TWCERT/CC 資安情資電子報

2018 年 11 月份

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team/Coordination Center

目錄

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、參與 2018 台灣賽門鐵克資安論壇

賽門鐵克於 11 月 2 日台北君悅飯店舉辦「2018 台灣賽門鐵克資安論壇」，此次研討會主要針對 2019 資安態勢、物聯網、金融及雲端防護做法，與資訊安全服務管理等面向進行研討，TWCERT/CC 主任陳永佳受邀擔任此次研討會中座談會的與談人，分享 TWCERT/CC 提供的服務內容，以及進行資安事件通報觀念宣導。此外，TWCERT/CC 亦於會場上擺設攤位，宣導 TWCERT/CC 業務及進行資安意識推廣。

2.2、參展 2018 資訊月

11 月 28 日至 12 月 3 日台北電腦公會將於台北世貿主辦 107 資訊月，資訊月活動成立於民國 69 年，是台灣最大型的消費性電子展，也是資訊教育的重要舞台，且免費入場，每年都吸引幾十萬人前往參觀。

TWCERT/CC 今年首度參與資訊月的活動，攤位將設在政府館的「成好習慣，資安威脅 Out!」，透過此次的活動，與參觀民眾互動，本次展示將以 TWCERT/CC 服務內容、遇到資安事件如何通報，及

宣導生活中常見的資安攻擊及防範作為，例如：企業客戶資料遭竊的連鎖效應、網路消費潛藏危機、E-Mail 信件潛藏危機、勒索軟體讓您的電腦變磚塊、免費的最貴，公用 WiFi 背後的真相、網頁挖礦程式的防範及家用路由器安全風險等，將以淺顯易懂的方式，教你如何進行自我防護。且當天只要於現場訂閱 TWCERT/CC 每月發布的免費資安情資電子報，即有機會免費玩一次夾娃娃機，夾自己喜歡的贈品。

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、大量銀行頁面遭仿冒，用於詐騙使用者個資

本中心近期接獲情資，發現有一惡意網域「http://www[.]fitnessrun[.]ru/inj/」，IP 為「31.184.252[.]3」，其冒充加拿大、匈牙利、印度、西班牙、法國、波蘭、肯亞、美國、英國、香港、烏克蘭、捷克、荷蘭、奧地利、紐西蘭、德國、澳洲及羅馬尼亞等地銀行登入頁面，意圖竊取使用者個資，截至目前尚未發現我國銀行被列入目標。該惡意網域目前已失效，IP 也已無法存取內容，但該網頁往後仍有可能被重啟，或利用其他惡意 IP/網域持續騙取使用者個資，民眾務必提高警覺。

TWCERT/CC 建議：

(1) 民眾使用網路銀行時，應由官方網站連入網站，並注意網站是否為釣魚網站。

(2) 若發現瀏覽之網站要求使用者輸入登入帳號密碼或個人機敏資訊，需確認該網站安全無虞後再行輸入相關資訊。

(3) 將惡意網域及 IP 等資訊加入防火牆阻擋清單，以避免使用者誤連。

Index of /inj

Name	Last modified	Size	Description
Parent Directory		-	
GoogleMail/	2018-06-15 20:46	-	
amazon/	2018-06-15 20:23	-	
at/	2018-06-15 20:53	-	
at_at.spardat.bcrmobile.php	2017-12-16 20:44	28K	
at_at.spardat.netbanking.php	2017-12-16 20:46	2.5K	
at_bawag.php	2017-10-10 01:28	57K	
at_com.bankaustria.android.olb.php	2017-12-16 20:48	12K	
at_easybank.php	2017-10-10 00:37	44K	
at_raiffeisen.php	2017-10-10 01:28	68K	
at_volksbank.php	2017-10-10 01:01	12K	
au/	2018-08-23 17:53	-	
au_SuncorpBank.php	2018-08-23 17:29	23K	
au_WestpacBank.php	2017-10-10 20:39	40K	
au_anzSingaporeDigitalBanking.php	2018-08-23 17:35	330K	
au_bankofqueenslandBOQ.php	2018-08-22 14:18	18K	

資料來源：

https://www.facebook.com/twcertcc/posts/2248284355401297?__xts__%5B0%5D=68.ARAqjucko6C56actSP50GCRJRt393-x2QIONuy4EIUXviuvZUqekQudw8uAO1tOo_SM2Bhz6NSsJw3Fw22i3oOAnyWgqEXot4h0r6817LHisDD1ZIyFX1oUmUN4Xo2Zz75j2f8eqF3cIfi0iBxWKei9M6TYGA_a7KLUT13Wa5gHzWEgKJL4umw&__tn__=-R-R

3.2、駭客攻擊事件及手法

3.2.1、SpankChain 遭駭，價值 38,000 美元加密貨幣被竊

SpankChain 是間專營成人行業的加密貨幣，以 Ethereum 區塊鏈來建立成人娛樂生態系統，是基於乙太坊 (Ethereum, ETH)的智慧合約 (Smart contract)應用平台，利用乙太坊和一個名為 BOOTY 的智慧 token 在現場 cam show 為成人模特兒提供小費。

SpankChain 的 token 用在 SpankChain 系統中提供支付和管理特權，近期由於智慧合約錯誤導致價值 38,000 美元的乙太坊被盜。根據 SpankChain 開發商的公告，攻擊發生在太平洋標準時間 10 月 6 日下午 6 點，由於支付頻道智慧合約中的一個 bug，一名身分不明的攻擊者偷走了 165.38ETH(約 38,000 美元)和 1,2701.88 BOOTY（價值 4,000 美元）。

SpankChain 表示，在被盜 ETH / BOOTY 中，34.99 ETH（約$ 8,000）和 1271.88 BOOTY 屬於用戶（約$ 9,300），其餘屬於 SpankChain。

該公司直到10月7日太平洋標準時間晚上7點才發現這次襲擊，便將 Spank.live cam 服務離線。SpankChain 預計以價值 9,300 美元的 ETH 替換用戶被盜的金額，並且計劃在修復錯誤升級到新的支付頻道智慧合約時保持他們的 cam 服務離線。

根據公告，駭客利用重入攻擊 (Reentrancy attack) 從 SpankChain 竊取加密貨幣。重入攻擊是指攻擊者能夠在上一個函數調用完成之前重複調用智慧合約中的函數。這允許攻擊者在合約意識到沒有餘額之前重複提取加密貨幣。

在聲明中表示，簡而言之攻擊者利用可重入 (reentrancy)的 bug，就像乙太鍊的 DAO 事件一樣，攻擊者建立一個偽裝成 ERC20 token

的惡意合約，其中利用多次調用 transfer()到支付頻道智慧合約中，每次耗盡一些 ETH。

不幸的是，當初 SpankChain 選擇不進行資安稽核，因為 3 萬至 5 萬美元的報價認為不值得。事後看來，他們現在覺得「這應該是值得的」。

資料來源：
https://www.bleepingcomputer.com/news/security/naughty-hacker-steals-38k-from-spankchain-cryptocurrency/
https://medium.com/spankchain/we-got-spanked-what-we-know-so-far-d5ed3a0f38fe

3.2.2、知名網路托管公司 Hetzner 南非分公司遭駭，客戶資料外洩

Hetzner 是著名的網路託管服務提供商，該公司的南非分支機構在過去一年中遭遇了第二次資料外洩事件。

根據受影響的用戶本週收到的電子郵件，10 月 5 日星期五該公司的技術團隊在資料庫中發現可疑活動，即透過資安團隊和網路資安專家進行全面稽核，以確保系統安全。

該公司表示，攻擊者設法存取了客戶詳細資訊，如姓名、電子郵件地址、電話號碼、地址、身分號碼、增值稅號碼和銀行帳號。Hetzner 表示，這通常是客戶為開發票所提供的資料類型，駭客無法存取信用

卡詳細資訊、密碼或用戶的網站和電子郵件內容。

據該公司稱，雖然沒有暴露高度敏感的細節，但 Hetzner 仍然敦促用戶留意網路釣魚詐騙。該公司有充分的理由認為，駭客可能會試圖利用他們竊取的資料，以發送訂製的網路釣魚電子郵件，這些電子郵件可能誘使用戶交出他們無法從其伺服器檢索的資料，例如帳戶登錄或信用卡資訊。

這一事件是 Hetzner 在過去 12 個月中在網上披露的第二次資料外洩行為。第一次駭客攻擊發生在 2017 年 11 月，攻擊者使用 SQL 注入漏洞來存取公司的「konsoleH」資料庫控制面板。與客戶細節的相關資料類型也在該事件中被盜，甚至有 FTP 密碼，該公司當時迅速重置，大約有 40,000 名客戶受到該事件的影響。

與其德國同名 Hetzner Online 的發言人表示不應與 Hetzner 南非有所混淆。Hetzner Online 與 Hetzner 南非是分開獨立的，發言人表示雖與合作夥伴保持聯繫，但不共享客戶資訊/資料庫。德國方面是完全獨立開發系統。儘管如此，德國分公司也沒有因此不被攻擊，在 2011 年及 2013 年皆曾遭遇安全漏洞。

