

區網網管會議

臺灣大學計資中心

李美雯

mli@ntu.edu.tw

3366-5010

2015/11/30

國立臺灣大學 National Taiwan University



主管機關政策討論

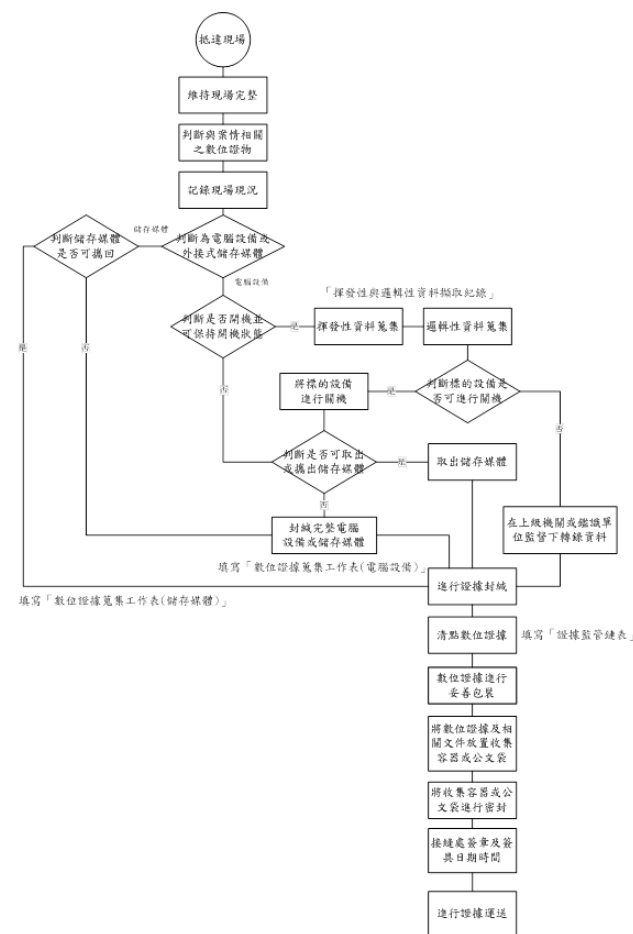


資通安全責任等級分級作業規定

| 法條項目 | 法條內容 | 討論項目 |
|---------------------|--|---|
| 資訊安全管理與防護具體做法中第(七)條 | 每年至少辦理2次 <u>網站安全弱點檢測作業</u> ，並對弱點進行修復作業 | <ol style="list-style-type: none">1. 針對網站的安全弱點檢測作業，僅能針對Web service上的弱點進行偵測，如Sql injection，Cross site Scripting等未完整檢測系統是否存在風險2. 若系統層存在弱點，如buffer overflow類型的弱點，攻擊者一樣可利用此弱點長驅直入取得管理者權限 |
| | <u>每2年至少辦理1次系統滲透測試作業</u> ，並依測試結果強化網路及系統資安防禦能力。 | <ol style="list-style-type: none">1. A.15.1遵循適法性要求 (ISO27001:2005)2. 各校通過ISMS問題 |
| | <u>每2年至少辦理1次資安健診作業</u> | <ol style="list-style-type: none">1. A.15.1遵循適法性要求 (ISO27001:2005)2. 各校通過ISMS問題 |

政府機關資安事件數位證據保全標準作業程序

數位證據保全標準作業流程圖



教育部 函

機關地址：臺北市中山南路5號
聯絡人：左寧生
電話：(02)7712-9082
Email：tso0815@mail.moe.gov.tw

受文者：國立臺灣大學

發文日期：中華民國104年8月11日

發文字號：臺教資(四)字第1040107120號

速別：普通件

密等及解密條件或保密期限：

附件：證據監管鍵表、證據取得清單、數位證據保全標準作業流程圖、數位證據蒐集工作表
儲存媒體、數位證據蒐集工作表_電腦設備、政府機關(構)資安事件數位證據保全標準作業程序

主旨：函轉行政院訂定「政府機關(構)資安事件數位證據保全標準作業

程序」(如附件)，自即日起生效試行1年，請查照並轉知所屬。

說明：依行政院104年8月4日院臺護字第1040036611號函辦理。

正本：部屬機關(構)、本部各單位、各直轄市及縣市政府教育局(處)、各公私立大專校院

副本：104/08/12
108/20/56

校級公文 104/08/12



收文號:1040061006

政府機關資安事件數位證據保全 標準作業程序

三、適用時機

各機關基於資安事件之調查，需進行電腦系統之數位證據識別、蒐集、擷取、封緘及運送作業時，適用本作業程序。

教育部 函

機關地址：臺北市中山南路5號
聯絡人：左寧生
電話：(02)7712-9082
Email：tso0815@mail.moe.gov.tw

受文者：國立臺灣大學

發文日期：中華民國104年8月11日

發文字號：臺教資(四)字第1040107120號

速別：普通件

密等及解密條件或保密期限：

附件：證據監管鏈表、證據取得清單、數位證據保全標準作業流程圖、數位證據蒐集工作表、儲存媒體、數位證據蒐集工作表、電腦設備、政府機關(構)資安事件數位證據保全標準作業程序

