TREND MICRO
Securing Your Journey to the Cloud

流動威脅及如何自我防護

李浩然
趨勢科技香港區顧問

議題

- 社交網絡的風險
  - 濫用機構網絡
  - 更多風險
  - 攻擊個案分析
- 社交網站用戶應作的準備
  - 如何設定 Facebook以保護私隱

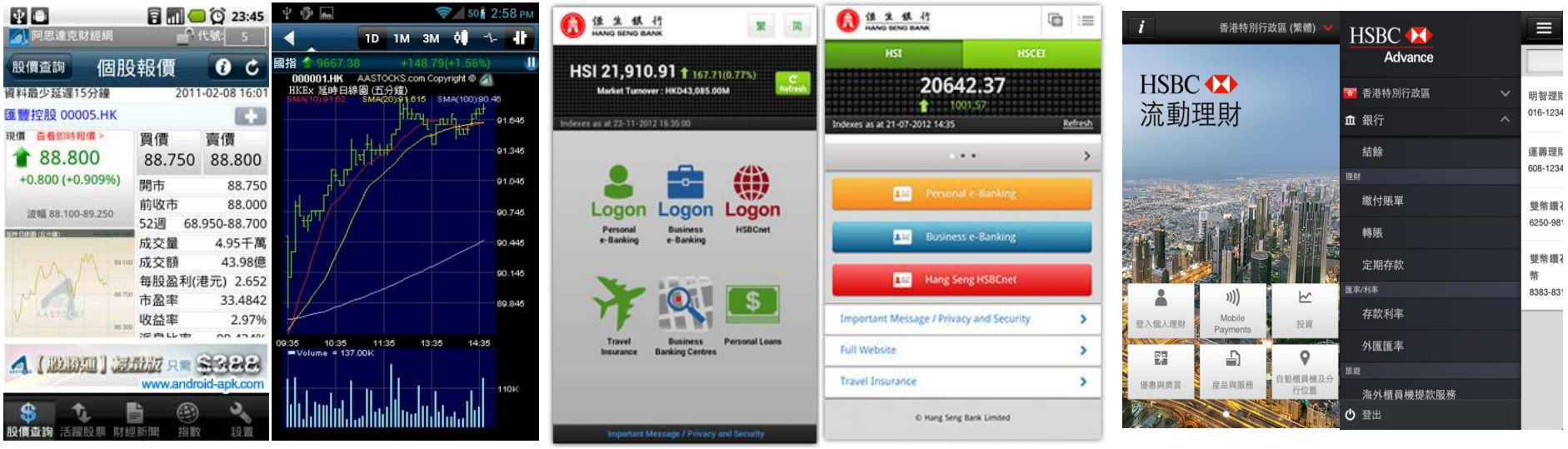
Why me?


Laptop PC
Android Tablet
Apple New iPad
Apple iPad
Nokia Symbian
Apple iPhone
Motorola Android

流動市場現況

網上金融

- 金融行業的流動裝置目前集中在手機銀行、證卷下單、掌上生活等應用，大多數是開發並用於終端的消費者便利使用。
- 以iOS作業系統為基礎的流動裝置作為載體，讓銀行、保險、證卷公司內部員工開發針對使用者服務與資料收集等APP，並快速產出文件與資料。



流動辦公室

- 將既有資料轉至流動裝置內，可解除機師飛行時所需攜帶的厚重文件
- 透過流動裝置，企業員工可在任何地點與時間存取所需的資料與交換訊息。

http://benevo.pixnet.net/blog/post/35750694-%E9%A3%9B%E8%88%AA%E6%89%8B%E5%86%8A%E8%88%87%E5%9C%96%E8%A1%A8%E6%8F%9B%E6%88%90ipad2%E9%80%B2%E6%A9%9F%E8%89%99

流動醫療 (Mobile Health)

- 日本NTT DoCoMo、卡塔爾電信(Qtel) 、AT&T、握達鋒等ISP業者最近部段發表新應用來拓展流動醫療市場
- 2011年中國解放軍第309醫院資訊化建設邁入一個新的嶄新領域，推行以iPad作為平台的護理流動工作站
- 用iPad所開發的護理流動工作站整合了該院現有的醫療資訊資源，包含放射中心的PACS系統、超音波、病理檢查報告系統、檢驗LIS系統、心電檢視系統、手術麻醉、放射化療、電子病歷等臨床醫用資訊系統
- 院區內覆蓋WIFY網路，醫生可透過iPad使用HIS伺服器，調閱病人的資料，例如電子病歷，各項影像學檢查：核磁共振影像（MRI）、電腦斷層掃描影像（CT）、X光片；病理報告、檢驗單等訊息，只要手指輕輕劃過即可在iPad上看到詳盡訊息

使用iPAD查房

醫囑介面

PACS影像

檢驗結果查詢

政府流動 app

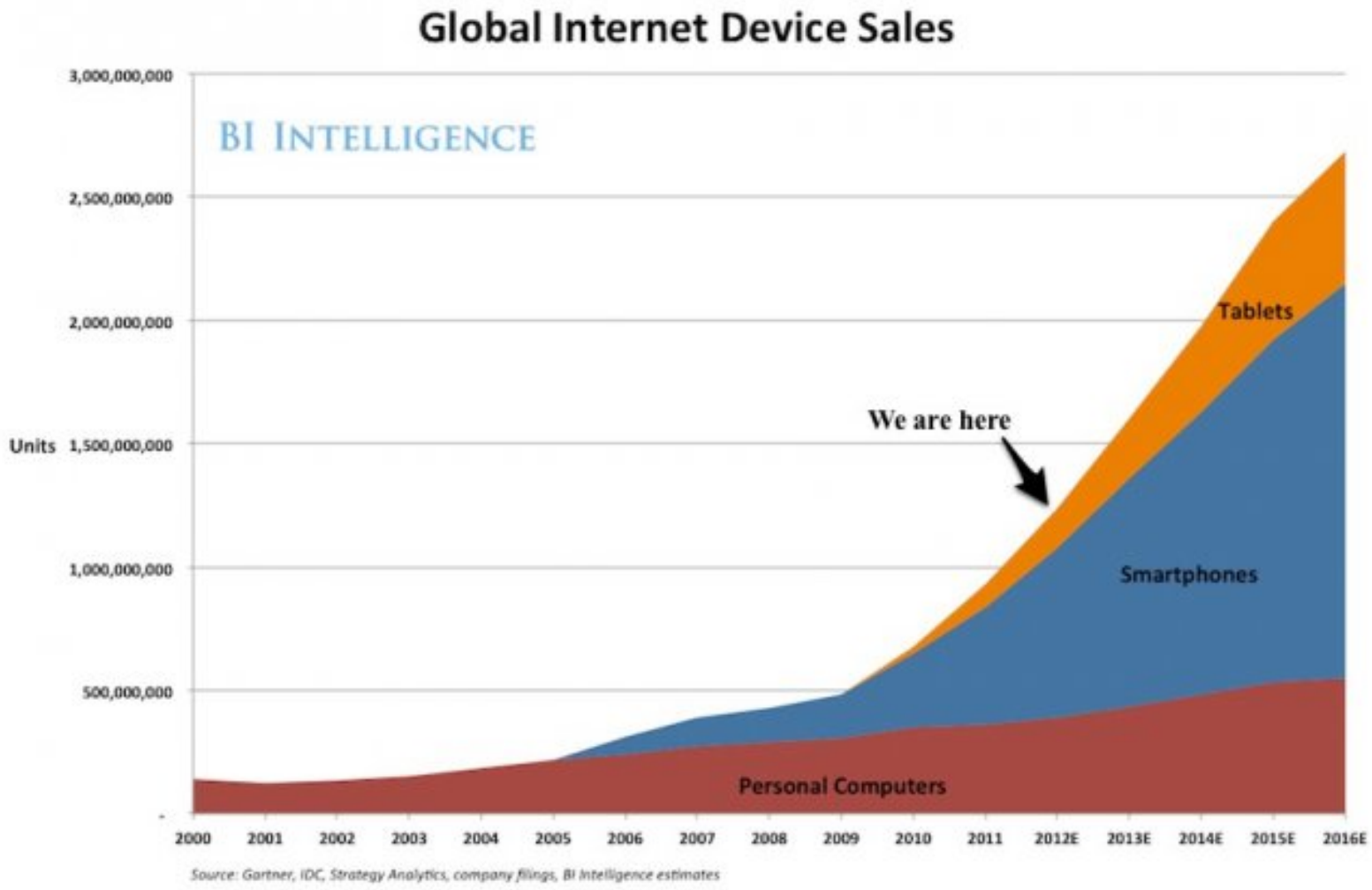
"Consumerization will be the most significant trend affecting IT during the next 10 years"

