The "Five W's" of Mobile Device Malware: Who, What, When, Where, and Why? … *and What Can be Done About It?*

Kevin McPeak, CISSP, ITILv3

Principal Cyber Architect, U.S. Federal

Symantec Public Sector Strategic Programs

Who Can Be Affected by Mobile Malware?

Governmental, Commercial, and Home Users

Apple iOS

Android

BlackBerry OS

Windows Phone

Who Creates & Distributes Mobile Malware?

Cyber Criminals and their Accomplices

Malware Developers

Mules

Mobile Botnet Operators

Cyber Thieves

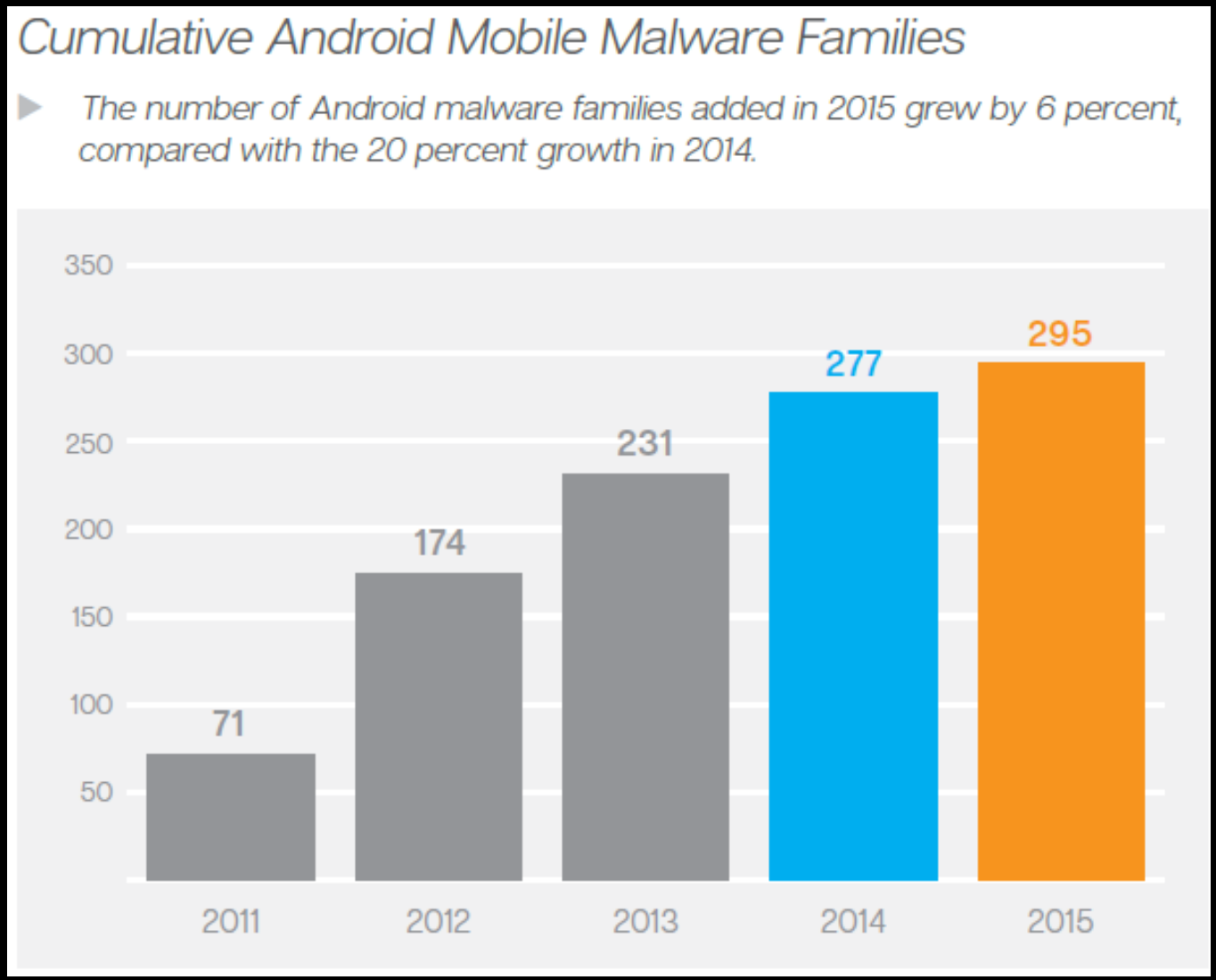
Espionage Rings

Hacktivists

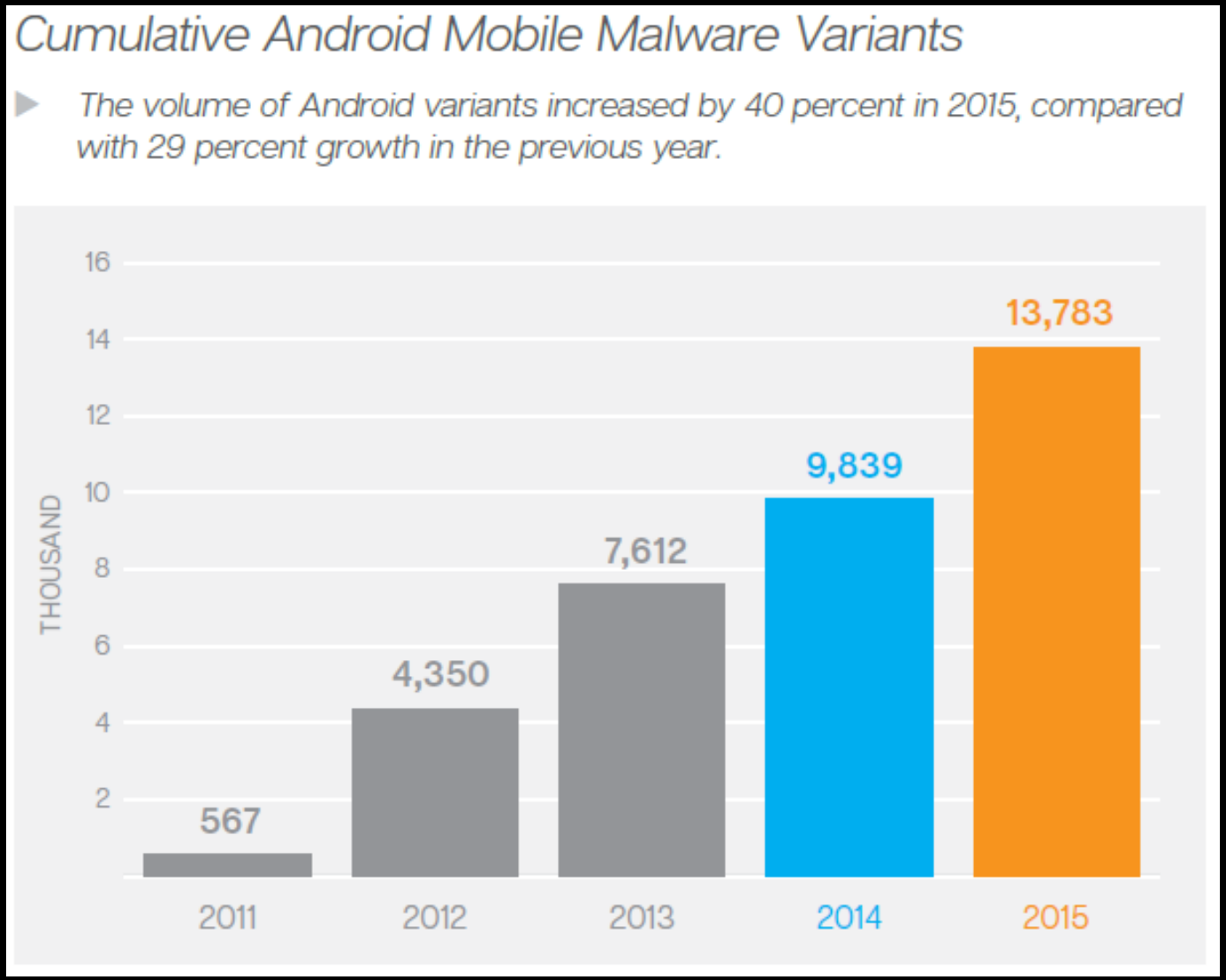
What is Mobile Malware and How Do We Count Them?

- Each of these applications contain the same piece of malware embedded in them
- Each piece of malware is counted as one Family
  - If this malware is modified the new version counts as a Variant
- We would count the five apps as Samples
- We do not report on Samples, but many vendors do

What is the Growth Rate of Android Malware by Families?