Hetzner 南非近期在網上遭到嚴厲批評，因為這一最新的安全漏洞，特別是它的通知電子郵件，它試圖用前兩句話來淡化這一事件。用戶表示該公司在聲稱已經提高安全措施並進行安全稽核後仍遭到駭客攻擊。

資料來源：

https://www.zdnet.com/article/hackers-breach-web-hosting-provider-for-the-second-time-in-the-past-year/

https://zdnet2.cbsistatic.com/hub/i/2018/10/11/3f6d4d4c-24ed-4e76-b973-a6fd0b73ee69/6d119cfd77d6c9aea39527ad9cf4a772/hetzner-message-breach-2018.jpg

https://hetzner.co.za/news/konsoleh-database-compromise/

3.2.3、冰島國內遭受大規模釣魚攻擊，Remcos 遠端工具遭利用

近日一場大規模網路釣魚活動震撼冰島，攻擊者向成千上萬的人發送了惡意電子郵件，企圖欺騙受害者安裝強大的遠端存取工具，當地警方也表示這是襲擊該國的最大網路攻擊。

襲擊事件發生在 10 月 6 日星期六晚上，攻擊者透過電子郵件冒充冰島警察發送訊息，信中要求收件人協助偵詢，並警告他們因其違規行為而導致逮捕令發出，信中一個連結將受害者導引至假冒版本的 Lögreglan「冰島警察」，並讓內容看起來似乎提供更多有關事件的詳細資訊。

Cyren 的研究人員在調查期間與警方合作時解釋，為了使一切看起來都是真實的，該釣魚活動的作者使用同形異義技巧來註冊一個看起來像原始「logreglan.is」的網域名稱，攻擊者註冊網域名稱

「www.logregian.is」，使用小寫「i」(乍看可能像小寫「L」或「l」)。

Cyren 高級威脅分析師 Magni Sigurdsson 表示，此次網路釣魚計劃的複雜性，對於冰島而言是一個全新的威脅，攻擊者使用的工具是 Remcos，是一種功能強大的工具，可作為存取遠端電腦的合法解決方案，但被用於惡意目的。

Sigurdsson 表示，攻擊中使用的版本是 2.0.7 Pro，它提供對其運行的工作站的完全存取權限，當惡意使用 Remcos 時，攻擊者也依賴在啟動時運行的 VBSscript，以確保 Remcos 的執行。 網路釣魚郵件中的連結將受害者帶到一個模仿冰島警方官方網站幾乎完美的網站，並要求用戶輸入他們的社會安全號碼 (SSN)。

在冰島可以通過銀行提供的服務對名稱和 SSN 進行公開諮詢，因此個人必須登錄當地銀行的在線帳戶才能執行此程式。 如果用戶輸入了錯誤的 SSN，則合法服務會顯示提示進行更正的警報。網路釣魚網站無法驗證數字的真實性，因此他們通常會接受用戶輸入的任何資訊。

但是，在此釣魚活動的情況下，攻擊者能夠以某種方式檢查數字的有效性，從而增加欺騙性。另一種理論是他們可能使用的是過去洩露的資料庫。

攻擊者建立了一個複雜的網路釣魚活動，普通用戶很難檢測到。假冒的冰島警方網站要求受害者輸入他們在網路釣魚郵件中收到的身分驗證碼，以獲取有關針對他們的警方案件的更多詳細資訊。

在下一步中，受害者在受密碼保護的檔案中接收所謂的文件，並在網頁上提供密鑰，該密鑰實際上是用於竊取資訊並允許攻擊者遠端存取受害電腦的打包 RAT。

Cyren 指出，提取的.rar 文件是一個.scr 檔案(Windows 螢幕保護程式) 偽裝成一個長文字的文字檔，因此檔案副檔名是隱藏的。文件名是「Boðun skýrslutöku LRH 30 Október.scr」，大致翻譯為「10

月 30 日被警方打電話詢問」。

研究人員發現，攻擊者利用 Remcos 竊取銀行資訊，因為它檢查受害者是否可以存取冰島最大的銀行，而對 RAT 的分析表明，設置接收被盜資料的命令和控制 (C2)伺服器位於德國和荷蘭。

此時攻擊者仍然不為人知，但警方認為該活動是熟悉冰島行政系統的人的工作，從電子郵件和虛假網站上的文字可以支持此理論。

該活動的防禦反應非常迅速，登入頁面的網域名稱在檢測到攻擊後的第二天即被刪除，在襲擊期間發送了數以千計的惡意電子郵件，但警方目前沒有發布有關受害者人數的任何資訊。

資料來源：

https://www.bleepingcomputer.com/news/security/largest-cyber-attack-against-iceland-driven-by-complex-phishing-scheme/

https://www.cyren.com/blog/articles/iceland-police-phishing-attack-targets-bank-credentials

https://twitter.com/malwrhunterteam/status/1050704965747003398

https://twitter.com/James_inthe_box/status/1050707007966044162

3.2.4、VestaCP 遭駭，開源原始碼被植入惡意程式以發動 DDoS

VestaCP (Vesta Control Panel)是一種類似於更知名的 cPanel 的 Web 控制面板技術，提供使用者視覺化的網頁主機環境控制介面開源軟體，允許託管公司或 Web 開發人員快速推出 Web 伺服器，具體取決於他們需要運行的自定義 IT 基礎架構。

VestaCP 近日承認因安全漏洞，遭不知名的駭客透過惡意軟體感染專案的原始碼，該惡意軟體會記錄密碼以及開啟 Shell，並且可以發起 DDoS 攻擊。

VestaCP 團隊成員 10 月 17 日在一個論壇帖子中表示他們的伺服器遭駭，駭客更改了所有安裝腳本以記錄管理員密碼和伺服器 IP，在其官方 GitHub 資料庫上分析 VestaCP 原始碼的用戶說，惡意代碼是在今年 5 月 31 日添加的，後來在兩週後於 6 月 13 日被刪除。

該代碼可讓攻擊者收集已安裝 VestaCP 的伺服器的管理員密碼。為了避免受感染伺服器的流量看起來可疑，攻擊者將密碼發送回可能攻擊者可以控制的官方 VestaCP 網域，然後攻擊者使用這些密碼存取受感染的伺服器，並在今天發布的 ESET 報告中安裝了一個名為 Linux / ChachaDDoS 的新惡意軟體。

ESET 表示，惡意軟體似乎是來自不同惡意軟體的混合代碼，其中大部分來自 XOR，這是一種 Linux DDoS 惡意軟體應用程式，最初於 2015 年底被發現。

ESET 研究員 Marc-EtienneM.Léveillé表示，惡意軟體包含各種功能，但攻擊者似乎只使用了 DDoS 功能。

Léveillé說，他觀察到一些活動指示遭駭的 VestaCP 伺服器發起針對兩個中國大陸 IP 的攻擊。 事實上，在雲端供應商開始向客戶發送通知他們租用的伺服器使用大量頻寬之後，才使這 DDoS 功能暴露了受感染的伺服器。

自 9 月中旬以來，收到這些警告的用戶一直在 VestaCP 論壇和社交媒體上投訴。經過數週後 VestaCP 團隊回覆正與一家名為 Acturus Security 的俄羅斯網路安全公司合作，分析過去一個月的用戶投訴。

工作人員 8 月 18 日發布了 VestaCP 0.9.8-23，並稱是 VestaCP 軟體的安全版本，用於解決 Acturus 調查期間報告的各種安全問題。

由於 VestaCP 團隊還可以存取攻擊者發送回伺服器的伺服器 IP 和密碼資料，該公司建立一個網站，讓伺服器所有者輸入伺服器的 IP 地址，以查看該伺服器是否安裝了有密碼竊取代碼的 VestaCP 版本。

VestaCP 團隊表示如果查詢符合，應該儘快更改管理員密碼，另外應確保伺服器上沒有安裝/ usr / bin / dhcprenew 二進制檔案，這個二進製檔案是某種能夠啟動遠端 DDoS 攻擊或打開 Shell 到伺服器的木馬程式。

資料來源：

https://www.zdnet.com/article/open-source-web-hosting-software-compromised-with-ddos-malware/

https://www.welivesecurity.com/2018/10/18/new-linux-chachaddos-malware-distributed-servers-vestacp-installed/

https://forum.vestacp.com/viewtopic.php?f=10&t=17641&start=180#p73907

https://forum.vestacp.com/viewtopic.php?f=10&t=17641&start=170#p73890

https://forum.vestacp.com/viewtopic.php?f=10&t=17641&start=180#p73920

https://twitter.com/vestacp/status/1044456891504562176

http://vestacp.com/test/?ip=

3.2.5、美國健保入口網站 HealthCare.gov 再度遭駭，75,000 名用戶資料被竊

美國健保入口網站 HealthCare.gov 早期即遭詬病其安全機制漏洞百出，駭客很容易就可以取得並竄改資料，上百萬美國公民的個資，幾乎是攤在陽光底下。

即使曾從 Google 找來 Todd Park 擔任 CTO，仍在 2014 年發現遭駭客成功在該站的一個伺服器上植入惡意程式，如今美國政府在 10 月 19 日星期五表示，駭客入侵 HealthCare.gov 註冊系統並掌握了大約 75,000 人的個人資訊。

