



TWCERT/CC 資安情資電子報

2018 年 3 月份

目錄

第 1 章、 摘要	1
第 2 章、 TWCERT/CC 近期動態.....	2
2.1、 協辦中華民國全國中小企業總會內部成員資安教育訓練座談會.....	2
2.2、 與內政部警政署刑事警察局合作一頁式廣告詐騙網站宣導事宜.....	2
2.3、 參與 2018 年 APCERT 網路攻防演練	2
2.4、 2018 年 3 月 13 日至 15 日 iThome 舉辦台灣資安大會.....	3
2.5、 2018 年 3 月 15 日與資安人合作進行 TWCERT/CC 專題採訪.....	3
第 3 章、 國內外重要資安新聞	3
3.1、 國內外資安政策、威脅與趨勢	3
3.1.1、 挖礦惡意軟體「WANNAMINE」悄然崛起	3
3.1.2、 NCC 攜經部，設資安檢測實驗室	4
3.1.3、 ATM 吐鈔攻擊，趨勢科技 7 大點提醒資安風險.....	4
3.1.4、 蘋果 IPHONE 的 IBOOT 原始碼在 GITHUB 遭公開	5
3.1.5、 亞洲網路間諜組織與比特幣挖礦惡意程式.....	5
3.1.6、 2017 年的微軟漏洞您都更新了嗎?三組 NSA 工具已被移植到 METASPLOITE 多次改造和利用	6
3.1.7、 惡意挖礦、竊幣事件頻傳，2018 儼然成為惡意挖礦年	6
3.1.8、 三種容易成為駭客肥羊的人.....	7
3.1.9、 美國能源部建立能源基礎建設之資安事件協處辦公室	7
3.1.10、 RISK BASED SECURITY 發布 2017 年度漏洞分析報告	8
3.1.11、 新加坡政府逐步完成道德駭客計畫	8
3.2、 駭客攻擊事件及手法	10

3.2.1、	惡意挖礦程式災情再傳，Mac 軟體蒐集站 MacUpdate 淪陷 ..	10
3.2.2、	詐騙集團假冒「財政部電子發票整合服務平台」寄發中獎通知電子郵件.....	11
3.2.3、	印度銀行 SWIFT 系統遭駭，遭試圖盜轉近 200 萬美元.....	12
3.3、	軟硬體漏洞資訊.....	14
3.3.1、	開發工具 Electron 有登錄值隱憂，危及 Windows 程式.....	14
3.3.2、	Mozilla 釋出例行更新，緊急追加 Firefox 修補項目	14
3.3.3、	封包分析工具 Wireshark 可能遭受 DoS 攻擊.....	15
3.3.4、	餐旅 POS 系統 Hospitality Symphony 測出路徑造訪漏洞	16
3.3.5、	全球 WordPress 開發網站皆面臨 DoS 嚴峻危機	17
3.3.6、	Lenovo 指紋辨識系統 hard-code 密碼隱憂	18
3.3.7、	VPN 軟體 Pulse Secure Linux 用戶 SSL 連線恐遭中間人操控 ..	19
3.3.8、	Joomla! 釋出新版防止 SQL injection 及 Cross-Site Scripting ..	19
3.3.9、	Skype 安全更新流程出現致命 DLL hijacking 破綻	20
3.3.10、	駭客藉 Telegram 0-day 漏洞 RLO 散佈挖礦病毒	21
3.3.11、	趨勢科技數款軟體 UMH 模組具 DLL 劫持弱點，另 IMSVA 日誌內容遭任意存取.....	22
3.3.12、	印度泰盧固語系文字造成 Apple 裝置通訊功能停擺	23
3.3.13、	駭客探勘 PyBitmessage 0.6.2 即時通 0-day 漏洞，利用 RCE 竊取比特幣錢包.....	24
3.3.14、	隨身碟 label 竟可在 Plasma 圖形桌面環境執行命令	24
3.4、	資安研討會及活動	25
第 4 章、	2018 年 02 月份事件通報統計	31

第 1 章、摘要

為提升我國民眾資安意識，TWCERT/CC 於每月發布資安情資電子報，統整上月重要資安情資，包含 TWCERT/CC 近期動態、資安政策、威脅與趨勢、駭客攻擊事件、軟硬體漏洞、資安研討會活動及資安事件通報統計分析等資訊。

第 2 章、TWCERT/CC 近期動態

2.1、協辦中華民國全國中小企業總會內部成員資安教育訓練座談會

TWCERT/CC 平時除了協助國內外資安事件通報應變外，亦協助民間企業組織/產業公協會進行資安宣導，TWCERT/CC 預計於 2018 年 3 月 19 日協助中華民國全國中小企業總會內部成員辦理資安教育訓練座談會，將針對較常遇到的資安事件案例進行宣導。

(註：若您的企業需要協助辦理資安宣導座談會，歡迎洽詢承辦人王小姐，alian.wang@cert.org.tw，02-2673-9638 #353412)

2.2、與內政部警政署刑事警察局合作一頁式廣告詐騙網站宣導事宜

我國近期一頁式廣告詐騙網站猖獗，因此本中心與內政部警政署刑事警察局合作，協助於本中心官網及臉書向大眾宣導相關訊息，以提升民眾資安意識，以免遭詐騙，導致個資外洩或金錢損失。



2.3、參與 2018 年 APCERT 網路攻防演練

本中心於 3 月 7 日參與一年一度之亞太區電腦緊急事件回應小組 2018 年網路攻防演練(APCERT CYBER DRILL 2018)，並於演練中擔任腳本設計及參與實際演練。本年度之演練主題為「透過 IOT 病毒導致資料外洩(DATA BREACH VIA MALWARE ON IOT)」，APCERT 之

官方新聞稿請參考：<http://surl.twcert.org.tw/aJwi4>。

2.4、2018 年 3 月 13 日至 15 日 iThome 舉辦台灣資安大會

iThome 將於 2018 年 3 月 13 日至 15 日舉辦台灣資安大會，今年將以「Cyber First, Cyber Taiwan」為願景，並首次規劃「臺灣資安館」，而 TWCERT/CC 亦於此次研討會中參加 iThome 的資安共同推廣計畫，協助 iThome 邀請民眾參與會議。



2.5、2018 年 3 月 15 日與資安人合作進行 TWCERT/CC 專題採訪

資安人將於 4 月 25 日至 27 日舉辦 2018 亞太資訊安全論壇暨展會，於會前將針對展會參與廠商與單位進行相關專題採訪，TWCERT/CC 主任陳永佳將於 3 月 15 日接受資安人採訪，主要針對 TWCERT/CC 服務項目等進行相關介紹。

