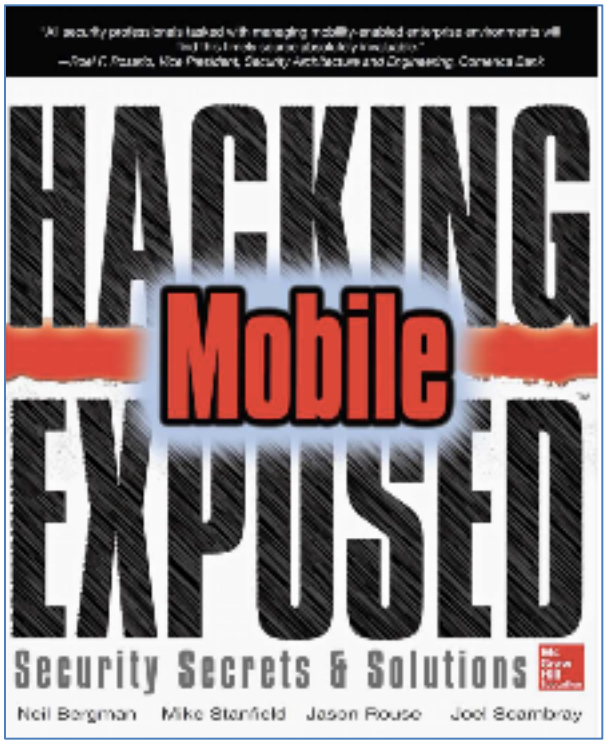
Ch 5: Mobile Malware

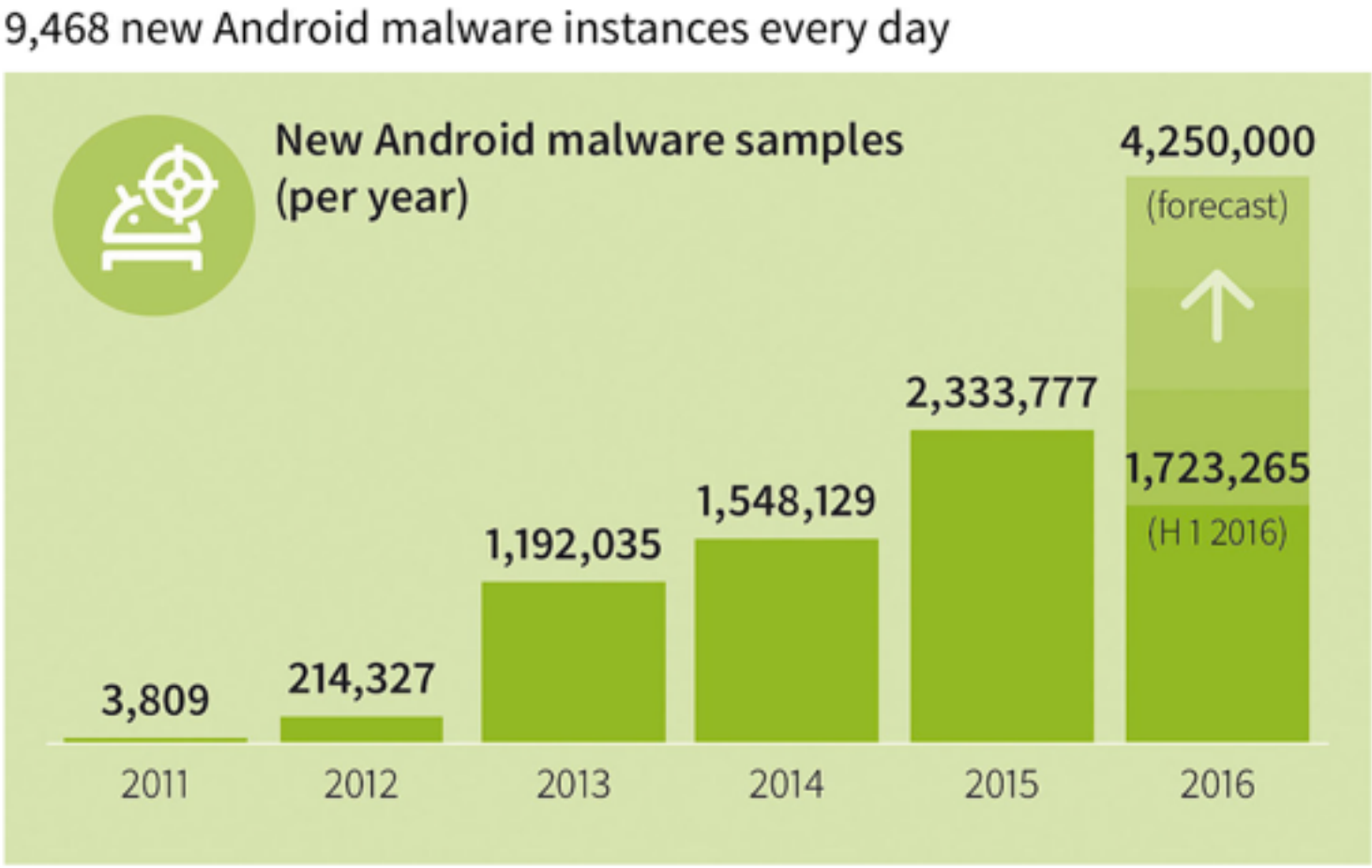


CNIT 128: Hacking Mobile Devices

Updated 3-7-17

Increase in Mobile Malware

- From link Ch 5h



1,723,265 new Android malware apps in the first half of 2016 represent an increase of more than 30 percent over the second half of 2015. On average, the G DATA experts detected 9,468 new malware apps for the Android operating system on a daily basis. This means that a new malware strain was reported every 9 seconds. The analysts have already identified more malware apps in the first half of the year than in the entire year of 2014.

