TWCERT/CC 資安情資電子報

2020 年 7 月份

目錄

第 1 章、 封面故事

微軟警告 Exchange Email Server 遭大規模駭侵攻擊，應儘速更新

微軟日前發出資安警告，指出目前觀測到針對 Exchange Email Server 已修補漏洞發動的大規模駭侵攻擊活動；用戶應儘速更新至最新版本。

微軟日前發出資安警告指出，該公司自四月起就觀測到針對 Exchange Email Server 已修補漏洞發動的大規模駭侵攻擊活動；用戶應儘速更新至最新版本。

這波攻擊行動鎖定的 Exchange Email Server 漏洞，是微軟早在今年二月就發出修補更新的 CVE-2020-0688；這個漏洞在於所有過去部署過的 Exchange Email Server 都採用相同的加密金鑰，導致駭侵者能夠輕易取得伺服器的控制權限。

雖然微軟早在二月就發布了修補更新，但資安專家指出，還是有很多 Exchange Server 並未及時更新；一份發表於四月份的資安研究報告說，網路上至少有 35 萬台 Exchange Server 存有應修補但未修補的資安漏洞。

Email Server 是駭侵者非常喜愛的攻擊目標，這是因為 Email Server 可說是公司行號或各種組織的訊息集散中心，只要攻陷 Email Server，就可以掌握非常大量的機敏資訊。

一般針對 Exchanger Server 的攻擊，在過去多半是以釣魚郵件來攻擊伺服器或桌機的資安漏洞；但四月觀察到的這波攻擊行動，主要是攻擊 Exchange Server 內的 IIS 內含的遠端執行任意程式碼漏洞。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688
  2. https://www.microsoft.com/security/blog/2020/06/24/defending-exchange-servers-under-attack/
  3. https://www.zdnet.com/article/over-350000-microsoft-exchange-servers-still-open-to-flaw-thats-under-attack-patch-now/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、TWCERT/CC 近期監控到四種惡意程式的感染趨勢增加，提醒大家注意防範

TWCERT/CC 近期發現有四種惡意程式的感染有增加的趨勢，分別名為 KratosCrypt、Quant Loader、Isrstealer 及 Mirai，圖 1 為遭受不同惡意程式感染的國內 IP 數量趨勢概況。

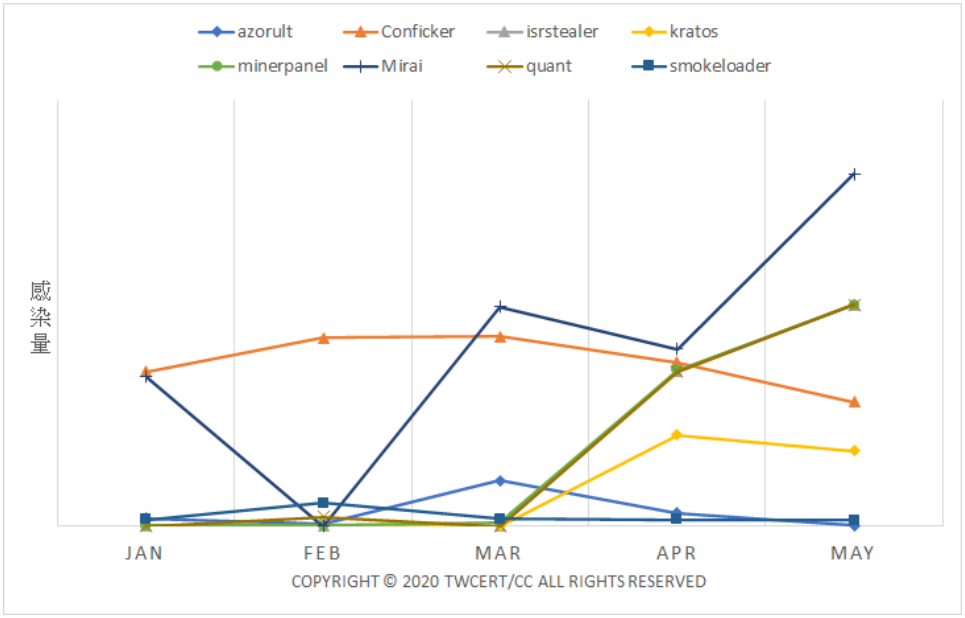


圖 1、2020 1-5 月我國國內感染各種惡意程式之 IP 趨勢概況

KratosCrypt 為一種勒索軟體(ransomware)，其目的是將檔案加密讓使用者無法存取，藉此向使用者勒索贖金，感染後檔案之副檔名會被強制修改成".Kratos"，且無法正常開啟。勒索軟體通常透過木馬病毒的方式傳播，或是社交工程郵件誘使下載。

Quant Loader 是一種惡意程式下載器，透過社交工程郵件誘導使用者點擊 Google 雲端硬碟連結下載 Quant Loader，再透過 Quant Loader 下載其他木馬程式盜取使用者資訊甚至成為殭屍電腦(bot)。研究發現殭屍病毒 Necurs 在 2017 年 4 月之後，結合 Quant Loader 出現新形態的攻擊手法，因 Quant Loader 本身不具有攻擊行為，在初期不易被防毒軟體檢測，Necurs 藉此感染電腦形成殭屍網路。目前已知 Quant Loader 還用來散播 Locky(勒索軟體)與 Pony(密碼竊取惡意程式)。

Isrstealer 是一種鍵盤側錄惡意程式，藉由紀錄鍵盤敲擊來竊取機敏資訊，根據研究顯示該惡意程式是由另一名為 Hackhound 的惡意程式修改而來的版本。該傳播方式通常透過釣魚網頁或是社交工程郵件誘使下載。研究發現部分攻擊手法在社交工程信件中夾帶 Microsoft Word，若受害者端未修補 Microsoft Office，打開後即馬上下載 ISR Stealer 並回傳鍵盤紀錄至惡意伺服器。

Mirai 是一種針對 Linux 為底層的殭屍病毒，主要感染目標為可存取網路的電子產品(IOT)，例如：網路攝影機、家用路由器等...。 2016 年駭客透過 Mirai 發動高流量 DDOS 攻擊知名資安網站，曾達到 620 Gbps 的驚人數字。 目前 Mirai 的原始碼已被公開於駭客論壇，其部分技術甚至被其他惡意程式採用。 根據趨勢科技發現 Mirai 目前有 13 種新型態的變種病毒，這 13 種型態利用的漏洞幾乎都在 Mirai 出現之前就已經存在，新型態的 Mirai 甚至利用 Windows 當跳板尋找 Linux 設備感染，或是具備暴力破解功能入侵設備。

近期感染趨勢增加的三支惡意程式(KratosCrypt、Quant Loader、Isrstealer)都是透過誘騙的方式來感染電腦， 在使用電子郵件或瀏覽網頁

時必須更加留意。而另一支 Mirai 則是針對有漏洞的 IOT 設備攻擊。

建議防範方式：

- IOT 設備：

1.修改預設帳號密碼並定期更改

2.若設備具備 Admin 帳號，視情況關閉

- 修改電子郵件設定：

1.開啟純文字模式

2.取消預覽功能

3.確認郵件來源

- 電腦本機端設定：

1.Windows Update 更新至最新

2.防毒軟體更新最新病毒碼

3.開啟防火牆

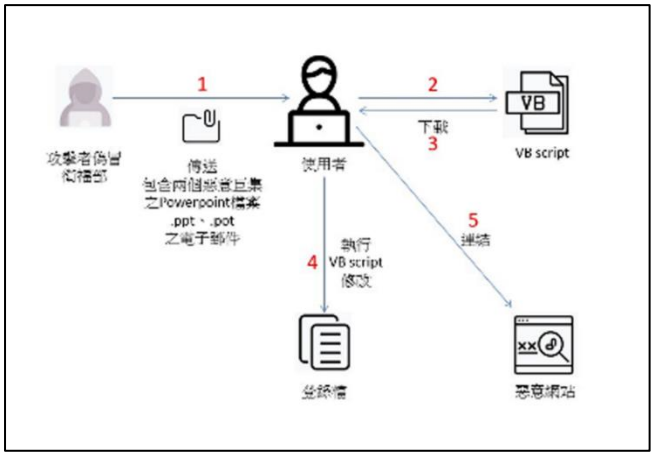
- 資料來源：

1. https://www.malware-traffic-analysis.net/2018/02/08/index.html
2. https://www.mcafee.com/enterprise/en-au/threat-center/threat-landscape-dashboard/ransomware-details.kratoscrypt-ransomware.html
3. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/phishing-attacks-employ-old-effective-password-stealer/
4. https://newsroom.trendmicro.com/news/new-necurs-variant-uses-internet-shortcuts-quant-loader-to-deliver-payloads/article/761510
5. https://community.rsa.com/community/products/netwitness/blog/2018/02/14/malspam-delivers-isr-stealer-2-13-2017

