RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Smartphone Security Winners & Losers

Cesare Garlati

VP Mobile Security

Trend Micro, Inc.

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

Consumerization of IT

RSA CONFERENCE CHINA 2012

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

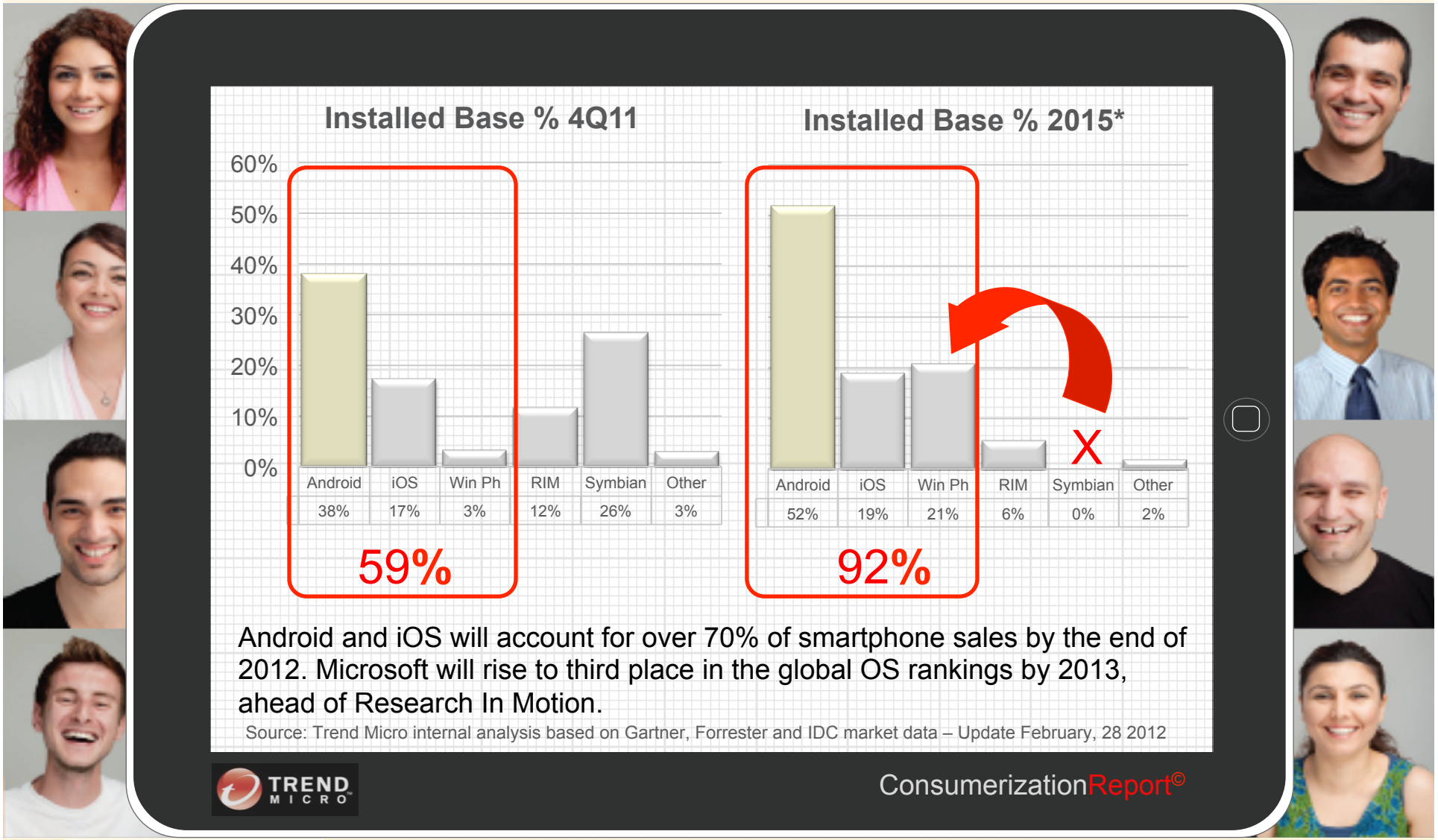
Gartner

- 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

RSA CONFERENCE CHINA 2012



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.