主旨：函轉行政院訂定「政府機關(構)資安事件數位證據保全標準作業程序」(如附件)，自即日起生效試行1年，請查照並轉知所屬。

說明：依行政院104年8月4日院臺護字第1040036611號函辦理。

正本：部屬機關(構)、本部各單位、各直轄市及縣市政府教育局(處)、各公私立大專校院
副本：

104/08/12
108/20/66

校級公文 104/08/12

第1頁，共1頁



收文號：1040061006

政府機關資安事件數位證據保全標準作業程序

8 月份資安事件等級統計表

| 事件等級 通報類型 | High(高) | | Medium(中) | Low(低) | 合計 |
|--------------|---------|-----|-----------|--------|------|
| | 4 級 | 3 級 | 2 級 | 1 級 | |
| 自行通報 | 0 | 0 | 0 | 11 | 11 |
| G-ISAC | 0 | 0 | 0 | 1 | 1 |
| SA-SOC | 0 | 0 | 0 | 482 | 482 |
| ABUSE | 0 | 0 | 0 | 18 | 18 |
| TACERT | 0 | 0 | 0 | 2 | 2 |
| NCKU | 0 | 0 | 0 | 4 | 4 |
| NA-SOC | 0 | 0 | 1 | 1001 | 1002 |
| Mini-SOC | 0 | 0 | 1 | 64 | 65 |
| MJIB | 0 | 0 | 0 | 11 | 11 |
| TWCERTCC | 0 | 0 | 0 | 0 | 0 |

政府機關資安事件數位證據保全標準作業程序

| 法條項目 | 法條內容 | 討論項目 |
|---|---|--|
| 政府機關 (構)資 安事件數 位證據保 全標準作 業程序 | 三、適用時機 各機關基於 <u>資安事 件</u> 之調查，需進行 電腦系統之數位證 據識別、蒐集、擷 取、封緘及運送作 業時，適用本作業 程序。 | 1. 無明確適用之資安事件 定義 2. 各校通過ISMS問題 A.15.1遵循適法性要求 (ISO27001:2005) 3. 建議適用範圍為 <u>三四級 資安事件</u> |

