TWCERT/CC 資安情資電子報

2019 年 8 月份

目錄

第 1 章、 封面故事

微軟證實 Windows 用戶正遭「地獄大公」惡意軟體大規模駭侵

微軟資安團隊發布公告，證實目前有個稱為「地獄大公」（Great Duke of Hell）的惡意軟體，針對 Windows 用戶進行大規模攻擊。

微軟指出，這個稱為「地獄大公」的惡意軟體，是所謂的「無檔案惡意軟體」；用戶通常是點擊了釣魚信件中的惡意連結；接著這個連結會開啟一個捷徑，以命令行指令執行一個 JavaScript 程式碼。

一旦用戶感染後，電腦中的登入資訊、按鍵輸入記錄等資料都會被送到遠端伺服器。也由於受害電腦沒有下載任何檔案，因此這種攻擊方式可以逃過多種防毒軟體的檔案檢測機制。

- 資料來源：
  1. https://www.theregister.co.uk/2019/07/08/microsoft_astaroth_examination/
  2. https://www.reactionarytimes.com/what-is-the-great-duke-of-hell-malware/

第 2 章、 國內外重要資安事件

2.1、國際政府組織資安資訊

2.1.1 進出新疆旅客，手機被強迫安裝惡意軟體

多家媒體指出，進出新疆邊境的外國旅客，最近開始遭到中國邊防單位強制於其手機中安裝惡意軟體，以取得手機內各種資訊。

包括紐約時報、南德日報、英國衛報、德國公共廣播 NDR、科技媒體 Motherboard 等都報導這項強制監控行動。

近來進出新疆的外國旅客，會在邊境檢查時被要求交出手機給邊防人員檢查，同時強制安裝一支名為「蜂采」的 Android 惡意軟體。

南德日報和 Motherboard 取得這支「蜂采」App 後，會同紐約時報、英國衛報與多個資安研究單位，對其進行分析；研究人員發現這支軟體會竊取手機中的各項資訊，如行事曆中的所有行程、通訊錄、通話記錄、用戶在各個 App 中的登入資訊等，並將資料上傳到某一台伺服器中。

這支 App 還會掃瞄用戶手機中的各種檔案，內建超過七萬三千種不同檔案的雜湊特徵碼；其中某些目標檔案屬於伊斯蘭極端主義相關或 IS 的線上出版物，但該 App 也會針對伊斯蘭經典古蘭經或達賴喇嘛相關內容進行

掃瞄。

通關旅客如果使用 iPhone，雖然不會被強制安裝惡意軟體，但手機也會被邊防人員取走，利用特殊機器加以掃瞄。

- 資料來源：
  1. https://www.vice.com/en_us/article/7xgame/at-chinese-border-tourists-forced-to-install-a-text-stealing-piece-of-malware
  2. https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones
  3. https://www.nytimes.com/2019/07/02/technology/china-xinjiang-app.html

2.1.2 德國媒體揭發中國駭侵團體透過 Winnti 惡意軟體的長年駭侵行為

北德廣播電台（Norddeutscher Rundfunk）和巴伐利亞廣播電視公司（Bavaria Radio and Television Network）共同進行深度調查，指出來自中國的駭侵團體，長年透過一個稱為「Winnti」的惡意軟體，對全球各大公私營單位組織進行監聽與駭侵的內幕。

在這份由 NDR 和 BR 協同進行的調查中，多位資安專家深入追查，發現中國駭侵組織透過 Winnti 惡意軟體，對包括遊戲產業、科技、製藥和重化工業的多家知名廠商進行駭侵與監聽；受駭廠商如下：

- 遊戲：Gameforge、Valve
- 軟體：Teamviewer
- 科技：西門子、住友、蒂森克虜伯（ThyssenKurpp）
- 製藥：拜爾、羅氏（Roche）
- 化工：巴斯夫、Covestro、信越

報告指出，這個駭侵團體一開始係以遊戲業為主要目標，以謀取不法利益。該團體首先於 2011 攻擊總部設在德國 Karlsruhe 的遊戲公司 Gameforge，以 Winnti 惡意軟體入侵該公司 40 台資料庫主機。

接下來該團體的駭侵重點轉移到大型製造業，2014 年起開始攻擊高科技、化工與藥廠等對象；最近甚至開始進行政治監聽活動，針對西藏流亡政府駐印度所在地的電信業者進行駭侵攻擊。

- 資料來源：

1. https://web.br.de/interaktiv/winnti/english/
2. https://hub.packtpub.com/winnti-malware-chinese-hacker-group-attacks-major-german-corporations-for-years/
3. https://www.europeanpharmaceuticalreview.com/news/95107/roche-confirms-cyber-attack-from-winnti-malware/

