. 다섯 중 하나 꼴(18%)이다.

이외에 금융권의 사이버 안전 관련 30개 조항 가운데, 정보처리 시스템 보호대책이나 해킹 방지대책 등 15개 항목은 검사 항목에 이예 빠졌거나 있더라도 부실하게 반영돼 있다고 밝혔다. 대량 정보유출이 결국 정부기관의 감독 소홀로 이뤄진 것임을 유추할 수 있다.

정보통신망법 위반 스타벅스코리아 등 10개사 과태료 받아

백상일 기자 baeksi@kyeonggi.com 노출승인 2018년 07월 11일 16:59 발행일 2018년 07월 11일 수요일



[서울=경기일보/백상일 기자] 방송통신위원회는 11일 제35차 전체회의에서 스타벅스커피코리아 등 정보통신망법의 개인정보보호 규정을 위반한 10개사에 과태료 총 2억2천만 원을 부과하고 시정명령을 내렸다고 밝혔다.

방통위에 따르면 지난해 2월 숙박앱 '여기어때'를 해킹한 해커에 대한 경찰 추가 조사에서 개인정보 유출이 확인된 사업자 8개사와 개인정보 노출 사실을 신고한 사업자 2개사에 대한 개인정보 취급·운영 실태를 지난 2월 22일부터 3월 23일까지 조사했다.

그 결과 네이버네트워크, 라인프렌즈, 스타벅스커피코리아 등 10개사 모두 정보통신망법을 위반한 사실이 확인됐다.