TWCERT/CC 資安情資電子報

2020 年 6 月份

目錄

第 1 章、 封面故事

家用路由器遭大規模憑證填充攻擊，建議重新設定密碼

資安專家指出，自 2020 年 3 月起，全球至少有 1200 台 Linksys 家用無線路由器遭到駭侵者以「憑證填充」攻擊得逞；Linksys 鎖定受害用戶的網路管理頁面帳號，以避免遭駭侵者進一步利用。

資安專家指出，自 2020 年 3 月起全球至少發現有 1200 台 Linksys 家用無線路由器，遭到駭侵者以「憑證填充」（credential-stuffing）攻擊得逞。

駭侵者以大量試誤的方式，與網路上取得的已外洩帳密檔案比對，找到受害用戶的路由器管理者可登入帳密後，接著就會修改路由器的 DNS 設定，導致用戶的網路瀏覽封包被挾持並轉向到惡意網站。

駭侵者攻擊的登入帳密，主要是 Linksys Smart WiFi App 服務的登入資訊；用戶可透過此服務管理自己的 Linksys 路由器設備。一但駭侵者取得此服務的帳密，就可以將用戶導向下載安裝一個稱為 Oski infostealer 的惡意軟體，進一步竊取受害者電腦中的各種機敏資訊。

駭侵者主要鎖定一些熱門網域進行 DNS 挾持，例如 Disney.com、Reddit Blog.com、AWS.amazon.com、Cox.net、Washington.edu 等。用戶進入這些網站時，會被導向到一個假冒的武漢肺炎病毒訊息頁面，如果按下畫面中的按鈕，就會被安裝 Oski infostealer 惡意軟體。

為了遏止這波攻擊，Linksys 自 2020 年 4 月起鎖定所有 Linksys Smart Wi Fi app 用戶的網路管理頁面帳號，並要求用戶重新設定密碼，以避免遭駭侵者進一步利用。

→建議採取資安強化措施

1、建議立即重新設定應用程式的密碼，並定期更換密碼。

2、建議使用 12 個字元以上，且為英文、數字與符號混合的密碼，應避免多個系統、網站及應用程式等服務皆使用同一組密碼。

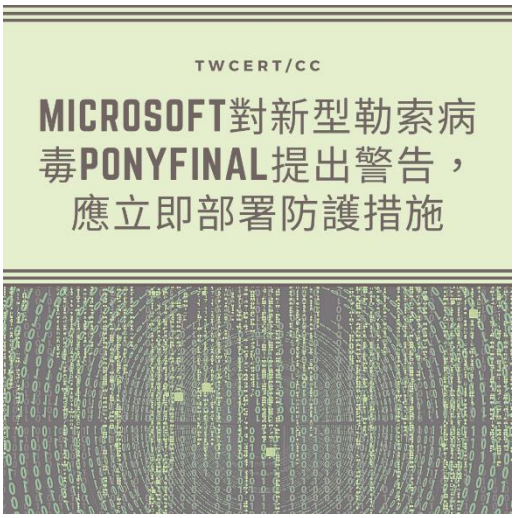
3、定期進行應用程式漏洞更新，安裝防毒軟體與防火牆，確保系統、設備與應用程式處於最新版本，避免受到駭客攻擊而造成損失。

- 資料來源：
  1. https://www.linksys.com/us/support-article?articleNum=317063
  2. https://www.linksys.com/us/support-article/?articleNum=246427
  3. https://threatpost.com/attacks-on-linksys-routers-trigger-mass-password-reset/154914/

第 2 章、 國內外重要資安事件

2.1、資安趨勢

2.1.1、Microsoft 對新型勒索病毒 PonyFinal 提出警告，應立即部署防護措施



Microsoft 針對近兩個月氾濫之勒索病毒 PonyFinal，提出嚴正警告，企業及組織都應立即部署相關防護措施，避免成為新型勒索病毒的受害者。

根據 Microsoft 的安全團隊於 Twitter 中一系列的貼文，近兩個月內，有一款名為 PonyFinal 的基於 Java 之新 Human-Operated 勒索病毒逐漸氾濫。此勒索病毒主要是倚靠人為攻擊者突破企業的網路，並且搜集企業系統及主機的資訊後，針對個別主機之架構或環境，進行最有效率的勒索病毒感染及配置。此種模式導致受害主機除了會遭受勒索之外，更可能有其他惡意程式或機敏資料外洩的威脅，並且透過長時間的隱藏和觀察，可在最佳的時間點感染受害主機後進行惡意行為。

為達到針對企業散播勒索病毒之目標，攻擊者會透過對目標企業伺服器以暴力破解方式，取得存取權限，並且於伺服器中部署一個 Visual Basic 腳本，運行後竊取其中的資料。此外，該病毒更部署了遠程控制系統(Remote Manipulator System)，以避開系統日誌(Log)的紀錄，以及清除相關事件日誌，減少被追查的風險。而此勒索病毒由於是以 Java 進行編寫，因此會透過竊取

的資訊或觀察等方式，針對有安裝 Java Runtime Environment (JRE)的主機進行攻擊，然而，微軟卻也有偵測到鮮少的狀況下，會替目標主機安裝 JRE 後，再進行勒索病毒的部署和執行。

此攻擊會先藉由植入一包括兩個批次檔與一勒索病毒的 MSI 檔，並在特定日期及特定時間對目標檔案進行加密。首先透過第一個批次檔 UVNC_Install.bat 產生工作排程來執行第二個批次檔 RunTask.bat。此檔案會進一步執行 PonyFinal 勒索軟體，並將加密檔案加入.enc 的副檔名，並且會產生一名為 README_files.txt 的文字檔案，裡面主要是說明如何支付贖金及相關訊息，要求受害者支付 300 比特幣。 一旦攻擊者收到款項後，會立即傳送金鑰給受害者進行解密。並且由於該勒索病毒較為新興且使用足夠強的加密方式，截至截稿為止，都尚未有針對 PonyFinal 的解密程式可解除勒索病毒的威脅。

勒索軟體識別網站 ID-Ransomware 表示，PonyFinal 最早是於 2020 年初首次被發現，截至目前的受害者不多，代表攻擊者應是有慎選攻擊目標後，才進行後續惡意行為。並且根據上傳 PonyFinal 樣本使用者的分析，顯示目前主要受害者的地理位置均位於印度、伊朗以及美國。

- 資料來源：
  1. https://twitter.com/MsftSecIntel/status/1265674287404343297
  2. https://www.zdnet.com/article/microsoft-warns-about-attacks-with-the-ponyfinal-ransomware/
  3. https://www.darkreading.com/attacks-breaches/microsoft-shares-ponyfinal-threat-data-warns-of-delivery-tactics/d/d-id/1337919

2.1.2、巴基斯坦三家電信業者，遭駭侵團體 Greenbug 長期竊聽

資安廠商指出，一個名為「綠臭蟲」（Greenbug）的駭侵組織，近來被發現長期駭入巴基斯坦三家電信業者的主機中，進行資料竊取與監聽活動。

資安廠商賽門鐵克（Symantec）日前發表研究報告，指出一個名為「綠臭蟲」（Greenbug）的駭侵組織，近來被發現長期駭入巴基斯坦至少三家電信業者的主機中進行資料竊取與監聽活動。

賽門鐵克說，這個綠臭蟲駭侵團體，利用虛擬「通道」長期和受害電信業者中的某些遭駭主機連線，持續不斷從這些業者中竊取各種機敏資訊。

賽門鐵克指出，Greenbug 混合利用市面上現成的各種攻擊工具，以及「離地攻擊」（Living-of-the-land）手法，以資料庫主機為主要的攻擊目標；先試圖竊取登入這些主機的帳密組合，接著再嘗試登入，以控制受害主機。

在報告中，賽克鐵克認為 Greenbug 和伊朗有關，也可能是過去造成極大破壞的 Shamoon 駭侵團體的分支。Shamoon 曾經在沙烏地阿拉伯的某些目標，發動清空儲存裝置以破壞資料的攻擊行動。

但賽門鐵克也說，目前尚未發現 Greenbug 利用何種管道入侵受害系統，只知道他們從去年十月就開始鎖定攻擊目標；其中一家電信業者的某台主機，被駭侵者透過內建的 Powershell 界面下了一些攻擊用的指令，安裝了一個稱為 CobaltStrike Beacon 的模組，以進行第二階段的駭侵攻擊；更被用來

在該公司的內部網路中尋找目標，建立攻擊行動控制伺服器。

- 資料來源：
  1. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia
  2. https://www.cyberscoop.com/greenbug-symantec-iran-hacking-pakistan。

