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

智能电话安全性赢家与输家

Cesare Garlati

移动安全副总裁

Trend Micro, Inc.

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012

IT 的消费化

RSA CONFERENCE CHINA 2012

“在未来 10 年中，消费化将成为影响 IT 行业的最重要趋势”

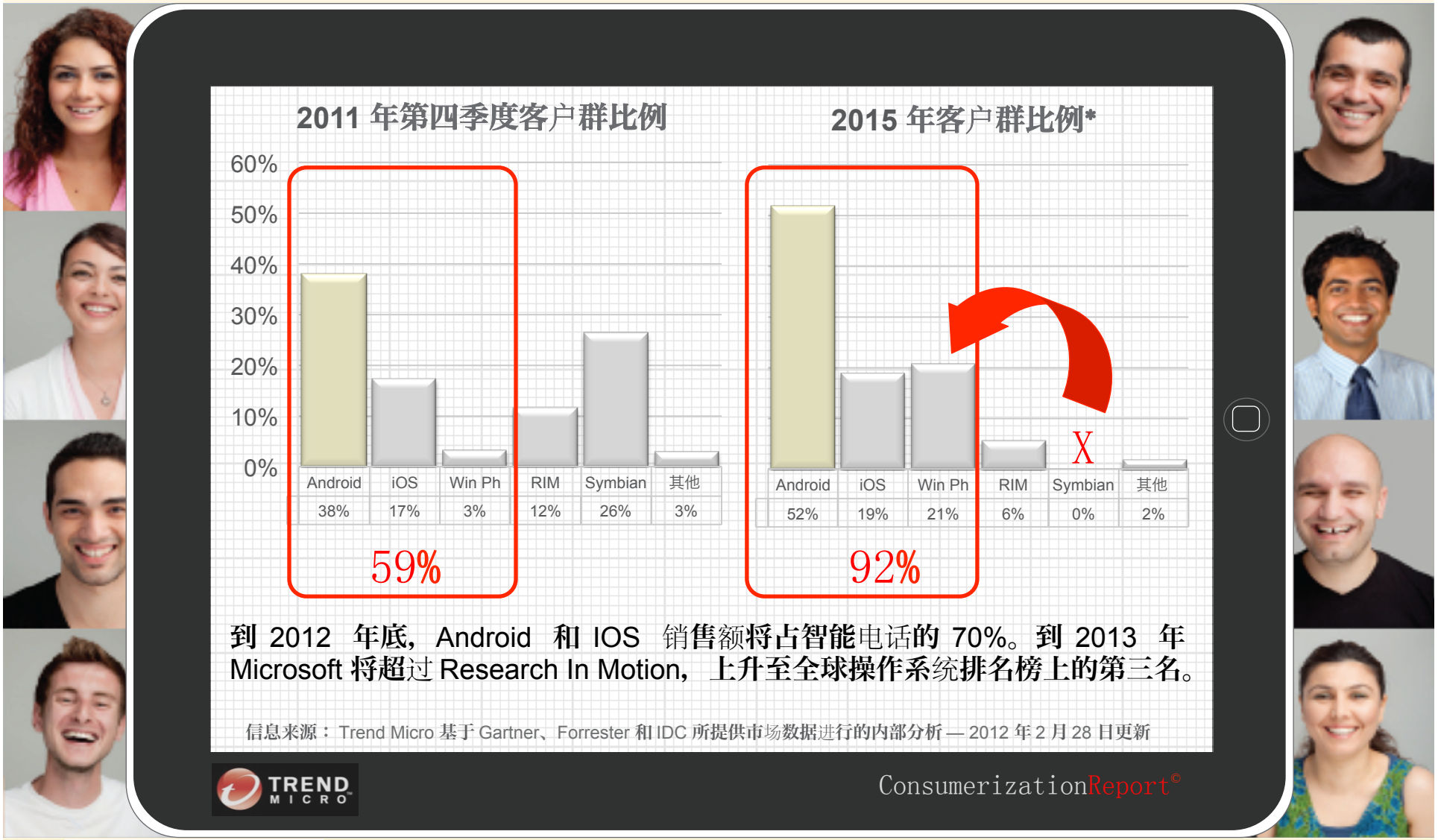
Gartner

- **新技**术**首先在消**费**市**场**中出**现，**然后**经员**工引入**，传**入商**业组织**内**
- **由于人**们**在**处**理工作事宜和个人事**务时**依**赖**相同的**设备**和**应**用程序**，IT **和消**费**型**电子产**品开始融合**。
- 势**不可**挡**的消**费**型技**术**浪潮冲**击**着企**业，IT 经**理使出**浑**身解数**，**通**过实**施策略保持控制力**

在 2001 年 CSC 前沿论坛上，D. Neal 和 J. Taylor 首先提出了消费化这一术语。

消费化报告

RSA CONFERENCE CHINA 2012



到 2012 年底，Android 和 IOS 销售额将占智能电话的 70%。到 2013 年 Microsoft 将超过 Research In Motion，上升至全球操作系统排名榜上的第三名。