Gartner

Consumerization of IT
IT消費化

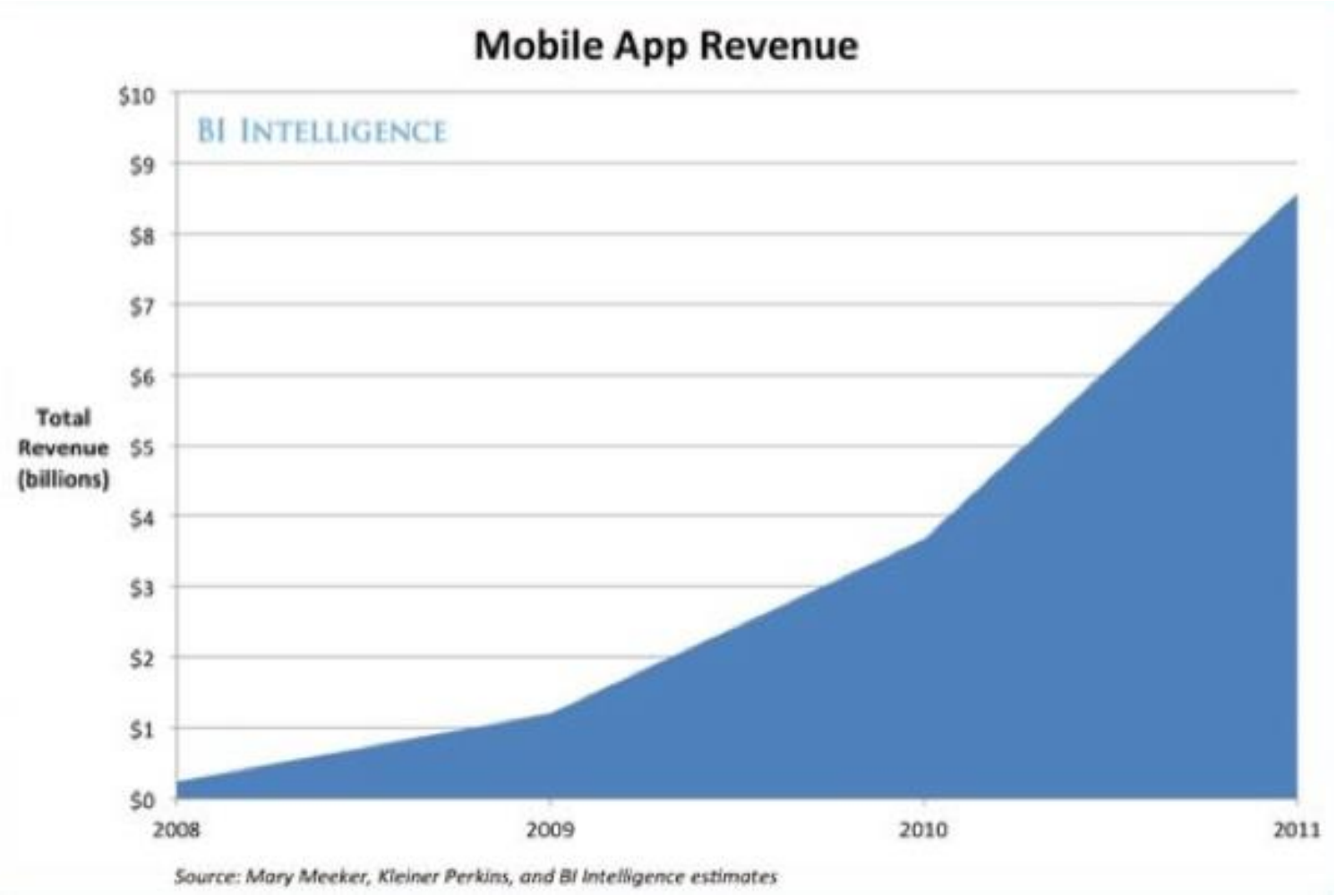
- IT消費化勢不可擋，電腦提供了每個人快速溝通、電子公務等功能。但隨著工作的需求，出差、旅行、拜訪客戶等，筆記型電腦的重量與續航性顯得更為艱鉅，流動裝置將是未來解決此類問題。
- 基於市場數據顯示，在2012年Smart Phone出貨量已經超越PC達到了4.8億台，而PC的出貨量下修到4.1億，其中一部分還是平板式電腦。
- IT消費化並不僅是員工在工作時刻使用自己的流動裝置與應用，IT消費化的使用者已經成為內部IT應用的主要客群，未來IT要管理包含員工的自帶流動裝置會更佳困難。

流動市場：裝置數量增長快速



Smartphones/Tablets will Outsell PCs by 4X

流動市場：Apps 數量增長快速



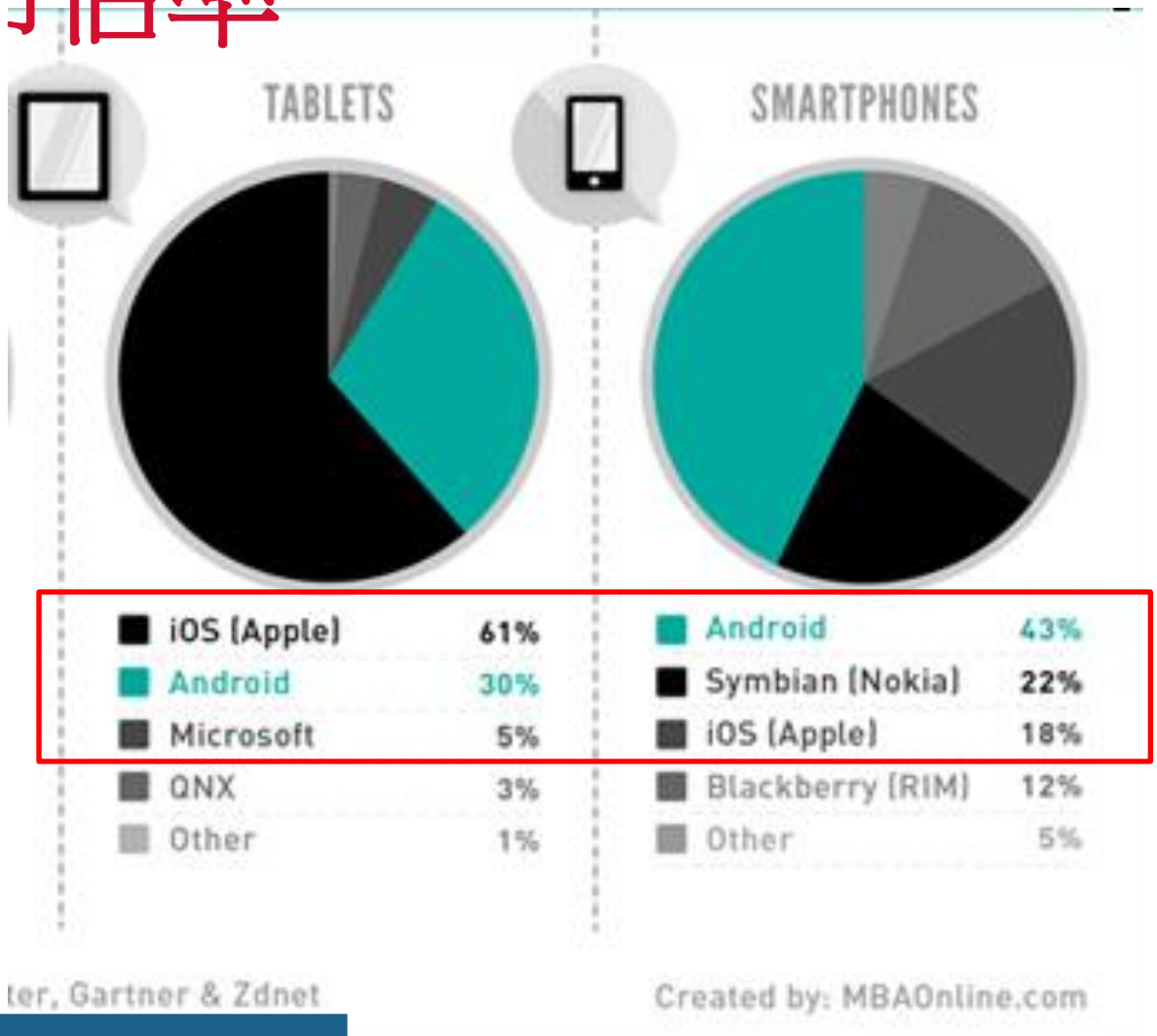
Mobile Apps is a $10B Market and Growing 100% per Year


