



TWCERT/CC 資安情資電子報

2018 年 4 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、 協辦中華民國資訊軟體協會舉辦之「資訊安全前瞻商機研討會」	2
2.3、 TWCERT/CC 與 TACERT 簽訂合作備忘錄.....	3
第 3 章、 國內外重要資安新聞	4
3.1、 國內外資安政策、威脅與趨勢	4
3.1.1、 中國平價手機成為惡意軟體感染幫兇.....	4
3.1.2、 澳洲國防部禁用微信	4
3.1.3、 從駭客的角度看資安	5
3.1.4、 行政院推資安產業發展行動計畫	5
3.1.5、 辨識同形異義的假冒網址以避免被網路釣魚.....	6
3.2、 駭客攻擊事件及手法	6
3.2.1、 人在台北 Uber 境外連 5 刷	6
3.2.2、 Download[.]com 被發現散播竊幣軟體已近一年	7
3.2.3、 知名線上遊戲 Fortnite 遭駭，玩家帳號被盜用進行線上交易.....	9
3.2.4、 知名訂票網站「Orbitz」個資外洩，80 萬筆個資遭竊.....	10
3.2.5、 駭客利用舊漏洞以及針對更新遲緩的使用群，將 Linux 伺服器成為挖礦苦工，受害者包括台灣.....	11
3.2.6、 資安專家發現駭客在 YouTube 影片描述暗藏惡意連結	13
3.2.7、 美國亞特蘭大市政府遭受大規模勒索病毒攻擊	15
3.2.8、 SWIFT 資金盜轉事件再添一筆，所幸馬來西亞順利遏止	16

3.2.9、 印度電力公司的系統遭受勒索軟體感染	17
3.3、 軟硬體漏洞資訊	19
3.3.1、 留心 DNS rebinding 讓µTorrent 用戶主機一覽無遺	19
3.3.2、 網路攝影機 Pelco Sarix 系列出現數多漏洞，易遭遠端接管系統及檔案控制權	20
3.3.3、 近距攻擊華為智慧機，駭客得惡意聲控及竊取個資	21
3.3.4、 Citrix 網管設備 NetScaler 系列 ADC 及 Gateway，恐有檔案訊息暨控制權流失之虞	22
3.3.5、 歷代 Exim 郵件代理器版本均有 Base64 解碼函數計算瑕疵，恐招致預授權 RCE 侵襲	23
3.3.6、 修補 NTP 雙漏洞，避免校時服務錯亂	24
3.3.7、 熊貓安全 Global Protection 發生 DACL 錯誤，將受本機任意用戶全權操縱	25
3.3.8、 攻擊 Samba 嚴重缺陷，能隨意竄改密碼並阻礙列印	26
3.3.9、 檢查 Adobe Dreamweaver CC 暨 Connect 狀態，阻止 command injection 及檔案消失	27
3.3.10、 VPN Unlimited 恐讓任何程式能以 root 控制 mac OS X	28
3.3.11、 客製化韌體 Asuswrt-Merlin 記憶體崩壞，影響華碩 28 種硬體型號	29
3.3.12、 更新 Mac OS 平台專屬 Google Updater 以改善本機擴權缺點	30
3.3.13、 防 hash 碰撞效果低落，可暴力破解 Bouncy Castle 第 1 版 keystore 格式檔案	31
3.3.14、 版主火速更新 Drupal，重度威脅須臾即至	32
3.4、 資安研討會及活動	33
第 4 章、 2018 年 03 月份事件通報統計	39

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 副主任吳專吉於 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，針對企業內部員工上班業務及生活中較常遇到的資安事件案例與防護做法進行相關宣導，包含社交工程、電子信箱保護、釣魚郵件(網站)、Webcam 保護、可卸除裝置及勒索軟體防護等相關資安常識。



2.2、協辦中華民國資訊軟體協會舉辦之「資訊安全前瞻商機研討會」

TWCERT/CC 主任陳永佳於 2018 年 3 月 28 日擔任中華民國資訊軟體協會舉辦之「資訊安全前瞻商機研討會」講師，針對 TWCERT/CC 服務、107 年資安威脅趨勢及防護等進行分享。





2.3、TWCERT/CC 與 TACERT 簽訂合作備忘錄

近年來台灣發生數起重大資安事件，許多業者受到重大影響，現今資安防禦亦不再是單打獨鬥的時代，需透過各資安組織間的互助合作，達到資安聯防的目的，107 年 3 月 31 日 TWCERT/CC 與 TACERT 簽訂合作備忘錄，攜手打造穩健的網路安全環境。



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、中國平價手機成為惡意軟體感染幫兇

網路資安公司 Dr.Web 專家警告，已知有 42 款低階的中國製平價 Android 手機，在出廠前已經被植入「Triada」惡意軟體到系統當中，也就是說使用這些手機代表個人資料可能被竊取。



資料來源：

<https://technews.tw/2018/03/06/malware-triada-found-preload-in-android-phones/>

3.1.2、澳洲國防部禁用微信

擔心洩露國防機密，澳洲國防部以安全為由，下令禁止員工在工作手機內下載中國的通訊軟體「微信」(WeChat)。澳洲是繼印度之後，另一個禁用微信的國家，這個舉動也突顯了中國有可能利用通訊軟體從事「間諜活動」的疑慮正持續加深。



資料來源：

<http://news.ltn.com.tw/news/world/paper/1183473>

3.1.3、從駭客的角度看資安

趨勢科技資深協理張裕敏在 2018 臺灣資安大會上表示，駭客攻擊活動分成 5 個階段，動機、發想、開發、測試及散播，現在全世界發生層出不窮的資安事件，不是駭客正在攻擊的、或者已攻擊完成的，不然就是正在散播階段。想要在這場資安攻防戰中，取得制勝先機，就得在發想階段、開發，甚至駭客動機階段，就得知駭客準備做什麼，或對哪些目標感興趣，才能做到更早的預警。

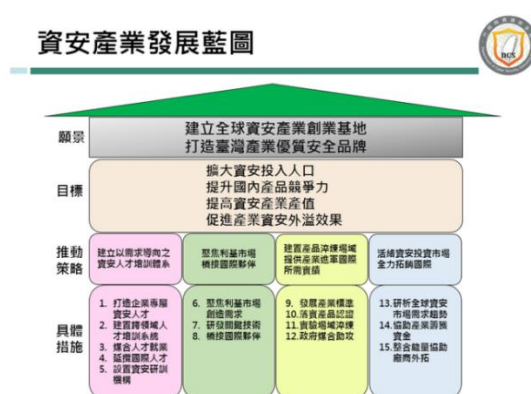


資料來源：

<https://news.tvbs.com.tw/life/886560>

3.1.4、行政院推資安產業發展行動計畫

行政院長賴清德於 22 日推「資安產業發展行動計畫」，以「建立全球資安產業創業基地，打造臺灣產業優質安全品牌」之願景，預期在 2025 年資安投入人口數成長至萬人，資安產值達 780 億元以上。



資料來源：

https://www.ey.gov.tw/News_Content.aspx?n=4E506D8D07B5A38D&s=25626DA37B0F05A7

3.1.5、辨識同形異義的假冒網址以避免被網路釣魚

IDNA 有一個致命的問題，那就是這種可以由不同語系字符組成的域名，可以透過註冊一個類似的網域名稱來仿冒成另一個網站，此一偽造的網站所註冊的網址採用了非屬美國訊息交換標準代碼 (ASCII) 的字符，這些字符看起來像英文字，但其實它們並不是。