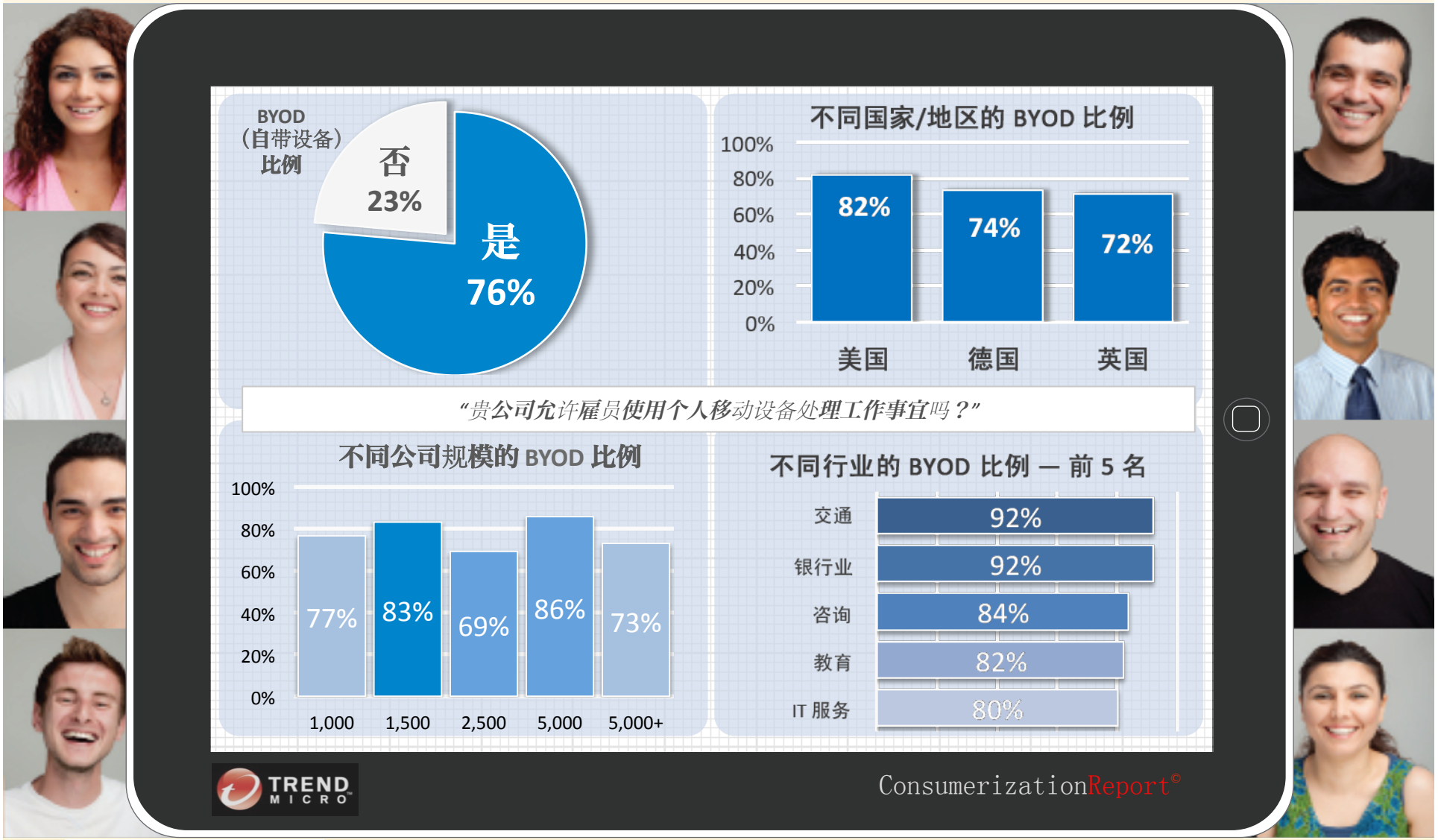
信息来源：Trend Micro 基于 Gartner、Forrester 和 IDC 所提供市场数据进行的内部分析 — 2012 年 2 月 28 日更新