Yes… They are real and growing!!
MOBILE MALWARE

Source: Brazilian Government

TREND MICRO

操作平台市佔率

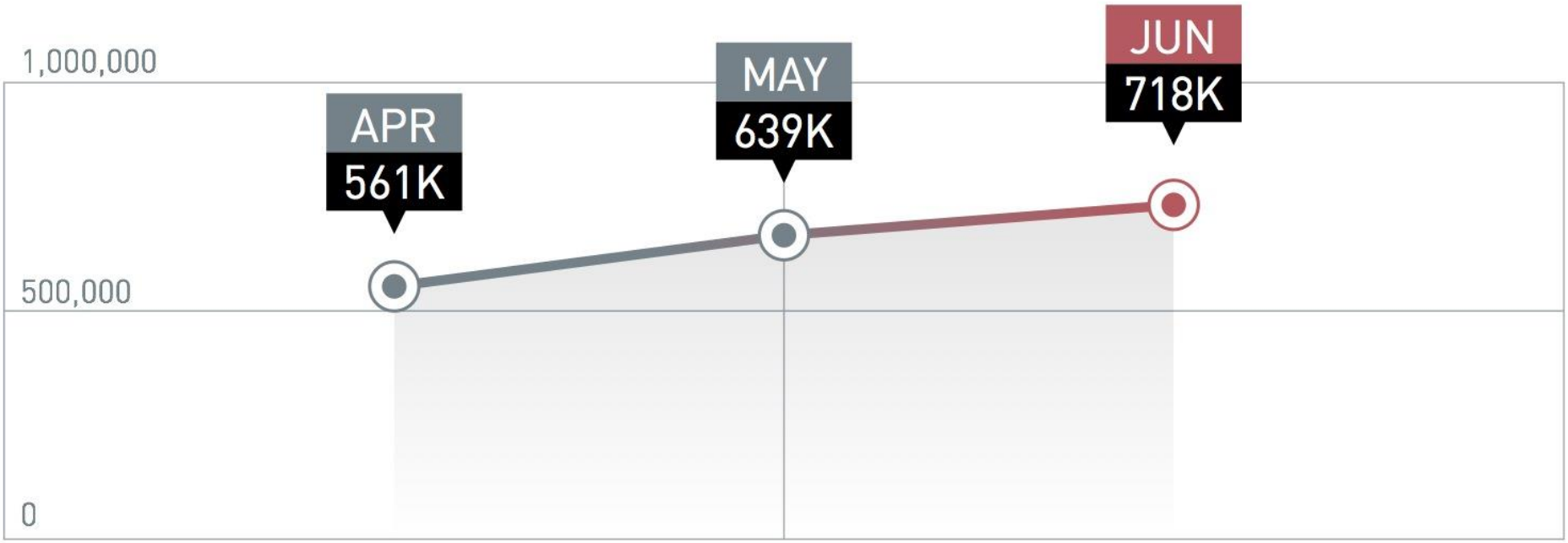


2012 (WW)		
Android	59%	152.9M Units
iOS	23%	

流動裝置惡意程式統計

- 15%: iPhone被破解的比例
- 400%: Android 在2012年中毒的成長率
- 挑戰:
  - 保護行動裝置
  - 偵測及攔阻惡意 apps
  - 保護企業IT資源被行動裝置感染

威脅數量持續增長



Android 威脅增長

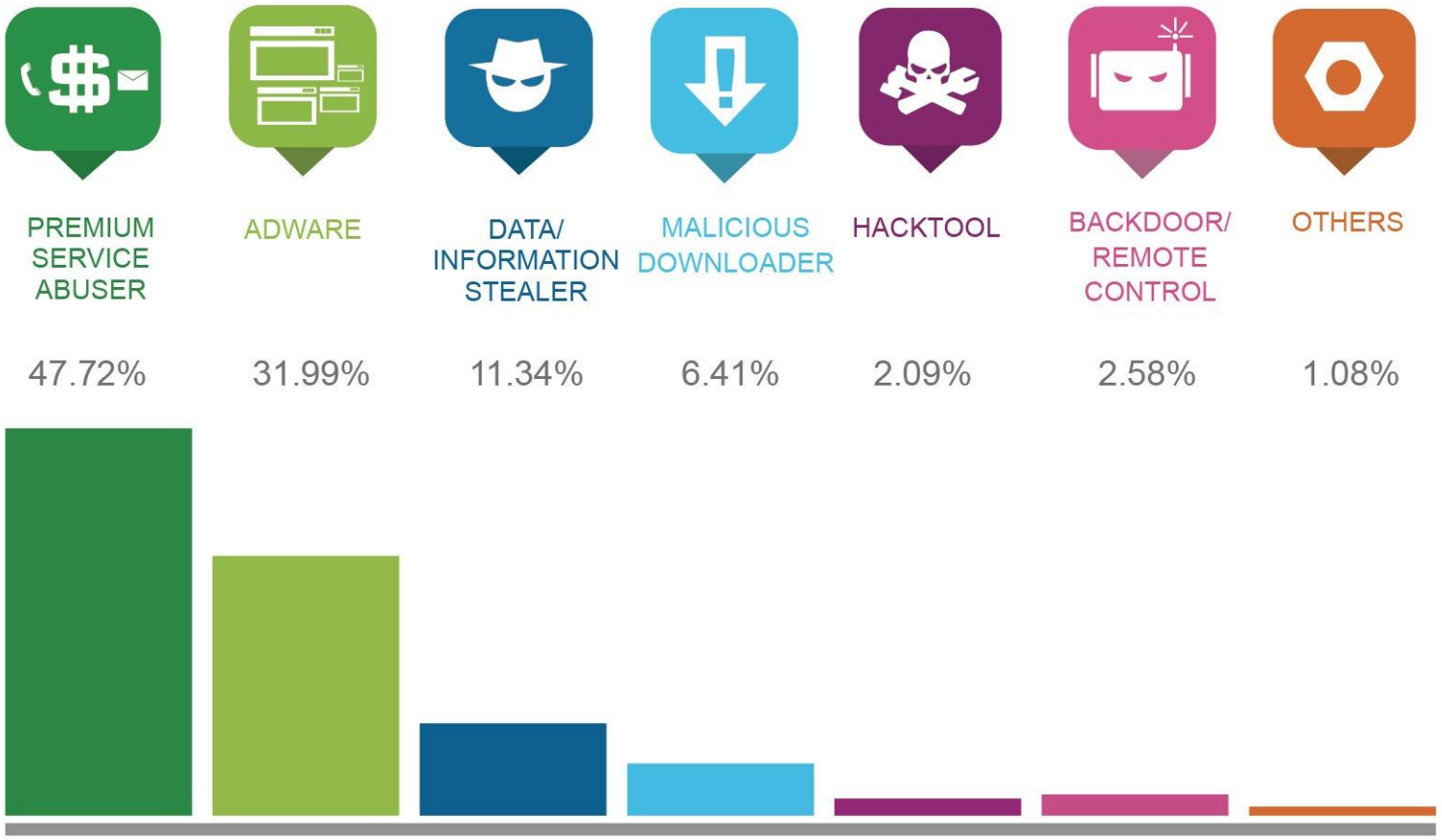
Source: Trend Micro Mobile Security Roundup 2012, January 2013

