行動應用App資安漏洞檢測與惡意App檢測

孫宏民 教授

資訊安全實驗室

國立清華大學資訊工程系

檢測技術

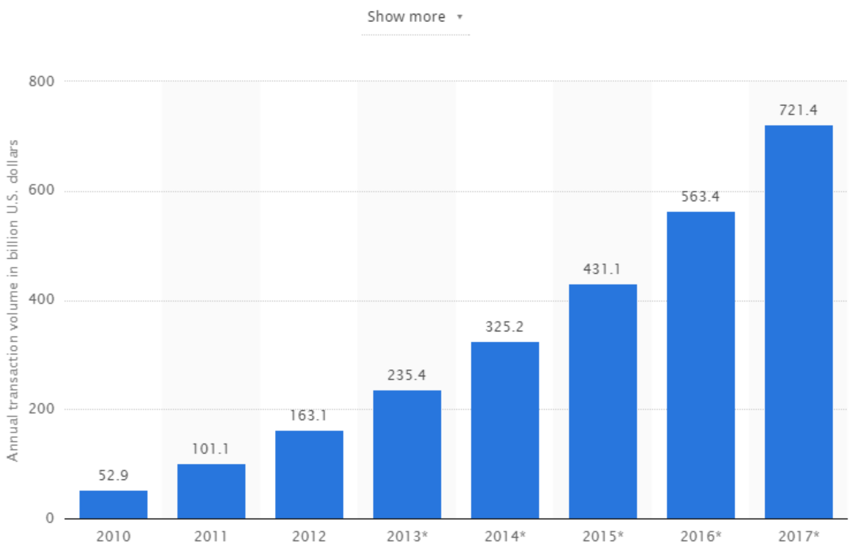
- App安全漏洞偵測
- 惡意軟體檢測

App安全漏洞偵測

背景說明

- 2015年Android手機出貨量為10.6億 支，占整體智慧型手機比重超過8成（82.3%）
- Fortinet所公布的「2015全年網路威 脅報告」指出，約96.5%的行動惡意軟 體鎖定Android平台
- 趨勢科技表示，2014年Android惡意 App數量為400萬個，到2015年估計超過800萬個
- 手機資安客戶端軟體市場，到2017年 的市場規模估計為29 億 美金

行動支付維持雙位數成長動能



Gartner表示，2017年全球行動支付交易額將達**7214億美元** *(Gartner, 2013)*

全球行動支付使用人數將增加至**4億5000萬人** *(Gartner, 2013)*

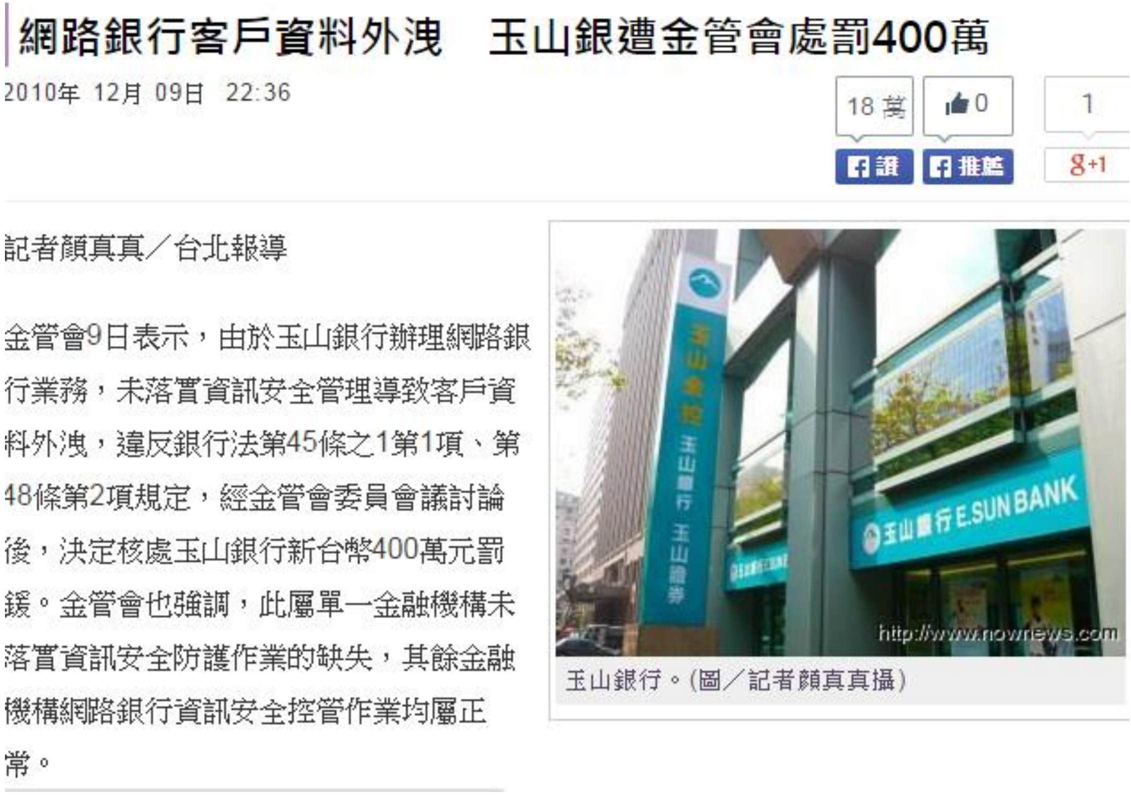
網銀 APP 面臨到的資安威脅

韓國農協銀行(NH Nonghyup Bank) 網銀 APP，遭Android 的 Master Key 漏洞攻擊

歹徒在第三方 App 程式下載網站上提供了一份惡意更新程式供人下載。此程式利用了 Android 的 Master Key 漏洞，在 App 程式內插入了一個惡意檔案，將它「木馬化」

造成個人資料外洩，還可能造成財務損失

銀行個資外洩遭處罰事件有前例可循



網路銀行客戶資料外洩　玉山銀遭金管會處罰400萬

2010年 12月 09日　22:36

記者顏真真／台北報導

金管會9日表示，由於玉山銀行辦理網路銀行業務，未落實資訊安全管理導致客戶資料外洩，違反銀行法第45條之1第1項、第48條第2項規定，經金管會委員會議討論後，決定核處玉山銀行新台幣400萬元罰鍰。金管會也強調，此屬單一金融機構未落實資訊安全防護作業的缺失，其餘金融機構網路銀行資訊安全控管作業均屬正常。

玉山銀行。(圖／記者顏真真攝)

- 金管會接獲有關訊息後，即要求玉山銀行應立刻採行有效的改善措施
- 玉山銀行稽核單位、及其所聘外部獨立的資安專家複核確認相關缺失均已完成改善
- 金管會也要求該行強化資本適足以因應作業風險發生之衝擊

但網銀APP 做好防範了嗎?
如APP 有漏洞，損失該由誰賠償？

APP 安全漏洞

- 導致用戶個資外洩。竊取使用者隱私。如獲取智慧手機使用者的簡訊、通話記錄、通訊錄等敏感個人資訊。大多數普通用戶對此並不知情。

- 用戶財產損失。支付類App的漏洞往往會給用戶帶來嚴重的財產損失。駭客通過破解支付類App，替換支付連結，誘導使用者向駭客人頭帳戶付費，或者直接竊取App帳號密碼，盜取資金，損害開發者及用戶利益。