What is the Growth Rate of Android Malware by Variants?



What is the Overall Growth Rate of Android Malware?

New Mobile Vulnerabilities

2013	2014	2015
127	168	528
–	+32%	+214%

New Android Mobile Malware Families

2013	2014	2015
57	46	18
–	-19%	-61%

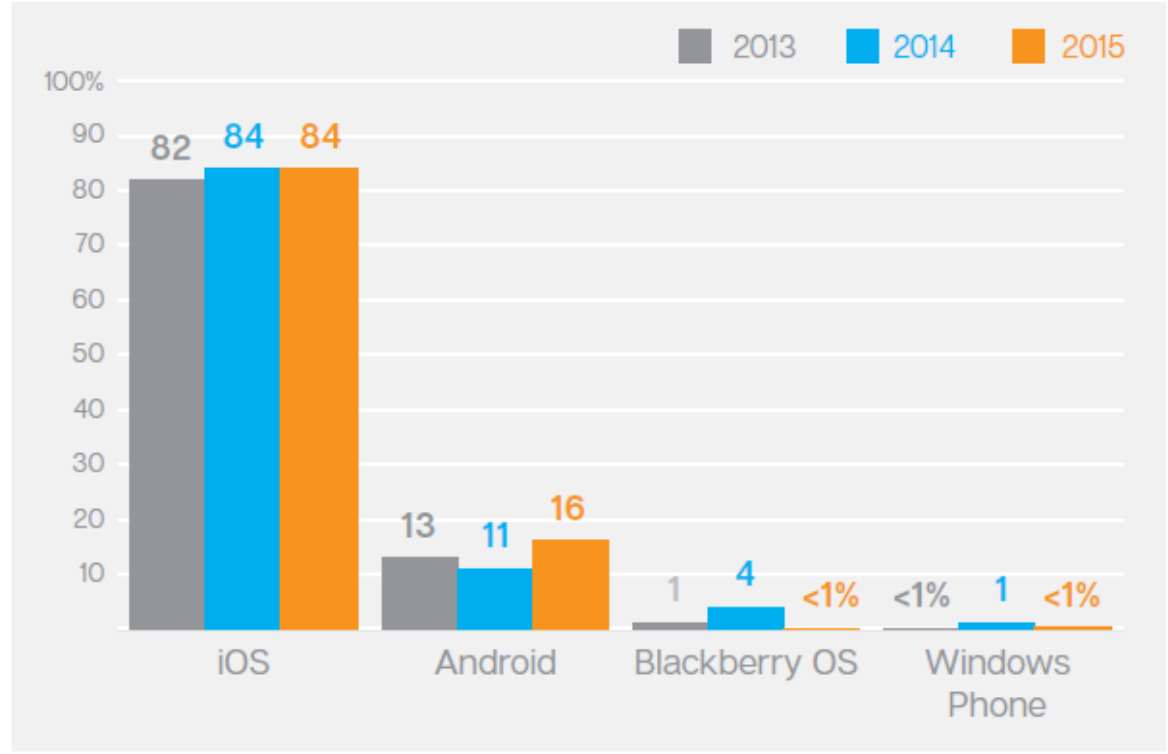
New Android Mobile Malware Variants

2013	2014	2015
3,262	2,227	3,944
–	-32%	+77%

What Mobile Platform Has the Most Vulnerabilities? …What Mobile Device Type Has the Most Threats?

Mobile Vulnerabilities by Operating System

- *Vulnerabilities on the iOS platform have accounted for the greatest number of mobile vulnerabilities in recent years, with research often fueled by the interest to jail-break devices or gain unauthorized access to install malware.*



What Types of Mobile Malware Exist?

When is Mobile Malware Active?

When Mobile Data is Collected: When IMEI7 and IMSI8 numbers are taken by attackers as a way to uniquely identify a device.

When Users Are Tracked: When communication data such as SMS messages, call logs, GPS coordinates, calendar events, or personal photos are exfiltrated.

When Bad Apps Send Out Content: When an app sends a text message to a premium SMS number, ultimately appearing on the mobile bill of the device's owner.

Or when a device is hijacked to serve as an e-mail spam relay system, thus allowing unwanted e-mails to be sent from addresses registered to the device.

When Device Settings are Changed: When an attempt is made to elevate privileges or modify OS settings to perform further actions on the compromised devices.