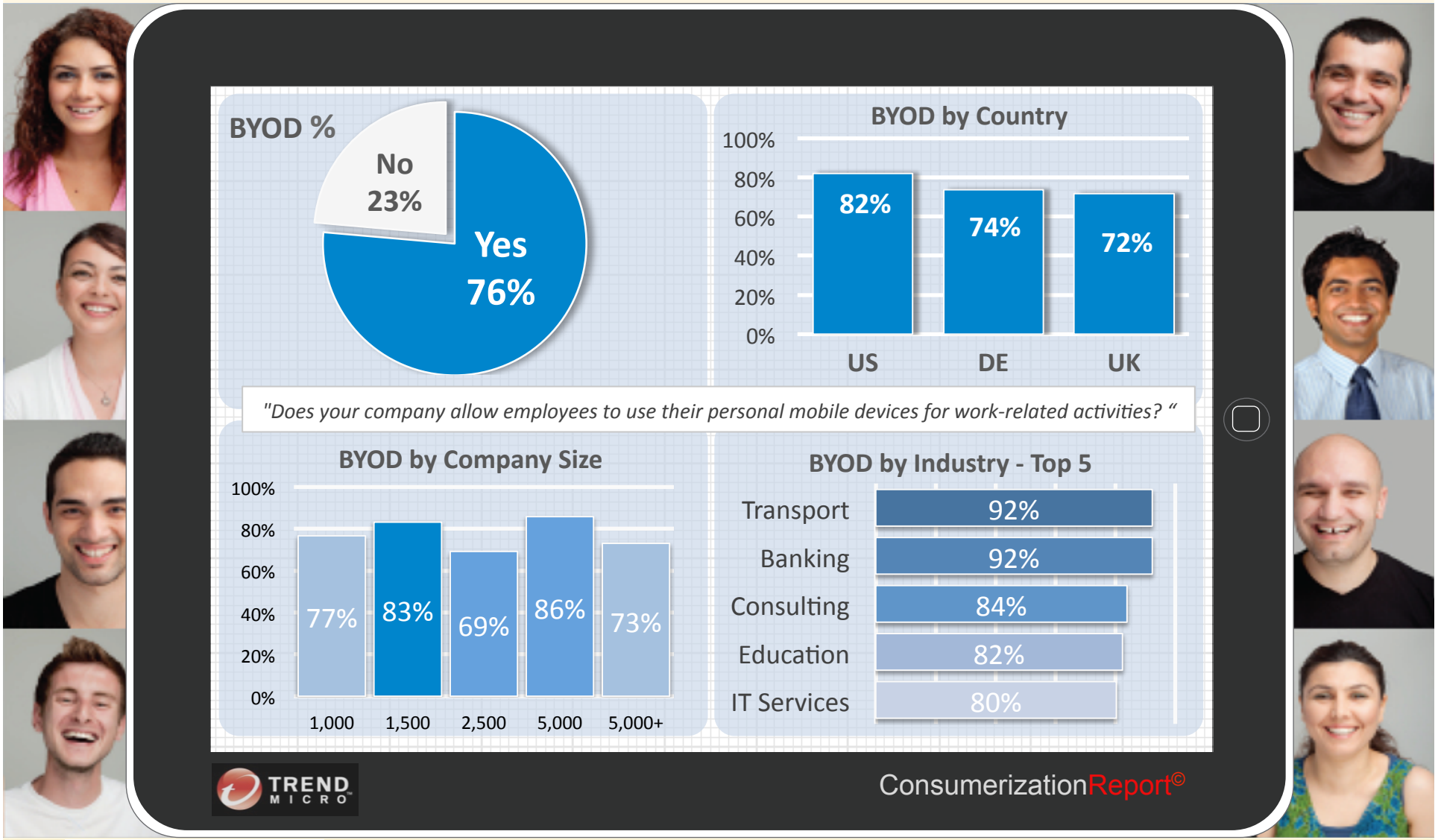
Source: Trend Micro internal analysis based on Gartner, Forrester and IDC market data – Update February, 28 2012