6. https://blog.trendmicro.com.tw/?p=60735

7. https://en.wikipedia.org/wiki/Mirai_(malware)

2.1.2、Covid-19 目標式釣魚郵件攻擊事件說明



近來發現多起針對科技公司的網路釣魚郵件攻擊，駭客假冒衛福部之名義發送標題為「免費分發 covid-19 防護設備(台灣衛生部)」之釣魚郵件。

近來發現多起針對科技公司的網路釣魚郵件攻擊，駭客假冒衛福部之名義發送標題為「免費分發 covid-19 防護設備(台灣衛生部)」之釣魚郵件，引誘使用者點擊信件且於信件中夾帶 2 個含有惡意巨集(Marco)的 PowerPoint 檔案，當使用者開啟該惡意 PowerPoint 檔案，會透過巨集指令連線到惡意網站，下載惡意 VBScript 再透過 VBScript 修改受害電腦的登錄檔藉此發動惡意行為。

TWCERT/CC 掌握該惡意檔案樣態，若企業資安單位有 IOC 的需求請使用企業信箱與我們聯繫，(聯繫信箱: twcert@cert.org.tw)，若有相關單位受害，亦可與我們聯繫進行協處，謝謝。

2.1.3、駭侵者針對 Office 365 遠距工作用戶發動釣魚郵件詐騙攻擊

資安廠商發現，近來有一波針對遠距工作 Office 365 用戶的釣魚郵件詐騙攻擊，佯稱用戶所屬單位要調整 VPN 設定，實則騙取駭入該單位所需的各項資訊。

Email 資安防護廠商 Abnormal Security 日前發表研究報告，指出該公司發現近來有一波針對遠距工作 Office 365 用戶的釣魚郵件詐騙攻擊；在釣魚郵件中，駭侵者佯稱用戶所屬單位要調整 VPN 設定，要求用戶輸入登入其 Office 365 的帳號密碼，以騙取駭入該單位所需的各項資訊。

廠商說，該公司在這波攻擊中已經觀察到至少 15,000 起針對不同目標的攻擊活動。由於疫情關係，全球有許多大型公司要求員工透過 VPN 在家工作，因此這波假稱更改 VPN 設定的釣魚攻擊相當有效。

攻擊者在發出的詐騙信件中，會竄改 sender 欄位，使用目標受害者所屬公司的網域名稱發送，以降低被駭者的戒心；駭客更會使用多個不同的 Email 發送地址和伺服器，以降低被追蹤發現的可能性。

但在信中駭客置入的惡意網頁連結，則都是同一個網址；這表示各個不同來源的釣魚攻擊，其實都由同一組駭侵者所發動。

受害者一旦誤點信中的釣魚連結，就會被導向到一個用來詐騙的虛假 Office 365 登入畫面；而且駭客把這個頁面放在微軟自己的 Azure Blob 雲端儲存

空間，所以網址不但會顯示為「web.core.windows.net」，而且還會顯示該網頁擁有微軟簽發的 SSL 加密憑證，更為降低用戶的警覺。

資安廠商指出，看到這類網頁的用戶，其實更應提高警覺；因為這類網頁只應該顯示為各員工自己公司擁有的網域名稱，不應該是外部雲端空間的網址。

- 資料來源：
  1. https://abnormalsecurity.com/blog/abnormal-attack-stories-vpn-impersonation-phishing/
  2. https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-remote-workers-with-fake-vpn-configs/。

2.1.4、Amazon 證實曾遭史上最大 DDoS 攻擊

Amazon 日前公布，該公司的 AWS 服務曾於今年二月間遭到史上最大的分散式服務阻斷攻擊（DDoS, Distributed Denial of Service），所幸成功阻擋下來。。

Amazon 日前對外公布 2020 年第一季資安威脅報告，報告中揭露該公司的 Amazon Web Services 雲端服務，曾於今年二月間遭到史上最大的分散式服務阻斷攻擊（DDoS, Distributed Denial of Service），所幸成功阻擋下來。

這波 DDoS 攻擊的流量高達 2.3Tbps，打破 2018 年 3 月 GitHub 遭到攻擊時創下的 1.7Tbps 流量記錄。

這份報告總結過去一季以來 AWS 主機阻擋下來的各式駭侵攻擊，而其中最大宗的就是以瞬時巨大流量進行的 DDoS 攻擊。

若和 2019 年第四季相比，AWS 遭受攻擊的次數，從 28 萬次左右上升到 31 萬餘次，增幅達 10%；單一攻擊事件的最大瞬時流量，則由 2019 年第四季的 0.6Tbps 快速上升到 2.3Tbps，增幅高達 283%。

以每周攻擊次數來看，AWS 每周至少遭到 20,000 次以上駭侵攻擊，最高則超過 60,000 次。

以 DDoS 的攻擊技術來分析，2020 年第一季透過 CLDAP 反射放大攻擊的規模和次數，較往年大幅提高；事實上發生在 2 月這次流量高達 2.3Tbps 的攻擊，就是屬於新型態的 CLDAP 反射放大攻擊。發生頻率次高的攻擊技術，則是 SYN 洪水攻擊。

- 資料來源：
  1. https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf
  2. https://www.pcmag.com/news/amazon-mitigates-biggest-ever-ddos-attack
  3. http://www.cc.ntu.edu.tw/chinese/epaper/0048/20190320_4801.html

2.1.5、日本與歐洲多國製造業最近大舉遭駭，尤以能源產業為甚

資安廠商指出，日本和歐洲多個國家的製造業業者，最近遭到手法十分複雜成熟的駭侵攻擊，而且攻擊所使用的惡意軟體，愈來愈難以偵測。

資安廠商卡巴斯基發表研究報告，指出該公司觀測到日本和歐洲多個國家的製造業業者，最近開始遭到手法十分複雜成熟的駭侵攻擊；而且攻擊所使用的手法與惡意軟體，愈來愈難以偵測。

卡巴斯基說，自 2020 年 5 月初開始，發現日本、德國、英國和義大利的多家重要工業設備製造業者和針對製造業者開發軟體的部分公司，陸續遭到駭侵團體鎖定攻擊。

報告指出，在遭駭的業者當中，駭侵者特別著重在能源產業的攻擊；雖然公司的防毒防駭服務已成功阻擋一些攻擊活動，但目前不知駭侵者的攻擊目的為何。

卡巴斯基指出，駭侵者主要的攻擊目標為這些企業的 IT 架構，而非營運或製造節點（OT）；攻擊的目標以竊取系統登入資訊為主。

在卡巴斯基攔截到的攻擊行為中，典型的攻擊樣態仍以釣魚郵件為開始；駭侵者針對攻擊對象發送以該國語言編寫的釣魚郵件，並在確定被駭主機作業系統的語言與釣魚信件一致後，才會展開下一階段的攻擊。

釣魚郵件中含有微軟 Office 文件檔案，內含惡意巨集程式碼；當受害者開啟文件，該巨集就會執行一個 PowerShell 指令檔，並且下載內含進一步攻擊指令的圖片。接著惡意軟體會解開圖片內含的惡意程式碼，產生另一個 PowerShell 指令檔，並且執行著名的密碼竊取軟體 Mimikatz。也因如此多重的手法，造成其攻擊偵測難度提升。

- 建議採取資安強化措施

1、應多加防範釣魚郵件，對可疑或聳動標題的電子郵件保有警覺心，收到陌生寄件者寄來的郵件，應使用其他管道加以查證對方身分，不隨意開啟電子郵件，也不點擊郵件內的任何附件、圖片與超連結等。

2、調整電子郵件設定的設定，開啟純文字模式、取消預覽功能。

3、對 Microsoft Office 文件之巨集功能予以限制或停用。

4、安裝防毒軟體及防火牆，確保防毒軟體保持最新狀態，並配合廠商發行的安全性修補程式，定期更新電腦系統、軟體與設備等，以修補資安漏洞。

- 資料來源：

1. https://www.securityweek.com/industrial-suppliers-japan-europe-targeted-sophisticated-attacks
2. https://www.ithome.com.tw/news/112744
3. https://docs.microsoft.com/zh-tw/windows/security/threat-protection/intelligence/macro-malware。

2.1.6、超過 300 種以上惡意軟體，利用肺炎全球大流行藉機肆虐

資安廠商指出，自今年三月全球陷入肺炎疫情大流行開始，偵測到超過三百種以上惡意軟體，在這段期間內大肆活動。

資安廠商 Palo Alto Networks 旗下的資安研究團隊 Unit 42，日前發表研究報告，指出自今年三月全球陷入肺炎大流行開始，該單位偵測到超過三百種以上惡意軟體，在這段期間內大肆活動。