When Ransomware Locks the Device: When the device is encrypted and the owner is instructed to pay ransom to unlock the device.

Where is Mobile Malware Found?

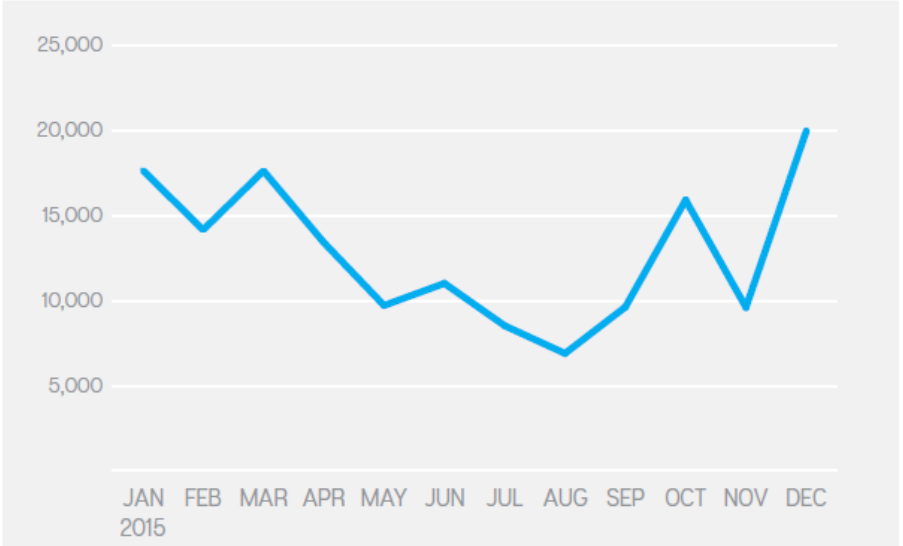
- In 2018, App revenues will be worth $92 Billion
- Currently there are 70 app stores
- The big 5 app stores contain approx. 1.9 Million apps
- Approx. 25% of apps downloaded are used just once
- Most used app: Facebook

Where is Mobile Malware Found?

Symantec research has consistently shown that third-party app stores host the most malware.

Android Malware Volume

- *There were more than three times as many Android apps classified as containing malware in 2015 than in 2014, an increase of 230 percent.*



Top Ten Android Malware

- *Thirty-seven percent of Android malware blocked by Symantec in 2015 related to variants of Android.Lotoor, which is generic detection for hacking tools that can exploit vulnerabilities in Android in order to gain root privilege access on compromised Android devices.*

Rank	Malware	Percentage
1	Android.Lotoor	36.8%
2	Android.RevMob	10.0%
3	Android.Malapp	6.1%
4	Android.Fakebank.B	5.4%
5	Android.Generisk	5.2%
6	Android.AdMob	3.3%
7	Android.Iconosis	3.1%
8	Android.Opfake	2.7%
9	Android.Premiumtext	2.0%
10	Android.Basebridge	1.7%

Where is Mobile Malware Found?

Apple iOS Users Now More at Risk than Ever

Thanks to Apple's tight control over its app store and operating system, threats to iPhones and iPads have been infrequent and limited in scale. This changed in 2015.

- In 2015, we identified nine new iOS threat families, compared to four in total previously.
- Bootlegged developer software, known as XcodeGhost, infected as many as 4,000 apps.
- The YiSpecter malware bypassed the app store altogether by using the enterprise app provisioning framework.
- Researchers found Youmi embedded in 256 iOS apps. This software is used in apps to display advertising, but also sends personal information to a remote location without users' consent.
- Vulnerabilities in Apple's AirDrop wireless file transfer system could allow an attacker to install malware on an Apple device.

