Introduction Smart Phone Security

Spring 2014

Contents

1. 개 요

2. 안드로이드 보안

3. 결 론

1. 개 요

2014-03-03

정보보안 패러다임의 변화

과거 = 수동적 정보수집

- 통신상에서의 정보 유출
- 암호해독 기술

통 신 망

서비스 서버
정보저장 서버

사용자

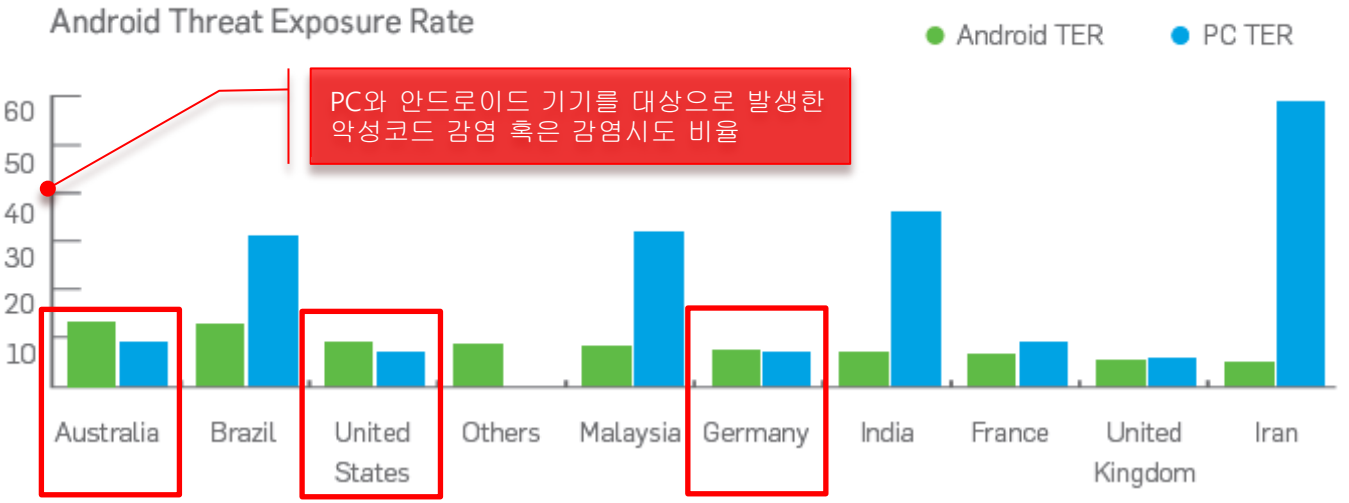
현재
=
해킹 통한 적극적 정보수집 및 파괴

- 서버 및 PC에서 정보 유출
- 다양한 해킹 기술
- DDoS 공격을 통한 서비스 방해
- 정교한 표적화된 공격

모바일 보안 위협 증가


Before Smartphone
이동식
도청장비
일반휴대폰
피처폰
특수장비
이용시 도청
가능
이동통신망
기지국
DDoS
일반휴대폰
피처폰
임의의 패킷 생성 불가
DDoS 불가
After Smartphone
악성코드에 의한
• 음성통화 도청
• 회의내용 유출
• 각종 개인정보 유출
이동통신망
DDoS
• 악 성 코 드 를 통 한
임의의 패킷 생성 가능
• DDoS 가능

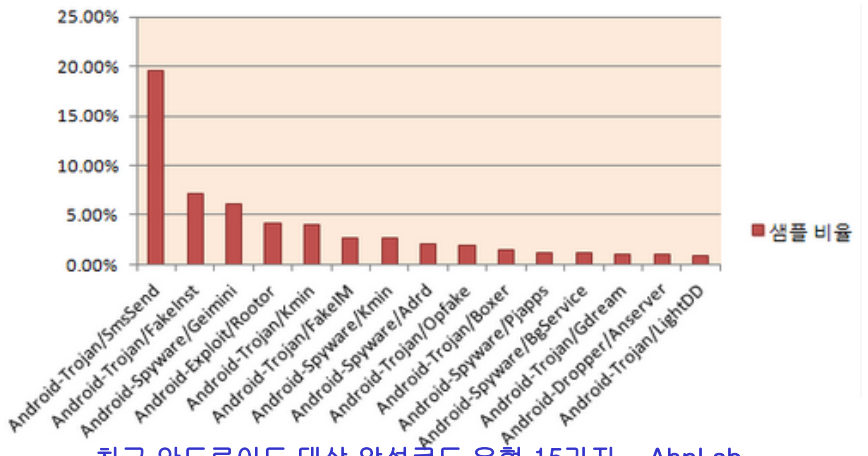
안드로이드 위협 가속화



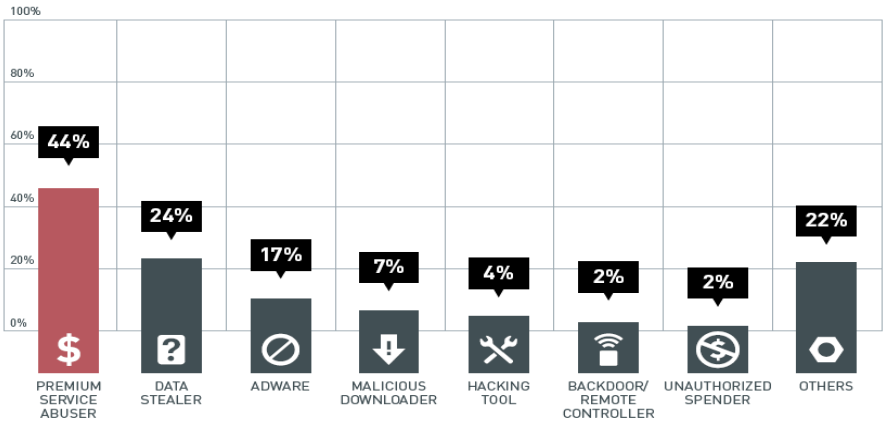
PC 환경에서의 보안 위협과 비교 될 정도로
안드로이드 환경에서의 보안 위협이 가속화

