Emergence on Mobile Malware Threats

Presented by Roland Cheung
HKCERT

Agenda

- Introduction
- Mobile Malware Evolution
- Malware Highlight
- Future Trends
- Protection

Introduction

Introduction

Mobile Device:

- A small, hand-held computing device
- A display screen with touch input and/or a miniature keyboard
- With network connectivity (3G/WIFI/Bluetooth)
- Running Mobile OS

Including:

- Mobile Phone (Smart Phone)
- Mobile Internet Device (MID)
- Tablet

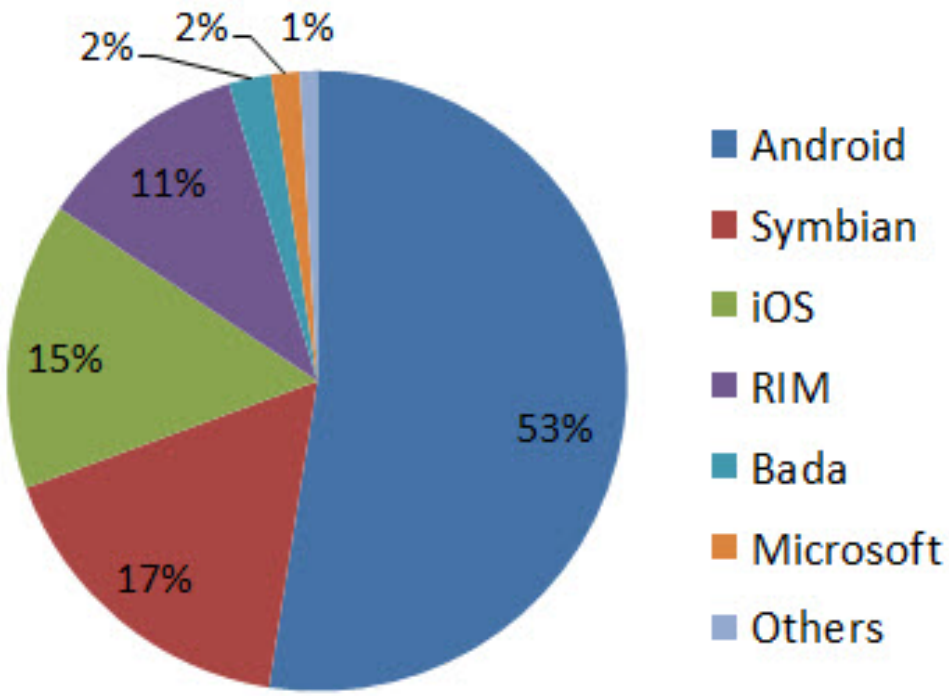
Introduction

Mobile Operating System (OS):

- Apple: iOS
- Google: Android (Opensource)
- HP : WebOS
- Microsoft: Windows Mobile and Windows Phone
- Nokia: Symbian, MeeGo (Opensource)
- RIM: BlackBerry OS
- Samsung: BaDa
- Embedded Linux distributions: Ubuntu Mobile. (Opensource)