資料來源：

<https://times.hinet.net/news/21613306>

3.2、駭客攻擊事件及手法

3.2.1、人在台北 Uber 境外連 5 刷

台北市林姓男子，接獲銀行簡訊指他的信用卡疑有異常消費，客服人員隨即來電告知，同一時間內有 5 筆在國外 Uber 消費，研判應是遭到盜刷，會立即幫林男停卡、換卡。刑事局表示，今年起開始出現多起盜刷 Uber 車資的案件，至今已接獲近 10 起報案。

多家銀行也主動發現多筆可疑消費。林男表示，當初下載 Uber App 時，有輸入、綁定扣款的信用卡號，但在去年 Uber 宣布退出台灣市場後，就刪除 App 不曾再叫車。

他說，此次遭盜刷的 5 筆都是以英鎊計費，換算台幣金額從 833 元到 400 多元台幣不等，與之前盜刷台幣不同，也看不到行車紀錄。

TWCERT/CC 提醒，在 2016 年 10 月 Uber 就發生過資料外洩事件，當時導致 5700 萬名客戶資料外洩，如參考連結 2，再次提醒

民眾：

- Uber 使用者應確認信用卡帳單有無異常交易。
- 若 Uber 的用戶發現曾有異常交易情況發生，則建議更換密碼為 20 個字元英文、數字、符號混和的強密碼，並立即通報發卡公司核對該筆交易。
- 為避免駭客冒用 Uber 公司名義發送密碼更改要求信件，用戶應詳細確認寄件來源與相關連結。
- 若有其他疑問或資安事件，歡迎向 TWCERT/CC 通報，官方資安通報網站或洽免付費服務電話：0800-885-066。



林姓男子已把手機上的Uber叫車軟體刪除，卻仍發現盜刷事件，圖為Uber在台灣使用情形。（林郁平翻攝、本報資料照片）

入帳 起息日	交易說明	新臺幣金額	卡號 後四碼	行動卡號 後四碼	消費 國家	幣別
01/30	網路轉帳繳款	-4,107				
02/08	一筆其實某韓式	500	1658		TW	TWD
02/14	國外交易手續費-UBERU	12	7544			
02/12	UBER UMMZP HELP.UBER.C	833	7544		NL	GBP
02/14	國外交易手續費-UBER2	7	7544			
02/12	UBER 2XOO2 HELP.UBER.C	486	7544		NL	GBP
02/14	國外交易手續費-UBERX	5	7544			
02/12	UBER XSHVJ HELP.UBER.C	364	7544		NL	GBP
02/14	國外交易手續費-UBERJ	7	7544			
02/12	UBER JDEDY HELP.UBER.C	460	7544		NL	GBP
02/14	國外交易手續費-UBERB	7	7544			
02/12	UBER BV	471	7544		NL	GBP

資料來源：

<http://www.chinatimes.com/newspapers/20180301000496-260106>

<http://news.ltn.com.tw/news/politics/breakingnews/2261369>

https://www.twcert.org.tw/subpages/securityReport/simple_normal.aspx

3.2.2、Download[.]com 被發現散播竊幣軟體已近一年

在 Download[.]com 被發現用以竊取 Bitcoin 虛擬貨幣的惡意軟體，能將受害者帳戶與攻擊者帳戶互換。

ESET 研究人員在 download[.]cnet[.]com 上發現了三個有木馬功能的應用程式，該連結根據全球知名的網站流量排名 Alexa，排名世界第 163 位。

根據最近的一篇部落格文章，截至 3 月 13 日，估計攻擊者設法竊取了相當於 80,000 美元的金額。文章表示，該惡意軟體自 2016 年 5 月 2 日以來一直託管在 Download[.]com，並且它已從該網域的原始創建者 CNET 下載總計超過 4500 次。

研究人員警覺到該惡意軟體，是因為在 Reddit 有用戶張貼了一張照片，顯示他們試圖複製和貼上他們的 Monero 錢包地址時，突然收到通知指出該地址因無效而被拒絕。

惡意軟體的來源是從 Download[.]com 下載有木馬功能的 Win32 Disk Imager 應用程式，研究人員檢查發現，惡意軟體會攔截複製貼上到剪貼簿中的錢包地址，並將其替換為攻擊者自己的硬編碼 (hard-code) 比特幣錢包地址。

雖然研究人員發現大約在 2017 年 3 月期間 Download[.]com 上的該惡意軟體已經被移除，仍然建議那些受影響的人可以透過刪除下載的反安裝程序，刪除惡意資料夾並從密鑰中刪除 ScdBcd 註冊表值來清理受感染的系統。



資料來源：

<https://www.scmagazine.com/eset-researchers-found-three-trojanized-applications-hosted-on-downloadcnetcom-163th-most-visited-site-in-the-world/article/751114/>

<https://www.welivesecurity.com/2018/03/14/stealing-bitcoin-download-c>

3.2.3、知名線上遊戲 Fortnite 遭駭，玩家帳號被盜用進行線上交易

Fortnite(堡壘之夜/要塞英雄)玩家請注意，據報導近日數個 Fortnite 帳號被駭客入侵並被用來透過綁定的信用卡或 Paypal 等線上交易進行數百美元的欺詐性購買。

Fortnite 是 Epic Games 開發的一款非常受歡迎的多人沙盒生存遊戲，擁有全球數百萬玩家，這也使得它成為駭客和網路犯罪分子的眼中肥羊。

最近有大量用戶抱怨說其帳號遭到入侵濫用，甚至有案例是某青少年將他母親的信用卡綁定在該帳戶上。駭客因此得以透過該帳號盜用支付約 800 歐元。

此事件波及許多玩家，網路上可見大量受害者發布了多條推文，揭露他們的帳號被駭客入侵的狀況以及用於欺詐性購買的大小不一的金額。

Epic Games 已知此情況，僅表示確認是很常見的駭客技術所為，並敦促相關受害者如有任何問題，可儘速透過以下聯絡連結 (<http://fortnitehelp.epicgames.com/customer/portal/emails/new>)與公司聯繫。

TWCERT/CC 建議，線上服務應啟用雙因素身分驗證(2FA)，不要與任何人分享密碼，不要再使用之前可能已被破解洩露的密碼，特別小心網路釣魚詐騙，例如聲稱提供免費升級或遊戲優惠券，並切勿點擊任何連結或從不明電子郵件下載附件。



資料來源：

<https://www.hackread.com/fortnite-accounts-hacked-for-fraudulent-purchases/>

<https://kotaku.com/fortnite-players-are-getting-fraudulent-charges-for-hack-un-1823698792>

<http://fortnitehelp.epicgames.com/customer/portal/emails/new>

3.2.4、知名訂票網站「Orbitz」個資外洩，80 萬筆個資遭竊

美國知名旅遊訂票網站「Orbitz」遭受大規模個資外洩事件，其中超過 80 萬名註冊用戶的個資和財務資料可能被未知駭客竊取。

在向媒體發表聲明中，Orbitz 表示於 2018 年 3 月 1 日經過該公司深入調查後確定，事件發生在 2017 年 10 月 1 日至 2017 年 12 月，當時駭客訪問了舊的旅遊預訂平台，並竊走從 2016 年 1 月和 2017 年 12 月兩年的資料。