該單位自三月一日到四月七日期間，監控全球所有 Prisma Cloud 網路上的異常活動，鎖定 20 個可疑的 IP 位址和網域，自 453,074 個網路連線活動中，偵測到非常多的攻擊活動。

Unit 42 說，一共發現 7 個特別可疑的雲端伺服器位址，和各種惡意軟體的網路連線活動有關；而這些惡意軟體的攻擊活動，都假借 Covid-19 之名而行。

以偵測方式而言，Unit 42 設計了一個稱為「AutoFocus」的偵測機制，特別著重觀測在惡意軟體活動時會使用的關鍵字，如「Corona」、「COVID」、「Pandemic」、「Virus」等，結果發現共有 446 種不同的惡意軟體樣式，共透過 20 個不同的 IP 或網域參與攻擊活動。

Unit 42 建議，各公司行號應該針對其使用公有雲端服務的部分，加強防火牆和其他惡意軟體偵防的能量，並進行正確的設定與必要的升級，以免公

司內部系統遭到來自公有雲惡意軟體的攻擊。

- 資料來源：
  1. https://backendnews.net/2020/06/08/unit-42-discovers-over-300-covid-19-themed-malware-in-public-cloud-environments/
  2. https://unit42.paloaltonetworks.com/covid19-cyber-threats/。

2.1.7、過去兩年來，全球加密貨幣交易所共被單一駭侵團體竊走超過兩億美元

資安廠商指出，過去兩年以來，全球各大加密貨幣交易所遭某個駭侵團體攻擊，因而被竊走的各種加密貨幣，總額高達兩億美元。

資安廠商 ClearSky 日前發表研究報告，指出過去兩年以來，一個名為 CryptoCore 的駭侵團體，針對全球各大加密貨幣交易所進行駭侵攻擊；因而被竊走的各種加密貨幣，總額高達兩億美元。

報告說，這兩年來被該團體攻擊的加密貨幣交易所近二十家，分布在美國、中東和亞洲各國；其中受害最深的幾家交易所均位於日本。

該報告沒有透露被駭交易所的清單，但廠商認為駭侵者可能與東歐、烏克蘭、俄羅斯和羅馬尼亞的駭侵者有關。

報告指出，這些駭侵者利用魚叉式釣魚攻擊，設法駭入加密貨幣交易所的熱錢包，或是針對這些交易所管理高層或 IT 技術人員的個人 Email 帳號進行攻擊。駭侵者會發送假冒受害對象所屬公司或其他公司高層的來信，以取信受害者，再取得相關系統的登入資訊，或在受害人員使用的電腦上安裝惡意軟體，以進行進一步的駭侵攻擊。

ClearSky 認為 CryptoCore 的攻擊手法，不算特別先進複雜，但卻相當有效；該公司從 2018 年五月起開始觀察到這個駭侵團體的攻擊活動，之後也一直持續觀察到來自該團體的各類駭侵攻擊；而攻擊行動可能因為肺炎疫情影

響，在 2020 年上半年逐漸趨緩，但未完全停止。

ClearSky 的研究報告，也揭露了詳細的攻擊手法分析。

- 資料來源：
  1. https://www.clearskysec.com/cryptocore-group/
  2. https://cointelegraph.com/news/someone-has-been-on-a-200m-crypto-exchange-hacking-spree
  3. https://securityaffairs.co/wordpress/105168/cyber-crime/cryptocore-stole-200m-crypto-exchanges.html。

2.1.8、駭侵者將惡意軟體藏在 EXIF 中，用以竊取信用卡資訊

資安廠商指出，一個專門竊取信用卡資訊的駭侵團體 Magecart，已經發展出將惡意軟體內嵌於 JPEG 圖檔描述資訊 EXIF 欄位的技術。

資安廠商 Malwarebyte 日前發表研究報告指出，一個專門竊取信用卡資訊的駭侵團體 Magecart，已經發展出將惡意軟體內嵌於 JPEG 圖檔描述資訊 EXIF 欄位的技術中；並且已經潛藏在某些網路商店使用的網頁圖檔內。

被 Malwarebyte 發現藏有惡意圖片的，是一些使用 WordPress 開發的網路商店模組 WooCommerce 進行線上零售的 WordPress 網站；由於採用 WooCommerce 打造網路商店的 WordPress 為數眾多，因此成為駭侵攻擊者的一大目標。

Malwarebyte 的研究人員發現，在受駭網路商店頁面中的 Javascript 惡意程式碼，夾藏在頁面用 JPEG 圖檔 EXIF 中的版權宣告區段內。

研究人員說，利用各種手法，在圖檔中夾藏惡意程式碼的手法並不少見，但這是首次運用於信用卡竊取之上。這段惡意程式還會把竊得的信用卡資訊，以 Base64 編碼後倒序輸出成圖檔格式，再以 POST 指令送出。

Malwarebyte 的報告中，詳細描述了 Magecart 這波攻擊的手法；在去年十月的一份研究報告中指出，有兩萬個以上的網路商店遭到 Magecart 集團的攻擊；2018 年發生在英國的一次 Magecart 攻擊中，共有五十萬人的信用卡資

訊遭竊。

- 資料來源：
  1. https://blog.malwarebytes.com/threat-analysis/2020/06/web-skimmer-hides-within-exif-metadata-exfiltrates-credit-cards-via-image-files/
  2. https://www.computing.co.uk/news/4017010/hackers-hide-magecart-script-favicon-image-exif-steal-credit-card-details

2.2、國際政府組織資安資訊

2.2.1、美國明尼蘇達州政府遭駭侵攻擊

明尼蘇達州首府明尼亞波利斯的州政府電腦系統，遭駭客攻擊而癱瘓。

當美國國內因為種族問題發生抗議事件時，事發地明尼蘇達州首府明尼亞波利斯的州政府與市政府電腦系統，亦遭駭客攻擊而癱瘓。

明尼亞波里斯一名政府發言人表示，該市政府所屬的官方網站，以及各項系統，在上周四起遭到強力的分散式服務阻斷攻擊（DDoS），各項系統遭到突如其來的超大流量襲擊，導致系統全面停擺。

該市的資訊人員，在遭到攻擊後的數小時內，就將系統回復到約 95% 的程度；該發言人表示，被攻擊的系統在隔天就能完全恢復正常運作。

目前這起攻擊事件，沒有傳出任何資料遭竊或被破壞的情形；但也還不清楚攻擊發動者的身分。

另外，明尼蘇達州警察局的官方網站，也同步傳出被駭消息；不具名的攻擊者駭入了警察局的網站系統，並在首頁放置了一段抗議的影片。

也有不具名駭侵團體散布消息，說他們從警察局竊得敏感資訊並部分釋放出來，但也有資安研究專家認為該批資料是從過去的外洩事件中拼湊而得，並非直接竊自警局系統。

明尼蘇達州州長指出，他們相信這起駭侵事件中的分散式服務阻斷攻擊，使用了相當成熟複雜的手法進行攻擊行動；雖然還不知道到底是誰發動這場攻擊，但州長認為應該不是普通駭客所為。

- 資料來源：
  1. https://thehill.com/policy/cybersecurity/500009-minneapolis-city-systems-temporarily-brought-down-by-cyberattack
  2. https://thehill.com/homenews/state-watch/500372-governor-minnesota-hit-by-cyberattack-as-efforts-to-contain-protests
  3. https://threatpost.com/anonymous-hack-minneapolis-police-department-fake/156171/。

2.2.2、美國警局所屬數十萬筆敏感資料，遭駭侵者公開

資安研究者指出，一個名為「BlueLeaks」的資料庫，最近在網路上遭到公開，內含數十萬筆來自美國各州警局的機敏資訊。

獨立資安研究人員 Brian Krebs 近日於個人部落格「KrebsOnSecurity」指出，一個名為「BlueLeaks」的資料庫，最近在網路上遭到公開；這個資料庫內含數十萬筆來自美國各州警局的機敏資訊。

公開這個資料庫的組織或個人，稱為 DDoSecrets；該組織如同 Wikileaks 一樣，專門在網路上公開各種政府與情治單位內部的機密資訊。

這次被公開的警方內部資料，整個資料庫的檔案大小高達 270 GB，來源疑似來自位於美國德州的網路設計與託管服務商遭到駭入，這家服務商同時託管許多美國政府不同部門之間共享的資料庫。

DDoSecrets 指稱，這個資料庫搜集來自 200 間警政相關單位十年來的累積資料，而 KrebsOnSecurity 也向當局求證後，確定資料庫內的各項資料都是真實資訊。

當局分析該資料庫後證實，這些資料的記錄年度從 1996 年八月開始，一直到 2020 年 6 月 19 日，足足橫跨 24 年之久。

資料庫中和個資相關的欄位，包括許多犯罪嫌疑人姓名、Email 地址、電話號碼、PDF 文件檔案、相片，以及多量的文字、影片、CSV 檔案和 Zip 壓縮檔；有些甚至還含有金融轉帳資訊等機敏資訊。