該系統被命名為聯邦促進交流 (Federally Facilitated Exchanges, FFE)，由醫療保險和補助服務中心 (Centers for Medicare & Medicaid Services, CMS)管理，醫療保險代理人和經紀人使用 FFE 透過官方 HealthCare.gov 入口網站將用戶註冊到所提供的歐巴馬健保改革計劃中。

被駭的電腦系統屬於保險公司的代理人和經紀人專用，以使他們可直接登錄參加保險的消費者，CMS 的其他所有登入系統都正常工作。

CMS 在新聞稿中表示，上週六（2018 年 10 月 13 日）的 FFE 中發現了「異常系統活動」，並立即展開調查。在過去的一周，即 10 月 16 日星期二，確認了入侵行為，CMS 已將與異常活動相關的代理商和經紀人帳戶停用，並將代理商和經紀人的直接註冊途徑禁用。

CMS 發言人門羅表示，普通民眾使用的 HealthCare.gov 網站沒有受到駭客攻擊的影響，受影響的只是代理人和經紀人使用的系統，他們的系統民眾是無法進入的。

政府機構表示，計劃在 10 月 28 日前重新啟用 FFE 直接註冊代理人和經紀人，美國公民仍可透過 HealthCare.gov 門戶網站或市場呼叫中心註冊歐巴馬健保改革計劃。

CMS 管理員 Seema Verma 表示已通知聯邦調查局，該機構計劃通知所有受影響的人，並正在努力儘快識別可能受影響的個人，以便可以通知他們並提供信用保護等資源，並表明 HealthCare.gov 和聯邦健保市場網站諮詢中心 (Marketplace Call Center)仍然可用，開放註冊不會受到負面影響。

資料來源：

https://www.zdnet.com/article/hackers-steal-data-of-75000-users-after-healthcare-gov-ffe-breach/

https://www.worldjournal.com/5935244/article-%E6%94%BF%E5%BA%9Ccms%E9%9B%BB%E8%85%A6%E8%A2%AB%E9%A7%AD-7-5%E8%90%AC%E5%81%A5%E4%BF%9D%E5%80%8B%E8%B3%87%E5%A4%96%E6%B4%A9/

https://www.linuxpilot.com/healthcare

https://www.gvm.com.tw/article.html?id=53470

https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal

3.2.6、國泰航空也傳出資料外洩，影響近千萬客戶

繼英國航空及加拿大航空資料外洩事件後，國泰航空也遭未知駭客成功侵入，高達 940 萬筆資料遭外洩。

國泰航空於 2018 年 10 月 24 日發布新聞表示，該公司在進行資訊安全檢測時，發現其資訊系統曾被未經授權的存取，該系統內含有約 940 萬筆乘客資料。

該公司表示，遭未經授權存取的資料包括乘客姓名、國籍、出生日期、電話號碼、電郵地址、地址、護照號碼、身分証號碼、飛行常客計劃的會員號碼、顧客服務備註及過往的飛行紀錄等資料。

此外，有 403 張已逾期的信用卡號碼以及 27 張無安全碼的信用卡號碼也都曾被不當存取。該公司補充表示，每位受影響的乘客被不當存取的資料有所不同。

國泰航空表示已即時採取行動進行調查及阻止事件發展，且並沒有證據顯示任何個人資料曾被不當動用。受影響的資訊系統與國泰航空的航班運作系統為兩個完全獨立的系統，不會對國泰航空的航班安全構成影響。

如任何顧客認為可能受此次事件影響，可透過以下途徑與國泰航空聯絡：

- 國泰航空為處理事件設立的專屬網站(infosecurity.cathaypacific.com)，顧客可於網站上獲得有關事件的資訊及保障個人資料的建議
- 國泰航空為處理事件設立的顧客專線(http://xn--infosecurity-9r3ti7o313b38vfwnjxf122dkp3a8pw606bwipc9e56q.cathaypacific.com/)
- 發送查詢電郵至 infosecurity@cathaypacific.com

資料來源：

https://news.cathaypacific.com/%E5%9C%8B%E6%B3%B0%E8%88%AA%E7%A9%BA%E5%85%AC%E4%BD%88%E6%B6%89%E5%8F%8A%E4%B9%98%E5%AE%A2%E8%B3%87%E6%96%99%E7%9A%84%E8%B3%87%E6%96%99%E5%AE%89%E5%85%A8%E4%BA%8B%E4%BB%B6

https://infosecurity.cathaypacific.com/en_HK.html

3.2.7、兒童個資價值高，加州女童子軍遭警告個人資料可能遭到外洩

2018 年 9 月，數以千計的加州女童子軍成員的個人資訊因未經授權的第三方存取官方其中一個電子郵件帳戶後，可能已經被盜。

報告顯示，在持續一天的事件中，橘郡多達 2800 名女童軍可能受到影響，這個匿名的第三方在今年 9 月 30 日至 10 月 1 日期間只存取該帳戶一天。

受影響的資訊可能包括姓名、電子郵件和家庭住址、駕駛執照詳細資訊、保險單編號和健康歷史資訊。

那些遭受資料外洩的人被告知，襲擊始於 9 月 30 日有未經授權的第三方獲得了官方童子軍橘郡旅遊電子郵件帳戶的存取權限，該帳戶曾用於「向他人發送電子郵件」(可能是網路釣魚電子郵件)。

該說明解釋說，該帳戶中儲存的一些電子郵件，其中包括日期可追溯至 2014 至 2018 年 10 月 1 日的電子郵件，其中包含有關會員的資訊，刻正通知所有資訊都在此電子郵件帳戶中的人。

重要的是，兒童的身分資料對駭客特別有吸引力，因為在提高警報之前它通常可以更容易地貨幣化，這是因為與未成年人身分相關的財務紀錄往往有限，因此更容易以他們的名義開設新的假帳戶。

根據 Javelin Strategy＆Research 今年早些時候的研究，2017 年，超過一百萬名美國兒童受到身分欺詐的影響，導致 26 億美元的損失和眾多家庭被迫支付共計達 5.4 億美元。

資料來源：

https://www.infosecurity-magazine.com/news/girl-scouts-alerted-to-possible/

https://abc30.com/4561129/

https://twitter.com/campuscodi/status/1056240359250976768

https://www.infosecurity-magazine.com/news/us-child-identity-fraud-victims/

https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study

3.2.8、知名音樂派對 Tomorrowland（明日世界）售票系統遭駭，上萬筆客戶資料外洩

Tomorrowland 是比利時熱門的電子舞蹈音樂節，於 2005 年首

次舉辦，後來成為世界上最大的音樂節之一，2018 年參加人數為 40 萬。

參加 2014 年 Tomorrowland 音樂節的約 64,000 名電子舞曲(EDM)粉絲的個人資訊被駭客竊取，他們設法破壞該節日用於線上銷售門票的 Paylogic 票務系統。

發言人 Debby Wilmsen 表示，受影響範圍僅限於 2014 年報名節日的觀眾部分，包含姓名、電子郵件地址、性別、年齡和郵政編碼，不包括付款細節，密碼和用戶地址。

雖然駭客無法竊取敏感資訊，如信用卡付款細節或社會安全號碼，但如果他們有足夠的資料，他們仍然可以嘗試利用其身分資料進行盜竊攻擊。

發言人 Wilmsen 補充，Paylogic 票務系統的管理員注意到舊系統上的異常活動，經過廣泛的分析，Tomorrowland 2014 年的舊資料文件出現在上面，所涉及的伺服器已立即離線。

在 2014 年參加 Tomorrowland 的 360,000 人中，大約有 64,000 人的個人資訊被盜，在被 Paylogic 告知他們的系統遭到入侵後，Tomorrowland 首先通知了隱私委員會，然後向所有受影響的節日觀眾發送電子郵件警報，告訴他們資料洩露和駭客設法竊取的資訊。

根據 Paylogic 的說法，資料洩露僅影響了 2014 年註冊門票的 Tomorrowland 與會者，其他所有 Paylogic 客戶顯然都沒有受到影響，這也暗示駭客已經滲透到 Tomorrowland 網站上的 Paylogic 註冊頁面的可能性，儘管在 Paylogic 的聲明中沒有提到具體細節。

Wilmsen 強調，客戶若收到有關門票銷售、促銷或其他地址的電子郵件時應務必保持警惕，這些電子郵件不是來自官方的 Paylogic 或 Tomorrowland 訊息，而來自 Tomorrowland 的所有訊息都皆僅由 tomorrowland.com 主導，Tomorrowland 門票銷售的連結只會透過 my.tomorrowland.com 或官方旅行合作夥伴找到。