盜竊私隱程式最多的10個區域

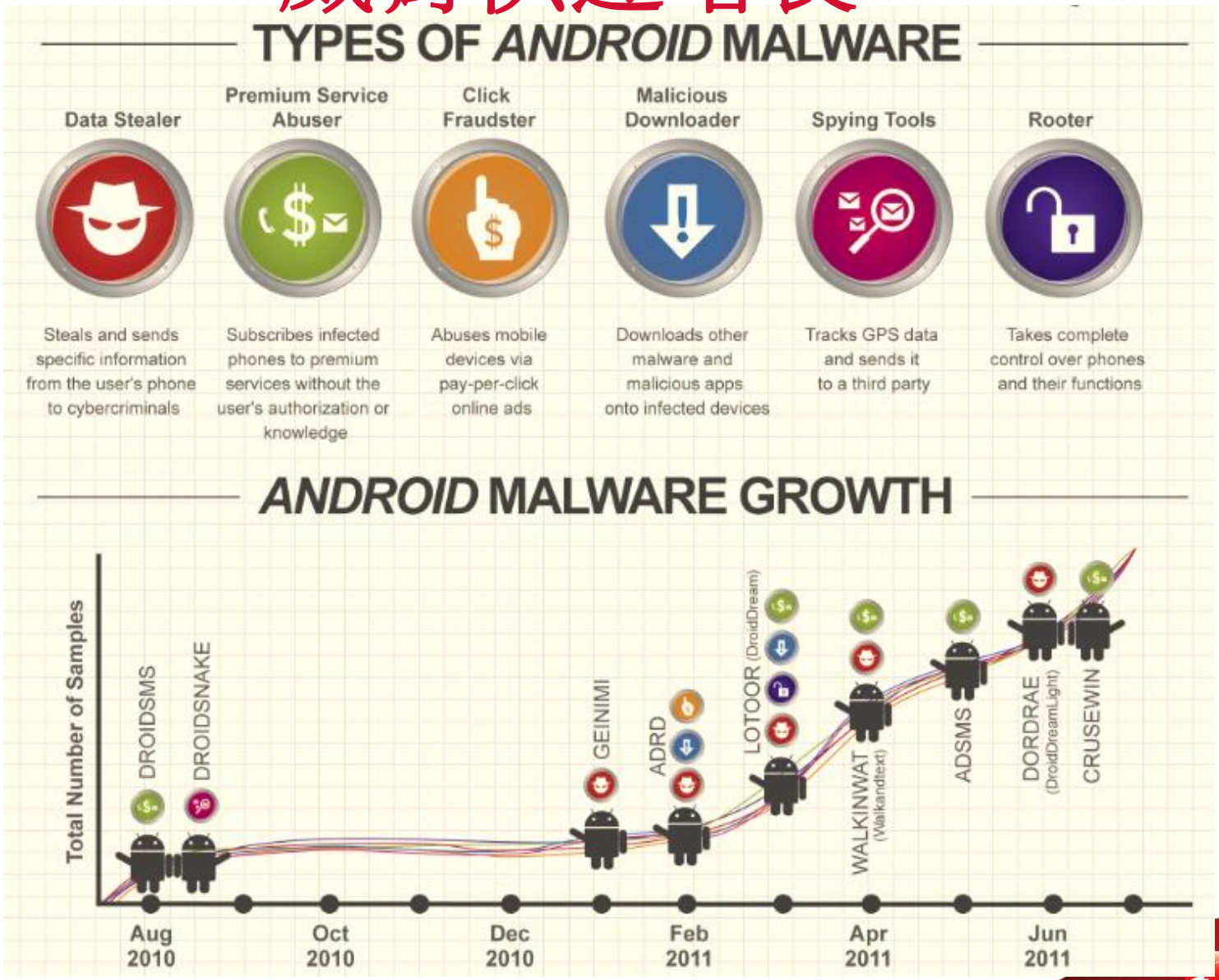
Source: Trend Micro Mobile Security Roundup 2012, January 2013

Ranking based on the percentage of apps rated as privacy risks over the total number of apps scanned per country.
Ranking limited to countries with at least 10,000 scans.
Rating based on yearly analysis of real-time threat detection via Trend Micro™ Mobile Security Personal Edition.