- 山寨盜版橫行。80%的APP 都有對應的山寨版本。

傳統檢測面對的挑戰

自行購置源碼檢測工具

價格高昂，對一般中小企業用戶不敷負擔

需要成本低廉，準確度高的掃描服務

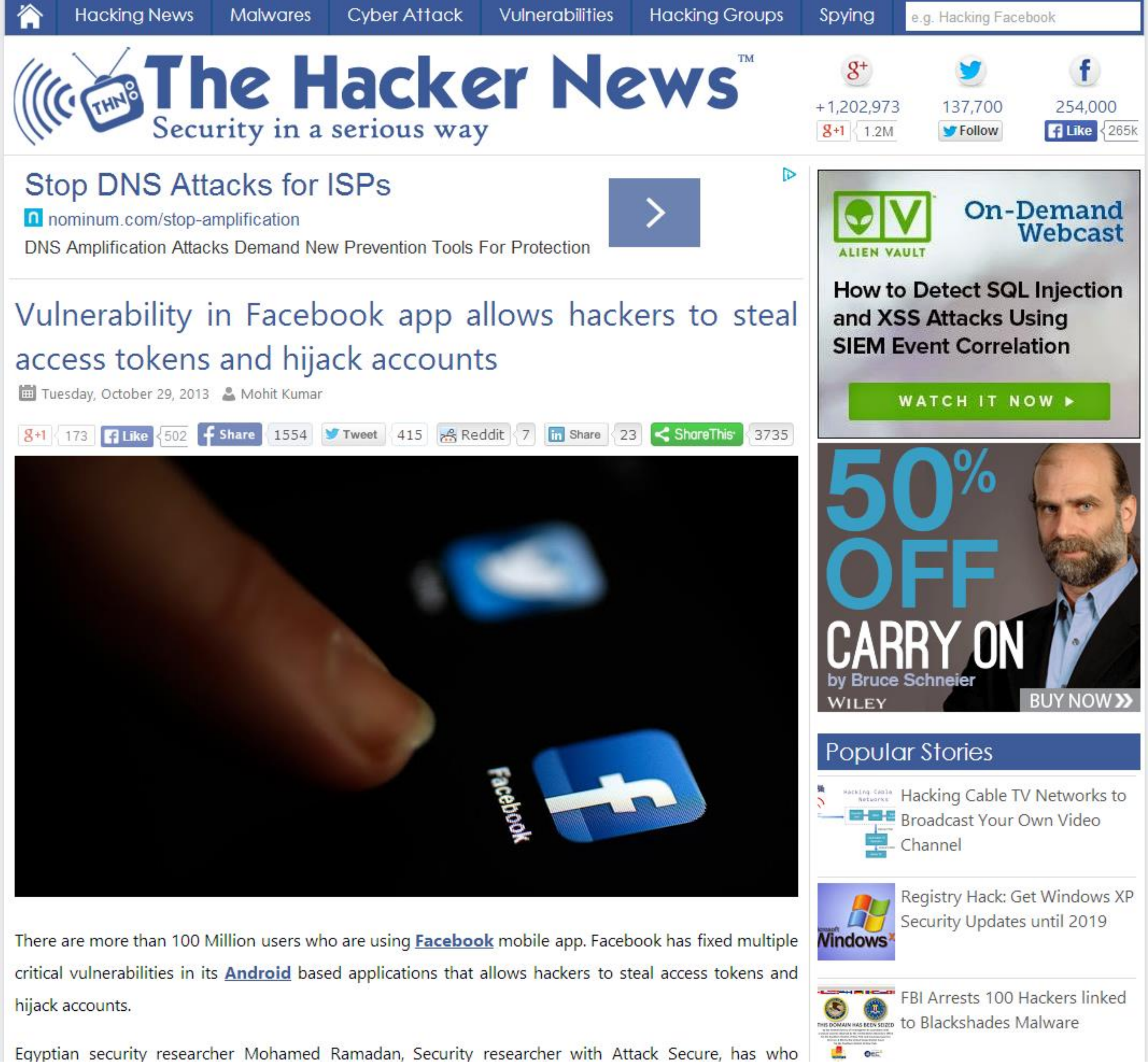
人工檢測費時費力，若沒有安全漏洞資料庫當樣本，所做出的錯誤檢測涵蓋率與準確率都會是問題

傳統的資安專家　≠　手機檢測專家

需要APP漏洞專業背景，快速檢測出安全弱點的服務

SECURITY HOLE EXAMPLES IN ANDROID APPS :

1. **Facebook**
2. **WhatsApp**
3. **Evernote**



The Hacker News™

Security in a serious way

Vulnerability in Facebook app allows hackers to steal access tokens and hijack accounts

Tuesday, October 29, 2013 Mohit Kumar

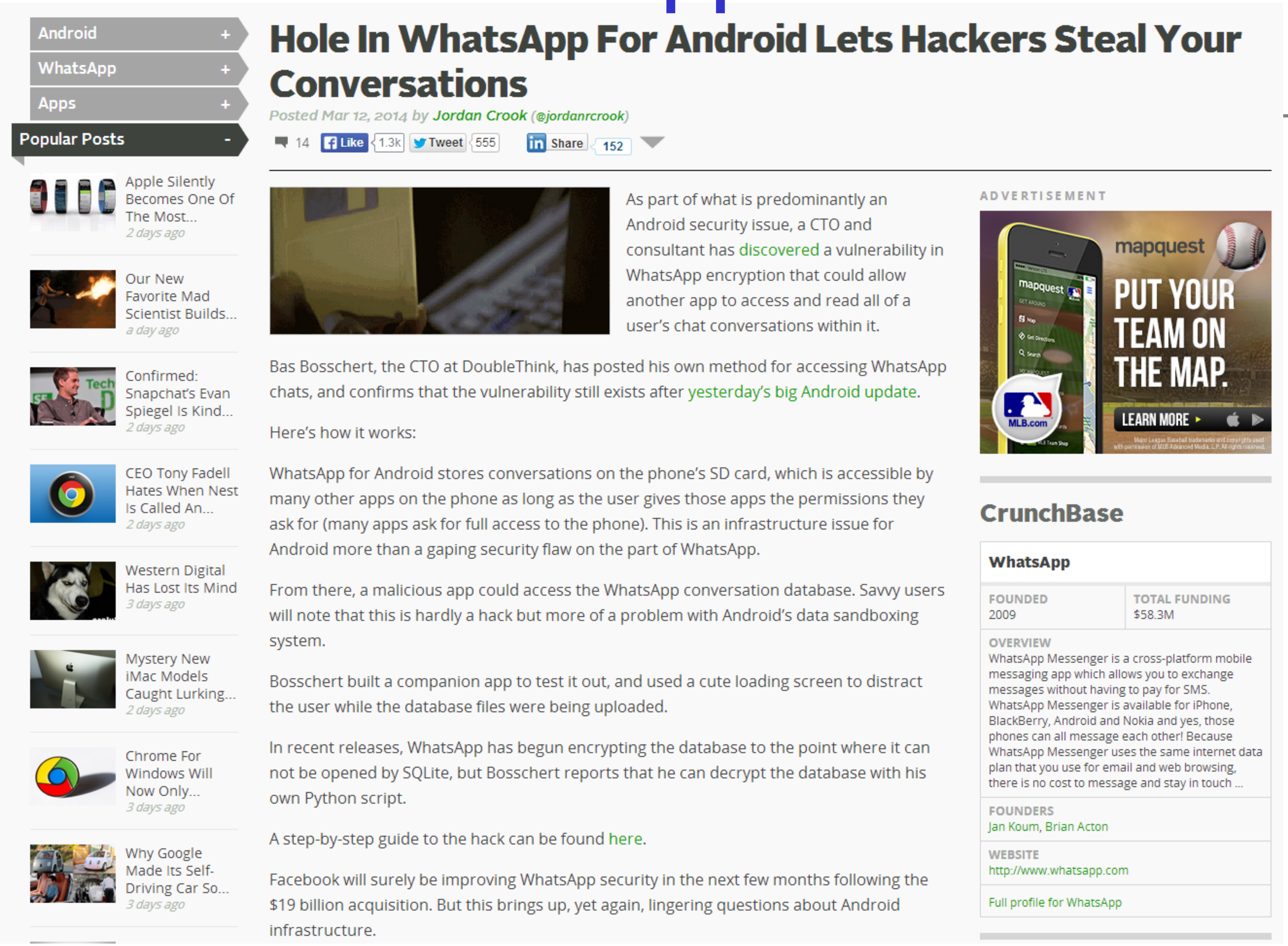
There are more than 100 Million users who are using **Facebook** mobile app. Facebook has fixed multiple critical vulnerabilities in its **Android** based applications that allows hackers to steal access tokens and hijack accounts.

Egyptian security researcher Mohamed Ramadan, Security researcher with Attack Secure, has who

Popular Stories

- Hacking Cable TV Networks to Broadcast Your Own Video Channel
- Registry Hack: Get Windows XP Security Updates until 2019
- FBI Arrests 100 Hackers linked to Blackshades Malware

WhatsApp



Apple Silently Becomes One Of The Most...
2 days ago

Our New Favorite Mad Scientist Builds...
a day ago

Confirmed: Snapchat's Evan Spiegel Is Kind...
2 days ago

CEO Tony Fadell Hates When Nest Is Called An...
2 days ago

Western Digital Has Lost Its Mind
3 days ago

Mystery New iMac Models Caught Lurking...
2 days ago

Chrome For Windows Will Now Only...
3 days ago

Why Google Made Its Self-Driving Car So...
3 days ago

Hole In WhatsApp For Android Lets Hackers Steal Your Conversations

Posted Mar 12, 2014 by Jordan Crook (@jordanrcrook)

As part of what is predominantly an Android security issue, a CTO and consultant has discovered a vulnerability in WhatsApp encryption that could allow another app to access and read all of a user's chat conversations within it.

Bas Bosschert, the CTO at DoubleThink, has posted his own method for accessing WhatsApp chats, and confirms that the vulnerability still exists after yesterday's big Android update.

Here's how it works:

WhatsApp for Android stores conversations on the phone's SD card, which is accessible by many other apps on the phone as long as the user gives those apps the permissions they ask for (many apps ask for full access to the phone). This is an infrastructure issue for Android more than a gaping security flaw on the part of WhatsApp.

From there, a malicious app could access the WhatsApp conversation database. Savvy users will note that this is hardly a hack but more of a problem with Android's data sandboxing system.

Bosschert built a companion app to test it out, and used a cute loading screen to distract the user while the database files were being uploaded.

In recent releases, WhatsApp has begun encrypting the database to the point where it can not be opened by SQLite, but Bosschert reports that he can decrypt the database with his own Python script.

A step-by-step guide to the hack can be found here.

Facebook will surely be improving WhatsApp security in the next few months following the $19 billion acquisition. But this brings up, yet again, lingering questions about Android infrastructure.