Early Malware

- LibertyCrack (2000)
  - Trojan masquerading as pirated software for Palm OS
  - Restored device to factory defaults

Early Malware

- Cabir (2004)
  - First phone worm
  - Infected Symbian phones
  - Spread via Bluetooth
    - Image from link Ch 5a

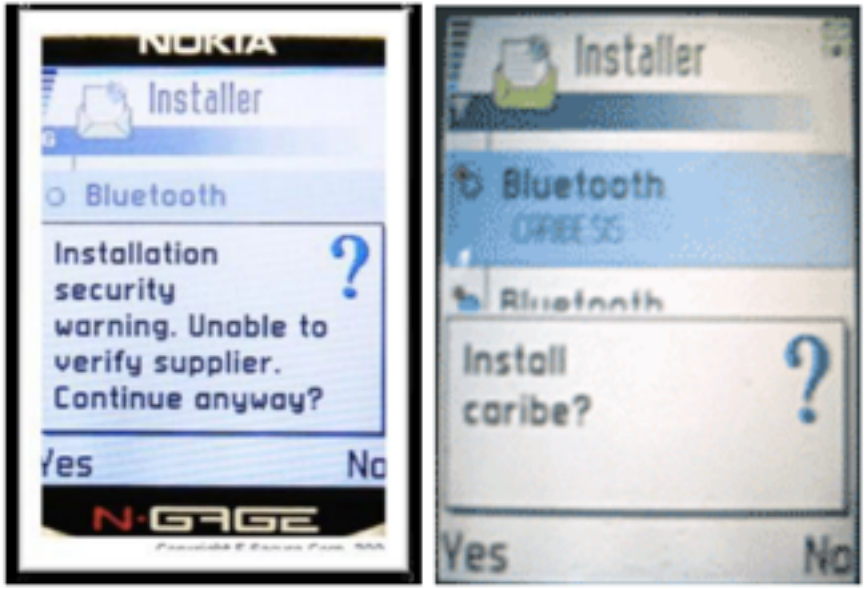


Figure 5, 6: Installation of Cabir Virus

Android Malware: New Reports

- Link Ch 5i

Methodology

We examined data using these:

- Almost one billion malware detections/incidences
- The June to November 2016 time period only
- Nearly 100 million Windows and Android devices
- Over 200 countries
- From both the corporate and consumer environments
- Concentrating on six threat categories: Ransomware, ad fraud malware, Android malware, botnets, banking Trojans, and adware