2.1.3 美國網戰司令部發布警告，指有網軍透過 Outlook 老舊漏洞進行駭侵

美國網路作戰司令部於日前在 Twitter 上發布警訊，指目前正有透過老舊 Outloook 漏洞，針對美國政府單位的網路攻擊，正在大規模發生中。

被利用來進行駭侵攻擊的 Outlook 漏洞，編號為 CVE-2017-11774，是兩年前就被確認的老舊漏洞；微軟已在 2017 年十月發行的安全更新中提供修補軟體。

這個漏洞可讓攻擊者跳過 Outlook 的沙盒限制，在目標電腦的作業系統中執行惡意程式碼。

資安研究單位 SensePost 指出，在 2018 年曾監測到由伊朗支持的 APT33 駭侵團體，利用此漏洞發動網路攻擊。

美國網戰司令部沒有列出可能的攻擊來源，但一般相信這次攻擊和伊朗有關；資安專家指出，未來來自伊朗的駭侵攻勢可能繼續升高。

資料來源：

1. https://twitter.com/CNMF_VirusAlert/status/1146130046127681536
2. https://www.zdnet.com/article/us-cyber-command-issues-alert-about-hackers-exploiting-outlook-vulnerabil

2.1.4 Telegram 遭受來自中國的大規模 DDoS 攻擊

資安公司 FireEye 的研究人員發現，一個名為 APT34 的駭侵團體，透過 LinkedIn 廣為發送夾帶惡意軟體的加友邀請。

FireEye 研究人員指出，該公司發現自今年六月起在 LinkedIn 上出現大量透過加友邀請夾帶惡意軟體檔案的駭侵活動，散布者疑似為 APT34 組織。

APT34 在 LinkedIn 邀請中會假扮成英國劍橋大學的人員，以取信於受害者；在邀請中夾帶的惡意軟體共有三類：後門軟體 TONEDEAF、瀏覽器帳密竊取工具 VALUEVAULT、鍵盤輸入密錄工具 LONGWATCH。

研究人員指出，這些惡意軟體是以微軟 Office 文件的巨集，藏在邀請訊息的附檔之中。

- 資料來源：
  1. https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
  2. https://www.scmagazine.com/home/security-news/apts-cyberespionage/fireeye-researchers-identified-a-phishing-campaign-conducted-by-apt34-masquerading-as-a-member-of-cambridge-university-to-gain-their-victims-trust-to-open-malicious-documents/

2.1.5 中國江蘇省公安局洩漏超過九千萬筆個人與公司行號資料

資安專家發現一個屬於中國江蘇省公安局的資料庫在網路上公開，內含超過九千萬筆以上的個人與公司行號資料。

資安研究人員發現一台屬於中國江蘇省公安局所有的 ElasticSearch 伺服器，含有兩個完全沒有套用任何安全措施的資料庫，在網路上可任意存取。

這兩個資料庫的資料大小合計高達 26GB，資料筆數多達九千萬筆以上，內含許多人的個資，包括姓名、出生日、性別、身分證字號、地理座標資訊、所屬城市等個人識別資料，另外還有公司行號資料，包括公司名稱、編號、營業類型、地址、所屬城市、附註說明等資料。

資安研究人員指出，這兩個資料庫不但沒有加密或任何保護，任何人也能擁有完整的管理與存取權限。

目前該資料庫已經自公開網路離線，無法存取。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/over-90-million-records-leaked-by-chinese-public-security-department/
  2. https://www.computing.co.uk/ctg/news/3078613/china-database-leak-90-million

2.1.6 國資安公司販售 BlueKeep 駭侵工具，用以測試資安環境

一家名為 Immuity Inc. 的公司，推出可利用 BlueKeep 嚴重安全漏洞的駭侵工具，該公司宣稱這可讓公司行號用以測試資安設定。

一家美國資安公司 Immunity Inc. 在日前在其資安測試工具 CANVAS 7.23 版中，新增了可利用 BlueKeep 漏洞進行駭侵測試的模組，引起資安界的討論。

透過該測試工具，就能成功利用 BlueKeep 取得遠端電腦的控制權，並執行任何程式碼。

BlueKeep 是最近 Windows 遠端桌面協定最嚴重的安全漏洞之一，CVE 編號為 CVE-2019-0708，可以用來散布例如 WannaCry 之類的惡意軟體。微軟已在五月時提供安全更新修補程式，但市面上仍有許多 Windows 電腦未及更新。