Introduction

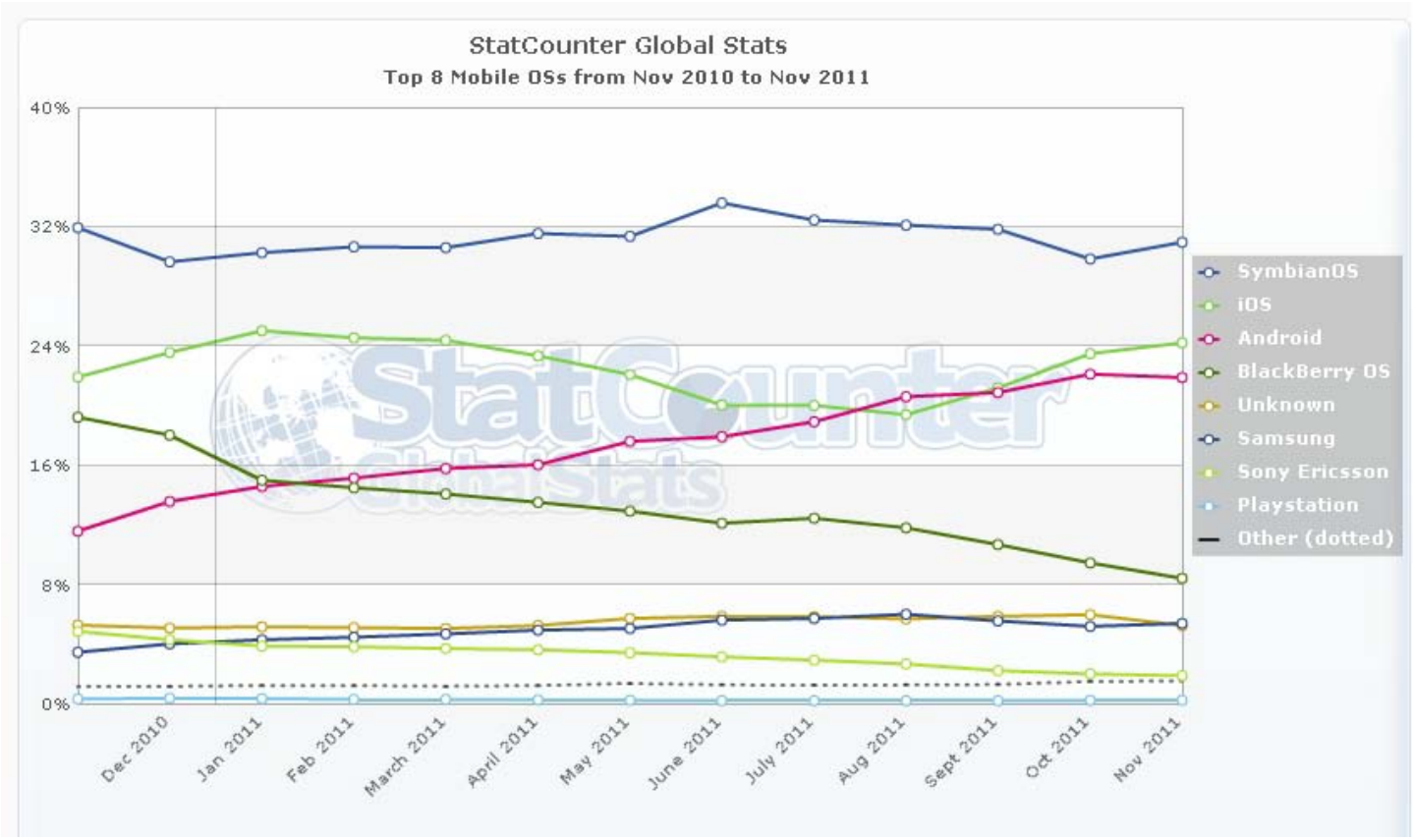
Mobile OS market share



Source: Gartner (Nov-2011)