일부 국가의 경우 안드로이드 보안 위협이
PC 보안 위협을 앞지르는 현상이 나타남

악성코드 유형별 분류



최근 안드로이드 대상 악성코드 유형 15가지 – AhnLab



TrendLabs 2Q 2013 Security Roundup, Trendmicro, 2013. 6

명 칭	특 성
Trojan/SmsSend	사용자 모르게 문자를 전송
Trojan/FakeInst	임의의 어플리케이션 설치 프로그램으로 위장하여 문자 전송 등으로 수익 도모 혹은 악성행위
Spyware/Geimini	정상 어플리케이션을 리패키징 , 개인정보 탈취
Exploit/Rootor	실행 시 취약점을 이용하여 시스템 권한 획득
Trojan/Kmin	웹 페이퍼 변경 어플리케이션으로 위장하여 악성어플리케이션 설치
Trojan/FakeIM	Trojan/FakeInst 와 유사
Spyware/Kmin	Trojan/Kmin 와 유사
Spyware/Adrd	정상적인 유틸리티를 리패키징 하여 다양한 악의적인 기능 수행
Trojan/Opfake	Trojan/FakeInst 와 유사
Trojan/Boxer	임의의 어플리케이션 설치 프로그램으로 위장 실제로는 유료 문자를 발송
Spyware/Pjapps	Spyware/BgService 를 통해 설치
Spyware/BgService	정상 어플리케이션을 리패키징 하여 악성코드 삽입
Trojan/Gdream	게임, 만화 등을 리패키징 하여 악성코드를 추가 시킨 악성코드의 종류
Dropper/Anserver	정상 어플리케이션을 리패키징 하여 다른 악성코드 설치
Trojan/LightDD	성인 어플리케이션으로 위장, 개인정보 유출

2. 안드로이드 보안

2014-03-03

안드로이드 보안 위협


1 개인정보 유출
Info
공격자
3 스미싱 (Smishing)
2 Kernel 공격
Linux Kernel
4 음성통화
5 모바일 봇넷
Attack
타겟 서버