第 3 章、國內外重要資安新聞

3.1、國內外資安政策、威脅與趨勢

3.1.1、挖礦惡意軟體「WANNAMINE」悄然崛起

美國國家安全局(US National Security Agency)開發的一個漏洞利用工具，2017 年被駭客揭露利用作為勒索軟體如「WannaCry」，

現在正被用來開採加密貨幣(Monero)。據網路安全專家表示，感染的設備數量正在上升。



資料來源：

https://motherboard.vice.com/en_us/article/yw5yp7/monero-mining-wannacry-nsa

3.1.2、NCC 攜經部，設資安檢測實驗室

NCC 與經濟部將共同設立資安檢測實驗室，提供台灣網通設備商檢測物聯網(IoT)相關連網設備的環境，藉此協助台灣廠商加快接單速度。此外，NCC 亦計畫培植民間檢測機構加入 IoT 連網設備檢測行列。



資料來源：

<http://www.chinatimes.com/newspapers/20180202000321-260204>

3.1.3、ATM 吐鈔攻擊，趨勢科技 7 大點提醒資安風險

全球兩大 ATM 提款機製造商 Diebold Nixdorf 和 NCR Corp.

發布 ATM 吐鈔攻擊警告，趨勢科技提醒 7 大要點防範潛在風險！

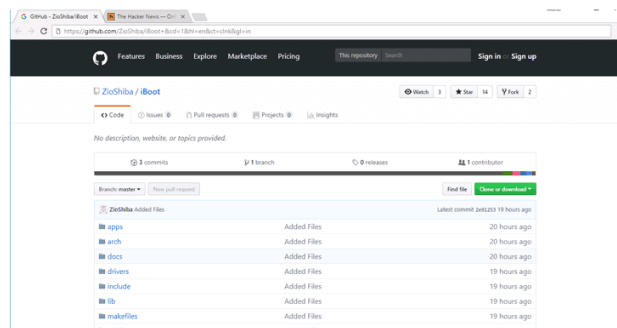


資料來源：

<https://tw.appledaily.com/new/realtime/20180207/1293346/>

3.1.4、蘋果 IPHONE 的 IBOOT 原始碼在 GITHUB 遭公開

蘋果 iPhone 操作系統核心組件 iBoot 原始碼據稱已經在 GitHub 上遭公開，這有可能使駭客從公開的 iBoot 原始碼中發現漏洞，持續開發惡意軟體或使 iPhone 更容易越獄。



資料來源：

<https://thehackernews.com/2018/02/iboot-ios-source-code.html>

3.1.5、亞洲網路間諜組織與比特幣挖礦惡意程式

安全研究人員發現一起被稱為「PZChao」的網路間諜活動，針對了亞洲和美國政府、科技、教育和電信機構。在過去幾個月對亞

洲造成嚴重破壞，並且能夠執行令人討厭的攻擊行為，比如密碼竊取、比特幣挖礦以及為駭客進行遠端控制。



資料來源：

<https://thehackernews.com/2018/02/cyber-espionage-asia.html>

3.1.6、2017 年的微軟漏洞您都更新了嗎？三組 NSA 工具已被移植到 METASPLOITE 多次改造和利用

資安研究員 Sean Dillon 將三個 NSA(美國國家安全局)開發的漏洞攻擊工具：EternalSynergy、EternalRomance 及 EternalChampion 移植到了 Metasploit 平台。



資料來源：

<https://github.com/rapid7/metasploit-framework/pull/9473>

3.1.7、惡意挖礦、竊幣事件頻傳，2018 儼然成為惡意挖礦年

別再讓自己電腦淪為他人的挖礦苦工!! 駭客植入挖礦程式或虛擬貨幣交易平台遭竊事件層出不窮，觸手甚至伸入政府網站，災情日益擴大，公私部門及民眾個人都不可不防。

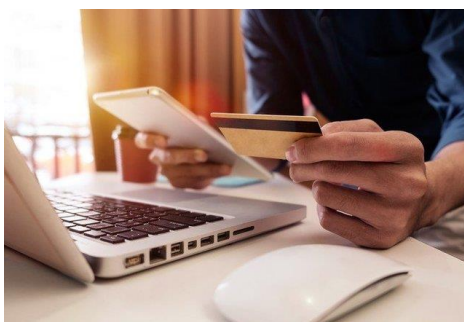


資料來源：

<https://blog.trendmicro.com.tw/?p=54355>

3.1.8、三種容易成為駭客肥羊的人

從刑事局公布的 2017 國內詐欺案件的資料顯示，高達近 10 億元的詐騙金額中，有 5 成的比例是因網購延伸而來的電信與網路詐騙，顯示假網拍真詐財的方式已經成為歹徒慣用的不肖伎倆。



資料來源：

<https://tw.appledaily.com/new/realtime/20180214/1298189/>

3.1.9、美國能源部建立能源基礎建設之資安事件協處辦公室

美國能源部(U.S. Department of Energy, DOE)於 2 月 14 日聲明中指出，他們將會於該部門下新建一個處理能源資安問題的辦公室(Office of Cybersecurity, Energy Security, and Emergency Response, CESER)，該辦公室將負責協助能源部處理能源基礎建設

相關資安問題，包含開發相關系統及裝置，以分享具時效性之重要情資，亦協助產業內公司對資安事件進行偵測、預防及復原作業。

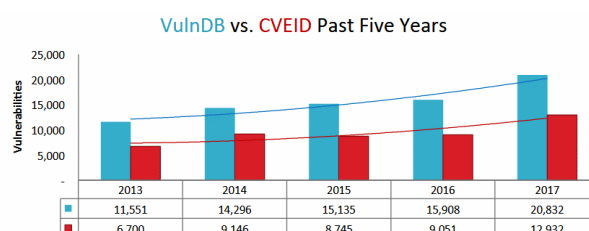


資料來源：

<https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>

3.1.10、RISK BASED SECURITY 發布 2017 年度漏洞分析報告

資安業者 Risk Based Security 公布了 2017 年度漏洞分析報告，並觀察到 2017 年所揭露之漏洞比起 2016 年多了 31%。



資料來源：

<https://pages.riskbasedsecurity.com/2017-ye-vulnerability-quickview-report>

3.1.11、新加坡政府逐步完成道德駭客計畫

2017 年 7 月中旬，新加坡政府推出「道德駭客註冊機制」並徵求意見，此外，新加坡國防部於 2017 年 12 月中旬首度舉辦網路漏洞獎勵挑戰賽(MINDEF Bug Bounty Challenge)，廣邀全球約 300 名「白帽駭客」入侵國防部電腦等網路系統，檢測系統安全，並於三週內解決了 35 個漏洞。