TREND MICRO

ConsumerizationReport©

The Consumerization Report

RSA CONFERENCE CHINA 2012

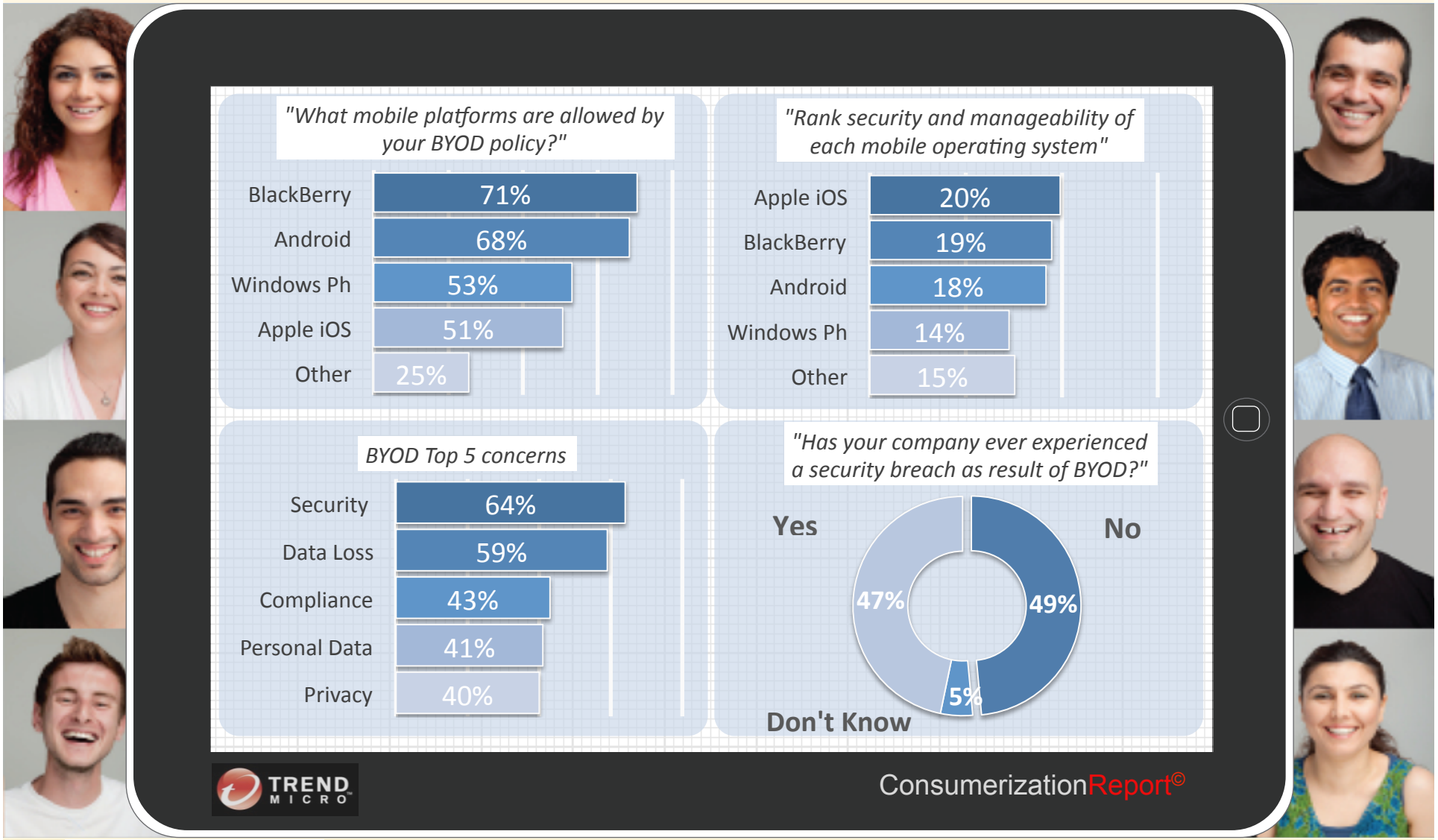


TREND MICRO

RSA信息安全大会2012

The Consumerization Report

RSA CONFERENCE CHINA 2012



How Secure and Manageable?