資料來源：

https://news.softpedia.com/news/crooks-stole-data-of-64-000-tomorrowland-festival-goers-523493.shtml

http://www.standaard.be/cnt/dmf20181027_03884570

3.3、軟硬體漏洞資訊

3.3.1、預設 Telegram Messenger 語音 P2P 連線方式，外流用戶 IP 隱私

繼 LINE 之後頗受矚目的跨平台即時通訊軟體，當屬源自俄羅斯之 Telegram Messenger，其伺服器係專有軟體，然客戶端為開放原始碼 (可中文化)，據研究員 Dhiraj Mishra 測試，若 Telegram 電話採用點對點連線，則從 Console Log 可觀察對方明文 IP 資料，使用 iOS 及 Android 手機者，尚可按步驟 Settings -> Private and Security -> Voice Calls -> Peer-To-Peer，設定成 Never，如此則語音傳送途經 Telegram server，IP 可匿名，相對犧牲音質及傳速，然而桌機版 tdesktop 1.3.14 與 Windows 行動裝置版 Telegram 3.3.0.0 WP8.1，竟無 P2P 組態選項停用功能，等同強制使用者交出 IP，且獲得者未受任何身分限制，Telegram 向來標榜訊息安全加密技術，對此亦說不出所以然，多半是考慮傳輸效率才作此安排，Telegram Messenger LLP 公司已製作 1.3.17 beta 版及 1.4.0 穩定版改善前述缺陷，然 1.4.0 版多出硬碟配額管理、優化動畫影像快取 2 項優勢，建議直接升級 1.4.0 版。

資料來源：

https://www.inputzero.io/2018/09/bug-bounty-telegram-cve-2018-17780.html

https://gbhackers.com/telegram-desktop-ip-leaks/

3.3.2、小心個資外流，Siri 可規避 iPhone 螢幕安全鎖

一位 iPhone 狂熱者 Jose Rodriguez，多次挖掘 iOS 瑕疵，連 Apple 以安全性自豪的 iOS 12，亦再度中招，根據探勘實作影片，駭客陸續使出 37 步驟，能迴避 Screen Lock 安全鎖，無須鍵入密碼，直接運作 Siri 的 VoiceOver 視障輔助功能，分別對目標 iPhone 以電話及簡訊連絡，造成作業系統為兩者顯示通知訊息時，發生 UI 衝突，從而侵入手機，竊取照片、電話號碼、電子信箱、通訊錄等隱私內容；尚能以 Siri 新建 Note，於附加媒體影像時，伺機啟動共享，探勘過程雖瑣碎但無甚技術門檻，此項破綻橫掃全數 iPhone 機種，包括最新 iPhone XS，換言之，遺失裝置等同外流個資，目前為止官方無 iOS 12 更新公告，建議 iPhone 用戶最好使用 Face ID 的臉部辨識，若所持機型僅支援 Touch ID 指紋辨識，則停用鎖定狀態時 Siri 功能。

資料來源：

https://www.youtube.com/watch?v=YYucGhyOjUE&feature=youtu.be

https://www.theinquirer.net/inquirer/news/3063853/apples-siri-can-be-exploited-to-bypass-ios-12-passcode-security

3.3.3、網站開發應用框架 Django 權限控制失誤，完整密碼 Hash 曝光

鑑於多數網站有同質性設計需求，如註冊、後台、表單等，憑藉 Django 公開原始碼，開發者毋須重複製造相同模組，僅需專注開發專屬程式，Django 是由 Python 寫成之網頁應用框架，採用了 MVT（Model、View 及 Template）軟體設計模式，其核心框架包括網頁伺服器、內建分發系統、表單序列化及驗證系統，並支援中介軟體。今年 8 月釋出 Django 2.1 版，經 Phithon Gong 研究測試，得知新擴充之 Model 操作權限「View」，能令使用者查閱任意帳號之完整密碼雜湊值，而管理者即使具備「Change」權限，亦僅見局部遮蔽之 Hash 資料，此權限管控失當事件，對運作 MD5、SHA1 等演算法之站台不利，其密碼仍存破解之虞，Django 軟體基金會已公告修補檔及升級軟體。

資料來源：

https://www.djangoproject.com/weblog/2018/oct/01/security-release/

https://hub.packtpub.com/django-2-1-2-fixes-major-security-flaw-that-reveals-password-hash-to-view-only-admin-users/

3.3.4、慎防 SNMP 指令，能撈取 Samsung SCX-6545X 管理者帳密

三星公司印表機產品 Samsung SCX-6545X，經測試披露出高風險漏洞，儘管其網頁介面設計具備身分驗證階段，但遠端駭客無須嘗試破解，僅賴簡單網路管理協定 (SNMP)，透過相關指令與 OID 參數 (snmpget -v 1 -c public 100.100.100.100 iso.3.6.1.4.1.236.11.5.11.81.10.1.5.0)，逕對目標設備 IP 發送請求，即可獲得系統資訊，包含管理者帳密，攻擊該破綻之複雜度甚低，亦免身分權限，可輕易取得帳密並管理印表機，CVSS 3.0 評分 7.5，目前暫無官方安全更新，建議企業網管部門以防火牆攔阻可疑 SNMP 封包。

資料來源：

http://misteralfa-hack.blogspot.com/2018/10/samsung-printer-password leak.html

https://exchange.xforce.ibmcloud.com/vulnerabilities/150825

3.3.5、隨意接聽 WhatsApp 視訊電話，當心駭客上門

全球約 15 億用戶的 WhatsApp Messenger，每日 650 億條訊息量，為了在智慧型手機跨平台傳送簡訊、檔案、圖片、影音，使用

protobuf2 點對點加密協定，任職 Google Project Zero 的研究員 Natalie Silvanovich，公開 Proof-of-concept 探勘技術資料，證實 WhatsApp 在 iOS 和 Android 的 APP，具有記憶體堆疊溢位瑕疵，癥結在於 WhatsApp Messenger 透過即時傳輸協定 (Real-time Transport Protocol, RTP)傳送影音串流，駭客僅需掌握受害者電話門號，待受害者回應惡意視訊電話，即可觸發該嚴重弱點，輕則造成當機，重則接管受害者 WhatsApp 帳號，官方已於一周前陸續修補 WhatsApp (適用 iOS 與 Android)，至於 WhatsApp 網頁版則無相關風險。

資料來源：

https://isupdate.com/whatsapp-fixes-video-call-bug-that-could-have-let-hackers-in-says-report-cnet/

https://bugs.chromium.org/p/project-zero/issues/detail?id=1654

3.3.6、速更新 MikroTik 路由器 RouterOS，攔阻 By the Way 入侵技術&多項 DoS 風險

拉脫維亞網路設備商 MikroTik，供應全球有數十萬部 WIFI 及路由器設備，以 Linux v3.3.5 核心為基礎，開發獨立作業系統 RouterOS，

可安裝於該公司 RouterBoard 路由器或標準 x86 平台，具備 Firewall、VPN、QoS & Band Management、鏡射監管流量 (Port Mirroring) 等功能。據 Tenable Research 機構研究成果，RouterOS 內 Winbox 控制臺舊有 Directory Traversal 缺點，原為中級程度，但受到 By the Way 入侵技術威脅，升級成嚴重風險，攻擊者避開身分驗證，從資料庫竊取管理者帳密，藉 Telnet 或 SSH 連線，開啟設備後門，獲得系統 root shell 存取權，恐針對路由器部署惡意 Payload 或停用防火牆；另擁有合法帳號之駭客，呼叫 sprintf()函數可觸發 stack 溢位，賡續發動 RCE 而獲致完整系統權限；尚有 DoS 事件 3 項，對檔案上傳封包加以變造、遞迴式 JSON 解析佔據 Stack、快速驗證瞬間斷線等手法，均可讓設備失能。MikroTik 已升級軟體改善程式缺陷，然截至 10 月 3 日 Shodan 掃描分析，約略 35,000 至 40,000 部 Mikrotik 設備完成升級，仍有 7 成產品（20 餘萬）未修補，分布於巴西、印尼、中國大陸、俄羅斯、印度等地，隨時淪為駭客囊中物。

資料來源：

https://blog.mikrotik.com/security/new-exploit-for-mikrotik-router-winbox-vulnerability.html

https://cxsecurity.com/issue/WLB-2018100099

3.3.7、甫測出 ASUS 產品瑕疵，RT-AC58U 系統訊息曝光且多網頁涉及 XSS

代號 remix30303 的獨立研究者，前 2 日在 GitHub 公布華碩 RT-AC58U 雙頻無線路由器韌體破綻，首先是入口網頁 Main_Login.asp 所記錄 DHCP 租用狀態，駭客逕使用探勘工具即可獲悉所有連線電腦之IP、hostname、所在時區；且Main_Login.asp、Logout.asp 等十來個 asp 檔案，均有回應式 Cross Site Scripting，在 URL 輸入惡意字串即可觸發事件，目前官方更新從缺，欲維護設備功能及隱私，建議建立防火牆白名單。