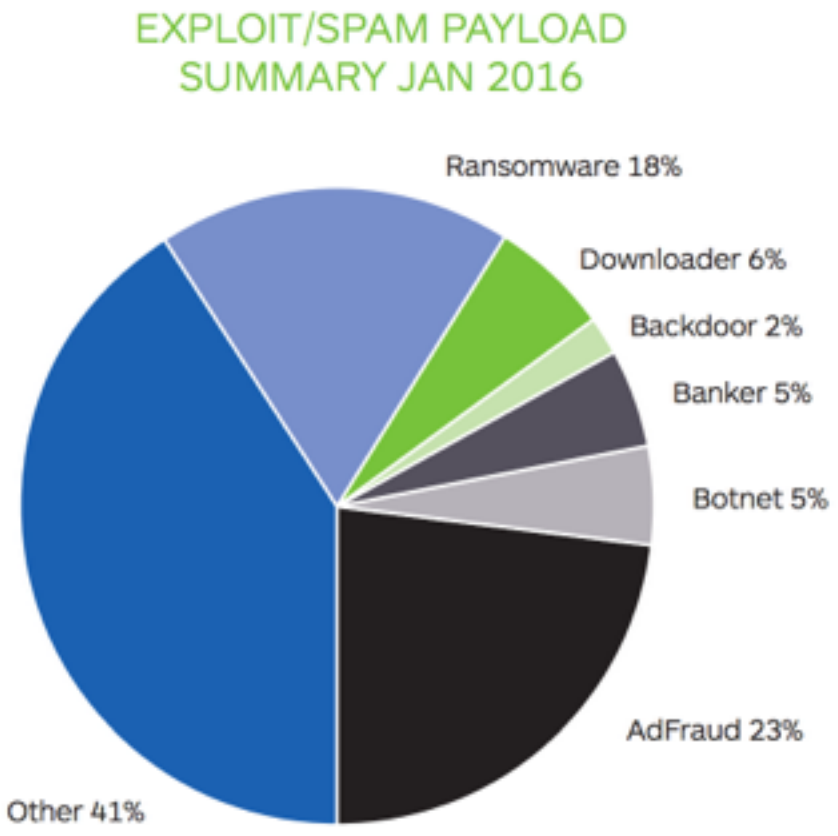


Figure 1. January 2016 payloads

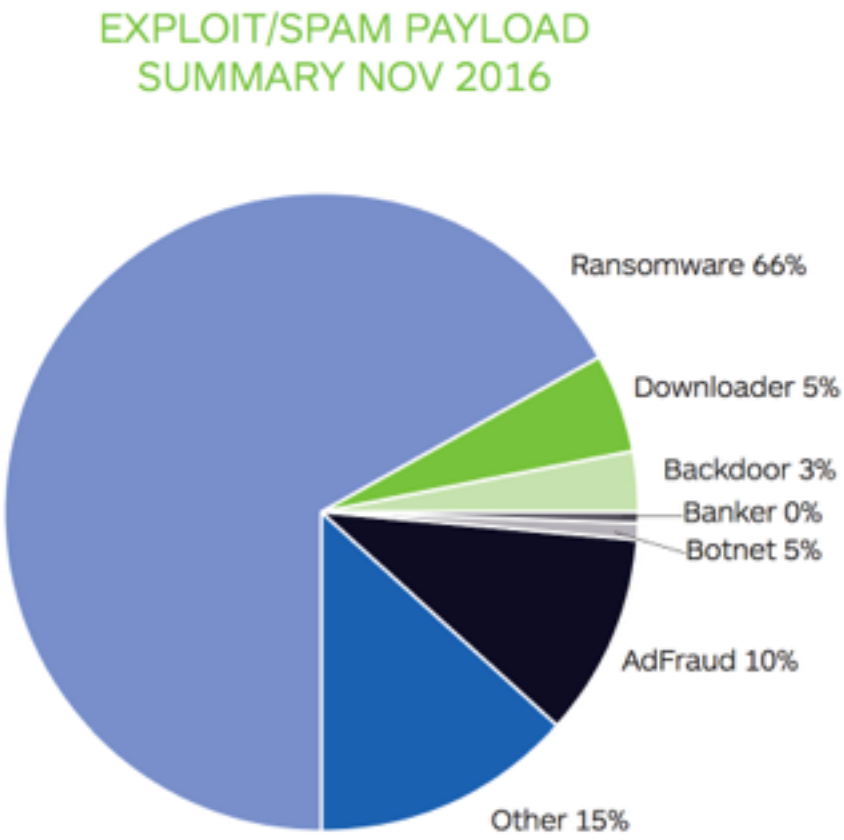


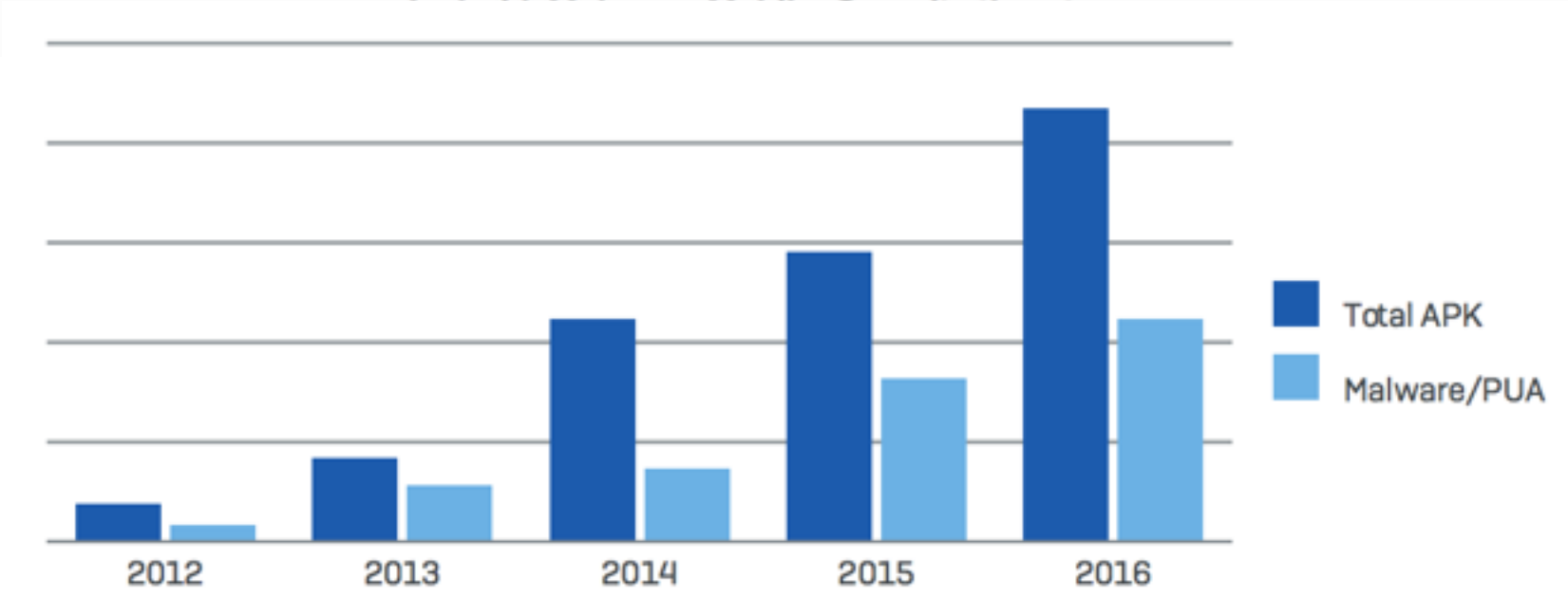
Figure 2. November 2016 payloads.

Three key takeaways

1. Ransomware grabbed headlines and became the favorite attack methodology used against businesses.
2. Ad fraud malware, led by Kovter malware, exceeded ransomware detections at times and poses a substantial threat to consumers and businesses.
3. Botnets infected and recruited Internet of Things (IoT) devices to launch massive DDoS attacks.