CrunchBase

WhatsApp

FOUNDED	TOTAL FUNDING
2009	$58.3M

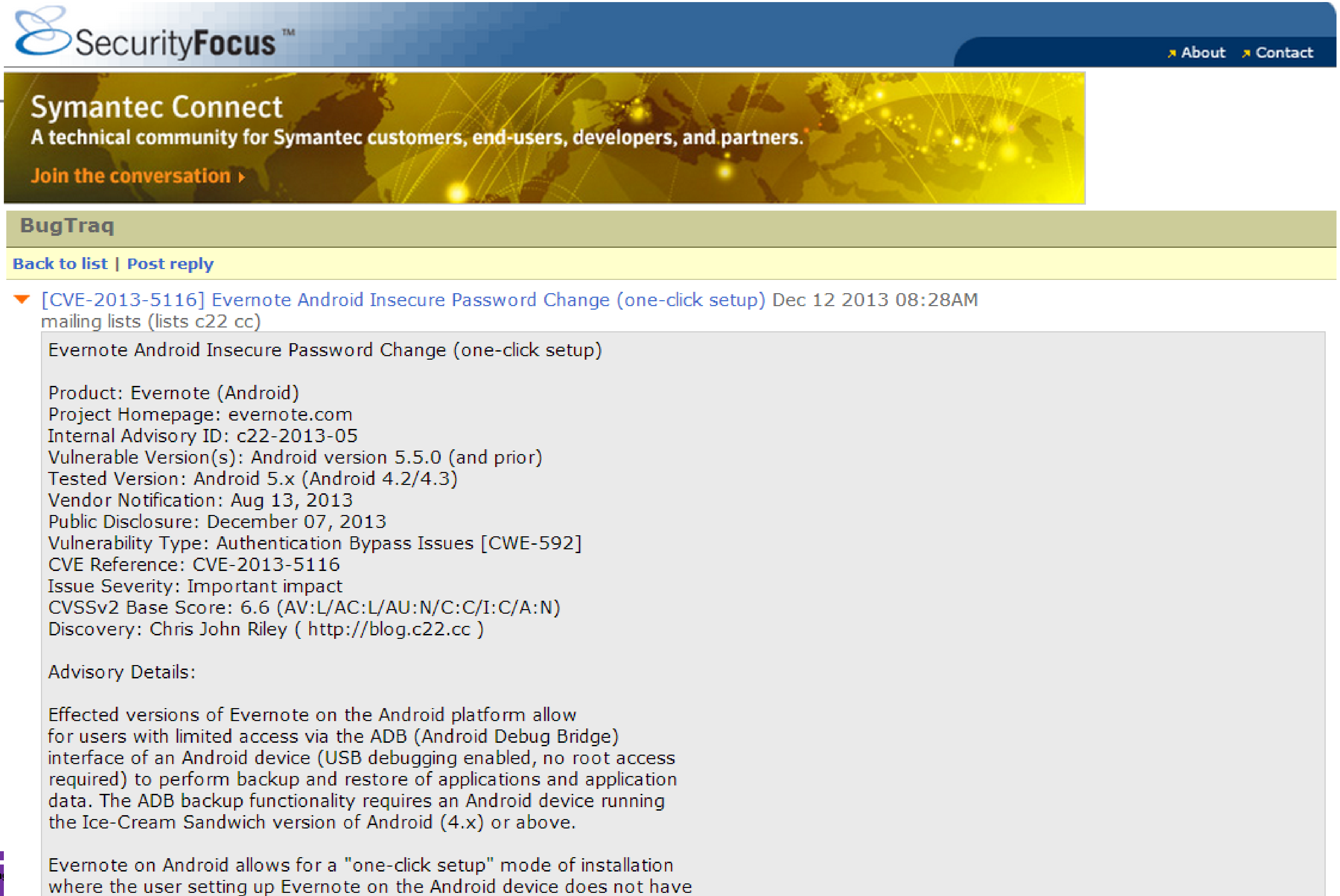
OVERVIEW
WhatsApp Messenger is a cross-platform mobile messaging app which allows you to exchange messages without having to pay for SMS. WhatsApp Messenger is available for iPhone, BlackBerry, Android and Nokia and yes, those phones can all message each other! Because WhatsApp Messenger uses the same internet data plan that you use for email and web browsing, there is no cost to message and stay in touch ...

FOUNDERS
Jan Koum, Brian Acton

WEBSITE
http://www.whatsapp.com

Full profile for WhatsApp

Evernote



BugTraq

Back to list | Post reply

[CVE-2013-5116] Evernote Android Insecure Password Change (one-click setup) Dec 12 2013 08:28AM
mailing lists (lists c22 cc)

Evernote Android Insecure Password Change (one-click setup)

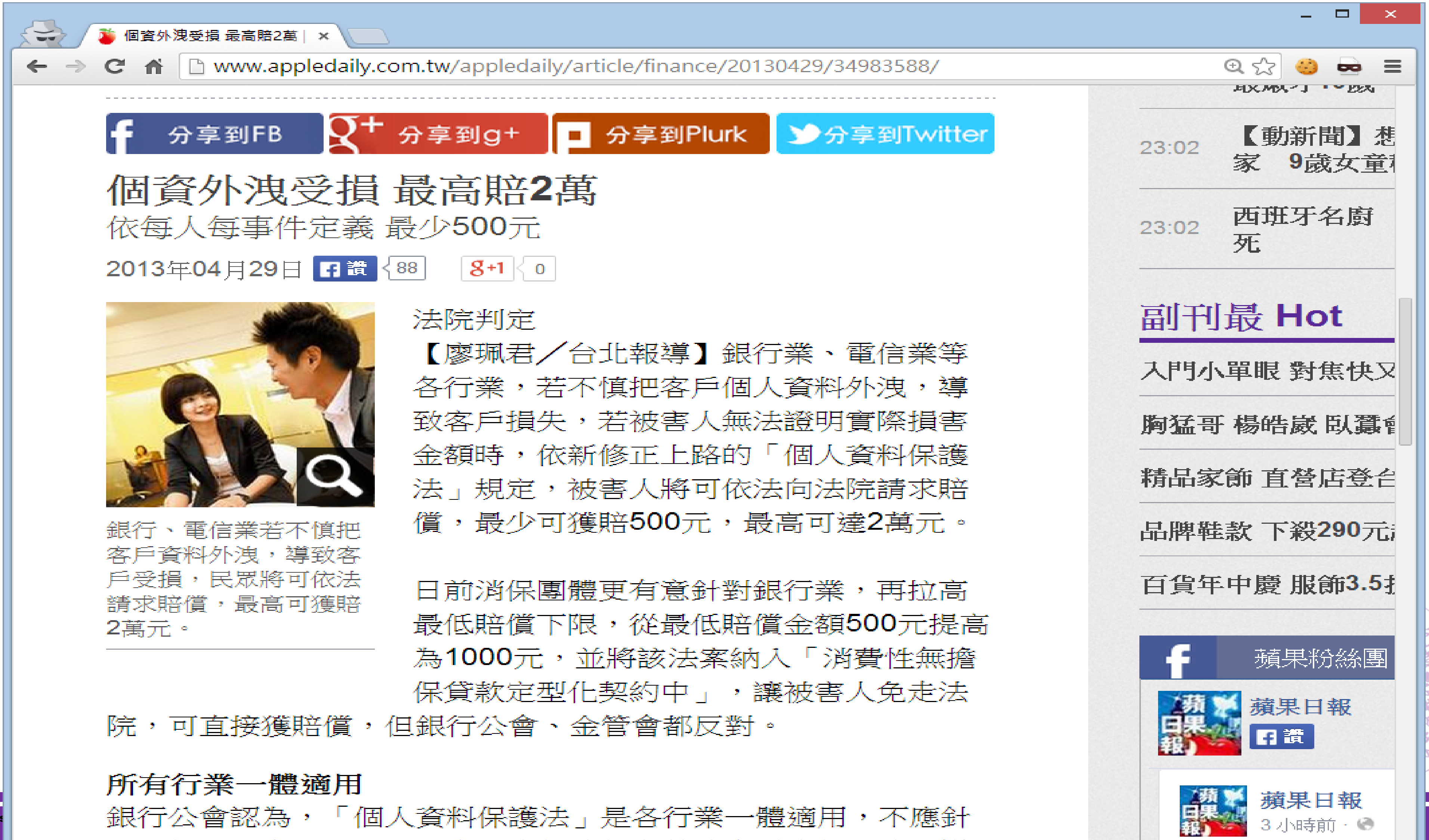
Product: Evernote (Android)
Project Homepage: evernote.com
Internal Advisory ID: c22-2013-05
Vulnerable Version(s): Android version 5.5.0 (and prior)
Tested Version: Android 5.x (Android 4.2/4.3)
Vendor Notification: Aug 13, 2013
Public Disclosure: December 07, 2013
Vulnerability Type: Authentication Bypass Issues [CWE-592]
CVE Reference: CVE-2013-5116
Issue Severity: Important impact
CVSSv2 Base Score: 6.6 (AV:L/AC:L/AU:N/C:C/I:C/A:N)
Discovery: Chris John Riley (http://blog.c22.cc)

Advisory Details:

Effected versions of Evernote on the Android platform allow for users with limited access via the ADB (Android Debug Bridge) interface of an Android device (USB debugging enabled, no root access required) to perform backup and restore of applications and application data. The ADB backup functionality requires an Android device running the Ice-Cream Sandwich version of Android (4.x) or above.