最常見的Android惡意程式



Android威脅快速增長



BYOV, BYOL, BYOM…

Common Mobile Threats

Malicious Marketplace – Social Engineering

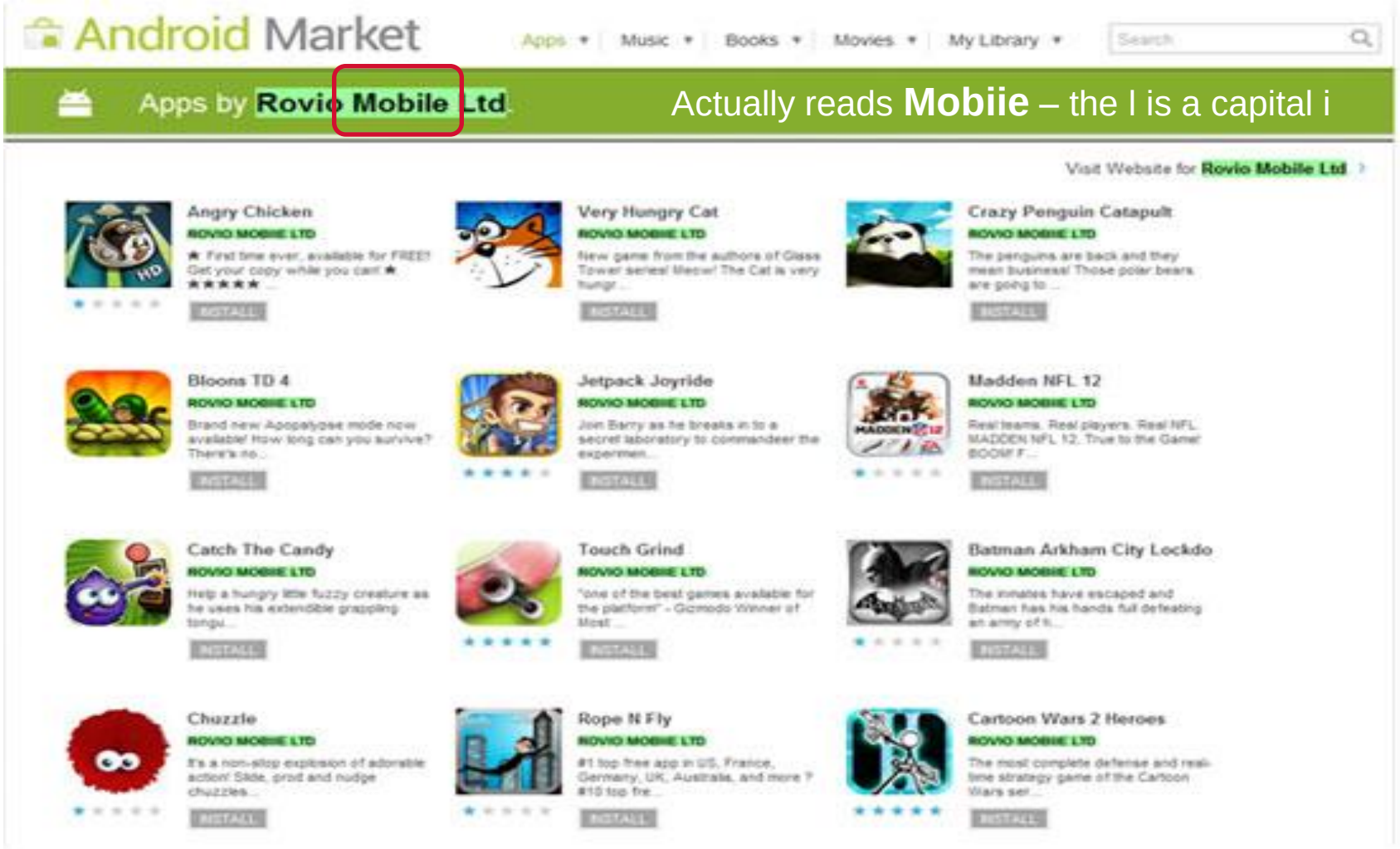


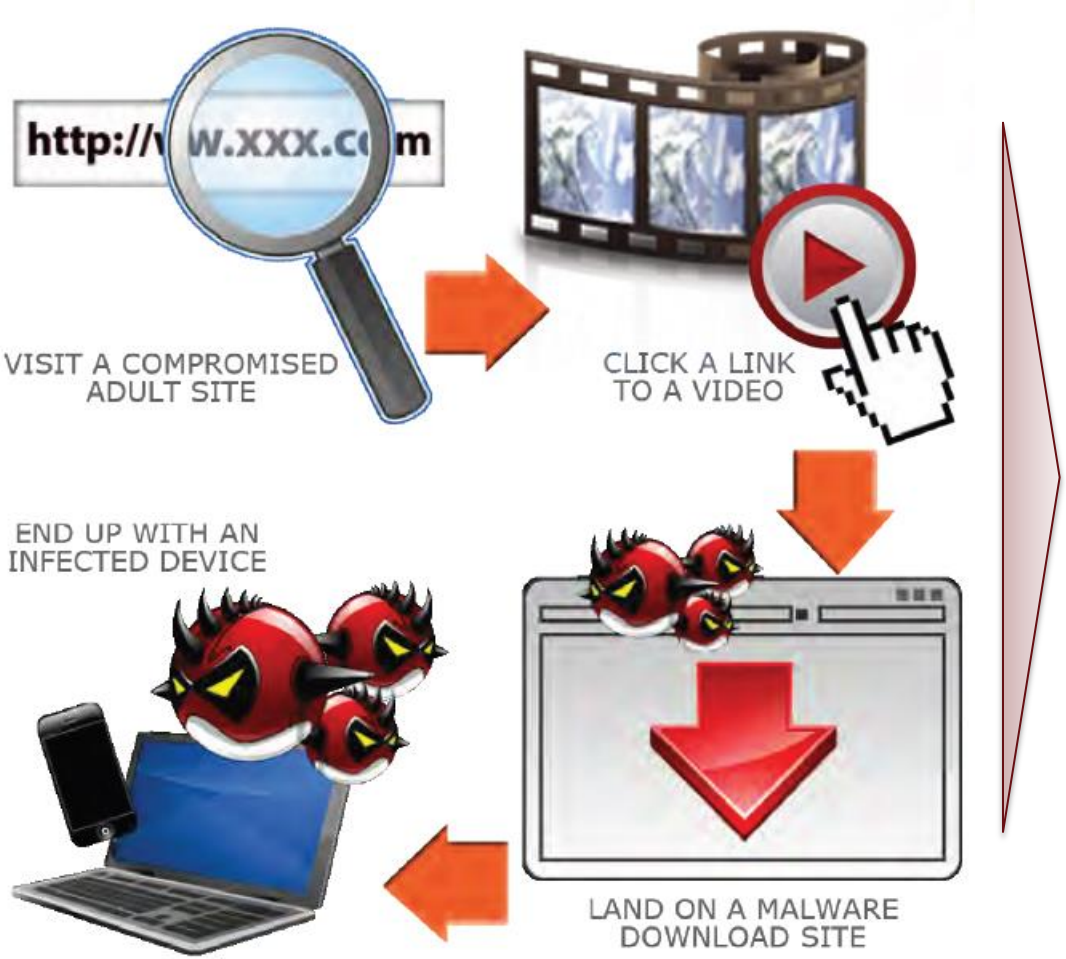
Figure 1. Apps supposedly offered by Rovio Mobile Ltd.

Fake GooglePlay

- **Full of Malicious Apps in those AppStores**

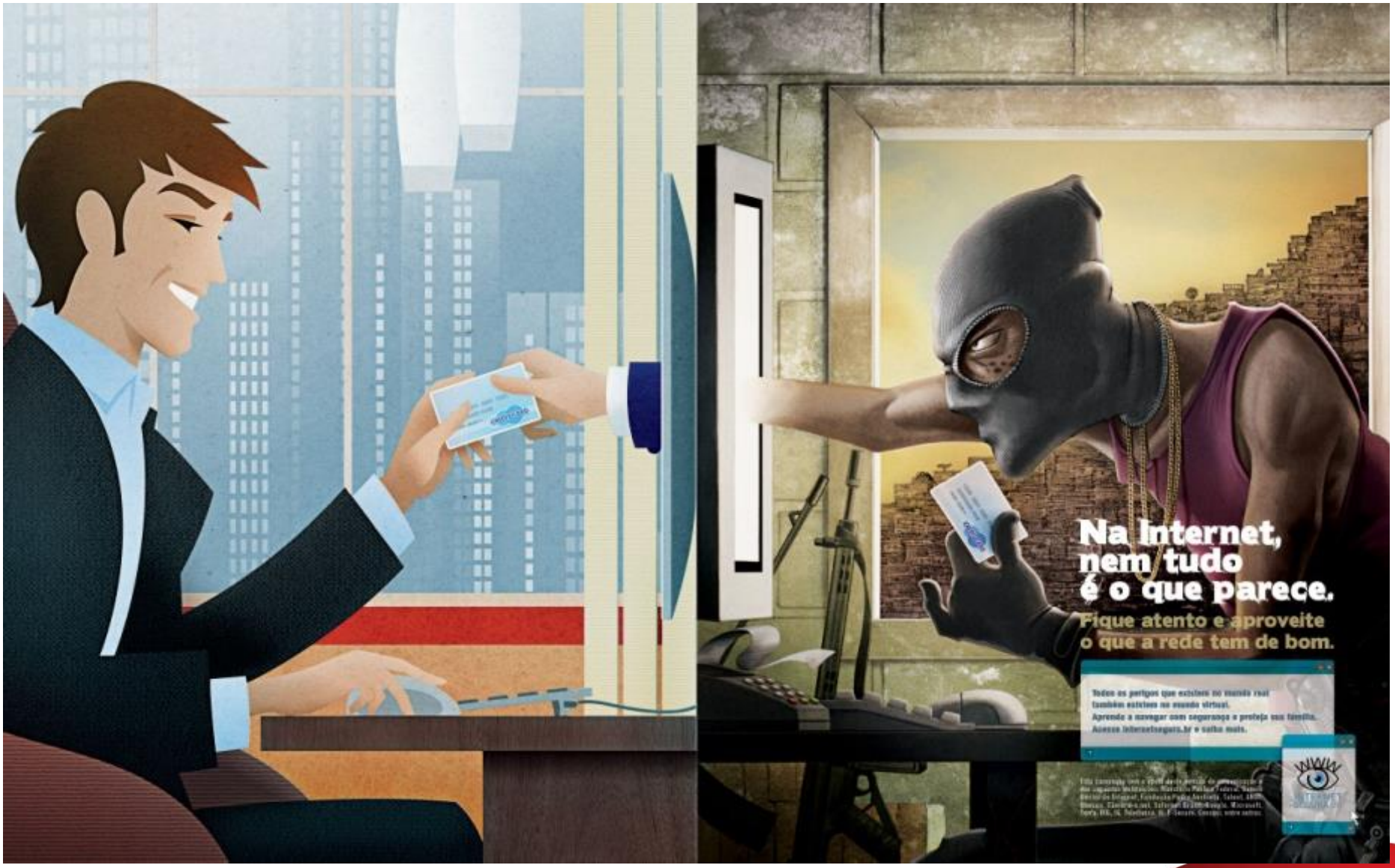
Source: TrendLab

One-Click Billing Fraud



Source: TrendLab

- **Japanese police arrested 6 suspects on one-click billing fraud campaign that netted ¥12M (US$148,800)**