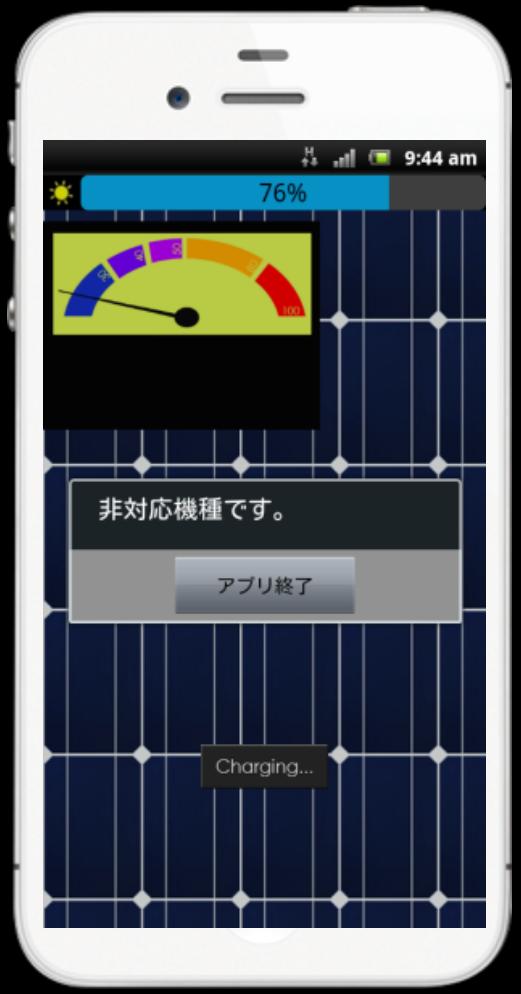
- **iOS App Developers Haunted by XcodeGhost**
- **YiSpecter Shows How Attackers Now Have iOS Firmly in Their Sights**
- **Targeting Non-Jailbroken iOS Devices and Certificate Abuse**
- **Exploiting Apple's Private APIs**
- **Cross-Platform Youmi Madware Pilfers Personal Data on iOS and Android**

Why is Mobile Malware Developed?

…. because There is Significant Illicit Money Being Made

- Stealing Information
- Ransomware
- Mobile Adware (Madware)
- IoT (Internet of Things)
- Premium SMS Messages
- Bank Fraud
- Botnets and Spam

Information Stealing Malware



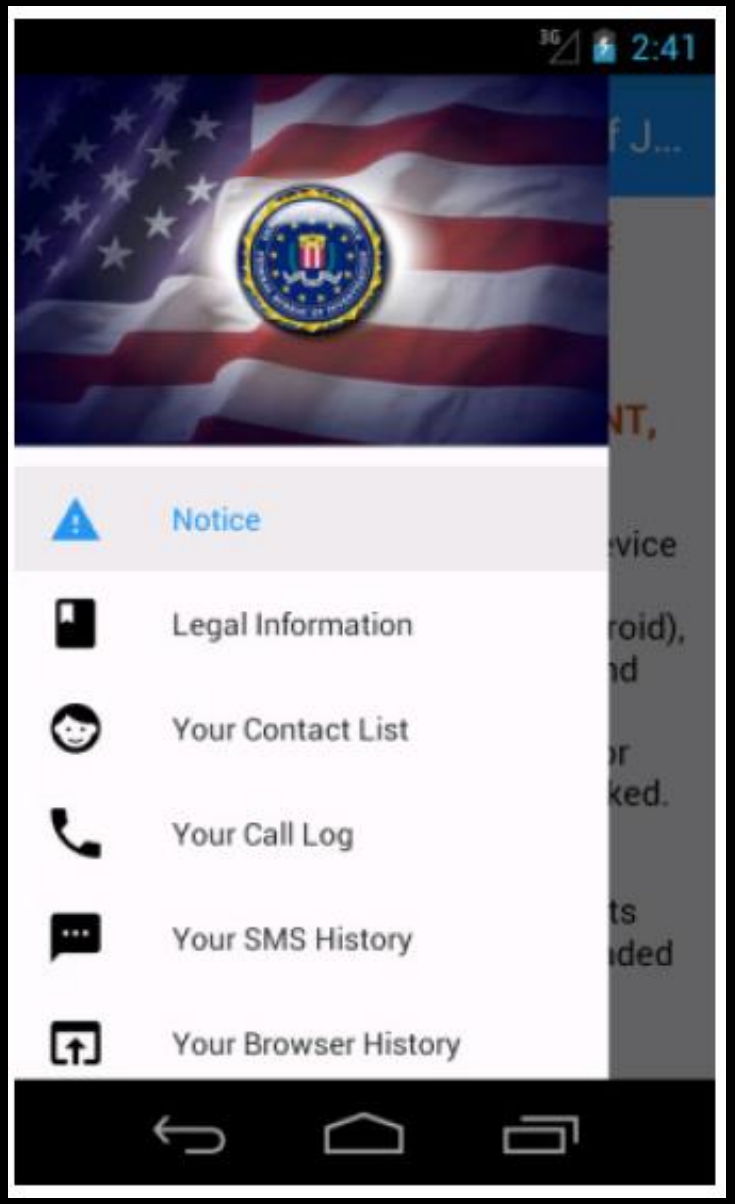
Android.Sumzand

1. User received email with link to download app
2. Steals contact information
3. Sends email promoting app to all contacts

