TREND MICRO™ | Securing Your Journey to the Cloud

APK File Infection on Android System

Bob Pan
Mobile Security Research Engineer

July 27, 2012

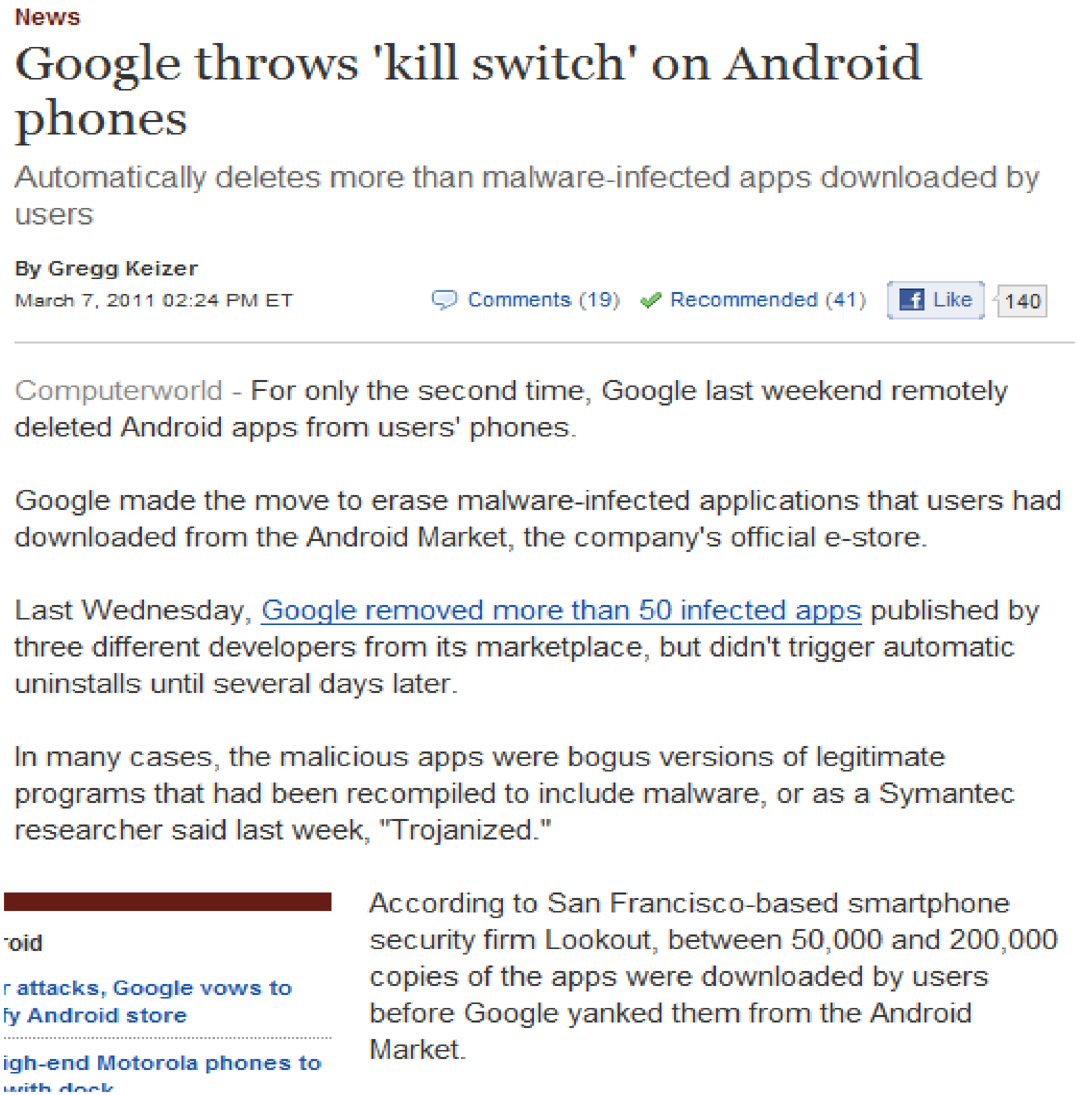
Who is Bob?

dex2jar

Tools to work with android .dex and java .class files

Industry Trends

Malware increasing on “App Stores”



News

Google throws 'kill switch' on Android phones

Automatically deletes more than malware-infected apps downloaded by users

By Gregg Keizer

March 7, 2011 02:24 PM ET

Computerworld - For only the second time, Google last weekend remotely deleted Android apps from users' phones.