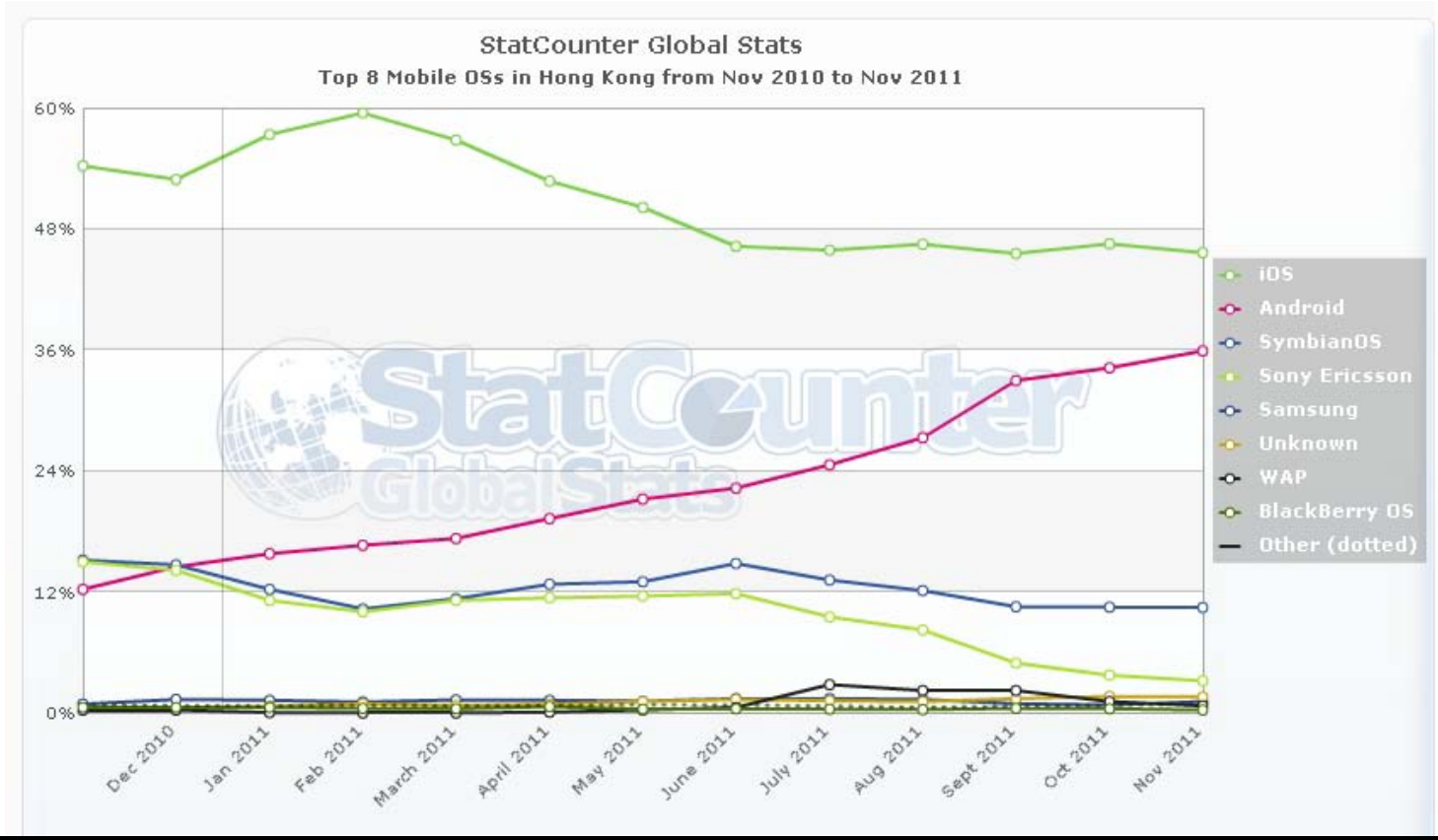
Introduction

Mobile OS Market share trends (Global)



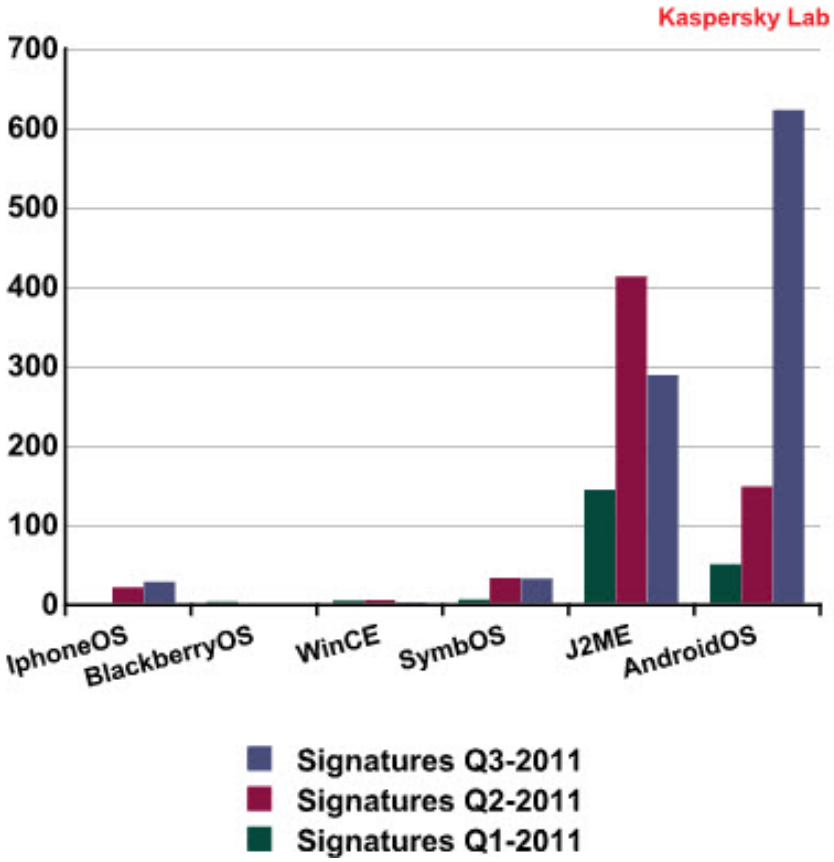
Introduction

Mobile OS Market share trends (Hong Kong)



