

Smartphone Security Winners & Losers

CESARE GARLATI
TREND MICRO



Session ID: MBS-308

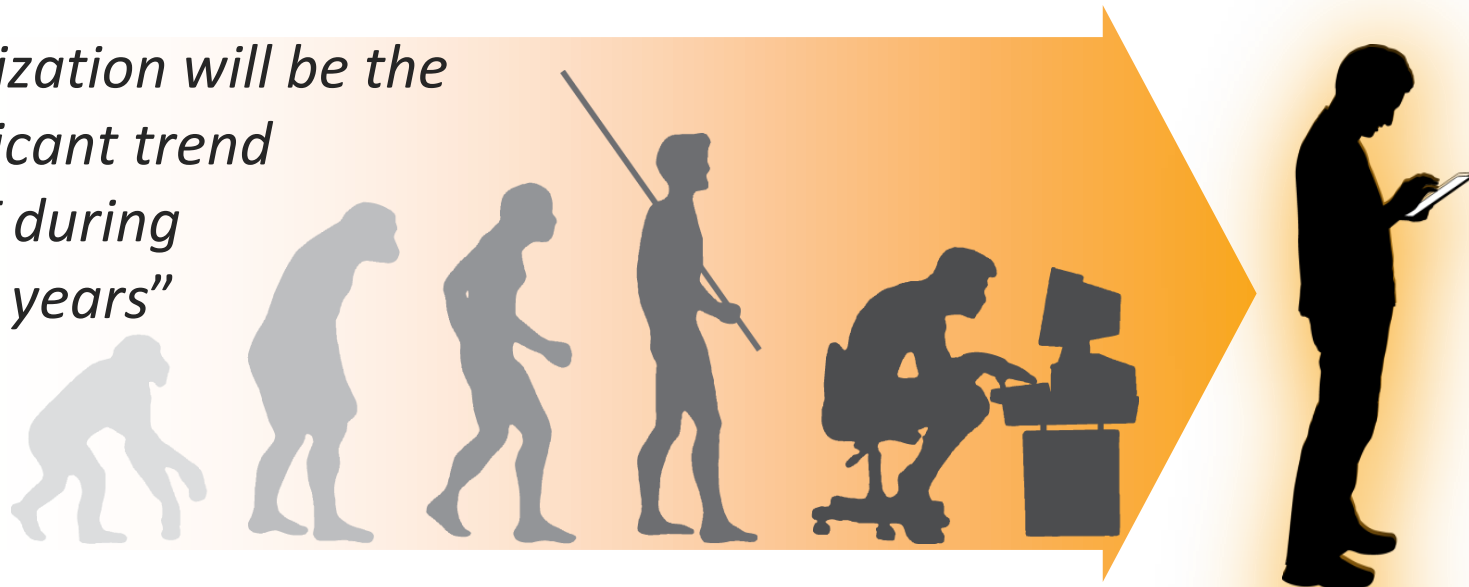
Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012

Consumerization of IT

“Consumerization will be the most significant trend affecting IT during the next 10 years”

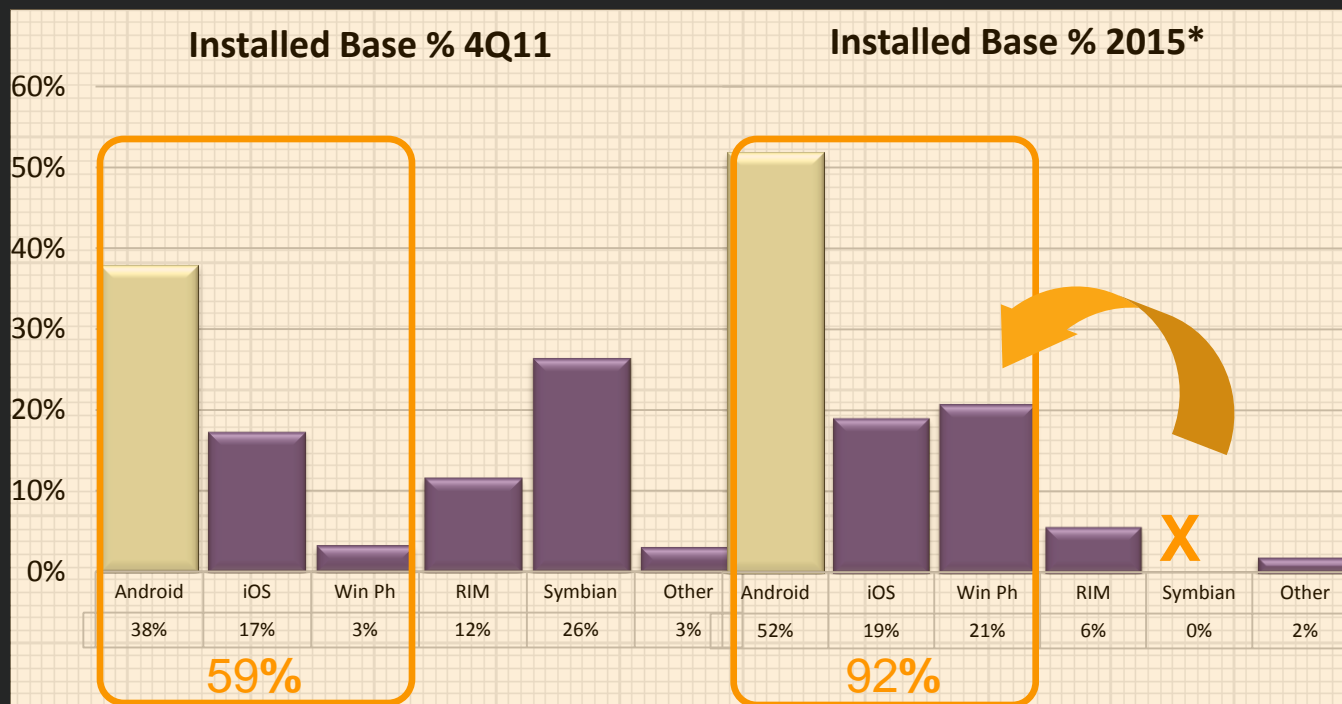
Gartner



- New technology emerges first in the consumer market and then spreads into business organizations brought in by the employees
- IT and consumer electronics converge as individuals rely on the same devices and applications for personal use and work-related activities
- Overwhelmed by the wave of consumer technology flooding the enterprise, IT managers struggle to enforce policies and maintain control

** Consumerization term first used in 2001 by D. Neal and J. Taylor of CSC's Leading Edge Forum*

The Consumerization Report



Android and iOS will account for over 70% of smartphone sales by the end of 2012. Microsoft will rise to third place in the global OS rankings by 2013, ahead of Research In Motion.