1 개인정보 유출

- 개인정보 유출 형태

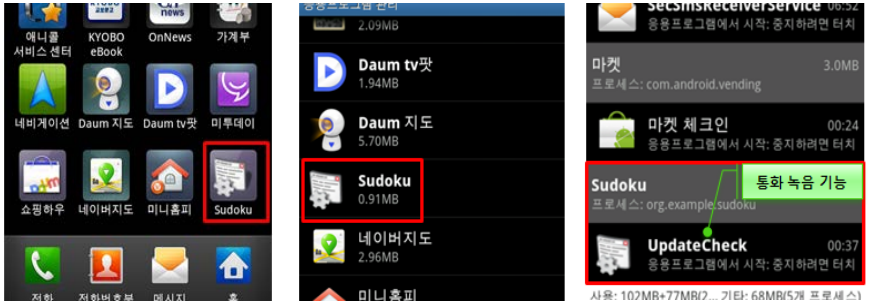
악성 어플리케이션에 의한 개인정보 유출

① 제작

② 감염

④ 데이터수집

③ 은닉 동작



메인 메뉴 | 응용 프로그램 관리 | 실행중인 서비스

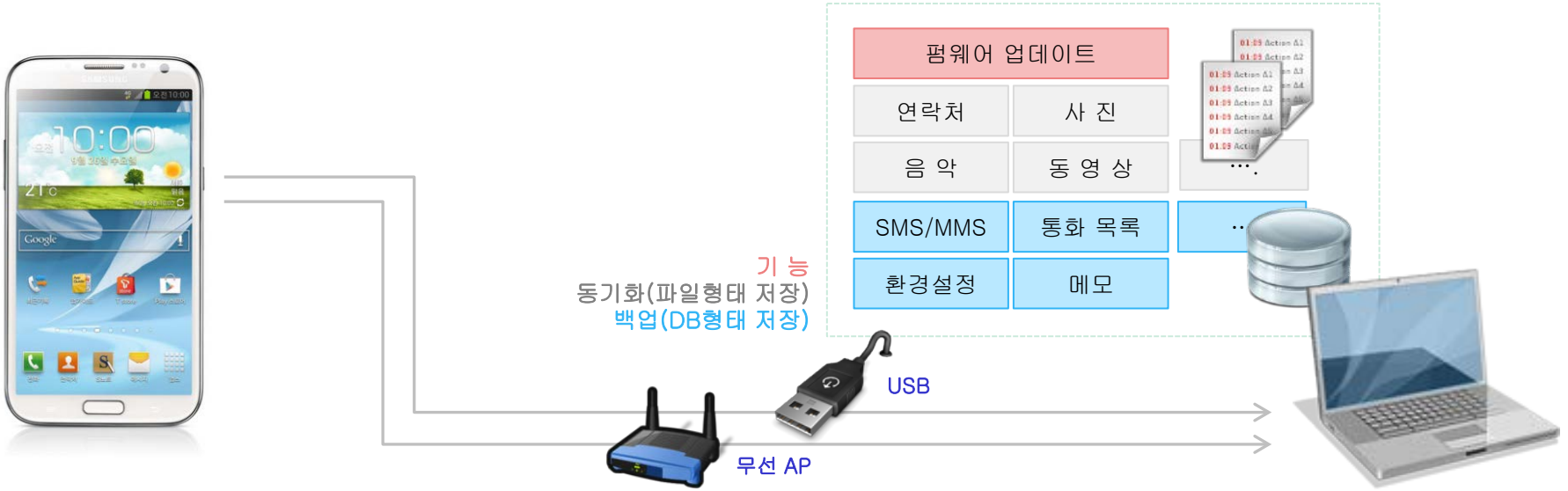
동기화 프로그램에서의 개인정보 유출

- 제조사별 동기화 프로그램

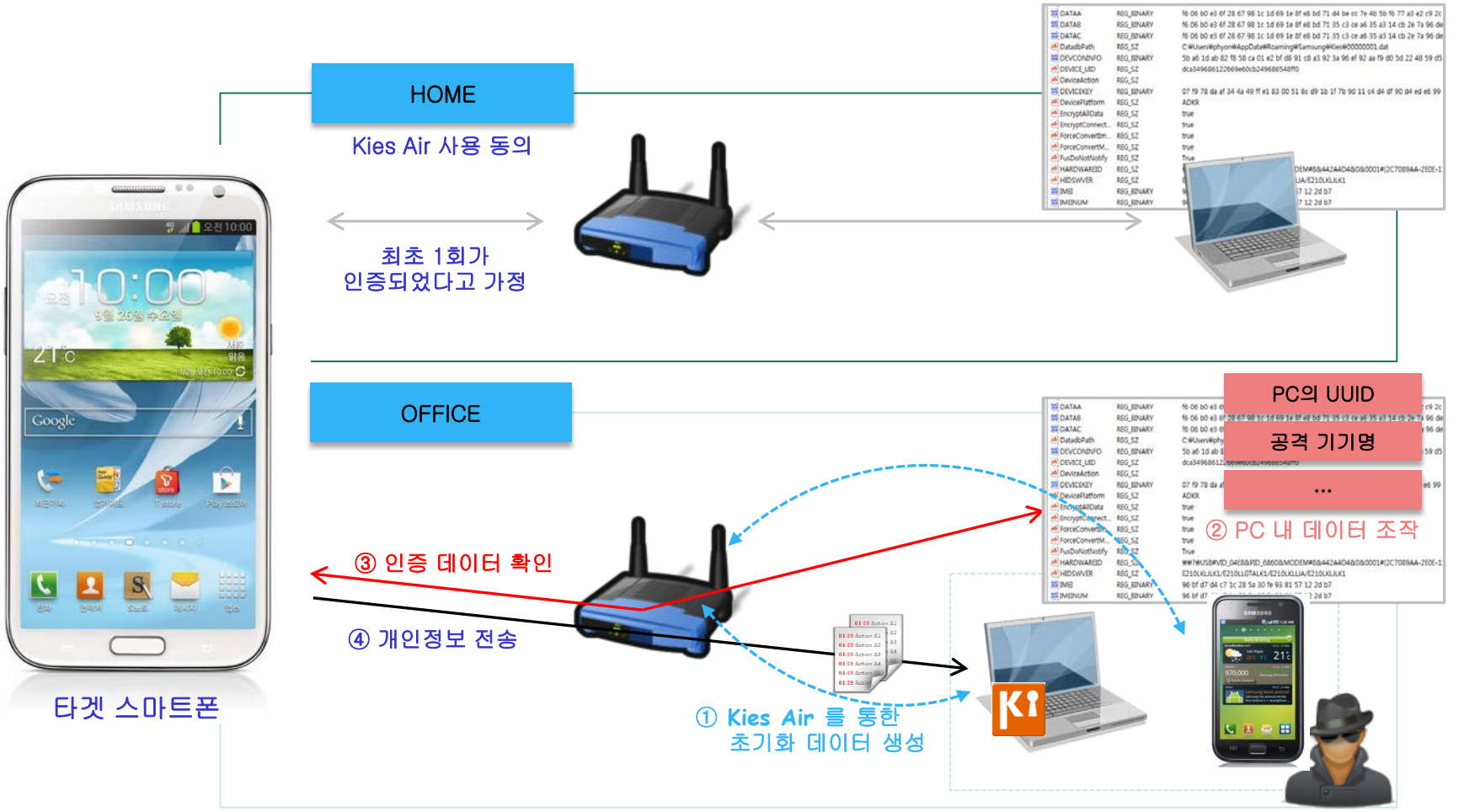
제조사	이름	연결방법
Samsung	Kies / Kies Air	무선 AP / USB
LG	LG PC Suite / LG Mobile Sync	USB
HTC	HTC Sync	USB
Sony	Sony Ericsson PC Companion	USB

※ 제공하는 기능

- ❖ **동기화 : 데이터 형태(JPG, MP4, …)로 PC 저장**
- ❖ **백업 : DB 형태로 PC 저장**



개인 정보 유출 시나리오


HOME
Kies Air 사용 동의
최초 1회가
인증되었다고 가정
OFFICE
PC의 UUID
공격 기기명
...
② PC 내 데이터 조작
③ 인증 데이터 확인
④ 개인정보 전송
① Kies Air 를 통한
초기화 데이터 생성
타겟 스마트폰

클라우드 서비스에서의 개인정보 유출

- 클라우드 서비스

❖ 각 통신사 마다 통신사의 클라우드 서비스 이용 어플리케이션 설치 후 판매
❖ 클라우드 서비스를 이용해 개인정보 및 데이터 동기화

항 목	SKT T Bag	KT uCloud	LGT U+ Box
SMS/MMS	O	X	X
연락처	O	X	X
사진	O	O	O
동영상	O	O	O
음악	O	O	O

통신사별 클라우드 서비스의 동기화 데이터

원격 제어

하우리 모바일 보안연구팀에 따르면 해커는 "□□□ 덕에 결혼했어요…많은 축복 바래요. 솔로분들 추천해요 ○○○.com" 라는 내용의 문자를 발송하여 스마트폰 사용자의 접속을 유도한다.