TREND MICRO

ConsumerizationReport©

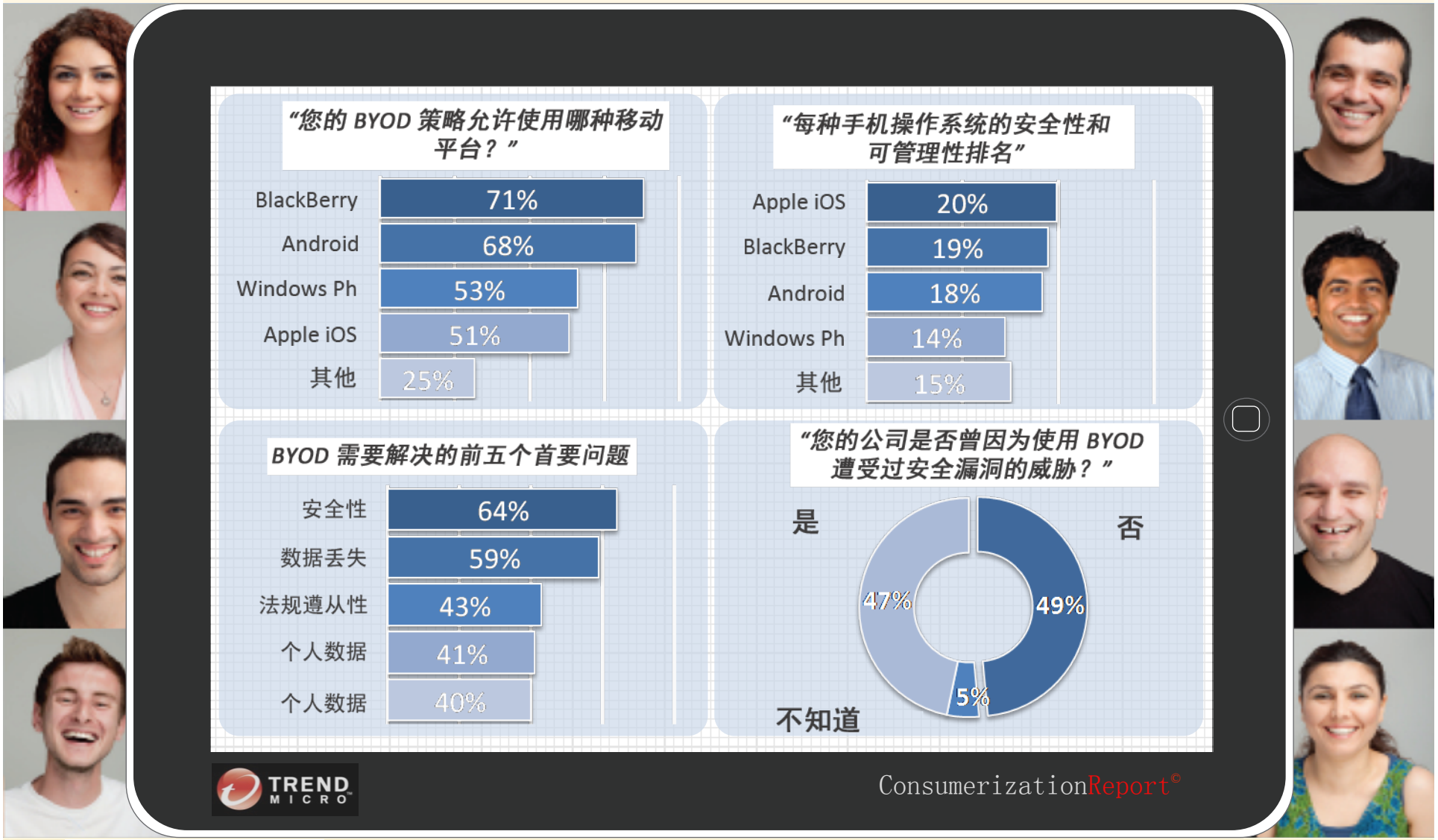
消费化报告

RSA CONFERENCE CHINA 2012



消费化报告

RSA CONFERENCE CHINA 2012



TREND MICRO

RSA信息安全大会2012

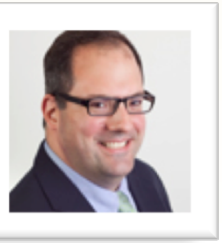
如何实现安全性和可管理性？

RSA CONFERENCE CHINA 2012

Raimund Genes

Trend Micro 首席技术官

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



Chris Ilg