- 資料來源：
  1. https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/
  2. https://www.zdnet.com/article/blueleaks-data-from-200-us-police-departments-fusion-centers-published-online/

2.3、社群媒體資安近況

2.3.1、三個 YouTube 頻道被駭，用以假借 SpaceX 名義進行比特幣詐騙

就在 SpaceX 成功發射載人火箭之際，有駭侵者盜取三個知名 YouTube 頻道後，假借 SpaceX 名義進行比特幣詐騙活動，獲利高達 15 萬美元。

SpaceX 成功發射載人火箭，將兩名美國太空人順利送進國際太空站；但同一時間有駭侵者盜取三個知名 YouTube 頻道，並且假借 SpaceX 與其創辦人 Elon Musk 名義進行比特幣詐騙活動，不法獲利高達 15 萬美元。

被盜的三個 YouTube 頻道分別是 Juice TV、Right Human 與 MaximSakulevich，各自有幾十萬追蹤者；駭侵者取得這三個頻道的控制權後，先把頻道名稱改為「SpaceX Live」或「SpaceX」，然後開始進行詐騙活動直播。

詐騙直播的內容是在畫面中間放一段 Elon Musk 受訪的錄影或 SpaceX 的發表會，假裝是立即直播，然後在畫面下方要求觀眾將小額比特幣匯入某個錢包的網址內，就可以收到加倍的匯回款。

直播吸引了約八萬人同步線上觀看，而自六月八日起，用來接收詐騙款項的比特幣錢包，一共收到了近 150,000 美元的比特幣匯入款。

在創業論壇 HackNews 的討論區中，也有用戶指出，每當 SpaceX 創辦人 Elon Musk 在 Twitter 上發表任何推文，下頭一定馬上就有和比特幣詐騙有關的回應貼文；而 Elon Musk 從 2018 年起就經常成為類似加密貨幣詐騙案最喜

歡假冒的對象。

資安媒體 BleepingComputer 曾就此事向 YouTube 詢問，但沒有得到任何回應；資安專家也指出，擁有人氣頻道的 YouTuber 網紅或經營者，應該加強對帳號密碼的保護，而且要對疑似釣魚郵件或釣魚網頁提高警覺，才能被免帳號被盜，並用來進行各式詐騙的風險。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/fake-spacex-youtube-channels-scam-viewers-out-of-150k-in-bitcoin/
  2. https://news.ycombinator.com/item?id=23470224
  3. https://nakedsecurity.sophos.com/2020/06/11/bitcoin-scammers-take-youtube-channels-for-a-spacex-ride/

2.3.2、多個約會 App 同時發生資料外洩事件，多達十萬用戶私密照片、影片流出

資安廠商發現，近來多個約會交友 App，同時發生用戶個資外洩事件；多達十萬用戶上傳的私密照片、影片檔和用戶間的對話記錄與語音對談檔案流出，檔案大小高達 845 GB。

資安廠商 vpnMentor 發表研究報告指出，該公司的資安研究團隊近來發現多個約會交友 App，幾乎在同時發生用戶資料外洩事件；多達十萬用戶上傳到這些服務的私密照片遭到流出，含有這些用戶個資的檔案大小，則高達 845 GB。

發生外洩事件的 App 包括 3somes、CougarD、Gay Daddy Bear、Xpai、BBW Dating、Casualx、SugarD、Harpes Dating 等。

據研究團隊指出，這些 App 雖然看似各自獨立，其實是由同一組開發團隊所推出，因此不同 App 的用戶資料，都放在 AWS 裡同一個帳號的儲存空間之下，所以才會同時發生資料外洩事件。

在這起資料外洩事件中的受害者人數估計高達十萬人，總資料筆數超過兩千萬筆；大多遭到外洩的相片，都屬用戶上傳的私密相片、影片與私密聊天內容，甚至很多都和親密行為相關，因此也對這些用戶的個人隱私造成嚴重衝擊。

造成資料外洩的原因，是因為這些 App 的開發者，沒有正確設定其在 AWS 上的資安選項。vpnMemtor 於五月下旬向其中一支 App 的開發者通報這

起資料外洩事件，對方回應要求提供更多資料後，就沒有再和 vpnMentor 聯絡；但所有 App 的資料庫資安設定都已同步修正。

- 資料來源：
  1. https://www.vpnmentor.com/blog/report-dating-apps-leak/
  2. https://www.wired.com/story/dating-apps-leak-explicit-photos-screenshots/

2.4、行動裝置資安訊息

國際外送 Foodpanda 及其他國際外送平臺顧客資料外洩

2020 年 5 月 19 日著名國外論壇發布一則個資資料外洩事件，並轉發至其他網路論壇。

共計 14 個國家 72 萬多筆個人帳戶，包含姓名、電話等個資及極為精確的地址座標資料均遭竊取外洩。

Foodpanda 國際外送公司總部位於德國柏林的 Delivery Hero 承認上述事件為其品牌外送商家資料遭竊，資料最早可追朔到 2016 年至今的個人帳戶資料，該公司已與相關當局密切合作調查以找出資安漏洞原因，並通知受影響各方。

據報導顯示，受外洩資料影響的國家有阿拉伯聯合大公國、瑞典、德國、西班牙、法國、香港、荷蘭、加拿大、澳大利亞等 Foodora 註冊用戶，在新加坡則為 Foodpanda 註冊用戶受個資遭竊影響。

資料外洩專家 Troy Hunt 說明，澳大利亞遭洩資料大約有 79,000 筆紀錄，其中包含 60 萬個電子郵件地址，資料是每個國家一系列 SQL 文件，標記為 CustomerAddress 和 Customers。分析指出外洩資料甚至還包含客戶訂單的註釋，例如服務評價或訂購人為某人訂購食品的關係，甚至非訂購人居住地址等隱私資訊外流之資安事件。

建議用戶立即重新設定密碼，使用 12 字元以上長度較長之密碼，並定期更換密碼。於業者推出新版本後，應將應用程式更新至最新版本，以修補資安漏洞。

- 資料來源：
  1. https://www.bankinfosecurity.com/delivery-hero-confirms-foodora-data-breach-a-14435
  2. https://blog.trendmicro.com.tw/?p=63243

2.5、軟體系統資安議題

2.5.1、Adobe 呼籲用戶盡速移除 Adobe Flash

Adobe 公司指出，曾經廣受歡迎的 Adobe Flash，即將於今年 12 月 31 日結束產品生命週期；仍在使用該產品的用戶，應盡速移除，以減少資安風險。

Adobe 公司指出，曾經廣受歡迎的 Adobe Flash 多媒體製播程式，即將於今年 12 月 31 日完全結束產品生命週期，屆時將不再提供任何更新檔；仍在使用該產品的用戶，應盡速移除，以減少資安風險。

Adobe 表示，除了在今年 12 月 31 日後不再提供更新外，還會從官網完全移除 Adobe Flash 的下載連結；甚至已安裝 Adobe Flash Player 的用戶，也無法播放任何既有的 Flash 內容。

資安專家指出，Adobe Flash 一直以來都是駭侵者相當喜愛的攻擊對象，除了經常被發現 0-day 漏洞外，也常被利用 Flash 的各種資安漏洞進行系統入侵攻擊，或是釣魚詐騙等。

在 HTML5 和 WebGL 等網路多媒體的公開標準出現後，先是 iOS 系列產品率先停止支援 Adobe Flash，接著是各種使用 Flash 製作的內容逐漸減少；Adobe 公司也早在 2017 年七月就宣布 Flash 的產品生命結束日期。

許多原本內建 Flash Player 外掛模組的瀏覽器，最近也陸續停用這個模組；Chrome 從 76 版開始停用 Flash，而 Firefox 則是自 69 版開始停止支援 Flash 內容播放。

- 資料來源：
  1. https://www.adobe.com/products/flashplayer/end-of-life.html
  2. https://threatpost.com/adobe-prompts-users-to-uninstall-flash-player-as-eol-date-looms/156794/。

2.5.2、QNAP NAS 設備漏洞遭勒索軟體攻擊，建議立即更新至最新版本

QNAP 技術團隊於今年5月收到多起攻擊通報，發現 NAS 設備漏洞遭 eCh0raix 勒索軟體攻擊。

經 QNAP 分析，遭攻擊的漏洞為 QTS 與 Photo Station 舊版本中的某些漏洞，QNAP 已於 2019 年 9 月發布相關補救措施與安全性建議 https://www.qnap.com/en/security-advisory/nas-201911-25。

敬請尚未更新修補漏洞之用戶，立即將 NAS 設備含有漏洞之相關產品更新至最新版本，以免遭受駭客攻擊而造成損失。詳細資訊請參閱 QNAP 安全性建議 https://www.qnap.com/zh-tw/security-advisory/qsa-20-02。