Source: Trend Micro internal analysis based on Gartner, Forrester and IDC market data – Update February, 28 2012



ConsumerizationReport[®]

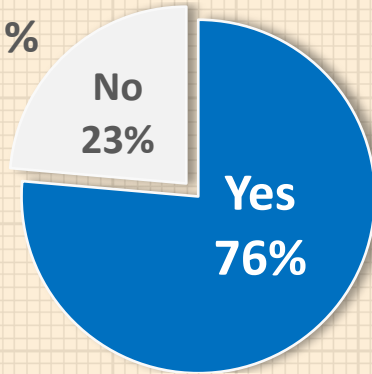


RSACONFERENCE
EUROPE 2012

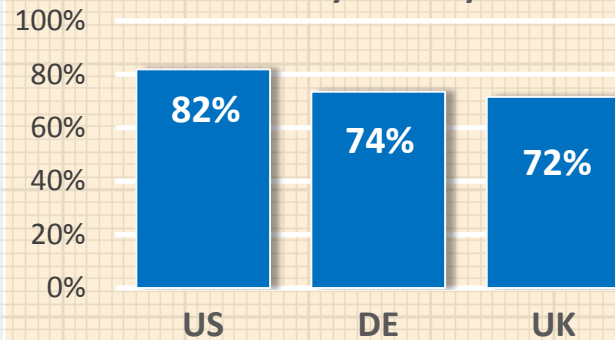


The Consumerization Report

BYOD %

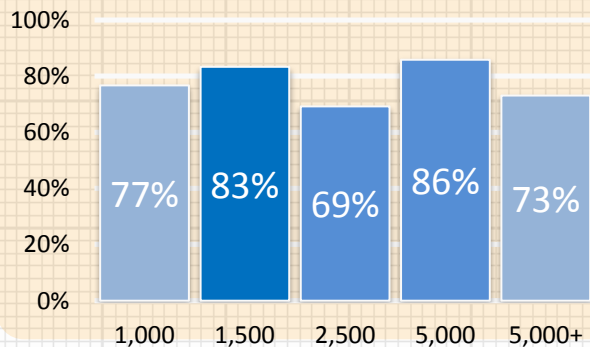


BYOD by Country

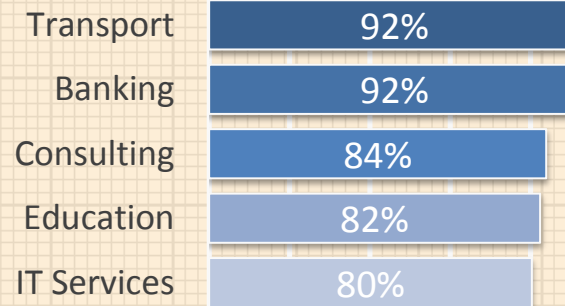


"Does your company allow employees to use their personal mobile devices for work-related activities?"

BYOD by Company Size



BYOD by Industry - Top 5

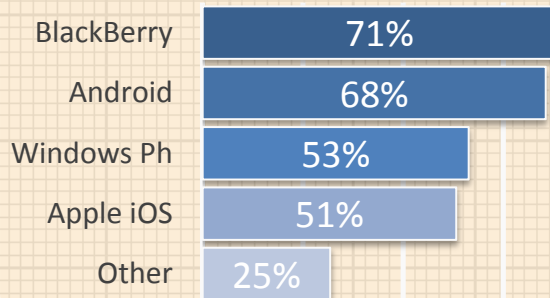


ConsumerizationReport®

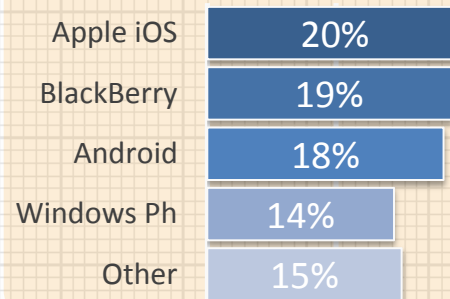


The Consumerization Report

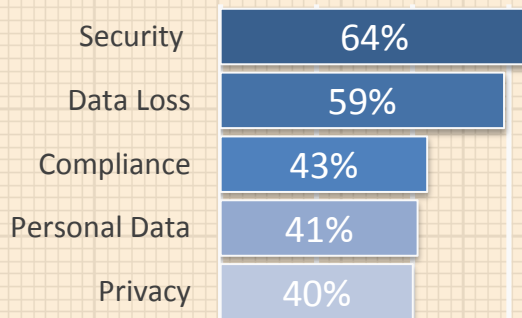
"What mobile platforms are allowed by your BYOD policy?"



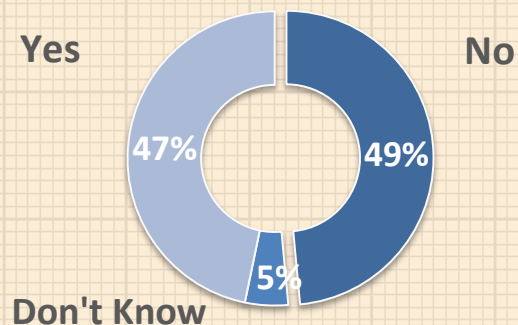
"Rank security and manageability of each mobile operating system"



BYOD Top 5 concerns



"Has your company ever experienced a security breach as result of BYOD?"



ConsumerizationReport®



RSACONFERENCE
EUROPE 2012



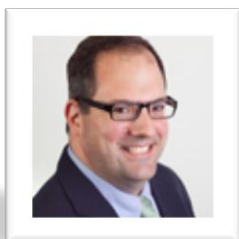
How Secure and Manageable?



Raimund Genes

Chief Technology Officer, Trend Micro

<http://trendmicro.com/our-contributors/raimund-genes>



Chris Silva

Industry Analyst, Altimeter Group

<http://www.altimetergroup.com/about/team/chris-silva>



Nigel Stanley

Practice Leader, Bloor Research

<http://www.bloorresearch.com/about/people/nigel-stanley.html>



Philippe Winthrop

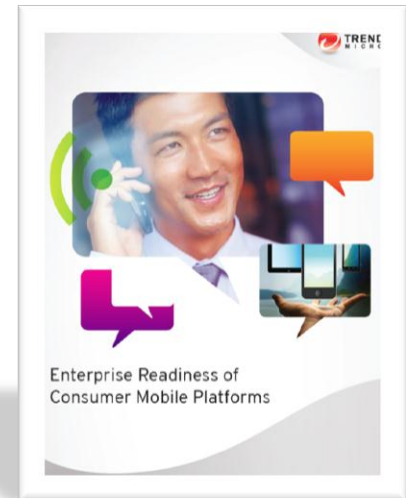
Managing Director, Enterprise Mobility Foundation