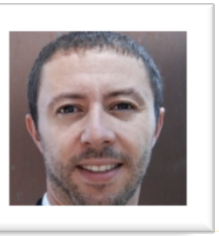
Altimeter Group 行业分析师

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

Nigel Stanley

Bloor Research 实践部领导

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



Philippe Winthrop

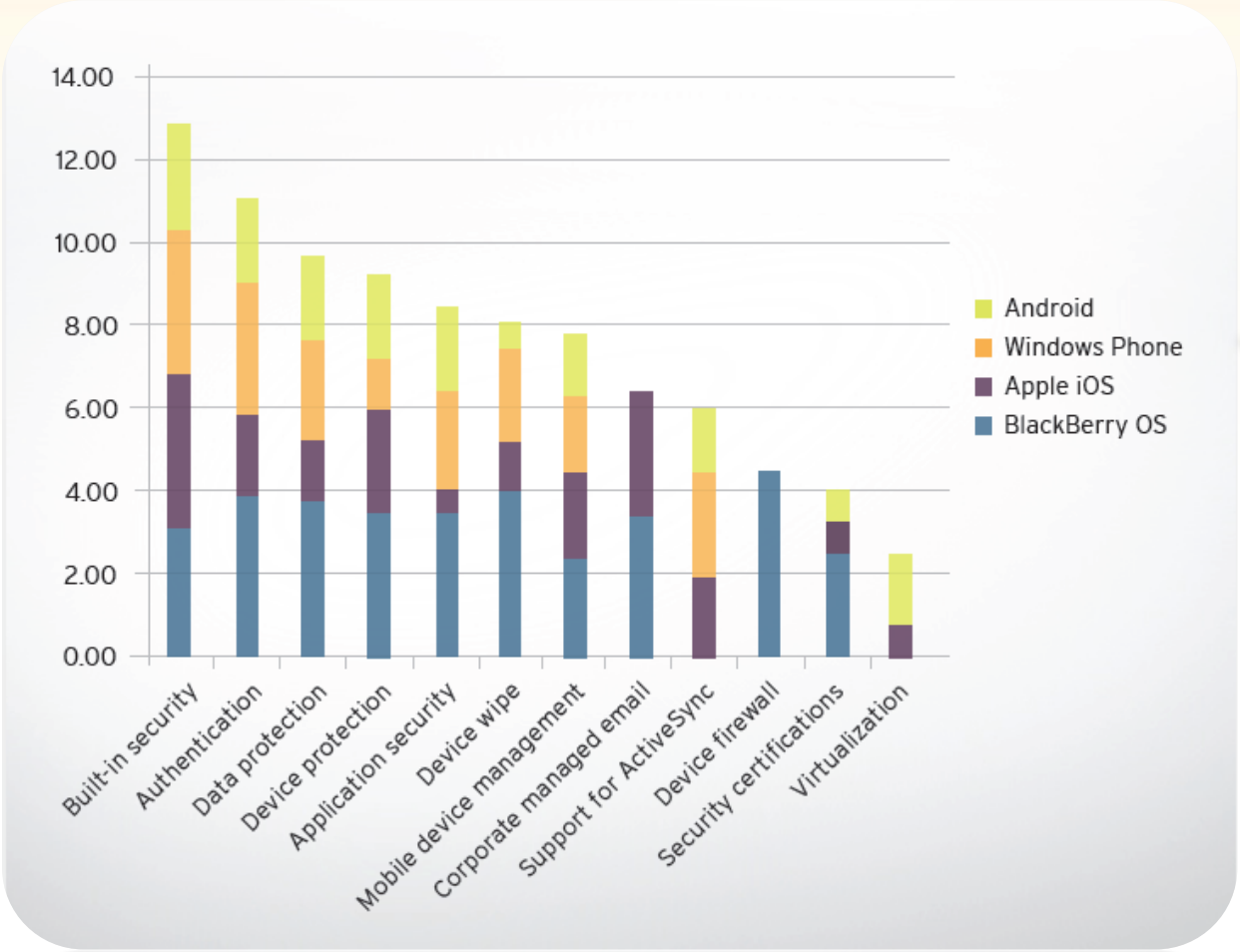
Enterprise Mobility Foundation 常务董事

http://www.ge.com/index.html

TREND MICRO