Evernote on Android allows for a "one-click setup" mode of installation where the user setting up Evernote on the Android device does not have

In Taiwan, a penalty of TWD$500-20,000 for leaking one user’s privacy is a law now.



個資外洩受損 最高賠2萬 |
www.appledaily.com.tw/appledaily/article/finance/20130429/34983588/
分享到FB
分享到g+
分享到Plurk
分享到Twitter

個資外洩受損 最高賠2萬

依每人每事件定義 最少500元

2013年04月29日

銀行、電信業若不慎把客戶資料外洩，導致客戶受損，民眾將可依法請求賠償，最高可獲賠2萬元。

法院判定

【廖珮君／台北報導】銀行業、電信業等各行業，若不慎把客戶個人資料外洩，導致客戶損失，若被害人無法證明實際損害金額時，依新修正上路的「個人資料保護法」規定，被害人將可依法向法院請求賠償，最少可獲賠500元，最高可達2萬元。

日前消保團體更有意針對銀行業，再拉高最低賠償下限，從最低賠償金額500元提高為1000元，並將該法案納入「消費性無擔保貸款定型化契約中」，讓被害人免走法院，可直接獲賠償，但銀行公會、金管會都反對。

所有行業一體適用

銀行公會認為，「個人資料保護法」是各行業一體適用，不應針

23:02 【動新聞】想家 9歲女童

23:02 西班牙名廚死

副刊最 Hot

入門小單眼 對焦快又

胸猛哥 楊皓崴 臥蠶

精品家飾 直營店登台

品牌鞋款 下殺290元

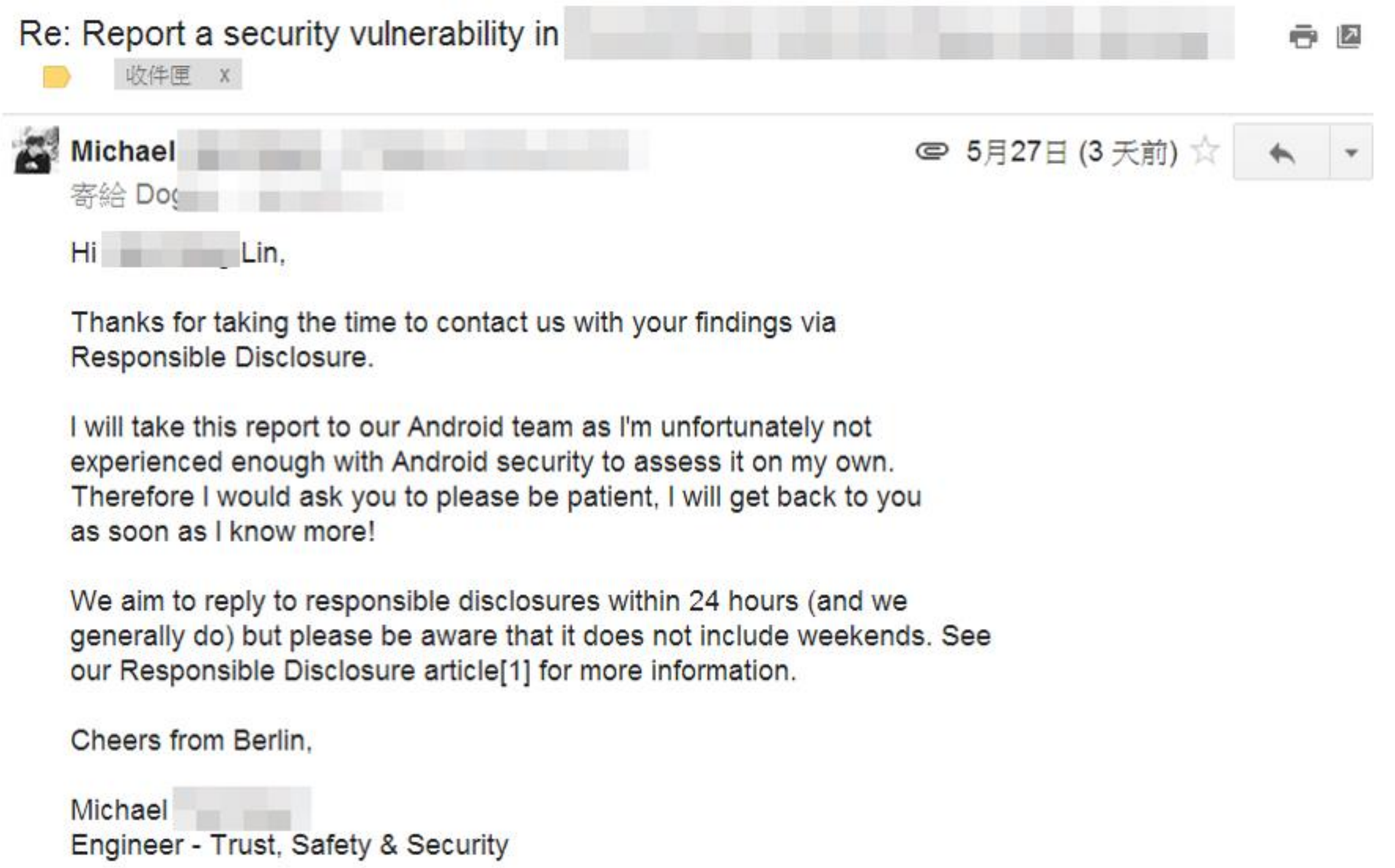
百貨年中慶 服飾3.5

BUT, MOST OF SECURITY EXPERTS ARE NOT FAMILIAR WITH MOBILE SECURITY.

They are familiar with XSS (Cross-site scripting) 、CSRF (Cross-site request forgery) 、SQL Injection、RCE (Remote Code Execution)… in desktop.

A well-known company is also not familiar with mobile security.

- 我們回報一個漏洞，這家公司的App有超過千



Re: Report a security vulnerability in [redacted]

Michael [redacted]

寄給 Do[redacted]

Hi [redacted] Lin,

Thanks for taking the time to contact us with your findings via Responsible Disclosure.

I will take this report to our Android team as I'm unfortunately not experienced enough with Android security to assess it on my own. Therefore I would ask you to please be patient, I will get back to you as soon as I know more!

We aim to reply to responsible disclosures within 24 hours (and we generally do) but please be aware that it does not include weekends. See our Responsible Disclosure article[1] for more information.

Cheers from Berlin,

Michael [redacted]
Engineer - Trust, Safety & Security

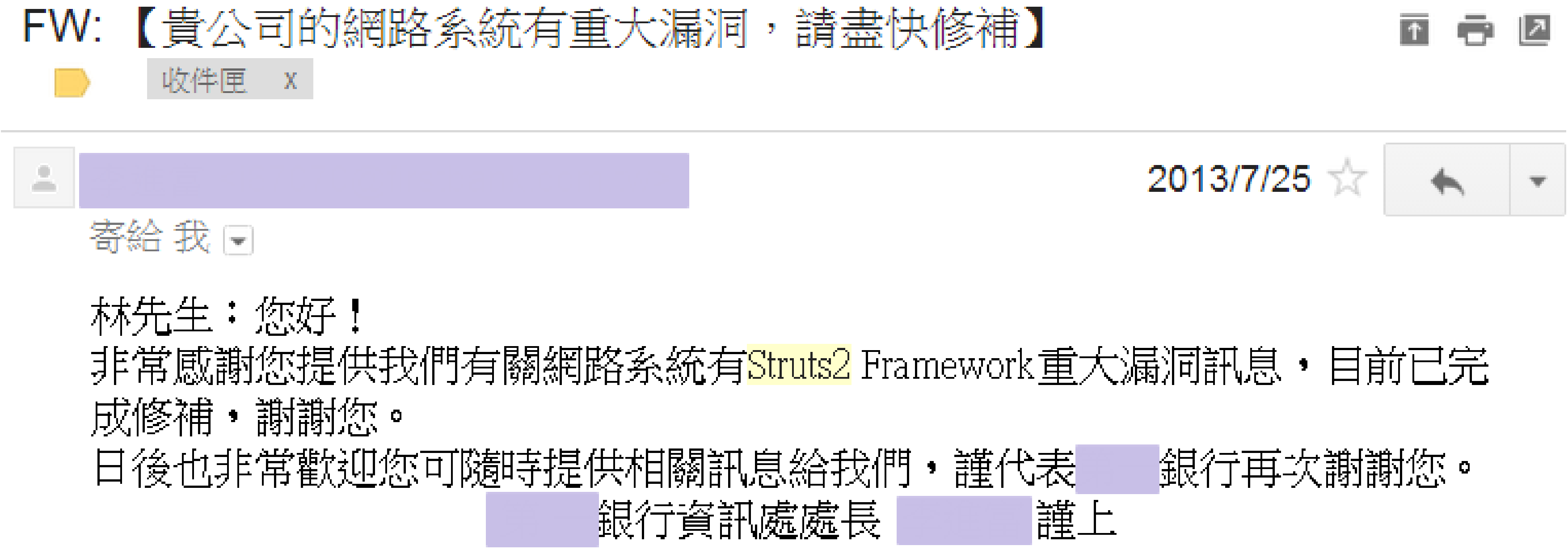
In fact, Microsoft Security Response Center (MSRC) doesn’t understand what mobile security holes are.