CANVAS 的售價達數千美元，該公司表示這個工具僅用於測試用途，而且不會自我複製並感染其他電腦；但有資安專家認為，這個工具的公開販售，等於是讓任何人都能擁有利用 BlueKeep 這個漏洞的強大駭侵工具，只要他出得起幾千美金。

- 資料來源：
  1. https://www.zdnet.com/article/us-company-selling-weaponized-bluekeep-exploit/
  2. https://twitter.com/Immunityinc/status/1153752470130221057

2.1.7 又一個美國小城為勒贖攻擊繳付贖款

繼佛羅里達小城利維拉市之後，另一個位在佛羅里達的雷克市決定繳付贖金，試圖救回被加密的市政檔案。

同樣位在佛羅里達州的雷克市，成為近來第二個決定繳付贖款，以救回遭加密市政檔案的美國城市。

該市議會緊急會議通過決議，同意繳付 42 個比特幣的贖款，以當時的比特幣匯價來看，約合美金五十萬元。

雷克市的市政檔案資料遭到勒贖軟體攻擊，雖然 IT 人員在發現之後緊急將市政系統離線處理，但大多數市政系統仍遭癱瘓，僅有處於不同網路的警政和消防系統倖免。

該市大多數市政因此停擺長達兩周之久，贖款於六月 25 日繳付，但至今天為止，該市官網仍未公告市政系統復原訊息。

- 資料來源：
  1. https://www.lcfla.com/community/page/press-release-cyber-attack
  2. https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/

2.1.8 俄國否認對以色列機場進行 GPS 信號干擾

以色列指控俄羅斯涉嫌干擾其機場附近的 GPS 信號，俄羅斯政府予以否認。

六月初起，位於以色列特拉維夫東南方的本-古里昂機場，開始持續發生 GPS 信號遭到干擾事件；班機無法在空中透過 GPS 正確定位，僅能以機場地面系統進行起降；雖然沒有釀成任何飛安事故，但對機場的正常運作造成很大衝擊。

以色列政府指稱，這是一起典型的攻擊事件，以色列政府高度懷疑這項攻擊係來自俄羅斯布署在敘利亞境內的電戰系統，該系統位於本-古里昂機場北方約 350 公里的空軍基地之中。

俄羅斯駐以色列大使駁斥這項指控，說這項指控是假新聞，根本不值一談。

- 資料來源：
  1. https://edition.cnn.com/2019/06/27/middleeast/israel-russia-gps-failure-intl/index.html
  2. https://sporaw.livejournal.com/638666.html

2.1.9 佛羅里達小城支付勒贖金，但市政檔案並未完全復原

受勒贖軟體攻擊的美國佛羅里達小城 Lake City，雖然支付了相當於 46 萬美元的比特幣贖金，但市政檔案並未完全復原，整體復舊遙遙無期。

最近一年以來有多個美國城市遭到惡意勒贖攻擊，市政相關檔案系統遭到加密，導致許多城市的政務推動與日常運作陷入癱瘓。其中有一些城市選擇支付贖金，例如佛羅里達小城 Lake City 便以比特幣支付了相當於 46 萬美元的贖款。

然而，贖款付了，市政系統的全面復舊卻仍然遙遙無期。

以 Lake City 的例子來說，雖然電話和 Email 系統能夠恢復運作，但仍有不少系統和檔案並未回復成功；更糟的是，累積了一百年以上的市政歷史資料，例如各種會議記錄、政令等數千份歷史文件，還是得以人工作業方式重新掃瞄建檔。

另外，Lake City 在支付贖金後，立即開除了其 IT 主管。

FBI 指出去年發生超過一千五百起各式加密勒贖攻擊事件，攻擊對象包括各種公私營機構；最近則有集中攻擊像 Lake City 這類有投保的小型城鎮的趨勢；這類小型地方政府多半缺乏足夠的 IT 技術資源抵禦攻擊，再加上有保險公司承保，比較傾向支付贖款以救回市政檔案與系統。

- 資料來源：
  1. https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html
  2. https://www.zdnet.com/article/florida-city-fires-it-employee-after-paying-ransom-demand-last-week/

2.1.10 又有一所美國大專院校遭勒贖，要求二百萬美元贖金

位於美國紐約的蒙洛學院（Monroe College）上周遭勒贖軟體攻擊；駭客要求的贖金高達二百萬美元。

蒙洛學院於七月十一日遭到勒贖軟體的駭侵攻擊，導致該校師生無法存取校務電腦系統；包括該校的網站、Email、教學輔助系統等都陷入癱瘓。

攻擊者要求該校以比特幣支付相當於二百萬美元的巨額贖款，以取回被加密鎖定的系統與校務檔案。

該校表示，目前尚不清楚攻擊者的身分；該校也尚未決定是否要支付高達二百萬美元的贖金。該校已經會同 FBI 進行調查，而資安研究單位認為最近幾起針對政府單位和學校的勒贖攻擊行動，很可能都是同樣幾個駭侵團體發動的。