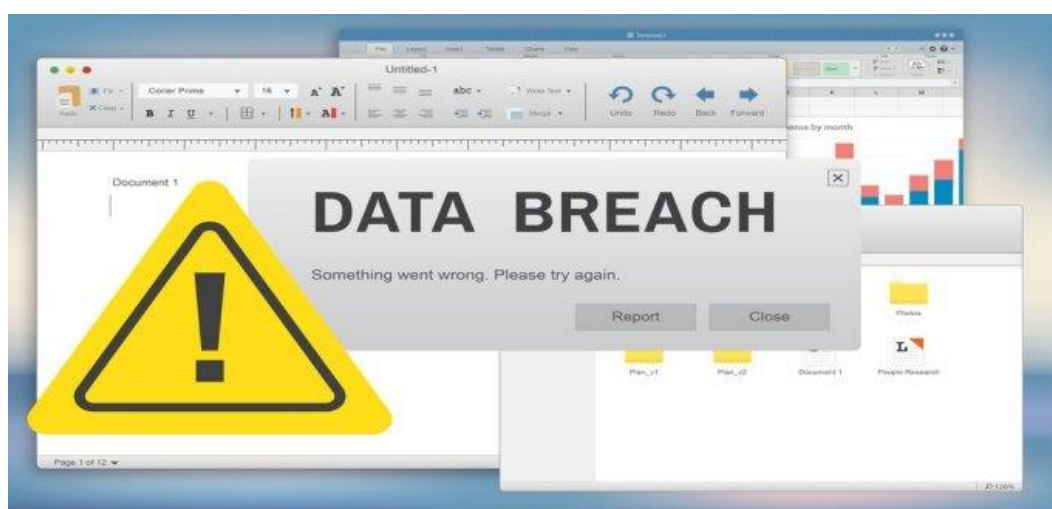
此外，在 2016 年 1 月 1 日至 6 月 22 日期間曾經透過平台進行交易的客戶的個人資料也可能被駭客存取。遭竊的資料細節包括姓名、電子郵件地址、電話號碼、性別、出生日期、郵遞區號、實際地址和銀行資訊如信用卡等詳細資料。

為了進一步調查這個問題，網路安全鑑識公司正在進行調查，同

時也向警方通報情況。該公司表示將儘快通知受影響的客戶和合作夥伴。並為受影響的個人提供一年的免費信用監控和身分保護服務。

此外，並向合作夥伴提供免費的客戶通知支援，以便合作夥伴在必要時通知其客戶。

TWCERT/CC 建議，「Orbitz」的使用者如曾在該平台登錄銀行或信用卡資料者，應詳細查看並管控近期信用卡或銀行交易紀錄，如有遭濫用情況之虞，務必儘速聯繫相關金融機構處理。



資料來源：

<https://www.hackread.com/hackers-steal-banking-personal-data-of-orbitz-users/>

3.2.5、駭客利用舊漏洞以及針對更新遲緩的使用群，將 Linux 伺服器成為挖礦苦工，受害者包括台灣

在 Tesla ASW 伺服器 and Jenkins 伺服器安裝執行 cryptocurrency 挖礦的網路駭客現在瞄準 Linux 系統的伺服器，到目前為止，已生成 7.4 萬多美元的 Monero 虛擬幣。

根據趨勢科技報告，新的駭侵活動使用合法的開源 XMRig cryptominer，並結合利用 Cacti 的 Network Weathermap 套件中的舊漏洞(CVE-2013-2618)。該漏洞是 Network Weathermap 版本

0.97b 之前 editor.php 的跨站腳本漏洞，允許遠程攻擊者透過 map_title 參數注入任意 web 腳本或 HTML。

這波駭侵活動較有針對性，主要影響日本、台灣、中國、美國和印度。趨勢科技表示，此次利用舊的安全漏洞的原因(從 2014 年 6 月起，Network Weathermap 目前只有兩個公開報告的漏洞)。可能是攻擊者不僅有可利用的安全缺陷漏洞，也可以針對那些更新遲緩的開源工具使用群。

趨勢科技將此駭侵活動追溯到與兩個 Monero 錢包相關的兩個用戶帳號，其中截至 3 月 21 日已存入 74,677 美元。然而，趨勢團隊注意到，這次活動背後的駭客在 Tesla 和 Jenkins 伺服器入侵事件時賺到了超過 300 萬美元，並都使用了 XMRig。

然而針對此活動，攻擊者需要透過具有特定設置的目標才能獲得成功。這包括運行 Linux(x86-64)的 Web 伺服器，並且伺服器必須可公開訪問。Cacti 套件必須在過時的 Network Weathermap(0.97a 及以前版本)的套件系統，Web 伺服器不能要求身分驗證，以及 Web 伺服器應以 root 權限運行。

趨勢研究人員推論除了上述前兩個問題較常見外，會使用公開共享網路資料(Cacti)以及以 root 身分運行 Web 伺服器的，應是伺服器運營商可能會對此進行設置，以便透過基本的瀏覽器書籤等方式來監控伺服器，但這也使任何駭客可以更輕鬆地搜尋到並獲取存取權限。

趨勢科技建議，由於將 Linux 伺服器轉變為挖掘作業，需要未修補較舊漏洞，因此防止此類攻擊的最佳方法是使用最新的修補程序更新系統。

TWCERT/CC 建議，使用任何平台及作業系統務必將作業環境及所有安裝的套件及應用程式等軟體保持最新版本與修補，防毒軟體並

應保持最新病毒碼，以免遭駭客利用。



資料來源：

<https://www.scmagazine.com/hackers-exploit-old-flaw-to-turn-linux-servers-into-cryptocurrency-miners/article/753144/>

<https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-distributed-via-php-weathermap-vulnerability-targets-linux-servers/>

3.2.6、資安專家發現駭客在 YouTube 影片描述暗藏惡意連結

俄羅斯資安公司 Dr. Web 資安研究人員發現有網路犯罪分子正透過 YouTube 網站傳播惡意軟體。

該惡意軟體命名為「Trojan.PWS.Stealer.23012」以及新版本「Trojan.PWS.Stealer.23198」，是由 Python 程式語言編寫，主要針對 Microsoft Windows 的設備，竊取電子郵件和社交媒體帳戶的登錄憑證。

駭客會在 YouTube 影片的評論和描述部分發布惡意連結，主要針對影片類型多為使用特殊應用的遊戲玩家和作弊示範或教學等影片，並會在影片敘述或留言的地方提供聲稱可以存取遊戲秘笈和其他有用的工具連結，並偽稱連結所下載的檔案是乾淨合法的，以引誘遊戲玩家點擊連結。

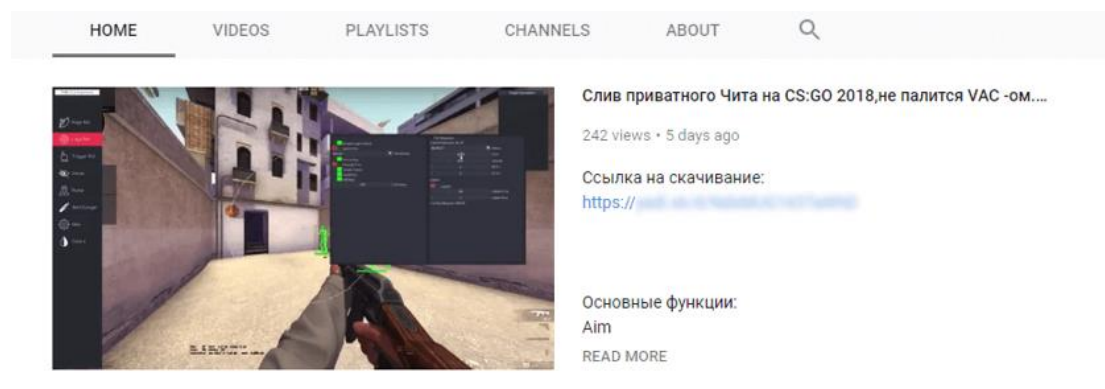
然實際上這些連結將用戶導向 Yandex Disk 伺服器上，該伺服器

是 Yandex 提供的俄羅斯雲服務，允許用戶將檔案儲存在雲端伺服器上並線上與他人共享。一旦受害者點擊連結，就會下載一個包含 Trojan.PWS.Stealer.23012 的自解壓 RAR 檔案。

