Mobile Apps:
The good, the bad, the ugly

Artem Kazantsev
security@duke.edu
http://security.duke.edu
@DukeITSO

Quick Demo first.... (USSD / MMI code vulnerability for Android phones)

http://securitywatch.pcmag.com/none/303097-dirty-ussd-hack-wipes-samsung-phones-is-yours-vulnerable

Threats Unique to the Mobile devices:

- Mobile devices = easy to steal, easy to lose

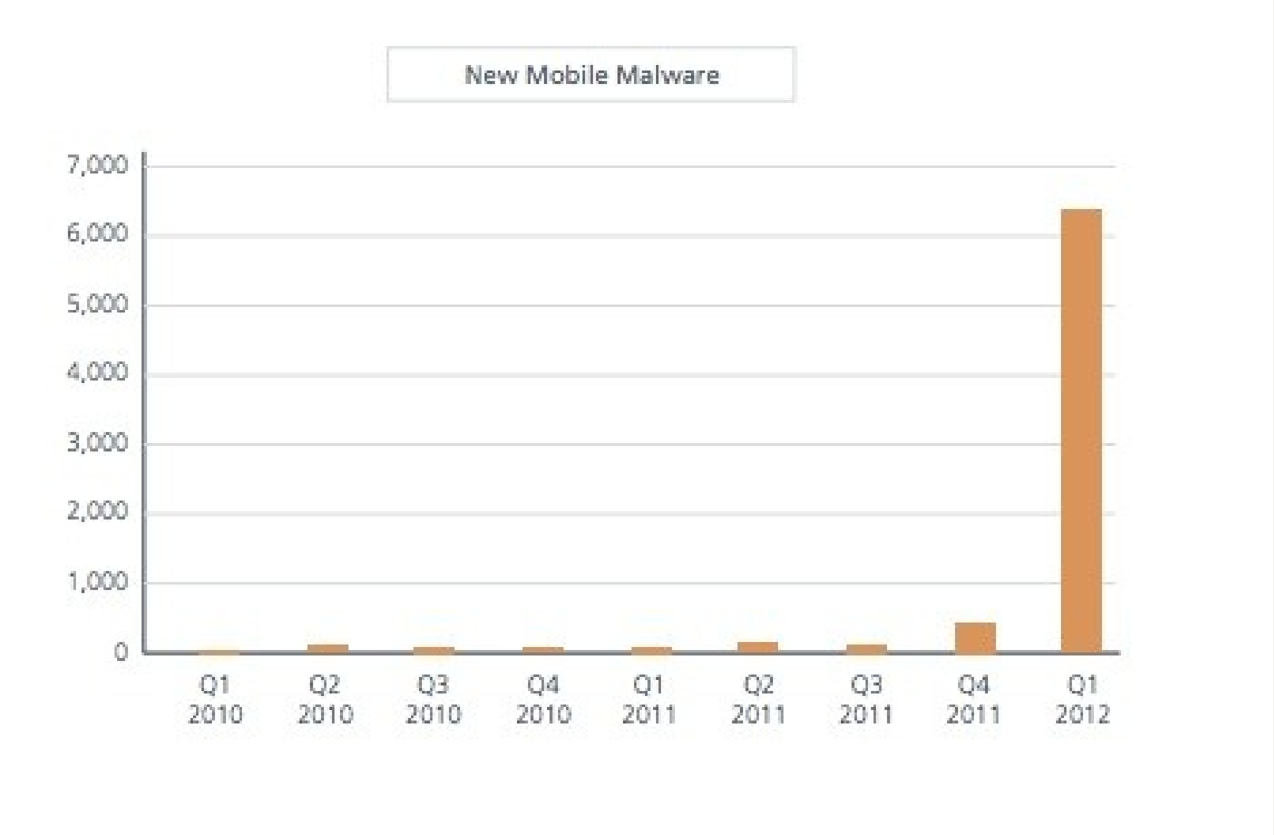
113 cell phones are lost or stolen every minute in the U.S.
56% of us misplace our cell phone or laptop each month
(http://www.micro-trax.com/statistics/)