資料來源：

<http://www.cna.com.tw/postwrite/Detail/229287.aspx#.WpTBO4NuaUk>

3.2、駭客攻擊事件及手法

3.2.1、惡意挖礦程式災情再傳，Mac 軟體蒐集站 MacUpdate 淪陷

MacUpdate 網站遭駭客掌握用來散播挖礦惡意程式，導致使用者 Mac 設備也可能成為駭客手底下的挖礦苦工。資安專家發現，知名的 Mac 軟體蒐集站 MacUpdate 已經成為黑客攻擊的受害者，該服務現正在向 Mac 使用者散播惡意挖礦程式。

這個惡意軟體被稱為「CreativeUpdate trojan / miner」，它是開源開發工具 Platypus 的一個縮小版，會從 Adobe Creative Cloud 伺服器下載挖礦程式。2018 年 2 月 1 日至 2 月 2 日下載該連結的使用者皆處於此風險中。

駭客入侵 MacUpdate 網站，並利用其散播挖礦程式，駭客修改 OnyX、Firefox 和 Deeper 等 APP，並將下載連結替換為引導用戶訪問惡意網站的連結，該假冒之惡意連結修改得看起來合法且令人信服。

如 Firefox 的 APP 是透過偽造的 URL「download-installer[.]cdn-mozilla[.]net」而不是 Mozilla[.]net 進行散播。當使用者安裝時，一如往常會被要求下載至應用程式資料夾，這類 APP 是透過 Platypus 開發。這個工具用於開發原生 Mac 應用程式，支援的語言包括 python、perl 和 ruby 或是 Shell 腳本。

當安裝假冒 APP 時，將從合法 URL「public[.]adobecc[.]com」下載檔案，便會開啟偽裝原始 APP 的偽冒副本並啟動惡意軟體。MacUpdate 發覺到這個問題後，立即由網站的編輯發出道歉聲明，並提供有關刪除惡意軟體的說明。

建議用戶直接從開發人員的官方網站或是官方 Mac App Store 下載 APP，雖不能保證 APP 是否有問題，然而至少較第三方 APP 下

載平台要來得安全。

「Mac 電腦不會得到病毒」，這個古老傳說被證明不再堅不可破。
永遠不要認為自己的 Mac 電腦不會受到感染。



資料來源：

<https://www.hackread.com/macupdate-hacked-to-distribute-mac-crypto-currency-miner/>

<https://blog.malwarebytes.com/threat-analysis/2018/02/new-mac-crypto-miner-distributed-via-a-macupdate-hack/>

3.2.2、詐騙集團假冒「財政部電子發票整合服務平台」寄發中獎通知電子郵件

財政部寄發中獎通知電子郵件內不會提供任何設定「中獎獎金匯入金融帳戶之網址連結」，請民眾注意。

民眾設定中獎獎金匯入金融帳戶，請自行至財政部電子發票整合服務平台官方網址：「<https://einvoice.nat.gov.tw>」進行設定。財政部提醒，電子發票服務不會指示您操作 ATM，如接獲不明及可疑電話或簡訊，應立即撥打財政部電子發票整合服務平台「客服專線 0800-521-988」或刑事局「165 反詐騙電話」，保持鎮定並再三查證，以免落入詐騙陷阱。

TWCERT/CC 提醒民眾，注意這起釣魚事件手法，切勿點選該電子郵件附件及相關連結，若發現資安事件可向 TWCERT/CC 通報。

以下連結為官方通報網站入口頁面，請多加利用：
https://www.twcert.org.tw/subpages/securityReport/simple_normal.aspx



資料來源：

<https://www.einvoice.nat.gov.tw/home/Article!showArticleDetail?articleId=1517278017153>

3.2.3、印度銀行 SWIFT 系統遭駭，遭試圖盜轉近 200 萬美元

印度 City Union Bank(城市聯合銀行)SWIFT 系統遭駭客攻擊，查證有三筆詐欺式交易，其中一筆超過百萬美金，所幸另外兩筆分別在銀行端以及接收銀行端被阻止，並表示非內部員工所為。

根據官方所發布之新聞稿指出，2 月 17 日及 18 日該銀行遭到駭客入侵其 SWIFT 系統試圖跨國匯款轉帳，並發現有三筆透過 SWIFT 金融平台嘗試未經授權的欺詐性匯款，總計金額近 200 萬美元。

其中一筆總額為 50 萬美元的匯款，在嘗試透過紐約渣打銀行帳戶發送給總部位於杜拜的銀行時被阻止，另一筆 30 萬歐元的轉帳則是透過法蘭克福的渣打銀行帳戶轉到土耳其帳戶，所幸土耳其銀行也阻止轉帳完成，第三筆總計 100 萬美元的轉帳交易則是透過在美國紐約的銀行帳戶發給了一家中國銀行，印度 City Union Bank 執行長在 2 月 18 日確認為中國杭州浙江農村信用合作社。

印度 City Union Bank 表示，目前沒有任何內部工作人員參與的證據，然確信該帳戶持有者應即為此事件關鍵人。銀行業安全專家表示，依賴 SWIFT 金融平台的印度銀行需要更加警惕。業內專家表示，印度有超過 100 家金融機構與包括央行在內都含有 SWIFT 相關系統。



資料來源：

<http://www.moneycontrol.com/news/business/companies/city-union-bank-cyber-attack-successfully-retrieved-block-money-in-2-out-of-3-cases-2510837.html>

https://www.cityunionbank.com/downloads/Press_Release_swift.pdf

3.3、軟硬體漏洞資訊

3.3.1、開發工具 Electron 有登錄值隱憂，危及 Windows 程式

GitHub 發展的開放框架 Electron(早期命名 Atom Shell)，可結合 Node.js 與 Chromium 引擎開發 GUI 應用程式，本次弱點生效條件為 Windows 作業系統上 APP，且編輯 APP 為登錄值內預設協定處理器，使用者在 Electron 開發之 APP 操作介面時，有可能因滑鼠點擊惡意 URL，而連結到遠端指令並即刻執行，鑒於 Electron 所開發軟體應用過於廣泛，GitHub 暫緩公開漏洞細節，待各開發商完成修補後，終端用戶始可更新。



資料來源：

<https://thehackernews.com/2018/01/electron-js-hacking.html>

<https://electronjs.org/blog/protocol-handler-fix>

3.3.2、Mozilla 釋出例行更新，緊急追加 Firefox 修補項目

近期 Firefox、雷鳥系列軟體常態更新，改善眾多元件功能，避免使用釋放後記憶體而衍生 crash，諸如 Skia library 運用不當記憶體區段而觸發 Integer overflow、XSL 轉換文件、widget listener、表單輸入值、媒體元件、字型等運算階段均有機會引起 Use-after-free 狀態；而從右至左文字經反序顯示網址，其 URL 將