RSA CONFERENCE CHINA 2012

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

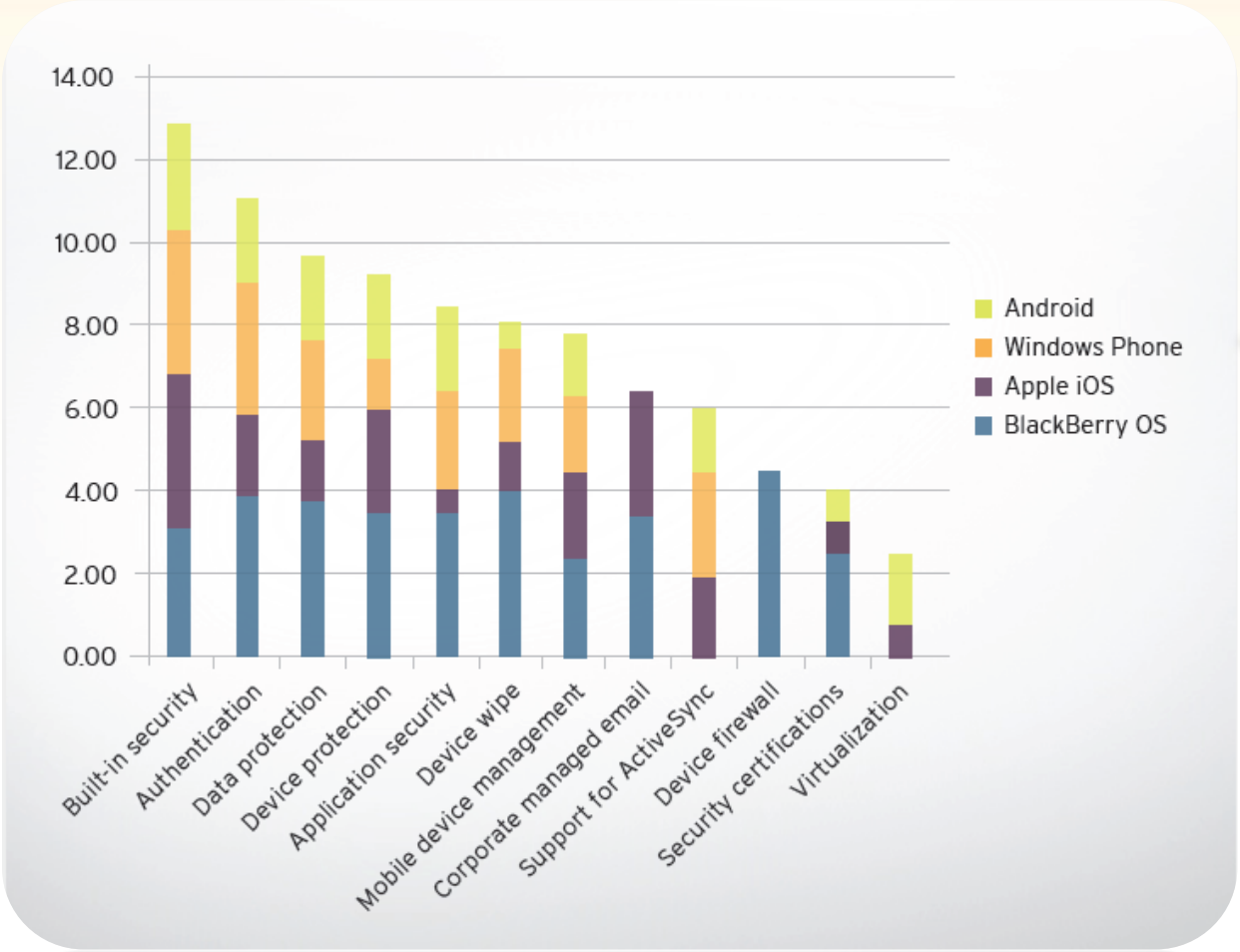
Philippe Winthrop

Managing Director, Enterprise Mobility Foundation

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

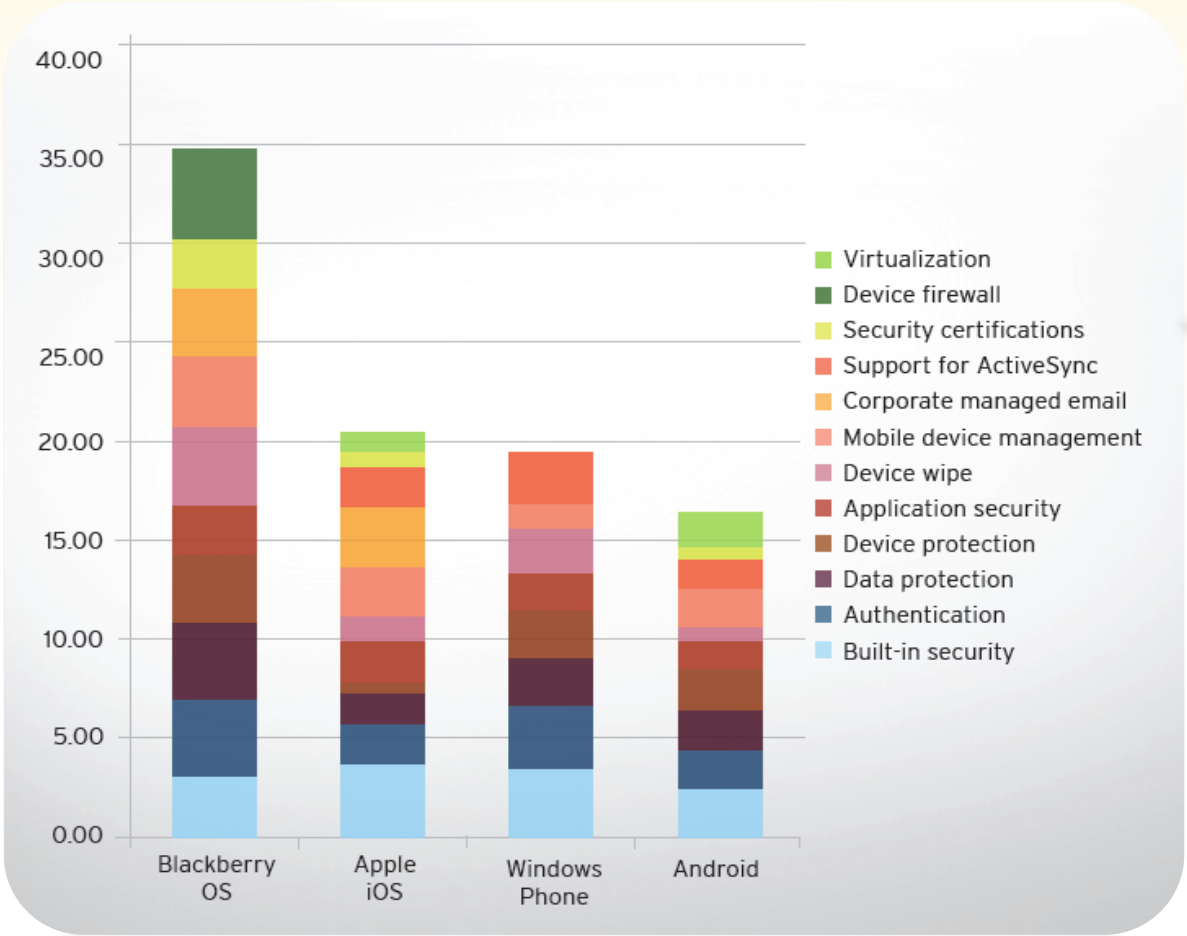
Ratings By Category

RSA CONFERENCE CHINA 2012



Ratings By Mobile Platform

RSA CONFERENCE CHINA 2012



Security and Management Criteria

RSA CONFERENCE CHINA 2012

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