另外，駭侵團體要求的勒贖金額也有升高的趨勢；數年前幾家美國大學院校被勒贖的贖款約在數千美元上下，然而近來贖金卻節節上漲。

- 資料來源：
  1. https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack
  2. https://nakedsecurity.sophos.com/2019/07/16/ransomware-attackers-demand-1-8m-from-us-college/

2.2、 行動裝置資安訊息

2.2.1 掀起全球流行的變臉軟體 FaceApp，資安疑慮引發各界關注

近來再度於社群平台上掀起全球話題俄羅斯變臉軟體 FaceApp，引發大量資安疑慮；資安專家認為用戶應該謹慎使用這類 App。

兩年前就已推出的手機變臉軟體 FaceApp，最近推出可以計算模擬人臉變老的模樣，因而再度掀起使用熱潮；許多用戶在社群平台上分享自己變老後的照片；但 FaceApp 是由俄羅斯團隊開發，再加上美國總統大選將至，因而引發各界的資安疑慮。

美國民主黨全國委員會就提出警訊，呼籲民眾不要安裝使用這支來自俄羅斯的 App，以避免潛在的資安風險；也有資安專家從其使用授權條款出發，認為這支 App 的使用條款要求太多權限，無法確保用戶隱私。甚至有人指出 FaceApp 會把用戶手機裡的所有相片上傳到俄羅斯的伺服器。

TechCrunch 和其它專家研究 FaceApp 的運作過程，指出並沒有觀察到除了用戶選定的相片之外，其他相片也被上傳的跡象；專家說 iPhone 版 FaceApp 使用的是 iOS 的標準 API，一次只能上傳一張用戶主動選取的相片。

FaceApp 團隊也出面說明，該

團隊雖然位在俄羅斯，但用戶相片是在 AWS 和 Google Cloud 中處理，並沒有傳送到俄羅斯。

- 資料來源：
  1. https://techcrunch.com/2019/07/17/faceapp-responds-to-privacy-concerns/
  2. https://edition.cnn.com/2019/07/17/politics/dnc-warning-faceapp/index.html

2.2.2 Google 發現能讓 iPhone 變磚的 iMessage 訊息炸彈

Google 的資安研究單位發現，特定的 iMessage 訊息能讓 iPhone 陷入反覆重開機的錯誤，除非將手機重設為出廠預設狀態，否則手機將無法使用。

根據 Google 資安研究單位 Project Zero 指出，該單位發現一個可讓 iPhone 無法使用（變磚）的 iMessage 文字訊息炸彈；iPhone 一旦接收到這個訊息，就會陷入不斷重新啟動的循環，導致用戶無法使用手機，甚至 hard reset 都無法解決問題。

研究人員說，用戶想要取回手機控制權的唯一方式，就是在重開機後立即進入恢復模式，然後清空手機內所有資料，回復至出廠狀態。這當然會造成用戶存在手機中的資料流失。

除了 iPhone 外，如果是 Mac 版 iMessage 接收到這個訊息，同樣會造成 MacOS 當機，但重新啟動後即可繼續使用，不會造成 Mac 變磚。

Google Project Zero 在發現這

個問題時便立即通報 Apple，Apple 也在問題提報的九十天之內就推出了修補軟體；只要 iPhone 在五月時更新到 iOS 12.3 之後的版本，就不用擔心這個問題。還沒有更新到此版本的 iPhone 使用者，請立即更新，並打開手機的自動更新開關。

- 資料來源：
  1. https://bugs.chromium.org/p/project-zero/issues/detail?id=1826
  2. https://www.forbes.com/sites/daveywinder/2019/07/07/google-confirms-apple-iphone-bricking-imessage-bomb/#296a19177a43

2.3、 軟體系統資安議題

2.3.1 中國製智慧家庭設備商，洩漏超過二十億筆個資項目

中國一家名為 Orvibo 的智慧家庭設備供應商，遭資安單位發現將二十億筆以上的個資資料庫曝露在網上，幾無保護，供人任意存取。

據資安研究人員指出，在這個資料庫中主要存有用戶姓名、Email、密碼、精確的地點座標資訊，筆數達二十億筆以上，含蓋幾乎全球各地的用戶，受害者遍及中國、日本、泰國、美國、英國、墨西哥、法國、澳洲、巴西等國。