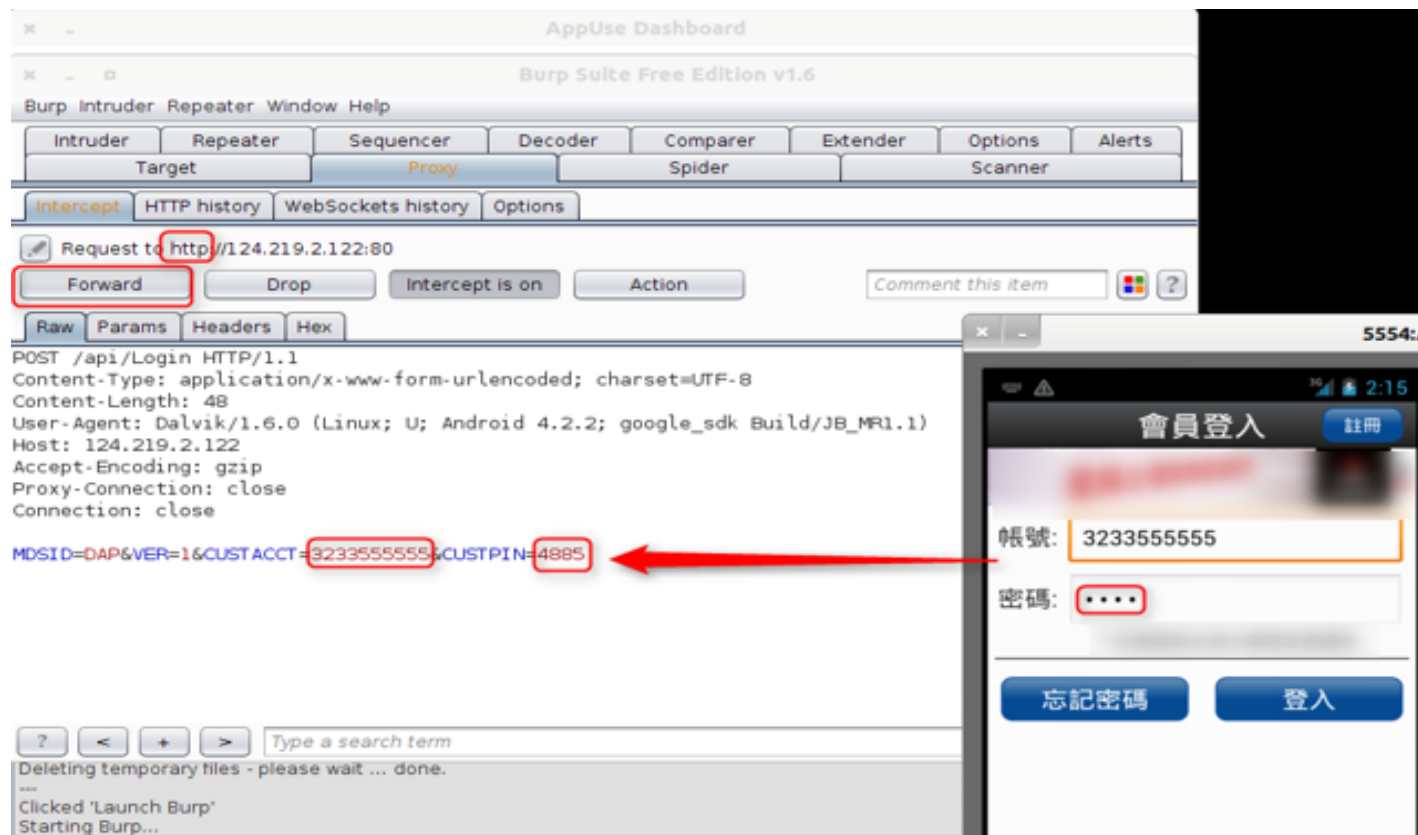


資安案例分享



手機APP資安漏洞分析(某叫車軟體為例)1/2

不安全的傳輸方式

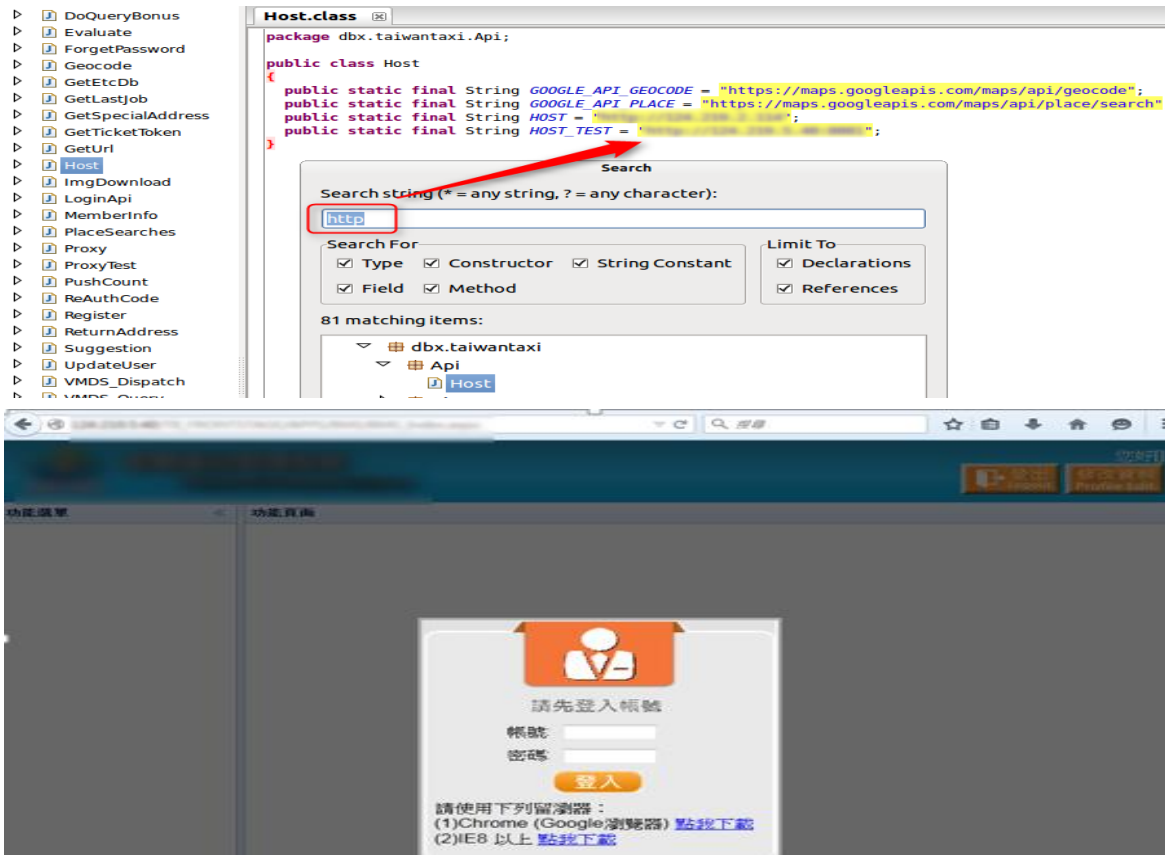


該叫車軟體在使用前，使用者須先註冊成會員後方可登入使用，因此我們針對該APP對於帳號及密碼在登入時所使用的傳輸方式進行分析，發現該APP將帳號與密碼使用明碼方式傳送，傳輸過程中無任何加密方式，有心人事只要偽裝成免費wifi網路後，即可透過封包側錄方式，取得使用者帳號密碼，若使用者有使用相同帳號或密碼的習慣，那麼很可能讓自己的機敏資訊處於高度的風險中。



手機APP資安漏洞分析(某叫車軟體為例)2/2

暴露的後台管理系統



進一步針對該APP原始碼進行分析，發現該APP對於後台管理系統的IP位置並未加密隱藏起來，有心人士很容易透過原始碼的逆向分析來找出所在位置，此資訊具有高度資安風險，因攻擊者可透過各種方式，像是密碼暴力破解、利用該web server上既有的漏洞來入侵、滲透伺服器，甚至發動DDoS攻擊來導致APP服務停擺，因此這類機敏資料是需要妥善加密儲存的。



課網爭議 匿名者攻擊始末

高中課網 DDOS事件



Torshammer DDOS攻擊

1. 匿蹤：

Torshammer可執行於tor網路（洋蔥路由）藏匿效果極佳

2. 手法：利用HTTP POST方式及回應緩慢，以達成阻斷服務目的

3. Web Server 連線數量達到上限時無法提供正常服務

Anonymousa Asia FB



Torshammer.py -t
www.edu.tw -p 80

Torshammer DDOS攻擊

Torshammer 攻擊封包分析

| | | | | | | |
|------|--------------------|-----------------|-----------------|-----|----|--|
| 3617 | 14:00:43.831744000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=301 win=65536 Len=0 |
| 3752 | 14:00:45.137603000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |
| 3779 | 14:00:45.422792000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=302 win=65536 Len=0 |
| 3822 | 14:00:45.792662000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |
| 3844 | 14:00:45.999772000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=303 win=65536 Len=0 |
| 4100 | 14:00:48.383190000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |
| 4128 | 14:00:48.666829000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=304 win=65536 Len=0 |
| 4168 | 14:00:49.037719000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |
| 4181 | 14:00:49.244917000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=305 win=65536 Len=0 |
| 4328 | 14:00:50.675729000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |
| 4351 | 14:00:50.882050000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=306 win=65536 Len=0 |
| 4392 | 14:00:51.378790000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |
| 4418 | 14:00:51.584201000 | 192.168.192.136 | 192.168.192.135 | TCP | 54 | 80-51141 [ACK] Seq=1 Ack=307 win=65536 Len=0 |
| 4594 | 14:00:53.469112000 | 192.168.192.135 | 192.168.192.136 | TCP | 60 | [TCP segment of a reassembled PDU] |

POST / HTTP/1.1
POST / HTTP/1.1
POST / HTTP/1.1
POST / HTTP/1.1
POST / HTTP/1.1

Torshammer DDOS攻擊

小型攻擊流量防禦措施

1. 限縮Web Server提供HTTP POST功能
2. 設定防火牆、IPS與WAF的Policy功能
3. 調整Switch、IPS與防火牆來源IP的最高連線數
4. Inline AntiDDOS設施