2.1.3、企業遭勒索病毒駭侵，建議提升員工資安意識

近期勒索病毒事件頻傳，發生多起企業遭駭客攻擊事件，導致感染勒索病毒而造成損害。

提醒大家須留意不明郵件、不隨意點擊可疑連結與檔案，並確保所有作業系統與軟體完成安全性更新，及時修補漏洞。

企業發生資安事件並造成實際損害的大部分原因，是遭受社交工程攻擊。常見的社交工程是駭客散布含有惡意程式的釣魚郵件，利用聳動的標題或內容，促使受害者點擊惡意連結或附檔，導致無意間洩漏個資、公司機密或是被駭客植入惡意軟體。社交工程還包含網路釣魚、USB 或 CD 儲存媒體暗藏惡意程式、偽裝成知名程式的惡意程式，以及透過社群媒體散播惡意程式等方式進行攻擊。

提高資安警覺，當收到電子郵件時，務必對寄件人身分進行確認，在未確認寄件人身分之前或是針對標題及內容可疑的郵件，不隨意打開郵件、不點擊或下載郵件中的任何連結與夾帶的附檔。進入可疑網站不輸入帳密和個資，即使看起來像官方網站，也務必要確認網址的正確性，避免到駭客建立的釣魚網站。員工也應避免在公司使用自己的外接硬碟設備，如 USB 隨身碟，以免受感染的設備感染公司電腦，造成更嚴重的擴大感染。

而企業內部網路，建議可藉由分段隔離來減少損害程度、提升各網段間的安全性。即使特定網段遭駭客入侵攻擊，也無法滲透感染到所有系統，不會使企業所有的電腦系統處於癱瘓狀態。此外，企業應定期對員工進行社交工程演練，落實資安宣導及舉辦資安教育訓練，提升員工的資安意識

不論個人或企業都應安裝防毒軟體及防火牆，定期更新電腦系統與軟體，確保設備軟體皆處於最新版本，防範駭客利用資安漏洞進行攻擊而造成重大損失。

- 資料來源：

1. https://www.us-cert.gov/ncas/tips/ST04-014
2. https://www.nomoreransom.org/zht_Hant/index.html
3. https://www.twcert.org.tw/tw/cp-104-3429-85df7-1.html
4. https://www.bnext.com.tw/article/57547/cpc-hack-ransomware
5. https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/0037B4A129E44701B19DE38807050098。

2.1.4、全球 RDP 暴力攻擊次數近來激增

資安廠商指出，在世界各國都觀察到針對 Windows RDP 進行暴力嘗試法攻擊的次數，於疫情大流行期間激增數倍。

俄國資安廠商卡巴斯基日前發布研究報告指出，該公司的研究人員在世界各國都觀察到針對 Windows RDP 進行暴力嘗試法攻擊的次數，於疫情大流行期間，以數倍的規模激增。

Windows RDP 是微軟 WIndows 工作站、伺服器使用的專有應用層連線協定，可用以遠端遙控操作；駭侵者利用暴力試誤法猜測受害者使用的可能登入資訊，不論是純以亂數猜測，或參考字典檔，甚至是透過已經外洩的該用戶其他帳號登入資訊，只要被駭侵者猜到了，系統就極可能遭到駭入。

卡巴斯基觀察到，在諸多因為疫情而封城、民眾必須在家工作的國家，這類針對 Windows RDP 進行的暴力試誤駭侵攻擊的上升幅度也愈大。

以美國為例，在疫情尚未爆發的二月初，每日觀察到的 RDP 暴力攻擊次數約為二十萬次上下；到了四月初則暴增至七倍，每日高達一百四十萬次。

同樣的情形也出現在德國，二月初這類攻擊每日愈觀測到十萬次，四月中旬則高達八十萬次；俄羅斯則是從二十萬次以下增加到近一百萬次，也有五六倍的成長。

卡巴斯基建議，企業的 IT 人員應確實做好 Windows RDP 連線的資安防

護設定，例如使用高強度密碼、僅容許 RDP 透過企業自有 VPN 連線、啟用二階段登入驗證等。如果不使用 Windows RDP，一定要封鎖 Port 3389 的連線。

另外企業也應對在家上班的員工，提供充分的資安宣導、培訓課程與技術支援，而且要及時更新各種應用軟體與作業系統，同時提供完善的備份機制。

- 資料來源：
  1. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/
  2. https://www.bleepingcomputer.com/news/security/rdp-brute-force-attacks-are-skyrocketing-due-to-remote-working/

2.1.5、英國廉航公司 EasyJet 遭駭，九百萬顧客個資被竊

英國廉價航空公司易捷航空（EasyJet）發生駭侵事件，有超過九百萬名顧客的個資恐遭駭客竊取。

英國廉價航空公司易捷航空（EasyJet）日前傳出駭侵事件。本周二該公司發布通告，指出有超過九百萬名顧客的個資恐遭駭客竊取。

這九百萬名顧客被竊的資料，包括 Email 地址與旅程細節等資訊，但不包括護照資料在內；其中有兩千多人的信用卡詳細資料，也在這次駭侵事件中一同被竊走。

該公司表示，已經和這兩千多名信用卡資料遭竊的顧客連繫，其他個資被竊的顧客會在五月二十六日前完成連繫。

信用卡資料被竊的顧客，料將面臨盜刷或其他金融詐騙的風險；而資料被竊的用戶，也能會成為駭侵者進一步發動釣魚或各式詐騙活動的目標。

該公司目前正在調查這起駭侵事件，但並未對外透露細節，僅表示駭侵使用的手法十分細緻，目前也無法得知是誰發動這次攻擊行動，也不知道攻擊是透過何種方式與手段進行。

該公司也已經向英國當局主管資安事務的國家資安中心（National Cyber Security Centre）與英國資訊專員辦公室（The Information Commissioner’ s Office）等單位通報此起資安事件。

一般預料該公司將會因此資安事件，遭主管單位重罰。英國航空於 2019 年七月時木發生過 50 萬名顧客資料遭竊的資安事件，遭到重罰一億八千三百萬英磅；同一時間萬豪酒店集團也因全球三億四千萬名顧客資料被竊，遭罰近一億英磅。

- 資料來源：
  1. http://otp.investis.com/clients/uk/easyjet1/rns/regulatory-story.aspx?cid=2&newsid=1391756
  2. https://www.theverge.com/2020/5/19/21263431/easyjet-hack-customer-details-email-addresses-credit-cards
  3. https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card

2.1.6、國內能源石化與資通產業連續遭駭侵攻擊

國內多家企業連續傳出遭惡意軟體攻擊事件，疑似駭侵團體發動目標式勒索病毒。

近期國內石化能源產業與資訊通訊製造業者等多家企業，傳出連續遭駭侵者以勒贖軟體攻擊事件，造成營運及商譽損失。

首先是一間石化能源產業傳出遭到勒贖軟體攻擊，包括官方網站、營業據點的部分系統，以及部分服務遭到阻斷無法使用；經緊急斷網處理並且啟動備份回復機制後，其官網與大多數營業據點均已恢復正常營運。

隔日，另一間石化能源產業也傳出遭駭侵攻擊事件，發現公司部分電腦設備出現異常；該公司關閉所有電腦並且斷網進行內部清查，於當天逐漸恢復正常，而其營業據點則仍維持正常運作。

同日一間屬於資通產業的企業也傳出災情，旗下某廠的部分伺服器亦遭勒贖軟體駭侵攻擊；該公司同樣採取斷網隔離作業，並回復受損資料，整體損失與對生產作業的影響有限。

遭受駭侵攻擊的石化能源產業，若屬於資通安全法中指定的關鍵基礎設施，在確認遭駭侵攻擊後，都已立即通報資安事件，政府也啟動相關的調查程序。

→建議採取資安強化措施

1、檢視 AD(Active Directory) 伺服器權限及帳密，避免駭客入侵電腦後，設定群組原則，導致勒索病毒檔案被下載並在受影響網域內的電腦上執行。

2、提高資安警覺，不開啟標題及內容可疑或聳動的電子郵件，不點擊其提供的任何連結與附加檔案，收到電子郵件的當下務必先確認寄件人的身分。

3、提防進入釣魚網站，即使看起來像官網也要確認網址的正確性，進到可疑網站不輸入個資與金融資訊，建議可以手動鍵入網址或是搭配網址識別套件防範釣魚網站。

4、避免在公司使用私人的外接硬碟設備，以免受感染的設備擴大感染公司的所有系統設備。

5、企業內部網路建議可藉由分段隔離來減少損害程度、提升各網段間的安全性，並定期將資料備份以減少損失。

6、落實資安宣導，定期舉辦資安教育訓練及社交工程演練，提高員工資安意識。

7、安裝防毒軟體及防火牆，定期更新軟體、作業系統與應用程式，防止駭客利用資安漏洞進行駭侵攻擊。

8、定期多重備份檔案於不同設備，並異地儲存一個備份。

- 資料來源：

1. https://www.cpc.com.tw/News_Content.aspx?n=28&sms=8920&s=4947
2. https://blog.trendmicro.com.tw/?p=64227
3. https://www.twcert.org.tw/tw/cp-104-3600-a5ce6-1.html
4. https://www.us-cert.gov/ncas/tips/ST04-014