RSA CONFERENCE CHINA 2012

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

RSA CONFERENCE CHINA 2012

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

TREND MICRO

Some recent vulnerabilities

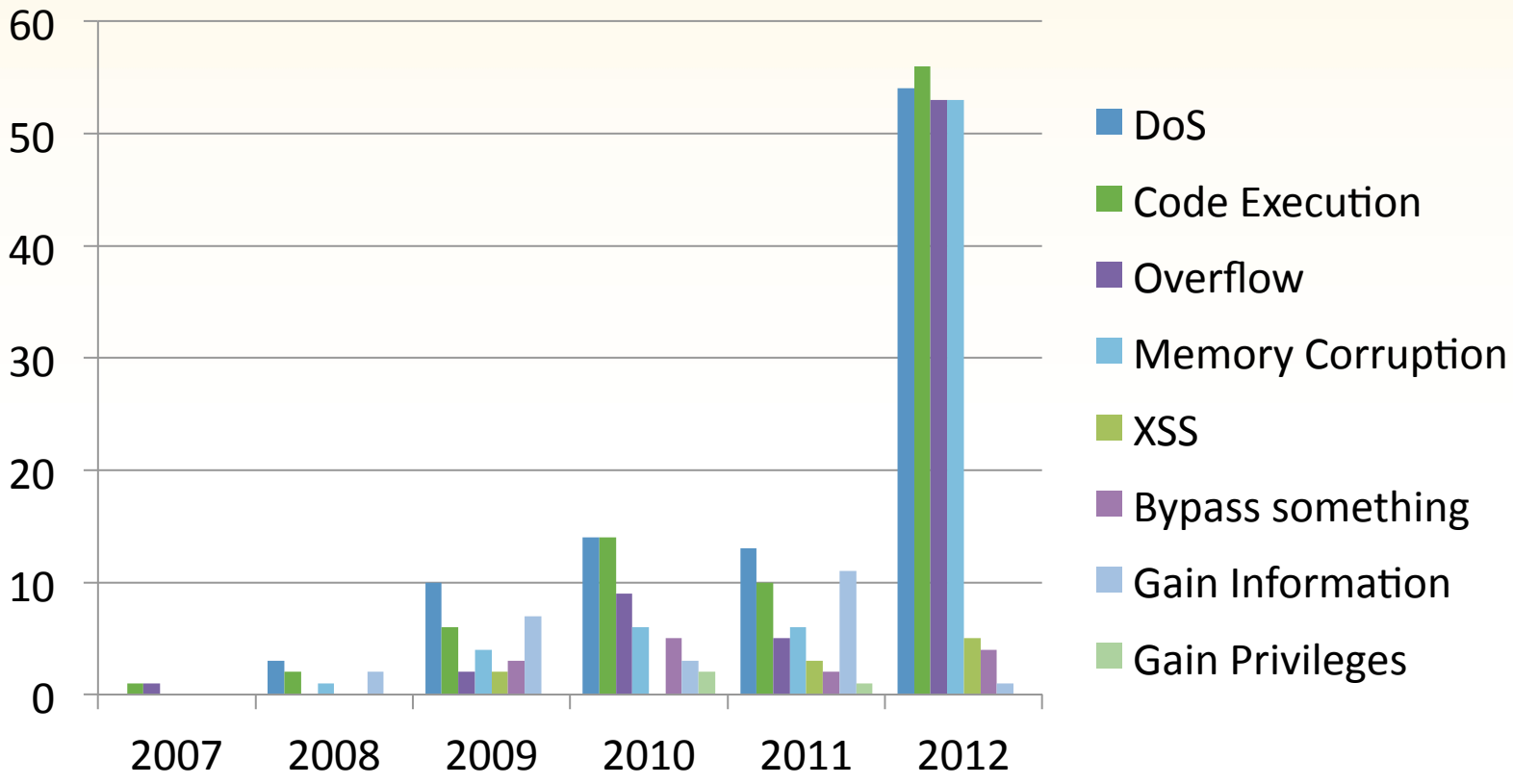
Android

- CVE-2011-3874 – Buffer Overflow allows code execution
- CVE-2011-1823 – Local code execution and root privileges (Gingerbreak)
- CVE-2011-1149 – Bypass sandbox and escalate privileges (KillingInTheNameOf)
- A multitude of Adob Flash vulnerabilities