Orvibo 主要的業務範圍包括各種智慧家庭解決方案，例如家用、業務用或旅館業者的各種系統，包括安全與能源管理系統，以及遠端監控與資料記錄分析服務，並透過其私有雲端服務平台加以整合。

這個資料庫的內容僅經過簡單的 MD5 雜湊加密，非常容易破解還原；資安研究單位在六月初就發送資安疑慮通知給 Orvibo 公司，但直到七月初，該公司才將這個資料庫加上較強的保護措施。

- 資料來源：
  1. https://www.bleepingcomputer.com/news/security/billions-of-records-including-passwords-leaked-by-smart-home-vendor/
  2. https://blog.avast.com/orvibo-smart-home-devices-leaked-records

2.3.2 廣受歡迎的線上會議服務 Zoom 被爆嚴重安全漏洞，網站可藉以綁架 Mac 攝影鏡頭

資安研究人員發現用戶極多的 Zoom 線上視訊會議服務，其 Mac 版應用程式內含嚴重安全漏洞，可直接開啟用戶 Mac 電腦上的攝影鏡頭，並自動將用戶加入任何視訊會議。

獨立資安研究者 Jonathan Leitschuh 發現 Zoom Mac 版應用程式存有極嚴重的 0-day 安全漏洞，任何網站都可利用這個漏洞，在用戶不知情的情形下，直接開啟 Mac 的攝影鏡頭，把用戶加入任一視訊會議之中。

更糟的是，Zoom 完全沒有告知用戶，其應用程式會在 Mac 上安裝一個在背景運作的網頁伺服器；即使用戶先前已將 Zoom 應用程式自 Mac 上移除，這個網頁伺服器也不會遭到移除，甚至還會自動重新安裝 Zoom 應用程式。

Letischuh 指出，這個漏洞會讓用戶的 Mac 陷入被 DoS 的風險之中，只要攻擊者持續發送大量 GET request 指令給 Zoom 秘密安裝的網頁伺服器，Zoom app 就會不斷向 MacOS 發出回到前景模式的要求，這樣就能有效阻斷用戶的正常操作。

Letischuh 在三月初發現這個漏洞後，立即向 Zoom 回報，但 Zoom 沒有立即處理，在一般公認的 90 天保密期中，也僅推出一個快速修補方案，但並沒有真正解決其安全問題。

在各大科技媒體這兩天廣泛報導後，Zoom 才推出緊急更新版本，完全移除隱藏版的網頁伺服器。

- 資料來源：

1. https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5
2. https://www.theverge.com/2019/7/8/20687014/zoom-security-flaw-video-conference-websites-hijack-mac-cameras
3. https://www.theverge.com/2019/7/9/20688113/zoom-apple-mac-patch-vulnerability-emergency-fix-web-server-remove
4. https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/

2.3.3 十五年前的惡意軟體 MyDoom，今日依然肆虐

十五年前誕生的 Email 惡意軟體 MyDoom，在十五年後的今天，仍然在網路上散布，繼續危害用戶。

據資安專家指出，於 2004 年出現的 Email 惡意軟體 MyDoom，在十五年後仍然在網路上自行散播感染。即使在 2019 年上半年，還是有近五十萬封夾帶 MyDoom 的惡意 Email 在網上流竄。

MyDoom 又名 Novarg、Mimail 或 Shimg，主要透過 Email 感染；受害電腦遭感染後會寄出更多夾帶 MyDoom 的垃圾信，有些變種也會透過區域網路散布。

MyDoom 在感染後會開啟 TCP 埠號 3127 到 3198 的後門，讓攻擊者能過遠端控制受害電腦，並進一步植入更多惡意軟體；某些變種也能用來發動 DoS 攻擊。

雖然已經過了十五年，但 MyDoom 在網路上的活動量不但沒有消失，甚至今年還有增加的趨勢，；目前受害者分布以美國和中國為主，科技業則是主要被攻擊的產業。

- 資料來源：
  1. https://blog.talosintelligence.com/2019/07/rats-and-stealers-rush-through-heavens.html
  2. https://www.bleepingcomputer.com/news/security/notorious-mydoom-worm-still-on-autopilot-after-15-years/

2.3.4 中國 Android 惡意軟體「狸貓換太子」，會將正版 App 替換成夾

資安研究人員發現一個來自中國的 Android 惡意軟體「史密斯探員」，會將用戶手機中的正版 App 偷換成會夾帶廣告詐騙機制的假 App，受害者已達兩千萬人。

資安公司 Check Point 指出，該公司發現一個來自中國廣州的 Android 惡意軟體，會將用戶手機中的各種正版 App 偷偷換成看起來很像，但是卻會暗中下載並點擊廣告的假 App。