<http://www.enterprisemobilitymatters.com/about.html>



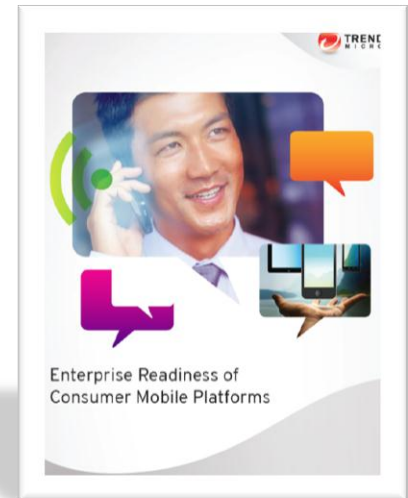
Security and Management Criteria

ID	ATTRIBUTE	BB 7.0	iOS 5	WP 7.5	ANDROID 2.3
1.00	Built-in security	3.13	3.75	3.50	2.50
1.10	Code signing	5.00	5.00	5.00	5.00
1.20	Keychain	2.50	5.00	0.00	0.00
1.30	Buffer overflow protection	2.50	2.50	4.50	2.50
1.40	Stack overflow protection	2.50	2.50	4.50	2.50
2.00	Application security	2.44	2.06	1.88	1.44
2.10	Centralized app signing	4.50	2.50	0.00	1.00
2.11	Developer app signing	4.50	2.50	4.50	1.50
2.20	Centralized application testing	3.50	2.50	4.00	1.00
2.30	User "allow" model	4.50	5.00	2.50	4.00
2.40	Anti-malware built in	2.50	4.00	4.00	2.00
2.41	Anti-malware support via open APIs	0.00	0.00	0.00	2.00
2.50	Web reputation built in	0.00	0.00	0.00	0.00
2.51	Web reputation via APIs	0.00	0.00	0.00	0.00
3.00	Authentication	3.90	2.00	3.20	2.00
3.10	Power-on authentication	2.50	2.50	4.50	2.50
3.20	Inactivity time out	5.00	2.50	4.50	2.50
3.30	SIM change	2.50	0.00	0.00	0.00
3.40	Password strength requirements	5.00	2.50	4.50	2.50
3.50	Protection from too many log in attempts	4.50	2.50	2.50	2.50



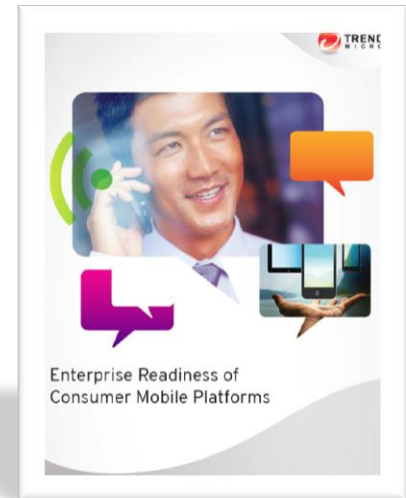
Security and Management Criteria

ID	ATTRIBUTE	BB 7.0	IOS 5	WP 7.5	ANDROID 2.3
4.00	Device wipe	4.00	1.25	2.25	0.63
4.10	Local wipe - after too many failed login attempts	4.50	2.50	4.50	0.00
4.20	Remote wipe - over IP	3.50	2.50	4.50	2.50
4.21	Remote wipe - over SMS/cellular	3.50	0.00	0.00	0.00
4.30	Selective wipe	4.50	0.00	0.00	0.00
5.00	Device firewall	4.50	0.00	0.00	0.00
5.10	Over Internet Protocol (IP)	4.00	0.00	0.00	0.00
5.20	Over Short Message Service (SMS)	5.00	0.00	0.00	0.00
6.00	Data protection	3.80	1.50	2.40	2.00
6.10	Data at rest - encryption	5.00	2.50	4.50	0.00
6.20	Data in use - file separation	0.00	2.50	2.50	2.50
6.30	Data in motion - VPN, 802.1X	5.00	2.50	5.00	5.00
6.40	Remote backup services prevention - iCloud	4.00	0.00	0.00	2.50
6.50	Removable media - SD/USB SIM	5.00	0.00	0.00	0.00
7.00	Device protection	3.50	0.63	2.38	2.00
7.10	Jail breaking/Rooting	1.50	0.00	3.00	0.00
7.20	Patching - OS/Apps	3.00	0.00	4.50	3.00
7.30	Over-the-air (OTA) updates of the OS	5.00	2.50	2.00	5.00
7.40	Block access to untrusted certificates - SSL	4.50	0.00	0.00	0.00

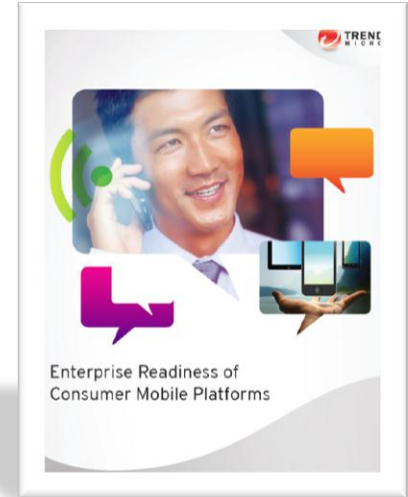
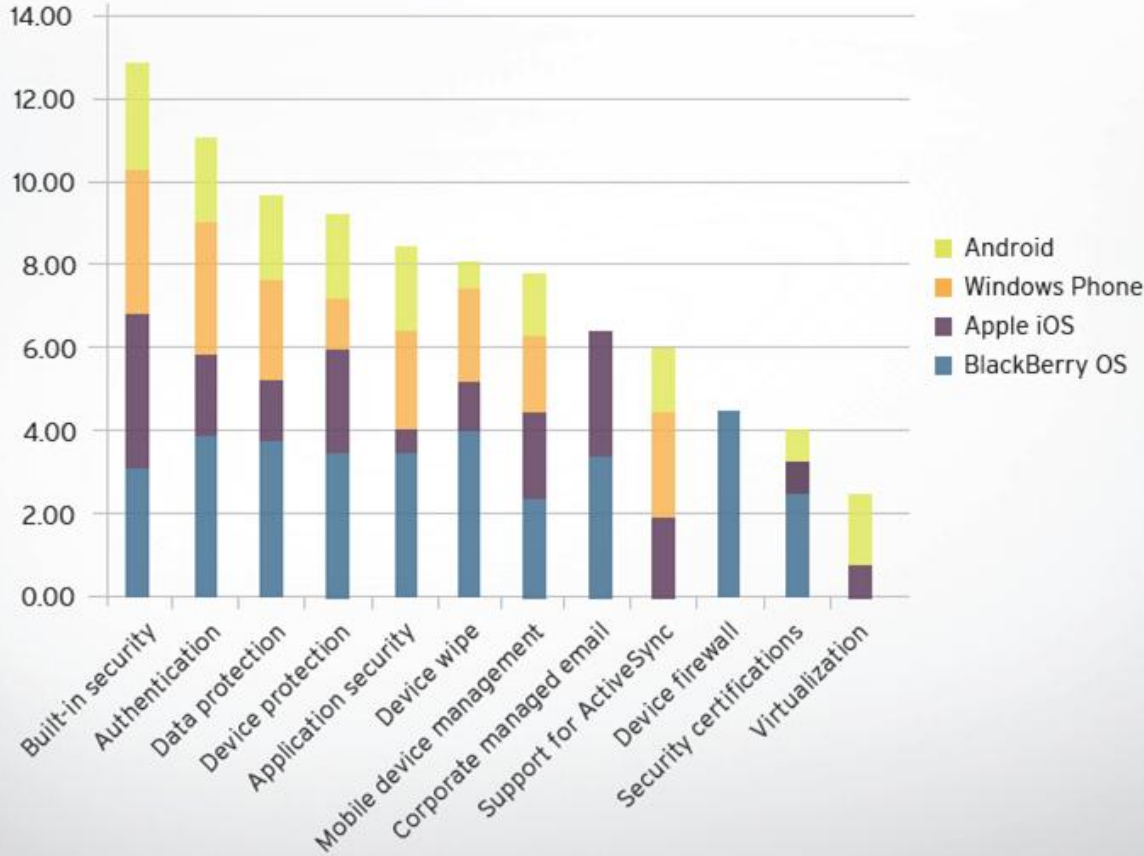