- Microsoft Security Response Center：「*If the user must install malware on their phone in order to encounter this issue, then Microsoft does not consider it a security vulnerability.*」
- In fact, Microsoft does not understand if an Android App doesn’t suffer from security holes, a malware can not do anything due to the isolations of APPs. This is the security design by Android operation system.
- After two weeks, Microsoft fixed this security holes, notified us, and gave us acknowledgement.

WE ANALYZE NOT ONLY NATIVE MOBILE APPLICATIONS，BUT ALSO WEB APPLICATIONS.

We reported back to a bank in Taiwan about Struts2 RCE bug (Java Web Framework)

感謝信from XX銀行資訊處處長



FW: 【貴公司的網路系統有重大漏洞，請盡快修補】

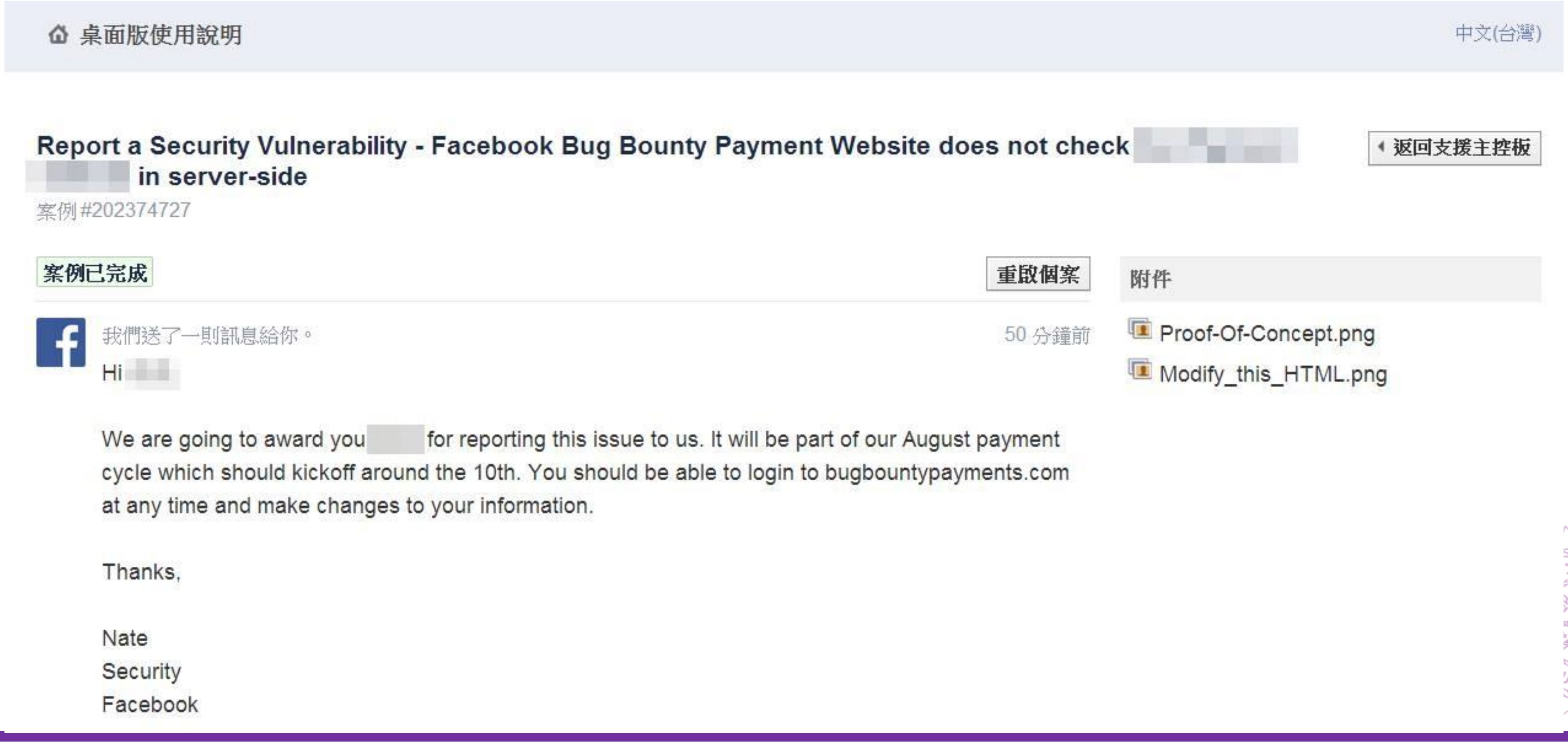
[redacted] 2013/7/25

寄給 我

林先生：您好！
非常感謝您提供我們有關網路系統有Struts2 Framework重大漏洞訊息，目前已完成修補，謝謝您。
日後也非常歡迎您可隨時提供相關訊息給我們，謹代表[redacted]銀行再次謝謝您。
[redacted]銀行資訊處處長 [redacted]謹上

Vulnerability in Facebook Bug Bounty Payment Website

- ❖Acknowledgement and reward from Facebook



Report a Security Vulnerability - Facebook Bug Bounty Payment Website does not check [redacted] in server-side

案例 #202374727

案例已完成

我們送了一則訊息給你。 50 分鐘前

Hi [redacted]

We are going to award you [redacted] for reporting this issue to us. It will be part of our August payment cycle which should kickoff around the 10th. You should be able to login to bugbountypayments.com at any time and make changes to your information.