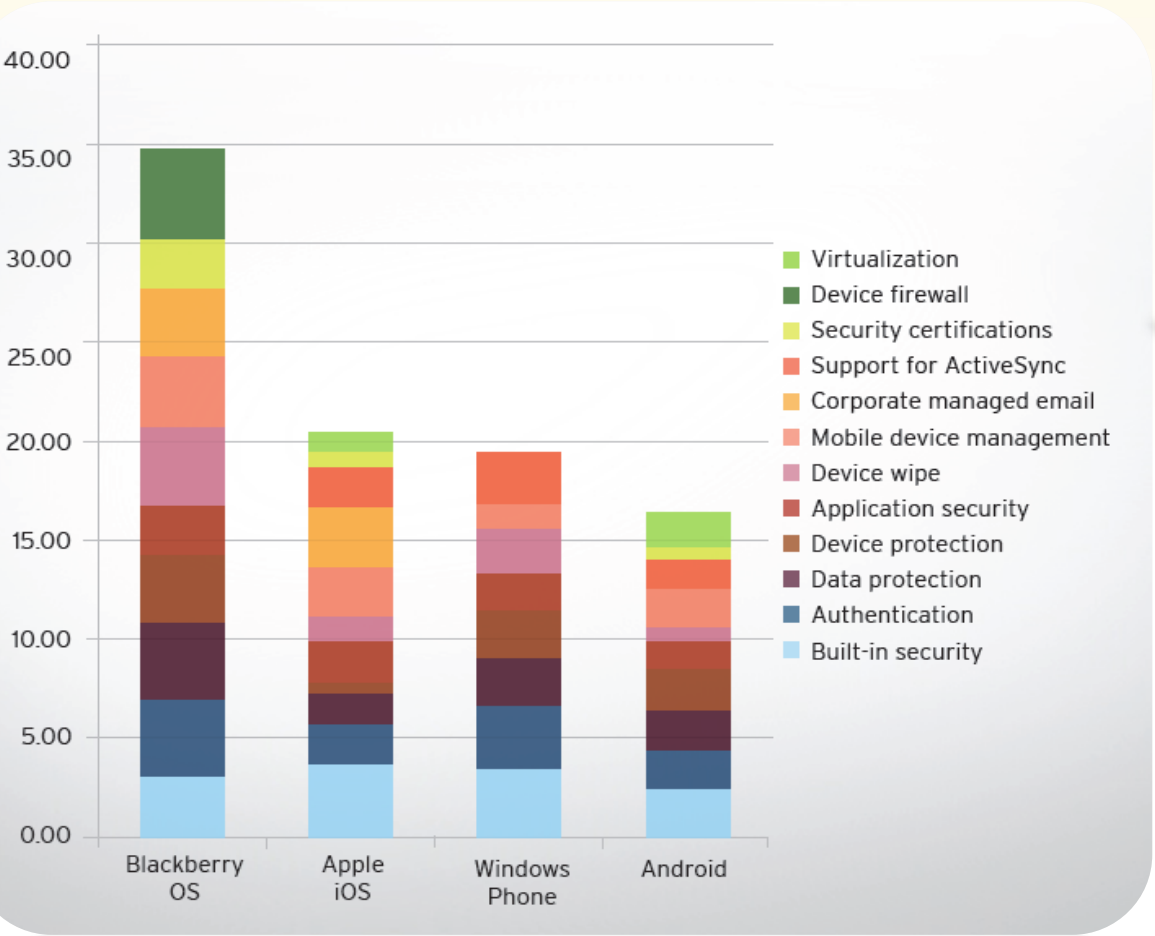
按类别评级

RSA CONFERENCE CHINA 2012



按移动平台评级

RSA CONFERENCE CHINA 2012



安全性和管理标准

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

安全性和管理标准

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

安全性和管理标准

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

RSA信息安全大会2012

最近出现的一些漏洞

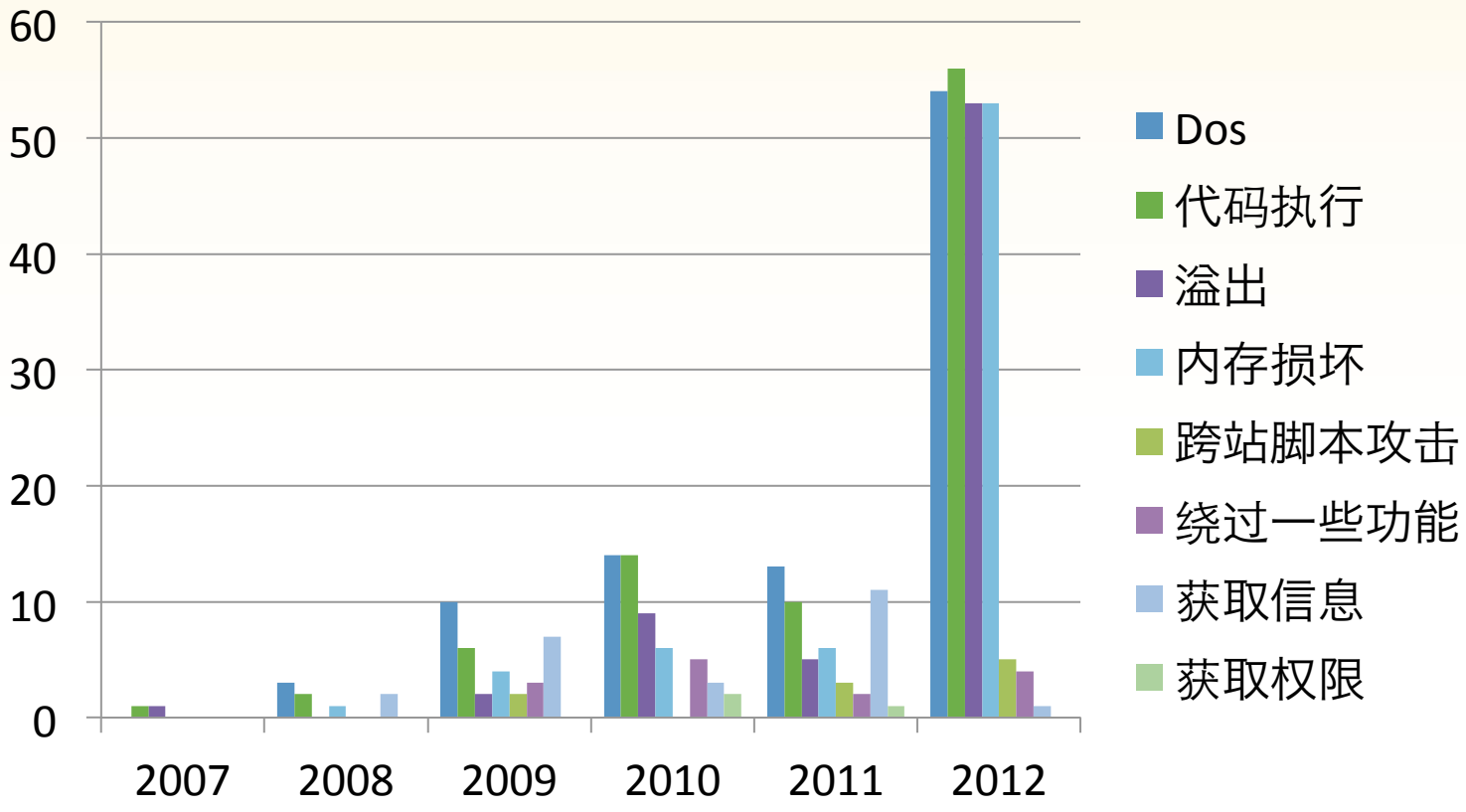