誤導使用者；當然也修補些許 Memory 安全性缺陷以杜絕遠距代碼執行，但安全更新甫公告未逾一週，Mozilla 旋即追加修補 Firefox 嚴重漏洞，肇因於 Chrome-Privileged 文件(瀏覽器介面)內存有片段 HTML 資料，缺乏完整過濾，難防惡意輸入之後遺，若用戶身為系統管理者而誤入社交工程陷阱，則控制權悉數轉移至駭客手中。囿於新版 Firefox 倉促釋出，雖解決安全瑕疵卻伴隨功能缺陷，經實測，其外掛程式互動詢問介面失去鍵控功能，使用時須留意。



資料來源：

<https://thehackernews.com/2018/01/firefox-browser-update.html>
<https://www.mozilla.org/en-US/security/advisories/mfsa2018-05/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2018-02/#CVE-2018-5091>

3.3.3、封包分析工具 Wireshark 可能遭受 DoS 攻擊

資訊界普遍運用之免費開放網路封包分析工具 Wireshark(前身 Ethernet)，以 C 語言編撰各副程式，其中 IxVeriWave 解析器無法辨識簽章的異常時間戳記；WCP dissector 未驗證有效 buffer 長度；而 JSON、XML、NTP、XMPP、GDB 等 dissector 俱有觸發堆疊 overflow 之機會，既然疏於妥處例外狀況，處理遠端注入惡意封包結構時，可能導致程式 Denial of Service 狀態，Wireshark 已釋出升級軟體進行安全更新。



資料來源：

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14297

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14251

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14253

3.3.4、餐旅 POS 系統 Hospitality Symphony 測出路徑造訪漏洞

餐旅業常用 POS(point-of-sale)支付系統輔助經營，Hospitality Symphony 原為酒店技服商 MICROS 公司開發，後 MICROS 為甲骨文收購，經測 Hospitality Symphony 存在目錄遍歷弱點，駭客能循 HTTP 協定回傳用戶姓名及密碼 hash 加以破解，鑒於全球用戶多達 33 萬，其風險不容小覷，Oracle 已修補相關版本軟體。



資料來源：

<https://thehackernews.com/2018/01/oracle-micros-pos.html>

<https://erpscan.com/advisories/erpscan-18-002-oracle-micros-pos-missi>

3.3.5、全球 WordPress 開發網站皆面臨 DoS 嚴峻危機

開放原始碼的部落格軟體 WordPress，以 PHP 和 MySQL 為開發基礎，世界上 29% 網站以其建置專屬內容管理系統(Content Management System, CMS)，以色列研究員 Barak Tawily 檢視原設計，考量管理效率，建立 load-scripts.php 批次載入功能與 wp_scripts 完整 javascript file 清單，綜合兩者發覺漏洞乃 1 次請求可載入 181 個 JS 模組，駭客無需身分驗證，即可無限發送正常 HTTP 請求，行使強力 DoS，若輔以 doser.py 或類似工具，在非對稱、連續性請求及回應封包往來過程中，癱瘓目標網站硬體資源，Barak Tawily 已就此事向 WordPress 官方申請錯誤通報獎金，然官方否認該漏洞係 OSI 第 7 層事件，故不予受理亦無更新計畫，Barak Tawily 請獎未果之餘，仍研發修補版 WordPress 並公布，網站維護者請迅速處置。



資料來源：

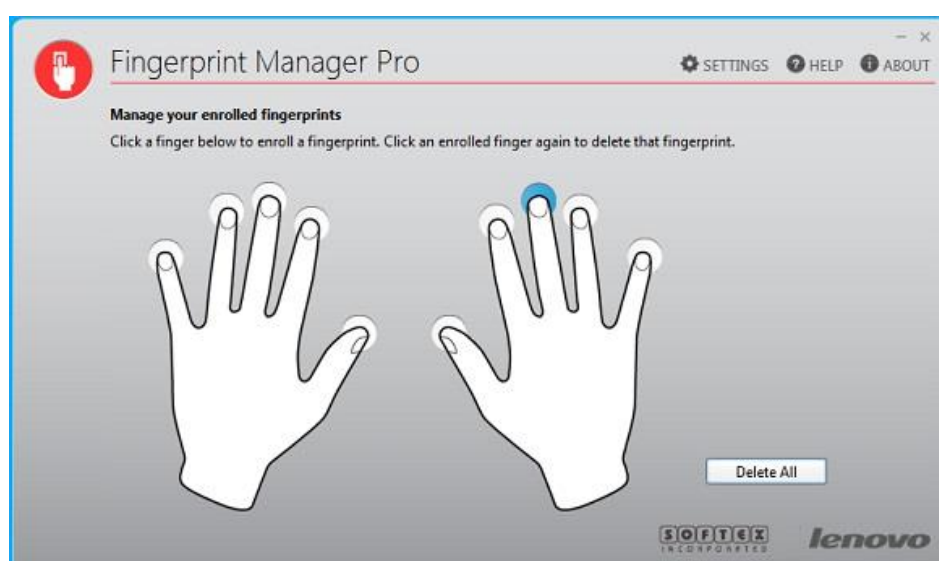
<https://www.youtube.com/watch?v=nNDsGTalXS0&feature=youtu.be>
<https://baraktawily.blogspot.tw/2018/02/how-to-dos-29-of-world-wide->

[websites.html](#)

<https://securityaffairs.co/wordpress/68709/hacking/cve-2018-6389-wordpress-dos-flaw.html>

3.3.6、Lenovo 指紋辨識系統 hard-code 密碼隱憂

近日聯想(Lenovo)公布其指紋辨識系統漏洞，原應保護硬體的 Fingerprint Manager Pro 反大開方便門，咎於一組寫死密碼，讓任何人可以操作 Fingerprint Manager Pro，順便破解聊勝於無的加密，取得機敏身分憑證後直接控制設備，影響遍及 36 種型號之筆電、桌機及工作站，除非作業系統是內建指紋辨識的 Windows 10 始得倖免，Lenovo 已釋出最新版軟體，但禍不單行，2016 年 10 月到 2017 年 10 月期間出廠的 ThinkPad X1 Carbon 筆電，恐因螺絲鬆脫釀成電池高熱起火，持有者請優先送修，切莫開機更新指紋辨識系統。



資料來源：

<https://www.youtube.com/watch?v=JRA34PzvANg&feature=youtu.be>

<https://pcsupport.lenovo.com/tw/zh/downloads/ds034486>

<https://thehackernews.com/2018/01/lenovo-fingerprint.html>

3.3.7、VPN 軟體 Pulse Secure Linux 用戶 SSL 連線恐遭中間人操控

Pulse Secure, LLC 過往隸屬 Juniper Networks 的 Junos Pulse 產品線，後由 Siris Capital 收購，專職開發 SSL VPN 遠端存取服務，近期檢測 Pulse Secure(Linux 版)用戶端程式 GUI，發現安全性弱點，囿於 WebKit 忽視 SSL 錯誤事件，且 WebKit 組態凌駕 JavaScript，導致程式疏於嚴謹查驗 SSL 憑證，無法警覺駭客介入 GUI 與 VPN 伺服器之間，任意變造連線內容，欺騙受害者誤信圖形介面所示資訊，據稱該公司企業客戶約 2 萬，包括數所國立大學，此漏洞應有一定影響規模，Pulse Secure 已完成升級版軟體，使用者可趁此契機，養成安全操作習慣，選擇適合網路環境，或者練習傳統指令。