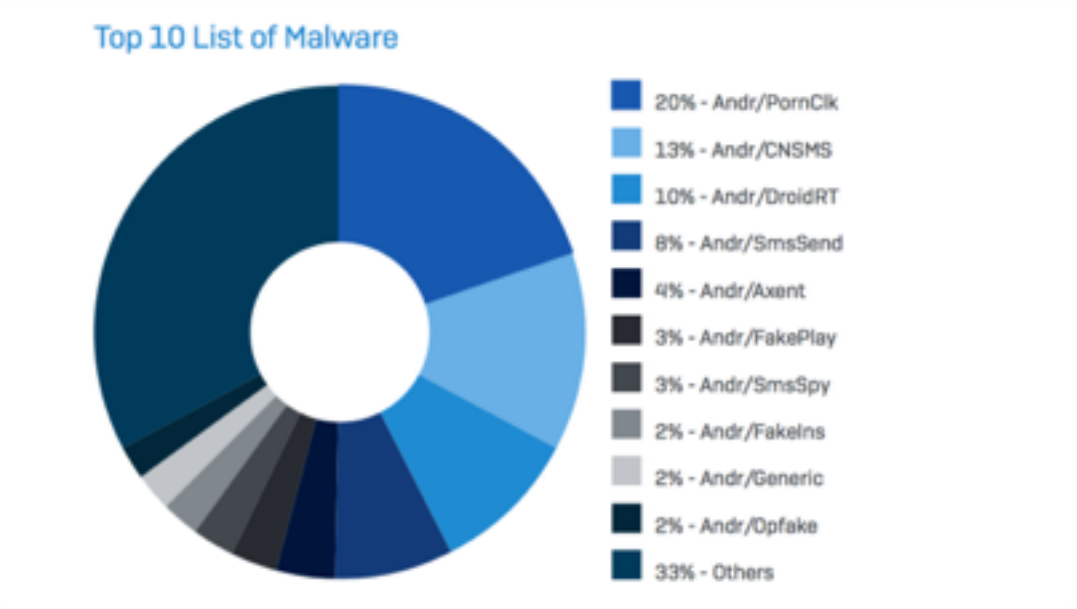
RSA 2017: SophosLabs report examines Top 10 Android malware

14 FEB 2017 1



- Ch 5j

When the lab reviewed the top 10 malware families targeting Android, Andr/PornClk is the biggest, accounting for more than 20% of the cases reviewed in 2016. Andr/CNSMS, an SMS sender with Chinese origins, was the second largest (13% of cases), followed by Andr/ DroidRT, an Android rootkit (10%), and Andr/SmsSend (8%). The top 10 are broken down in this pie chart:



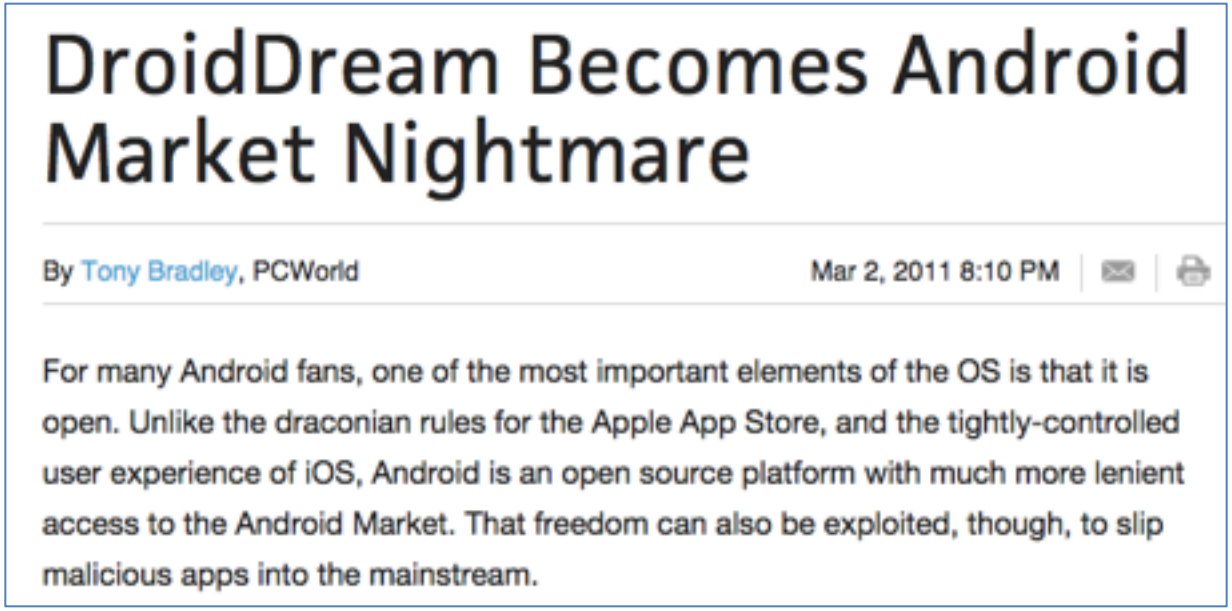
PornClk makes money through advertisements and membership registrations. It takes advantage of root privilege and requesting administrative access on the device. It then:

- Downloads additional APKs
- Creates shortcuts on home screens
- Collects sensitive information such as device IDs, phone numbers and models, Android versions and Geo IPs.

Android Malware: From Textbook

DroidDream (2011)

- Was primarily distributed by the Google Play store
- Legitimate apps were repackaged to include DroidDream and then put back in the Play store



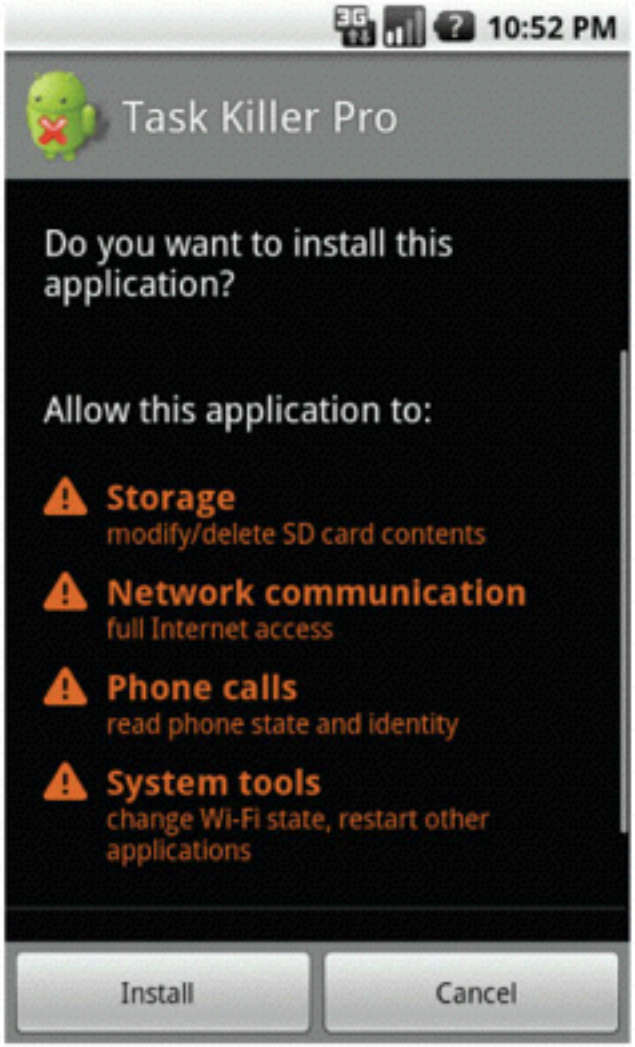
DroidDream Becomes Android Market Nightmare