安裝該檔案後，便會感染 Windows 電腦，並從網頁瀏覽器(包括 Chrome、Opera、Vivaldi 等)竊取 cookie。此外，惡意軟體也竊取保存在受害者網頁瀏覽器中的登錄憑證，並在其設備上截取用戶活動的螢幕截圖。並且從 Windows 桌面複製檔案，針對的檔案副檔名包括".txt"、".pdf"、".jpg"、".png"、".xls"、".doc"、".docx"、".sqlite"、".db"、".sqlite3"、".bak"、".sql"和".xml"。

收集完資料後，惡意軟體會將其儲存在受害者本機 C 槽的資料夾路徑"C : / PG148892HQ8"的 Spam.zip 檔案中，並將其發送到由駭客設置的命令和控制伺服器(C&C)。

TWCERT/CC 建議遊戲玩家和 YouTubers 避免點擊 Youtube 網站或任何其他網站評論(留言)區留下的未經驗證的連結，以免遭駭客利用。



資料來源：

<https://www.hackread.com/hackers-spread-password-stealer-malware-from-youtube/>

<https://news.drweb.com/show?i=11780&lng=en>

3.2.7、美國亞特蘭大市政府遭受大規模勒索病毒攻擊

美國亞特蘭大市政府在當地時間於 3 月 22 日被勒索病毒 SamSam 攻擊，要求支付比特幣來解鎖整個系統，尚不知道市政府是否支付贖款，但 5 天後終於可以開啟桌上電腦。

紐約時報報導，美國亞特蘭大市政府的八千名員工於 27 日接獲期待已久的指示：可以開電腦了。但是，全市的網站仍無法正常運作，民眾無法在上頭繳水電費、罰單等，全球最繁忙的亞特蘭大機場，仍然無法使用無線網路，包括法院無法發拘捕令、警員只能手寫報案單，求職申請也只能暫停，市政運作及居民生活大受影響。

依據報導，亞特蘭大市政府是在 22 日一早就被勒索軟體攻陷，市政府檔案被改為「我很抱歉」(I' m sorry)，並要求市政府支付價值 5.1 萬美金的比特幣解鎖，這是對美國主要城市所發動持續最久、破壞最大的網路攻擊之一。

亞特蘭大市長巴頓斯表示：「我們正在處理這個狀況。」專家分析，此攻擊使用屬於 SamSam 的勒索軟體。SamSam 可以輕易攻擊基於 JAVA 寫成的伺服器，用開源工具去蒐集憑證，並搜集已連接網路電腦的資訊，以及加密系統中的文件。

如果病毒在掌控系統之前沒有被攔截，用戶就會無法使用系統，需要駭客的鑰匙來解鎖。專家表示，通常付了贖金之後，也無多大作用，重啟使用的唯一方法是整個系統重灌。



資料來源：

<http://news.ltn.com.tw/news/world/breakingnews/2379898>

<https://www.udn.com/news/story/6813/3057850>

3.2.8、SWIFT 資金盜轉事件再添一筆，所幸馬來西亞順利遏止

馬來西亞國家銀行在 3 月 27 日檢測到並阻止了一個網路安全事件，該事件涉及試圖使用偽造的 SWIFT 資訊進行未經授權的資金轉移。而所有未經授權的交易都透過與 SWIFT、其他中央銀行和金融機構迅速緊密合作行動而順利遏止。

該銀行表示在這次事件中沒有遭受任何經濟損失，也沒有對其他支付和結算系統造成干擾，目前正在就這一事件與當地和國際執法機構合作進行全面調查。

該銀行表示迄今為止所有的風險控制措施有效地遏止了這一事件。並也已採取額外的保障措施來保護其利益攸關方。且將保持高度

警惕與警戒，因為未來的事件可能涉及更高程度的複雜度和設計。

馬來西亞國家銀行向公眾保證，馬來西亞的支付和結算系統仍然不受影響，並繼續正常運作。

全球 SWIFT 系統組織歷經俄羅斯銀行、台灣遠東國際銀行和尼泊爾 NIC 亞洲銀行事件後，所採取的保護措施和合作機制可謂有所成效。



資料來源：

http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=465

[1](#)

<https://www.businesstimes.com.sg/government-economy/bank-negara-fuels-attempted-cyber-attack>

3.2.9、印度電力公司的系統遭受勒索軟體感染

印度 Panchkula 的 Uttar Haryana Bijli Vitran Nigam(UHBVN·哈里亞納邦電力公司)的 AMR 系統(自動抄表系統)上週成為未知駭客的網路攻擊的受害者。

據新印度快報(TNIE)報導，駭客竊取了從 UHBVN 電腦系統的計

費紀錄，並要求從州政府以比特幣形式的 1000 萬印度盧比(大約 153,800 美元)來解密檔案和恢復 AMR 系統的存取。

UHBVN 是哈里亞納邦兩大電力公司之一，由塔塔諮詢服務有限公司(TCS)安裝、運營和管理。負責監測九個哈里亞納邦地區的電費。駭客攻擊事件發生在 3 月 21 日午夜 17 分。駭客在 UHBVN 總部電腦上傳贖金訊息。根據 TNIE 的說法，3 月 22 日，當電腦打開時，顯示駭客的需求的贖金訊息即顯示在螢幕上。

有關官員、IT 和網路安全專家集體進行了全面的系統研究，發現資料庫被加密，哈里亞納邦警方官員聲稱，該部門的網路專家正在調查事件並試圖追蹤 IP 地址以確定襲擊的起因。

但是，專家認為，考慮到 IP 地址可以在幾秒內被修改，因此攻擊者可能偽造了 IP 地址，這不是一件簡單的事情。據官員稱，由於已存在備份，消費者帳單也不受影響，因此沒有帳單紀錄丟失，但無論如何，由於缺乏數據而難以估算當前的消費量，事件可能對計費活動產生重大影響。

有報導稱，UHBVN 現在應無擁有消費者的電費單紀錄，只有拖欠的紀錄留在設備中，但 UHBVN 官員稱 4000 個產業消費紀錄皆沒有受到影響。Nigam 公司已經採取了很多措施逐步淘汰該系統，並將被最新、強大且技術先進的雲服務系統取代，該系統將於 2018 年 5 月底投入運行。



資料來源：

<https://www.hackread.com/hackers-demand-ransom-indian-power-billing-records/>

<https://securityaffairs.co/wordpress/70836/hacking/power-company-ransomware.html>

<http://www.newindianexpress.com/nation/2018/mar/29/billing-data-from-uhbvn-hacked-rs-one-crore-demanded-in-bitcoins-from-haryana-government-1793978.html>

3.3、軟硬體漏洞資訊

3.3.1、留心 DNS rebinding 讓µTorrent 用戶主機一覽無遺

以 C++ 語言編譯之 µTorrent(亦稱 uTorrent 或 microTorrent；縮寫 µT、uT)，已由 BitTorrent Inc 收購經營，適用 Windows 以及 Mac OS X，為小型輕量的 BitTorrent 客戶端免費軟體，低度消耗系統資源，受眾多 BT 用戶選擇，經分析其漏洞，因µTorrent Web 及µtorrent Classic 之 HTTP RPC server 分別使用 port 19575 及 10000，本機背景服務 XMLHttpRequest()可接收任何網站請求，此工作模式成為駭客藉以實施 DNS rebinding 的途徑，並結合暴力破解技術形成 RCE，能隨意調整受害主機 BT 存放路徑，並指定下載檔案來源，同時獲得重要系統資訊，即便最低權限客戶亦無法倖免，相同攻擊手

法亦見效於 Transmission BitTorrent 產品，但探勘門檻偏高，目前已公布各版升級軟體，亦可手動設定 HTTP RPC port，毋沿用預設值。