Google made the move to erase malware-infected applications that users had downloaded from the Android Market, the company's official e-store.

Last Wednesday, Google removed more than 50 infected apps published by three different developers from its marketplace, but didn't trigger automatic uninstalls until several days later.

In many cases, the malicious apps were bogus versions of legitimate programs that had been recompiled to include malware, or as a Symantec researcher said last week, "Trojanized."

According to San Francisco-based smartphone security firm Lookout, between 50,000 and 200,000 copies of the apps were downloaded by users before Google yanked them from the Android Market.

Chris Di Bona from Google, November 2011:

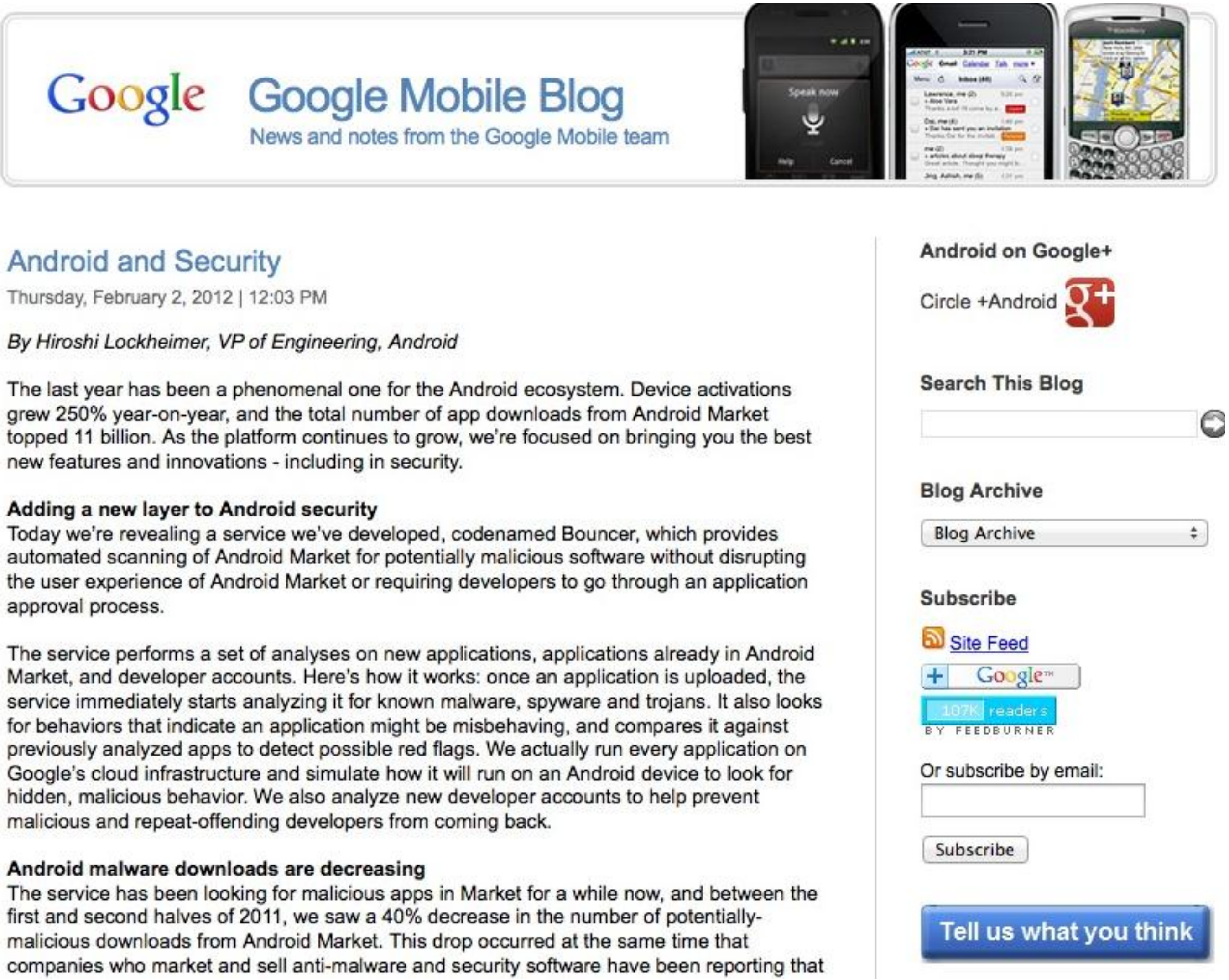
”virus companies are playing on your fears to try to sell you bs protection software for Android, RIM and IOS. They are charlatans and scammers. IF you work for a company selling virus protection for android, rim or IOS you should be ashamed of yourself.”