문자에 적혀있는 URL을 클릭하게 되면 실제 존재하는 결혼정보 회사의 웹사이트를 보여줌과 동시에 악성 애플리케이션을 다운받도록 한다.

또한 일반적인 스미싱 문자는 단축 URL 주소를 사용하지만 이 문자는 일반적인 Full 링크를 사용하고 악성 애플리케이션 배포서버에 정상 웹페이지의 IFRAME 태그를 삽입하여 악성 웹 페이지 로드시 정상 웹페이지도 같이 로드 되도록 구현됐다.

즉, 해당 URL을 클릭시 사용자의 스마트폰에는 정상 웹페이지가 구동되며 해커는 이를 이용해 자신이 제작한 악성 애플리케이션을 설치 한다.

(사진=하우리 홈페이지 화면 캡처)

해당 악성 애플리케이션에 감염 되면 원격 제어는 물론, 파일 유출, 도청 및 위치추적, 추가 악성 애플리케이션 다운로드, 문자 메시지 탈취 등 스마트폰의 주요 제어 권한이 해커에게 장악돼 치명적인 피해가 발생할 가능성이 높다.

* 출처 : CBS 노컷뉴스 2013/07/26

안드로이드 원격 제어 악성코드 동작과정

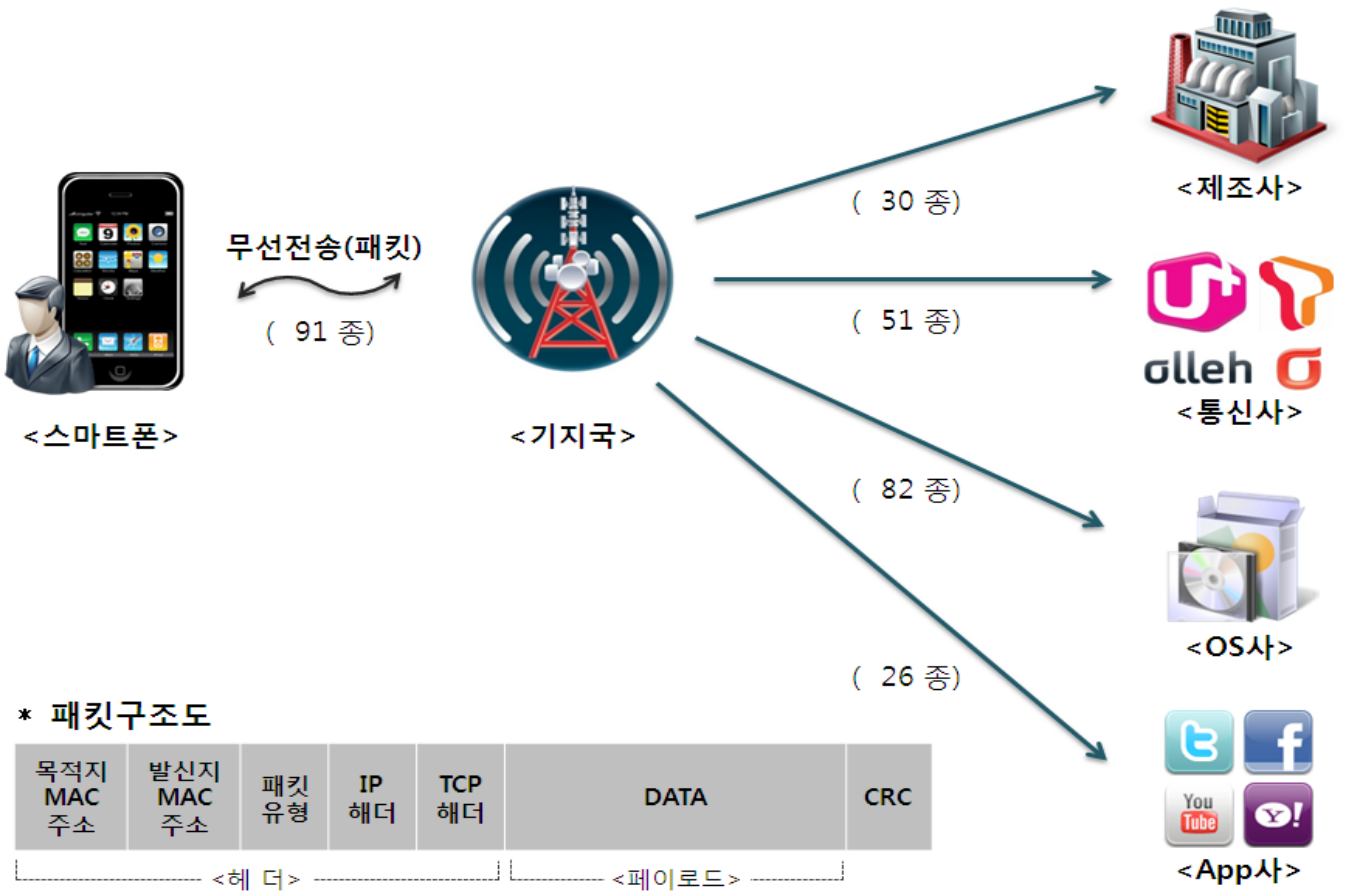
안드로이드 원격 제어 프로그램/어플리케이션

모비즌(mobizen)
루팅 불필요, 국산

팀뷰어(TeamViewer)
루팅 불필요


에어드로이드(AirDroid)
루팅 필요

사업자에 의한 개인정보 유출



스마트폰에서 전송되는 정보

제조사 (30종)	모델번호, 펌웨어 버전, 커널버전, 빌드번호, SMS 데이터 양(Size), 메시징 시작시간, 메시징 종료시간, 통화시간(Calling lap time, Start, End), App 다운로드 시간, 다운로드 App 이름, 다운로드 제조사, SMS/MMS 구분 식별자, 네트워크(통신사), SMS/MMS 전송시간(Sending, Receiving time), Wi-Fi Stat On/Off, Wi-Fi MAC Address, Phone NO, Bluetooth address, GPS On/Off, GPS Support On/Off, USIMInfo
통신사 (51종)	Keyword 데이터, 모델번호, 펌웨어 버전, 커널버전, 빌드번호, SMS 데이터 양(Size), 메시징 시작시간, 메시징 종료시간, 통화시간(Calling lap time, Start, End), IMSI, IMEI, App 다운로드 시간, 다운로드 App 이름, 다운로드 제조사, SMS/MMS 구분 식별자, Wi-Fi Stat On/Off, SMS/MMS 전송시간(Sending, Receiving time), Wi-Fi MAC Address, Phone NO, Bluetooth address, GPS On/Off, GPS Support On/Off, USIMInfo, 네트워크(통신사), SMS 특정 문자열, MMS 특정 문자열, 전화걸기, 문자메시지 전송, 주소록 검색, 웹브라우저 열기/웹 검색, 기타응용 Apps 열기, 기타응용 Apps 검색, 기타응용 Apps 열기 기타작업, SNS, 기저대역, 메일계정, 패스워드, GPS MAC Address, 웹 브라우저 사용내역(닫기, URL, History)