資料來源：

<https://engineering.bittorrent.com/2018/02/22/httprpc-security-vulnerabilities-resolved-in-utorrent-bittorrent-and-utorrent-web/>

<https://thehackernews.com/2018/02/torrent-download-software.html>

3.3.2、網路攝影機 Pelco Sarix 系列出現數多漏洞，易遭遠端接管系統及檔案控制權

網路攝影機 Pelco Sarix Professional 系列的產品，檢測出 IMPS110-1、IMP1110-1E、IMP219-1ER、IBP319-1ER、IMP519-1 相關型號具瑕疵，關鍵在韌體設計，import.cgi 遭受 XML 外部實體注入，導致變數內容被不當引用而暴露機敏資訊；無權限者可規避身分驗證開啟 ssh 服務、操縱控制台，或利用寫死憑證管理設備；ssldownload.cgi 未檢驗 SSL 憑證、檔名路徑，且 set_param 程式忽略 system.delete.sd_file 參數，造成系統檔案被任意下載、刪除；最嚴重者乃 set_param、export.cgi 輸入值驗證缺失，駭客將 shell 超字元結合特定參數一併提交，能以最高使用者身分執行系統命令；

另在網頁圖形介面輸入超長度字串恐觸發 Buffer Overflow，繼而遠程執行代碼，Schneider Electric 公司已公開升級版韌體，改善諸多危安因素。



資料來源：

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=9351939573&p_File_Name=SEVD-2018-058-01+Pelco+Sarix+Professional+v1.1.pdf&p_Reference=SEVD-2018-058-01

3.3.3、近距攻擊華為智慧機，駭客得惡意聲控及竊取個資

華為內部測試旗下智慧機安全性，發掘數個內建軟體漏洞，普遍運用之 HiCinema 影像程式，其專用介面未能正確核驗使用權，導致同網段攻擊者有機會遂行中間人攻擊，以竊取受害者資訊；而在 Mate 9 Pro 機種 LON-AL00B 系列型號，提供近距離無線通訊的 NFC 模組，在特定惡意操作後將洩漏隱私；LON-AL00B 系列上 soundtrigger 模組破綻則是迴避身分認證，只要被詐騙誤裝惡意程式，攻擊者能以聲響控制發簡訊、撥電話等非法操作，HUAWEI 已就相關版本軟體提供對應之安全更新。



資料來源：

<http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180307-01-phone-en>

<http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180307-01-smartphone-en>

3.3.4、Citrix 網管設備 NetScaler 系列 ADC 及 Gateway，恐有檔案訊息暨控制權流失之虞

經檢測 NetScaler 系列網管產品，得知軟體定義之應用程式傳遞控制器(ADC：Application Delivery Controller)及 Gateway 有 6 項共同軟體瑕疵，任何人均可 bypass 帳密認證，逕於 SSH login prompt 執行讀檔專用系統命令而不當獲得機敏資料；其他 web 介面亦因未嚴謹篩選輸入字串，易觸發 XSS 而危害連線者隱私個資；且駭客得藉低階 webapp 帳號建立 server-side request forgery，謀取 nsroot 帳號以獲高級管理權；其餘漏洞受駭客探勘，將可遍歷設備內路徑、自由下載檔案及擴權，Citrix 公司對弱點版本修補後釋出，僅供會員取得。



資料來源：

<https://support.citrix.com/article/CTX232199>

<https://support.citrix.com/article/CTX232161>

3.3.5、歷代 Exim 郵件代理器版本均有 Base64 解碼函數計算瑕疵，恐招致預授權 RCE 侵襲

1995 年發源於英國劍橋大學的 Exim(EXperimental Internet Mailer)以 C 語言撰寫，原屬網路郵件實驗用途，主要搭配類 UNIX 系統，後成為高普及率之免費 MTA(mail transfer agent 或 message transfer agent)。據國內 DEVCORE 研究人員分析指出，其 Base64 解碼函數 `b64decode()` 某列算式出現邏輯錯誤，Base64 以 6 bit 為單位，每 4 個 Base64 單位占用 24 bit 空間，等同 3 byte 長度，而 `b64decode()` 函數進行解碼計算時，對非 4 倍數長度值處理方式不符解碼後儲存實需，導致配置記憶體量不足 1 byte，此 off-by-one 的 buffer 溢位情境，可能被攻擊者利用特製 SMTP 資料觸發，而連鎖產生 pre-auth remote code execution，未受身分驗證即可促使 Exim 不當執行指令，該漏洞自初版存在迄今，儘管 Exim maintainers 不認同其嚴重性，然全球 56%郵件伺服器運行刻正運行 Exim，且 DEVCORE 已公開探勘技術，恐危及逾 40 萬郵件伺服器，修補版已置於 Exim FTP 站台供自由取得。



資料來源：

<https://devco.re/blog/2018/03/06/exim-off-by-one-RCE-exploiting-CVE-2018-6789-en/>

3.3.6、修補 NTP 雙漏洞，避免校時服務錯亂

歷時 24 年的 Network Time Protocol 主從式架構，全球電腦均賴以同步化系統時間，經研究其程式碼，察覺部分瑕疵能造成校時功能遭 DoS，受駭客特製 mode 6 封包影響，函數 `ctl_getitem()` 之變數 `sp2` 運算結果，將產生越界讀取 `buffer` 位址之後果；而針對 `interleaved` 模式設計偽造封包，附帶 1 個 0 值來源 `timestamp` 與 1 個非 0 收領 `timestamp`，可破壞一對 `peer` 既有關聯性，持續發送假封包就會永遠中斷時間服務，NTP Developers 已備妥升級版軟體。



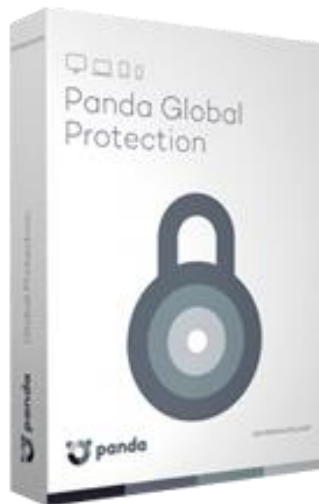
資料來源：

<http://support.ntp.org/bin/view/Main/NtpBug3453>

<http://support.ntp.org/bin/view/Main/NtpBug3412>

3.3.7、熊貓安全 Global Protection 發生 DACL 錯誤，將受本機任意用戶全權操縱

成立於西班牙熊貓安全公司(Panda Security SL)，曾率先提出 SaaS(Security as a Service)概念，旗下軟體 Global Protection 17.0.1 被巴西研究員 Filipe Xavier Oliveira 分析出弱點，由於命名管道(Named Pipes)之自訂式存取控制清單(DACL)安全機制異常，任何低階帳號用戶均可恣意更新 Discretionary Access Control List，後續挾其擴張權限創造(\\.\pipe\PSANMSrvCpPal)，利用該惡意 named pipe 模擬其他命名管道，可能衍生安全軟體 DoS，造成作業系統防護真空，據推測其他 Global Protection 其他版本亦有相同邏輯瑕疵，目前業者尚無抑制措施。



資料來源：

<http://seclists.org/fulldisclosure/2018/Mar/26>

3.3.8、攻擊 Samba 嚴重缺陷，能隨意竄改密碼並阻礙列印

考量同網段上相異作業系統(Windows、Linux、UNIX、IBM System 390)資源共享便利性，便催生 open-source 的 Samba，Samba 建基於 NetBIOS (Network Basic Input/Output System)通訊協定，可連接 Windows 的 SMB(Server Message Block)與 CIFS (Common Internet File System)，讓 PC 間破除 OS 的隔閡，分享資料夾及印表機，近期測試漏洞，發現 RPC spoolss service 設定為 external 時，若接收惡意 RPC calls，因缺乏過濾機制，恐觸發 null pointer 而中斷列印功能；最嚴重破綻在於網域控制站 LDAP server，因預設權限配置疏失，讓任何帳號用戶，均可恣意修改全體帳號(自身、管理者、系統 service)密碼，Samba Team 已公布各版修補檔。