Apple iOS

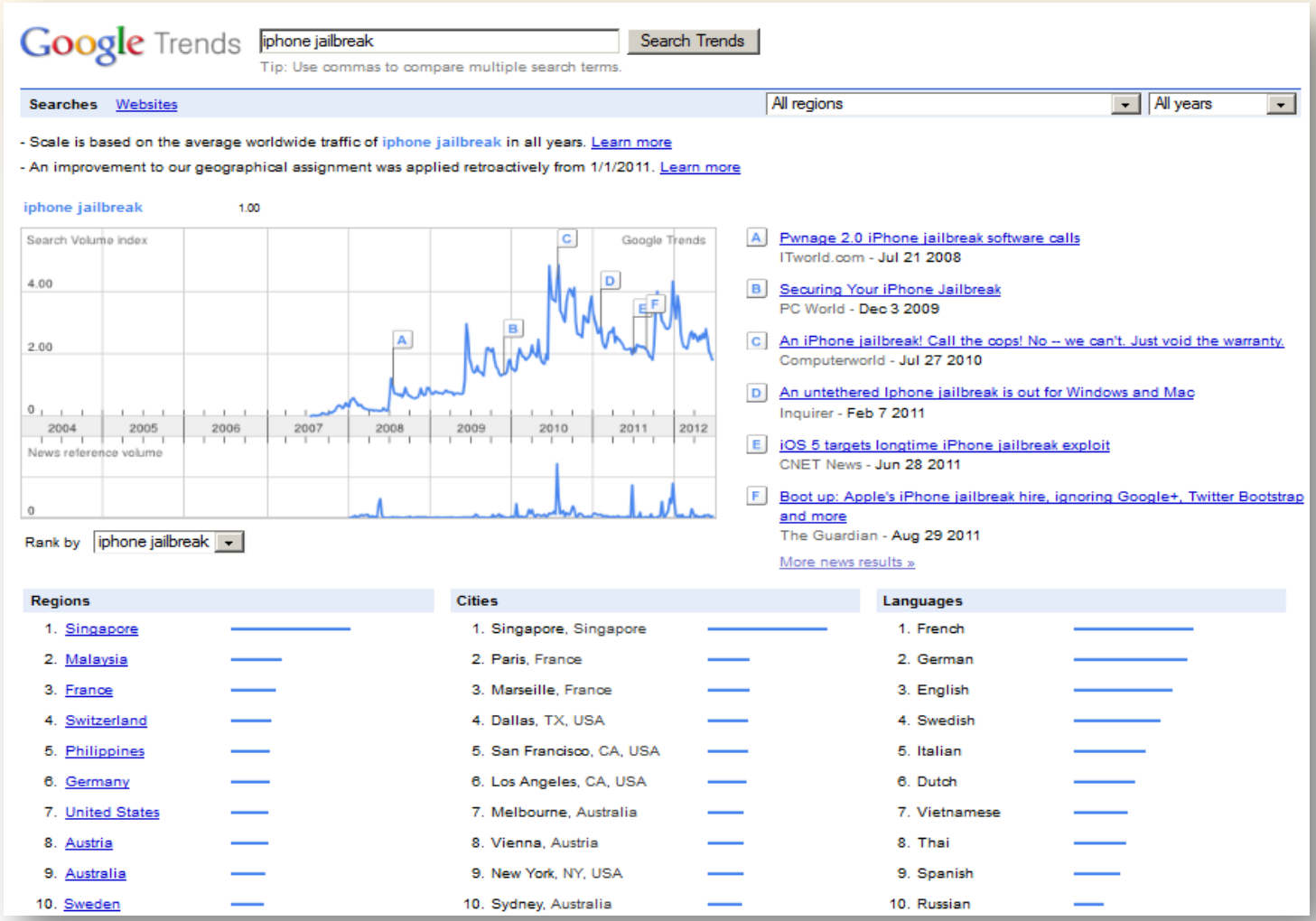
- CVE-2011-3246 – Malicious URLs disclose sensitive information
- CVE–2011-3439 – Malicious font leads to arbitrary code execution
- CVE-2011-3442 – Ability to bypass code-signing checks
- CVE-2011-3255 – Apple ID & password could be intercepted by installed apps