“The barriers to spreading such a program from phone to phone are large and difficult enough to traverse when you have legitimate access to the phone, but this isn’t independence day, a virus that might work on one device won’t magically spread to the other.”

All the major vendors have app markets, and all the major vendors have apps that do bad things, are discovered, and are dropped from the markets.

Industry Trends

Google’s Bouncer



Google Mobile Blog

News and notes from the Google Mobile team

Android and Security

Thursday, February 2, 2012 | 12:03 PM

By Hiroshi Lockheimer, VP of Engineering, Android

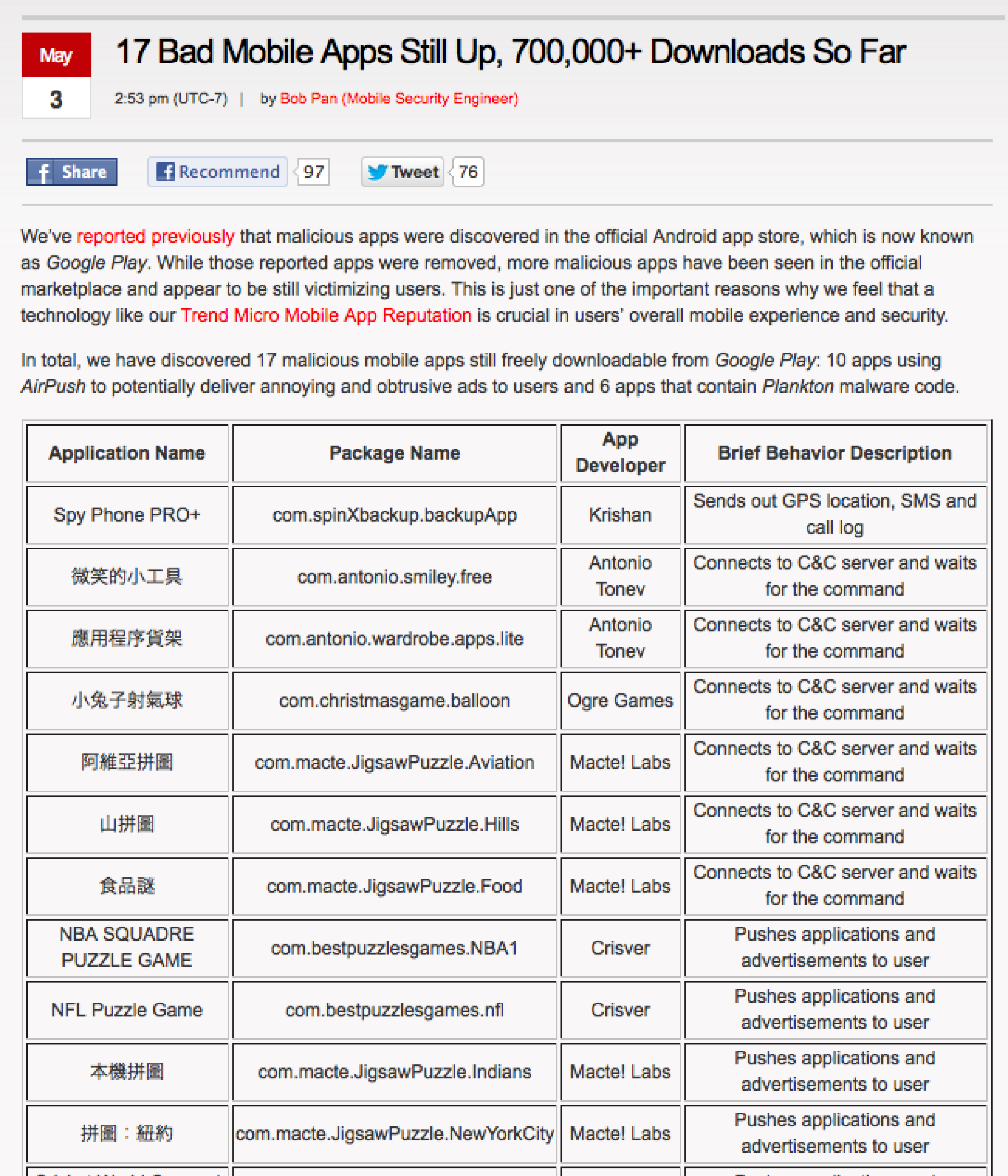
The last year has been a phenomenal one for the Android ecosystem. Device activations grew 250% year-on-year, and the total number of app downloads from Android Market topped 11 billion. As the platform continues to grow, we're focused on bringing you the best new features and innovations - including in security.