5. https://www.nomoreransom.org/zht_Hant/index.html
6. https://www.bnext.com.tw/article/57547/cpc-hack-ransomware
7. https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/0037B4A129E44701B19DE38807050098

2.1.7、資安廠商揭露駭侵者針對工業 4.0 的攻擊手法

資安廠商趨勢科技發表研究報告，指出駭侵者可能已經發展出針對製造業採用工業 4.0 架構的工廠的攻擊手法。

資安廠商趨勢科技發表研究報告，指出駭侵者可能已經發展出針對製造業採用工業 4.0 架構的工廠的全新攻擊手法，即使是處在隔離境中的製造設備，也可能遭受攻擊。

報告指出，一般傳統攻擊方式，如使用惡意程式等的攻擊手法，通常會被已經相當普及的網路防護措施阻擋下來；但該公司和米蘭理工大學合作研究，在該校實驗室與知名大型製造業的設備上，實際模擬出駭侵者可能的攻擊流程。

報告說，工業 4.0 整體架構中的弱點，就是在用來操控各項設備與系統的節點上；雖然大多數工業 4.0 的實際設備可以架設於隔離的內網，但操作節點往往必須與外部公眾網路連接。這就給駭侵者可乘之機。

報告指出，多數製造業採用的設備，已經具備傳統 IT 系統的運算效能；這些多餘效能很可能會被駭侵者利用來執行惡意程式碼，而不被企業發覺。

再者，由於多數設備因為處於內網，其安全主要仰賴環境的隔離，設備本身並不具備較強的資安防護能力，因此只要節點遭到駭入，就有可能導致駭侵者長驅直入，導致設備故障、資料遭竊、生產受到影響等問題。

這份報告也建議所有採用工業 4.0 架構的製造業者，對於這些較脆弱的控制節點，如製造執行系統（MES）、人機界面（HMI）、各種客製化的 IIoT 設備，都應加強資安防護，以避免遭到駭侵突破，成為資安防護破口。

- 資料來源：
  1. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-consequences-a-security-analysis-of-smart-manufacturing-systems
  2. https://www.businesswire.com/news/home/20200511005054/en/Trend-Micro-Research-Identifies-Critical-Industry-4.0

2.1.8、駭侵者以肺炎為名，透過魚叉式網路釣魚，散布惡意 Excel 檔

微軟資安研究團隊指出，觀測到有駭侵者利用主題為肺炎大流行資訊的魚叉式釣魚信件，散播內含遠端遙控工具的惡意 Excel 檔。

微軟資安研究團隊日前指出，該團隊觀測到五月上旬開始有駭侵者，利用主題為肺炎大流行資訊的魚叉式釣魚信件，散播內含遠端遙控工具的惡意 Excel 檔。

微軟說，駭侵者將信件偽造為寄自約翰霍普金斯大學的疫病相關研究單位，信件標題為「世界衛生組織 COVID-19 疫情報告」（WHO COVID-19 SITUATION REPORT），用以取信被害人。

在這封魚叉釣魚郵件中夾帶的惡意 Excel 檔，名稱為「covid_usa_nyt_8702.xls」，屬於 Excel 4.0 格式；打開後會看到一個安全提問訊息；如果用戶同意的話，就會自網路上下載一個巨集程式，同時執行內含的 RAT 遠端遙控工具。

雖然這個稱為 NetSupport Manager 的 RAT 遠端遙控工具，本身並非惡意軟體，而是系統管理者經常用來遠端控機其他主機的常用軟體，但過去經常傳出該工具被駭侵者惡意運用的案例。

以這個案例來說，一旦成功執行巨集中的 NetSupport，駭侵者就會在受害系統中植入多個 .dll、.ini、.exe 等程式，同時安裝一個 VBScript，再透過 P

owerSploit 連線到一台駭侵攻擊使用的控制伺服器。

- 資料來源：
  1. https://twitter.com/MsftSecIntel/status/1262504864694726656
  2. https://www.centerforhealthsecurity.org
  3. https://threatpost.com/coronavirus-emails-netsupport-rat-microsoft/156026/

2.1.9、駭侵團體於暗網大量散布竊取自 11 家公司的資料

資安媒體和廠商發現，近來有駭侵團體於暗網上連續散布竊取自 11 家公司的用戶資料，並且公開求售。

資安媒體與廠商發現，近來有一個名為「放閃獵人」（ Shiny Hunters ）的 駭侵團體，於暗網上連續散布竊取自 11 家公司的用戶資料，並且公開求售。

被陸續公開遭竊資料的公司，包括印尼最大的線上零售業者 Tokopedia，有過九千一百萬筆用戶資料遭到公開，印度最大級線上教學平台 Unacademy 也有兩千兩百萬筆用戶資料被竊；甚至連微軟旗下的開源專案平台 GitHub，也有部分只限內部員工存取的檔案被拿出來公開。

另外，諸如食材訂購服務商 HomeChef、線上相片印製商 ChatBooks、提供高等教育情報服務的 Chronicle.com，也都各自有數百萬筆用戶資料遭到該組織於暗網公開販售。

到目前為止，全部 11 家公司有超過一千萬筆資料被待價而沽，其中 Tokopedia 的九千一百萬筆資料「報價」為五千美元，HomeChef 的八百萬筆資料則要價 2,500 美元。

資安媒體 BleepComupting 取得部分外洩資料加以分析，認為這批資料確實來自被竊公司的可能性很高，但無法 100% 確認；Bleeping Computing 洽詢了這些資料遭竊的公司，但尚未有任何公司提供回饋。

目前 Unacademy 和 ChatBooks 已針對資料遭竊事件，向可能受影響的用戶發送資安通報，說明資料遭竊的情形與處理措施。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/hacker-group-floods-dark-web-with-data-stolen-from-11-companies/
  2. https://securityaffairs.co/wordpress/103003/cyber-crime/shiny-hunters-dark-web.html

2.2、國際政府組織資安資訊

2.2.1、印尼近 230 萬選民資料，遭駭侵團體曝光

印尼選委會表示，該國有近 230 萬名選民的個資，遭駭侵團體於其網站公開；駭侵團體更威脅將公開更多選民資料。

負責印尼大小選舉事務的印尼選舉委員會，於上周五公布資安通報，指出有駭侵團體於其網站，公布近 230 萬名印尼選民的個資；其檔案大小高達 2.36GB。

這批資料是在上周三公布在一個專門討論駭侵相關議題的論壇上，印尼選委會隨後證實這批資料的正確性，並表示部分資料可追溯到 2013 年。資安專家指出，這些個資足以讓受害者面臨後續的詐騙或其他駭侵風險。

印尼選委會否認該批資料係直接自該單位所屬的伺服器中竊得。印尼法律規定，這類選務資料須分享給各政黨與總統候選人，因此有可能是從其他來源外洩。

竊取該批選民資料的駭侵團體，並未自行透露身分，但除了公布這批 230 萬人的個資外，還在該論壇留言，表示將在近期公開另外兩億名印尼選民的個資。

以去年為準，印尼共有一億九千兩百萬名選民，有資格在中央和地方選舉中投票。

印尼最近頻頻傳出個資竊取事件，五月初印尼主要的電子商務平台 Tokopedia 剛發生大規模個資遭竊事件，有九千一百萬名客戶的個資遭駭侵團體竊走。

印尼公民團體十分憂心這類事件一再發生，顯示印尼政府和民間單位的資安防護過於薄弱。

印尼選委會目前已經開始調查整個駭侵案件的來龍去脈，但公民團體認為這麼大量的選民個人資料，應享有更強大的防護措施。

- 資料來源：
  1. https://www.hackread.com/hacker-leaks-indonesian-citizenship-voter-data-for-download/
  2. https://www.reuters.com/article/us-indonesia-cyber-breach/indonesia-probes-breach-of-data-on-more-than-two-million-voters-idUSKBN22Y15K