- New ecosystem = no tradition of security

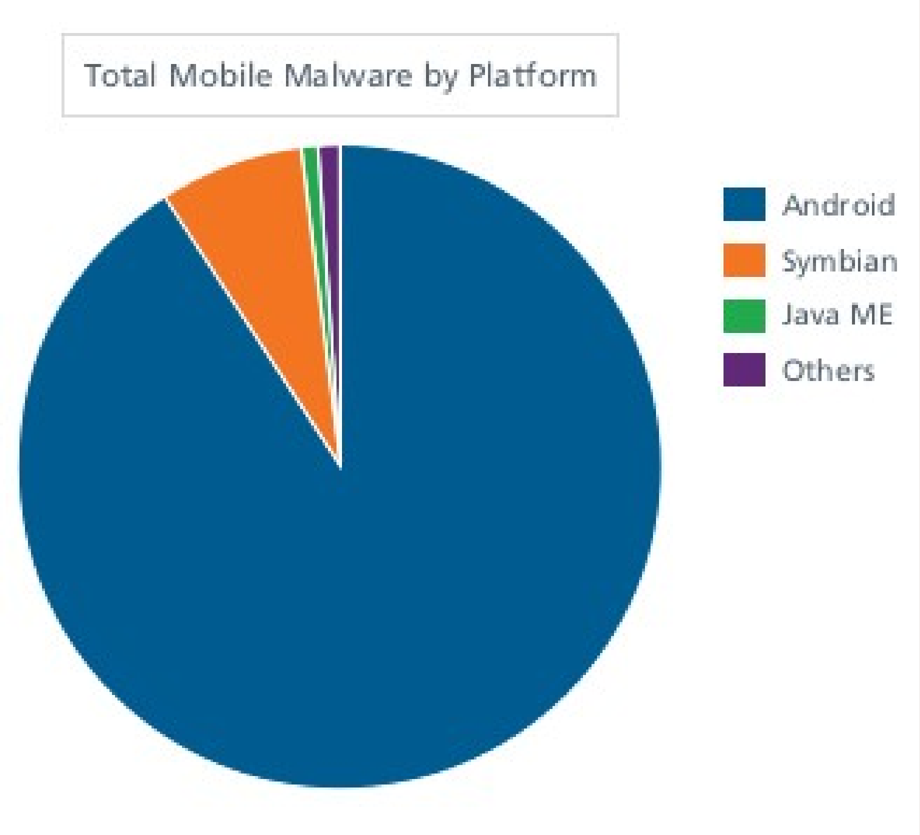
- Life cycle ~ 2 years = vendors are not issuing upgrades

- GPS, camera, multiple network options = new attack surface, more ways to steal data

McAfee Threats Report: Second Quarter 2012



McAfee Threats Report: Second Quarter 2012



Are Android antimalware programs effective?

AV-Test:

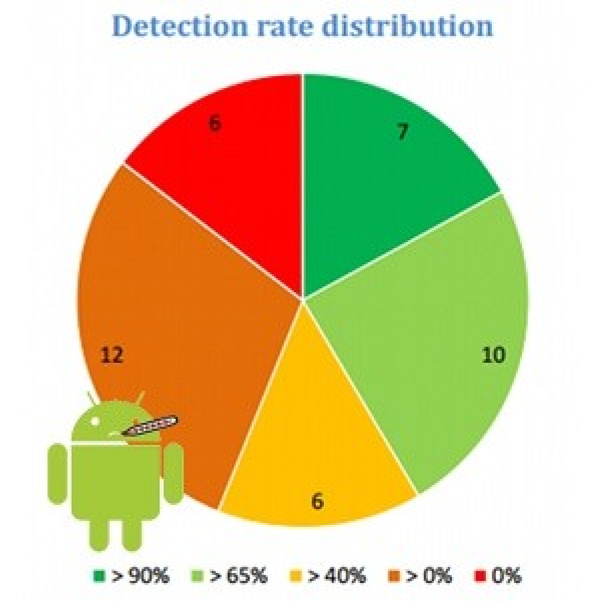
“*During February and March 2012 we reviewed 41 different Android Anti-Malware solutions. ...*

The best products in our tests (with detection rates of 90% and above) come from the following top 10 companies, listed in alphabetic order: Avast, Dr. Web, F-Secure, Ikarus, Kaspersky, Lookout, McAfee, MYAndroid Protection, NQ Mobile and Zoner.”

http://www.av-test.org/fileadmin/pdf/avtest_2012-02_android_anti-malware_report_english.pdf

Are Android antimalware programs effective?

- http://www.makeuseof.com/tag/study-suggests-android-antivirus-apps-effective-news/



What do the attackers want?

46 pieces of malware identified by by behavior:

Exfiltrates user information	28
Premium calls or SMS	24
Sends SMS advertisement spam	8
Novelty and amusement	6
Exfiltrates user credentials	4
Search engine optimization	1
Ransom	1

A Survey of Mobile Malware in the Wild
http://www.cs.berkeley.edu/~afelt/mobilemalware.pdf

How do we protect ourselves?

Follow these tips for securing mobile devices:

	iOS 6	Android OS 4.x
Set a passcode / screen lock	(Settings → General → Passcode Lock)	(Personal → Security → Screen Lock)
Enable encryption	Enabled once the Passcode Lock is configured	(Personal → Security → Encryption)
Set up remote wipe	1. Sign in to iCloud with your Apple ID at https://www.icloud.com 2. Choose “Find My iPhone.” 3. Choose the appropriate device. 4. Click “Erase iPhone” from the device screen. ** Requires iCloud configuration and the Find My iPhone app.*	Not all Android devices provide remote wipe capabilities by default. Check your mobile provider to see if they offer apps with this functionality. Alternatively, check the Play Store for many 3rd party remote wipe products. *Hint: check exchange.oit.duke.edu Phone / “Wipe device”*

Did you give a permission to the app to send all your contacts to Romania? :)

Android OS has 22 permissions, from access to your contacts and location to the system configuration

http://techpp.com/2010/07/30/android-apps-permissions-secure-private-data/

Discussion and questions...