No Platform is immune: Apple iOS Detail

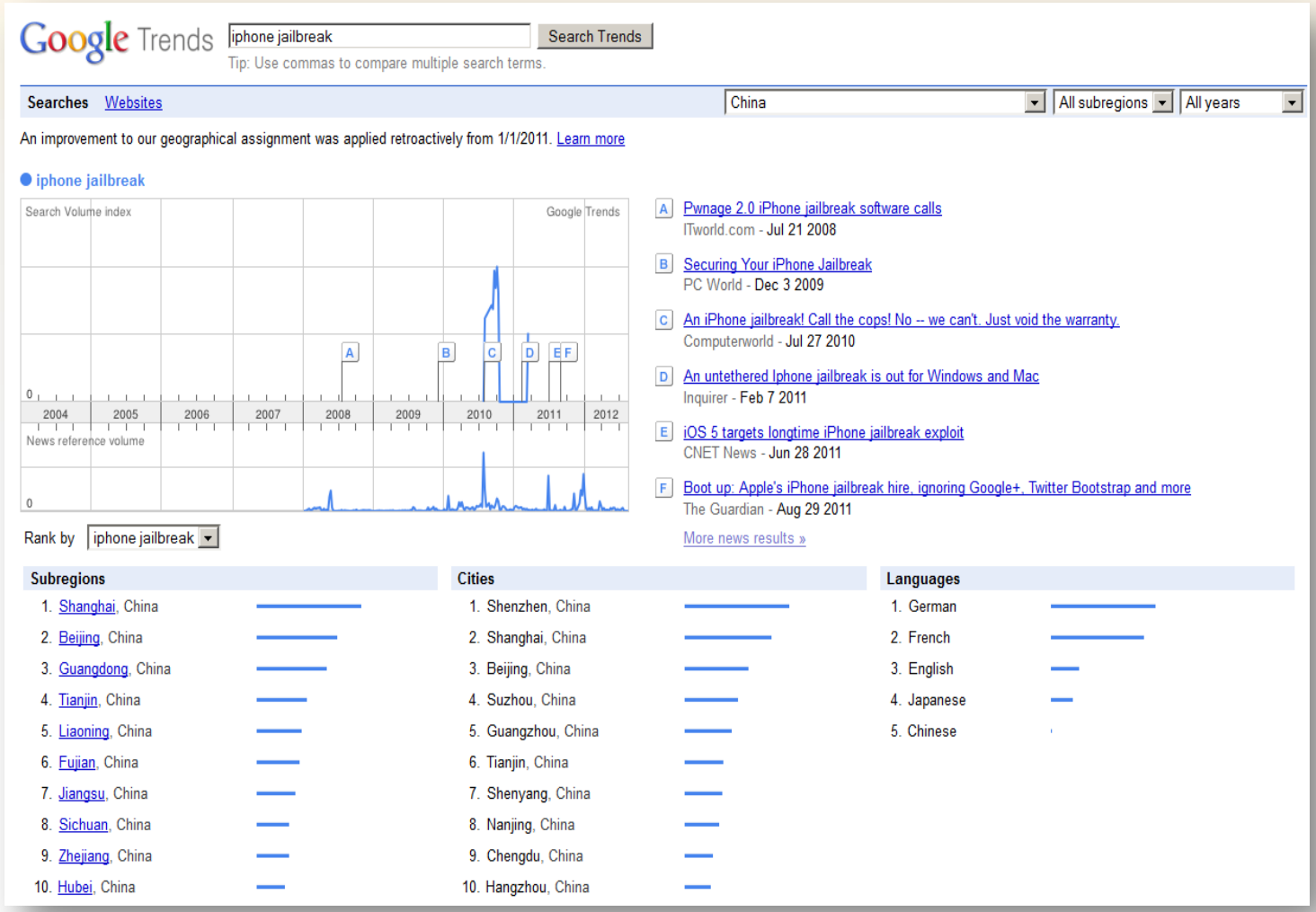


Source: National Vulnerability Database via CVEDetails.com – as of June 20, 2012

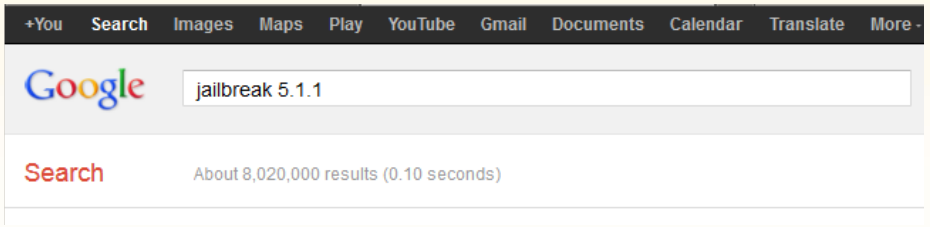
Jailbreaking Trends



Jailbreaking Trends - China Detail



How To Jailbreak iOS 5.1.1



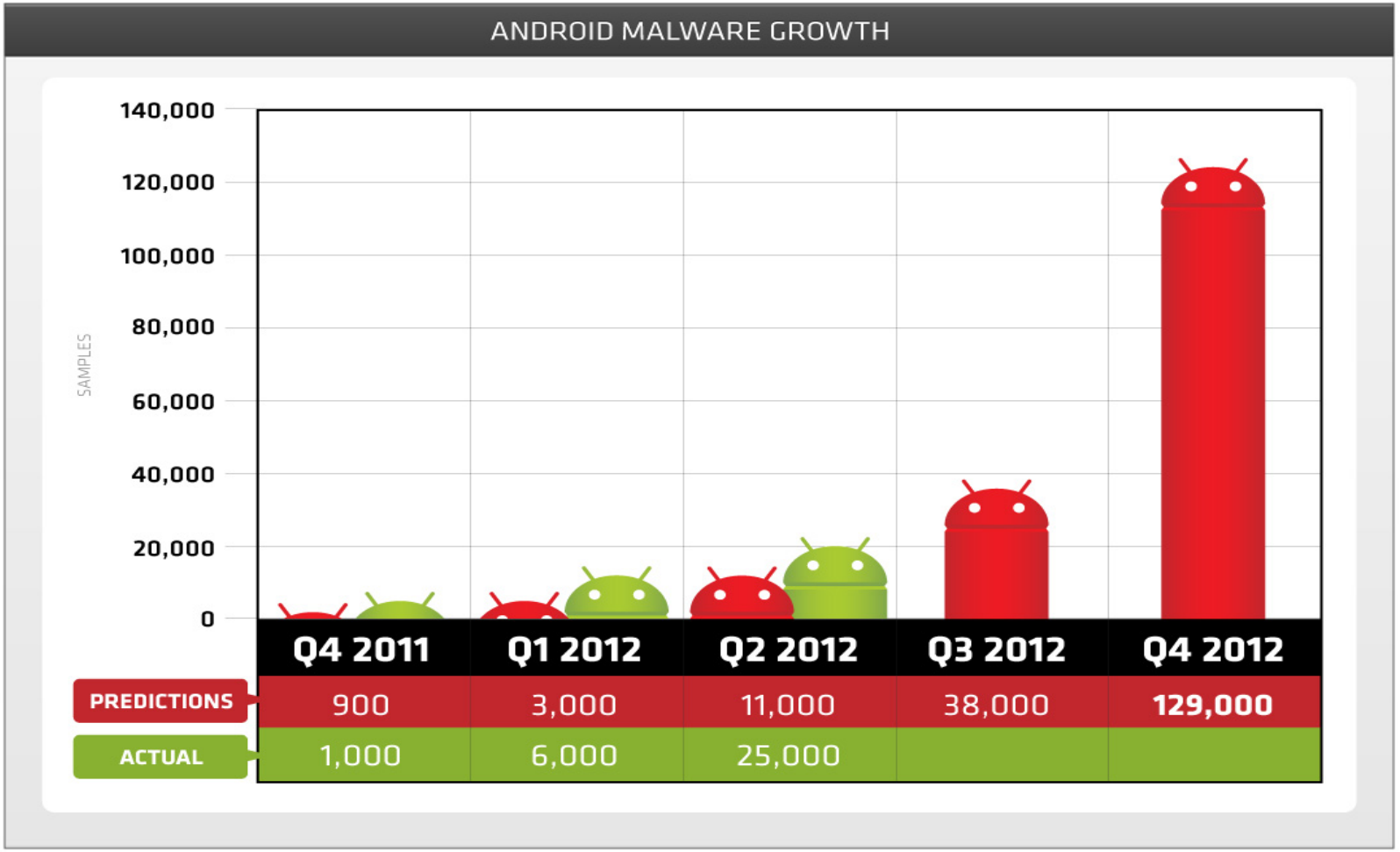
Download Links
Xxxx v2.0.4 MacOSX (10.5, 10.6, 10.7)
Xxxx v2.0.4 Windows (XP/Vista/Win7)
Xxxx v2.0.4 Linux (x86/x86_64)

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

Android is where the action is

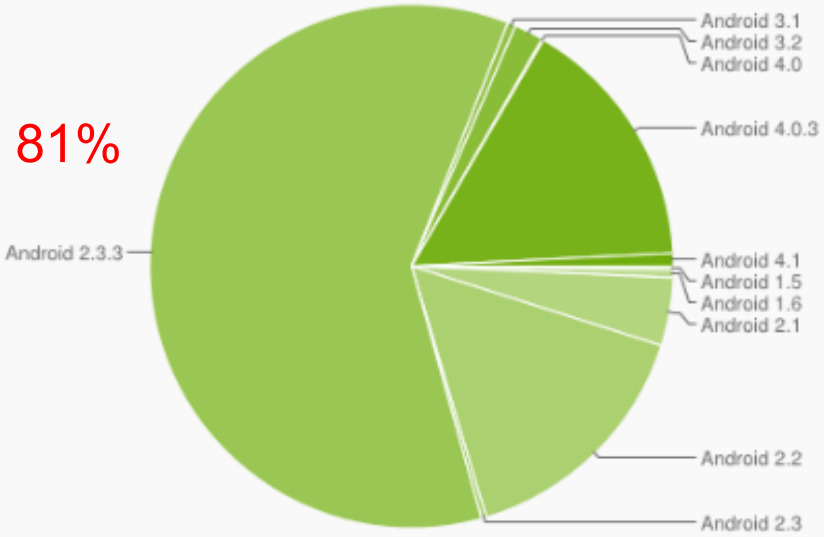


Source: Trend Labs, Trend Micro Inc. – as of Q2 2012

Android Versions Distribution

Version	Codename	API Level	Distribution
1.5	Cupcake	3	0.2%
1.6	Donut	4	0.5%
2.1	Eclair	7	4.2%
2.2	Froyo	8	15.5%
2.3 - 2.3.2	Gingerbread	9	0.3%
2.3.3 - 2.3.7		10	60.3%
3.1	Honeycomb	12	0.5%
3.2		13	1.8%
4.0 - 4.0.2	Ice Cream Sandwich	14	0.1%
4.0.3 - 4.0.4		15	15.8%
4.1	Jelly Bean	16	0.8%

81%



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

Source: Google http://developer.android.com/resources/dashboard/platform-versions – as of August1, 2012

Malicious Apps on Legit Marketplace

Figure 1. Apps supposedly offered by Rovio Mobile Ltd.

Malicious Apps on Legit Marketplace

TrendLabs

MALWARE BLOG

Threat News and Information Direct from the Experts

TREND MICRO

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

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

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

Search our blog:

Go

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 Spytool App for

Android Spy Apps

Figure 2.

Figure 3. Screenshot of a web site that tracks devices

Takeaways

- 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_Garlati@TrendMicro.com

http://BringYourOwnIT.com

Twitter @CesareGarlati

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012