2.2.2、部分國家軍隊內部網路，可能遭駭侵團體以 USB 惡意軟體攻擊並竊取資料

資安廠商指出，觀測到某駭侵團體以寄生於 USB 儲存裝置的惡意軟體，竊取與公眾網路相互隔離的軍隊內網資料。

資安廠商趨勢科技，日前發表研究報告指出，該公司觀測到某駭侵團體，以寄生於 USB 儲存裝置的惡意軟體，竊取與公眾網路相互隔離的軍隊內網資料，且受害時間可能長達六年之久。

在這份報告中提及的惡意軟體，名為 USBFerry，感染系統後，不但會試圖自我複製到其他日後插到系統上的 USB 儲存裝置，例如 USB 隨身碟或 USB 外接硬碟，還會竊取 USB 儲存裝置中的檔案和資料，並在下次該裝置插上具備 Internet 連線的電腦時，將竊得的資料傳送出去。

透過這種方式，駭侵者即可入侵未連接公眾 Internet 的重要機關內網，並竊得所需的機密檔案與資料。

趨勢公司指出，該公司自 2018 年起開始追蹤 USBFerry 的活動，發現該惡意軟體自 2014 年起就十分活躍，攻擊時間長達六年之久。

該公司也說，發動這類攻擊的駭侵組織「Tropic Tropper」也知道這些重要機關的內網有多重防護措施：除了與外網隔開外，還有例如生物特徵辨識、加密傳輸等，所以該組織會先攻擊這些單位的外圍組織，因為這些外圍組織的防護通常比較鬆散，再伺機攻入主要目標。

趨勢科技說，他們觀察到的攻擊成功案例，就是先駭入軍方所屬醫院的系統，接著再駭入軍隊的隔離內網。

- 資料來源：
  1. https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf
  2. https://www.zdnet.com/article/hackers-target-the-air-gapped-networks-of-the-taiwanese-and-philippine-military/

2.3、社群媒體資安近況

五億 Facebook 用戶個資檔案，遭駭侵者以三萬美元求售

資安媒體揭露某駭侵者於駭侵相關論壇上，以三萬美元價格兜售大批 Facebook 用戶個資，據稱受駭用戶人數高達五億人。

資安媒體 HackRead.com 獨家報導指出，某駭侵者於一個惡名昭彰的駭侵相關論壇上，以三萬美元價格兜售大批 Facebook 用戶個資；據稱受駭用戶人數高達五億人。

據該媒體報導，駭侵者於本月 12 日開始在論壇上出售這批個資。駭侵者宣稱資料收集自 82 個不同國家，其中包括台灣在內。

這批臉書用戶個資的資料欄位相當完整，包括用戶名稱、性別、所在地點、城市名稱、姓氏、職業、婚姻狀態、手機號碼、Emal 地址和臉書個人檔案頁面網址等。

以下是駭客宣稱這批資料中來自主要國家臉書的用戶人數：

- 阿根廷：230 萬人
- 奧地利：730 萬人
- 孟加拉：380 萬人
- 加拿大：340 萬人

- 智利：680 萬人
- 中國：67 萬人
- 哥倫比亞：1790 萬人
- 捷克：130 萬人
- 埃及：4480 萬人
- 法國：1980 萬人
- 香港：290 萬人
- 印度：610 萬人
- 伊拉克：1700 萬人
- 義大利：3560 萬人
- 日本：42 萬人
- 約旦：310 萬人
- 科威特：446 萬人
- 墨西哥：1330 萬人
- 荷蘭：540 萬人
- 摩洛哥：1890 萬人
- 奈及利亞：1163 萬人
- 阿曼：500 萬人
- 俄國：990 萬人
- 沙烏地阿拉伯：2880 萬人
- 新加坡：300 萬人
- 南非：1430 萬人

◎ 西班牙：1080 萬人

◎ 蘇丹：940 萬人

◎ 敘利亞：690 萬人

◎ 台灣：73 萬人

◎ 突尼西亞：1950 萬人

◎ 阿聯：690 萬人

◎ 英國：1150 萬人

◎ 葉門：720 萬人

駭侵者還把這一大包資料切成三種不同包裝方式，以不同價格標示；例如一百萬名個資為美金 1500 元，十萬名為 450 美元，整個五億人的完整資料為三萬美元。

駭侵者也表示，資料取得期間是自 2019 年 11 月，到 2020 年 5 月之間。而據 Hackread.com 的分析，該媒體認為資料可能取自某家行銷公司未受適當保護的線上資料庫。

- 資料來源：
  1. https://www.hackread.com/hacker-selling-500-million-facebook-user-data/

2.4、行動裝置資安訊息

2.4.1、Google 自 Play Store 中下架 813 個「偷窺軟體」

在一份針對 Android 平台上的「偷窺軟體」研究報表發表後，Google 隨即自 Play Store 中下架多達 813 個偷窺軟體。

在一份由 NortonLifeLock Research Group、康乃爾科技大學與紐約大學合組的研究團對，針對 Android 平台上的「偷窺軟體」研究報表發表後，Google 隨即自 Play Store 中下架多達 813 個偷窺軟體。

這份研究報告名為「偷窺軟體（Creepware）進行人與人之間攻擊的各種樣態」（The Many Kinds of Creepware Used for Interpersonal Attacks），論文所指的「偷窺軟體」（Creepware），其定義是不像間諜軟體（Spyware）或跟蹤軟體（Stalkerware）那樣擁有完整惡意功能，但仍可對用戶進行跟蹤、騷擾、詐騙、威脅等惡意行為的軟體。

在論文中，研究者先提出一套稱為「偷窺指數」（CreepRank）的計量演算法，以這套演算法來評估各個偷窺軟體的行為與其損害程度，然後為每支偷窺軟體計分。被列入計分標準的惡意行為，包括竊取手機的簡訊或即時傳訊軟體對話內容、假冒其他用戶身分、發動 DDoS 攻擊、隱匿其他 App、控制其他 App、監控手機所在地座標資等。

接著研究團隊以此指標，從超過五千萬支 Android 手機的匿名使用資料中進行分析，最後找出多達 857 支 Android App，其偷窺指數高到可以算是偷窺軟體；其中有 114 支 App 會進行假冒詐騙、80 支 App 會騷擾使用者， 63 支 App 會進行其它駭侵攻擊。

研究團隊也指出，全球有超過一百萬支以上 Android 手機，都安裝過這些偷窺軟體。

去年夏季，研究團隊將這份偷窺軟體名單交給 Google，Google 隨即認可 CreepRank 的有效性，而且自 Play Store 中下架了 813 個名單上的偷窺軟體。

- 資料來源：
  1. http://damonmccoy.com/papers/Creepware_SP.pdf
  2. https://www.zdnet.com/article/google-removed-813-creepware-apps-from-the-android-play-store/

2.4.2、泰國 Android 用戶遭 WolfRAT 鎖定，攻擊熱門聊天 App 以竊取資訊

資安廠商指出，一個名為 WolfRAT 的惡意軟體，現正鎖定泰國的 Android 用戶進行大規模攻擊，竊取用戶在熱門聊天 App 中的對談記錄與各種資訊。

資安廠商 Cisco Talos 的研究人員近日發表研究報告，指出有一個名為 WolfRAT 的惡意軟體，現正鎖定泰國的 Android 用戶進行大規模攻擊；用戶一旦不慎安裝含有 WolfRAT 的 App，App 內含的惡意程式碼，就會在背景中竊取用戶於熱門聊天 App 中的對談記錄與各種資訊。

這個 WolfRAT 惡意軟體，目前仍在積極發展中；研究人員指出它會暗藏於偽裝成一般正常的 App 內，一般不那麼熟悉資安議題的用戶，很難光從 Google Play Store 中的訊息判斷其是否為安全的應用程式，甚至會以為這些惡意 App 是 Android 作業系統的必備程式。

一旦用戶下載後，WolfRAT 便會開始竊取用戶在常用聊天軟體如 WhatsApp、Facebook Messenger 中的對話記錄、用戶名單、簡訊通聯記錄等機敏資訊。

研究人員表示，他們也觀察到 WolfRAT 開始針對 LINE 在東南亞的廣大用戶群發動攻擊；即使用戶開啟更強的端到端加密通訊，也還是處在被 WolfRAT 監聽的風險之下。

研究人員說，他們認為 WolfRAT 很可能是由德國境內的惡意軟體開發團隊 Wolf Research 主導開發工作，並透過釣魚郵件或垃圾訊息中的連結來散布，例如在泰國找到的一個惡意軟體控制伺服器，其外顯的內容就是和泰國美食有關。

- 資料來源：
  1. https://blog.talosintelligence.com/2020/05/the-wolf-is-back.html
  2. https://www.cisomag.com/new-android-malware-wolfrat-targets-whatsapp-facebook-messenger-and-other-android-apps/
  3. https://threatpost.com/wolfrat-android-malware-whatsapp-facebook-messenger/155809/