Adding a new layer to Android security
Today we're revealing a service we've developed, codenamed Bouncer, which provides automated scanning of Android Market for potentially malicious software without disrupting the user experience of Android Market or requiring developers to go through an application approval process.

The service performs a set of analyses on new applications, applications already in Android Market, and developer accounts. Here's how it works: once an application is uploaded, the service immediately starts analyzing it for known malware, spyware and trojans. It also looks for behaviors that indicate an application might be misbehaving, and compares it against previously analyzed apps to detect possible red flags. We actually run every application on Google's cloud infrastructure and simulate how it will run on an Android device to look for hidden, malicious behavior. We also analyze new developer accounts to help prevent malicious and repeat-offending developers from coming back.

Android malware downloads are decreasing
The service has been looking for malicious apps in Market for a while now, and between the first and second halves of 2011, we saw a 40% decrease in the number of potentially-malicious downloads from Android Market. This drop occurred at the same time that companies who market and sell anti-malware and security software have been reporting that

Google’s Bouncer effective?



May
3

17 Bad Mobile Apps Still Up, 700,000+ Downloads So Far

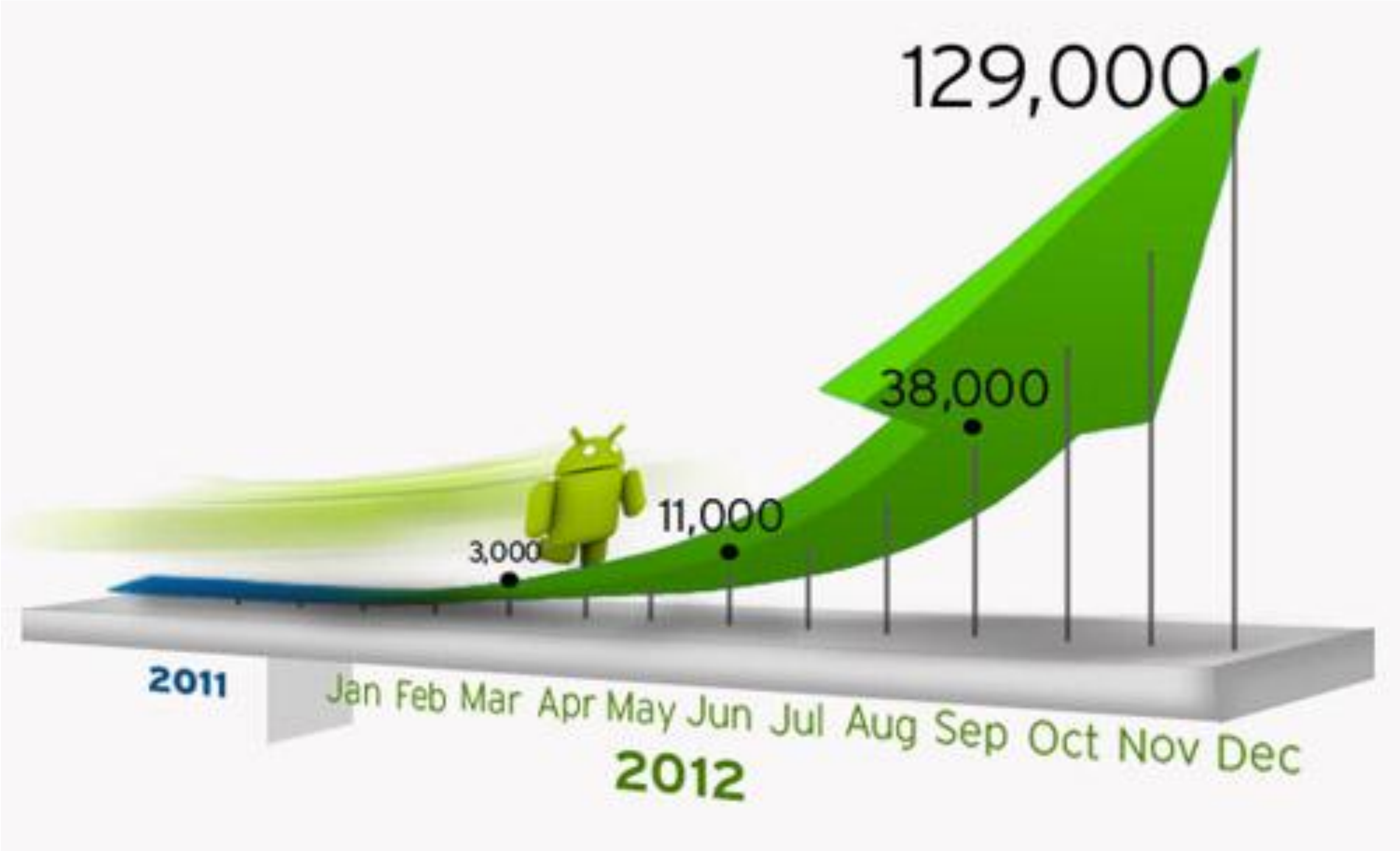
2:53 pm (UTC-7) | by Bob Pan (Mobile Security Engineer)

We've reported previously that malicious apps were discovered in the official Android app store, which is now known as *Google Play*. While those reported apps were removed, more malicious apps have been seen in the official marketplace and appear to be still victimizing users. This is just one of the important reasons why we feel that a technology like our Trend Micro Mobile App Reputation is crucial in users' overall mobile experience and security.

In total, we have discovered 17 malicious mobile apps still freely downloadable from *Google Play*: 10 apps using *AirPush* to potentially deliver annoying and obtrusive ads to users and 6 apps that contain *Plankton* malware code.