Why is Mobile Malware Developed? *…. because There is Significant Illicit Money Being Made*

Ransomware Goes Mobile

- *Imagine the frustration of a user who downloads a cool new app to their phone only to find the device locked with an FBI warning on the home screen when they try to log in.*
- *They have two options: pay a 'fine' and hope that the attackers unlock the phone or give up access to precious photos, contacts, and memories.*



Why is Mobile Malware Developed?

…. because There is Significant Illicit Money Being Made

Malware, Grayware, Madware

App Analysis by Symantec's Norton Mobile Insight

- *Symantec analyzed 71 percent more apps in 2015 and more than three times as many (230 percent) more were classified as malicious. A 30 percent rise in grayware was owing in large part to a 77 percent rise in apps containing unwanted madware.*

	2013	2014	2015
Total Apps Analyzed	6.1 Million	6.3 Million	10.8 Million
Total Apps Classified as Malware	0.7 Million	1.1 Million	3.3 Million
Total Apps Classified as Grayware	2.2 Million	2.3 Million	3.0 Million
Total Grayware Further Classified as Madware	1.2 Million	1.3 Million	2.3 Million
Malware Definition	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.		
Grayware Definition	Programs that do not contain viruses and that are not obviously malicious, but that can be annoying or even harmful to the user, (for example, hacking tools, accessware, spyware, adware, dialers, and joke programs).		
Madware Definition	Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.		

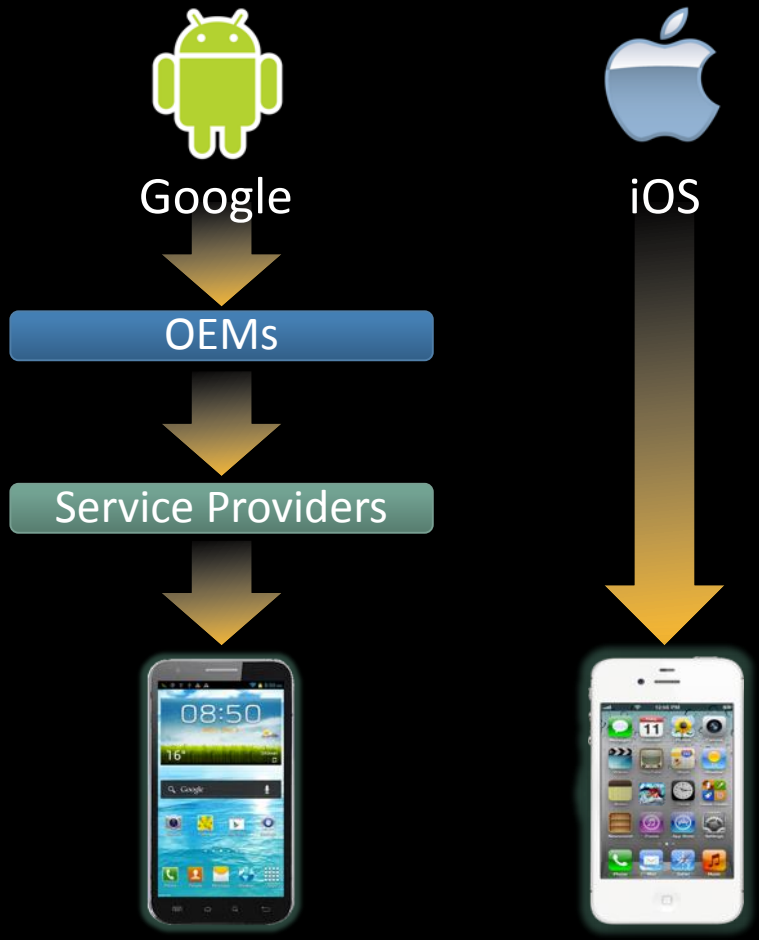
Why is Mobile Malware Developed?

…. because There is Significant Illicit Money Being Made

IoT (Internet of Things)

… Lastly, What Can be Done About It?