Android

- CVE-2011-3874 — 缓存溢出允许代码执行
- CVE-2011-1823 — 本地代码执行与 root 权限 (Gingerbreak)
- CVE-2011-1149 — 绕过沙盒与权限升级 (KillingInTheNameOf)
- 大量 Adobe Flash 漏洞

Apple iOS

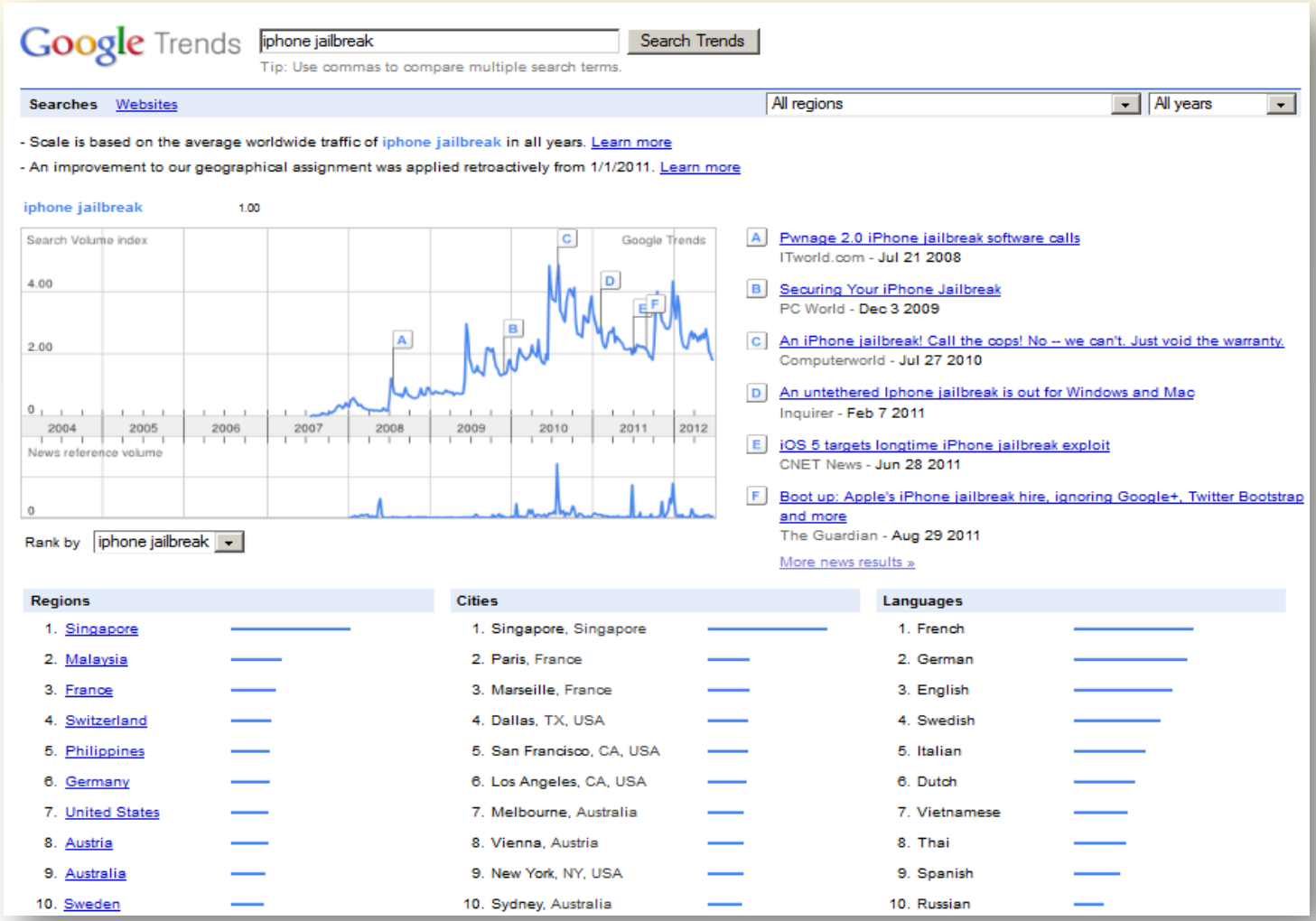
- CVE-2011-3246 — 恶意 URL 披露敏感信息
- CVE–2011-3439 — 恶意字体导致任意代码执行
- CVE-2011-3442 — 绕过代码签名检查的能力
- CVE-2011-3255 — Apple ID 和密码可能会被安装的应用程序拦截