資料來源：

http://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA43620

<http://www.kb.cert.org/vuls/id/319904>

3.3.8、Joomla! 釋出新版防止 SQL injection 及 Cross-Site Scripting

開放原始碼的架站軟體 Joomla!，具備網頁內容管理功能，經查

具 4 項輸入值驗證缺失，迫使後台模板 hathor 受 SQL injection 影響，可能於 postinstallation message 介面不當暴露隱私資料；另外 Cross-Site Scripting 亦發生在 Uri 類別、com_fields 參數及 chromes 模組等三方面，相關參數夾藏惡意 payload 且未經充分過濾，分別於相異介面環境執行腳本碼，恐讓駭客竊取 cookie 類型憑證資料，Joomla! 原已針對安全性漏洞升級至 3.8.4，然一週內又改善部分錯誤，公布 3.8.5 版軟體供下載更新。



資料來源：

<https://developer.joomla.org/security-centre/722-20180105-core-sqli-vulnerability.html>

<https://paper.seebug.org/529/>

3.3.9、Skype 安全更新流程出現致命 DLL hijacking 破綻

通訊應用軟體 Skype 曾陸續被 eBay、Microsoft 收購，可運行於各種桌機與行動裝置，據最新資安消息，其安全更新流程出現瑕疵，若受害者下載惡意動態連結函式庫(DLL：Dynamic-link library)，假冒 DLL 檔名變更後瞞過更新檔 installer，令 Skype 使用惡意函式庫內程式，駭客將獲得系統管理者權力，遠端接管作業系統，然微軟宣稱不投注人力重編程式進行安全更新，待下回新版用戶端發行時一併解決，此件 DLL hijacking 波及範圍不限於 Windows，漏洞已揭發且使用者眾，恐釀嚴峻資安災情。



資料來源：

<http://www.zdnet.com/article/skype-cannot-fix-security-bug-without-a-massive-code-rewrite/>

3.3.10、駭客藉 Telegram 0-day 漏洞 RLO 散佈挖礦病毒

俄羅斯 Telegram Messenger LLP 公司設計之 Telegram Messenger，算是繼 LINE 之後，頗受矚目的一款跨平台即時通訊軟體，其 client 端開放原始碼(可中文化)，然 server 是專有軟體，經查 Telegram Messenger 有一 0-day 漏洞已遭資訊犯罪者濫用，散播 Monero、ZCash 等挖礦程式，且能暗植各種後門，劫持主機控制權，其手法與 2009 年如出一轍，俱利用 Unicode16 進位的 RLO(right-to-left override)反轉字元，將後段主副檔名反轉，以此障眼法結合社交工程遂行駭侵行動，目前受害者集中於俄境內 Windows 版 Telegram Messenger 用戶，Kaspersky 通知 Telegram Messenger LLP 公司後，該公司即刻回應修補對策，本次弱點從發現到修復頗為迅速，尚來不及申請 CVE 編號。



資料來源：

<https://securelist.com/zero-day-vulnerability-in-telegram/83800/>

<https://thehackernews.com/2018/02/hackers-exploit-telegram-messenger-zero.html>

3.3.11、趨勢科技數款軟體 UMH 模組具 DLL 劫持弱點，另 IMSVA 日誌內容遭任意存取

Trend Micro 發展反制勒索軟體之 User-Mode Hooking 引擎技術，能提供 API 事件訊息給其他模組，支援預判與監視相關決策，經測試存在 DLL 劫持缺失，恐引發執行任意碼，鑒於 DLL 本是微軟共享函数的方法，此漏洞影響 Windows 平台上 OfficeScan、Worry-Free Business Security、Deep Security、Endpoint Sensor 及 Trend Micro Security 等企業級軟體安全性；另駭客能經由 InterScan Messaging Security Virtual Appliance 之網頁介面，接觸/widget/repository/log/路徑下系統日誌，分析獲取重要憑證資料，趨勢科技已就各版軟體提供對應之更新程式。



資料來源：

<https://success.trendmicro.com/solution/1119326#>

<https://korelogic.com/Resources/Advisories/KL-001-2018-006.txt>

3.3.12、印度泰盧固語系文字造成 Apple 裝置通訊功能停擺

印度傳統母語泰盧固文字(如圖)，若出現在 Apple 裝置上將造成系統當機，囿於 tvOS、watchOS、iOS、macOS 等作業系統均內建 CoreText 元件，用途為處理字串，一旦面對 Telugu 符號，則不斷重複無效載入，已確知該瑕疵能干擾 iMessage、slack、Facebook Messenger、WhatsApp、Gmail、Outlook for iOS 及 Safari 等網路通訊，Apple 針對此輸入驗證弱點，於春節期間改善 4 種 OS，由於此類 text bomb 手法無須駭客技術，普通人即可引發 DoS，故尚無法安裝更新的 Apple 裝置持有者，遇此窘境可請旁人傳訊(絕非泰盧固文)，促使通訊程式跳轉至新訊息通知，趁機清除被印度文困住的執行緒，年假為國人問候訊息最為頻密時期，應謹慎留意聊天軟體異狀。



資料來源：

<https://support.apple.com/en-us/HT208535>

<https://www.pcmag.com/news/359282/this-indian-character-symbol-can-crash-your-iphone>

3.3.13、駭客探勘 PyBitmessage 0.6.2 即時通 0-day 漏洞，利用 RCE 竊取比特幣錢包

奧地利 Peter Šurda 仿 Bitcoin 原理開發 Bitmessage 即時通軟體，適用 Linux、Mac 及 Windows 平台，無需中央伺服器即可於本機交換密鑰，支援 P2P 通信協定，以 37 字元 hash 值作用戶地址，落實隱匿身分來源效果，其正式版 PyBitmessage 0.6.2 近日遭駭客鎖定，利用訊息內容引發 RCE，使自動化 script 對受害主機進行搜尋，嘗試找出比特幣錢包密鑰後，反向 Shell 回傳，據報已有多起資訊犯罪案件，皆與加密貨幣市場熱潮有關，經測試僅有 PyBitmessage 0.6.2 版涉此弱點，Bitmessage 已公開解決方案，舊版 0.6.1 或升級 0.6.3.2 版，用戶擇一即可，若仍有顧慮，可換密並產生新 key。