Vulnerability Patching



… What Can be Done About It? (Continued)

Fig 1. Google Android

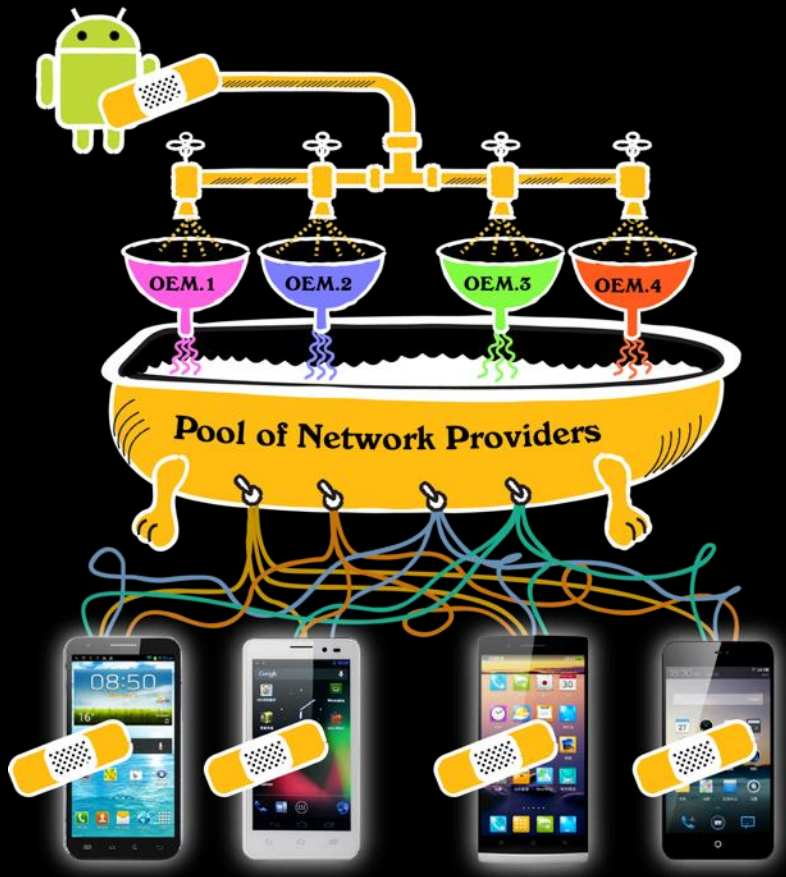
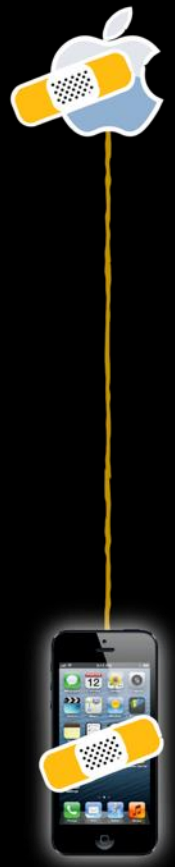


Fig 2. Apple iOS



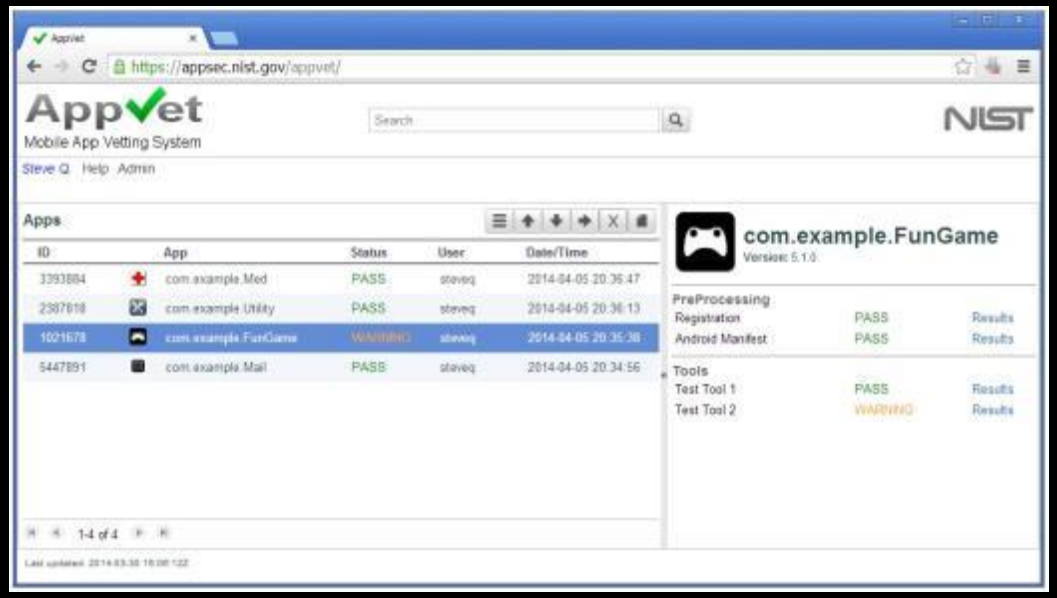
… What Can be Done About It? (Continued)