這個被命名為「史密斯探員」（Agent Smith）的 Android 惡意軟體在 2018 年初首次出現，一開始只出現在 Adnroid 平台上一個稱為 9Apps 的第三方 App Store，但 Check Point 最近發現「史密斯探員」也出現在 Google 官方的 Play Store 平台中，已經發現有 11 支 App 內含該惡意軟體。

目前該惡意軟體的受害者已達兩千萬人左右，主要分布在印度、巴基斯坦與孟加拉；Check Point 擔心這

支惡意軟體侵入 Google Play Store 後，受害者會大幅增加。該公司估計目前新增的受害者已達一千萬名。

Check Point 也在第一時間通報 Google，目前 Google Play Store 已將確認感染的 App 下架，但 Android 用戶仍應提高警覺，因為類似的惡意軟體種類相當多。

- 資料來源：
  1. https://blog.checkpoint.com/2019/07/10/agent-smith-android-malware-mobile-phone-hack-virus-google/
  2. https://www.zdnet.com/article/new-android-malware-replaces-legitimate-apps-with-ad-infested-doppelgangers/

2.3.5 變種惡意軟體 TrickBooster 肆虐，已感染超過兩億五千萬組 Email 帳號

由 TrickBot 變種而來的新惡意軟體 TrickBooster 近來大舉肆虐，據估計已經感染超過兩億五千萬組 Email 帳號。

由三年前的 TrickBot 變種而來的惡意軟體 TrickBooster，近來在歐洲造成大量用戶遭感染，據估計受害者已超過兩億五千萬個 Email 帳號。

TrickBooster 係透過垃圾郵件擴散。用戶電腦感染後，TrickBooster 會取得用戶的 Email 帳密、通訊錄、收件匣和寄件匣，發送夾帶惡意軟體的垃圾信給通訊錄上的連絡人後，再刪除掉寄件備份和垃圾信箱，所以用

戶難以發現自己的 Email 被用來寄垃圾惡意信件。

資安研究單位追蹤到 TrickBooster 的控制伺服器，並且取回了存有駭侵記錄的資料庫；分析之後發現在兩億多個受害帳號中，有上百萬個 Email 屬於英國政府及其海內外附屬單位，包括英國國防部、外交部、大英國協相關單位、健保單位，還有多個英國地方政府與民意機關。

- 資料來源：
  1. https://www.governmentcomputing.com/security/digital-disruptions/trickbot-email-addresses-deep-instinct
  2. https://www.deepinstinct.com/2019/07/12/trickbooster-trickbots-email-based-infection-module/

2.4、 軟硬體漏洞資訊

2.4.1 微軟 Excel 存有遠端執行任意程式碼漏洞

微軟 Excel 被發現存有可被遠端執行任意程式碼的資安漏洞。

當 Excel 無法適當處理記憶體中的物件時，就可能遭駭客利用此漏洞進行攻擊。

如果當時被駭用戶以系統管理員權限登入，駭客即可取得系統管理權限，進行各種高階操作。

這個漏洞僅出現在特定版本的微軟 Excel，但作業系統則橫跨 Windows、RT 版和 Mac 版。駭客可以使用夾帶特定檔案或連結的釣魚信或即時訊息，引誘用戶點擊後開啟檔案，以進行攻擊。

- 影響產品：
  - Microsoft Excel 2010、2013、2016、2019 for Windows 32/64、RT、Mac
  - Office 365 ProPlus for 32/64 bit systems
- 解決方案：透過系統更新安裝修補程式
- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1110
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1110

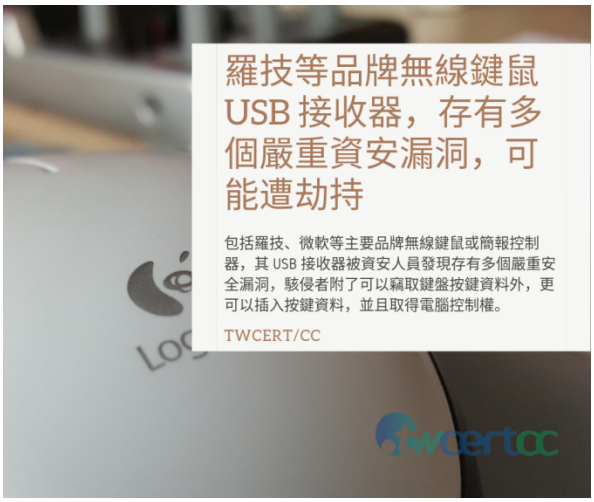
2.4.2 Windows Defender Application Control 安控機制可被跳過的漏洞