Security and Management Criteria

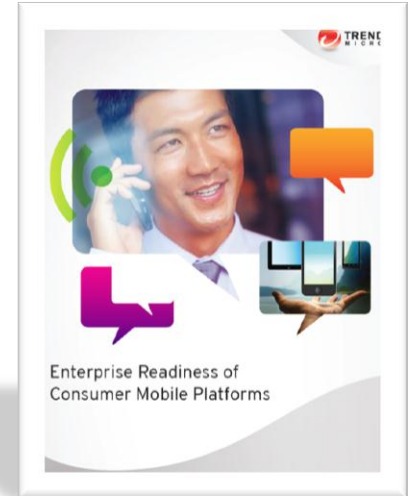
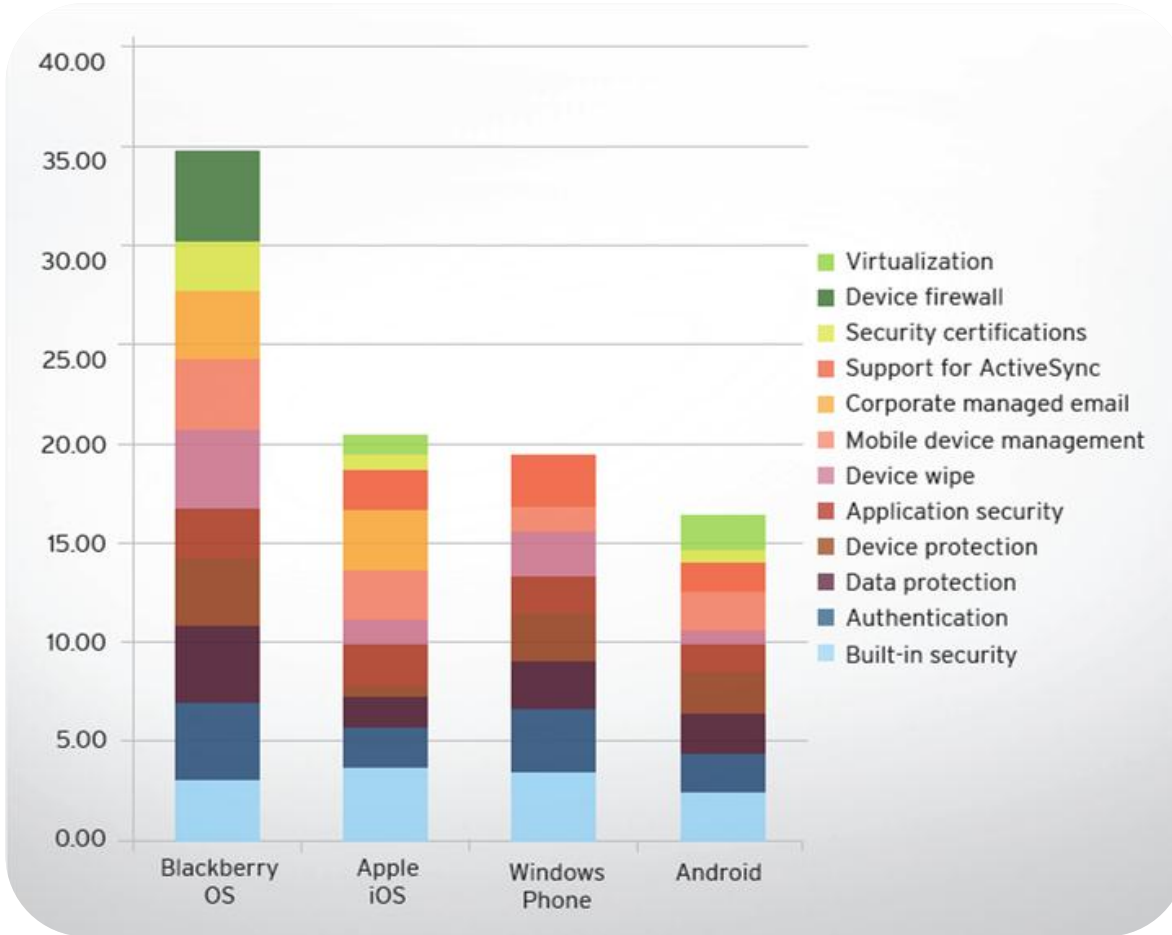
ID	ATTRIBUTE	BB 7.0	IOS 5	WP 7.5	ANDROID 2.3
8.00	Corporate managed email	3.42	3.00	0.00	0.00
8.10	Remote account removal	2.50	3.00	0.00	0.00
8.20	Email forwarding prevention	4.50	3.00	0.00	0.00
8.30	Cross-in-box email move prevention	0.00	3.00	0.00	0.00
8.40	Applications use preclusion	4.50	3.00	0.00	0.00
8.50	Cut and paste preclusion	4.50	3.00	0.00	0.00
8.60	S/MIME email authentication and encryption	4.50	3.00	0.00	0.00
9.00	Support for ActiveSync	0.00	2.00	2.50	1.50
9.10	Number of policies supported - latest ActiveSync	0.00	2.00	2.50	1.50
9.20	Number of policies supported - legacy ActiveSync	0.00	2.00	2.50	1.50
10.00	Mobile device management	3.50	2.50	1.25	2.00
10.10	Richness of the API	2.00	2.50	0.00	1.50
10.20	Vendor-provided server	5.00	2.50	2.50	2.50
11.00	Virtualization	0.00	0.83	0.00	1.67
11.10	Virtual native OS	0.00	2.50	0.00	0.00
11.20	Virtual native apps	0.00	0.00	0.00	5.00
11.30	Split-user profile	0.00	0.00	0.00	0.00
12.00	Security Certifications	2.50	0.83	0.00	0.67
12.10	Federal Information Processing Standard (FIPS) 140-2	2.50	2.50	0.00	2.00
12.20	Evaluation Assurance Level (EAL) 4	5.00	0.00	0.00	0.00
12.30	FDA approval	0.00	0.00	0.00	0.00
OS Average Score		2.89	1.70	1.61	1.37