스마트폰에서 전송되는 정보

OS사 (82종)	Keyword 데이터, 모델번호, 펌웨어 버전, 커널버전, 빌드번호, SMS 데이터 양(Size), 메시징 시작시간, 메시징 종료시간, 통화시간(Calling lap time, Start, End), App 다운로드 시간, 다운로드 App 이름, 다운로드 제조사, SMS/MMS 구분 식별자, SMS/MMS 전송시간(Sending, Receiving time), App 버전정보, 사용정보(In Use/No Use) ID, 패스워드, 통신방법(Wi-Fi/LET), 네트워크(통신사), Wi-Fi MAC Address, Wi-Fi Stat On/Off, Phone NO, Bluetooth address, GPS On/Off, GPS Support On/Off, USIMInfo, Security Policy, Data Sharing, Network forwarding all, Admin/UserMode, Phone ID, Installed Apps info, Downloaded, Upgraded app info, Location direction, Location search 이전검색 cache, Location search 사용 cache, Languages Time, Date-local, Phone-Address, NFC(Near Filed Comms), On Service list] 전화걸기, 문자메시지 전송횟수, 주소록 검색, 웹브라우저 열기/웹 검색, 기타 응용Apps열기/검색, 기타 응용Apps 기타작업, SNS, SMS특정 문자열, MMS 특정 문자열, IMSI, IMEI, 기저대역, 메일계정, 패스워드, GPS위치정보, GPS MAC Address, 웹 브라우저 사용내역(닫기, URL, History), 주소록(전화번호부), CPU모델, 캐쉬 된 Apps정보(기본설정, On/Off여부, 버전정보), URL
App사 (26종)	ID, 패스워드, 통신방법(Wi-Fi/LTE), 네트워크(통신사), 주소록(전화번호부), URL, 메일계정, 안티바이러스 설정 비밀번호, 기기 모델버전, 모델명, 제조사, 운영체제 형태, 운영체제 버전, 운영체제 빌드번호, 펌웨어 버전, IMEI, SMS지정 문자열, MMS지정 문자열, 쿠키, 사진, 동영상, Bluetooth/Wi-Fi MAC Address(실시간 검색 On), App Name(On인 경우), App Version(On인 경우)