Windows Defender Application Control 存有一個可被駭侵者跳過的安全漏洞，使駭侵者能免於被 PowerShell 的安控機制阻擋。

駭侵者若想跳過 WDAC，必須先取得系統管理權限，且 PowerShell 係在 Constrained Language 模式下運作；這樣駭侵者便能跳過系統資安機制，取用系統資源。

- 影響產品(版本)：PowerShell Core 6.1、6.2
- 解決方案：安裝最新微軟安全更新程式
- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1167
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1167
  3. https://twitter.com/CVEnew/status/1152242978649444353

2.4.3 羅技等品牌無線鍵鼠 USB 接收器，存有多個嚴重資安漏洞，可能遭劫持



包括羅技、微軟等主要品牌無線鍵鼠或簡報控制器，其 USB 接收器被資安人員發現存有多個嚴重安全漏洞，駭侵者附了可以竊取鍵盤按鍵資料外，更可以插入按鍵資料，並且取得電腦控制權。

資安人員指出，這些漏洞也能讓駭客取得用於加密鍵鼠通訊的密鑰；甚至還能跳過阻擋不明鍵鼠連線的安全系統。

存有這些安全漏洞的裝置，包括羅技全系列使用「Unifying」USB 接收器的產品線；羅技自 2009 年起使用 Unifying USB 接收器於所有無線滑鼠、鍵盤、軌跡球、簡報控制器等周邊之上。

事實上，這個漏洞並非羅技產品獨有，只要是採用了相同的控制晶片的產品，都存有這個漏洞；受影響的品牌除羅技外，還包括 HP、Dell、Gigabyte、Lenovo、AmazonBasics、微軟的無線鍵鼠產品等；而且因為是硬體的安全漏洞，所以和作業系統無關，包括 Windows、OSX、Linux 等皆受影響。

目前僅有部分廠牌推出更新修補程式，建議以上廠牌無線鍵鼠用戶盡速更新，以免成為駭侵對象。

- 影響產品(版本)：羅技、HP、Dell、Gigabyte、Lenovo、AmazonBasics、微軟等多種無線

鍵鼠產品

- 解決方案：至各廠牌網站下載安裝更新修補程式

- 資料來源：
  1. https://www.bastille.net/research/vulnerabilities/mousejack/affected-devices?fbclid=IwAR2-XqecmMnE4SfV39NQBMUB68cG3opAQi6Lufu_BT66zh7HiUCmZNY3Smg
  2. https://www.zdnet.com/article/logitech-wireless-usb-dongles-vulnerable-to-new-hijacking-flaws/?fbclid=IwAR2lndtglgv4poJXZzC2p9URXqHNyeLdB6VEOGu9J2MsOsh7tPQfBY43Ec8
  3. https://www.theverge.com/2019/7/14/20692471/logitech-mousejack-wireless-usb-receiver-vulnerable-hack-hijack?fbclid=IwAR0vBhtQYrWsIcnTngnjl2nUg7nsequXBTFtBfeVIBvuNW4dKUa36SgzovE

第 3 章、 資安研討會及活動

2019 數位政府高峰會 _ Digital Government Summit 2019	
活動時間	2019/8/28（三） 09:00 - 16:40
活動地點	台北富邦國際會議中心 B2
活動網站	https://egov.ithome.com.tw/
活動概要	  數位政府高峰會將介紹外界最關心的換發數位身分識別證 (New eID) 最新規劃，說明依據智慧政府發展藍圖，在便捷生活、保障隱私、高安全性及資訊自主原則下，規劃發行數位身分識別證，將國民身分證結合自然人憑證，作為實體世界及網路身分之人別辨識之鑰匙，並說明 New eID 個資、資安保護作為及相關更便利、更安全、更自主、更加值之各項情境。本議程邀請內政部戶政司司長張琬宜蒞臨分享數位身分識別證 (New eID) 虛實整