Ratings By Category



Ratings By Mobile Platform



Some recent vulnerabilities

Android

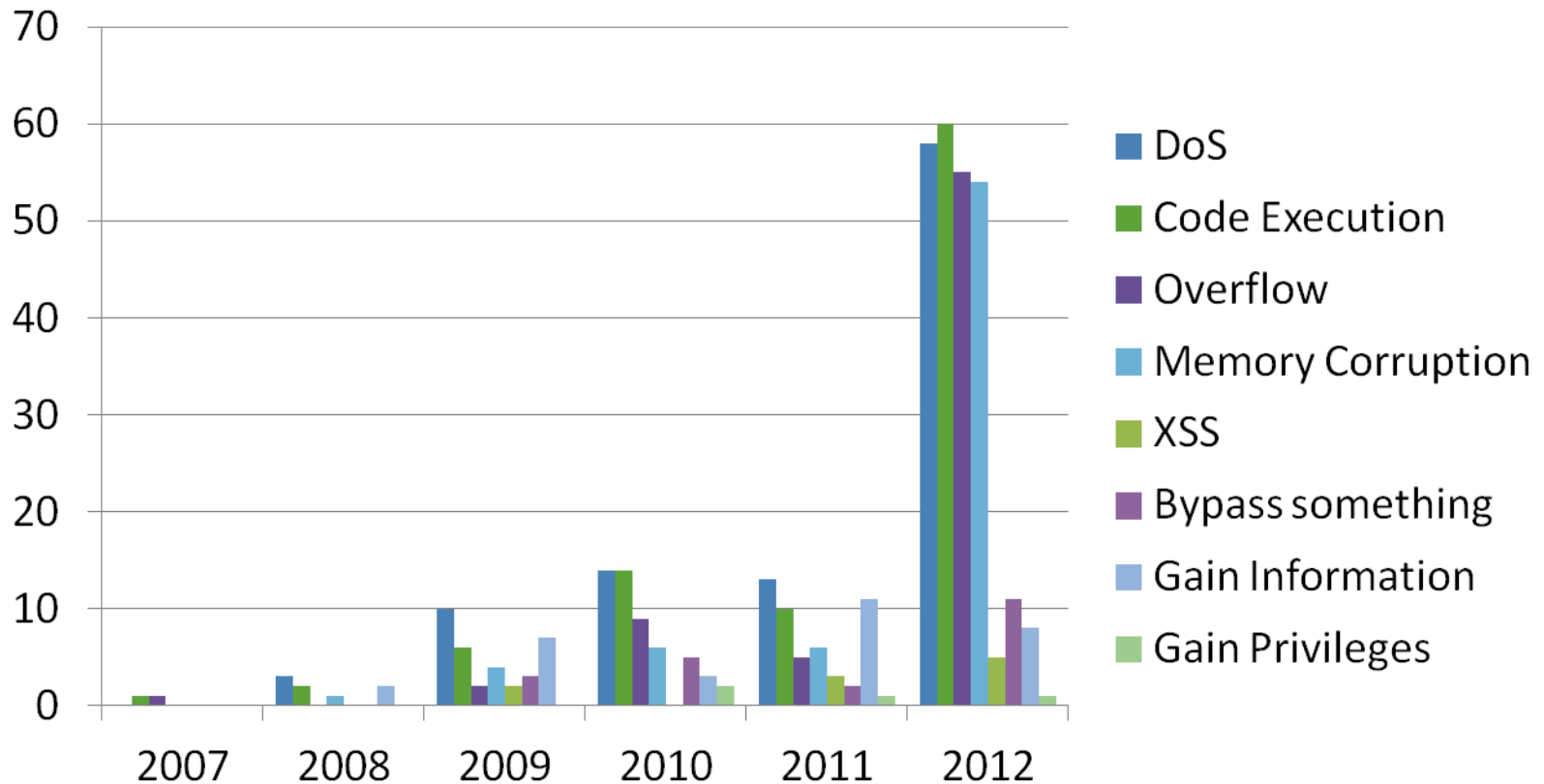
- **6.8** CVE-2012-3979 – log_print function, allowing remote attackers to execute arbitrary code via a crafted web page that calls the JavaScript dump function.
- **9.3** CVE-2011-3874 – Stack-based buffer overflow in libsysutils allows user-assisted remote attackers to execute arbitrary code via an application call.
- **4.3** CVE-2011-4276 – Bluetooth service allows remote attackers within range to obtain contact data via an AT phonebook transfer.

Apple iOS

- **9.3** CVE-2012-0643 – Malicious code allows remote attackers to bypass sandbox restrictions and execute arbitrary code.
- **9.3** CVE-2012-0646 – Format string vulnerability in VPN allows remote attackers to execute arbitrary code via a crafted racoon configuration file.
- **9.3** CVE-2012-0642 – Integer underflow allows remote attackers to execute arbitrary code via a crafted catalog file in an HFS disk image.



No Platform is immune: Apple iOS Detail



Source: National Vulnerability Database via CVEDetails.com – as of October 4, 2012

Apple iOS Jailbreaking Trends

Trends

Web Search Interest: **iphone jailbreak**. Worldwide, 2007-2012.



Explore trends

Hot searches

Search terms

iphone jailbre:

+ Add term

▶ Other comparisons

Limit to

Web Search

Worldwide

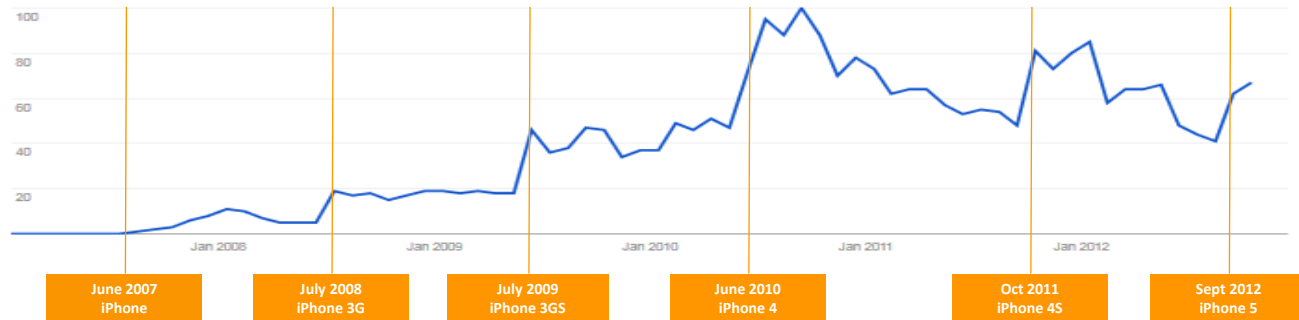
January 2007
- December
2012

All Categories

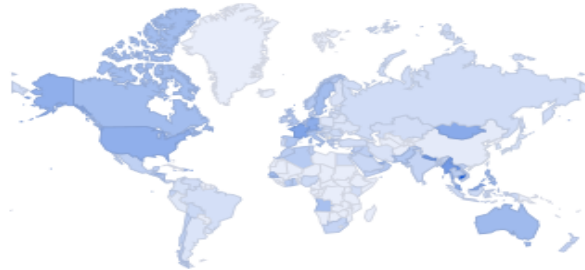
Interest over time

The number 100 represents the peak search volume

News headlines Forecast



Regional interest



0 100

▶ View change over time

Region | City

Regional interest



Region | City



Apple iOS Jailbreaking Trends - UK

Trends

Web Search Interest: **iphone jailbreak**. United Kingdom, 2007-2012.