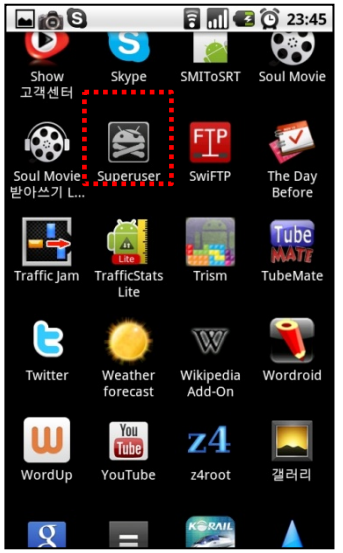
2 커널(Kernel) 공격

- 안드로이드 루팅

❖ 운영체제를 해킹하여 관리자(시스템)의 권한을 얻는 행위
❖ 즉, 시스템 권한으로 보안 메커니즘 우회 가능

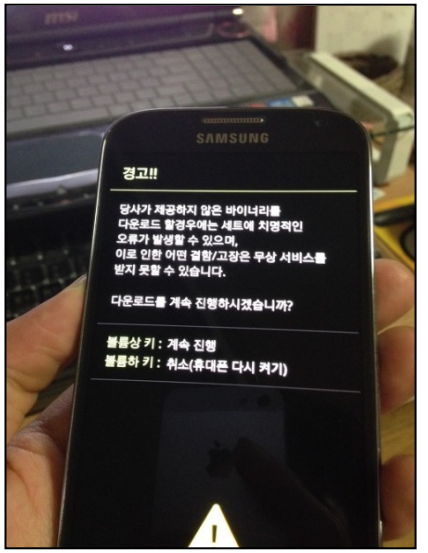
시스템 취약점 이용

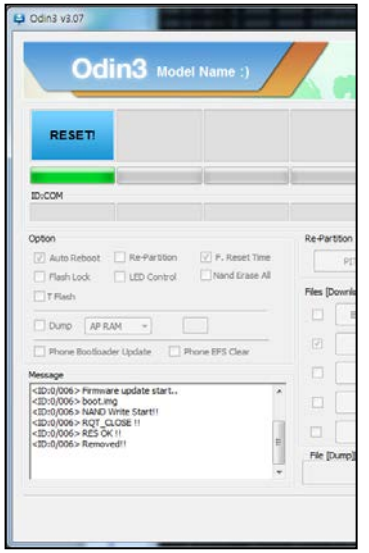
시스템 취약점을 이용한 루트 권한 획득 앱



펌웨어 변경 프로그램 이용

Odin, fastboot 등의 펌웨어 변경 프로그램



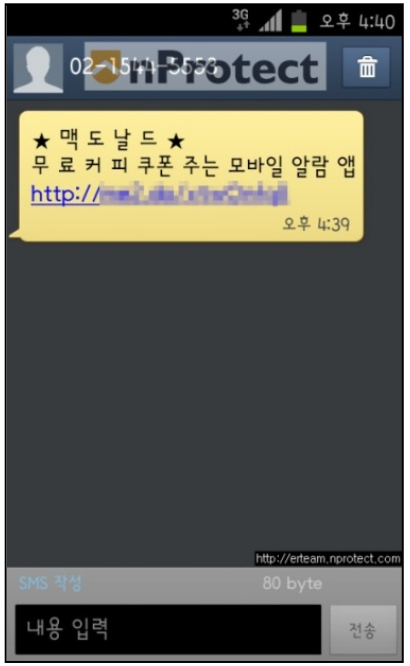


3 스미싱 Smishing

- 스미싱이란?

❖ **SMS + Phishing : SMS를 통해 악성앱 설치를 유도하는 스마트폰 해킹 기법**

❖ **개인정보, 금융정보 유출 및 스마트폰 소액결제 수행**



악성앱 설치 유도

악성앱 설치

악성 앱 확인

정상 앱으로 위장 및 실행

스미싱 차단 솔루션

❖ SMS 내용 또는 발신번호를 바탕으로 필터링 하거나 사용자에게 알림

S-GUARD @ SeWorks

- SMS 내의 URL을 블랙리스트와 비교

T-guard @ SKT

- SMS 내의 URL을 블랙리스트와 비교
- 설치된 악성앱 탐지(백신)

M& MessageTong @ Infobank

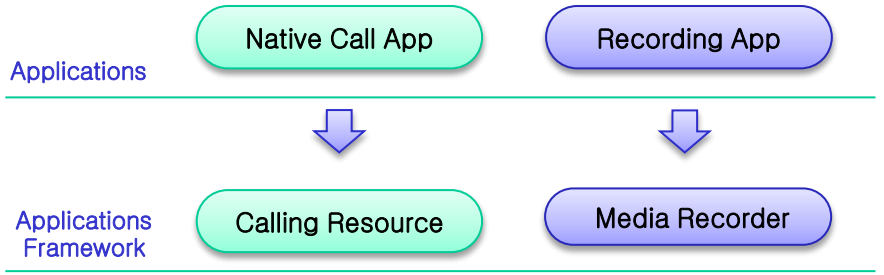
- SMS 유형별로 자체 DB에 저장 (금융관련 메시지 분류화)

4 음성통화 감청

- 스마트폰 통화는 안전한가?