資料來源：

https://github.com/remix30303/AsusXSS/

https://github.com/remix30303/AsusLeak

3.3.8、發現微處理器 FreeRTOS 嚴重缺陷，危及科技工業領域

心搏器能在正確時機調節患者心肌脈搏，禁不起任何誤差，然若裝置 OS 被外力介入干擾，可就人命關天，除醫療外，尚有航太、汽車工業、物聯網等 40 餘類產業刻正面臨共同風險。據 Zimperium 研究室 (zLabs)分析多種 IoT 技術，發覺問世 14 年的 FreeRTOS 竟存在 13 項嚴重漏洞，其通訊模組在運算 TCP/IP stack 時，涉及 RCE、DoS、資訊洩露等事件，FreeRTOS 是個開源的嵌入式 RTOS（Real-time operating systems)，可驅動微電腦，其精密、可靠、輕巧的特性，應用於追蹤、感應或其他自動化裝置，一旦駭客觸發相關弱點，勢將破壞依賴精密計算的工作流程，包括 Amazon、WITTENSTEIN、Texas Instruments、STMicroelectronics、NXP、Microchip、Espressif、Infineon 等廠均受該批漏洞影響，自 2017 年 11 月亞馬遜公司接手營運 FreeRTOS 專案，負責維護 Kernel 及元件，現已釋出升級後版本，而 zLabs 為保留安全更新時程，細部探勘技術俟 30 天後公諸於世。

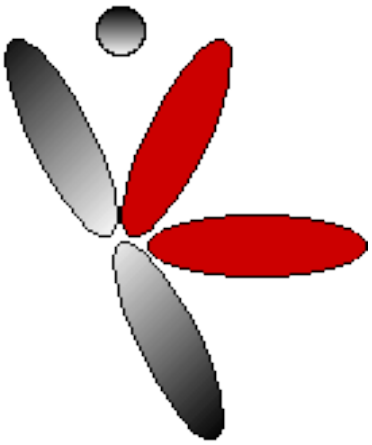
資料來源：

https://blog.zimperium.com/freertos-tcpip-stack-vulnerabilities-put-wide-range-devices-risk-compromise-smart-homes-critical-infrastructure-systems/

https://threatpost.com/aws-freertos-bugs-allow-compromise-of-iot-devices/138455/

3.3.9、嚴重緩衝區溢位問題恐癱瘓 LIVE555 串流媒體 RTSP Server

由 Live Networks, Inc 以 C++開發的 LIVE555 Streaming Media，係公開原始碼，跨平台支援多種影音格式，包含 MPEG、H.265、H.264、H.263+、VP8、DV、AAC、AMR、AC-3、Vorbis，經 Cisco Talo 分析原始碼，證實確有堆疊緩衝區溢位問題，其 CVSS V3 評分 10.0，乃罕見嚴重破綻，關鍵程式為 RTSP Server 元件內 lookForHeader()函數，其 HTTP 封包解析功能未顧慮異常條件，駭客特製封包，若包含鉅量「Accept」或「x-sessioncookie」字串，持續複製資料，可無窮盡增加指標指向位址，觸發緩衝區溢位問題，甚能衍生惡意執行代碼事件，對於安裝 RTSP Server 之主機形成威脅，因其技術廣泛運用於播放器和 IP Camera，且原始碼極易取得，攻擊門檻低，幾乎是掌握 IP 即能循 Port 80、8000、8080 入侵，目前已釋出改良版，線上影音業者及監控產品原廠，宜關注設備修補作業。另 VLC 澄清其軟體僅使用 LIVE555 RTSP client，無涉 RTSP Server，使用者可安心。



資料來源：

https://talosintelligence.com/vulnerability_reports/TALOS-2018-0684

https://thehackernews.com/2018/10/critical-flaw-found-in-streaming.html

3.3.10、Signal Desktop 疏於本機資料保護，愛好者當心隱私外流

非營利軟體開發機構 Open Whisper Systems，負責維護 Signal 即時通訊軟體，Signal 早先僅能支援行動電話 Android、iOS，在 PC 上須安裝 Chrome 瀏覽器始得與其他 Signal 用戶進行 P2P 通訊，為擺脫 Chrome 桎梏，2017 年 10 月 31 日推出獨立 Signal 桌機版，讓慣用 Firefox 或 Safari 者省去麻煩。近日各方披露 Signal Desktop 設計不當，如從 Chrome extension 轉換成桌機版，升級過程會將舊訊息內容以明文儲存為 messages.json，後續匯入桌機版資料庫，且未警告安裝者，若忘記刪除，則長期留置硬碟；而 Signal Desktop 之訊息資料庫 db.sqlite 儘管經過加密，然其 Decryption Key 以明文儲存於 config.json，找到 config.json 就能存取 db.sqlite；而過時訊息被刪除後，相關附檔仍留存，效果不盡理想。由於 Signal Desktop 橫跨 Linux 各分支、Windows、MacOS 等主流作業系統，用戶群廣泛，若電腦遭入侵極易外洩隱私，Signal 向來以通訊安全自豪，但其儲存安全有待改善，雖弱點版本不明，根據資料時間與 Github 版本歷程，研判最新版 v 1.17.0 亦受影響，Open Whisper Systems 得知此事迄今仍無回應，該公司與松鼠郵遞一樣依賴捐款，想來效率無法強求。

資料來源：

https://www.bleepingcomputer.com/news/security/signal-upgrade-process-leaves-unencrypted-messages-on-disk/

https://www.bleepingcomputer.com/news/security/signal-desktop-leaves-message-decryption-key-in-plain-sight/

3.3.11、近期數版 X.Org Server 出現 Command Line 參數核驗缺陷，易受入侵接管

X.Org 基金會負責維護的 X Window System (X11)，為開放原始碼之自由軟體，提供 Linux 使用者圖形介面，以 Server/Client 架構跨多平台運作，自 X Server1.19.0 版以後，存在 Command Line 介面參數過濾缺失，攻擊者即使帳號權限低，實體接觸可入侵提權，藉由探勘–modulepath 與-logfile 二參數 (僅限 root)，可觸發任意代碼執行，甚至恣意覆寫檔案內容，插入式驗證模組 (Pluggable authentication module, PAM)控制台的設計理念，是禁止沒操作 PAM console 者隨便啟動軟體，即使透過遠端 SSH 也不行，但普通帳號透過 PAM console，竟然避開權限檢查，而獲得 root 權力，官網於 10 月 24 日公告修補方式。

資料來源：

https://lists.x.org/archives/xorg-announce/2018-October/002927.html

https://gitlab.freedesktop.org/xorg/xserver/commit/032b1d79b7

3.3.12、研華改善 WebAccess HMI/SCADA 遠端監控軟體數項弱點

國內研華科技 (Advantech)生產工業自動化、IoT 商品，旗下

Advantech WebAccess 軟體為跨平台、瀏覽器之人機介面，屬資料採集與監控系統 (Supervisory Control and Data Acquisition, SCADA)，適用於自動化設備動態圖形顯示和即時資料掌控，經趨勢 Zero Day Initiative 分析出 6 種漏洞，如 STACK-BASED BUFFER OVERFLOW 及 PATH TRAVERSAL，一旦觸發則攻擊者能執行任意程式碼；操縱特製.dll 元件能刪除重要內部檔案；囿於軟體安裝期間用戶被剝奪控制權且事後不回復，加諸部分檔案權限配置不善，駭客得伺機採取管理者行為。針對上述重要安全事件，研華公司已升級軟體版本並公告。

資料來源：

https://ics-cert.us-cert.gov/advisories/ICSA-18-296-01

https://ics-cert.us-cert.gov/advisories/ICSA-18-298-02

3.3.13、兩款 AudioCodes IP Phone 受中間人攻擊，將洩露 Skype for Business 帳號隱私

以色列 AudioCodes 公司研製 IP 話機、閘道器、會談邊界控制器等通訊產品，其 440HD、450HD 二型 IP Phone 皆屬 Skype for Business 搭配之高端機種，具易操作、多功能特色，經 SySS GmbH 分析出中級程度漏洞，話機循 https 協定傳送帳密資訊給 skypewebpool 站台時，不受 X.509 憑證保護，故攻擊者建立 man-in-the-middle 攻擊條件，即可操作 Burp Suite 工具，重新安排路由後截收相關請求，獲得受害者隱私，甚至假冒其 Skype 身分，且發動入侵期間，IP Phone 毫無異常告警，SySS GmbH 所測試韌體版本為 3.1.1.43.1、3.1.2.89，經查官網目前最新韌體 image 檔亦然，故暫無安全更新，AudioCodes 設備遍及全球百餘國，購置網路電話之企業客戶宜關注修補進度。