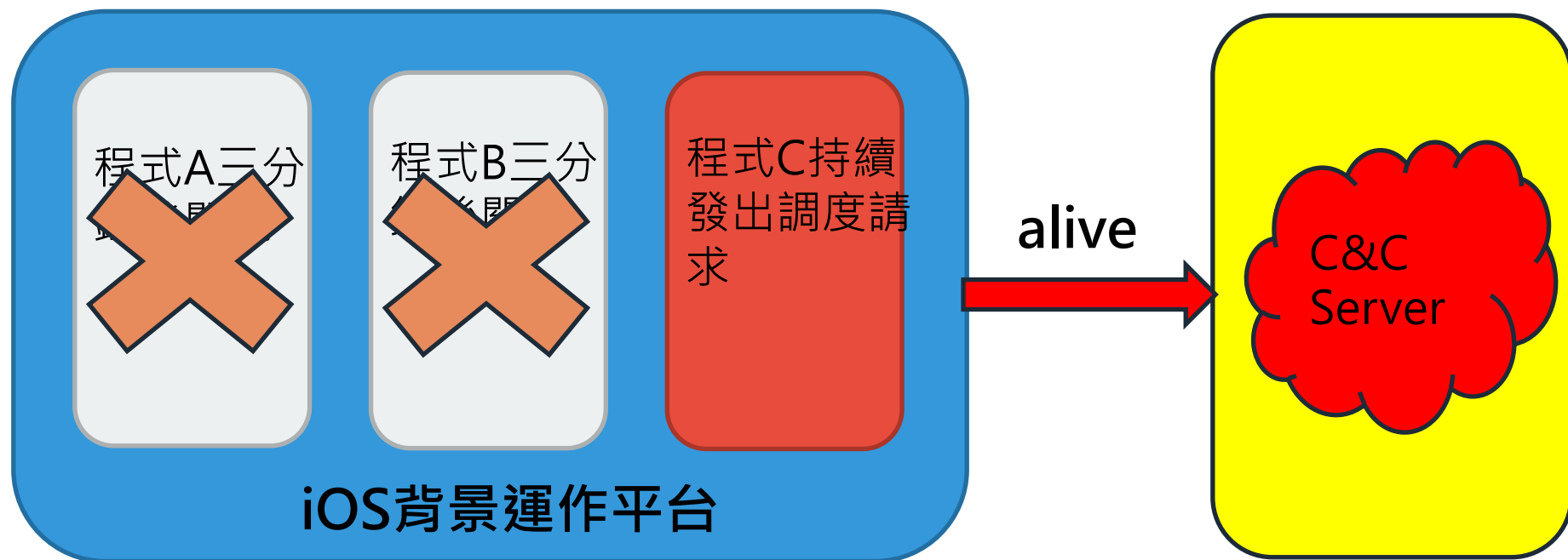
大型攻擊流量防禦措施

| 封包檢查位置 | 正規表示法 | 攔截率 |
|----------------------------------|---------|-----|
| Payload Regular Expression | ^.{1}\$ | 94% |

佈署反制措施

進行攻擊流量清洗作業

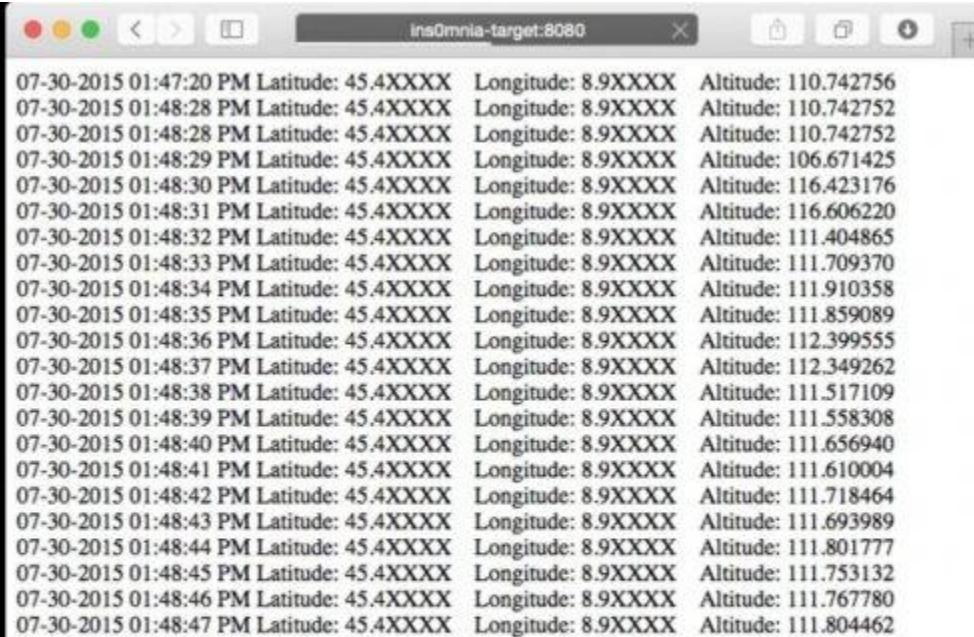
iOS不越獄也有風險-ins0mnia漏洞(1/2)



蘋果的iOS系統在8月份被揭漏了一個安全性漏洞-ins0mnia。iOS系統的用戶在預設情況下，要離開應用程式時會使用Home鍵來進行，但此時應用程式並未真正被關閉，而是暫時被存放至背景中運作。而iOS有一機制限制了應用程式在背景運作的時間，這個機制為了安全上的考量，會將應用程式在背景中運作的時間限制在三分鐘左右，一旦有惡意程式進行惡意的連線行為，即便在背景常駐，此機制也可在一定時間內關閉其運作終止存取行為。