Explore trends

Hot searches

Search terms

iphone jailbre:

+ Add term

▶ Other comparisons

Limit to

Web Search ▶

United Kingdom ▶

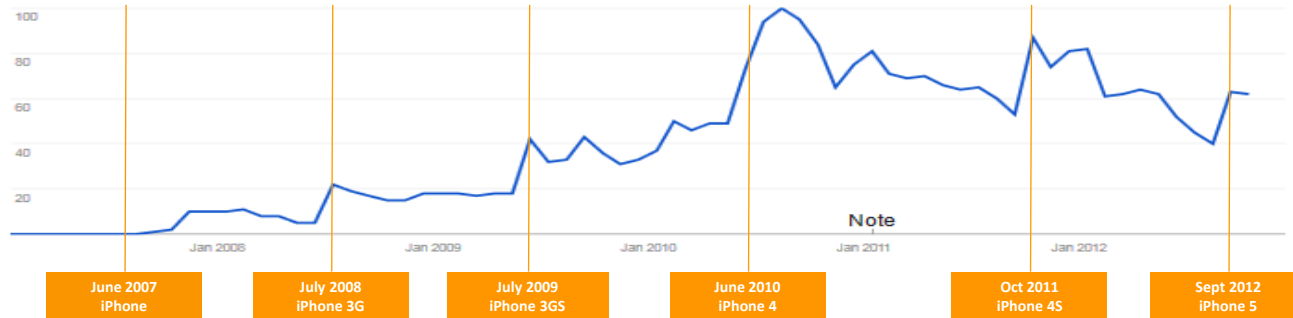
January 2007 - December 2012 ▶

All Categories ▶

Interest over time

The number 100 represents the peak search volume

News headlines Forecast



Regional interest

Worldwide > United Kingdom



0 100

▶ View change over time

Subregion | City

Regional interest

Leicester	100	
Lambeth	91	
Poplar	86	
Kensington	86	
Nottingham	80	
London	77	
Glasgow	75	
Leeds	75	
Liverpool	72	
Birmingham	69	

Subregion | City



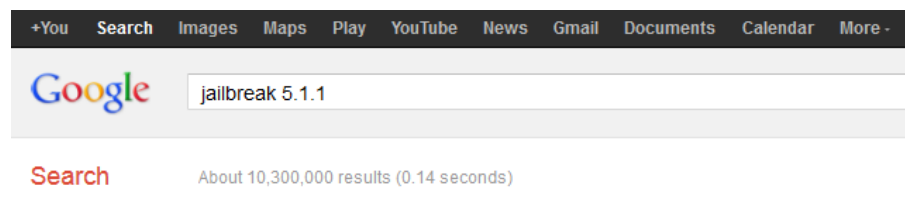
How To: Jailbreak iOS (5.1.1)

Download Links

Xxxx v2.0.4 MacOSX (10.5, 10.6, 10.7)

Xxxx v2.0.4 Windows (XP/Vista/Win7)

Xxxx v2.0.4 Linux (x86/x86_64)



How To Use Xxxxx 2.0:

1. Make a backup of your device in iTunes by right clicking on your device name under the 'Devices' menu and click 'Back Up'.
2. Open Xxxxx and be sure you are still connected via USB cable to your computer.
3. Click 'Jailbreak' and wait.... just be patient and do not disconnect your device.
4. Once jailbroken return to iTunes and restore your backup from earlier.

Xxxxx 2.0 supports the following devices on 5.1.1:

iPad 1, iPad 2, iPad 3 (iPad2,4 is now supported as of Xxxxx 2.0.4)

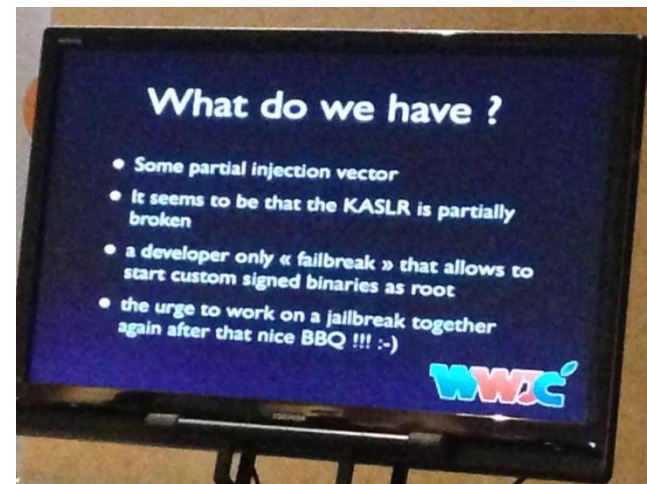
iPhone 3GS, iPhone 4, iPhone 4S

iPod touch 3rd generation, iPod touch 4th generation

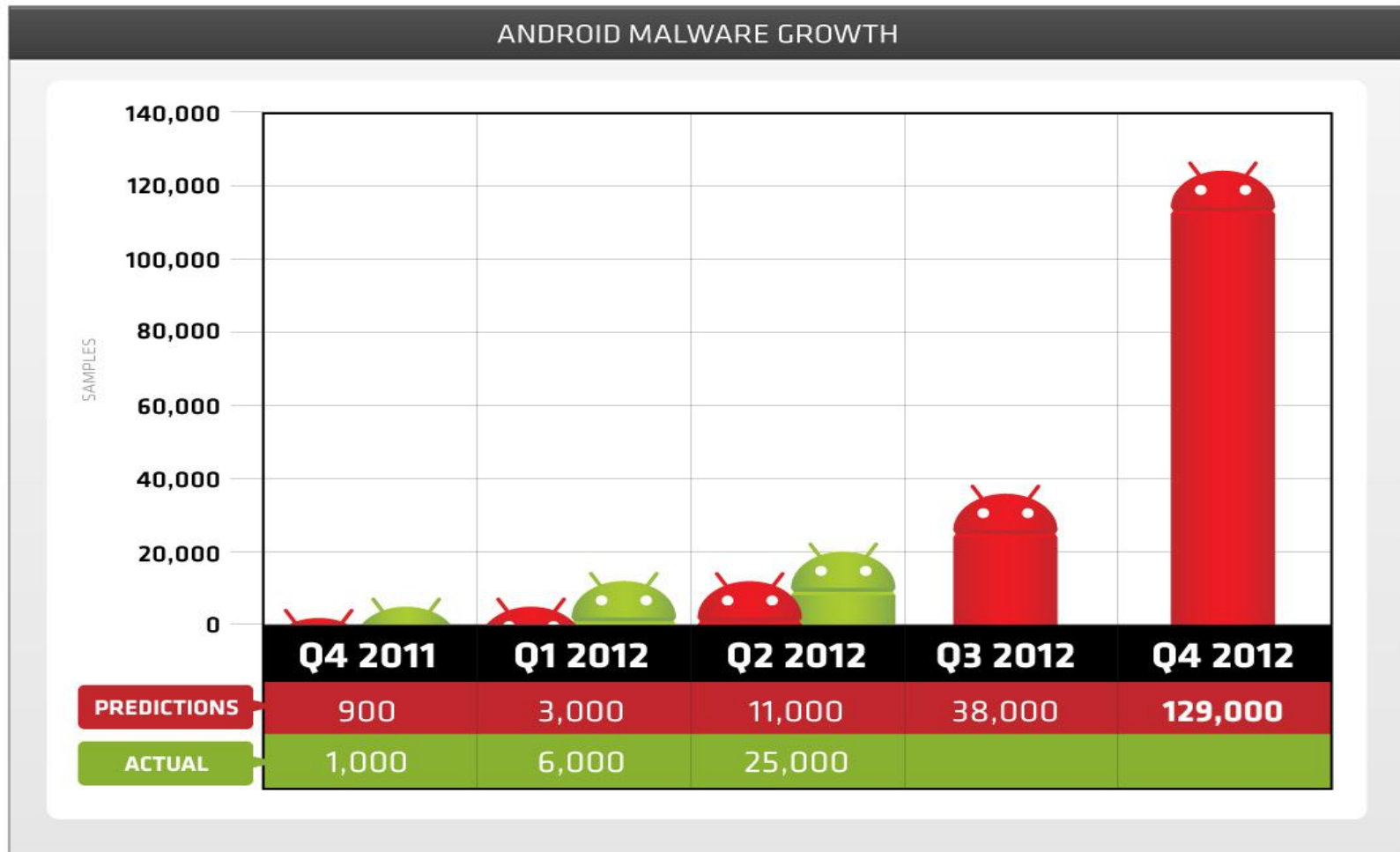
Taller screens like Cydia too. :)