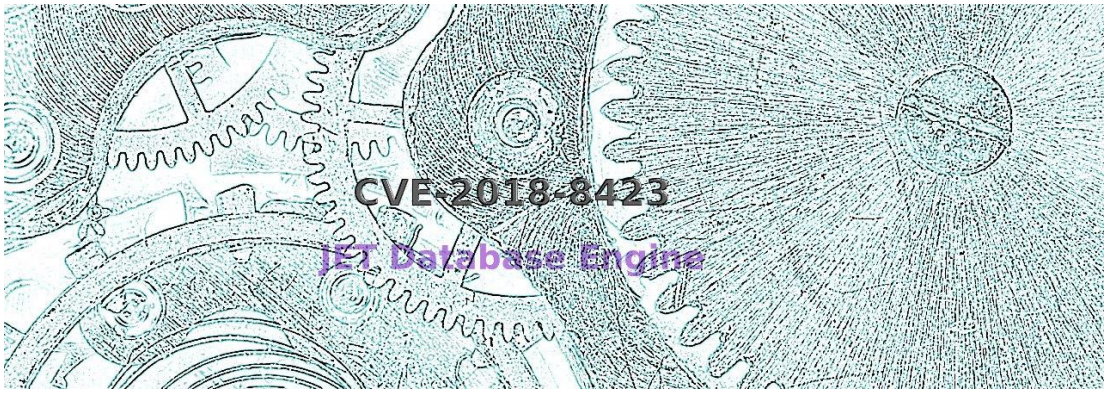
資料來源：

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2018-026.txt

https://zh.wikipedia.org/wiki/X.509

3.3.14、更新未臻完善，Windows Jet 資料庫引擎 0-Day 威懾依舊

光輝十月對 Microsoft 用戶而言似乎不盡美好，10 月 2 日所公布的 Windows 系統更新造成部分個人檔案被刪除，已令人餘悸猶存，繼此風波後仍有安全更新成效疑慮，因 TrendMicro Zero Day Initiative 前於 9 月 20 日公開 Jet Database Engine 之 0-Day 弱點，證實 32 位元的 c:\windows\SysWOW64\wscript.exe 執行檔可被惡意檔案 poc.js 觸發記憶體越界寫入，並導致 RCE，惟攻擊者須經釣魚等社交工程，將惡意檔案循 email、隨身碟交給受害者點擊，鑑於原始設計瑕疵在 msrd3x40.dll 動態連結函式庫，9 月 21 日 Acros Security 提出 in-memory 為基礎的微修補 (Micropatch)方案，然而 10 月官方安全更新同步替換成新版 msrd3x40.dll，因加密 hash 值變更導致 micropatch 失效，偏偏官方更新不完整，漏洞未澈底根除，Acros Security 總裁 Mitja Kolsek 表示微軟重啟該項漏洞，但亦再度發布本月 micropatch 以因應上述事態，並在官方有效解決問題之前，保留弱點技術細節不予公開。



資料來源：

https://blog.0patch.com/2018/10/patching-re-patching-and-meta-patching.html

https://www.bleepingcomputer.com/news/security/microsoft-fix-for-windows-jet-database-bug-not-perfect-micropatch-available/

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
107/10/24-12/23	全民資安素養自我評量網路活動開跑！	活動網站：https://isafeevent.moe.edu.tw/ 活動方式： □依據參加者所選取的身分別，由電腦自動選出 10 個題目，只要答對 7 題（含）以上，留下正確的抽獎資訊，即可參加抽獎。 □每位參加者最多可累積 300 次抽獎機會。 □抽獎獎項： 頭獎 1 名：15 吋筆記型電腦 貳獎 1 名：掃地機器人 參獎 1 名：靜音碎紙機 肆獎 20 名：藍牙耳機 參加獎 105 名：實用禮券 300 元 □抽獎方式： □ 本活動預計於中華民國 107 年 12 月 31 日前以電腦方式進行抽獎，屆時將安排律師進行見證，以確保本活動的公平性。 □ 每位參加者只有 1 次中獎機會，若抽中 2 個以上獎項，以市價高者為準。 詳細活動辦法：https://isafeevent.moe.edu.tw/rule 活動概要： 教育部為提升民眾的資訊安全素養與在網路世界的自我防護能力，自即日起至 107 年 12 月 23 日，舉辦「全民資安素養自我評量網路活動」(https://isafeevent.moe.edu.tw/)，歡迎大家至活動網站自我挑戰，不僅可以快速瞭解自己的資安素養認知程度，還有機會抽中筆記型電腦及掃地機器人等豐富獎品。
2018/11/23	網站安全與稽核簡介(II)（可抵內	【資安訓練課程】網站安全與稽核簡介 (II)（可抵內稽） 日期：2018 年 11 月 23 日 9:30~16:30

時間	研討會/課程名稱	研討會相關資料
	稽）	上課地點：電腦稽核協會訓練教室（位置圖：http://www.caa.org.tw/map.asp） 110 台北市信義區基隆路 1 段 143 號 2 樓之 2（捷運市政府站 1 號出口） 主辦單位：電腦稽核協會（CAA） 課程資訊及報名： http://www.caa.org.tw/education.asp?type=55+ISACA%E5%B0%88%E6%A5%AD%E7%B3%BB%E5%88%97#ISP102-b2018 課程大綱： 1.個資法施行衝擊與網站安全因應之道 2.網頁圖像保護 3.原碼檢測、網站弱點掃瞄與滲透測試簡介 4.網站 DDoS 攻擊防護 5.網站及後端主機所需防火牆及 IDS/IPS 簡介 6.以上主題之檢測與稽核 筆試測驗 16:30 ~ 課程簡介： 新版個資法施行後加重罰則與駭客攻擊手法翻新，對於組織之網站安全維護帶來衝擊，ISO 27001:2013 版新增加有關加密之領域，本課程從個資法、電子簽章法解析、ISO 27001:2013 改版等之標準與法規遵循、DigiNotar CA 與 Comodo CA 遭受攻擊等資安事件、技術與管理等多面向，討論如何稽核網站安全，並能針對企業如何慎選 CA 與善用 SSL 憑證、程式碼簽章、網頁圖像保護技術、網站弱點掃瞄及滲透測試，來因應網站安全議題。
2018/11/24-12/8	認證資訊系統安全專家 CISSP 輔導班	【資安訓練課程】認證資訊系統安全專家 CISSP 輔導班 日期：2018 年 11 月 24 日至 12 月 8 日 活動地點：台北市復興南路一段 390 號 2 樓

時間	研討會/課程名稱	研討會相關資料
		主辦單位：財團法人資訊工業策進會 數位教育研究所數位人才培育中心 課程資訊及報名： http://taipei.iiiedu.org.tw/course/security/247-asq901.html 課程費用：35 小時 / 56000 元，優惠價 32000 元 承辦人：羅小姐 電話： (02)66316586 E-Mail：showyann@iii.org.tw 課程簡介： 1.培養學員具通過 CISSP 考試之實力。 2.培養學員具評估及建置企業整體資訊安全管理之知識與能力。 3.培養學員具備基本通訊、網路安全技術（Firewall, VPN, NAT...等）及系統存取控制等相關概念。 4.培養學員具資訊安全之整體架構、原理、標準與應用，並具相關之資訊法律、電腦犯罪調查等之知識。
107/11/30	2018 FIDO Taipei Seminar - No More Passwords	【資安研討會】2018 FIDO Taipei Seminar - No More Passwords 日期： 107 年 11 月 30 日 08：30-17：00 地點：大直維多麗亞酒店 1F 大宴會廳（台北市中山區敬業四路 168 號） 指導單位：行政院科技會報、國家發展委員會 主辦單位：神盾股份有限公司、身分識別標準組織(FIDO Alliance) 會議網站：https://www.digitimes.com.tw/seminar/Egis_20181130/ 活動概要： 身分識別機制是現今所有接取應用服務的第一道關卡，亦是資訊社會與數位經濟發展所不可或缺的基礎。近年來，隨著網路服務與智慧型手機的普及，新的規格

時間	研討會/課程名稱	研討會相關資料
		或標準利用行動載具、安全模組，以及生物特徵感測技術，能達到兼顧方便性、安全性，以及隱私性的特點，也讓行動身分識別機制與相關應用更快速普及到日常生活中。 身分識別標準組織 FIDO Alliance 於今 (2018)年的亞洲行程中，首度新增台北站，於大直維多麗亞酒店舉辦 2018 FIDO Taipei Seminar，共同研討 No More Passwords、擁抱全球的新境界。
107/12/01	基礎網頁安全與滲透測試	【資安訓練課程】基礎網頁安全與滲透測試 課程時間：2018 年 12 月 1 日（六）09：30-16：30（12：30-13：30 休息） 共 6 小時 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） 主辦單位：亥客書院 線上報名連結： https://hackercollege.nctu.edu.tw/?p=302 報名費：每人$7000 含教材。若報名人數不足，將不予開辦。多人報名或一人同時報名多門課程均有優惠，詳情請洽 蔡小姐 (03)5731762 E-mail: wltt@nctu.edu.tw 課程簡介： 滲透測試是一種檢驗系統安全強度的技術，透過各種專家知識和最佳法則 (best practices)所研擬的流程方法，由一組安全技術團隊，以探察、分析、驗證到記錄的流程，模擬駭客的行為找出系統上邏輯性錯誤或更深層次的漏洞。 目前企業對外聯通管道主要以網頁與電子郵件為主，因此本課程將先說明基本滲透測試的知識與技能，了解目前國內外常見的網頁弱點，並實際操作具有弱點的虛擬網站，探討實務上的測試方式，了解潛在的安全威脅與問題。