- 資料來源：
  1. https://www.qnap.com/en/security-advisory/nas-201911-25
  2. https://www.qnap.com/en/security-advisory/qsa-20-02。

2.5.3、美國頂尖航太供應商遭 Maze 勒贖軟體攻擊，損失資料量達 1.5TB

位在德州的美國頂尖航太產業供應商 VT SAA，日前證實其公司網路遭到 Maze 勒贖軟體駭侵攻擊，儲存於該公司內部網路的敏感資料遭竊，且資料量高達 1.5TB。

位在德州的美國頂尖航太產業供應商 VT SAA，在海洋、陸地和航太領域的軍用電子設備都是領導者；日前該公司證實其內部網路遭到 Maze 駭侵團體發動勒贖軟體駭侵攻擊；儲存於該公司內部網路的敏感資料遭竊，且資料量高達 1.5TB。

該公司總工程師兼副總裁 Ed Onwe 的聲明中說：「一個名為 Maze group 的駭侵團體，以複雜而先進的手法，非法進入本公司的內部網站，並且布署發動勒贖攻擊。」

據 VT SSA 的說明，這起攻擊事件共有兩波，第一波於三月七日發動，第二波則在五月發動。該公司是在發現部分內部資料檔案遭到更名並加密後，才發現自己遭駭。該公司立即進行斷網處理，開始進行調查，並且向相關主管機關發送資安事件通報。

在該公司開始進行內部調查，釐清受害範圍與程度後，確認主要遭竊的資料，屬於其母公司 ST 工程公司在美國的商業活動相關資料，包括該公司和多個政府組織、NASA、美國航空公司等合作單位的合約等機敏資訊，甚至還包括和各合作伙伴的各項計畫的細節，如計畫內容、時間表、行程、所需零

件和機具、財務記錄等等。

在這起事件爆發之前數日，Maze 駭侵團體也於暗網上公開了該組織竊自某家美國核電技術供應商的大量內部資料。

- 資料來源：
  1. https://www.hackread.com/us-aerospace-service-provider-breach-data/
  2. https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/

2.5.4、義大利國家電力公司 Enel 集團，遭 Snake 勒贖軟體攻擊

繼本田汽車遭到 Snake 勒贖軟體攻擊後，近日再傳歐洲大型電力集團 Enel（義大利國家電力公司）亦遭 Snake 攻擊事件。。

繼本田汽車遭到 Snake 勒贖軟體攻擊，造成該公司部分系統停擺後，近日再傳歐洲大型電力集團義大利國家電力公司 Enel 之內部網路亦遭 Snake 攻擊事件。

資安媒體 BleepingComputer 報導指出，Enel 集團向該刊確認，該公司的內部網路防毒防駭系統，偵測到一起惡意軟體攻擊事件；雖然 Enel 沒有公布惡意軟體是哪一支，但經外部資安專家分析後，確認就是先前攻擊 Honda 的 Snake（又名 EKANS）勒贖軟體。

Enel 指出，該公司的資安系統，在該惡意軟體開始於其內網散布之前，就加以截獲，並立即採取短暫的隔離斷網措施；在斷網調查修復完成後，隔天就順利恢復上線運作。

Enel 說，目前沒有發現遭到嚴重破壞的事件，所有電廠也都正常運轉，客戶相關資料也沒有被外洩至任何第三方處；僅有在斷網時造成客戶無法連線該公司進行相關操作，造成不便。

值得注意的是，Snake 在針對目標發動攻擊前，會先確認其運作環境所處的內部網域與 IP 位址；如果發現不是在正確的內部網路中執行，Snake 就不

會執行，也不會加密任何檔案。

Enel 的聲明中沒有提到特定的惡意軟體名稱，但有資安專家透過於 6 月 7 日提報到 VorusTotal 的惡意軟體取樣資訊，發現有個 Snake/EKANS 的取樣，內含網域名稱「eneling.global」；而這個網域名稱為 Enel 集團所有，而且會導向到該公司的全球網頁。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/

2.5.5、本田汽車遭勒贖軟體攻擊，全球部分業務停擺

日本車廠本田汽車的日本本部與歐洲分部，日前遭駭侵攻擊，致使部分重要業務停擺。

日本最大車廠本田汽車的日本本部與歐洲分部，日前遭駭侵攻擊，致使部分重要業務停擺。

本田汽車是在 6/8 發現日本和歐洲本田的電腦系統，疑似遭到 SNAKE 勒贖軟體攻擊，造成客服與汽車融資服務的 IT 系統無法運作，但沒有對生產線和銷售系統造成影響，不過為了安全起見，本田仍然短暫關閉部分生產線的運作。

隔日，一位資安研究人員在 Twitter 上發表系列圖片，指出有一支勒贖軟體不斷地存取本田汽車內部網路的網域，從 IP 解析來看，分別是位於日本和美國的本田內網主機。

資安媒體 BleepingComputer 也連絡上在背後操控 SNAKE 的控制者，對方不承認也不否認 SNAKE 涉及駭入本田汽車。

目前仍不清楚本田公司的受害程度與造成的損失金額，本田公司也說正在進行內部調查，尚無太多細節可對外公開；不過本田表示目前可確定沒有外洩任何資料，也沒有任何顧客受到這波攻擊的影響。

資安專家指出，SNAKE 勒贖軟體是在 2019 年底被發現的新興勒贖程式，雖然本身並沒有非常複雜成熟的技術，但是它會在某些條件下自動停止運作，這也造成追蹤上的困難。

也有資安專家表示，由於疫情關係，大量企業員工被迫遠距工作，也導致駭侵者可透過這些外部連線伺機駭入企業內網，發動各種攻擊。

- 資料來源：
  1. https://twitter.com/HondaCustSvc/status/1270048801307234304
  2. https://www.forbes.com/sites/daveywinder/2020/06/10/honda-hacked-japanese-car-giant-confirms-cyber-attack-on-global-operations-snake-ransomware/#15fecb0853ad
  3. https://www.bleepingcomputer.com/news/security/honda-investigates-possible-ransomware-attack-networks-impacted/

2.5.6、針對 Office 365 大型企業用戶的釣魚郵件攻擊，使三星、Adobe、牛津大學受害

資安廠商指出，包括三星、Adobe、牛津大學在內多家採用 Office 365 的大型企業或組織，近來遭到一波釣魚郵件的駭侵攻擊。

資安廠商 Check Point 近日發表研究報告，指出包括三星、Adobe、牛津大學在內多家採用 Office 365 的大型企業或組織，近來連續遭到一系列釣魚郵件的駭侵攻擊。

報告指出，由於採用 Office 365 解決方案的用戶非常多，近來經常成為駭侵攻擊活動的目標。最近該公司觀測到一起不甚成熟的釣魚攻擊活動，就是利用這些大企業的主機來轉送釣魚郵件，做為攻擊用的跳板，也藉以逃過防毒系統的偵測。

Check Point 於今年四月時發現，有一波釣魚郵件攻擊行動從 NordVPN 發出，透過牛津大學的 Email SMTP 伺服器寄送給受害者；由於牛津大學的網域是經認證的合法安全網域，所以這些攻擊信件就多半會被放行；甚至在 Office 的 Mail 界面上還會顯示「信件來自受信任的伺服器」訊息。

用戶收到這些名為「未聽取的語音留言」信件後，會看到一個「聽取或下載留言」的按鈕，按下後就會進入偽造的 Office 365 登入頁面；駭侵者就能藉以取得受害用戶的 Office 365 登入資訊。

也有釣魚攻擊行動是透過三星加拿大分社的 Adobe Comapign 伺服器轉寄，把用戶導向含有惡意頁面和惡意程式碼的 WordPress 網站，再發動後續的攻擊活動。

- 資料來源：
  1. https://research.checkpoint.com/2020/phishing-campaign-exploits-samsung-adobe-and-oxford-servers/
  2. https://www.computerweekly.com/news/252484788/Check-Point-uncovers-targeted-Microsoft-Office-365-phishing-campaign。

2.5.7、小心用以散播勒索病毒的 Magnitude 網站滲透工具

網站滲透測試工具(Exploit Kit)為一種以善意作為出發點所的檢測工具。

該工具納入多種瀏覽器或相關應用程式已知漏洞，並模擬駭客針對漏洞進行攻擊，以判別系統是否存有未修補之弱點。然而，由於該工具知道諸多的系統漏洞，因此也有許多攻擊者透過滲透工具進行惡意攻擊，並非僅使用在檢測方面。不過現在越來越多的瀏覽器及應用程式會在發現漏洞後，自動且立即進行修補作業，導致攻擊者即便使用滲透工具攻擊，也因為漏洞以修補完畢，而無用武之地，因此以滲透測試工具攻擊的模式及類型也大幅減少，已不如過往普遍。