Introduction

Mobile Malware statistics



Source: Kaspersky Lab

Introduction

Mobile Malware Incentive

- Provide the major functionality as PC
- Personal use and not share, stored a lot of personal data
- Mobile Financial service is available
- Stable Network connection
- Install apps is more easy than in PC
- Jailbreak, Rooted the device is common
- Install security protection is not common (less 4%, source: Canalys Oct-2011)

Introduction

Mobile Malware Infection Channel/Attack Vector

- OS vulnerability exploit

  Apple iOS: 36, Android: 58 (Source: NIST Vuln. Database)
- Application vulnerability exploit
  - Adobe PDF, Web Browser, Flash Player, QuickTime etc.
- Unknown source Apps
  - Forum, 3rd party market, QR code
- Default security setting after Jailbreak/Rooted
  - SSH without password
- Remote install
  - Compromise Gmail account

Introduction

Mobile Malware Payload

- Send SMS to premium rate number.
- Make international fee-based calls.
- Stolen personal data, e.g. contact list information
- Stolen financial data, e.g. bank account credential
- Become a “Bot” and can be controlled remotely
- Disable the phone / application

Mobile Malware Evolution

Mobile Malware Evolution

Law of computer virus evolution

1. Platform must popular
2. Well-documented development tools
3. Presence of vulnerabilities or coding errors, e.g. handles files and services

Mobile Malware Evolution

Source: www.mikewithart.com

Mobile Malware Evolution

Jun 2004

- SymbOS/Cabir - The first mobile malware
- Spread via Bluetooth
- No payload (Proof of concept code by Hacker Group “29A”)
- Reported in 10th World Championships in Athletics

Mar 2005

- SymbOS/Comwar - The first mobile malware spread via MMS
- No payload

Mobile Malware Evolution

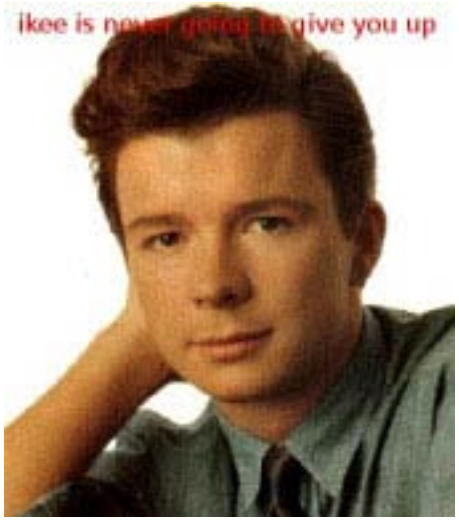
Feb-2006

- RedBrowser – Cross platform mobile malware written in Java Micro Edition (J2ME)
- Advertised itself as software that makes it easier for users to browse Web sites
- PoC code targeted to mobile phone users in Russia
- First mobile malware attempt to stole money by sending SMS

Mobile Malware Evolution

Nov-2009

- lKee.A - The first mobile malware targeting to iPhone
- Only affected the Jailbreak iPhone and without change the default SSH password
- Self propagate to infect other iPhone
- Variant “lKee.B” found in 2 weeks later



Mobile Malware Evolution

Aug-2010

- Trojan-SMS.AndroidOS.FakePlayer - The first mobile malware targeting to Android
- Spread via the web search.
- Download "pornoplayer.apk" if the user arrived Eastern Europe address.
- Sent SMS to Russian premium rate numbers.