Thanks,

Nate
Security
Facebook

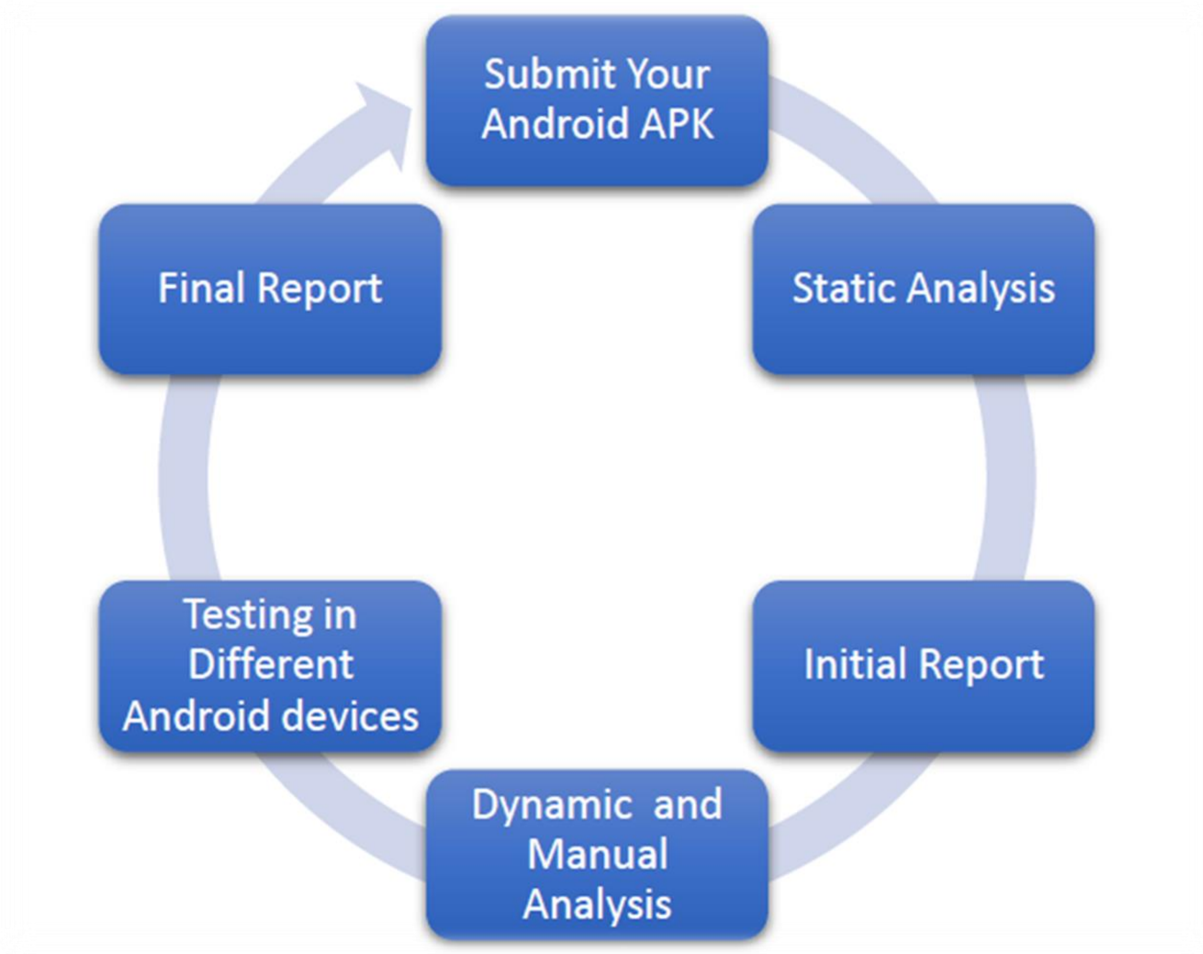
附件

- Proof-Of-Concept.png
- Modify_this_HTML.png

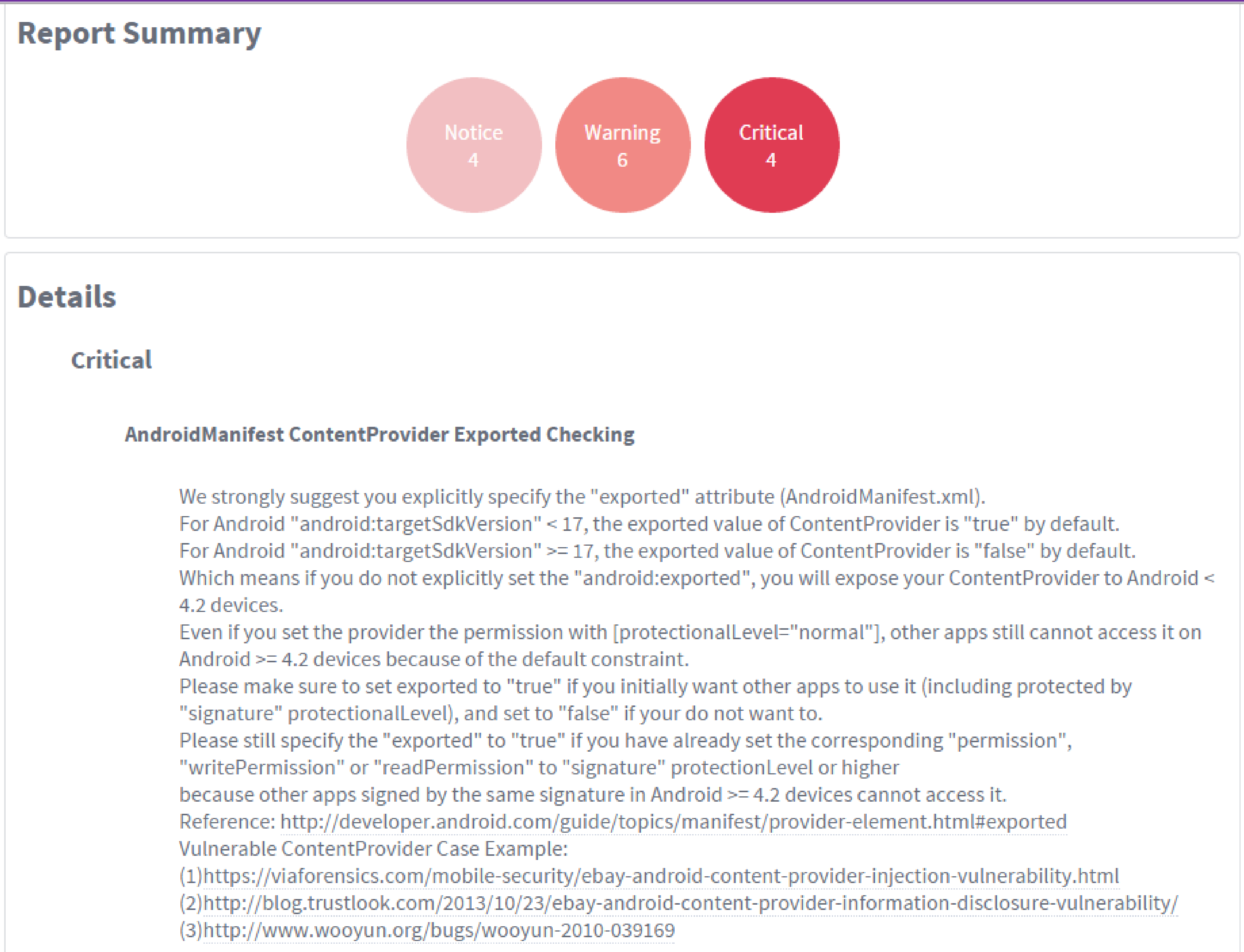
技術內容

- 我們開發了全世界第一套自動化APP 安全漏洞檢測系統 –
- 每天可分析10000支APP
- 不須原始碼 (Source)

How do we process the overall flow?



1. 開發者提交給我們Android APK
2. 透過我們開發的靜態分析檢測系統找到潛在的安全漏洞。
3. 我們透過逆向工程與動態分析來確認漏洞，這包含了在不同的裝置上完整的手動測試來評估App的安全風險。
4. 我們確認漏洞後將確認的漏洞、PoC、詳細說明、相關案例等製成最終報表。
5. 開發者修補完漏洞後將已修補的APK再交由我們測試以確認漏洞已修復。



Report Summary

Notice 4 | Warning 6 | Critical 4

Details

Critical

AndroidManifest ContentProvider Exported Checking

We strongly suggest you explicitly specify the "exported" attribute (AndroidManifest.xml).
For Android "android:targetSdkVersion" < 17, the exported value of ContentProvider is "true" by default.
For Android "android:targetSdkVersion" >= 17, the exported value of ContentProvider is "false" by default.
Which means if you do not explicitly set the "android:exported", you will expose your ContentProvider to Android < 4.2 devices.
Even if you set the provider the permission with [protectionalLevel="normal"], other apps still cannot access it on Android >= 4.2 devices because of the default constraint.
Please make sure to set exported to "true" if you initially want other apps to use it (including protected by "signature" protectionalLevel), and set to "false" if your do not want to.
Please still specify the "exported" to "true" if you have already set the corresponding "permission", "writePermission" or "readPermission" to "signature" protectionLevel or higher
because other apps signed by the same signature in Android >= 4.2 devices cannot access it.
Reference: http://developer.android.com/guide/topics/manifest/provider-element.html#exported
Vulnerable ContentProvider Case Example:
(1)https://viaforensics.com/mobile-security/ebay-android-content-provider-injection-vulnerability.html
(2)http://blog.trustlook.com/2013/10/23/ebay-android-content-provider-information-disclosure-vulnerability/
(3)http://www.wooyun.org/bugs/wooyun-2010-039169

快速、精準的檢測平台

5~15秒給您一份專業級的APP
安全檢測報告

- ☑ 程式碼安全漏洞
- ☑ APP 安全等級
- ☑ 漏洞修補建議
- ☑ 專業級的資安顧問

技術內容

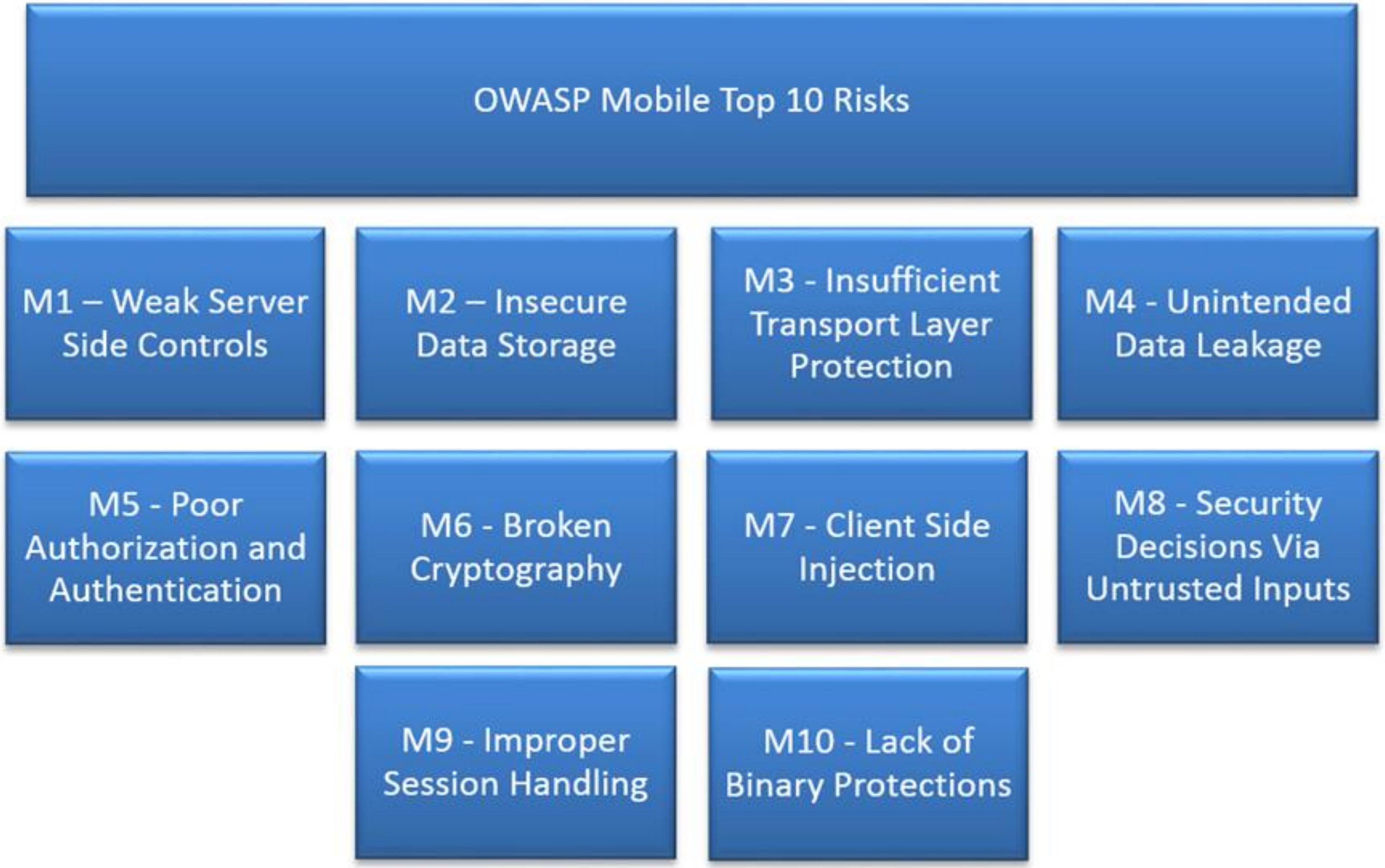
- 檢測行動裝置App是否存在安全漏洞
- 透過逆向工程來確認漏洞
- 將結果輸出成檢測報告，內容包括：
  - 檢測程式碼安全漏洞
  - App安全等級
  - 漏洞修補建議