일반 통화 녹음

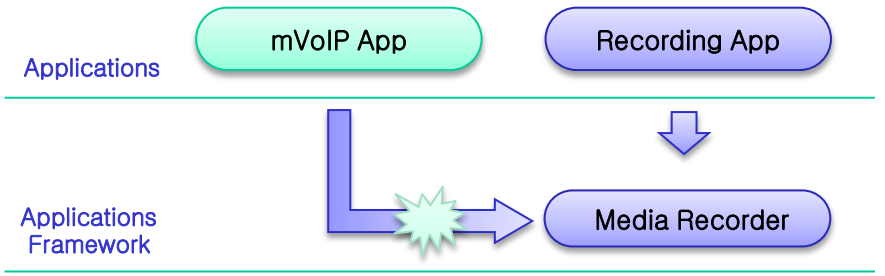
일반 통화에 대한 녹음 기능 수행 가능



- MediaRecorder 리소스를 사용하지 않는 일반 통화에 대한 녹음 수행 가능

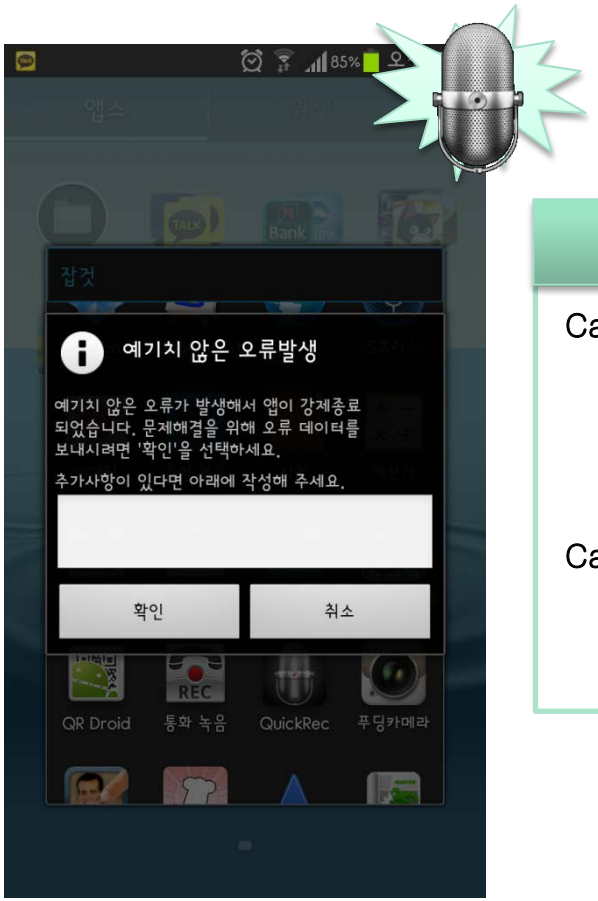
mVoIP 통화 녹음

리소스 선점으로 인한 정상적인 녹음 불가



- 음성 처리를 수행하는 MediaRecorder 리소스 선점 문제 발생
- 특정 앱에 의해 선점된 리소스는 타 앱에 의한 접근 불가

음성통화 감청



mVoIP 앱과 녹음 앱 간의 리소스 선점에 따른 문제점

Case 1. mVoIP 앱이 먼저 실행된 경우

-> mVoIP 서비스 정상 작동

-> 녹음 기능을 수행하는 앱 작동시 오류 발생

Case 2. 녹음 앱이 먼저 실행된 경우

-> 녹음 앱 자체는 정상 작동

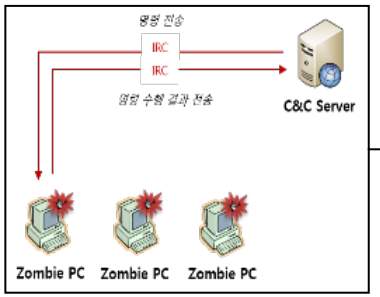
-> mVoIP 통화 불가, 또는 mVoIP 앱 오류 발생

5 모바일 봇넷

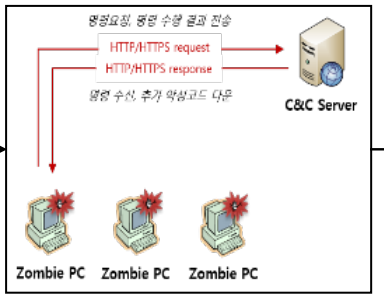
- 봇넷의 진화

PC 봇넷

IRC Bot

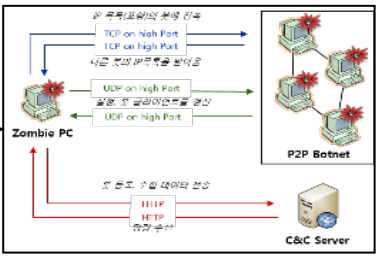


HTTP Bot

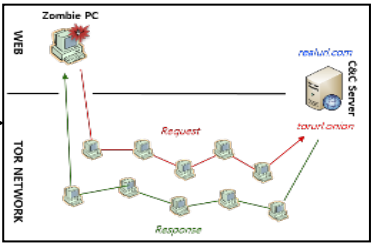


C&C 의존성 제거