然而，在 2019 年 10 月，卻出現了以 Magnitude 滲透測試工具進行惡意行為之攻擊，該攻擊除了利用漏洞進行入侵等惡意行為之外，甚至大量散播勒索病毒，並且主要針對亞太地區特定國家使用者進行攻擊，包括台灣、南韓及香港。Magnitude EK 其實早在 2013 年就已出現，但當時主要是在地下論壇中提供及使用，直到去年(2019)才被用來進行檯面上且針對亞太地區國家的大規模攻擊。

在透過 Magnitude EK 進行攻擊事件中，其攻擊範圍侷限在使用中文、韓文、馬來西亞語的系統及國家，如果感染的電腦所使用的語言並非上述語系，則勒索病毒將會停止運作。此外，攻擊者更透過新興的安全漏洞進行攻

擊，在 2019 年期間是透過 Internet Explorer 的新漏洞 CVE-2018-8174，在 2020 年則是使用更新的 IE 漏洞 CVE-2019-1367，做為駭侵及散播勒索病毒的主要漏洞。導致諸多未及時更新及修補漏洞的使用者，尤其是仍使用已不會再更新的舊系統/應用程式的使用者，將會受到嚴重的威脅。

因此，為減少類似攻擊事件及勒索病毒所帶來的威脅，除了建議使用者應針對系統或經常使用的應用程式定期更新以修補漏洞外，由於 Windows 在 2015 年所發佈的 Windows 10 中，已經以 Microsoft Edge 取代傳統 IE，因此建議使用者應更新並使用 Windows 10 以上的作業系統，並且盡量不要將 IE 做為預設瀏覽器，而是以仍持續更新及維護的瀏覽器為主，避免攻擊者透過已知的安全漏洞進行攻擊，產生莫大損失。

- 資料來源：

1. https://securelist.com/magnitude-exploit-kit-evolution/97436/。

2.5.8、全新勒贖＋DDoS 惡意軟體，一次攻擊多個漏洞

資安廠商指出，一個名為「Lucifer」的全新惡意軟體，鎖定 Windows 系統大肆傳染中；而且這個惡意軟體會同時鎖定多達 8 個常見資安漏洞進行攻擊。

資安廠商 Palo Alto Networks 旗下的資安研究單位 Unit 42，日前發表研究報告指出，一個名為「Lucifer」的全新惡意軟體，目前正鎖定 Windows 系統大肆傳染中；而且這個惡意軟體會同時鎖定多達 8 個常見資安漏洞進行攻擊。

這個前所未見的惡意軟體，鎖定下列 8 個常見資安漏洞：

- Rejetto HTTP File Server (CVE-2014-6287)
- Oracle Weblogic（CVE-2017-10271）
- ThinkPHP RCE（CVE-2018-20062）
- Apache Struts（CVE-2017-9791）
- Laravel framework（CVE-2019-9081）
- Microsoft Windows（CVE-2017-0144、CVE-2017-1045、CVE-2017-8464）

一旦 Lucifer 成功入侵系統，就會連上駭侵控制伺服器，並且在系統上執行任意程式碼。受駭系統就會變成用來進行 DDoS 攻擊的僵屍網路節點，也會將系統上的檔案進行加密勒贖，以及加密貨幣 XMR 的挖礦程式。

研究人員指出，Lucifer 還會透過多種方式，在區域網路內進行擴散；它會掃瞄系統上的 TCP Port 1433 或用於遠端程序呼叫的 RPC Port 135，並且進行暴力試誤登入。

- 資料來源：
  1. https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/
  2. https://threatpost.com/self-propagating-lucifer-malware-targets-windows-systems/156883/

2.6、軟硬體漏洞資訊

2.6.1、國內網通設備廠商修復存於家用路由器的嚴重資安漏洞

國內網通設備廠商修復存於家用路由器的部份資安漏洞，建議仍在使用不支援安全性更新的網通設備產品用戶，應考慮更換並升級至最新版本軟硬體產品組合。

資安廠商 Palo Alto 網路公司的資安研究團隊 Unit 42，日前公布六個台灣網通設備廠商家用路由器 DIR-865L 的嚴重資安漏洞；除了這款路由器外，其他採用相同程式碼的路由器亦可能出現相同的漏洞。

這六個漏洞分列如下：

CVE-2020-13782：指令中的特殊元素處理不當，可讓駭侵者植入指令

CVE-2020-13786：跨站請求偽造（CSRF）漏洞

CVE-2020-13785：不適當的加密強度

CVE-2020-13784：可預測的亂數產生器

CVE-2020-13783：以明文儲存機敏資訊

CVE-2020-13787：以明文傳輸機敏資訊

這些漏洞本身的危險程度評級，從 7.5 分的「高等級」到 9.8 分的「嚴重」等級，然而資安專家指出，當駭侵者組合利用這些漏洞時，就會增加駭侵風險。

舉例來說，駭侵者可以先利用明文傳輸與儲存機敏資訊的漏洞，設法取得工作階段的 cookie，然後以此存取管理者權限的各項資源，例如內網的檔案分享服務，並藉以植入更多的惡意軟體程式碼，竊取用戶的各種檔案，任意刪改檔案內容，甚至更可把遭駭路由器當做發動 DDoS 攻擊的僵屍網路節點。

該產品公司在接獲通報後，透過發行 beta 版本韌體的方式，修復了其中三個漏洞；該公司在聲明中指出，DIR-865L 是相當老舊的路由器產品，於 2016 年 2 月 1 日就已結束後續的產品支援，所以未來也不會繼續提供支援。

- 建議採取資安強化措施

建議使用老舊且已不支援安全性更新的網通產品用戶，應考慮升級至最新版本的軟硬體產品組合，並維持產品的軟硬體與系統皆處於最新狀態，避免因為無法取得原廠支援而造成資安損失。

- CVE 編號：CVE-2020-13782~13787
- 影響版本：D-Link DIR-865L
- 解決方案：使用廠商提供的部分漏洞修補程式進行更新，或是升級至最新的軟硬體產品組合

- 資料來源：
  1. https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174
  2. https://unit42.paloaltonetworks.com/6-new-d-link-vulnerabilities-found-on-home-routers/
  3. https://www.cyberscoop.com/d-link-home-routers-vulnerabilities-palo-alto-networks/

2.6.2、Cisco WebEx 被發現記憶體傾印資安漏洞

Singtel 旗下的資安廠商 Trustwave，旗下的研究人員於近日發布研究報告，指出廣為全球各大企業使用的視訊會議服務 Cisco WebEx，其 Windows 應用程式存有一個記憶體傾印資安漏洞。

Singtel 旗下的資安廠商 Trustwave，旗下的研究人員於近日發布研究報告，指出廣為全球各大企業使用的視訊會議服務 Cisco WebEx，其 Windows 應用程式存有一個記憶體傾印資安漏洞。

這個資安漏洞發生在 Cisco WebEx 視訊會議的 Windows 客戶端應用程式 40.4.12.8 版本，當用戶安裝好這個應用程式並於背景執行時，只要用戶開始啟動視訊會議，這個常駐程式，就會在磁碟上開啟多個檔案，檔案內容包括當時記憶體內容的傾印（dump）。

然而 Cisco WebEx 並未給與這些檔案足夠的保護措施，使得已登入系統的駭侵者，可以自由存取這些檔案中包含的用戶機敏資訊，例如用戶用以登入 WebEx 視訊會議時使用的 Email 地址，以及會議本身的 URL 等。

更嚴重的是，這些檔案中還會包含用以登入會議內的 WebAccessToken 權杖資訊，任何人只要取得這個 token，就能取得用戶的 WebEx 帳號存取權。

Trustwave 的研究人員在報告中，完整揭露了利用這種手法，於另一台電腦取得 WebEx 帳號存取權的流程。

這個漏洞的 CVSS 危險程度評分為 5.5 分，其危險評級為「中等」。

Cisco 在接獲漏洞通報後，已經在更新版本中修復了這個漏洞；用戶只要更新至 40.6.0 與之後的版本即可。

- CVE 編號：CVE-2020-3347
- 影響版本：Cisco WebEx Windows client 40.4.12.8
- 解決方案：更新至 Cisco WebEx Windows client 40.6.0 與之後版本

- 資料來源：
  1. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cisco-webex-memory-for-the-taking-cve-2020-3347/
  2. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-NBmqM9vt
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3347
  4. https://nvd.nist.gov/vuln/detail/CVE-2020-3347

2.6.3、Zoom 緊急修補 2 個可導致遠端執行任意程式碼的嚴重漏洞

廣受全球遠距會議用戶愛用的 Zoom，近來被發現兩個嚴重資安漏洞，可能導致駭侵者利用此漏洞，遠端執行任意程式碼。。

第一個漏洞編號為 CVE-2020-6109，發生在 Zoom 處理 GIF 圖像時發生的錯誤；駭侵者可傳送一個特製的訊息到欲攻擊的線上會議用戶或群組，並以該用戶當時擁有的權限範圍內，在任意目錄中寫入一個檔案。