By Tony Bradley, PCWorld Mar 2, 2011 8:10 PM

For many Android fans, one of the most important elements of the OS is that it is open. Unlike the draconian rules for the Apple App Store, and the tightly-controlled user experience of iOS, Android is an open source platform with much more lenient access to the Android Market. That freedom can also be exploited, though, to slip malicious apps into the mainstream.

Excessive Permissions

- App trojaned by DroidDream asks for too many permissions



Information Theft

- When it is installed, DroidDream launches a "Setting" service
- Steals private information and sends it to a remote server
  - International Mobile Station Equipment Identity (IMEI)
  - International Mobile Subscriber Identity (IMSI)

Botted

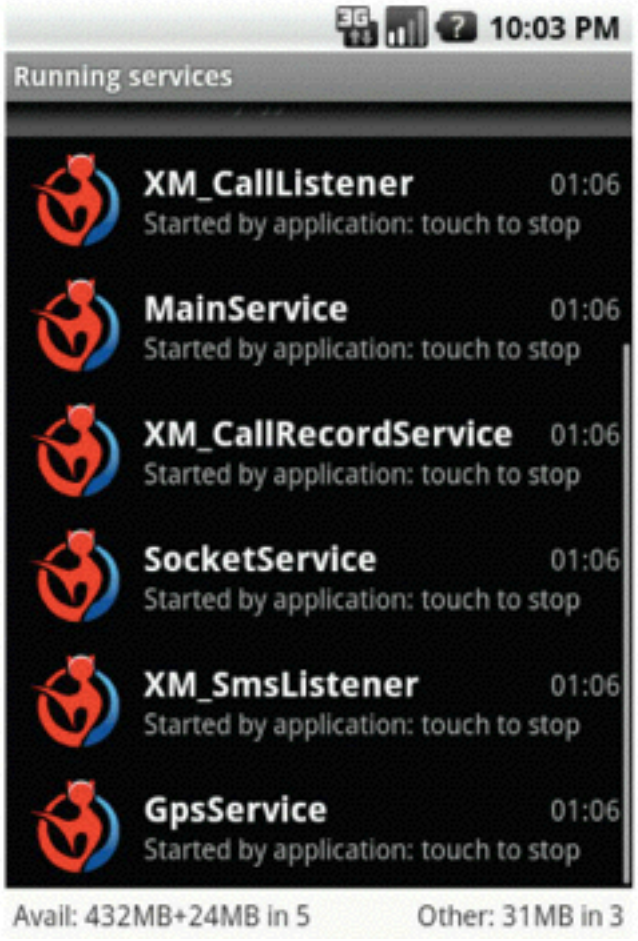
- DroidDream then roots the device
- Hijacks the app downloading and installing code
- Makes it a bot under remote control

Google's Response

- Google removed the repackaged apps from the Play Store
- But 50,000 – 200,000 users were already infected

NickiSpy

- Packaged into other software
- At next reboot, it launches the services shown to the right
- Steals IMEI, location, SMS messages and records voice phone calls
- Records sound when phone is not in use



Google's Response to NickiSpy

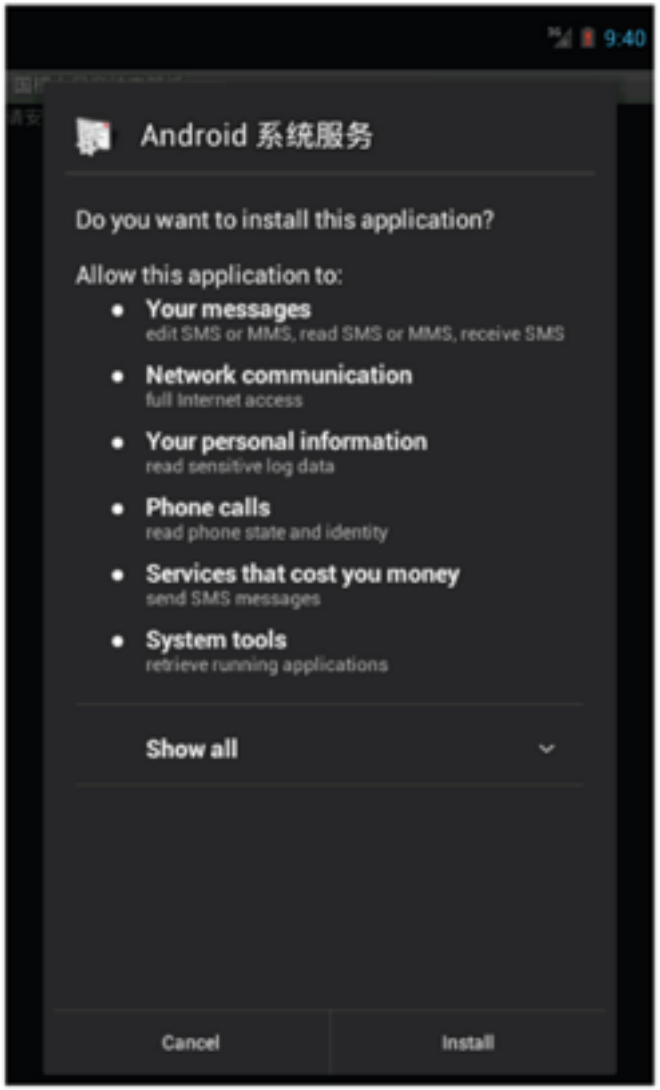
- Android 2.3 removed the ability for an application to change the phone state without user interaction
- So an app could no longer turn on the microphone as stealthily