P2P Bot



Tor Bot



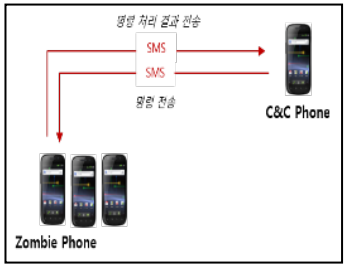
Tor Proxy 를 이용하여
C&C 서버 은닉

초기 악성코드 네트워크 모델

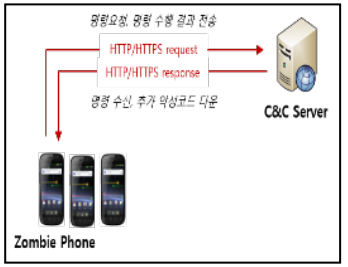
발전된 악성코드 네트워크 모델

모바일 봇넷

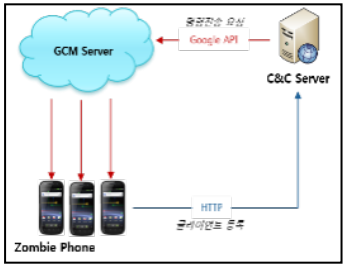
SMS Bot



IRC/HTTP Bot



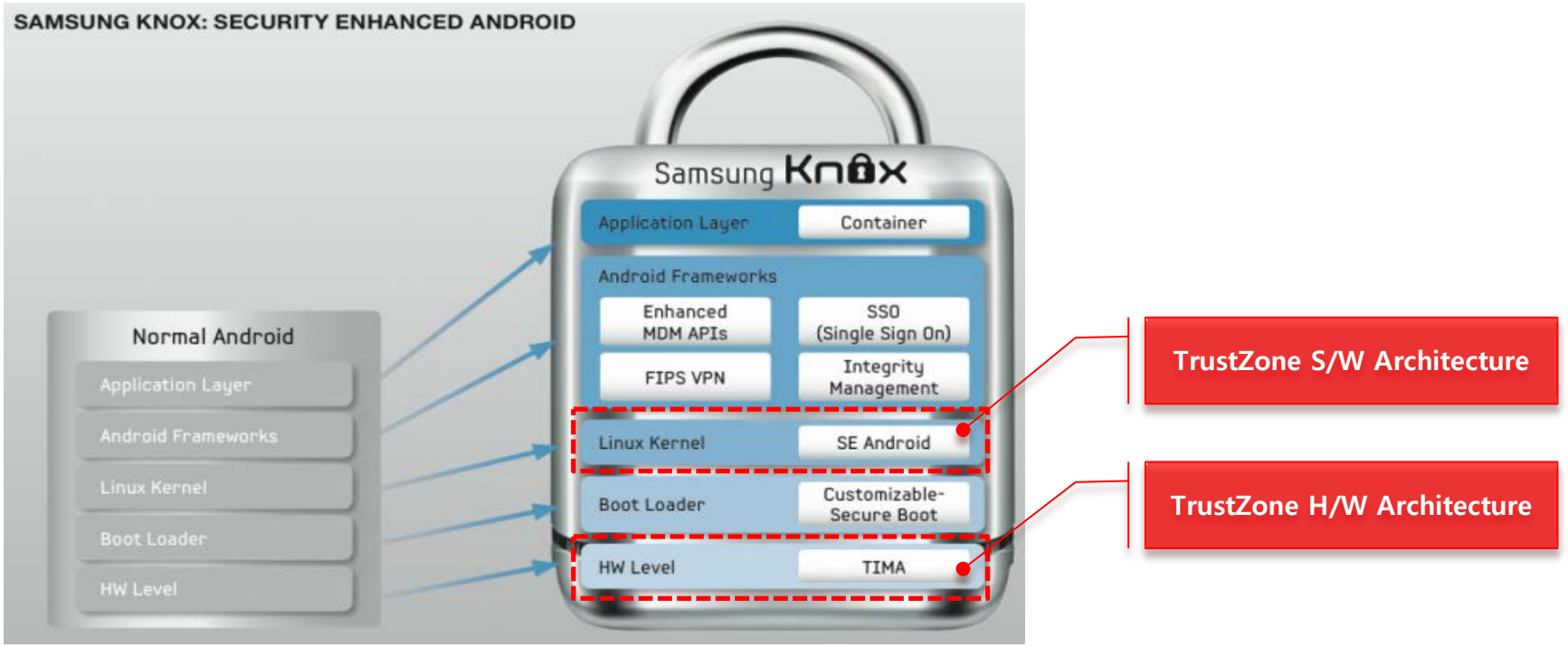
PUSH Bot



An Example

- 적용 사례 : 삼성 KNOX

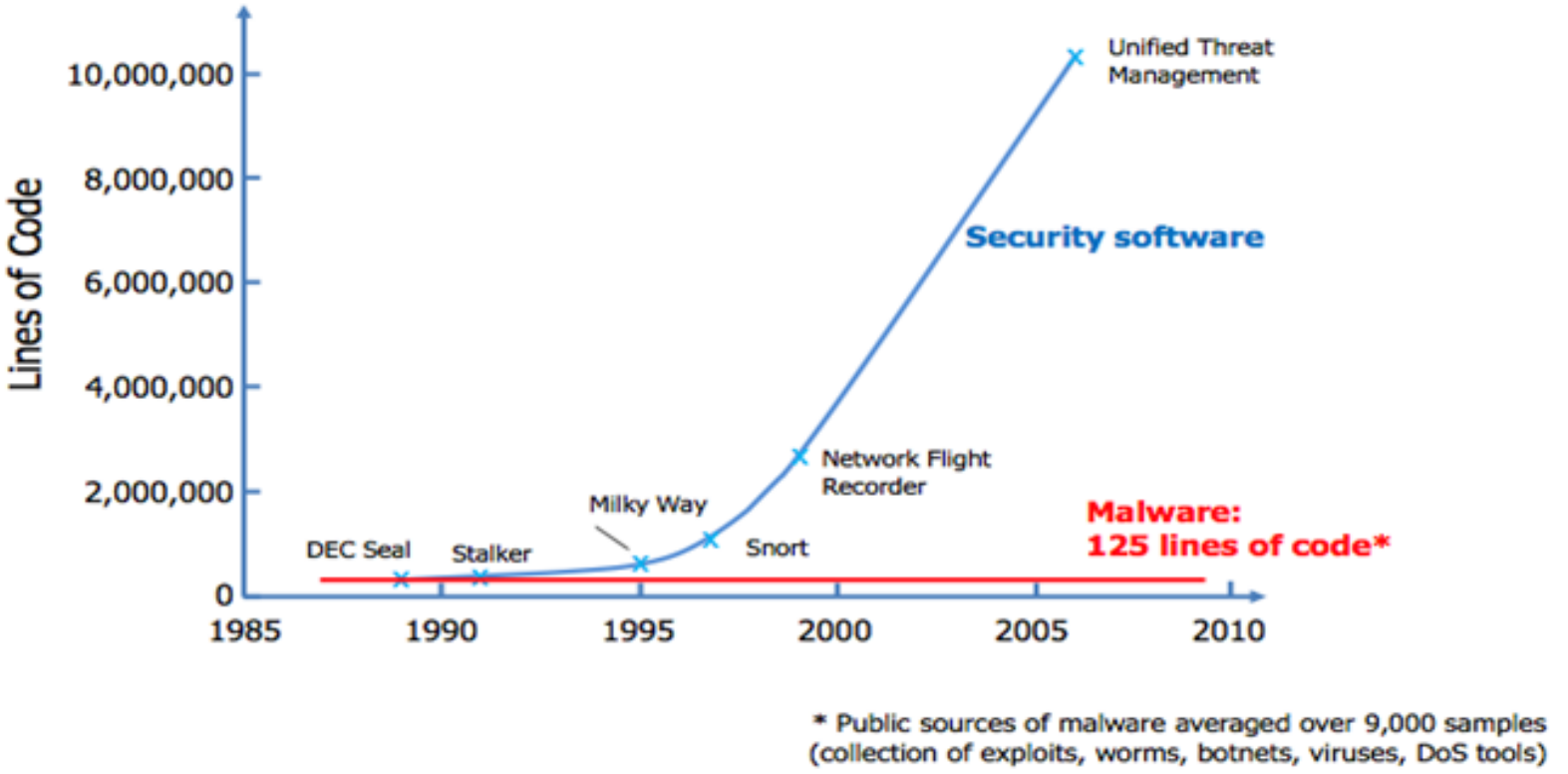
  - ❖ TrustZone 기술을 이용한 삼성의 보안 플랫폼 (미국 국방부 보안인증 획득-안드로이드 최초)
  - ❖ 단말기 내에 개인용/업무용 공간이 독립적 존재, 서로 다른 공간의 데이터



3. 결 론

2014-03-03

Security Software



* Public sources of malware averaged over 9,000 samples
(collection of exploits, worms, botnets, viruses, DoS tools)

Challenges in the Future

Reference

- 류재철, 스마트폰보안, OSIA TA Workshop, 2013.12