檢測項目(OWASP Mobile 十大弱點風險)

- 弱伺服器端的控制 (Weak Server Side Controls)
- 不安全的資料儲存 (Insecure Data Storage)
- 傳輸層保護不足 (Insufficient Transport Layer Protection)
- 側通道資料洩漏(Unintended Data Leakage)
- 粗糙的授權與認證(Poor Authorization & Authentication)
- 加密失效(Broken Cryptography)
- 客戶端注入 (Client Side Injection)
- 安全決策是經由不受信任的輸入(Security Decisions via Untrusted Inputs)

檢測項目(Cont.)

- ❖不適當的會話處理(Session Handling)
- ❖執行碼缺乏保護(Lack of Binary Protection)



OWASP Mobile Top 10 Risks

M1 – Weak Server Side Controls

M2 – Insecure Data Storage

M3 - Insufficient Transport Layer Protection

M4 - Unintended Data Leakage

M5 - Poor Authorization and Authentication

M6 - Broken Cryptography

M7 - Client Side Injection

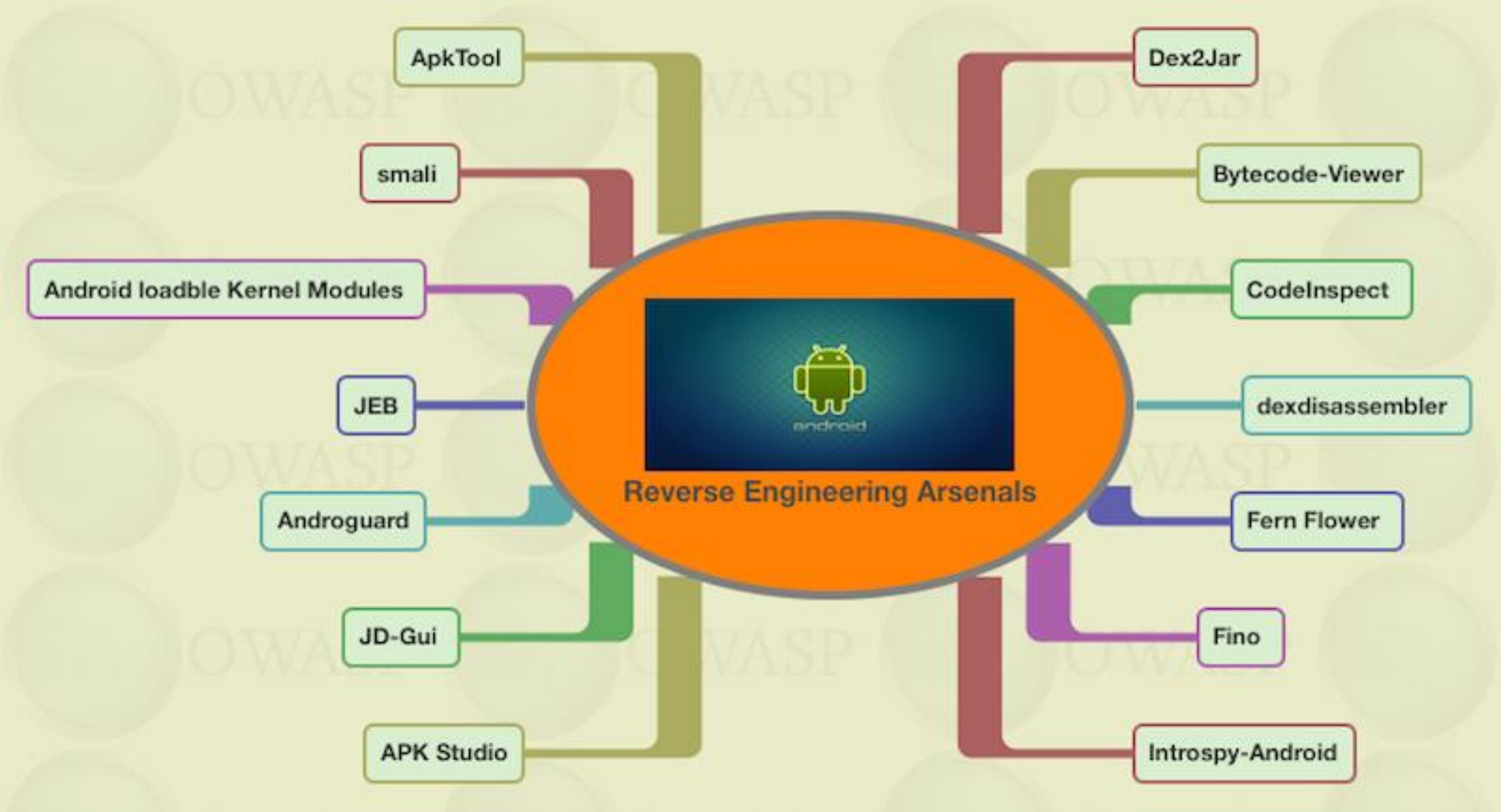
M8 - Security Decisions Via Untrusted Inputs

M9 - Improper Session Handling

M10 - Lack of Binary Protections

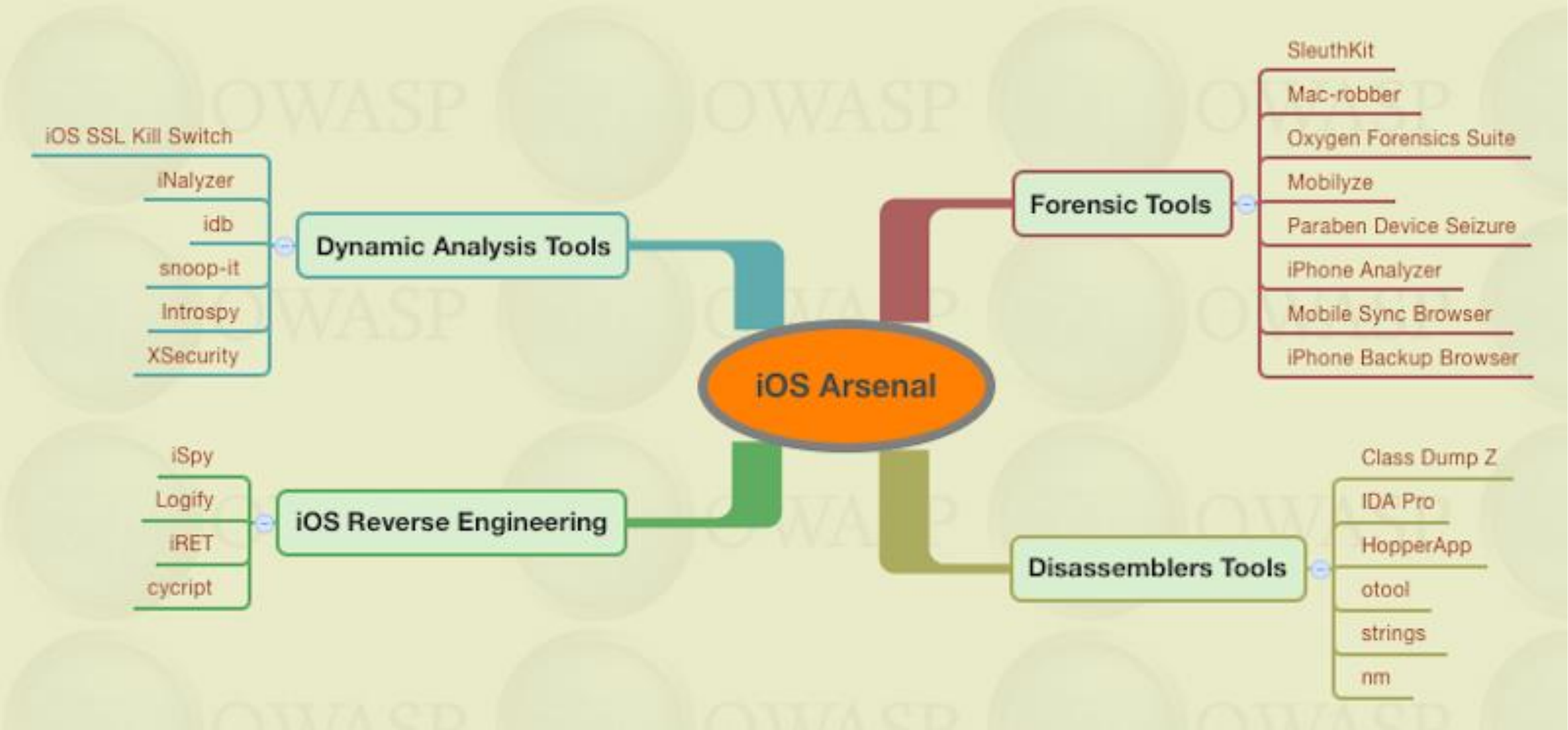
Final List 2014

檢測工具(Android)



https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=M-Tools

檢測工具(IOS)



https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=M-Tools

在各家知名公司APP的發現

- 使用者的帳號密碼直接遭到竊取、使用其他服務的帳號密碼遭到竊取
- 使用者的Access Token被竊取
- 不需要帳號密碼就能盜用帳號
- 應用程式的SQLite資料庫被竊取、竄改
- 使用者的私人對話訊息遭到竊取
- 使用者的私人檔案可被任意Apps偷取

在各家知名公司APP的發現(Cont.)