Mobile Malware Evolution

2011

- Android is the most flavor platform for malware authors

  http://paulsparrows.wordpress.com/2011/08/11/one-year-of-android-malware-full-list

- A lot of 3rd party market (China, Russia) and the main source of malware

Malware Highlight

Malware Highlight

Case Study:

1. Zitmo, Spitmo

- Affected: Symbian, Windows Mobile, Android

2. DroidDream

- Affected: Android

Man in the Mobile (MITMO)

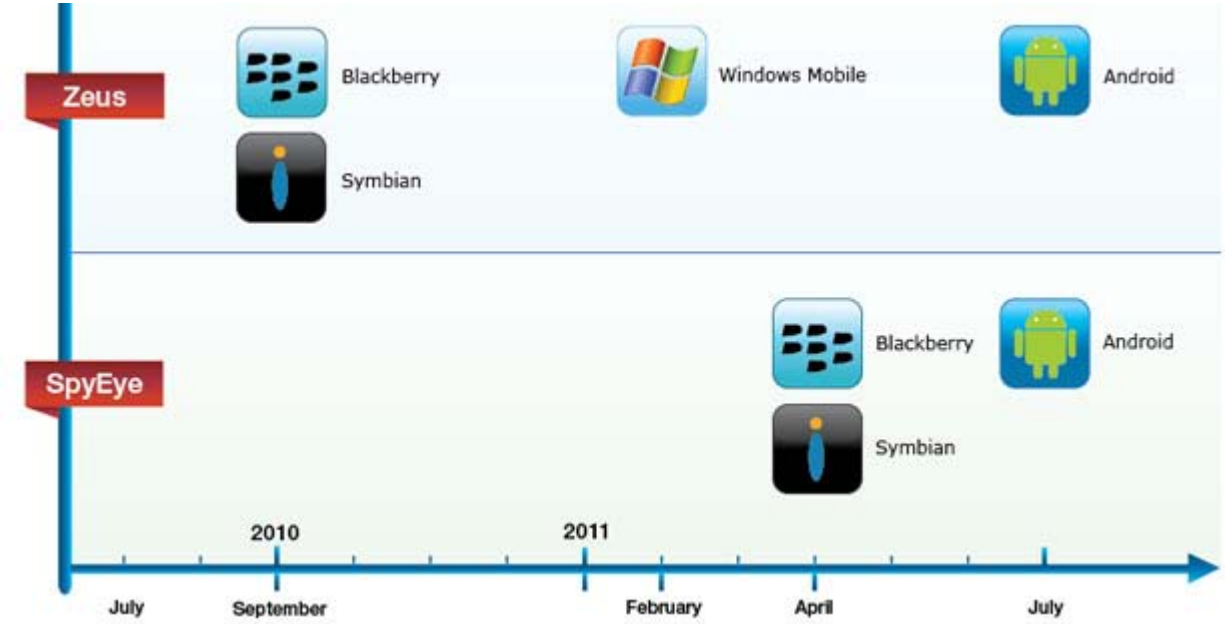
Mobile version banking trojan

- Zitmo – Zeus

Found in Sep-2010

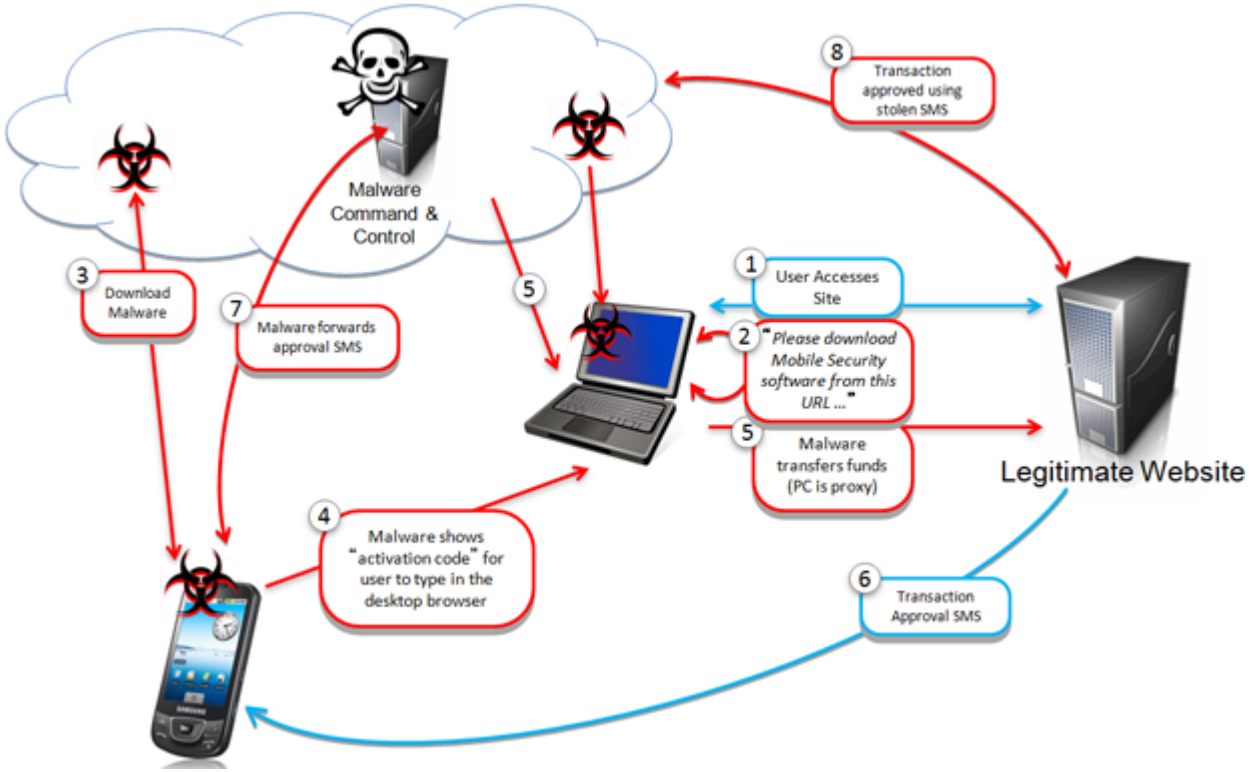
- Spitmo – SpyEye

Found in Apr-2011



Man in the Mobile (Mitmo)

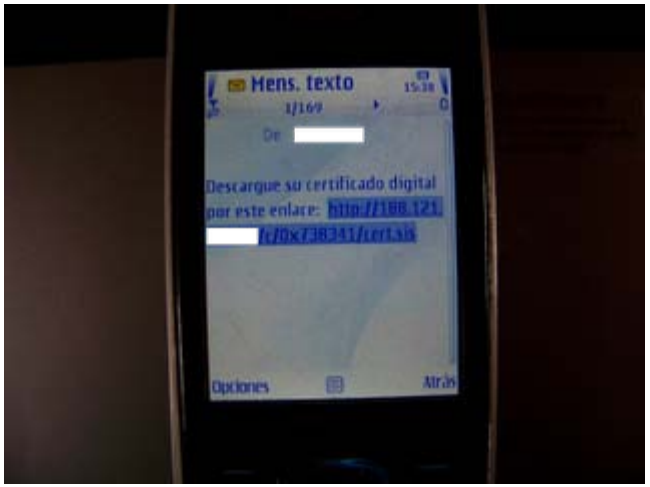
Operation Workflow:

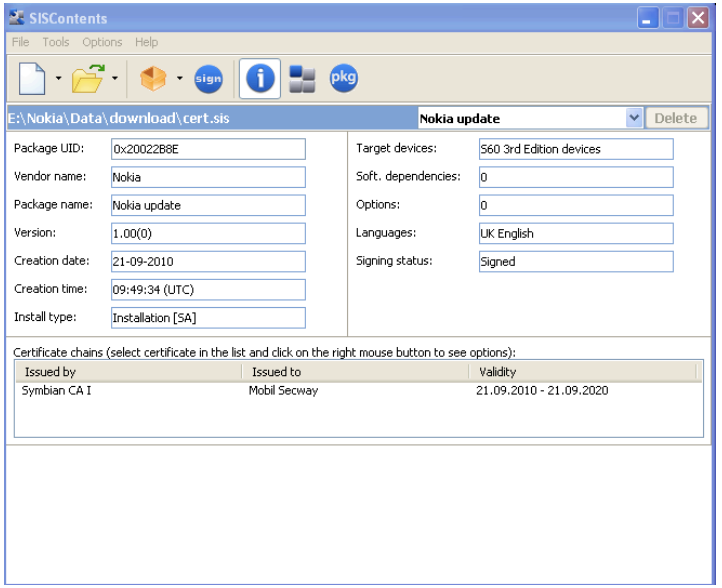


Source: Trusteer

Man in the Mobile (Mitmo)

Operation Screen shots:



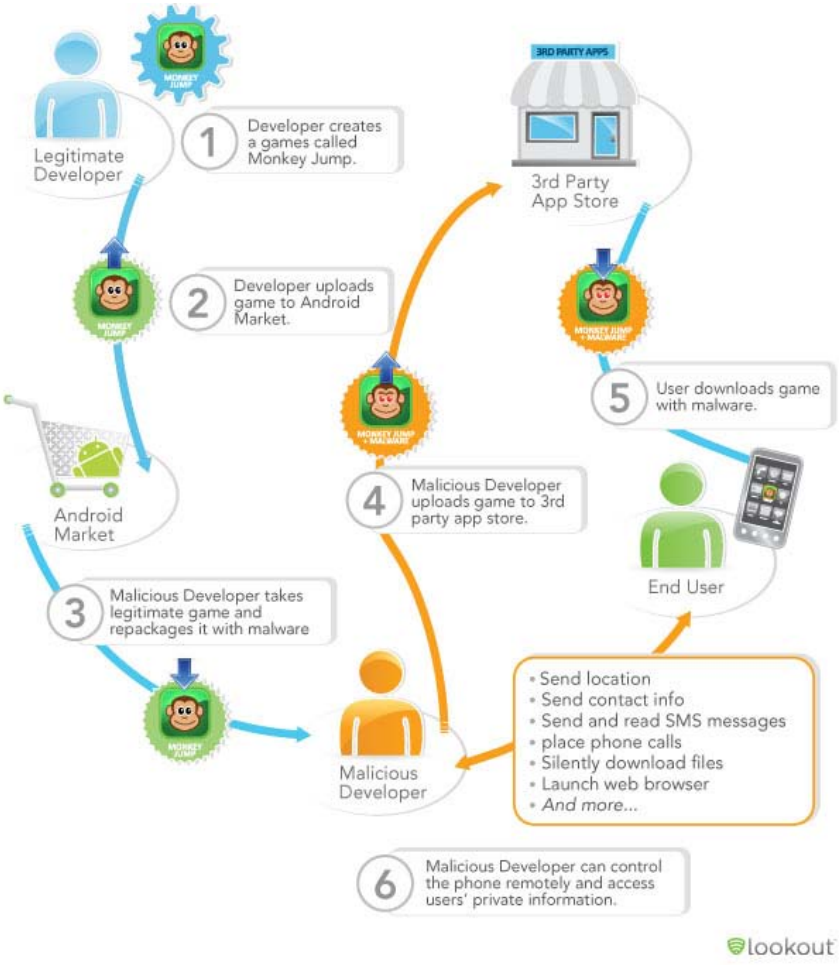


Source: S21sec

Droid Dream – Android

- Found in Mar-2011
- Inject root exploit code to free apps taken from Official Android Market and performed repackage
- At least 50 popular free apps with malicious code
- At least 50,000 downloaded
- Variant (aka: DroidDream Light) found in May and July of 2011

Droid Dream – Android



Source: Lookout

Droid Dream – Android

- Bot connects to Command & Control Center (C&C)
- Stole data (Device Information: IMEI, IMSI, Contact list, SMS data etc)
- Send SMS to premium rate number
- Download additional program (Downloader)
- Variant “Droiddream Light” found in May and July

Future Trends

Future Trends

- Evade the Official App store security mechanism
- App Update attack
- QR Code

Evade the Official App store security mechanism

App Store/Market

- Apple – App store
- Android – Android Market
- Microsoft – Windows Phone Marketplace
- Nokia – Nokia OVI
- Blackberry – App World
- Others: Amazon, Samsung , Nook etc.

Evade the Official App store security mechanism

Apple App Store

- Nov-2011, Charlie Miller discovered a iOS flaw which allow a malicious app on the App Store to download and execute arbitrary unsigned code.

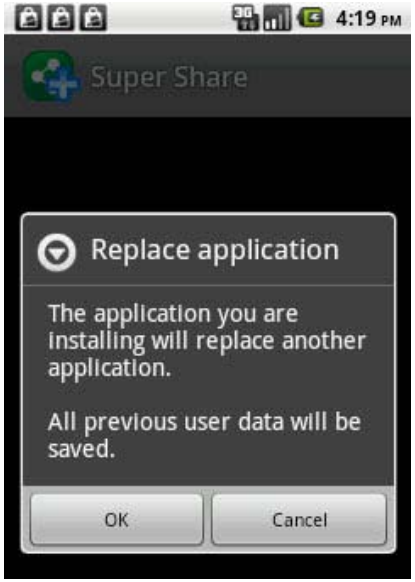
Android Market

- Allow to use self signed certificate to sign apps and insufficient control of apps content.
- Mar-2011, Google used “kill switch” to remove malware from Android market