資料來源：

<https://www.antimalware.news/how-hackers-attacked-pybitmessage-to-steal-bitcoin-wallet-key/>

<https://zh.wikipedia.org/wiki/%E6%AF%94%E7%89%B9%E4%BF%A1>

https://bitmessage.org/wiki/Main_Page

3.3.14、隨身碟 label 竟可在 Plasma 圖形桌面環境執行命令

國際性自由軟體協會 KDE，就 Linux、BSD、Solaris、Windows 及 macOS 等作業系統，開發跨平台應用程式，旗下「電漿工作空間 (Plasma Workspace)」專案團隊專職設計圖形環境，其中 Plasma Desktop 為多數 Linux 發行版的預設桌面，用戶較廣泛，經測試出現

高風險漏洞，Plasma Desktop 對隨插即用 USB 儲媒以通知器面板開啟時，對磁碟 label 名稱無過濾機制，label 內以貨幣符號加括弧 \$() 或雙撇 ``，中間加藏指令字串會被 Plasma Desktop 執行，KDE 已公布新版軟體及修補檔。



資料來源：

http://www.theregister.co.uk/2018/02/12/kde_naming_usb_drive_vuln/

<https://www.kde.org/info/security/advisory-20180208-2.txt>

3.4、資安研討會及活動

時間	研討會/課程名稱	研討會相關資料
2018 年 03 月 09 日、16 日、23 日	金融科技資 訊安全專業 精修班	【資安訓練課程】金融科技資訊安全專業精修班 主辦單位：台灣金融研訓院、中華民國電腦稽核協會 課程時間：2018 年 03 月 09 日、16 日、23 日 受訓地點：台灣金融研訓院本部(台北市羅斯福路三段 62 號) 線上報名連結： http://service.tabf.org.tw/tw/user/325462/ 課程簡介： 資通訊科技帶來許多金融創新契機，卻也成為全球駭客入侵之犯罪溫床，近年來勒索攻擊事件層出不窮，動輒數千萬美金的損失，也讓各國機構企業無不正視資訊安全問題。本院特辦理「金融科技資訊安全專業精修班」課程，邀聘各界優秀師資，以資安專才應具備之專業職

時間	研討會/課程名稱	研討會相關資料
		能為根基，進行課程主題規劃，以期完備資安專業培訓內容與需求，協助企業於投入金融服務創新之際，打造最安全的後盾，全面提升組織資安防禦力！ 課程大綱： 1. Fintech 應用與科技風險 2. 網路弱點辨識與評估實務 3. 網路身分認證 4. 個資安全稽核 5. 資通訊網路安全技術與應用 6. 智慧金融治理與應用程式開發安全實務
2018 年 03月15日	舞弊稽核與數位鑑識系列_常見駭客入侵手法說明及滲透測試檢測實務	【資安訓練課程】舞弊稽核與數位鑑識系列_常見駭客入侵手法說明及滲透測試檢測實務 主辦單位：中華民國電腦稽核協會 課程時間：2018 年 03 月 15 日(四) 受訓地點：電腦稽核協會訓練教室(台北市信義區基隆路 1 段 143 號 2 樓之 2) 線上報名連結： http://bit.ly/2Ey4rOK 課程簡介： 針對常見駭客入侵手法進行介紹，另於課程中會帶領學員操作常見鑑識分析工具，如針對伺服器與系統稽核日誌，並將其所對應調查之證據來源予以說明。 課程大綱： 1. 網路安全趨勢概述 2. 駭客入侵手法說明 3. 滲透測試於資安防禦之應用 4. 滲透測試檢測工具說明 5. 滲透測試檢測實作

時間	研討會/課程 名稱	研討會相關資料
2018 年 03月13日 至03月15 日	2018 臺灣資 安大會	【資安研討會】2018 臺灣資安大會 主辦單位：iThome 日期：2018 年 3 月 13 日至 15 日 地點：台北國際會議中心 TICC (台北市信義路五段 1 號) 線上報名連結：http://bit.ly/2kWAwUB 活動概要： 今年主題聚焦「Cyber First Cyber Taiwan 建構資安優先意識、看見臺灣的資安動能」，三天會期總計超過 140 場議程，涵蓋高達 60 種熱門資安議題與技術面向，更從新興科技、典範轉移，以及軟體開發與硬體設計等面向深入資安死角，全方位關照資安。 現場更囊括 700 種以上主流資安產品與解決方案一次看盡，無論你對資安的了解或多或少，來到現場都能找到下一步對策，再造企業核心競爭力！ ● Keynote 國內外資安專家齊聚演講 ● Cyber First 熱門資安議題技術論壇 ● Cyber LAB 史上最強攻防實機體驗 ● Cyber Taiwan 臺灣資安館聚焦自主研發 ● Cyber Security Expo 百大資安展遍覽知名廠牌 ● CIO/CISO 資安長專屬前瞻策略會議
2018 年 03月14日 - 15 日	2018 臺灣資 安大會 CISO 論壇	【資安研討會】2018 臺灣資安大會 CISO 論壇 主辦單位：iThome 日期：2018 年 3 月 13 日至 15 日 地點：台北國際會議中心一樓 103 會議室(台北市信義路五段 1 號) 線上報名連結：

時間	研討會/課程 名稱	研討會相關資料
		https://seminar.ithome.com.tw/live/2018CISO/index.html 活動概要： 資安威脅無所不在，不再是一句嚇人的話。2017 年所發生的大大小小資安事件，除了記憶猶新的 WannaCry 勒索軟體肆虐與駭客盜領銀行數百億，其實上自宇宙的衛星通信，下至地面的陸海空交通、工業工廠、金融服務、電力供應等關鍵基礎設施，皆已淪為網路犯罪組織與國家駭客的囊中物。 甫出爐的世界經濟論壇 2018 全球風險報告，更將網路攻擊列為僅次於氣候變遷與天然災害的全球第三大風險。因為，資安威脅已不可同日而語，我們現在所經歷的網路攻擊，不僅速度快、衝擊大，影響規模甚至動輒遍及全球。 資安威脅已成為新常態，駭客攻擊足以讓執行長下臺，而董事會也得開始面對資安議題。現在，是重新思考資安策略的時候了。2018 臺灣資安大會 CISO 論壇將邀請國內外知名資安長，分享資安典範轉移與資安策略新思維，與大家一起重新思考資安新策略。
2018 年 03月15日	2018 資安&雲端應用新趨勢-嶄新價值共創企業生產力研討會	【資安研討會】2018 資安&雲端應用新趨勢-嶄新價值共創企業生產力研討會 主辦單位：Acer 宏碁資服商軟 日期：2018 年 3 月 15 日(四) 地點：台北維多麗亞酒店 3 樓維多麗亞廳(104 台北市敬業四路 168 號) 線上報名連結： https://www.accupass.com/event/1802231053001265935370 活動概要： 經過 2017 年眾多資安事件的摧殘，大家應該更有體