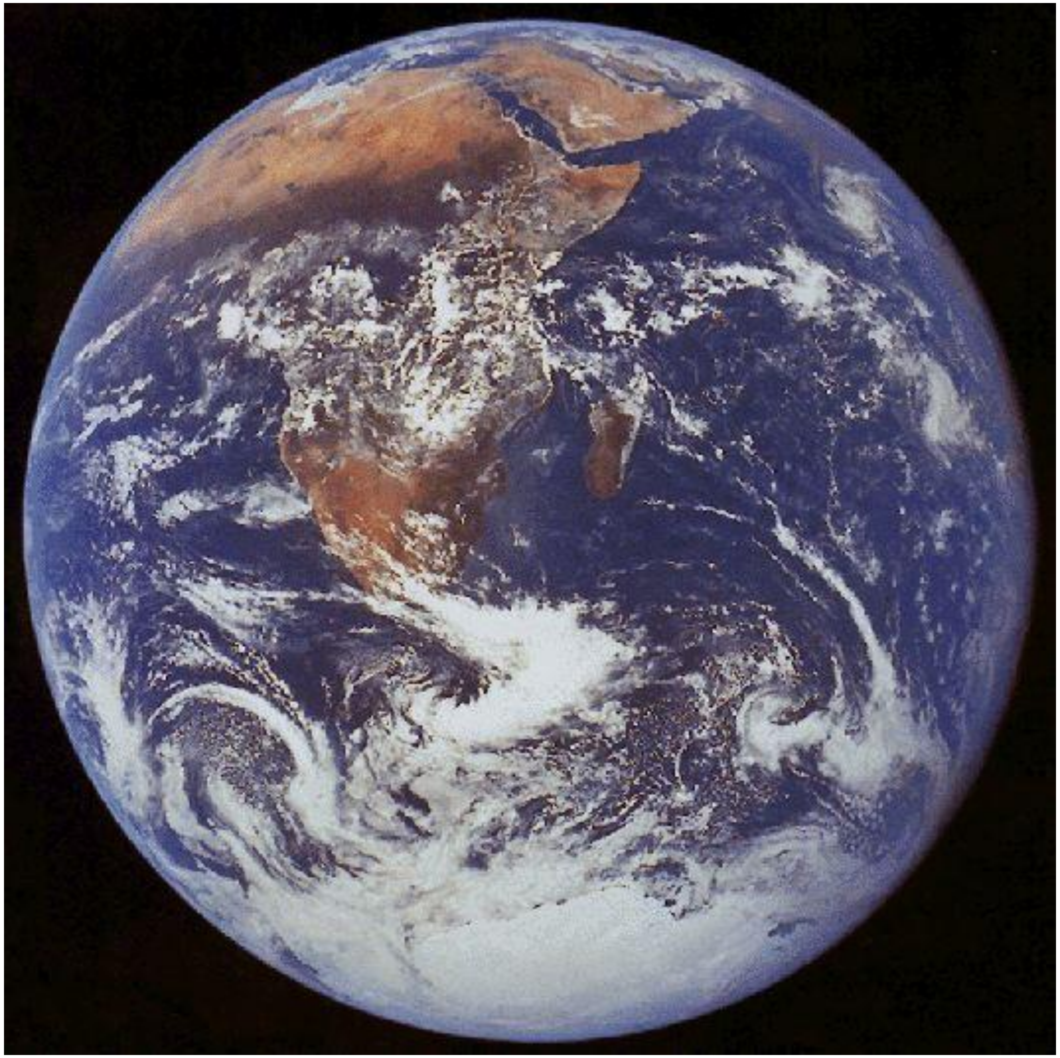
Application Name	Package Name	App Developer	Brief Behavior Description
Spy Phone PRO+	com.spinXbackup.backupApp	Krishan	Sends out GPS location, SMS and call log
微笑的小工具	com.antonio.smiley.free	Antonio Tonev	Connects to C&C server and waits for the command
應用程序貨架	com.antonio.wardrobe.apps.lite	Antonio Tonev	Connects to C&C server and waits for the command
小兔子射氣球	com.christmasgame.balloon	Ogre Games	Connects to C&C server and waits for the command
阿維亞拼圖	com.macte.JigsawPuzzle.Aviation	Macte! Labs	Connects to C&C server and waits for the command
山拼圖	com.macte.JigsawPuzzle.Hills	Macte! Labs	Connects to C&C server and waits for the command
食品謎	com.macte.JigsawPuzzle.Food	Macte! Labs	Connects to C&C server and waits for the command
NBA SQUADRE PUZZLE GAME	com.bestpuzzlesgames.NBA1	Crisver	Pushes applications and advertisements to user
NFL Puzzle Game	com.bestpuzzlesgames.nfl	Crisver	Pushes applications and advertisements to user
本機拼圖	com.macte.JigsawPuzzle.Indians	Macte! Labs	Pushes applications and advertisements to user
拼圖：紐約	com.macte.JigsawPuzzle.NewYorkCity	Macte! Labs	Pushes applications and advertisements to user