SMSZombie

- Packaged inside live wallpaper apps in a Chinese marketplace named Gfan
- Makes fraudulent payments using China Mobile SMS Payment
- No permissions are requested during installation, because it starts as a wallpaper app
  - No clue to warn the user

Malicious App

- It then downloads another app and shows the user a box with only one option "Install" to get "100 points!"
- That installs another app that does ask for permissions



Becoming Administrator

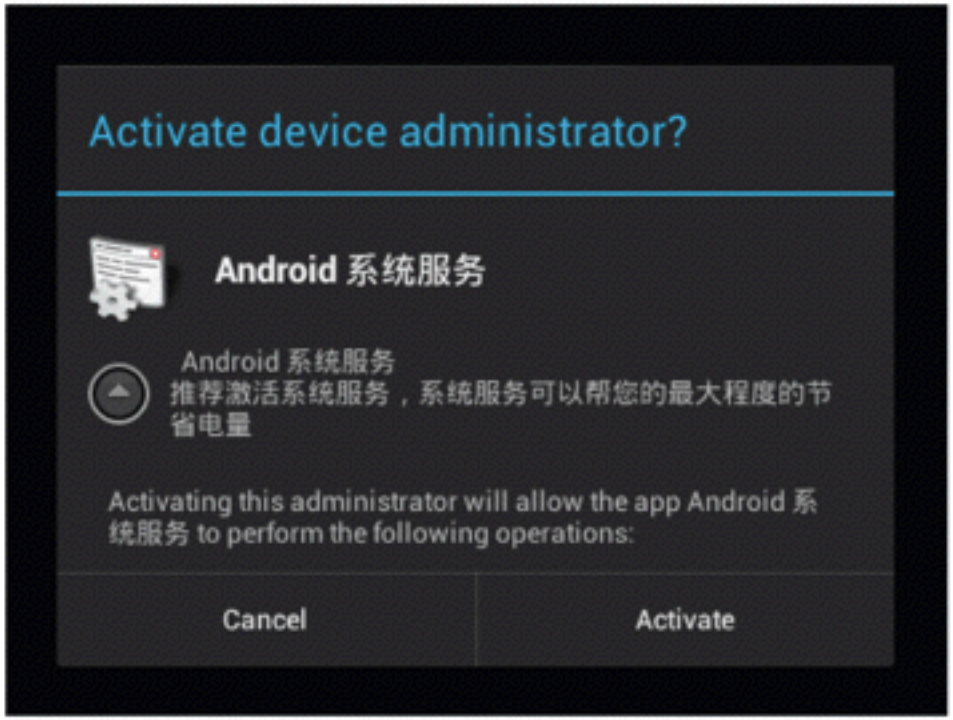


Figure 5-4 SMSZombie becoming a device administrator

Payload

- SMSZombie sends all SMS messages currently on the device to a target phone #
- It then scans all SMS messages to stealthily steal and delete ones that are warning the phone user about fraudulent SMS transactions

Banking Malware

Man-in-the-Browser (MITB) Attack

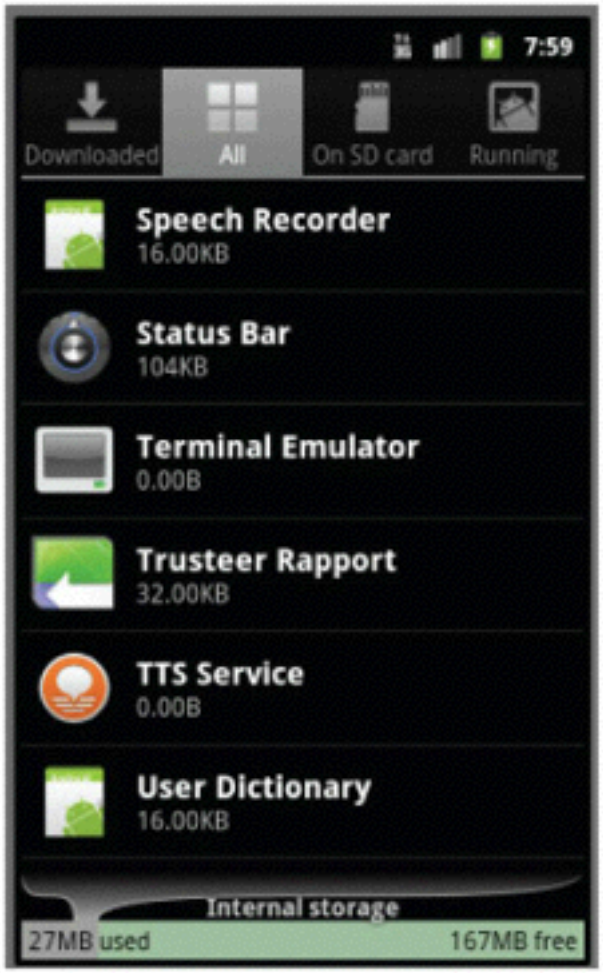
- A Trojan installed on a PC hooks Windows API networking calls such as `HttpSendRequestW`
- Allows attacker to intercept and modify HTTP and HTTPS traffic sent by the browser
- Can steal banking credentials and display false information to the user