時間	研討會/課程名稱	研討會相關資料
		課程大綱： 基礎網頁安全（上午） 1.Web 應用程式安全趨勢 2.網頁安全常見威脅 3.OWASP Top 10 4.CWE/SANS Top 25 5.CVSS 與常見網頁攻擊手法 基礎網頁滲透測試（下午） 1.滲透測試簡介 2.常用之滲透測試方法論 3.網頁滲透測試框架 4.網頁滲透測試流程與細節 5.網站應用程式弱點實作 ★ 本學院課程提供務實的技術演練，課程中將進行虛擬軟體模擬演練，教導學員安裝軟體及實務案例操演，使學員於課後能夠持續使用與練習。 ★ 本課程提供一人一機筆記型電腦上課使用。如欲自備自備筆記型電腦，電腦軟硬體需求: i3 以上 CPU、4G 以上記憶體、40G 可用硬碟空間、安裝 64-bits 作業系統、VirtualBox 5.1.10 以上版本。
107/12/06	2018 InfoSec Standards 國際資安標準管理年會	【資安研討會】2018 InfoSec Standards 國際資安標準管理年會 時間：2018 年 12 月 6 日（四）13：00-17：00 地點：財團法人張榮發基金會國際會議中心 1101 會議室 (台北市中正區中山南路 11 號） 會議網站： https://www.accupass.com/event/1810231129091532941078 活動概要： BSI 英國標準協會為國際標準制定機構，成立於 1901 年，為全球第一個國家標準機構，也是國際標準組織 (ISO) 的創始會員。

時間	研討會/課程名稱	研討會相關資料
		BSI 英國標準協會年度盛會，根據全球管理趨勢、企業需求與時事趨勢訂定「資訊安全」與「網路安全」相關研討議題，並邀請產官學研界的菁英專家進行分享，協助國內企業組織互相交流、接軌國際。 自 2003 年開辦以來，每年皆吸引近 300 位貴賓與會，並藉由表揚典禮後的專家演講獲取國內外的重要趨勢、國際標準動態、最佳實務做法與時事新訊，會後皆表示受益良多且給予年會極佳的正面評價。 更多【資安活動】請參考 https://www.twcert.org.tw/subpages/securityInfo/securityactivity.aspx
107/12/06	亞洲資安新趨勢研討會	【資安研討會】亞洲資安新趨勢研討會 時間：2018 年 12 月 6 日（四）13：00-17：00 地點：台北寒舍艾麗酒店 5 樓蘭廳（台北市信義區松高路 18 號，捷運市府站 3 號出口） 會議網站： https://www.accupass.com/event/1811020247021600151855 活動概要： 大數據時代，無論是 On-line 或 Off-line 的檔案資料，都需要與時俱進的保護與管理。 2018 年歐盟實施 GDPR，2019 年台灣資安法強化，當前各大企業不可不知的相關規定，讓資料儲存與管理專家告訴你，並分享亞洲最新網路安全與資料保護法規發展。
107/12/13-14	HITCON Pacific 2018	【資安研討會】HITCON Pacific 2018 時間：2018 年 12 月 13 日至 14 日 地點：台北文創大樓 6F（台北市信義區菸廠路 88 號） 主辦單位：HITCON、iThome 報名網址：

時間	研討會/課程名稱	研討會相關資料
		https://hitcon.kktix.cc/events/hitcon-pacific-2018 活動簡介： 本次 HITCON Pacific 主題為「Transforming: Cybersecurity and Resilience」，會議將聚焦在各式強韌性資安技術、安防措施等可加強企業關鍵系統的議題上，以因應日新月異的攻擊手法，以期能協助企業與政府單位，有效地縮短資安事件致使的服務停擺時間，進而降低資安事件對其所造成之影響。
107/12/15	進階網頁滲透測試	【資安訓練課程】進階網頁滲透測試 課程時間：2018 年 12 月 15 日（六）09：30-16：30（12：30-13：30 休息）共 6 小時 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） 主辦單位：亥客書院 線上報名連結： https://hackercollege.nctu.edu.tw/?p=323 報名費用：每人$8000 含教材。若報名人數不足，將不予開辦。多人報名或一人同時報名多門課程均有優惠，詳情請洽蔡小姐 (03)5731762 E-mail: wltt@nctu.edu.tw 課程簡介： 滲透測試是由資通安全專家模擬駭客的攻擊行為，以找出企業資訊網路或系統中的漏洞，並提供修補建議以完善整體網路安全。 本課程將延續基礎滲透測試的知識與技能，提供近年來重大漏洞的實務滲透經驗分享、錯誤的程式修補、以及防禦繞過與漏洞利用的技巧，透過實務工具操作與練習，讓學員身歷其境了解網頁安全漏洞之理論與實務。 課程大綱： 進階網頁滲透技術（上午） 1.網頁安全常見威脅簡介

時間	研討會/課程名稱	研討會相關資料
		2.滲透測試流程簡介 3.滲透測試各階段方法說明 4.實務滲透案例與漏洞回報經驗談 5.滲透測試自修資源分享 進階網頁滲透實驗（下午） 1.滲透測試工具操作 2.實務漏洞利用練習 3.滲透測試測資產生 ★ 本學院課程提供務實的技術演練，課程中將進行虛擬軟體模擬演練，教導學員安裝軟體及實務案例操演，使學員於課後能夠持續使用與練習。 ★ 本課程提供一人一機筆記型電腦上課使用。如欲自備自備筆記型電腦，電腦軟硬體需求: i3 以上 CPU、4G 以上記憶體、40G 可用硬碟空間、安裝 64-bits 作業系統、VirtualBox 5.1.10 以上版本。

第 4 章、2018 年 10 份事件通報統計

本中心每日透過官方網站、電郵、電話等方式接收資安事件通報，2018 年 10 月通報總計 1857 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。