然而某些情況下iOS允許應用程式繞過此一安全機制，其中一個情況是當應用程式發送調度中的請求訊息時，iOS平台便會忽略此一安全機制，讓此應用程式持續運行。攻擊者便利用此漏洞不斷地發送調度中的請求訊息，藉此來中斷iOS後台此安全機制的運作。如此一來，惡意程式便可能在用戶未察覺的情況下進行不間斷的連線行為。

iOS不越獄也有風險-ins0mnia漏洞(2/2)



```
ins0mnia-target:8080
07-30-2015 01:47:20 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 110.742756
07-30-2015 01:48:28 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 110.742752
07-30-2015 01:48:28 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 110.742752
07-30-2015 01:48:29 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 106.671425
07-30-2015 01:48:30 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 116.423176
07-30-2015 01:48:31 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 116.606220
07-30-2015 01:48:32 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.404865
07-30-2015 01:48:33 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.709370
07-30-2015 01:48:34 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.910358
07-30-2015 01:48:35 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.859089
07-30-2015 01:48:36 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 112.399555
07-30-2015 01:48:37 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 112.349262
07-30-2015 01:48:38 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.517109
07-30-2015 01:48:39 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.558308
07-30-2015 01:48:40 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.656940
07-30-2015 01:48:41 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.610004
07-30-2015 01:48:42 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.718464
07-30-2015 01:48:43 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.693989
07-30-2015 01:48:44 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.801777
07-30-2015 01:48:45 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.753132
07-30-2015 01:48:46 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.767780
07-30-2015 01:48:47 PM Latitude: 45.4XXXX Longitude: 8.9XXXX Altitude: 111.804462
```



FireEye概念性驗證程式-ins0mnia

以往iOS系統出現的漏洞大多針對已越獄 (Jailbreak) 的用戶，而這個漏洞因為是利用了iOS自身的安全機制來進行，亦即就算是未越獄的用戶也在威脅範圍內。揭漏此漏洞的FireEye亦設計了此漏洞的概念驗證此程式存在的風險。建議用戶盡快將iOS的版本更新至8.4.1之後的版本，並且避免使用來路不明的應用程式。

iOS 新型態惡意程式 YiSpecter



#Yi Specter透過網站或社交工程來意圖散佈感染

近期iOS出現名為“Yi Specter”的新型態惡意程式，“Yi Specter”透過Apple原先提供給企業用戶所使用的企業用戶專案來散播感染，企業用戶專案可允許取得相關認證的企業，提供使用者自行開發的iOS行動程式，而不必透過Apple官方的App Store。

“Yi Specter”不僅盜用了取得認證的企業憑證，甚至使用了僅供Apple官方內部測試用的Private APIs，Private APIs相較於一般開發者所使用的API，擁有較大權限，甚至可以在背景運行手機的相機或藍芽功能。

iOS平台的惡意程式並不是新聞，但大多是針對已JB的裝置感染，而“Yi Specter”因盜用合法企業所使用的專案憑證，因此即使未JB的裝置也會遭受感染，多透過非官方的程式集或社交網站來散佈感染，一旦裝置遭感染，將會被植入惡意程式，藉此強制在裝置上播放廣告並會裝置資訊上傳至外部伺服器，由於惡意程式可完全隱藏因此難以刪除。

Apple官方於iOS 8.4版後修正相關弱點，建議使用者宜盡速更新至iOS 8.4以上的版本，避免受此風險影響。

iOS APP潛在風險-XcodeGhost(1/3)