時間	研討會/課程名稱	研討會相關資料
		認：在資訊安全的世界裡，無法達到所謂百分之百的安全，在事件發生時，為了要降低可能的損害，就需要事先建立處理應變的方式，才能將衝擊降到最低，以便在災害擴大時，仍能保持業務營運的正常水準。接下來，台灣各產業將迎面號稱史上最嚴格的歐盟資料保護規範(GDPR)、無論您的產業及產品是否與歐盟相關，都應該關注這個全球矚目的新動態！面對全球化、數位化所帶來快速變局的您，怎麼不能好好把握這個時機，一起來快速提升產業價值，創造企業生產力！
2018 年 03月17日	事故回應與處理	【資安訓練課程】事故回應與處理 主辦單位：亥客書院 課程時間：2018 年 03 月 17 日(六) 受訓地點：國立交通大學 台北校區(台北市中正區忠孝西路一段 118 號) 線上報名連結： https://hackercollege.nctu.edu.tw/?p=590 課程簡介： 本課程內容包含資安事件處理流程與步驟、資安事件應變處理技術、運用 autopsy 處理資安事件案例、及運用 SIFT 處理資安事件案例等。 課程大綱： 1. 資安事件處理流程與步驟 2. 資安事件應變處理技術 3. 運用 autopsy 應變處理資安事件案例 4. 運用 SIFT 應變處理資安事件案例
2018 年 03月22日	化被動為主動的資安新思維	【資安研討會】化被動為主動的資安新思維 主辦單位：華電聯網 日期：2018 年 3 月 22 日(四) 地點：台北威斯汀六福皇宮(台北市中山區南京東路三

時間	研討會/課程 名稱	研討會相關資料
		段 133 號) 線上報名連結： http://www.digitimes.com.tw/seminar/HwaCom_20180322/ 活動概要： 隨著物聯網的世代來臨，資安防護備受重視。但資安設備產生的大量數據資料，如何被即時的分析，並協助企業採取正確的資安防衛，是企業面臨的重大挑戰。 將於本次活動提出具體且有效的解決方案：快速存取的數據方案、大數據分析的平台、以數據分析來做行為模式分析的資安思維、化被動為主動的資安新思維。
2018 年 04月15日	106-107 年 週日閱讀科學大師系列 講座-資訊安全威脅與防護	【資安研討會】106-107 年週日閱讀科學大師系列講座-資訊安全威脅與防護 承辦單位：國立科學工藝博物館、國立高雄應用科技大學、國立成功大學、財團法人國家實驗研究院國家高速網路與計算中心 日期：2018 年 4 月 15 日 10:00-12:00 地點：國立科學工藝博物館南館國際演講廳(高雄市三民區九如一路 797 號) 講師：國立成功大學暨國網中心 李忠憲 教授 報名方式： (1)網路報名：先於報名系統 (https://serv.nstm.gov.tw/)註冊會員，登入後即可報名 (2)電話報名：(07)380-0089 分機 5137 或 8100 線上直播： http://demo.dracosky.net/cs_demo/nchc/ 資料來源： http://science.nchc.org.tw/web/index?cp=home

第 4 章、2018 年 02 月份事件通報統計

本中心每日透過官方網站、電子郵件、電話等方式接收資安事件通報，2018 年 2 月收到通報計 286 筆，以下為各項統計數據，分別為通報來源統計圖、通報對象統計圖及通報類型統計圖。

通報來源統計圖為各國遭受網路攻擊事件，屬於我國疑似遭利用發起攻擊或被攻擊之 IP，向本中心進行通報之次數，如圖 1 所示；通報對象統計圖為本中心所接獲之通報中，針對通報事件責任所屬國家之通報次數，如圖 2 所示；通報類型統計圖則為本中心所接獲的通報中，各項攻擊類型之筆數，如圖 3 所示。