2.5、軟體系統資安議題

2.5.1、Thunderbolt 3 漏洞無法修復，加密資料可能遭竊

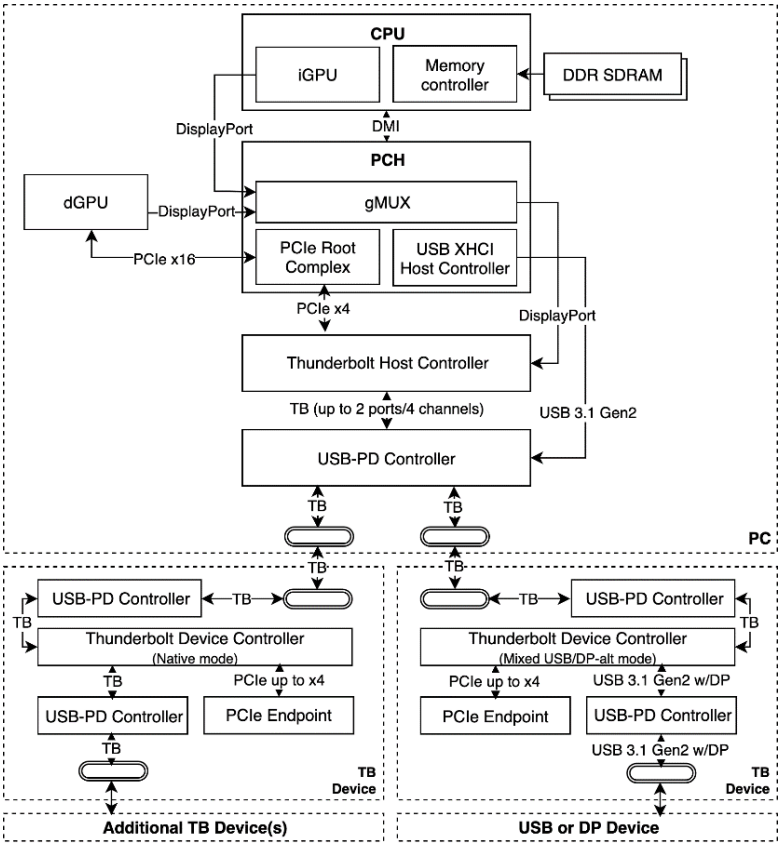
荷蘭安荷芬科技大學（Technische Universiteit Eindhoven）的研究人員 Björn Ruytenberg，日前發表研究報告指出，廣泛內建於高階主機和筆記型電腦的高速傳輸界面 Thunderbolt 3 存在嚴重的硬體安全漏洞，允許駭侵者能輕易地於數分鐘內，破解電腦安全加密並竊取使用者資料。

根據該研究人員於 2020 年 4 月的研究報告，藉由 Thunderbolt 3 直接存取系統記憶體（Direct Memory Access）的機制，即使使用者電腦已設定登入安全措施，或設定硬碟加密，駭侵者仍能於五分鐘內竊取電腦的資料及存取權。

由於該漏洞存在於 Thunderbolt 3 硬體中，在所有 2019 年以前所生產的電腦設備上，該漏洞均無法被修復，而 2019 年後出廠的電腦當中，也有部分設備存在該漏洞。根據 Intel 和 Microsoft 的聲明，使用者須啟用 Windows 10 中的「內核 DMA 保護」功能才能降低受侵駭的風險。而生產於 2019 年以前，硬體上不支援「內核 DMA 保護」的電腦設備，研究人員則建議將 Thunderbolt 3 介面永久停用。

在研究人員的測試中，僅有部分於 2019 年以後生產的 HP 和 Lenovo 設備有內建相對應的保護措施，並且在 Windows 和 Linux 系統上受危害的程度將大於使用 macOS 的電腦設備。

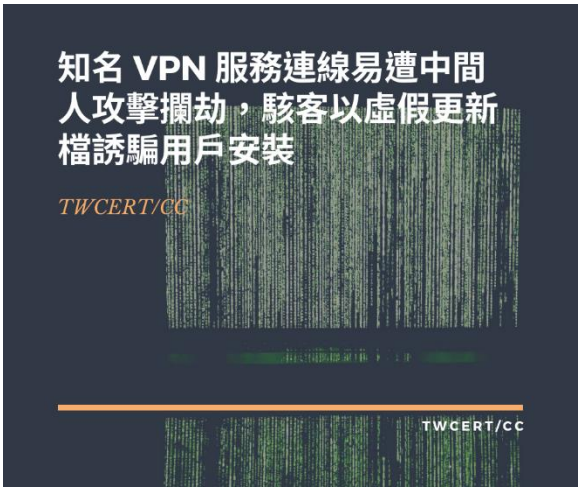
報告中也建議，使用者應依照 Microsoft 的建議，正確設定 Thunderbolt 3 的內核 DMA 保護，若無法自行設定相關安全措施，應聯絡製造商或其他技術支援服務來確保設備安全。切勿將不信任的周邊設備連接電腦，並且在 Thunderbolt 3 介面已啟用的情形下，勿讓電腦設備離開視線或借予他人，以避免遭受該漏洞攻擊。



(Image by Björn Ruytenberg. Licensed under CC BY 4.0.)

- 資料來源：
  1. https://thunderspy.io/assets/reports/breaking-thunderbolt-security-bjorn-ruytenberg-20200417.pdf
  2. https://docs.microsoft.com/zh-tw/windows/security/information-protection/kernel-dma-protection-for-thunderbolt
  3. https://www.wired.com/story/thunderspy-thunderbolt-evil-maid-hacking/
  4. https://thunderspy.io/

2.5.2、知名 VPN 服務連線易遭中間人攻擊攔劫，駭客以虛假更新檔誘騙用戶安裝



資安廠商指出，有多個用戶眾多的 VPN 服務經測試後易遭駭侵者以中間人攻擊方式，攔劫用戶網路通訊內容；有些甚至會被植入假的軟體更新檔案。

專門針對各種 VPN 服務進行資安檢測的資安廠商 VPNpro，近日發表研究報告指出，該公司發現有多個廣受歡迎，用戶眾多的 VPN 服務，經測試後易遭駭侵者以中間人攻擊方式攔劫用戶網路通訊內容；有些甚至會被植入假的軟體更新檔案，造成更大的損害。

VPNpro 的報告中指出，在該公司檢測的 20 個最受歡迎 VPN 連線服務中，有四個無法抵擋駭侵者攔劫用戶的通訊內容；駭侵者可以透過中間人攻擊的方式，攔劫並解密用戶的網路通訊內容。

一旦用戶的 VPN 連線遭到攔劫，除了通訊內容會遭到竊聽外，駭侵者還會鼓勵用戶連上有害的公共 Wi-Fi 網路，或是掃瞄用戶電腦附近的無線路由器，並試圖駭入。

在上述四個有資安疑慮的 VPN 服務中，\PrivateVPN 和 BetterNet VPNs 這兩個服務會遭到駭侵者偽造其名義，發送虛假的系統更新，PrivateVPN 應用程式還會自動執行假的系統更新檔。

用戶如果不慎安裝了虛假的更新檔，駭侵者就可以在受害者電腦上植入惡意軟體竊取更多資訊、遠端執行任意程式碼，或是安裝挖礦軟體或勒贖軟

體。

VPNpro 在發現這些問題後，隨即通報各該 VPN 業者，被測出問題的業者均已提供資安修補更新；這些 VPN 服務的用戶，應立即以官方提供管道更新自己電腦中的應用程式。

- 資料來源：
  1. https://vpnpro.com/blog/privatevpn-betternet-vulnerabilities/
  2. https://www.securityweek.com/two-popular-vpns-exposed-users-attacks-fake-updates

2.5.3、某駭侵團體於一周內攻擊九十萬個 WordPress 網站

資安廠商發現一周以來，全球有超過九十萬個以 WordPress 架設的網站，遭到某特定駭侵團體鎖定駭入。

資安廠商 Wordfence 發表研究報告指出，該公司的資安團隊近期發現針對 WordPress 網站的大規模駭侵行動。

該公司說，四月底開始觀察到某特定駭侵團體的攻擊活動開始大量增加達三十倍之多；一周以來，全球有超過九十萬個以 WordPress 架設的網站，遭到該特定駭侵團體鎖定駭入。

Wordfence 指出，攻擊活動來自高達 24,000 個以上不重覆 IP 位址，且於 5 月 3 日時達到最高峰，約有 50 萬個不同的網域名稱，遭到高達兩千萬次以上的攻擊嘗試。