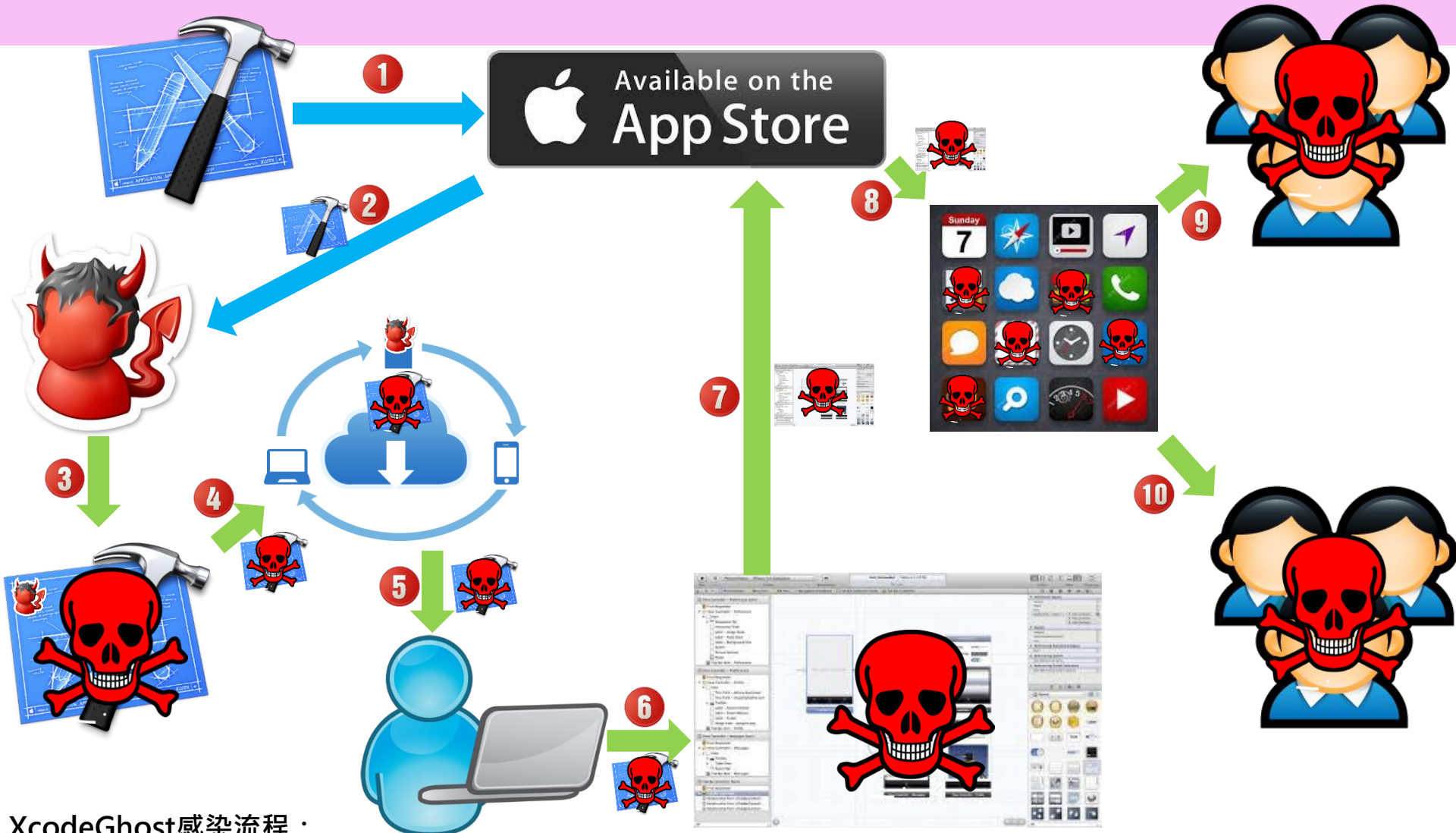
今年九月Apple iOS出現了大量的App感染。不同於以往的攻擊者致力於開發惡意的App並試圖進行攻擊，此次攻擊者所採取的手段是將惡意代碼植入於開發工具內，如此一來，便可躲過Apple嚴謹的上架審查機制，使得眾多使用者一開始在下載App Store的App時，即遭受感染。



正常狀況下iOS App上架流程：

Apple官方提供Xcode開發工具予開發者使用(編號1&2)→開發者開發相關App(編號3)→開發完成後上架於App Store(編號4)→App Store提供相關平台供使用者下載使用(編號5-7)

iOS APP潛在風險-XcodeGhost(2/3)



XcodeGhost感染流程：

Apple官方提供Xcode開發工具予開發者使用，攻擊者於此階段取得Xcode開發工具(編號1&2)→攻擊者於開發工具內植入惡意源代碼(編號3)並發布於雲端空間上提供開發者下載(編號4&5)→開發者使用已受感染的工具，連帶感染自身開發的App(編號5&6)→開發者發布受感染的App於App Store(編號7)→App Store發布受感染的App予使用者(編號8-10)

iOS APP潛在風險-XcodeGhost(3/3)