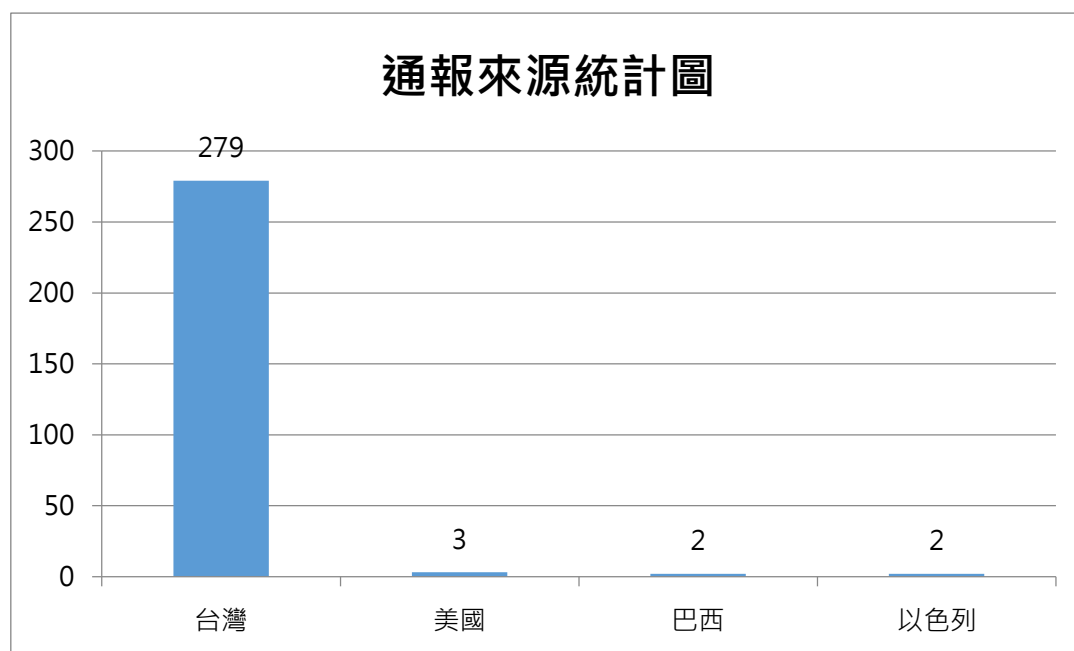


圖 1、通報來源統計圖

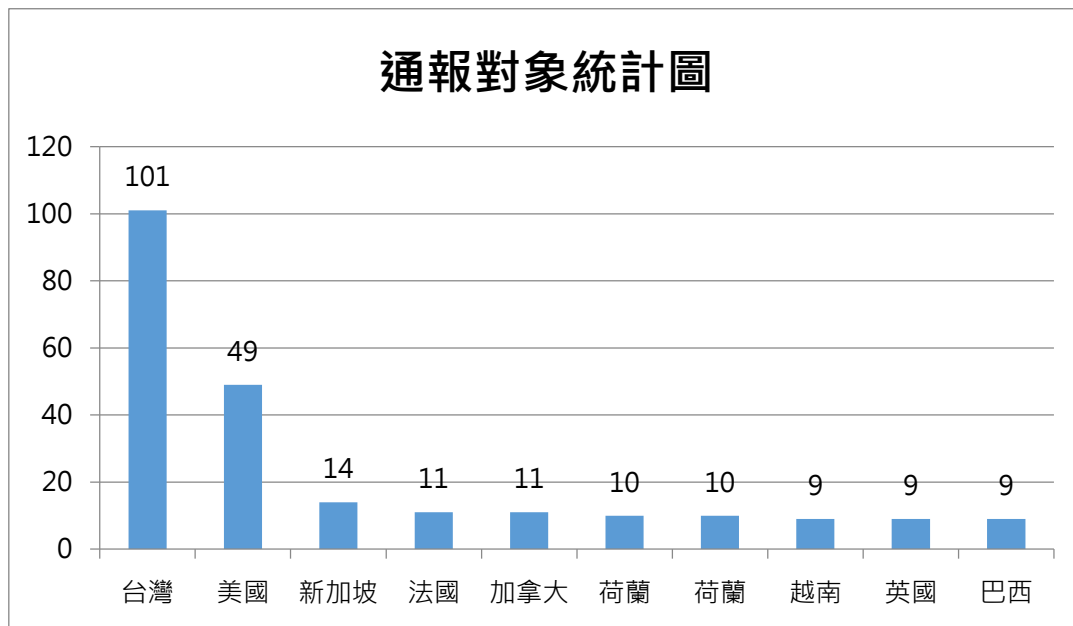


圖 2、通報對象統計圖

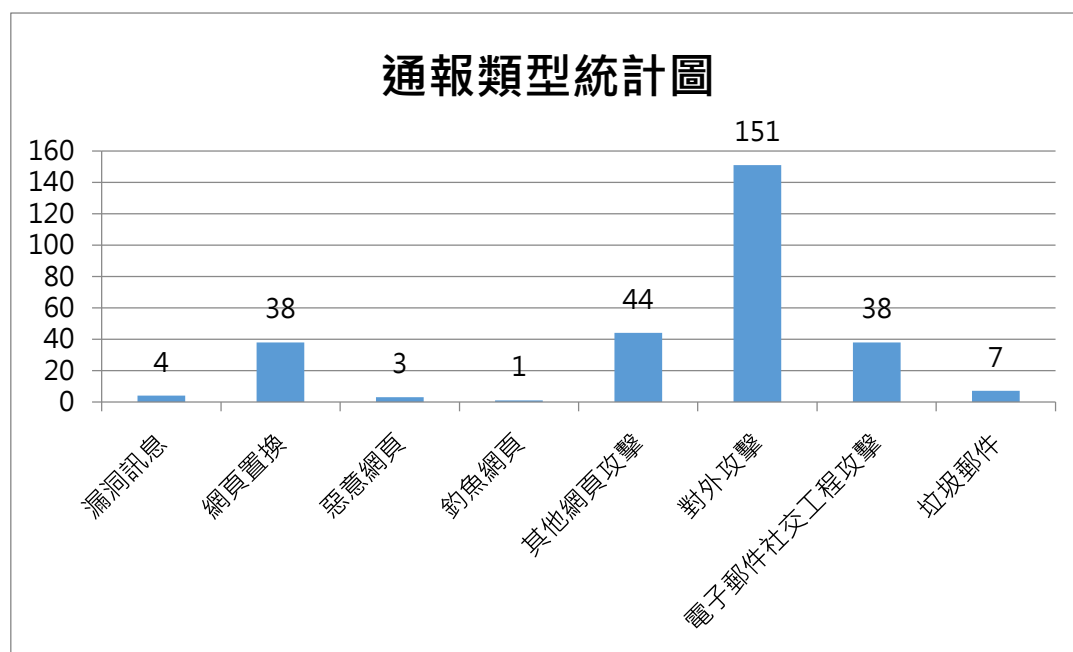


圖 3、通報類型統計圖

本月以「遭植入挖礦腳本」網站屬特殊案件。挖礦(Mining)是獲取比特幣的探勘方式的暱稱。比特幣則由比特幣網路產生，該網路一開始是每十分鐘產出一定數量的比特幣，而產生的速度會再隨著時間

遞減。想得到比特幣，只能利用隨機產生 hash 值，並看該值是否能夠碰撞，若能產生碰撞則可取得比特幣，而這個運算 Hash 值並取得比特幣的過程就稱作挖礦。

剛開始是通過 Intel 或 AMD 的 CPU 產品來挖礦，後來有些礦工為了結省自行購買 CPU 之成本，將挖礦程式寫成惡意程式，例如 Coinhive(coinhive.min.js)，並嵌入至網頁中，而使用者瀏覽網站時，透過執行 JavaScript 程式，則可利用使用者電腦的資源挖礦賺取虛擬貨幣，造成使用者之電腦資源耗竭，若未告知使用者，可能會有潛在法律與道德的問題。有些線上免費套件會內藏此程式，而網頁開發者可能在不知情狀況下引用到內含惡意程式之套件。

近期頻傳駭客利用已知漏洞將原本用以傳播勒索軟體的工具改用以散播挖礦程式的事件，如 Smominru、WannaMine 病毒等利用來自 NSA 的漏洞攻擊工具感染數以萬計的電腦。

針對網頁挖礦的防堵，趨勢科技建議[1]，要避免瀏覽器執行 JavaScript 應用程式，防止 Coinhive 挖礦程式使用 CPU 資源。並定期修補、定期更新軟體，尤其是網頁瀏覽器，以降低加密貨幣挖礦程式的影響。

TWCERT/CC 建議，在發現開啟特定網頁時會造成 CPU 使用率大幅上升，導致電腦運行緩慢等嚴重影響效能等情事時，應即關閉瀏覽器離開頁面，若遇到已遭挖礦程式植入裝置之情況，則透過裝置管理員查找其惡意程式或使用防毒軟體偵查，並保持病毒碼最新，以免遭駭客挾持成為挖礦苦工。

資料來源：

[1] <https://www.bnext.com.tw/article/48162/mining-code-embedded>

發行單位：台灣電腦網路危機處理暨協調中心

(Taiwan Computer Emergency Response Team/Coordination Center)

出刊日期：2018 年 3 月 9 日

編輯：曾佩雅

服務電話：03-4115387

市話免付費服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官 網：<https://www.twcert.org.tw/>

粉絲專業：<https://www.facebook.com/twcertcc>

資安電子報訂閱：<http://i-to.cc/S5HzJ>

如有任何疑問或建議，歡迎您不吝指教。