没有平台能够幸免： Apple iOS 详情

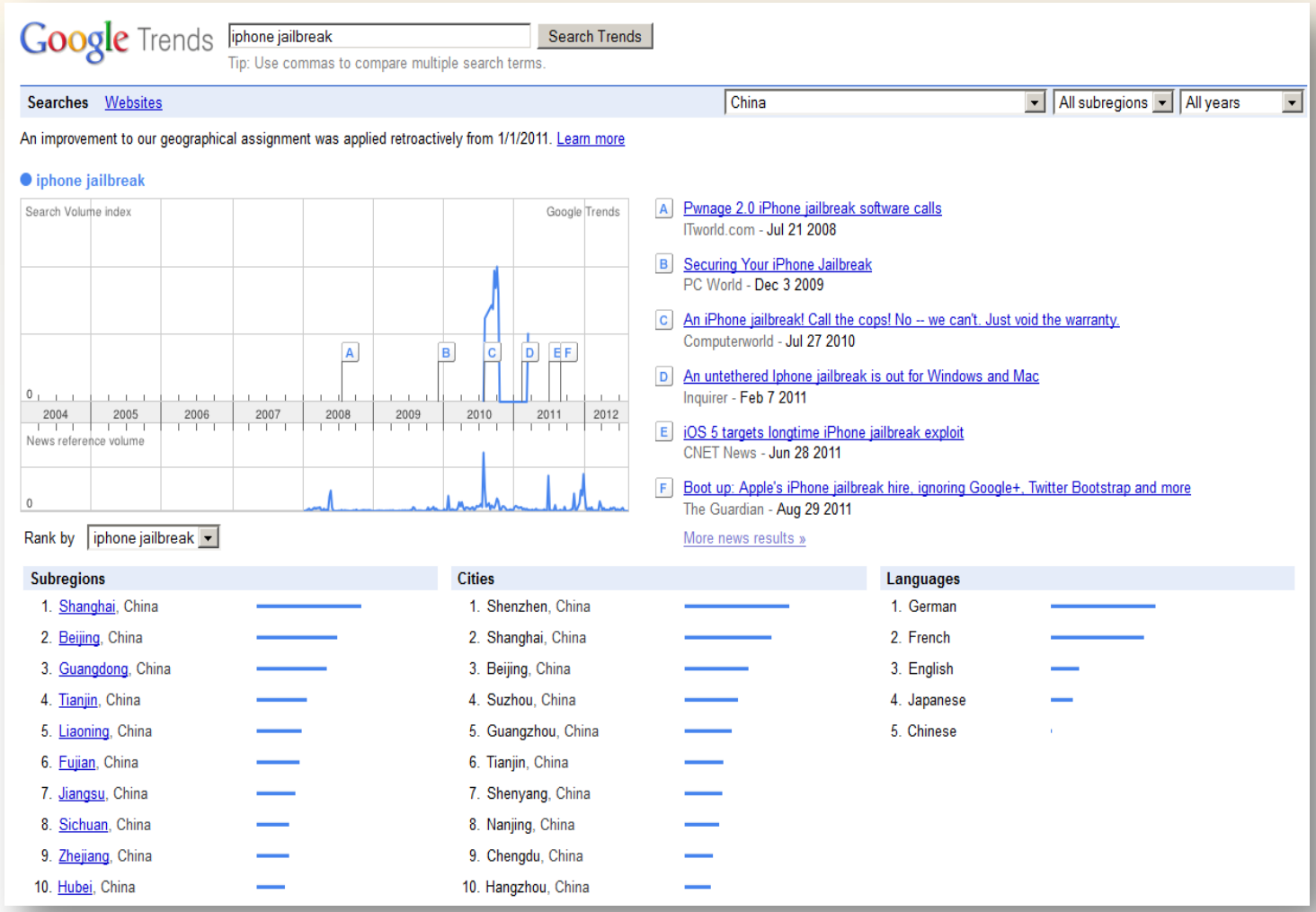


信息来源： 通过 CVEDetails.com 发布的国家漏洞数据库 — 截止 2012 年 6 月 20 日

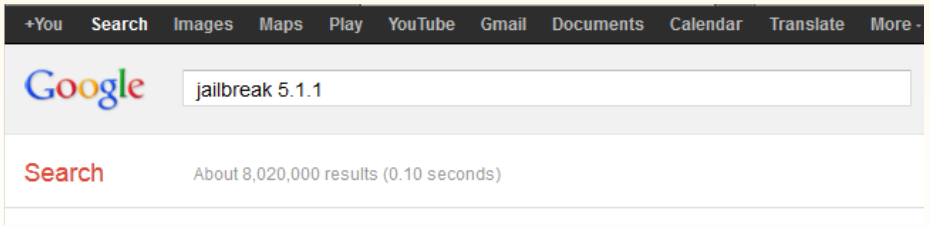
越狱动态


Google Trends
iphone jailbreak
Search Trends
Tip: Use commas to compare multiple search terms.
Searches
Websites
All regions
All years
- Scale is based on the average worldwide traffic of iphone jailbreak in all years. Learn more
- An improvement to our geographical assignment was applied retroactively from 1/1/2011. Learn more
iphone jailbreak
1.00
Search Volume index
Google Trends
4.00
2.00
0
2004
2005
2006
2007
2008
2009
2010
2011
2012
News reference volume
0
Rank by
iphone jailbreak
A Pwnage 2.0 iPhone jailbreak software calls
ITworld.com - Jul 21 2008
B Securing Your iPhone Jailbreak
PC World - Dec 3 2009
C An iPhone jailbreak! Call the cops! No -- we can't. Just void the warranty.
Computerworld - Jul 27 2010
D An untethered Iphone jailbreak is out for Windows and Mac
Inquirer - Feb 7 2011
E iOS 5 targets longtime iPhone jailbreak exploit
CNET News - Jun 28 2011
F Boot up: Apple's iPhone jailbreak hire, ignoring Google+, Twitter Bootstrap and more
The Guardian - Aug 29 2011
More news results »
Regions
1. Singapore
2. Malaysia
3. France
4. Switzerland
5. Philippines
6. Germany
7. United States
8. Austria
9. Australia
10. Sweden
Cities
1. Singapore, Singapore
2. Paris, France
3. Marseille, France
4. Dallas, TX, USA
5. San Francisco, CA, USA
6. Los Angeles, CA, USA
7. Melbourne, Australia
8. Vienna, Austria
9. New York, NY, USA
10. Sydney, Australia
Languages
1. French
2. German
3. English
4. Swedish
5. Italian
6. Dutch
7. Vietnamese
8. Thai
9. Spanish
10. Russian

越狱动态 – 中国详情


Google Trends
iphone jailbreak
Search Trends
Tip: Use commas to compare multiple search terms.
Searches Websites
China
All subregions
All years
An improvement to our geographical assignment was applied retroactively from 1/1/2011. Learn more
iphone jailbreak
Search Volume index
Google Trends
2004 2005 2006 2007 2008 2009 2010 2011 2012
News reference volume
A Pwnage 2.0 iPhone jailbreak software calls
ITworld.com - Jul 21 2008
B Securing Your iPhone Jailbreak
PC World - Dec 3 2009
C An iPhone jailbreak! Call the cops! No -- we can't. Just void the warranty.
Computerworld - Jul 27 2010
D An untethered Iphone jailbreak is out for Windows and Mac
Inquirer - Feb 7 2011
E iOS 5 targets longtime iPhone jailbreak exploit
CNET News - Jun 28 2011
F Boot up: Apple's iPhone jailbreak hire, ignoring Google+, Twitter Bootstrap and more
The Guardian - Aug 29 2011
More news results »
Rank by iphone jailbreak
Subregions
1. Shanghai, China
2. Beijing, China
3. Guangdong, China
4. Tianjin, China
5. Liaoning, China
6. Fujian, China
7. Jiangsu, China
8. Sichuan, China
9. Zhejiang, China
10. Hubei, China
Cities
1. Shenzhen, China
2. Shanghai, China
3. Beijing, China
4. Suzhou, China
5. Guangzhou, China
6. Tianjin, China
7. Shenyang, China
8. Nanjing, China
9. Chengdu, China
10. Hangzhou, China
Languages
1. German
2. French
3. English
4. Japanese
5. Chinese