- 不必安裝惡意Apps下能在使用者不知情下發送付費簡訊
- 任一Apps在沒有GPS權限下取得使用者裝置的GPS位置
- 在未root下能直接存取Apps內所儲存的所有檔案
- 應用程式當掉 …
- More and More ….

案例說明

- 銀行App帳號及密碼外洩漏洞
- App應用儲存的檔案可允許任意應用存取，例如：瀏覽紀錄、Cookie
- 啟用SDcard訊息備份時，任何一個有存取SDCard權限的App皆可讀取到訊息

解決多家知名廠商資安問題

公司	認可	漏洞APP數量	時間
Google	Android Security Acknowledgement	5	2014
Facebook	WhiteHat Security Acknowledgement	2	2014
Evernote	Security Hall of Fame	1	2014
Alibaba(阿里巴巴)	Security Acknowledgement	8	2014/04
Microsoft	Security Acknowledgement	2	2014/5，6
AT&T	Security Hall of Fame	1	2014
Twitter	Security Hall of Fame(通過HackerOne平台)	1	2014
Sina Weibo	Security Acknowledgement	3	2014/4
Yahoo	通過HackerOne平台	1	2014/5
Badoo	Badoo	2	2014/5
Yandex	Bug Bounty Hall of Fame	2	2014/6，7
Baidu(百度)	通過Wooyun平台	1	2014/3
Sony	Hall of Thanks	1	2014
eBay	eBay Classifields branded ‘WhiteHat’	1	2014/5
Adobe	Adobe Product Security Incident Response Team	1	2014/5
Huawei (System APP)	Huawei Company	2	2014/8
Many Banks	Demo PoC	many	2014~2015

惡意軟體檢測

Beginning….

- It is difficult to judge an application is normal or malicious because both have the same permission rights.

- The following application in Google Play is a real case in April, 2014.

- A paid APP appeared in Google Play on April 2, 2014.

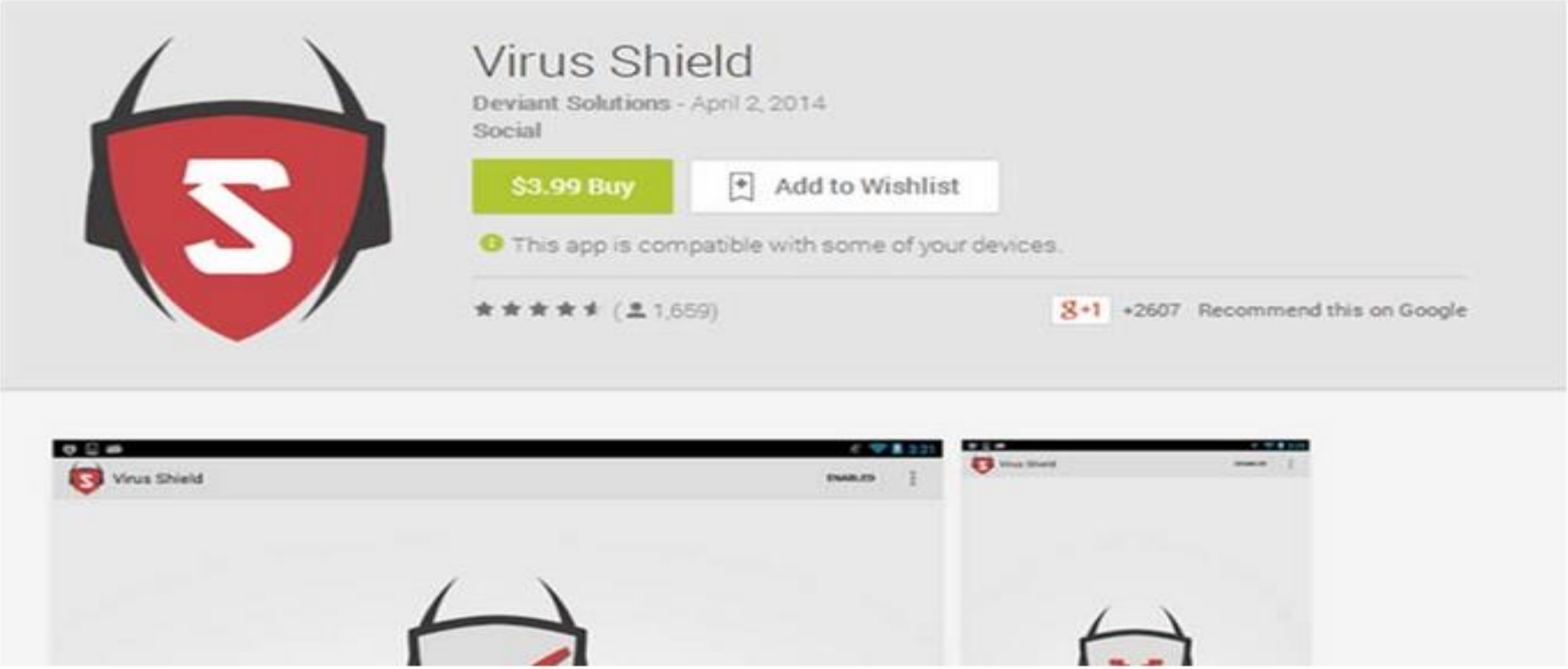
- It is an Anti-Virus APP, called Virus Shield, with cost USD$4.

- Within one week, it got the #1 paid application in Google Play with over 10,000 download.

- However, it is a fake APP with doing nothing. (It runs empty for a few minutes and reports back to the user that your mobile phone is safe.)

Fake Antivirus Apps hit Google Play

MAY 20, 2014 BY JONATHAN — LEAVE A COMMENT



Virus Shield

Deviant Solutions - April 2, 2014

Social

$3.99 Buy

Add to Wishlist

This app is compatible with some of your devices.

★★★★½ (1,659)

g+1 +2607 Recommend this on Google

It started in April with the #1 paid app ("Virus Shield") on Google Play being revealed as a fake anti-virus App. With over 10,000 downloads at $4 each, after just one week, this quickly made headlines when it was revealed as a fraud. What is worse, is that users of the App were so impressed with it that they gave it an impressive 4.7 star rating. Of course, the App did nothing, so it just shows how difficult to know whether an App on Google Play is

背景說明

- 在過去，最常用來檢測惡意軟體的方法是，比對惡意程式特徵碼的特徵值就可以快速的判斷是某否為惡意軟體
- 現在，越來越多惡意軟體開發者增進惡意軟體的強度，特別是對於從未出現過的特徵碼已經無法被檢測出來
- 因此，本技術主要是基於行為分析的方法來檢測 ，透過收集執行時所作的真正行為

技術內容

- 預先處理App設定檔的資訊
- 在執行期，蒐集並記錄App產生的行為
- 使用自動化觸擊觸發所有可能的行為
- 最後用機器學習的方法分析該App是否為惡意軟體

檢測項目

- 紀錄洩漏的資訊、洩漏方法，像是手機的電話號碼、IMEI碼、簡訊內容、GPS位置等等
- 記錄所有連出去或是連進來的網路行為
- 記錄所有檔案的讀取
- 呼叫哪些加密API
- 對於電話來電、簡訊都會有監控

檢測的軟體數量

- 檢測1246個惡意App和818個正常App
- 其中惡意App包含了高達49個家族
- 使用不同機器學習方法準確率皆在95%以上

準確率比較

Tsai			Comparsion	Our method		
TPR	FPR	Accuracy	Algorithm	Accuracy	FPR	TPR
0.967	0.062	95.5%	RandomForest	97%	0.036	0.971
0.946	0.085	93.4%	J48	95%	0.08	0.97
0.907	0.153	88.4%	RandomCommittee	96.2%	0.053	0.973
0.937	0.095	92.5%	Bagging	95.1%	0.076	0.969
0.968	0.099	94.15%	IBK(KNN)	95.3%	0.082	0.977