資料來源：

<https://www.samba.org/samba/security/CVE-2018-1057.htm>

<https://www.samba.org/samba/security/CVE-2018-1050.html>

3.3.9、檢查 Adobe Dreamweaver CC 暨 Connect 狀態，阻止 command injection 及檔案消失

據 Adobe 安全公告指出，三款軟體發現漏洞，其網頁開發工具 Dreamweaver CC 在 Windows 環境，因 URI 處理器瑕疵之故，誤把惡意注入之作業系統命令交付執行；而 Connect 與 Dreamweaver 有類似的 URI 處理器瑕疵，然損失大相逕庭，將刪除非預期檔案或移除應用程式，Connect 尚有上傳流程邏輯錯誤，未對異常 SWF 格式檔案把關，引發 XSS；使用者眾的 Flash Player，出現 Use-After-Free 及 type confusion 兩種缺陷，雖然技術屬性相異，但俱可衍生嚴重 RCE，Adobe 就相關軟體提供對應之安全更新。



資料來源：

<https://helpx.adobe.com/security/products/dreamweaver/apsb18-07.htm>

！

<https://helpx.adobe.com/security/products/flash-player/apsb18-05.html>

3.3.10、VPN Unlimited 恐讓任何程式能以 root 控制 mac OS X

駐居中國大陸境內，想上外國網站查找資料、種子，多少依賴翻牆軟體，VPN Unlimited 算是熱門選擇之一，能搭配 Android、iOS、Linux、macOS、Windows 多種平台與 Chrome、Firefox 瀏覽器，建置全球各地 70 餘處 VPN server，且保護個人數據，免被「無授權地」蒐集統計，適用 macOS 之 VPN Unlimited 系列經 Benjamin Watson 研究，VPN Unlimited 內具備高級權限之 Helper Tool 元件，其建置 XPC 介面，竟允許任意應用程式比照 root 執行系統命令，完全違悖 XPC 服務原始保護精神，XPC 切割權限予個別 process 的沙箱機制，本意是簡化每個 process 權限到最低，減少外部威脅途徑，然此次暴露出嚴重權限管理缺失，導致 mac OS 系統控制權外放，目前 KeepSolid Inc 仍無解決方案。



資料來源：

<https://github.com/VerSprite/research/blob/master/advisories/VS-2018-014.md>

<https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingXPCCServices.html>

3.3.11、客製化韌體 Asuswrt-Merlin 記憶體崩壞，影響華碩 28 種硬體型號

華碩無線路由器除正版韌體外，另有一客製化選擇，Asuswrt-Merlin，由 Eric Sauvageau 開發維護，其宗旨是本著不動搖韌體基礎架構之原則，強化既有效能兼隨時改善缺陷，囿於其韌體 httpd daemon 所呼叫 deleteOfflineClient() 函數，原程式設計未顧及參數資料過長情境，存在記憶體崩壞瑕疵，若遭遇特製 http GET 請求封包，觸發 stack buffer overflow，惡性覆寫 stack，賡續操縱指標計數器、control flow，最後實施 Return-Oriented Programming，將導致 RCE，該弱點影響硬體型號多達 28 種，修補 code 已公開於 Asuswrt-Merlin 網站。



資料來源：

https://github.com/coincoin7/Wireless-Router-Vulnerability/blob/master/Asus_DeleteOfflineClientOverflow.txt

<https://asuswrt.lostrealm.ca/changelog>

3.3.12、更新 Mac OS 平台專屬 Google Updater 以改善本機擴權缺點

在 Mac OS X 10.4 版以後作業系統，能運行 Google Updater，即是 Google 產品安裝工具，能集中檢視已安裝及可供安裝之軟體現況，及執行安裝、更新、解除等管理層操作，近日 Updater 遭披露漏洞，因 Updater 服務要求 root 級權限，所產生 distributed objects 卻不具備安全使用條件，本機駭客利用 plist 序列化程式碼錯誤處理物件，將假造內容當作 CFString 來處理，繼之賦予函數 `_flattenPlist()` 惡性參數值，恐導致 stack 指標大幅偏差，落於有效堆疊空間之外，觸發 memory corruption 及後續損害，Google 基於安全顧慮，平素罕見其公開弱點細節，且該弱點被視為高危險程度，想來是修補版已釋出，加上 Updater 能自體更新，索性讓 Project Zero 成員 `ianbeer` 主動介紹探勘技術也無妨，但據悉尚有數十處潛藏類情，可能讓攻擊者有機可趁，原因在開發階段未導入安全設計規範，致使程式結構存在眾多不當跨越權限邊界的分散式物件。



資料來源：

<https://bugs.chromium.org/p/project-zero/issues/detail?id=1486>

<https://tools.google.com/mac/updaterfaq.html>

3.3.13、防 hash 碰撞效果低落，可暴力破解 Bouncy Castle 第 1 版 keystore 格式檔案

來自澳大利亞的軟體社群 Legion of the Bouncy Castle Inc，開發充氣城堡(Bouncy Castle)並持續維護，在此非指兒童遊樂設施，而是為 C 與 Java 應用程式所設計之加密運算函式庫，支援範圍包括 Android，儲存檔案格式稱 BKS(Bouncy-Castle KeyStore)，類似 Sun 或 Oracle 的 JKS keystore，檔案內裝載公鑰、私鑰、憑證，由於 Bouncy Castle 之金鑰雜湊訊息鑑別碼(HMAC)本應具 160 bit 長度之 hash 運算結果，受程式設計錯誤拖累，致使 HMAC 鍵僅有 16 bit，一旦遭受本機暴力破解攻擊，數秒內可猜測其 HMAC 值而瓦解資料完整性，儘管密鑰與密碼未破解，實際資料內容仍受保護，然不排除 BKS V1 檔案被詳盡分析，帶來後續攻擊之可能性，此缺陷已被注意 6 年之久，迄今始正式提出警告，尤其是 84% 的 Android 應用程式正使用 BKS V1 檔案，恐帶來不少衝擊，改良版軟體已公開供應。



資料來源：

<https://cryptosense.com/blog/bouncycastle-keystore-security/>

<https://insights.sei.cmu.edu/cert/2018/03/the-curious-case-of-the-bouncy-castle-bks-passwords.html>

<https://en.wikipedia.org/wiki/HMAC>

3.3.14、版主火速更新 Drupal，重度威脅須臾即至

以 PHP 開發之 Drupal，係自由開源的內容管理系統(CMS)，中文化後在國內有固定支持者推廣其應用技術，Drupal 平台將內容視同 node，藉由後端 module 調整顯示、排列、分類等方式，搭配權限控管可架構論壇網站，近日發現名喚 Drupalgeddon 2 之高危漏洞，堪稱慘劇，囿於其 core 級元件未嚴謹過濾輸入字串，致使惡意請求能伺機偷渡 payload，衍生 RCE 攻擊，然 core 牽涉多種子系統共同應用方式，故駭客無須準備帳號，直接匿名造訪網站，便可循不同網頁途徑入侵，恣意更動系統檔案、限閱資料，Drupal team 已針對主流版本進行升級並公告，部分舊版已逾維護範圍，因全球 Drupal 開發網站過百萬，建議網管者即刻因應，阻止誕生機率極高之入侵工具，鎖定修補遲緩的站台下手。



資料來源：

<https://groups.drupal.org/security/faq-2018-002>

<http://www.zdnet.com/article/update-drupal-asap-over-a-million-sites-can-be-easily-hacked-by-any-visitor/>