- @saurik – Jay Freeman
- Cydia: 1.5M Apps per day
- 5% to 10% of Apple iOS devices
- \$8M revenues 2011 (developers)



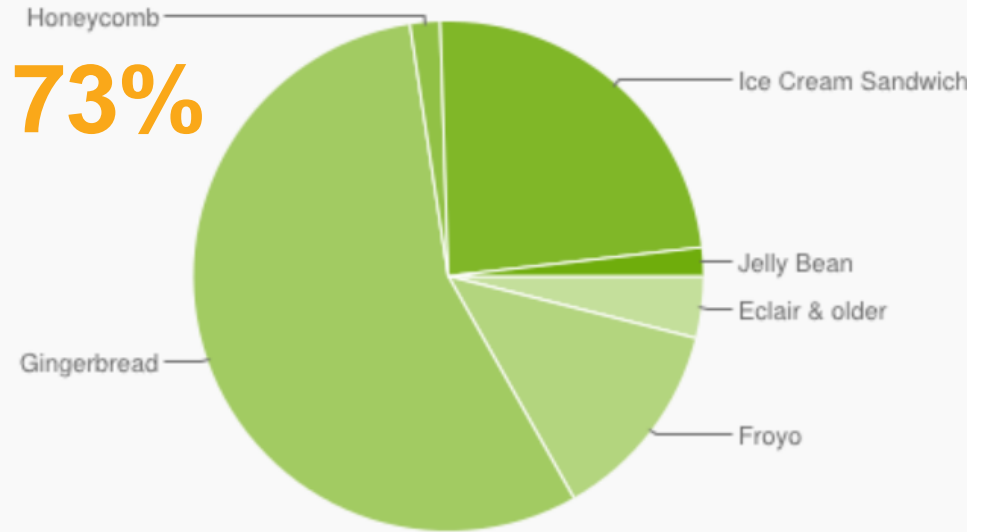
Android is where the action is



Source: Trend Labs, Trend Micro Inc. – as of Q2 2012

Android Versions Distribution

Version	Codename	API	Distribution
1.5	Cupcake	3	0.1%
1.6	Donut	4	0.4%
2.1	Eclair	7	3.4%
2.2	Froyo	8	12.9%
2.3 - 2.3.2	Gingerbread	9	0.3%
2.3.3 - 2.3.7		10	55.5%
3.1	Honeycomb	12	0.4%
3.2		13	1.5%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	23.7%
4.1	Jelly Bean	16	1.8%



Fragmentation



Vulnerable Devices

Data collected during a 14-day period ending on October 1, 2012

Source: Google <http://developer.android.com/resources/dashboard/platform-versions> – as of August 1, 2012

Malicious Apps on Legit Marketplace

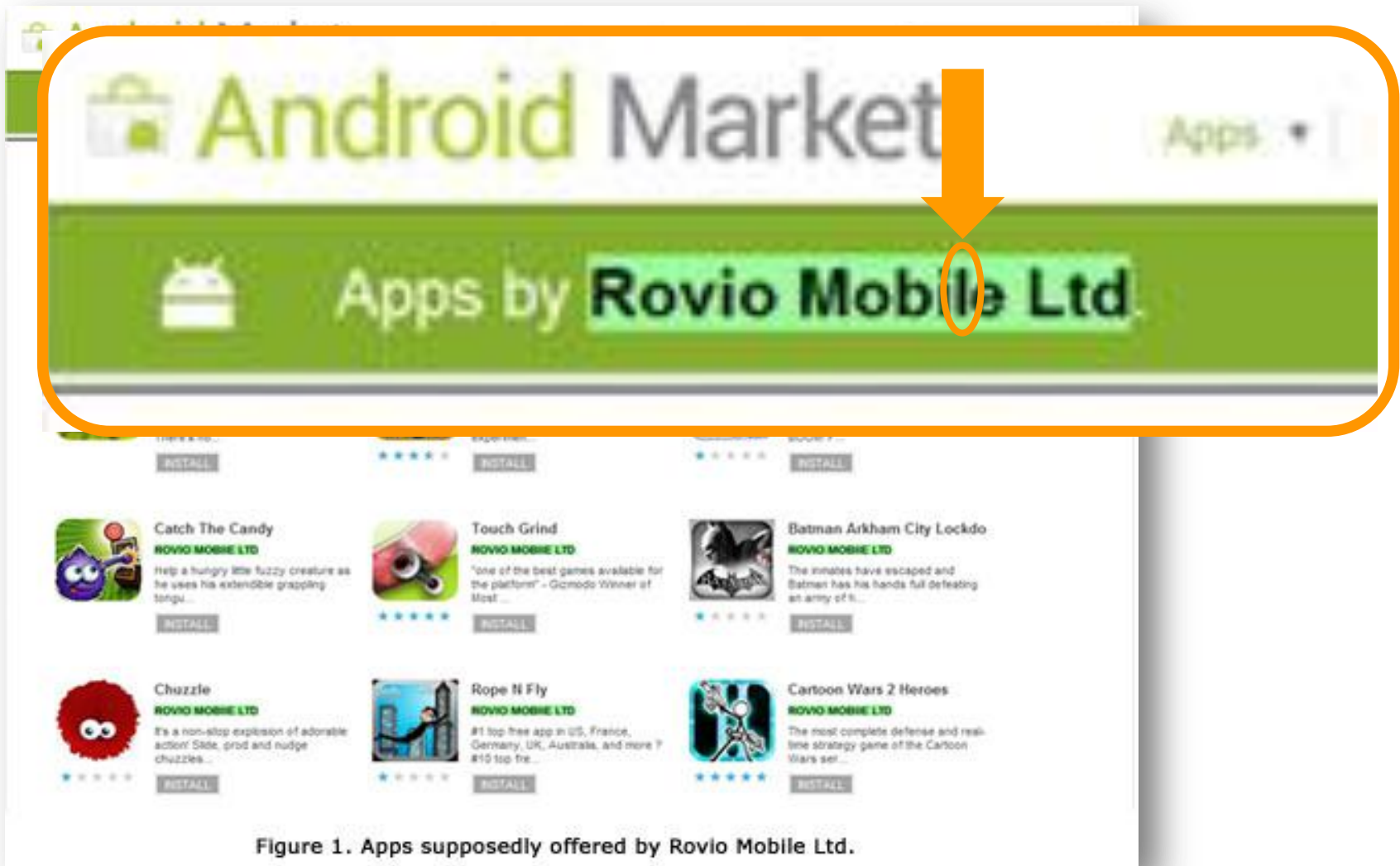


Figure 1. Apps supposedly offered by Rovio Mobile Ltd.