Two-Factor Authentication (2FA)

- This was the response by banks to resist MITB attacks
- Use an SMS to a phone as the second factor for 2FA
  - Message contains a *mobile transaction authentication number (mTAN)*
- Customer types mTAN into the banking web app on the PC

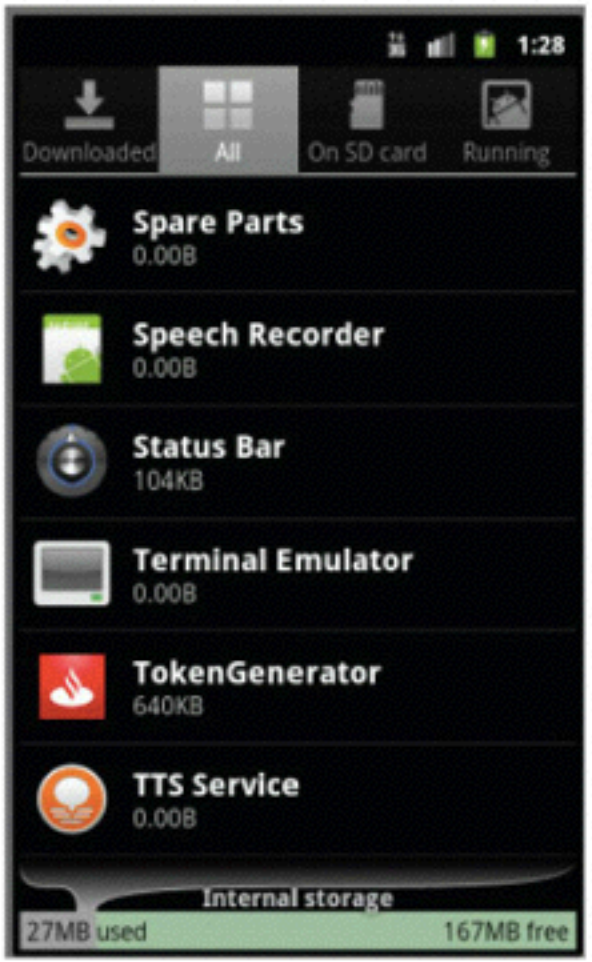
Zeus and Zitmo Defeat 2FA

- Zeus malware on the PC
  - Manipulates HTTPS traffic to encourage user to install fake Trusteer mobile security software
  - Looks like legitimate security software on the phone
  - Steals SMS messages from the phone to defeat 2FA



FakeToken

- User is tricked into installing **TokenGenerator** app
- It requests suspicious permissions, including
  - Install and delete apps
    - An error by the malware designers: only system apps can have that permission
  - Send and receive SMS messages



Payload

- TakeToken steals SMS messages to defeat 2FA
- Can also steal contact list

Google's Bouncer Malware Tool Hacked

BY STEPHANIE MLOT JUNE 5, 2012 05:18PM EST 4 COMMENTS

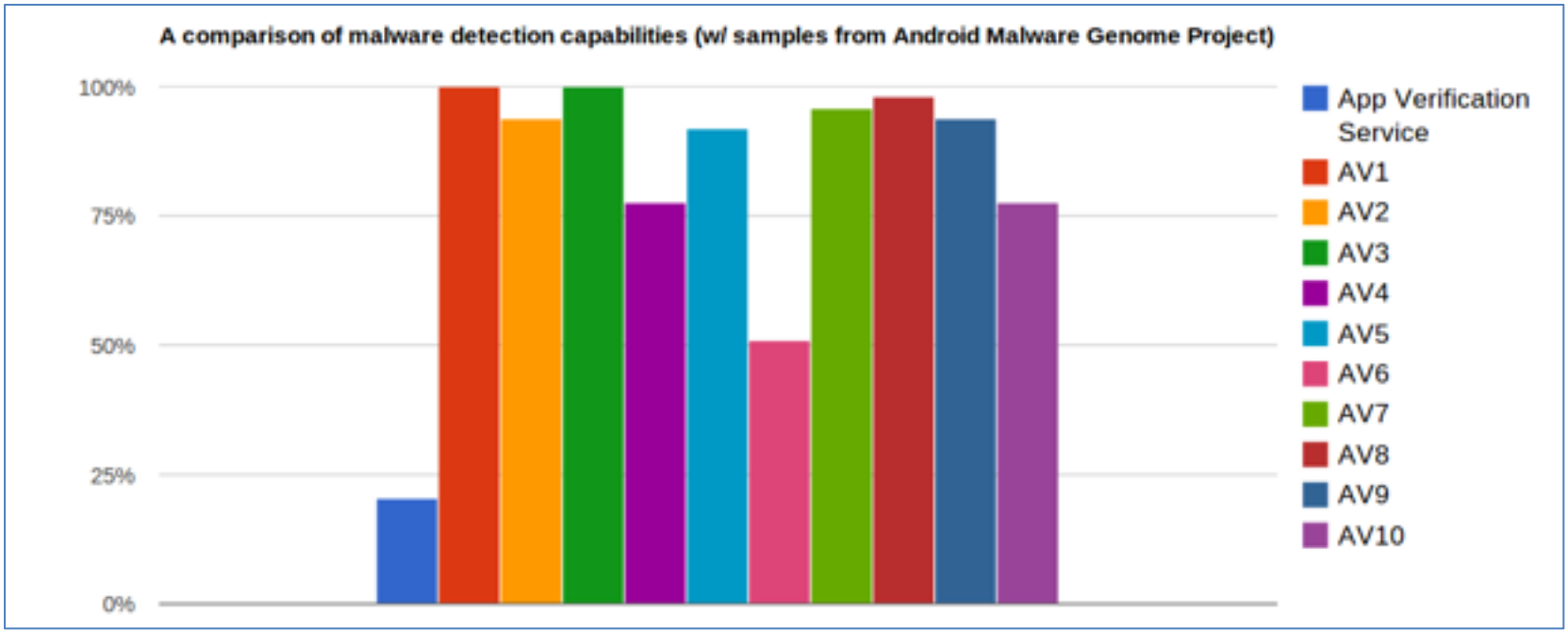
Google's malware blocker Bouncer has been hacked by security analysts Jon Oberheide and Charlie Miller, who claim that their workaround will allow malicious malware to access apps even with a Bouncer scan.