| 前24大遭XcodeGhost感染的惡意App | | 資料來源：蘋果公司，2015年10月 |
|--|--|--------------------|
| ●微信 (版本：6.2.6) | ●滴滴出行 (版本：4.1.0)58同城-招聘找工作、二手車、二手房、租房 (版本：6.2.2) | |
| ●網易雲音樂 (版本：3.0.0) | ●高德地圖 (專業的手機地圖) (版本：7.5.0) | |
| ●洋碼頭—海外掃貨神器 (版本：2.5.1) | ●鐵路12306 (版本：2.11) | |
| ●自由之戰-真•5V5 (第一MOBA手遊) (版本：1.1.0) | ●同花順 (版本：9.62.01) | |
| ●航海王啟航 (正版授權-跨服公會戰500VS500!)(版本：2.8.1) | ●中國聯通手機營業 (官方版)(版本：3.3) | |
| ●下廚房-美食菜譜 (版本：4.4.0) | ●保衛蘿蔔2：每日一戰 (版本：1.7.1) | |
| ●《混沌與秩序之英雄戰歌》—多人玩家線上遊戲 (版本：2.2.1) | ●奇跡暖暖 (版本：1.5.0) | |
| ●暗黑黎明-冰臨城下 (全球第一ARPG手遊) (版本：1.6.1) | ●我叫MT2-跨服天梯賽 (版本：2.0.6) | |
| ●喜歡和你在一起 (版本：1.1.7) | ●憤怒的小鳥2-李易峰至愛手遊 (版本：2.2.1) | |
| ●保衛蘿蔔1 (版本：1.8.0) | ●百度音樂 (版本：5.2.10) | |
| ●同花順HD (版本：5.84.01) | ●鈴聲多多 (版本：1.4.0) | |
| ●摩擦 - 同城陌生人交友聊天必備神器 (版本：2.5.2) | ●喜馬拉雅FM (聽書社區) 電臺有聲小說英語相聲新聞(版本：4.3.20) | |

使用者建議措施：

- 1.建議用戶立即更改舊的Apple ID的密碼並開啟二階段認證確保Apple ID的帳號安全。
- 2.利用檢測工具或檢查相關感染清單後確認受感染的檔案，並進行移除與更新至最新版。

開發者建議措施：

- 1.建議開發者採用官方所發布的開發工具，避免使用來路不明的檔案。
- 2.如果無法確認開發工具是否官方，檢查SHA1驗證碼是否為官方所發布。

透過網路監視器發動新型態DDoS攻擊



目前全球有超過兩億台連上網路的監視器(CCTV)，而在物聯網時代下，透過CCTV所發動的新型態的DDoS攻擊手法也讓我們體會到所面臨的資安環境有多嚴峻。

許多CCTV作業系統是採用嵌入式的開源Linux 套件“Busy Box”，攻擊者針對此作業系統進行大規模掃描，並透過ssh方式暴力破解來嘗試登入，一旦登入成功並會自動下載安裝惡意程式，成為被大量被挾持的CCTV之一。

雖然攻擊手法相當粗糙卻是意外的有效，因為Busy Box平台有預設的使用者名稱及密碼，許多使用者甚至連預設密碼都沒修改，即使修改了，也會因使用者名稱固定加上密碼強度不足而被破解，而即使設備遭到感染，甚至對外發動DDoS攻擊時，由於疏於管理，使用者可能仍然無法察覺到任何異常，因此面對此類型攻擊管理者不可不慎，以免在不知情的狀況下成為惡意流量的幫兇。

加密勒索軟體新變種 - CryptoWall 4.0

繼CryptoLocker後，加密勒索軟體CryptoWall 正在網際網路上大肆蔓延。

不同於CryptoLocker，CryptoWall 採用Tor(洋蔥網路)與其C&C server進行通訊，利用高度隱密及層層加密的特性，讓管理者難以阻斷受感染主機與C&C server間的通訊。一旦從遠端伺服器取得加密公鑰後，便開始進行檔案加密作業，4.0除了加密資料之外連檔案名稱也加密，加密完成後，便會出現如左圖般的勒索訊息，而解密的贖金甚至會隨著時間而不斷增加。

一旦遭到CryptoWall 4.0感染，受害者只有兩個選擇，一是重新格式化系統並從最近的備份回復資料，二是支付贖金但無從保證能夠拿到解密金鑰。

CryptoWall 多利用各式釣魚郵件散播，只要執行附件的*.js file，系統就會遭受感染。

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?



- You should register Bitcon wallet ([click here for more information with pictures](#))
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
 - [Coin.mx](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
 - [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
 - [bitquick.co](#) - Buy Bitcoins Instantly for Cash
 - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
 - [Cash Into Coins](#) - Btcoin for cash.
 - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
 - [anxpro.com](#)
 - [bittylicious.com](#)
 - [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
- Send 1.19 BTC to Bitcoin address: **16ydt1Wj2NZa2uLZ6W4UDCDJ2Ttw92uFaT7** [Get QR code](#)
- Enter the Transaction ID and select amount:
 1.19 BTC ≈ 500 USD [Clear](#)
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)
- Please check the payment information and click "PAY".

[PAY](#)

| Your sent drafts | | | | |
|--------------------------|------------|--------------------------------|--------|--------|
| Num | Draft type | Draft number or transaction ID | Amount | Status |
| Your payments not found. | | | | |

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.



Q & A