駭侵者可以傳送一個以 GIF 副檔名結尾的檔案，但檔案內容實際上是一段可執行的指令碼或 script；駭侵者就可以利用這段偽裝的程式碼來進行駭侵攻擊。

這個漏洞的 CVSS 3.0 危險評分高達 8.5 分。

編號 CVE-2020-6110 的漏洞則和檔案處理的錯誤有關。駭侵者可以發送一段特製訊息給會議室中的個人或群組，並利用這個漏洞在部分特定目錄中寫入一個自我解壓縮的 zip 檔，以執行其他駭侵攻擊活動。

這個漏洞的 CVSS 3.0 危險評分也相當高，達 8.0 分。

兩個漏洞都存於 Zoom 4.6.10 之前的各作業系統版本，另一個漏洞則也存於新一點的 Zoom 4.6.11。

發現這兩個漏洞的，是網通大廠 Cisco 旗下的資安研究團隊 Talos。該單位在發現漏洞後即通報 Zoom 進行修補，目前這兩個漏洞均已在最新版本的

Zoom 中得到解決。

尚未更新至最新版本 Zoom 的用戶，請盡速更新，以避免遭駭侵者利用此二漏洞發動攻擊。

- CVE 編號：CVE-2020-6109、CVE-2020-6110
- 影響版本：Zoom 4.6.11 與先前版本
- 解決方案：更新至 Zoom 最新版本
- 資料來源：
  1. https://blog.talosintelligence.com/2020/06/vuln-spotlight-zoom-code-execution-june-2020.html
  2. https://www.securityweek.com/zoom-patches-two-serious-vulnerabilities-found-cisco-researchers

2.6.4、Firefox 推出最新更新，修補多個加密資料外洩漏洞

廣受歡迎的開放源碼瀏覽器 Mozilla Firefox，近日針對兩個嚴重的資安漏洞，推出安全更新。

這兩個得到更新的資安漏洞，其 CVE 編號分別為 CVE-2020-12410 與 CVE-2020-12411；這兩個漏洞都發生在 Mozilla Firefox 在處理各種記憶體管理與資料加密時發生的記憶體崩潰與緩衝區溢位錯誤，可能導致駭侵者利用此漏洞執行任意程式碼，造成嚴重的資安風險。

CVE-12410 的資安危險程度評分高達 7.5 分，其危險評級為「高」；目前尚未傳出有任何駭侵攻擊行動是基於這兩個漏洞進行。

這兩個漏洞由 Mozilla 開發者 Tom Tung 和 Jarl Tomlinson 發現並提報給 Moziila，在 Firefox 多個版本，包括一般版的 Firefox 76.x 與先前版本、提供企業支援的 Firefox 68.9.0ESR 與先前版本，以及基於 Firefox 68.9.0ESR 的 Tor 私密瀏覽器 9.5，都含有這兩個漏洞。

這次更新另外還修補了多個危險層級較低的資安漏洞與錯誤，仍在使用舊版 Firefox 的用戶，應儘速安裝最新資安更新軟體，以避免因這些漏洞未及時修補而遭不必要的駭侵攻擊。只要透過 Firefox 內建的系統更新機制操作，即可下載並更新至最新版本 Mozilla Firefox。

- CVE 編號：CVE-2020-12410、CVE-2020-12411
- 影響版本：一般版的 Firefox 76.x 與先前版本、提供企業支援的 Firefox 68.9.0ESR 與先前版本，以及基於 Firefox 68.9.0ESR 的 Tor 私密瀏覽器 9.5
- 解決方案：透過 Firefox 內建的系統更新機制，下載並更新至最新版本 Mozilla Firefox

- 資料來源：
  1. https://www.mozilla.org/en-US/security/advisories/mfsa2020-20/
  2. https://nakedsecurity.sophos.com/2020/06/03/firefox-fixes-cryptographic-data-leakage-in-latest-security-update/
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12410

2.6.5、iPhone 0-day 越獄漏洞得到修補

針對被發現且已遭利用的 iOS 嚴重 0-day 漏洞，Apple 立即推出 iOS 小改版升級，以修補此一漏洞。

這個編號為 CVE-2020-9859 的 0-day 漏洞，是在上周公開，且已遭 iOS 裝置越獄軟體 Unc0ver jailbreak 利用來破解各型 iOS 裝置。而在 Apple 發表的 iOS 更新中，已經修補了這個漏洞。

這個漏洞的發生原因，是在系統處理記憶體資料時的問題，可讓駭侵者以核心權限執行任意程式碼。能夠取得核心執行權限，基本上就能在 iOS 系統中為所欲為，駭侵者可用以竊取資訊、攔截並修改程式或資料，當然也能執行更多惡意軟體。

Unc0ver 越獄程式支援的 iOS 版本範圍相當廣，甚至連最新版的 iOS 13.5 都可利用此越獄程式加以破解。

這類越獄程式雖然可讓 iOS 裝置用戶安裝使用各種非官方 App，或是突破 Apple 因為各種商業或資安考量在系統設立的限制，讓越獄用戶更能完全控制其裝置，但這也給駭侵者大開方便之門；駭侵者將能繞過 Apple 原先設計的各種資安關卡，在越獄用戶無法查覺的情形下，於其裝置植入惡意軟體。

Apple 呼籲所有 iOS 裝置用戶，包括 iPhone、iPad、Apple TV、HomePod、Apple Watch 的使用者，都應透過系統更新服務，立即更新到最新版的 iOS 作業系統，以避免因為這個 0-day 漏洞而遭到駭侵攻擊。

- CVE 編號：CVE-2020-9859
- 影響版本： iOS 13.5 以前、iPad OS 13.5 以前、watchOS 6.2.5 以前、tvOS 13.4.5 以前各版
- 解決方案： 透過系統更新服務，升級到最新版本 iOS

- 資料來源：
  1. https://support.apple.com/en-us/HT201222
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9859
  3. https://threatpost.com/apple-jailbreak-zero-day-patch/156201/

第 3 章、 資安研討會及活動

RSA Conference 2020 Asia Pacific & Japan	
活動時間	**2020-07-15**
活動地點	**Virtual Learning**
活動網站	**https://www.rsaconference.com/apj**
活動概要	 **詳細活動相關細節、報名及議程請見官方網站。** **主辦單位：RSA** RSA Conference 2020 Asia Pacific & Japan is happening July 15 – 17 A Free Virtual Learning Experience Connecting with your peers to discuss the latest cybersecurity information is vital to confronting cyberthreats—now more than ever. That's why we're pleased to be able to offer RSA Conference 2020 Asia Pacific & Japan as a free virtual learning experience. From 15–17 July, during Singapore business hours, you'll have access to dozens of timely and relevant sessions covering regional and global cybersecurity issues, networking opportunities, interactive programs and more.

APNIC DNS/DNSSEC online tutorials - part 1	
活動時間	**2020-07-22 13:00 ~ 17:00**
活動地點	**線上研討會**
活動網站	**https://training.apnic.net/events/online-20200722**
活動概要	 **線上研討會活動詳情與報名方式，請見官方網站。** **APNIC 7 月 22-23 日線上舉辦 DNS/DNSSEC online tutorials** Live online: DNS/DNSSEC tutorial – part 1 Start：13:00 - 22 July 2020 End：17:00 - 22 July 2020 Location：East Asia/South East Asia，Time shown in UTC +10.00 Synopsis： The Domain Name System (DNS) is a critical part of Internet infrastructure and the largest distributed Internet directory service. DNS translates names to IP addresses, a required process for web navigation, email delivery, and other Internet functions. However, the DNS infrastructure is not secure enough unless the security mechanisms such as Transaction Signatures (TSIG) and DNS Security Extensions (DNSSEC) are implemented. To guarantee the availability and the secure Internet services, it is important for networking professionals to understand DNS Security concepts, configurations, and operations. APNIC Training Email: training@apnic.net

APNIC DNS/DNSSEC online tutorials - part 2	
活動時間	**2020-07-23 13:00 ~ 17:00**
活動地點	**線上研討會**
活動網站	**https://training.apnic.net/events/online-20200723**
活動概要	 **線上研討會活動詳情與報名方式，請見官方網站。** **APNIC 7 月 22-23 日線上舉辦 DNS/DNSSEC online tutorials** Live online: DNS/DNSSEC tutorial – part 2 Start：13:00 - 23 July 2020 End：17:00 - 23 July 2020 Location：East Asia/South East Asia，Time shown in UTC +10.00 Synopsis： The Domain Name System (DNS) is a critical part of Internet infrastructure and the largest distributed Internet directory service. DNS translates names to IP addresses, a required process for web navigation, email delivery, and other Internet functions. However, the DNS infrastructure is not secure enough unless the security mechanisms such as Transaction Signatures (TSIG) and DNS Security Extensions (DNSSEC) are implemented. To guarantee the availability and the secure Internet services, it is important for networking professionals to understand DNS Security concepts, configurations, and operations. APNIC Training Email: training@apnic.net