<https://zh.wikipedia.org/wiki/Drupal>

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
預招	白帽駭客入門班	【資安訓練課程】『預招』白帽駭客入門班 12hr 主辦單位：NTC 人才培訓中心 線上報名連結： https://bit.ly/2FYb7HM 課程簡介： 1. NTC.im 合作單位包含文大、中興、北科大、第一科大等，以下統稱 NTC.im。 2. 課程資訊如有變更以 NTC.im 官網公布資訊為主。 3. 異動、開課提醒等以簡訊/eMail/電話等方式進行通知說明。 4. NTC.im 保有修正、暫停、遞延或終止各課程之權力。 5. 部分課程收費方式以達到開班人數時開始通知繳費。

時間	研討會/課程 名稱	研討會相關資料
		6. 預先收費課程，如因故無法如期開課或遞延開課，學員可選擇遞延課程或由 NTC.im 進行全額退費。 課程諮詢： 02-2701 0928 黃小姐 (info@ntc.im) 或 Line 線上客服： https://line.me/R/ti/p/%40mwo5792l
預招	Python 滲透 測試者開發 入門班	【資安訓練課程】『預招』Python 滲透測試者開發入門班 24hr * 需有 Python 應用開發經驗 主辦單位：NTC 人才培訓中心 線上報名連結： https://bit.ly/2FYb7HM 課程簡介： 1. NTC.im 合作單位包含文大、中興、北科大、第一科大等，以下統稱 NTC.im。 2. 課程資訊如有變更以 NTC.im 官網公布資訊為主。 3. 異動、開課提醒等以簡訊/eMail/電話等方式進行通知說明。 4. NTC.im 保有修正、暫停、遞延或終止各課程之權力。 5. 部分課程收費方式以達到開班人數時開始通知繳費。 6. 預先收費課程，如因故無法如期開課或遞延開課，學員可選擇遞延課程或由 NTC.im 進行全額退費。 課程諮詢： 02-2701 0928 黃小姐 (info@ntc.im) 或 Line 線上客服： https://line.me/R/ti/p/%40mwo5792l
2018/04/ 25-27	2018 亞太資	【資安研討會】2018 亞太資訊安全論壇 日期：2018 年 04 月 25 日(三) - 04 月 27 日(五)

時間	研討會/課程名稱	研討會相關資料
	訊安全論壇	地點：台北南港展覽館 5 樓 (台北市南港區經貿二路 1 號) 主辦單位：資安人雜誌 參與對象：各行業(政府、金融、製造業、電商、醫療業、中小企業與零售業之資訊、資安、網管、IT、程式人員等。 活動網址： https://www.informationsecurity.com.tw/Seminar/2018_all/ 活動概要： 觀念上，資安不再躲在資訊身後，而是影響與帶動企業營運的推動力。 組織上，企業組織應設立專職單位，看顧與落實繁雜的資訊安全工作，不容一絲疏忽。 管理上，2018 年所被關注的除觀念認知外，也須將採用工具的評估具體呈現其效力。 技術上，2018 年資安人員加強網路威脅防禦的規劃、防範與事件處理的能力。 歡迎各行業資安領域的優秀人才們共同參與。
2018/04/27	舞弊稽核與數位鑑識系列_新興科技環境的數位鑑識挑戰與因應	【資安訓練課程】舞弊稽核與數位鑑識系列_新興科技環境的數位鑑識挑戰與因應 主辦單位：中華民國電腦稽核協會 課程時間：2018 年 04 月 27 日(五) 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： 資訊背景人員可藉由本課程依序瞭解，何謂數位鑑識與數位資料的關聯及在法律攻防上的意義，並針對目前新興的不同型科技環境，瞭解數位鑑識有哪些相應做法以及注意重點。 課程大綱： 1.數位證據與法律

時間	研討會/課程 名稱	研討會相關資料
		2.鑑識調查之基礎概念 3.BYOD 與行動環境之證據與鑑識準備 4.雲端環境之證據與鑑識準備 5.物聯網環境之證據與鑑識準備
2018/05/ 02-05/03	駭客任務.資 安戰役	【資安研討會】駭客任務.資安戰役 主辦單位：新竹科學工業園區、國家高速網路與計算中心 日期：2018 年 05 月 02 日(三) - 05 月 03 日(四) 地點：宜蘭傳藝老爺行旅(宜蘭縣五結鄉季新村五濱路二段 201 號) 線上報名連結： http://most.nchc.org.tw/index.html 活動概要： 2018 年 IRCON 移師宜蘭，邀請資安研究專家、CERT、CSIRT 資安事件應變單位共同分享，以提供相關資訊安全事件處理的經驗。2018 資訊安全研發平台計畫成果發表研討會，為科技部指導國家高速網路與計算中心（國網中心）執行之兩項計畫「科技部雲端攻防演練平台及惡意程式資料庫研製暨科學園區資訊分享與分析中心建置計畫」及「雲端攻防暨培訓平台建置計畫」共同舉辦之聯合成果發表研討會，將安排計畫相關議題及研發成果分享、資訊安全技術實作課程以及資安攻防競賽等精彩內容。
2018/05/ 05	程式撰寫常 見失誤－緩 衝區溢位攻 擊與預防	【資安訓練課程】程式撰寫常見失誤－緩衝區溢位攻擊與預防 主辦單位：亥客書院 課程時間：2018 年 05 月 05 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=311 課程簡介： 程式撰寫上的安全漏洞所造成的傷害，比起惡意程式可

時間	研討會/課程名稱	研討會相關資料
		能危害更烈，因此如何用安全的方法撰寫程式非常重要，卻也相當不容易。 常見的幾種失誤，以及最常發生的重要議題：「緩衝區溢位攻擊」。課程將先簡介常見的程式撰寫失誤，接著從 process 堆疊、function 的 activation record 等基礎開始，最後進入緩衝區溢位攻擊的成因、變形、預防方法、以及攻防演練實驗。 課程大綱： 緩衝區溢位攻防概論(上午) ● process layout 與 process 堆疊段使用方式 ● activation record 架構與功能 ● 緩衝區溢位攻擊 ● 字串參數的傳遞方式、function prologue、function epilogue ● return-into-libc 攻擊 緩衝區溢位攻防演練實驗(下午) ● 初級緩衝區溢位攻擊 ● 進階緩衝區溢位攻擊 ● 初級 return-into-libc 攻擊 ● 進階 return-into-libc 攻擊
2018/06/01	舞弊稽核與數位鑑識系列_事件應變第一線人員之數位證據保全實作	【資安訓練課程】舞弊稽核與數位鑑識系列_事件應變第一線人員之數位證據保全實作 主辦單位：中華民國電腦稽核協會 課程時間：2018 年 06 月 01 日(五) 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： 對於個人電腦或伺服器進行數位鑑識蒐證前之準備工作說明，及現場數位證據保全程序說明，現場蒐證工具說明及操作現場數位證據保全工具。

時間	研討會/課程 名稱	研討會相關資料
		課程大綱： 1.數位證據特性及保全要點 2.ISO/IEC 27037 介紹 3.數位證據保全建議程序 4.第一線工具適用時機及功能簡介 5.實務操作

第 4 章、2018 年 03 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 3 月收到通報計 2508 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。