Wordfence 說，這波大規模攻擊行動主要都是攻擊這些 WordPress 網站外掛程式的 XSS 漏洞。被攻擊的網站使用的多種外掛程式，大多含有多種未被修復的資安漏洞，主要都是 XSS 防護方面出現問題，因此遭到駭侵者鎖定。

至於到底是哪個駭侵團體發動此波攻擊，目前尚無清楚的資訊。

Wordfence 建議全球為數眾多的 WordPress 網站管理者，一定要隨時將 WordPress 主程式與外掛程式更新到最新版本，也建議在自己的網站上安裝「網站應用程式防火牆」（website application firewall, WAF」，以阻擋可能發生的攻擊。

- 資料來源：
  1. https://www.wordfence.com/blog/2020/05/nearly-a-million-wp-sites-targeted-in-large-scale-attacks/
  2. https://www.zdnet.com/article/a-hacker-group-tried-to-hijack-900000-wordpress-sites-over-the-last-week/

2.5.4、域名商 GoDaddy 遭駭，顧客的網站託管登入資訊外洩

全球規模最大的網域註冊託管服務商 GoDaddy.com，日前遭駭侵者攻擊，導致網站託管登入資訊遭到外洩。

全球規模最大的網域註冊託管服務商，管理七千七百萬個網域、客戶人數超過 1900 萬名的 GoDaddy.com，對外公布遭駭侵者攻擊的資安通報；該攻擊事件導致儲存在該公司的的網站託管登入資訊遭到外洩。

GoDaddy 是在一封寄給受影響用戶的 Email 中揭露這次攻擊事件，據了解，該公司在去年 10 月 19 日起觀察到某些伺服器發生異常，經過調查後發現有不明駭侵者取得了某些伺服器 SSH 連線服務的使用權，受到影響的帳號約有 28,000 個。

SSH 是對伺服器發出指令以進行遠端操作的重要基礎服務，一旦駭侵者可以取得 SSH 連線權限，就有極高機會可以進行各種操作，包括取得更高權限、不法竊取伺服器內的資料和檔案，甚至遠端執行任意程式碼。

GoDaddy 發出的資安通報說，這次外洩的資訊，僅限於網站託管服務用戶用於其網站的登入資訊，並不包括用戶登入整個 GoDaddy 網站的登入資訊，也不包含個資。目前 GoDaddy 已經重置所有潛在受害者的登入密碼，未提供這次駭侵攻擊的其他詳細資訊。

- 資料來源：
  1. https://oag.ca.gov/system/files/Customer%20Notification.pdf
  2. https://threatpost.com/godaddy-hack-breaches-hosting-account-credentials/155475/

2.5.5、提交給 Linux 基金會的 HKSP 核心資安加強程式碼，被發現暗藏後門

資安研究團隊發現，由華為提供給 Linux 基金會，用以加強 Linux 核心資安防護能力的 HKSP 程式碼，藏有後門，可能導致未來新版 Linux 出現資安風險。

資安研究團隊 Grsecurity 發現，由華為提供給 Linux 基金會，用以加強 Linux 核心資安防護能力，一段名為「HKSP」（Huawei Kernel Self Protection）的程式碼，藏有後門，可能導致未來新版 Linux 都出現資安風險。

Grsecurity 在其研究報告中指出，他們在華為提報給 Linux 基金會的 HKSP 安全修補加強程式碼中發現一個資安漏洞，看不出是針對哪個類型資安威脅提出修補建議，也不包括相關的防禦程式碼。

Grsecurity 進一步指出，檢視華為提出的程式碼後，他們還發現一個可利用來進行駭侵攻擊的資安漏洞；如果 Linux 基金會接受該修補程式，將這段程式碼放入未來版本的 Linux 核心，將造成相當嚴重的資安風險。

Grsecurity 的研究報告，詳細分析了華為程式碼中的弱點，以及可能造成的資安風險。

在 Grsecurity 發表此報告後，華為立刻回應，表示該段程式碼僅為示範之用、提報至 Linux 基金會的舉動，也只是某個華為資安工程師的「個人行為」，不代表華為公司；華為公司也未將這段程式碼使用於任何華為產品。

但 Grsecurity 也隨即於其報告中新增華為回應，並且指出交付該程式碼的工程師屬於技術職中職級最高（20 職等）的資安工程師。

- 資料來源：
  1. https://grsecurity.net/huawei_hksp_introduces_trivially_exploitable_vulnerability
  2. https://www.zdnet.com/article/huawei-denies-involvement-in-buggy-linux-kernel-patch-proposal/
  3. https://androidrookies.com/huawei-dev-team-sends-a-buggy-hksp-patch-with-backdoor-to-linux-foundation/

2.5.6、微軟用以解決反向 RDP 攻擊的修補程式，可用第三方 RDP 連線程式繞過

資安廠商連續兩次發現，微軟針對反向 RDP 攻擊所發行的資安修補包，都可以用簡單的方法加以跳過，並未真正從根本解決問題所在。

資安廠商 Check Point 日前發表研究報告，指出微軟於去年七月推出的資安修補包中，有一個針對反向 RDP 攻擊漏洞的修補軟體；這個修補方式後來被該公司的資安專家找到繞過的方法：只要把路徑中的倒斜線換成一般正斜線即可。

為了修補這個問題（CVE-2020-0655），微軟於今年二月的資安修補包中又提供了一個新的修補程式；然而資安廠商 Check Point 又發現，微軟解決這個問題的方式，只是利用一個簡單的 workaround，並未從根本解決核心問題所在的 API。

Check Point 指出，微軟於二月提出的解決方案，雖然能解決 Windows 用戶端的反向 RDP 攻擊（ CVE-2019-0887 ），但無法用於第三方的 RDP 用戶端連線上；只要是用非 Windows 作業系統的 RDP 用戶端軟體，就可以跳過微軟設計的所有安全檢查關卡，輕鬆進行反向 RDP 攻擊。

Check Point 的報告中詳細描述了他們兩次發現微軟未能完全解決漏洞的流程，也已經通報給微軟公司資安團隊，然而目前還沒有得到任何回應。

Check Point 指出，該公司強烈建議所有軟體開發者和資安研究者，應該正視這個尚未解決的資安漏洞，同時確認自己的產品有所準備，避免受此漏洞影響。

- 資料來源：
  1. https://research.checkpoint.com/2020/reverse-rdp-the-path-not-taken/
  2. https://thehackernews.com/2020/05/reverse-rdp-attack-patch.html

2.5.7、微軟推出 2020 年 5 月資安修補包，修復多個重大資安漏洞

微軟推出 2020 年 5 月資安修補包，共有 111 個資安漏洞得到修復。用戶請盡速更新。

微軟公司每月固定的推出「Patch Tuesday」逐月資安修補包的 2020 年 5 月版本於日前釋出，一共修補多達 111 個資安漏洞；其中包括 16 個嚴重等級漏洞，另有 96 個重要等級，都可在這次的修補包中解決。

值得注意的是，這個月的資安修補包修復的漏洞，沒有任何一個已經被駭侵團體用以進行各種規模的攻擊；也就是說都是屬於未被公開的漏洞。

在這些得到修復的漏洞中，絕大多數「重要」等級的漏洞，多半是屬於「權限提升」類型，數量達 56 個；主要都存於 Microsoft Windows 作業系統中各種子系統的元件。如果用戶的 Windows 電腦遭到駭侵者駭入，這些漏洞即有可能被用來提升駭侵者的操作權限，造成更大的損害。

至於其他被列為「嚴重」等級的資安漏洞，其中有兩個存於 Microsoft Color Management 色彩管理子系統中，CVE 編號為 CVE-2020-1117；另一個存於 Windows Media Foundation 子系統中，編號為 CVE-2020-1126；駭侵者可透過社交工程等方式駭入系統後，直接利用這兩個漏洞執行各種系統操作，包括刪改檔案、竊取資料或增刪用戶帳號等。

另外，SharePoint 有兩個 RCE（遠端執行任意程式碼）的漏洞，也在這次得以修補，其 CVE 編號分別為 CVE-2020-1023 與 CVE-2020-1102；這兩個漏洞可讓駭侵者任意執行任何程式，潛在為害甚大。

微軟各種產品的用戶，應盡速透過這個資安修補包進行更新，以獲得更全面的保護。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-May
  2. https://threatpost.com/microsoft-111-bugs-may-patch-tuesday/155669/