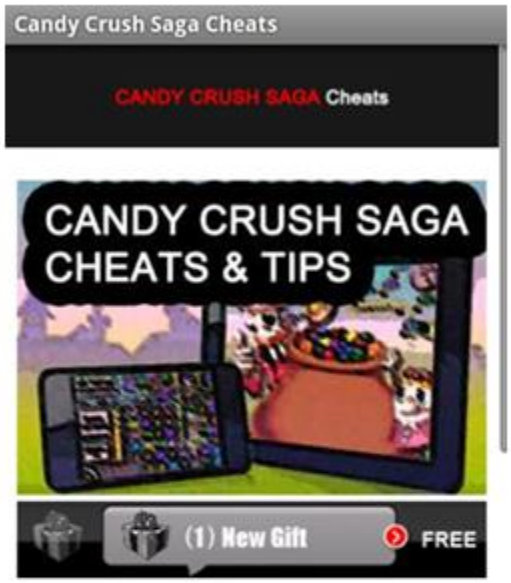

Na Internet,
nem tudo
é o que parece.
Fique atento e aproveite
o que a rede tem de bom.
Todos os perigos que existem no mundo real
também existem no mundo virtual.
Aprenda a navegar com segurança e proteja sua família.
Acesse internetseguro.br e saiba mais.

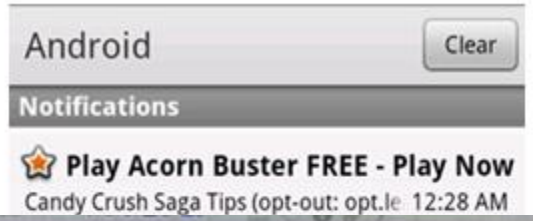
TREND MICRO


93% 12:13 下午
詳細資訊
蘋果動新聞
3.0.9
低度風險
此應用程式會從您的行動裝置搜集下列資訊並可能會透過網路將此資訊傳送出去
更多詳細資訊
IMEI
可能會利用您行動裝置的唯一識別碼來獲取您的資料
解除安裝
信任此應用程式


93% 12:14 下午
詳細資訊
Hong Kong Movie
1.28
低度風險
此應用程式會從您的行動裝置搜集下列資訊並可能會透過網路將此資訊傳送出去
更多詳細資訊
IMEI
可能會利用您行動裝置的唯一識別碼來獲取您的資料
解除安裝
信任此應用程式

Steals Personal Information





TREND MICRO

Mobile SPAM

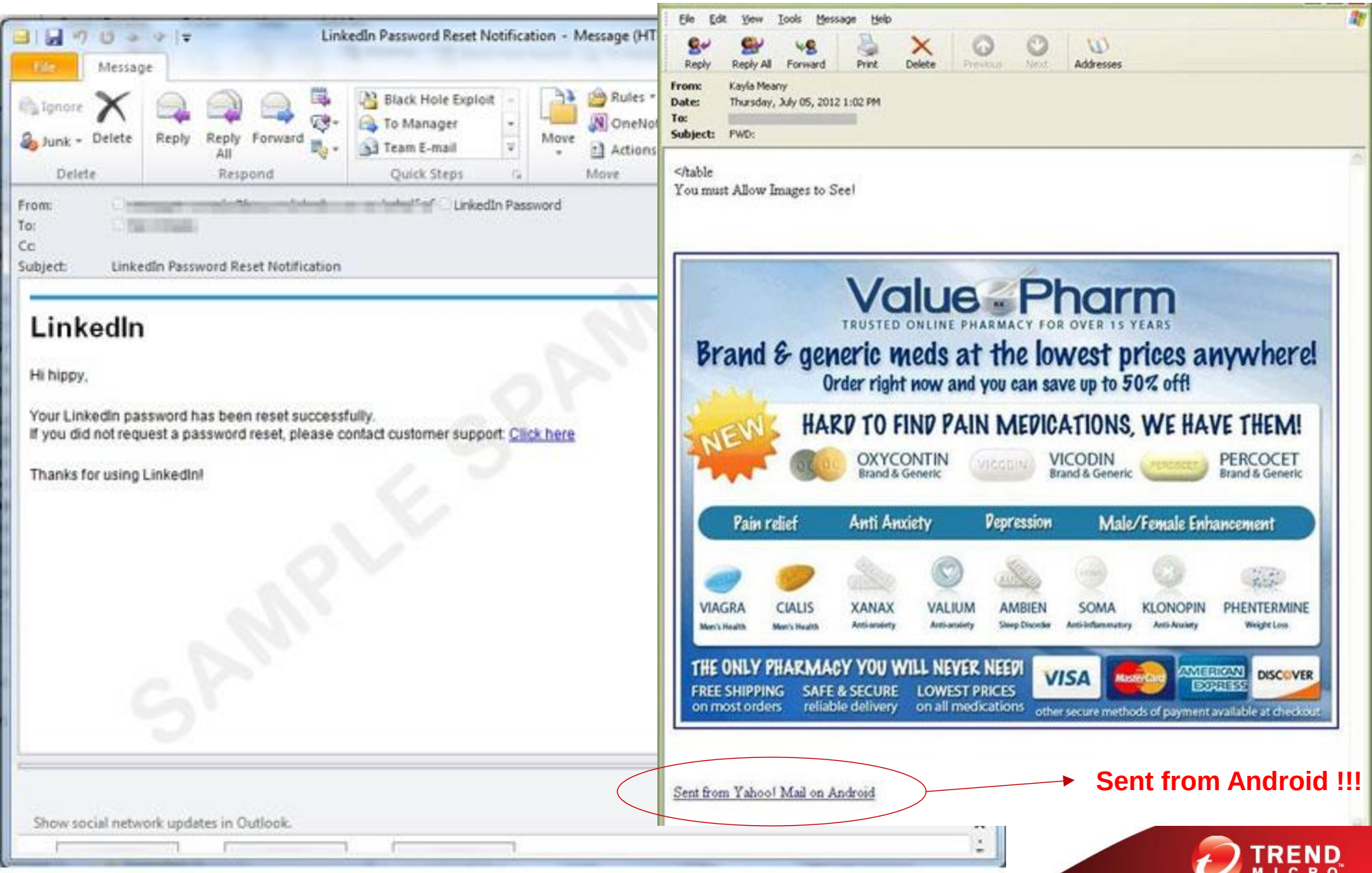
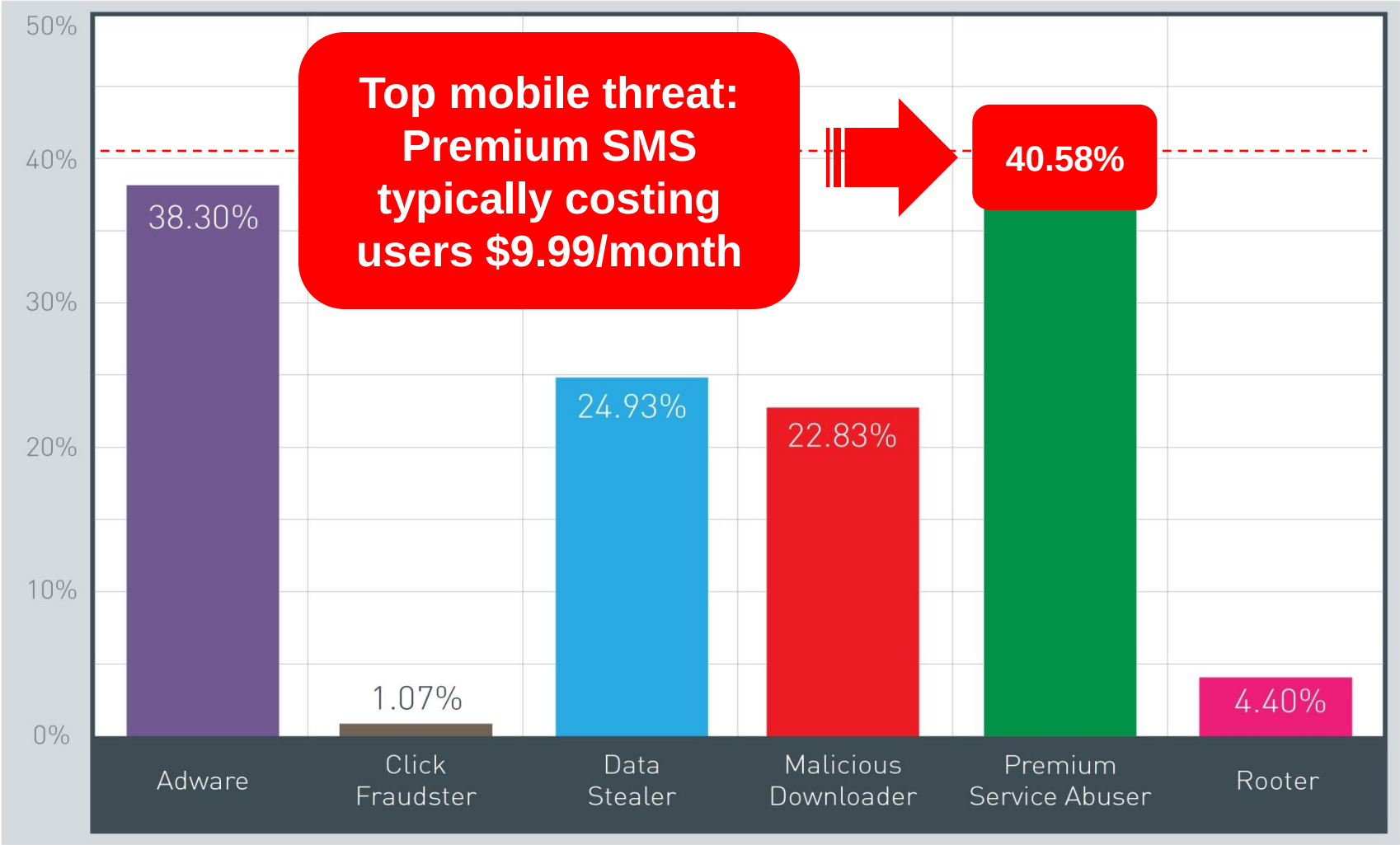