How Bouncer was Hacked

- Researchers submitted an app containing a remote shell
- When Bouncer ran the app in a virtual machine, it phoned home to the researchers
- They explored the VM and exploited Bouncer itself
- With a remote shell inside Bouncer, they explored it and found ways to defeat it

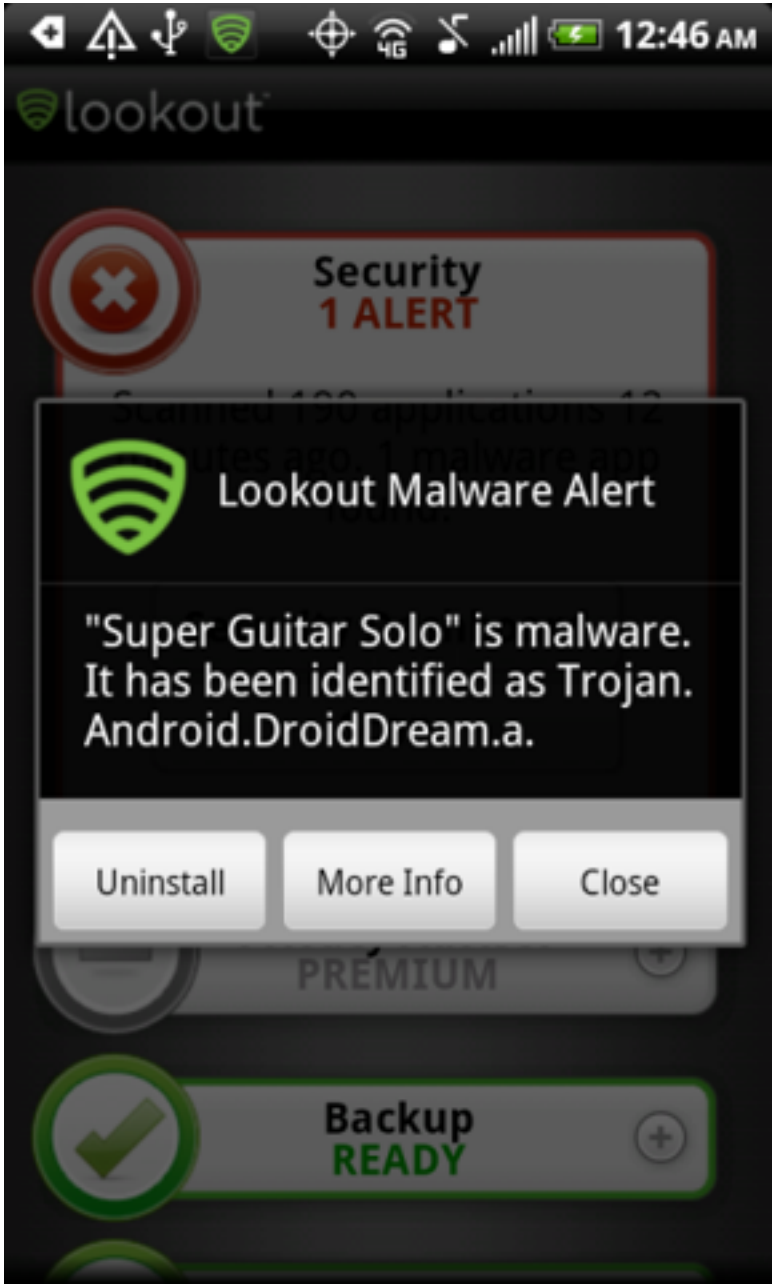
Google Application Verification Service

- Launched in 2012
- Tries to detect malicious apps
- Much less effective than 3rd-party AV
  - Link Ch 5e



Moral: Get Real AV

- Avast! won in a review from Feb., 2015
  - Link Ch 5g
- There are plenty of others, including
  - Lookout
  - AVG
  - Kaspersky
  - Norton
  - McAfee



iOS Malware

What iOS malware?

Risk is Very Small

- Very few items of malware, very few users actually infected, no real harm done
- An academic exercise in theoretical computer security, not a real risk for users

Fake Update

- "iPhone firmware 1.1.3 prep software"
- Only for jailbroken devices
- Supposedly written by an 11-year-old
- Broke utilities like Doom and SSH
- A minor annoyance

Jailbroken iPhones with Default SSH Password

- Dutch teenager scanned for iPhones on T-Mobile's 3G IP range
  - Pushed ransomware onto phones in Nov. 2009
- Australian teenager wrote the iKee worm to Rickroll iPhones in 2009
  - A later version made an iPhone botnet

iOS Malware in the Apple App Store

- "Find and Call"
  - First seen in 2012
  - Also in Google Play
  - Uploads user's contacts to a Web server
  - Sends SMS spam to the contacts with install links
  - Spreads but does no other harm

Malware Security: Android v. iOS

Why the Huge Difference?

- Market share
- App approval process
  - $25 to register for Google Play
    - Apps appear within 15-60 min.
  - $99 to register for Apple's App Store
    - A week of automated & manual review before app appears in the store
- Third-party app stores
  - Allowed on Android, but not on iOS (unless you jailbreak)