2.6、軟硬體漏洞資訊

2.6.1、Adobe 推出修補程式，以解決遠端程式碼執行漏洞

Adobe 近日在例行的每月更新修補包之外，另行推出針對 Adobe Character Animator 內含嚴重資安漏洞的修補程式。

這次修補的漏洞，編號為 CVE-2020-9586，主要的問題在於當用戶以此軟體開啟惡意檔案或含有惡意程式碼的網頁時，可能遭駭侵者用以遠端執行任意程式碼。

這個問題的根源在於 PostScript 子系統在針對 BoundBox 元素進行分析時的錯誤，會導致堆疊緩衝區發生溢位錯誤。該系統對於用戶輸入的資料長度，沒有事先進行適當的驗證流程，就直接把資料複製到堆疊緩衝區中。

資安廠商趨勢科技的資安研究員 Dustin Chiles 指出，這個錯誤可讓駭侵者在現正執行的程序內遠端執行任意程式碼。

這個漏洞的 CVSS 評分為 7.7 分，屬於「高危險」等級；不過 Adobe 指出，目前並未發現有任何駭侵行動利用這個漏洞進行；而在 Adobe 提供的更新優先等級，則被指定為「3」。

Adobe 建議所有仍在執行 Adobe Character Animator 3.2 與先前所有版本（包括 WIndows 與 Mac 版）的用戶，視情形升級至 3.3 或更新版本，以解決這個問題。

- CVE 編號：CVE-2020-9586
- 影響版本：Adobe Character Animator for Mac/Windows 3.2 與所有先前版本
- 解決方案：升級至 Adobe Character Animator 3.3 以上版本

- 資料來源：
  1. https://helpx.adobe.com/security/products/character_animator/apsb20-25.html
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9586
  3. https://www.cybersecurity-help.cz/vdb/SB2020052019
  4. https://threatpost.com/adobe-patches-critical-rce-flaw-character-animator/155882/

2.6.2、Android 平台漏洞 StrandHogg 2.0 可導致裝置上的 App 遭挾持

資安廠商 Promon 的研究人員，近日發表一篇針對 Android 平台安全性的研究報告。

揭露一個名為 StrandHogg 2.0 的嚴重資安漏洞，可能導致用戶手機和平板上的 App 遭到挾持，多種機敏資訊亦可能遭竊。

StrandHogg 2.0 的運作原理，和去年發現的 StrandHogg 相當類似，都可在感染後將自己隱藏在正常的軟體身後；當用戶開啟正常軟體時，真正執行的並不是這個正常版的軟體，而是植入了惡意軟體程式碼的「分身」。

新版 StrandHogg 2.0 除了上述的類似功能外，還能讓惡意軟體偽裝成任意的 Android App；先前的版本只能偽裝成 TaskAffinity 這支 App，甚至能在用戶點按開啟任何 App 時立刻偽裝成該 App。

用戶一旦感染利用此嚴重漏洞的惡意軟體，各種透過遭偽裝 App 進行的活動記錄和產生的資訊，都可能曝露在嚴重資安風險之下；包括各種通聯記錄、相片或影片、各種登入資訊、金融帳戶活動與登入個資、手機所在位置座標資料等，都有可能被竊。

目前尚未傳出有任何攻擊行動是基於 StrandHogg 2.0 這個嚴重漏洞，資安廠商 Promon 發展出了概念證明的範例攻擊程式，同時提供說明影片。

這個編號為 CVE-2020-0096 的危險程度評分高達 7.8 分，屬於「高」危

險等級。過去針對第一代 StrandHogg 的修補手法，並不適用於 StrandHogg 2.0。

Google 已針對這個漏洞發表適用於 Android 9、8.1、8 的修補程式；但較舊的 Android 版本仍有近四成的使用量，尚未獲得適當的修補。最新版的 Android 10 並無此一漏洞。

- CVE 編號：CVE-2020-0096
- 影響版本：Android 9 與之前版本
- 解決方案：Android 9、8.1、8 用戶可更新至最新版本，其餘較舊版本尚無修補工具

- 資料來源：
  1. https://promon.co/strandhogg-2-0/
  2. https://nvd.nist.gov/vuln/detail/CVE-2020-0096
  3. https://threatpost.com/strandhogg-2-critical-bug-android-app-hijacking/156058/

2.6.3、ARMv7 處理器內含的記憶體崩潰漏洞，可能導致智慧車輛遭遠端遙控

網通大廠 Cisco 的資安研究團隊，日前發表研究報告，指出一個內藏在 ARMv7 處理器中的記憶體崩潰漏洞，可能導致任何使用此處理器的裝置受到駭侵攻擊；特別是智慧汽車很可能被駭侵者遠端遙控。

這個漏洞發生在 ARMv7 內 GNU glibc 2.30.9000 的 memcpy() 函數，在處理記憶體資料時發生的程式漏洞；不但可讓駭侵者遠端執行任意程式碼，甚至在程式已經無法執行的情形下繼續遙控。

Cisco 的資安研究人員，在針對智慧汽車進行各種資安滲透攻擊的測試時，發現這個嵌入在在智慧車控系統中的 web 伺服器存有整數溢位錯誤漏洞；由於這個嵌入式的 web 伺服器可經由車內的 Wi-Fi 網路連結存取，因此只要能進入該無線網路的人，都可以存取該伺服器，進而發動攻擊。

Cisco 在其研究報告中，完整描述了利用這個漏洞進行概念證實攻擊的方法與步驟。

這個漏洞的 CVE 編號被定為 CVE-2020-6069，其危險程度評分為 8.1 分，評級為「高」。

值得注意的是，雖然有許多 Unix 家族作業系統也都內建 GNU glibc 函數庫，但如 RedHat、SUSE 等 Linux 發行版都不受這個 CVE-2020-6069 的影響。

- CVE 編號：CVE-2020-6069
- 影響版本：ARMv7 各版本

- 資料來源：
  1. https://blog.talosintelligence.com/2020/05/cve-2020-6096.html
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6096
  3. https://nvd.nist.gov/vuln/detail/CVE-2020-6096
  4. https://www.suse.com/security/cve/CVE-2020-6096/

第 3 章、 資安研討會及活動

數位轉型攻略：後疫時代企業生存法則	
活動時間	**2020 年 6 月起 14:35~15:15 每月線上全新開播 (每堂 45 分鐘)**
活動地點	**Webinar**
活動網站	**https://webinar.ithome.com.tw/index.html?v=1590985286#info**
活動概要	 主辦單位：iThome iThome Webinar 時間 2020 年 6 月起 14:35~15:15 每月線上全新開播 (每堂 45 分鐘) 型式本活動為線上講座，將透過 iThome 影音平台播出 講題線上跟您分享如何應用新興科技，強化企業 IT 韌性的產品、技術與服務等數位轉型攻略議題。 收看請於首播前上線報名，待主辦單位確認您的報名資料後， 將於活動前夕提供線上專屬收視連結，請於開播前登入以利準時參與課程。 觀眾企業 IT、企業 MIS 及資訊相關同仁 **詳細活動日期、議程與報名方式，請見活動官方網站。**

為您的網站和應用程序打造難以穿越的防禦屏障	
活動時間	**2020/6/11，下午 2 點**
活動地點	**Webinar**
活動網站	**http://surl.twcert.org.tw/s4eB4**
活動概要	主辦單位：Cloudflare 活動時間：2020/6/11，下午 2 點 如今的網路世界充滿各式各樣的在線攻擊 ，Web 應用程序攻擊也已經變得更加複雜，並利用了多種高級攻擊策略。同時，由於更多公共 API、系統轉移到雲端，以及日益增加的第三方集成，使客戶受到更大的攻擊風險。Cloudflare 創建了互鎖的(Interlocking)應用程序安全解決方案套件，比如 DDoS 防護，和 TCP/UDP 應用程序防護。這些工具結合在一起，可以在您的網站和應用程序周圍打造難以穿透的防禦屏障，為您的互聯網資源提供基於雲的、永遠在線的安全保障! Cloudflare 網路直播研討會系列，了解如下內容： 網路威脅日益嚴重，企業架構面臨哪些挑戰? 如何防護現代分散式攻擊? 如何保護網站伺服器，和其他 TCP/UDP 應用？ 如何在保證速度和性能的前提下，保證您的企業網路擁有安全且可靠的維運? **詳細活動介紹與報名方式請見官方網站。**