Figure 1. Spoofed *LinkedIn* email message

流動裝置安全威脅 – ROOT與越獄的風險

常見威脅類型



Source: Trend Micro Mobile Security Roundup 2012, January 2013

12 million iPhone and iPad device IDs hacked from the FBI, Anonymous claims

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com Do it!

Don't show me this again X

by Graham Cluley on September 4, 2012 | Comments (13)
FILED UNDER: Data loss, Featured, Law & order, Vulnerability

Hackers have published a collection of what they say is over a million Unique Device Identifiers (UDID), connected with Apple iPhones and iPads.

The data, claims the hackers, is just part of a larger database of 12,367,232 UDIDs, and personal information such as full names, cellphone numbers, addresses and zipcodes belonging to Apple customers. The data was allegedly stolen via a Java vulnerability from a laptop belonging to an FBI cybersecurity agent:

"During the second week of March 2012, a Dell Vostro

Mac電腦不再安全？

Flashback 偽裝為 Flash Player，感染 60 萬台 MAC

CNN Tech

SEARCH

POWERED BY Google

Justice | Entertainment | Tech | Health | Living | Travel | Opinion | iReport | Money » | Sports »

APPLE

Apple: Update will fix Mac 'Flashback' virus

April 13, 2012 | By Doug Gross, CNN

Share | Twitter | Email

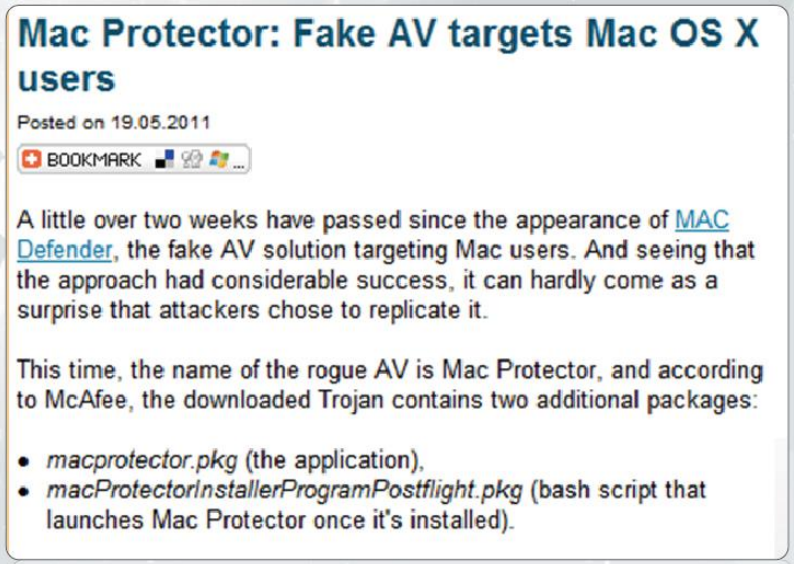
Recommend | 1,052 people recommend this. Be the first of your friends.

Apple says a new software update provides tools to get rid of the so-called "Flashback" virus that has infected hundreds of thousands of Mac computers.

In a post on its support forums, Apple said the update to the Java software platform "removes the most common variants" of the Flashback malware.

Mac用戶搜尋Google圖片被導向惡意網頁

SEO 黑帽搜尋引擎最佳化攻擊，利用 Google 的圖片搜索將 Mac 和 Windows 用戶分別轉向不同的惡意程式網頁



Mac Protector: Fake AV targets Mac OS X users

Posted on 19.05.2011

BOOKMARK

A little over two weeks have passed since the appearance of MAC Defender, the fake AV solution targeting Mac users. And seeing that the approach had considerable success, it can hardly come as a surprise that attackers chose to replicate it.

This time, the name of the rogue AV is Mac Protector, and according to McAfee, the downloaded Trojan contains two additional packages:

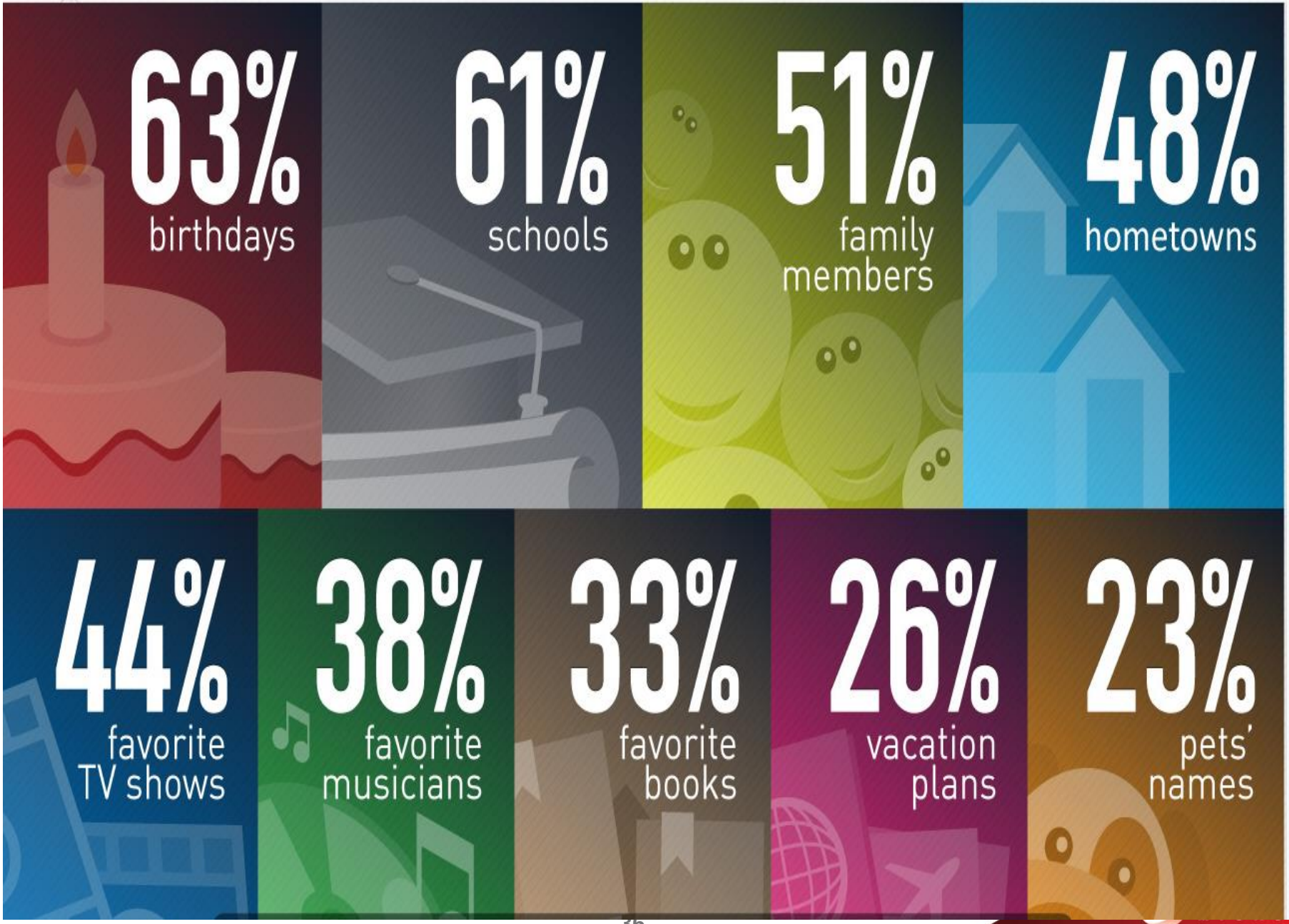
- *macprotector.pkg* (the application),
- *macProtectorInstallerProgramPostflight.pkg* (bash script that launches Mac Protector once it's installed).

TREND MICRO 趨勢科技

The Social Networking

社交網站泛濫

TREND MICRO



案例分享 – 當Facebook的帳號外洩後

即時新聞 | 要聞 | 20130425 | Facebook易洩私隱 僅37%設限

Facebook易洩私隱 僅37%設限

讚 35

建立時間: 0425 18:04

昔日東方 返回今日 電子報 即時新聞 東方新版意見箱 1

2011年2月20日 星期日

facebook公開電話號碼洩私隱 上一則 下一則

facebook公開電話號碼洩私隱

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

私隱政策聲明 搜尋 網站指南

- 公署簡介
- 個人資料 (私隱) 條例
- 2012年修訂條文
- 公署活動
- 資訊廊
- 個人資料私隱通識網
- 青少年專題網站
- 公署出版的刊物及錄影帶

晴報

主頁 | 港聞 | 娛樂 | 財經

今日晴報

相片自動上載Facebook易洩私隱

05/12/2012

網絡社交平台Facebook近日為了更方便智能手機用戶隨時分享生活片段，特地在旗下的Android與蘋果iOS手機App當中加入了一個名為「Photo Sync（照片同步）」的功能，時就不需要另外上載。

同樣的照片自動同步及上載功能，其實於Dropbox、iCloud，甚至被視作Facebook頭號對手的Google+上，都已不是甚麼新功能，只不過，出於香港人熱愛在Facebook事無大小都要分享的習慣，相信有不少用家均覺得這功能非常方便。

但方便之餘，這個功能亦有一定危險性。雖然在Photo Sync功能預設當中，所上載的照片不會即時公開，但我必須提一提大家，任何上載至Facebook平台的內容，在上載之時都被視作將版權交予Facebook，可以將照片用於宣傳而毋須知會用戶。（在登記時其實已有相關條文，只不過十之八九的用戶都沒詳細閱讀。）

換言之，用家在上載圖片時，你原來的「私照」將會成為Facebook工具，不想被人利用的話，這個Photo Sync功能還是不開為妙。

社交網站的風險

- 個人資訊外洩
  - 對社交逐漸失去控制
  - 共享資訊，如圖像或個人資料
    - 通過廣告、下載軟件鏈接、填寫調查盜取資料
    - 免費影片和音樂下載嵌入的木馬程式
- 不當的接觸
  - 網上誘騙
  - 網上欺凌
- 具侵略性或非授意的商業行為
  - 盜取信息
  - 垃圾電郵
  - 盜取身份
- 在本質上，社交網站活動會令人上癮

十大風險來源

TREND MICRO

充分準備: 一般用戶

- 使用暱稱或代號
- 將個人資料設定私人權限
- 小心守護個人資訊
- 慎思所要張貼的內容
- 保持更新資訊保安軟件
- 領會言外之音
- 避免親自會面
- 己所不欲勿施於人
- 適當對應
- 謹慎使用手機

如有懷疑，切勿點擊可疑連結或電郵

充分準備: 一般用戶

- 小心密碼被盜
  - 設定難於破解的密碼
  - 交替使用多組密碼
- 小心虛假訊息
  - 惡意連結
  - 殭屍網絡
- 小心守護個人資訊
  - 假如必須在網上填寫個人資訊，請只填入最基本的資料，並確認有關網站已經加密（即網址以https開始）
- 保持更新資訊保安軟件

充分準備: 機構管理層

- 在資訊保安系統定期測試中包含社交工程
- 保持更新資訊保安軟件
- 其他網上行為可能構成更大危機
  - Webmail（gmail 、 yahoo mail 、 hotmail）
  - 即時通訊（MSN 、 QQ 、 Skype）
  - 端到端及網上分享檔案（BT、Foxy）

• 你肯定Facebook會主動為你的隱私權把關嗎？

隱私不再重要？ 臉書CEO惹爭議

・聯合新聞網 2010/01/13

當紅社群網站Facebook近來因隱私權政策引發爭議，但執行長查克柏格（Mark Zuckerberg）顯然無懼於此。他日前表示，隨著人們習慣在網路上分享資訊，個人隱私的重要性逐漸降低。此話一出，輿情譁然。

【經濟日報／編譯余曉

個人隱私的重要性逐漸降低

當紅社群網站Facebook近
議，但執行長查克柏格（Mark Zucker
無懼於此。他日前表示，隨著人們習慣在網路上
分享資訊，個人隱私的重要性逐漸降低。此話一
出，輿情譁然。

Facebook執行長查克柏格（Mark Zuckerberg）。圖／經濟日報提供

25歲的查克柏格日前在2009年Crunchies頒獎典禮上，對著台下來自新創科技公司的聽眾表示，社會常規會改變，人們對隱私權的需求已不似過去那麼高。

查克柏格說：「剛起步時，人們常問我們『為何我要把個人資訊放到網路上』。但過去六年來，網路世界出現長足的進展，人們愈來愈習慣在網路上和更多人公開分享各種資訊。」他接著說，Facebook向來致力於調整政策，以跟上使用者的腳步，「我們持續創新，不斷更新系統，以反映當下的社會常規」。

TREND MICRO


MEMEBASE.COM

社交網站自衛術

不要亂加新朋友

不要亂按 

不要亂參加活動

Q & A

Thank You