NIST Special Publication 800-163 "Technical Considerations for Vetting 3rd Party Mobile Applications" (NIST Guideline)
Allows Federal agencies to assess the following for any given mobile app:

- Security
- Behavior
- Reliability
- Performance

AppVet:
In conjunction with DARPA, NIST developed the AppVet program:

- Allows Feds to submit an app for testing
- Uses open source and commercially available tools



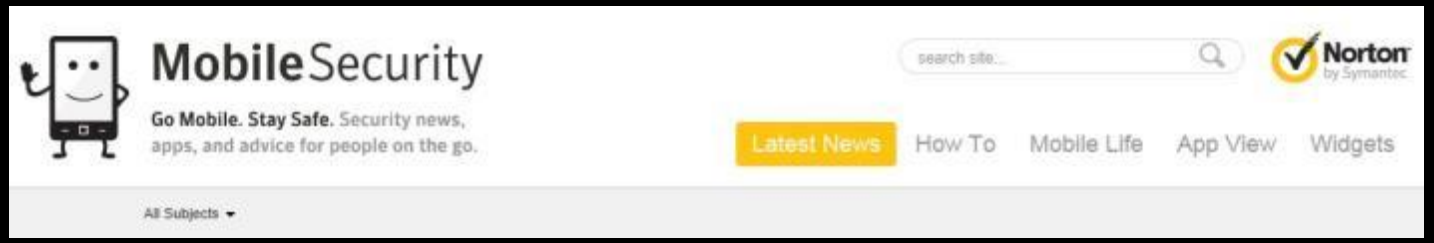
… What Can be Done About It? (Continued)

Enforce User Mobile Security Training: Users must be constantly reminded to avoid clicking on suspicious links in messages, to keep their personal mobile devices updated, and to only download apps from officially sanctioned App Stores.

Deploy Mobile Security Software Throughout Your Organization: At a minimum, this software should scan and identify threats from any mobile apps or content that the user downloads.

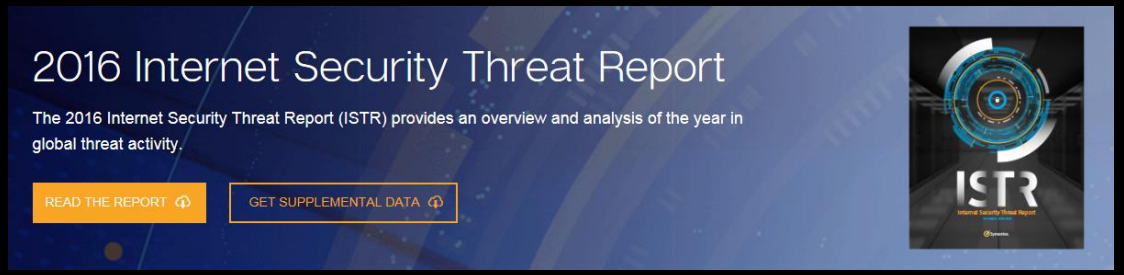
Establish a Robust, Highly Secure Mobile Device Management Framework for Your Agency: Managing your organization's mobile devices is not just about remote wipe commands for lost/stolen devices and OTA password resets. You should also setup a system for mobile app management across the entire app lifecycle. Likewise, you should manage your organization's mobile content ecosystem in the same secure end-to-end manner.

mobilesecurity.com/



Thank you!

symantec.com/threatreport



Kevin McPeak

kevin_mcpeak@symantec.com

@kevin_mcpeak