Android Malware



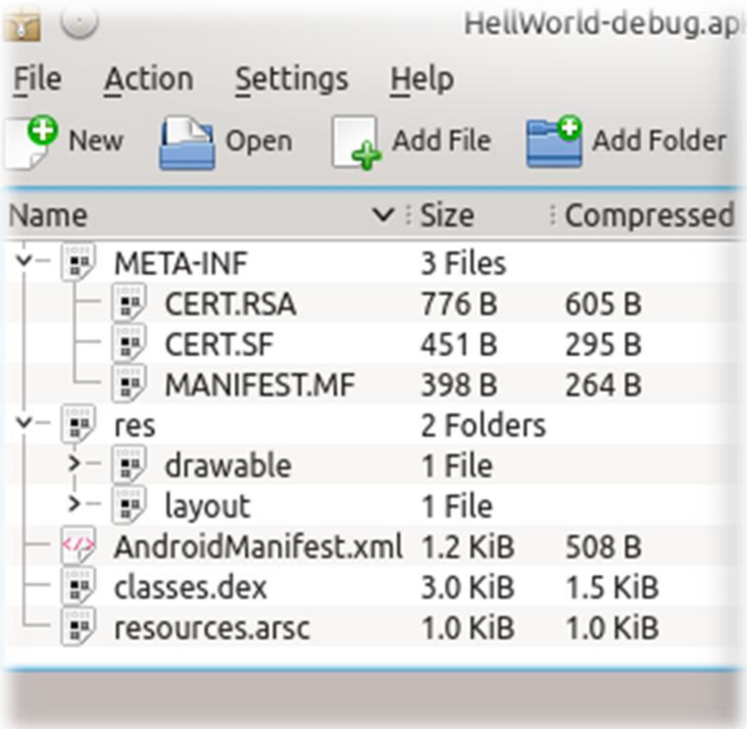
http://blog.trendmicro.com/how-big-will-the-android-malware-threat-be-in-2012/

Where’s the challenge?



The Inside of an APK File

- AndroidManifest.xml contains the meta information;
  - Package name & version
  - Activities
  - Services
- classes.dex contains all the code for Dalvik Virtual Machine.
- META-INF/ contains the certificate and signature.



Name	Size	Compressed
META-INF	3 Files	
CERT.RSA	776 B	605 B
CERT.SF	451 B	295 B
MANIFEST.MF	398 B	264 B
res	2 Folders	
drawable	1 File	
layout	1 File	
AndroidManifest.xml	1.2 KiB	508 B
classes.dex	3.0 KiB	1.5 KiB
resources.arsc	1.0 KiB	1.0 KiB

APK are signed zip files

The AndroidManifest File Google’s Binary xml File

- Format is not documented
- Tools for reading Binary xml files are readily available
- Tools for writing Binary xml files are limited