6 月例會_連網設備的資安風險與信任管理策略	
活動時間	**2020-06-16 14:00 ~ 17:00**
活動地點	**新竹市光復路二段 153 號 2 樓**
活動網站	**https://www.caa.org.tw/coursedetail-3345.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association 主辦單位：中華民國電腦稽核協會、ISACA Taiwan Chapter 報名時間:2020-05-13~2020-06-15 上課時間: 2020-06-16 14:00 ~ 17:00 活動時間：2020/6/16(二)，下午 2:00 ~ 5:00 (改期，原訂於 6/23 舉辦) 活動地點：新竹市光復中學-國中部東側教學大樓推廣中心 第一演講廳 地址：新竹市光復路二段 153 號 2 樓 演講大綱：1.當今環境的資安風險與挑戰 2.傳統資安工具 vs 內稽內控的挑戰 3.業界公認資安指南與資安框架建議的做法 主講講師：張恩綾 美商 Forescout Technology 台灣區總經理 證照：ITIL Foundation、Cybersecurity and Its ten Domain 適合對象：中華民國電腦稽核協會之會員、稽核人員、資訊安全人員、IT、MIS 部門等或對此相關議題有興趣者 報名費用：中華民國電腦稽核協會會員(含團體會員公司同仁)免費，非會員 500 元 **詳細活動相關細節及報名方式請見官方網站**

Psychology of Passwords: Combatting Cognitive Dissonance in Password Creation	
活動時間	**2020/6/25**
活動地點	**Webinar**
活動網站	**https://staysafeonline.org/event/psychology-of-passwords/**
活動概要	As more and more people work and socialize exclusively online, protecting your digital identity is more important than ever. Most people believe they are knowledgeable about the risks of poor password security; however, they are not using that knowledge to protect themselves from cyber threats. Will 2020 finally be the tipping point that causes people to show more concern for their online data? Join the National Cyber Security Alliance as we talk with LogMeIn's Chief Information Security Officer (CISO), Gerald Beuchelt, about their latest LastPass Psychology of Passwords research. In this webinar, you will learn: -What online behaviors are putting you and your peers at risk -Why people are continuing to ignore safe password practices -What more you can be doing to secure your accounts Featured Speaker: Gerald Beuchelt, CISO, LogMeIn **詳細活動資訊與報名方式，請見官方網站。**

6 月例會_一場無聲的網路戰爭	
活動時間	**2020-06-30 14:00 ~ 17:00**
活動地點	**台北市信義區基隆路一段 143 號 3 樓**
活動網站	**https://www.caa.org.tw/coursedetail-3349.html**
活動概要	中華民國電腦稽核協會 Computer Audit Association 報名時間:2020-05-25~2020-06-29 主辦單位：中華民國電腦稽核協會、ISACA Taiwan Chapter 活動地點：宏電科技-ATEN CIC Room 互動應用展示中心 地址：台北市信義區基隆路一段 143 號 3 樓 演講大綱：1.近期資安重大事件分享 2.手法分析 3.結論 適合對象：中華民國電腦稽核協會之會員、稽核人員、資訊安全人員、IT、MIS 部門等或對此相關議題有興趣者 報名費用：中華民國電腦稽核協會會員(含團體會員公司同仁)免費，非會員 500 元 **詳細活動相關細節及報名方式請見官方網站**

AWS SUMMIT ONLINE	
活動時間	**2020 年 7 月 10 日，10:00AM - 4:00PM（9:00AM 平台開放登入）**
活動地點	**Webinar**
活動網站	**https://aws.amazon.com/tw/events/summits/online/taipei/**
活動概要	 【2020 AWS 雲端高峰會】7 月 10 日重磅來襲！ 7 月 10 日，您將同時與業界技術同好，一齊線上參與精彩的雲端技術交流，以及由 AWS 與合作夥伴聯手打造的豐富展覽內容。這些主題的深入討論將由 AWS 主題專家進行，他們將與您分享最佳實踐和真實的客戶案例。無論您著重於產業解決方案 (Business Track) 或是雲端開發技術 (Technical Track)，滿滿 42 堂分享，讓您滿載而歸。 活動主題： 企業上雲策略 (Strategy)、微服務 (Microservices)、人工智慧與機器學習 (AI/ML)、數據分析 (Data & Analytics)、資安與合規 (Security & Compliance)、網路 (Networking)、無伺服器服務 (Serverless)、容器服務 (Containers) **詳細活動議程及報名方式請見官方網站。**

RSAConference2020 Asia Pacific & Japan	
活動時間	**2020 年 7/15-17**
活動地點	**Online**
活動網站	**https://www.rsaconference.com/apj**
活動概要	 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. **詳細活動相關細節、報名及議程請見官方網站。**

CYBERSEC 2020 臺灣資安大會	
活動時間	**8/12(二) – 8/14(四) 08:30 ~ 17:00**
活動地點	**台北市南港區經貿二路 2 號 (南港展覽二館)**
活動網站	https://r.itho.me/sec2020
活動概要	 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 8/12-8/14 於南港展覽二館盛大登場！ 匯聚世界級資安大神、國內資安頂尖高手，從提供超過 200 堂資安面向的議程、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 家以上全球與國內知名標竿資安品牌，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，與來自臺灣與亞太地區超過 8,000 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。 主辦單位：iThome 了解更多大會資訊：https://r.itho.me/sec2020

第 4 章、 2020 年 05 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。

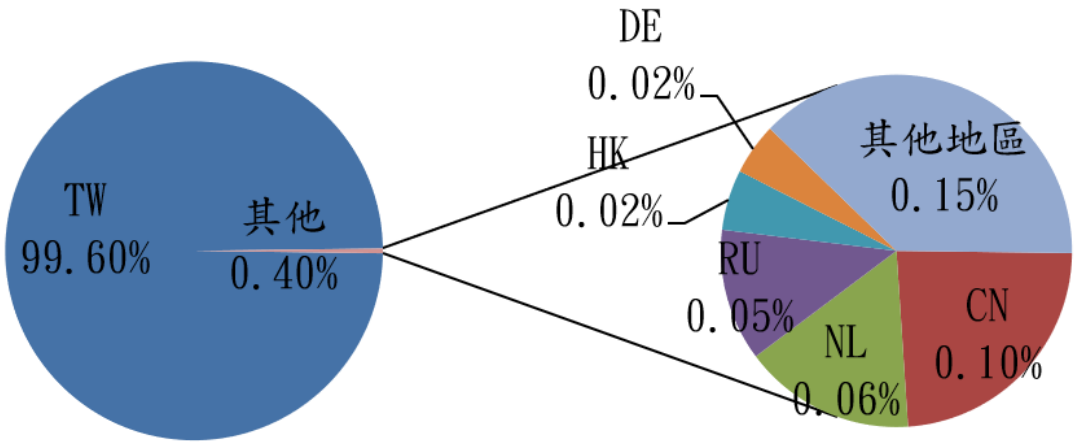


圖 1、分享地區統計圖

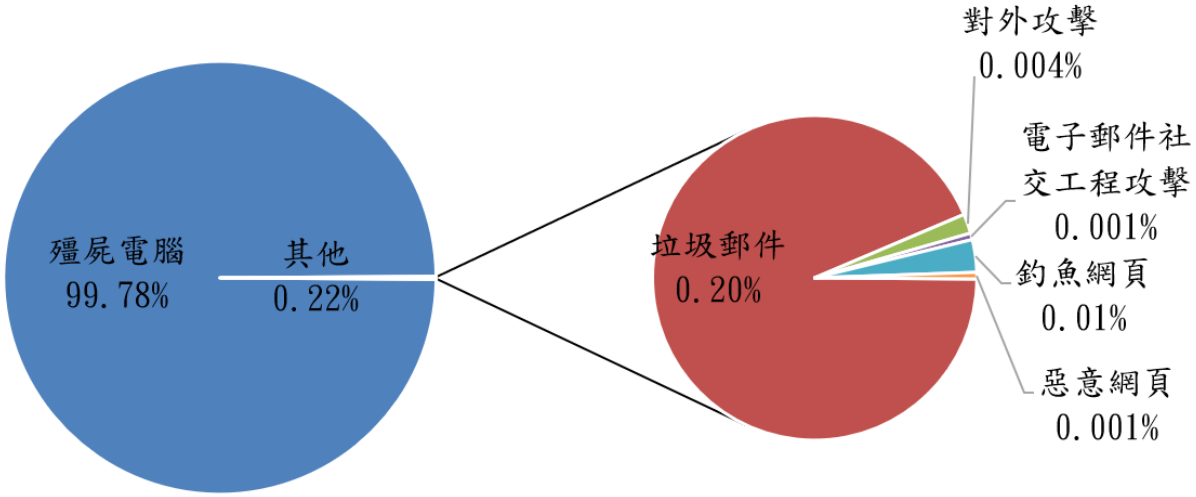

殭屍電腦
99.78%
其他
0.22%
垃圾郵件
0.20%
對外攻擊
0.004%
電子郵件社
交工程攻擊
0.001%
釣魚網頁
0.01%
惡意網頁
0.001%

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 6 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**