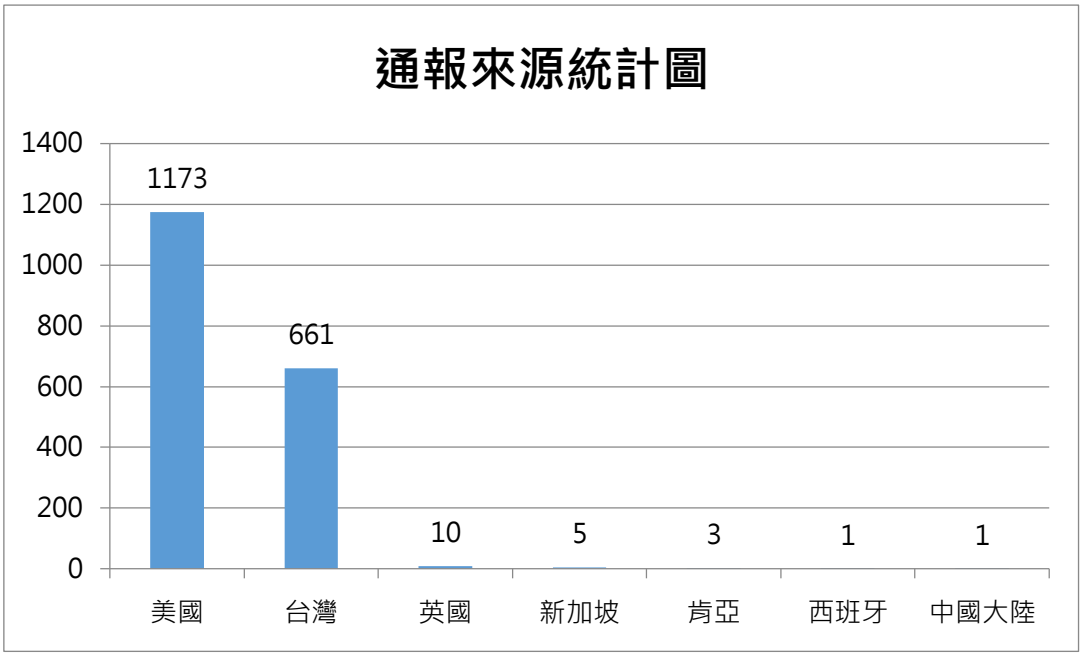


圖 1、通報來源統計圖

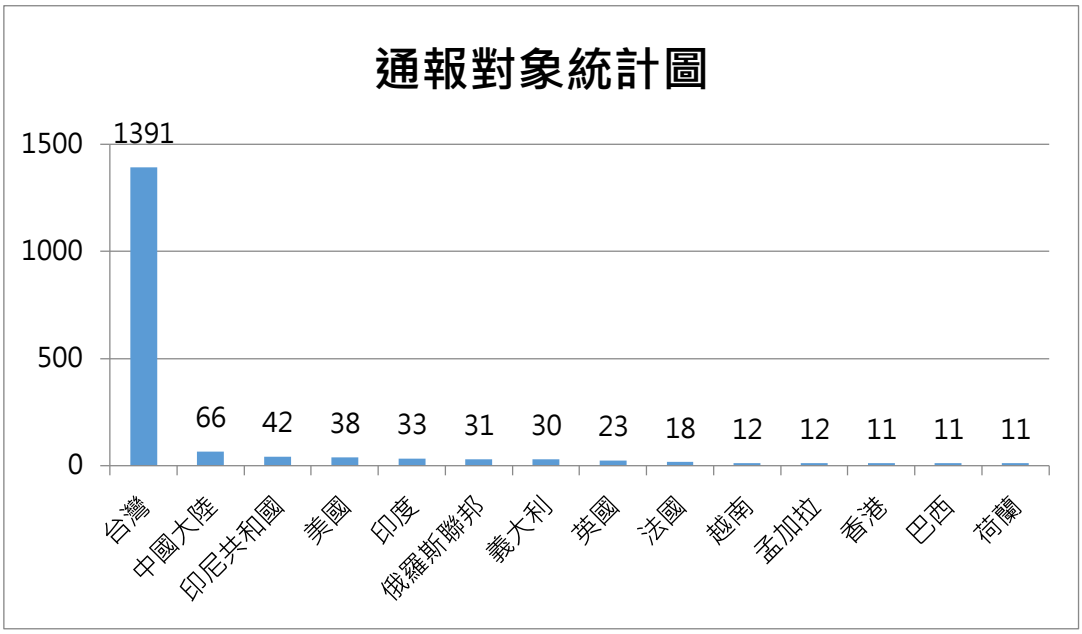


圖 2、通報對象統計圖

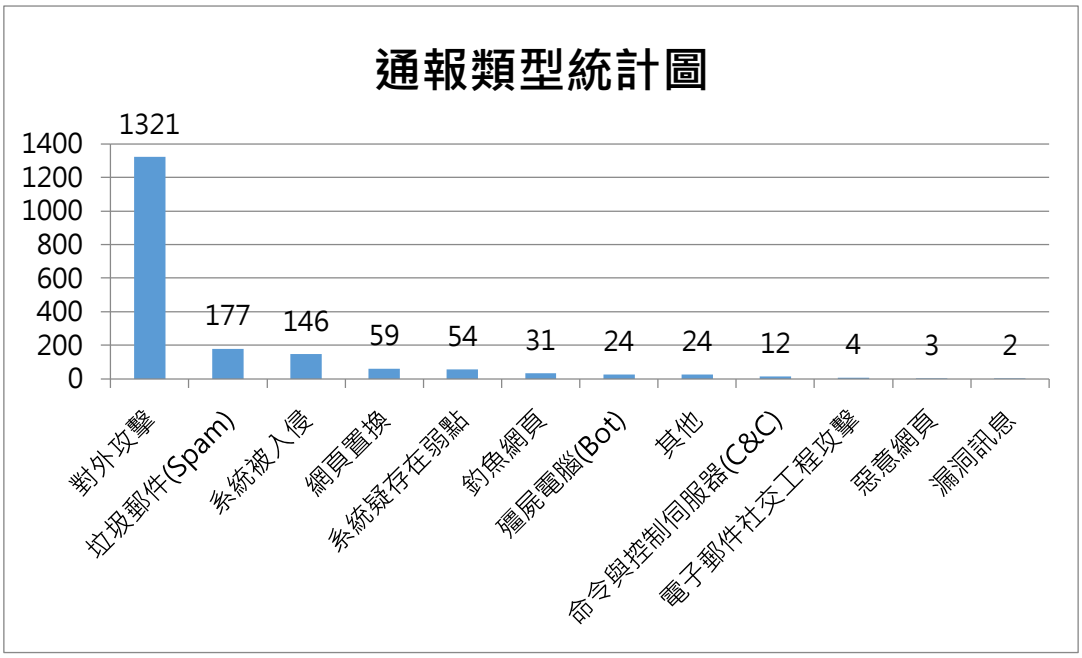
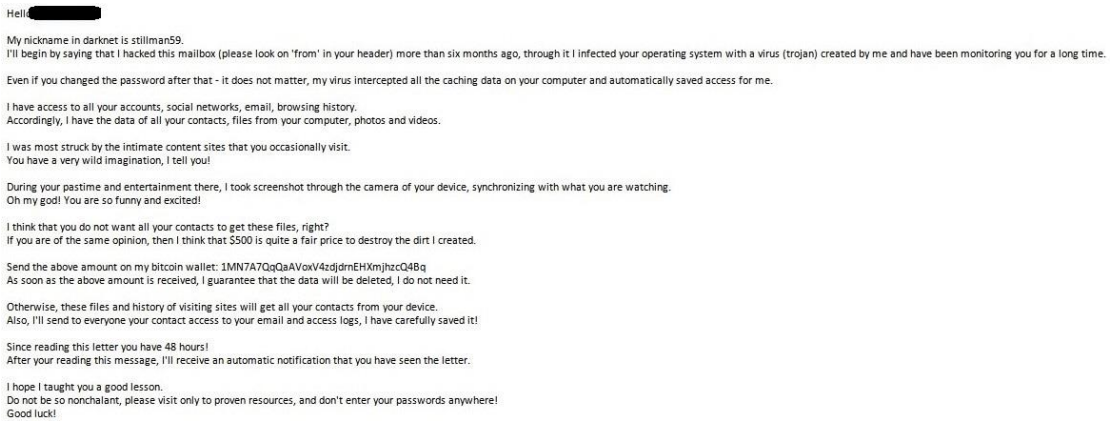


圖 3、通報類型統計圖

本中心近期接獲通報，表示收到有人掌握其硬碟檔案並要求於 48 小時內支付 500 美金之恐嚇信，經本中心查找與比對信件內容及比特幣錢包 SiteKey 等特徵，發現 10 月 15 日網路上亦有相同案例，

如圖所示，認定為發信者未真正掌握受害人檔案系統之詐騙事件，提醒民眾勿匯款。



Hello[redacted]

My nickname in darknet is stillman59.
I'll begin by saying that I hacked this mailbox (please look on 'from' in your header) more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.
You have a very wild imagination, I tell you!

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.
Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?
If you are of the same opinion, then I think that $500 is quite a fair price to destroy the dirt I created.

Send the above amount on my bitcoin wallet: 1MN7A7QqQaAVoxV4zdjdrnEHXmjhzcQ4Bq
As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.
Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

Since reading this letter you have 48 hours!
After your reading this message, I'll receive an automatic notification that you have seen the letter.

I hope I taught you a good lesson.
Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere!
Good luck!

信件特徵：

(1) 信件開頭以「my nickname in darknet is XXXX」，其中 XXXX 可能隨機更換。

(2) 信件內容表示對方已掌握帳戶密碼、瀏覽器歷史紀錄等資料，並取得您的所有通聯紀錄、硬碟資料與照片。

(3) 要求 48 小時內支付 500 美元的比特幣至指定的帳戶。

TWCERT/CC 提供以下防護建議：

(1) 密碼建議使用 12 個字元以上且英文、數字、符號混合。

(2) 應避免多個服務使用同一組密碼，以免遭到撞庫攻擊 (說明如註解)。

(3) 收到電子郵件不任意開啟信件之附件或網路連結，以避免遭植入惡意程式竊取資訊。

(4) 確實持續更新電腦的作業系統、Office 應用程式等至最新版本。

(5) 更新電腦防毒軟體病毒碼。

註解：什麼是撞庫攻擊?

人們與網路服務連結越來越深，各大網路都有帳號跟密碼資訊，但人們可能難以依據資安建議，一個服務用一個獨一的密碼，常是好幾個不同服務，所輸入的帳號密碼組合一樣，免得帳密常常忘記，得時常重設。人類的記性不足以及惰性，給予駭客可趁之機。只要取得某次服務帳密外洩的資料庫，賭一把看看其他服務是不是採用一樣的帳密，嘗試登入看看，不必用暴力破解法多次嘗試，就可合法登入受害者系統或服務。

●參考連結：

[1] https://malwaretips.com/threads/email-received-from-supposed-darknet-hacker.87366/

[2] https://productforums.google.com/forum/#

[3] https://www.scamwarners.com/forum/viewtopic.php?f=9&p=374862

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 11 月 15 日

編　　輯：羅文翎

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。