App update attack

Update Attack

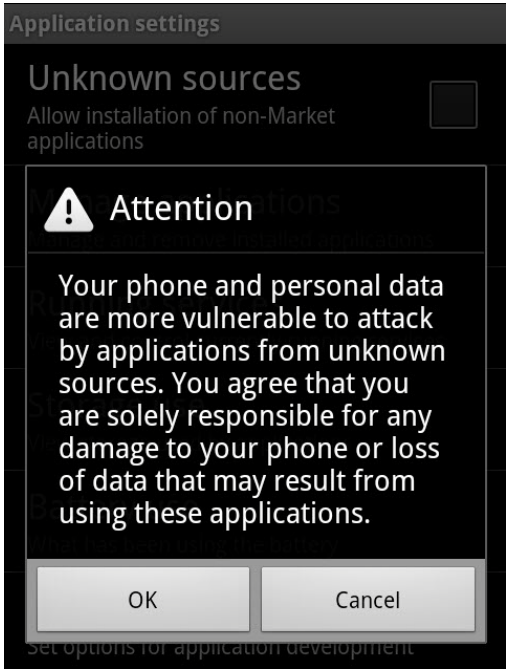
- First releases a legitimate application containing no malware.
- Once they have a large enough user base, the malware writer updates the application with a malicious version.
- Used in Android Market



QR Code

QR Code

- With a camera and QR reader application to scan these codes.
- The codes can direct users to websites or online videos, and send text messages and emails.
- Download and install a program directly if allow installation of non-Market applications e.g. JimmICQ client



Protection

Protection

Required:

- Maintain the Mobile OS and software up to date
- Do not download/install application from unknown source and check the feedback from other users
- Verify the application permission granted if applicable (Android)
- Verify the download URL when using QR code
- Install mobile security application
- Use stronger password
- Turn off Bluetooth and WIFI when not use

Protection

Verify the application permission granted (Android)

- Manifest.xml – list out the permission required by the apps

http://developer.android.com/reference/android/Manifest.permission.html

Coin Pirates

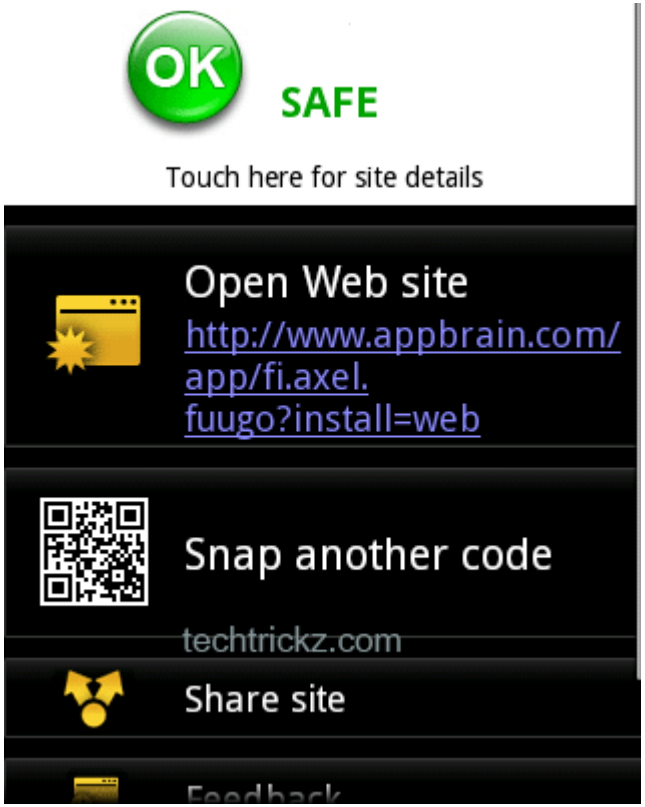
Trojanized Coin Pirates

Original Coin Pirates

Source: TrendMicro

Protection

Verify the download URL when using QR code



Protection

Mobile Security Application Features:

- Real-time scan / Manual scan
- Automatic updates
- Scan mail, SMS and downloads
- Unauthorized access protection
- Task Manager

Reference: AV Tools test report

http://www.av-test.org/fileadmin/pdf/avtest_2011-11_free_android_virus_scanner_english.pdf

Q & A

Thank You

Email: hkcert@hkcert.org