如何越狱 iOS 5.1.1



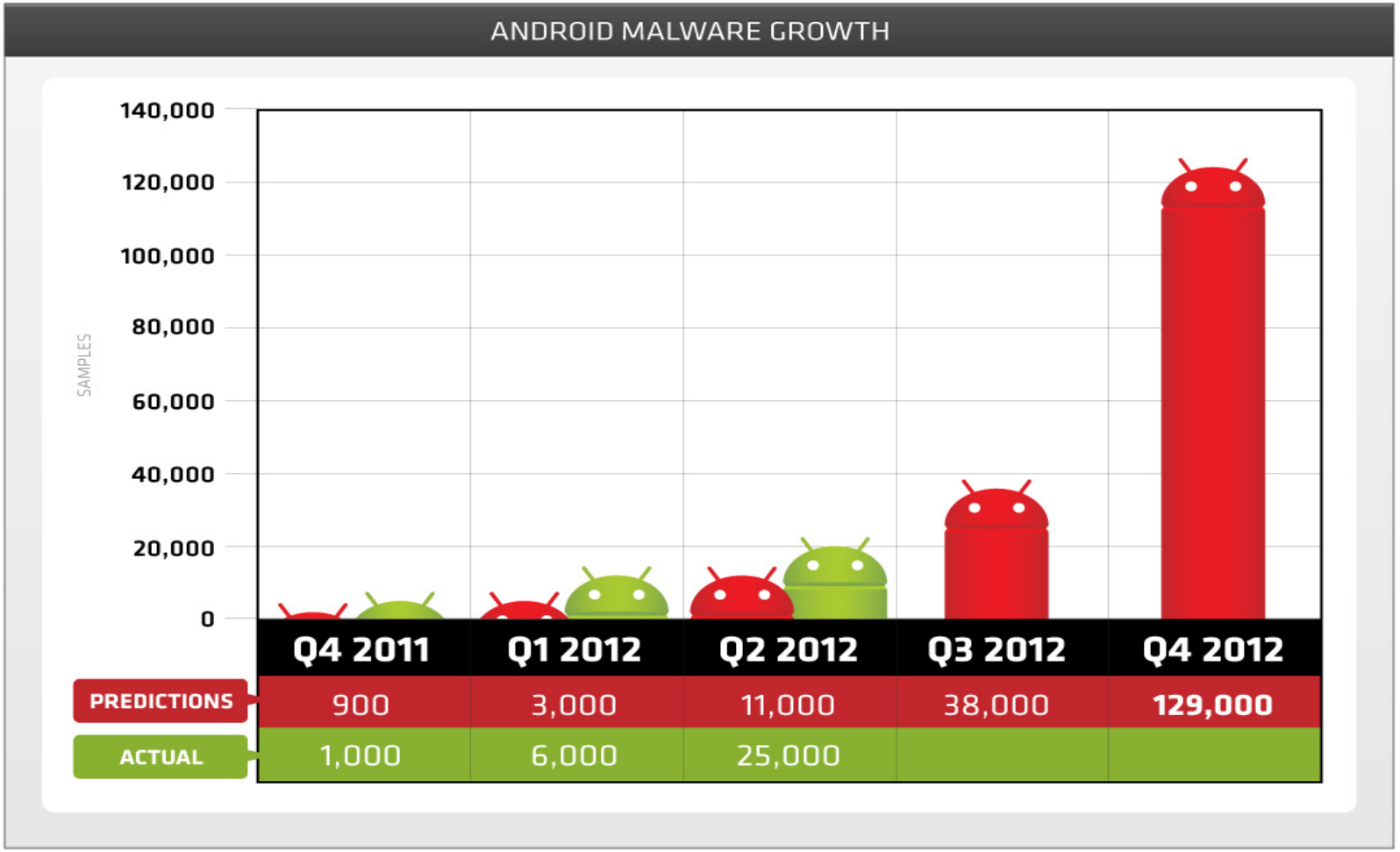
下载链接
Xxxx v2.0.4 MacOSX (10.5, 10.6, 10.7)
Xxxx v2.0.4 Windows (XP/Vista/Win7)
Xxxx v2.0.4 Linux (x86/x86_64)

如何使用 Xxxxx 2.0：

1. 在 iTunes 中备份您的设备（在“设备”菜单下，右键单击设备名称，然后单击“备份”）。
2. 打开 Xxxxx 并确保您的设备仍通过 USB 电缆与计算机连接。
3. 单击“越狱”并耐心等待…请不要断开设备连接。
4. 越狱结束后，返回 iTunes 并恢复先前的备份。

Xxxxx 2.0 支持 5.1.1 上的以下设备：
iPad 1、iPad 2、iPad 3（现在 Xxxxx 2.0.4 也支持 iPad2）
iPhone 3GS、iPhone 4、iPhone 4S
iPod touch 第三代、iPod touch 第四代

Android 是针对的目标

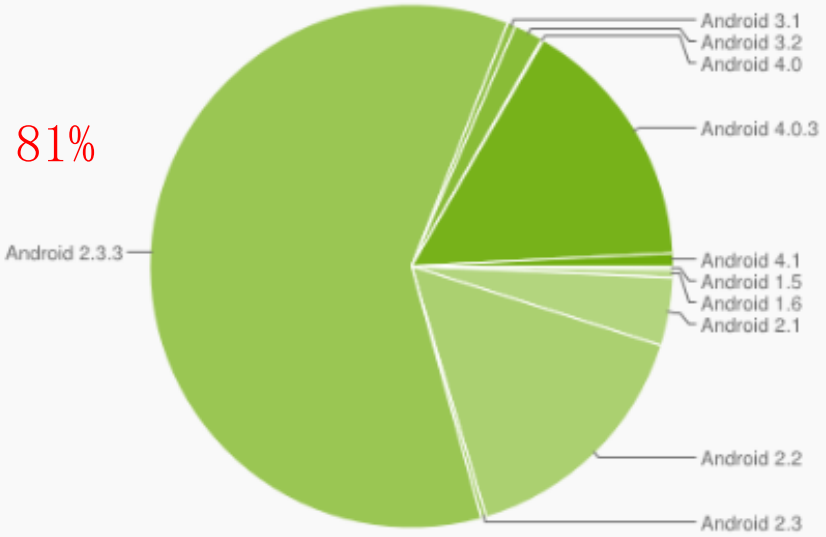


信息来源： Trend Micro Inc. 公司 Trend 实验室结果 — 截止 2012 年第二季度

Android 版本分布情况

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

信息来源： Google http://developer.android.com/resources/dashboard/platform-versions — 截止 2012 年 8 月 1 日

正规卖场中的恶意应用程序

Figure 1. Apps supposedly offered by Rovio Mobile Ltd.

正规卖场中的恶意应用程序

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 间谍应用程序

Figure 2.

Figure 3. Screenshot of a web site that tracks devices

小结

- 消费型移动技术正在入侵企业，您无法阻止它的脚步
- 消费型技术不能达到企业的安全性和管理要求
- 即使有些平台比其他平台更加安全，但是无一能够幸免于难

1. *拥抱消费化*
2. *了解各种平台上的风险情况*
3. *部署新的安全性和管理工具*

谢谢大家！

Cesare_Garlati@TrendMicro.com

http://BringYourOwnIT.com

Twitter @CesareGarlati

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012