CYBERSEC 2020 臺灣資安大會 8/11-12 重磅回歸！	
活動時間	**2020 年 8 月 11-12 日**
活動地點	**南港展覽二館（臺北市南港區經貿二路 2 號）**
活動網站	https://r.itho.me/sec2020
活動概要	 **詳細活動報名及議程請見官方網站。** **主辦單位：iThome** 國際級資安大會 X 超規格資安大展【CYBERSEC 2020 臺灣資安大會】，即將在 8/11-8/12 於南港展覽二館盛大登場！ 匯聚超頂尖資安高手現身說法，提供超過 180 堂資安跨領域、多面向的議程、量身打造最扎實的 CyberLab 實戰演練課程，探討國際最新、最熱門且最全面的資安議題與技術，讓您全方面迎戰資安風險。即刻提升實戰能力。 現場網羅超過 250 家以上業界知名標竿資安品牌，展示 1000+業界最新、最適切的資安產品與服務。平日難以跟進的所有資安產品資訊、市場與發展，都可以在此一次獲得！ 邀請您與我們一同參與這年度資安盛會，與超過 5,000 位菁英進行交流，從技術層面與策略層面，探討資安百種面向、交流技術與知識，讓資安戰場更加壯大，得以更快速地反應、更快速地處理，形成足以跟攻擊者匹敵的更強力防禦。 活動全程免費，請立即報名↘ https://r.itho.me/2020_singup

第 19 屆暨展會亞太資訊安全論壇	
活動時間	**2020 年 9 月 1 日 (二)、9 月 2 日 (三)**
活動地點	**台北市信義區菸廠路 88 號**
活動網站	https://www.informationsecurity.com.tw/event/event_info.aspx?eid=1498
活動概要	 **詳細活動報名及議程請見官方網站。** **主辦單位: 資安人媒體** 參加對象: 政府、金融、醫院、高科技製造業等產業資安、網管、IT、程式等人員 。 參加方式: 全程免費參加 / 報名請務必留下公司 email 及電話。 同期展出: 政府論壇、關鍵資訊基礎、金融論壇、製造業論壇、醫療論壇等專屬研討會。 參加提醒: 請務必攜帶任職公司的個人職務名片前來報到換取會議入場證。 注意事項: 主辦單位享有審核參與人員之權力，同時本活動因須審核產業屬性，恕不接受現場報名。 交通路線: 於捷運板南線國父紀念館站 5 號出口，自光復南路右轉菸廠路，步行約 500 公尺。 活動洽詢: 02-8729-1042 潘小姐 / Iris.Pan@newera.messefrankfurt.com

第 4 章、 2020 年 06 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

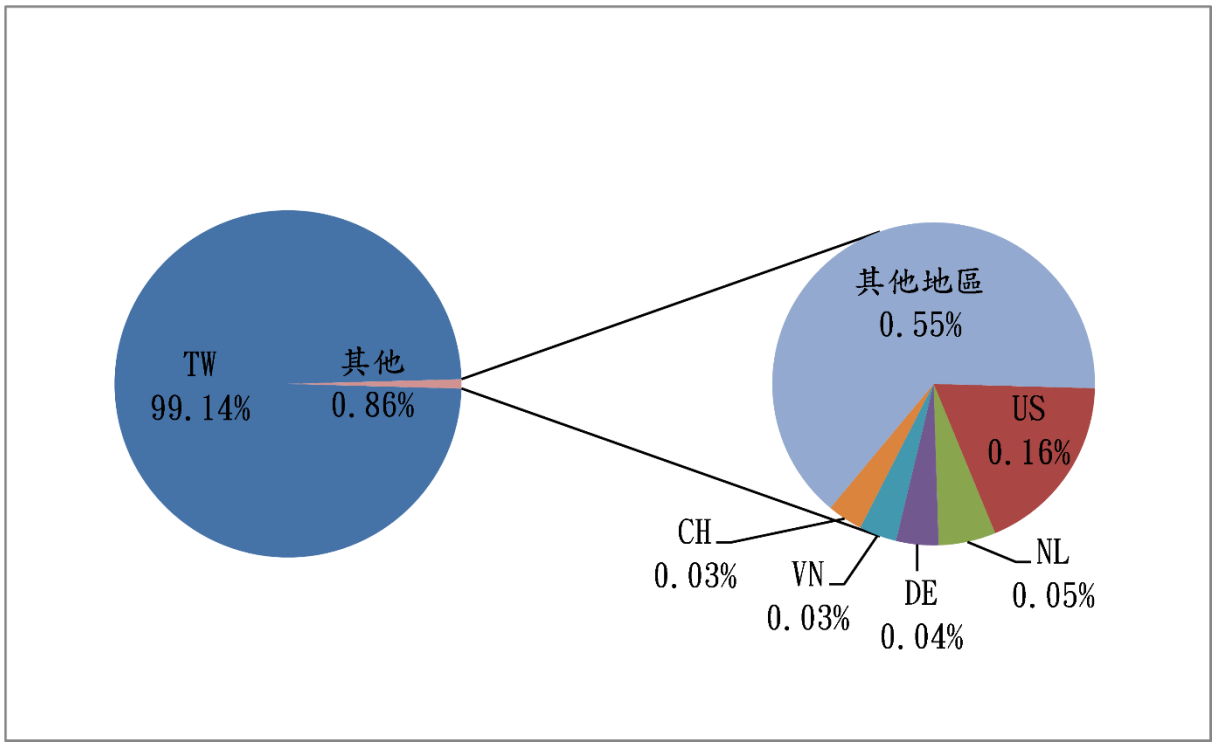


圖 1、分享地區統計圖

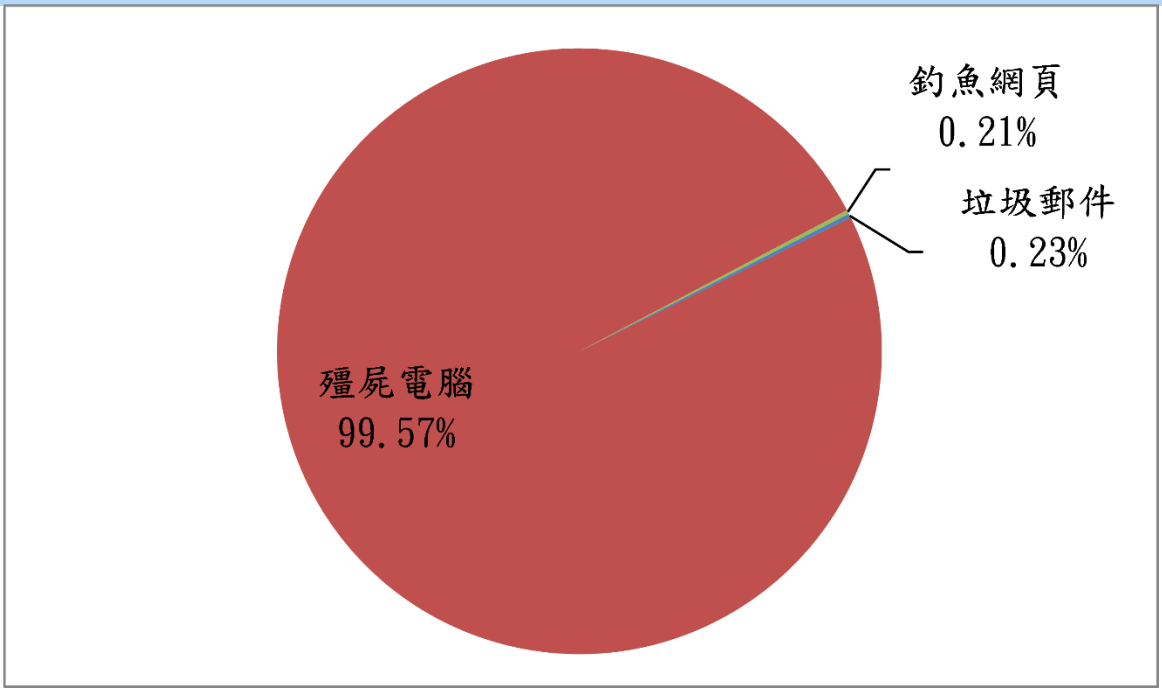


圖 2、分享類型統計圖

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：**2020 年 7 月 10 日**

編輯：**林克容、江奕昉、洪彩馨**

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**http://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**

Twitter：**@TWCERTCC**