Malicious Apps on Legit Marketplace

The screenshot shows a web browser displaying a blog post from Trend Micro's Malware Blog. The page has a red header with the Trend Micro logo and the text 'MALWARE BLOG Threat News and Information Direct from the Experts'. Below the header is a navigation menu with categories like 'Bad Sites', 'Botnets', 'Data', 'Exploits', 'Hacked Sites', 'Mac', 'Malware', 'Mobile', 'Olympics', 'Social Media', 'Spam', 'Targeted Attacks', and 'Vulnerabilities'. The main content area features the article title '17 Bad Mobile Apps Still Up, 700,000+ Downloads So Far' dated May 3, 2:53 pm (UTC-7), by Bob Pan (Mobile Security Engineer). Below the title are social sharing buttons for Facebook, Twitter, and Google+, along with a 'Recommend' button showing 97 recommendations. The article text discusses the discovery of 17 malicious mobile apps still available on Google Play, mentioning 'AirPush' and 'Plankton' malware. A table lists the details of these apps, including their names, package names, developers, and brief behavior descriptions. On the right side of the page, there are social media icons for Facebook, Twitter, RSS, and YouTube, a search bar, and a section titled 'Emerging Mobile Threats' with a list of five items.

TrendLabs

MALWARE BLOG

Threat News and Information Direct from the Experts

Bad Sites Botnets Data Exploits Hacked Sites Mac Malware Mobile Olympics Social Media Spam Targeted Attacks Vulnerabilities

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

May 3 2:53 pm (UTC-7) | by **Bob Pan (Mobile Security Engineer)**

Share Recommend 97 Tweet 76 +1 22

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

Emerging Mobile Threats

- Trend Micro Fix Tool for Malicious Library File Found on 48 Utility Apps
- Library File in Certain Android Apps Connects to C&C Servers
- Are You Protecting the Data Packets in Your Pocket?
- ZTE Score M Scores a Backdoor Vulnerability
- Beta Version of Spyttool App for Android Steals SMS Messages




Android Spy Apps




Figure 3. Screenshot of a web site that tracks devices


3D Porsche Sports Car HD Live Wallpapers




★★★★★ (83)
Free



PicSpeed HD Wallpapers 3...
SRSDEV
★★★★★ (168,528)
Free




Car Sound Effects Ringtones
SANCRON SOUND EFFECTS & ...
★★★★★ (787)
Free



Car Audi Locus
DEVELOPDROID
★★★★★ (460)
Free

Users who installed this also installed



Supercars Lite Live-Wallpa...
CLEAVER
★★★★★ (177)
Free

NETWORK COMMUNICATION

FULL INTERNET ACCESS

Allows the app to create network sockets.

YOUR PERSONAL INFORMATION

READ SENSITIVE LOG DATA

Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the tablet, potentially including personal or private information. Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.

PHONE CALLS

READ PHONE STATE AND IDENTITY

Allows the app to access the phone features of the device. An app with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.

STORAGE


MODIFY/DELETE USB STORAGE CONTENTS MODIFY/DELETE SD CARD CONTENTS

Allows the app to write to the USB storage. Allows the app to write to the SD card.

SYSTEM TOOLS

PREVENT TABLET FROM SLEEPING PREVENT PHONE FROM SLEEPING

Allows the app to prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.

 Hide

YOUR LOCATION

ACCESS EXTRA LOCATION PROVIDER COMMANDS

Allows the app to access extra location provider commands. Malicious apps may use this to interfere with the operation of the GPS or other location sources.

NETWORK COMMUNICATION

VIEW NETWORK STATE

Allows the app to view the state of all networks.

SYSTEM TOOLS

AUTOMATICALLY START AT BOOT

Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the tablet and allow the app to slow down the overall tablet by always running. Allows the app to have itself



VScan:AndroidOS_ADWLeadbolt.HRY

Subject: Market On-line Virus Daily Report

Message | GooglePlayOnline.csv (14 KB) | GfanOnline.csv (57 KB) | AnzhuoOnline.csv (266 B) | NduoOnline.csv (3 KB)

Date	Virus Found	Count
2012-09-07		132
	prosche.sp	
	@ https://play	
	id=prosche.sp	
	com.colors	
	@ https://play	
	com.aniwid	
	@ https://play	
	id=com.aniwid	
	com.midni	
	@ https://play	
	id=com.midni	

GooglePlayOnline (2).csv - Microsoft Excel

Home Insert Page Layout Formulas Data Review View

A1 EF4CAB0DEEBF27729532714591F873CBD7AEA8FF

	A	B	C
1	EF4CAB0DEEBF277295327145	prosche.sport.car.live.wallpaper	VScan:AndroidOS_ADWLeadbolt.HRY
2	C09F66F6F2BD78381CB0CBCE	com.colorsplurge.android	VScan:AndroidOS_ADWLeadbolt.HRY
3	4850B0054438E4FB10BED259	com.aniwidgets.rainingbluefairy	VScan:AndroidOS_ADWLeadbolt.HRY
4	04FAFE08DDEF90068DB9CF00	com.midnitarinc.sexycleaner	VScan:AndroidOS_ADWLeadbolt.HRY
5	9379CE00734F6D888C71FB1F	com.stargalaxy.galacticlivewallpae	VScan:AndroidOS_ADWLeadbolt.HRY
6	EA86D549664F1A3ED1507FB4	com.dong.youLoveLiveWallpaper	VScan:AndroidOS_AIRPUSH.HRY
7	4248BF2BE0A8A185AAC95B75	appinventor.ai_kekzilla22.CatSour	VScan:AndroidOS_ADWLeadbolt.HRY
8	F9BBD9F211E8B52D3E185D07	mcoprod.livewallpaper.WaterRipp	VScan:AndroidOS_AIRPUSH.HRY
9	F33F84F66EC56BFABD8E0E91	it.hkitty.fans6	VScan:AndroidOS_TROJCounterclank.HRY
10	970CD0A6F3354D9E4E526B92	mcoprod.livewallpaper.WaterRipp	VScan:AndroidOS_AIRPUSH.HRY
11	1652FB465166DA8D0A6A27F4	com.aktmedia.quoteDirectory1	VScan:AndroidOS_Applovin.HRY
12	22F9D5F314D8CE65CD594365	com.cliffwork.TMhorse	VScan:AndroidOS_AIRPUSH.HRY
13	1D94D8EBF070E569A9857E77	tnt.hacks.tips.tricks3.demo	VScan:AndroidOS_AIRPUSH.HRY
14	384C6BEEF91DFD33C53BC325	com.hazkiel.golauncher.theme.jell	VScan:AndroidOS_TROJCounterclank.HRY
15	3AEDF76022F14A88414E5686	com.rotatingheartimbh.app	VScan:AndroidOS_ADWLeadbolt.HRY
16	6207A11B920518CEC2A55D13	com.TLapp.runwaycontrolLite	VScan:AndroidOS_ADWLeadbolt.HRY

GooglePlayOnline (2) | Ready | Count: 3

How to Apply What You Have Learned Today

- Consumer mobile technology is invading the enterprise and you won't be able to resist it
- Consumer technology is not as secure as manageable as required by the enterprise
- No platform is immune from attack, although some are safer than others

1

Embrace Consumerization

2

Understand the risk profile of the various platforms

3

Deploy new security and management tools



THANK YOU!

Cesare_Garlatti@TrendMicro.com

Blog: <http://BringYourOwnID.com>

Twitter: @CesareGarlatti