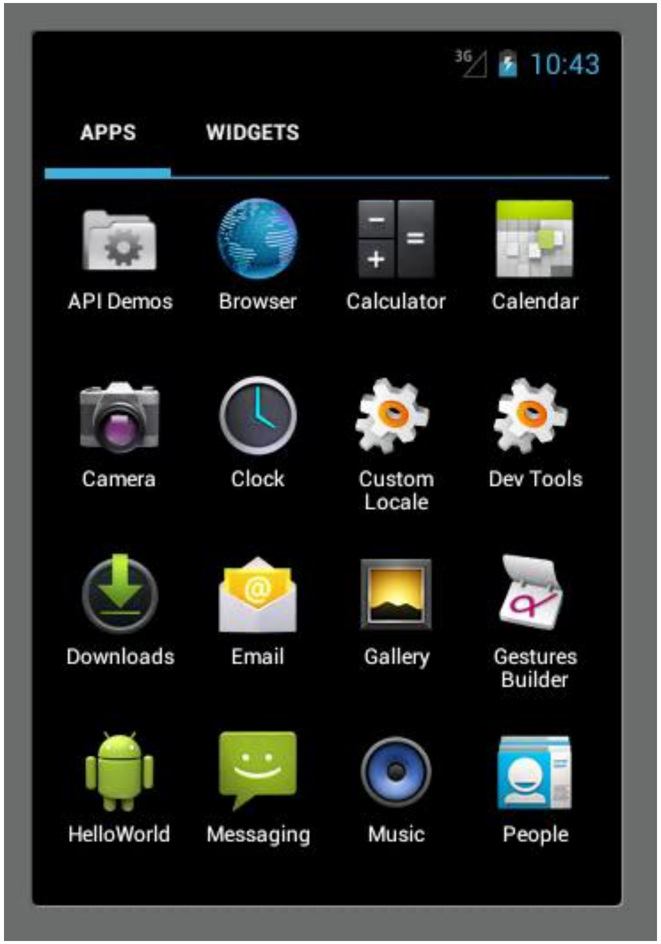
The Dex File
Dalvik Executable Format

- Format is well documented
- Many modification tools available
  - asmdex
  - smali/baksmali
  - Dexmaker
- APKs can only use 16 to 32MB of memory so a separate Dalvik VM should be started

The META-INF/ Folder Certificate & Signature

- Format is well documented
- Many creation tools available
  - jarsigner from JDK
  - signapk from Android Source
- Minor modifications must be done to run on an Android device

Infection Demonstration



Architecture of the Virus

Part A

The “Loader” of the Virus

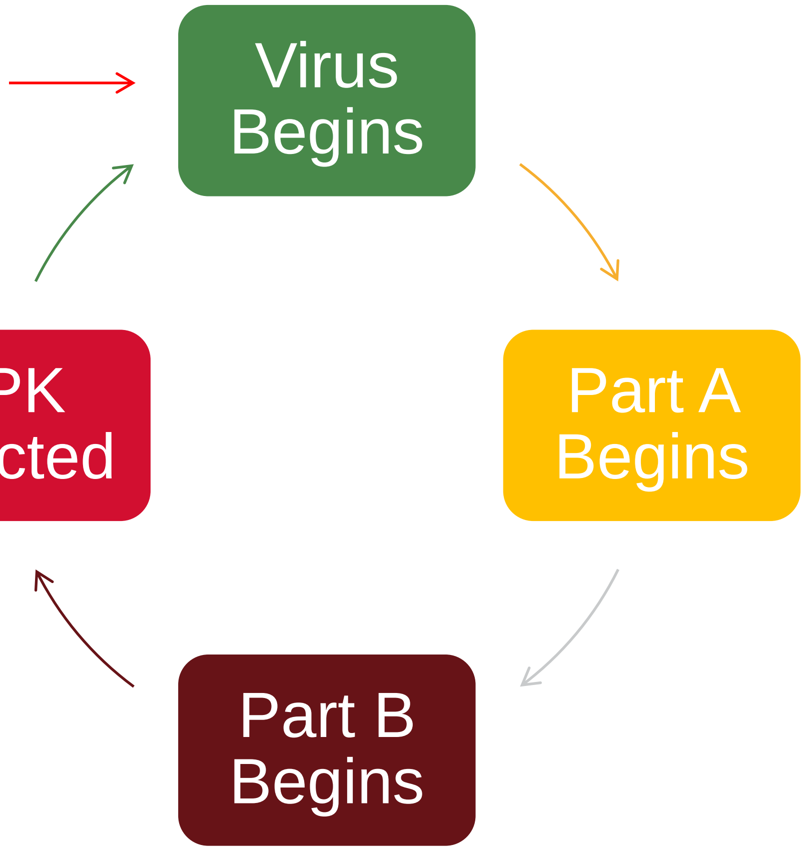
- Extract & load Part B
- Initiate Part B

Part B

The “Payload” of the Virus

- Locate uninfected APK file
- Inject Part A into classes.dex and AndroidMainfest.xml
- Copy itself to the APK file
- Sign the APK file
- Prompt the User to install the APK file

Infection Cycle



Virus Begins

Part A Begins

Part B Begins

APK Infected

Securing Your Journey to the Cloud

谢谢!

Thank You!

Feel free to contact me anytime at
bob_pan@trendmicro.com.cn