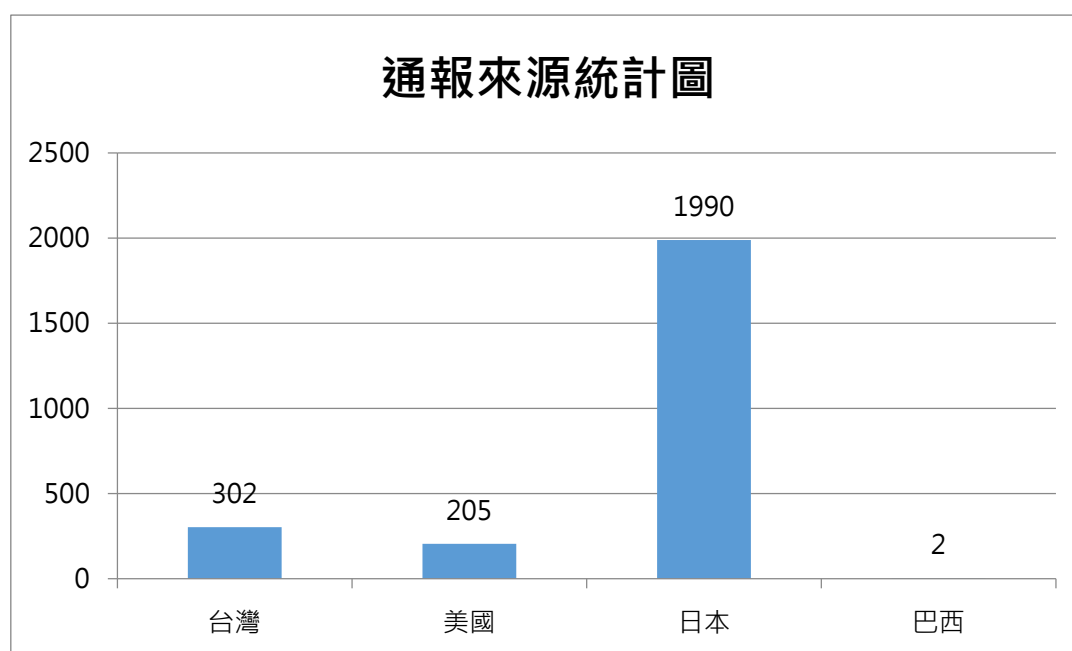


圖 1、通報來源統計圖

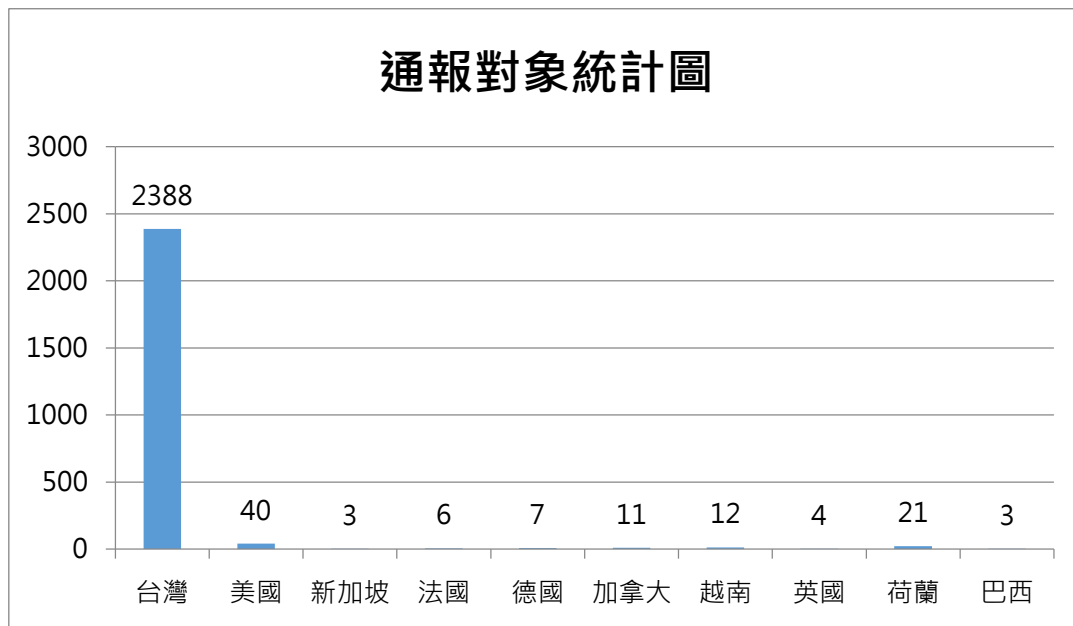


圖 2、通報對象統計圖

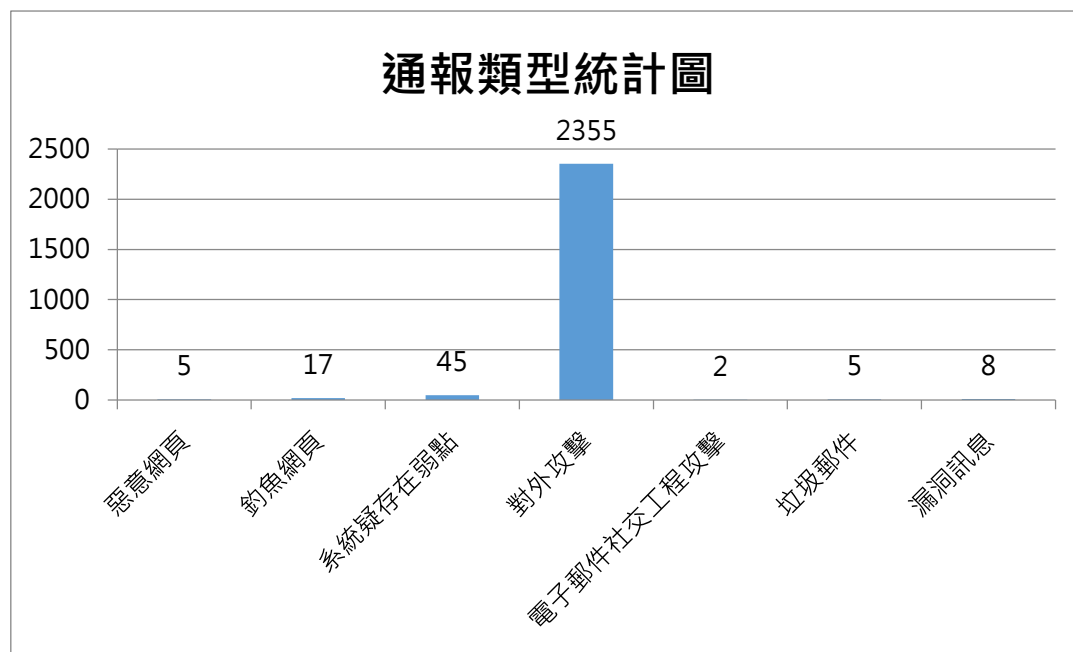


圖 3、通報類型統計圖

本月通報較大宗來自國外 CERT 提供之情資，攻擊手法為「嘗試利用台灣 IP 以不同的 Email 進行目標系統登入」，嘗試登入的次數從數十次到上百次之多，有部分帳號已成功登入，疑似該遭利用之 IP

已遭有心人士利用。

建議大家於平常要做好資訊設備的監控措施，若確認該資訊設備已遭入侵，建議重新安裝作業系統，並更新至最新修補程式，若作業系統無法重新安裝，需執行惡意程式檢測，亦建議更換系統使用者之相關密碼。若暫時無異常行為，建議持續觀察一個星期左右。安裝防毒軟體，更新至最新版，並注意病毒碼須持續更新。於事前勤更新相關弱點及漏洞，事發時立即處理，後續本中心仍持續提醒相關用戶對於所收到之事件通報進行相關處理，減少駭侵事件發生時所造成的損害。

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 4 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/>

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

資安電子報訂閱：<http://i-to.cc/S5HzJ>

線上電子報閱覽：<https://twcertcc.blogspot.tw/>

如有任何疑問或建議，歡迎您不吝指教。