	合之規劃方向。2019 數位政府高峰會，內容不僅多元且豐富，一同探討數位轉型浪潮下公務員應具備的新能力，一起參與推動政府進步創新的行列。

2019 CYBERSEC 101	
活動時間	2019/9/6(五)、9/20(五)、10/25(五)、11/8(五)、11/29(五)
活動地點	台北市松山區敦化南路一段 108 號 B2
活動網站	https://cybersec101.ithome.com.tw/
活動概要	 CYBERSEC 101 為全新系列研討會，藉由定期舉辦，持續對資安實務做更全面更深入的探討與交流，期能擴大 IT 與資安人員的資安視野，精進資安防禦技能，持續提升企業組織的資安防禦水平。 2019 年 CYBERSEC 101 資安實務研討會的第一場次，將以當前全球最受企業與政府矚目的「NIST Cybersecurity Framework」為主題，透過此一完整涵蓋企業五大防禦構面的資安藍圖，由資安專家帶領 IT 與資安人員，以每個月一個子題的節奏，依序探討 NIST Cybersecurity Framework 的五大資安防禦功能（Identify、Protect、Detect、Respond、Recover），完整檢視企業資安防禦的全貌，為企業資安防禦奠定持續改善的基礎。

新全民公敵—不實訊息	
活動時間	108 年 8 月 19 日（星期一）14 時至 17 時
活動地點	IEAT 會議中心 3F 第 1 會議室(臺北市中山區松江路 350 號 3 樓)
活動網站	https://twnic-icann.kktix.cc/events/108-5
活動概要	網路不實訊息所導致的社會不信任與分歧的負面現象，甚至對民主的干預，已經成為許多國家的擔憂。 以 5 月底甫結束的歐洲議會大選為例，為防止俄羅斯以不實資訊活動干擾選情，歐盟早在去年 12 月 5 日發布《對抗不實訊息行動方案》，從增加專業資源投資、建立即時預警系統、要求業者落實自律規範、提升大眾認知等 4 大方向著手。 國際間也有從訂立法律或擬訂政策以為因應的做法，例如在去年通過與實施的法國《打擊資訊操弄法案》、德國《網路執行法》（NetzDG）；以及今年 5 月通過的新加坡《防止網路虛假與操弄法案》等；這些做法中或從維護選舉公正性為出發點，也有從抑制網路仇恨言論散播的角度為立法初衷。 綜觀國際間防制不實訊息的不同做法，或可區分在短期間可奏效者包括從立法、平臺自律、或設立事實查核中心等；以及長期可收效的提升民眾媒體素養、健全媒體結構等。 本座談將聚焦於，釐清臺灣社會面對不實訊息帶來的威脅當中應優先處理的議題為何？針對優先處理議題，現有來自於政府與民間推動的措施是否足以因應？缺口為何？國際經驗中，又有哪些得以借鏡之處？ ● 主持人　胡元輝 教授（中正大學電訊傳播研究所） ● 與談人（※依姓氏筆畫排序） 何吉森 副教授（世新大學廣播電視電影學系） 沈伯洋 副會長（台灣人權促進會） 黃兆徽 經理（華視新聞部） 羅秉成 政委（行政院）

2019 NGO 資安種子講師培訓	
活動時間	2019/08/29(四) 09:00 - 2019/09/01(日) 17:00
活動地點	CLBC 德惠弐參 T23 / 10491 台北市中山區德惠街 23 號
活動網站	https://ocftw.kktix.cc/events/cscs2019tot
活動概要	 台灣擁有在國際間相當知名的開源社群，亦有著極為活躍的公民社會。為了促進這兩個社群之間的交流，開放文化基金會國際交流組與華人民主書院、台灣駭客協會、台灣人權促進會共四個組織共同開啟「CSCS 專案：Civil Society Cyber Shield」，讓社會運動與組織者能夠接觸最新的資安工具、對抗資安威脅，在安全的線上環境中推動社會議題。 同時，台灣身為亞洲少數高度民主的國家，更期許以豐厚的民主土壤培養跨國資安支援網絡，將高品質的資安培訓提供到亞洲各國活躍的更多社會運動者與高危險社群。 2017 年，在台灣舉辦「東亞及華人社群人權工作者資安隱私保護工作坊」，超過 14 國、50 位跨國參加者及多個國際組織共襄盛舉，開啟後續更多深度合作，後半年起並於東南亞數國舉辦數場資安培訓。 CSCS 社群由志工講師及台灣的公民團體代表組成，由 OCF 擔任活動的統籌祕書處，協助社群發展。

	● 課程大綱 如何向新手介紹資安？ 手機、電腦、線上通訊的安全性，如何教學？ 台灣公民團體（NGO）的資訊科技使用現狀 如何建立與公民團體（NGO）的合作關係 NGO 資安培訓實作經驗分享

第 4 章、 2019 年 7 月份事件通報概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資通報，以下為各項統計數據，分別為通報地區統計圖及通報類型統計圖。

通報地區統計圖為本中心所接獲之通報中，針對通報事件責任所屬地區之通報次數比率，如圖 1 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比率，如圖 2 所示。

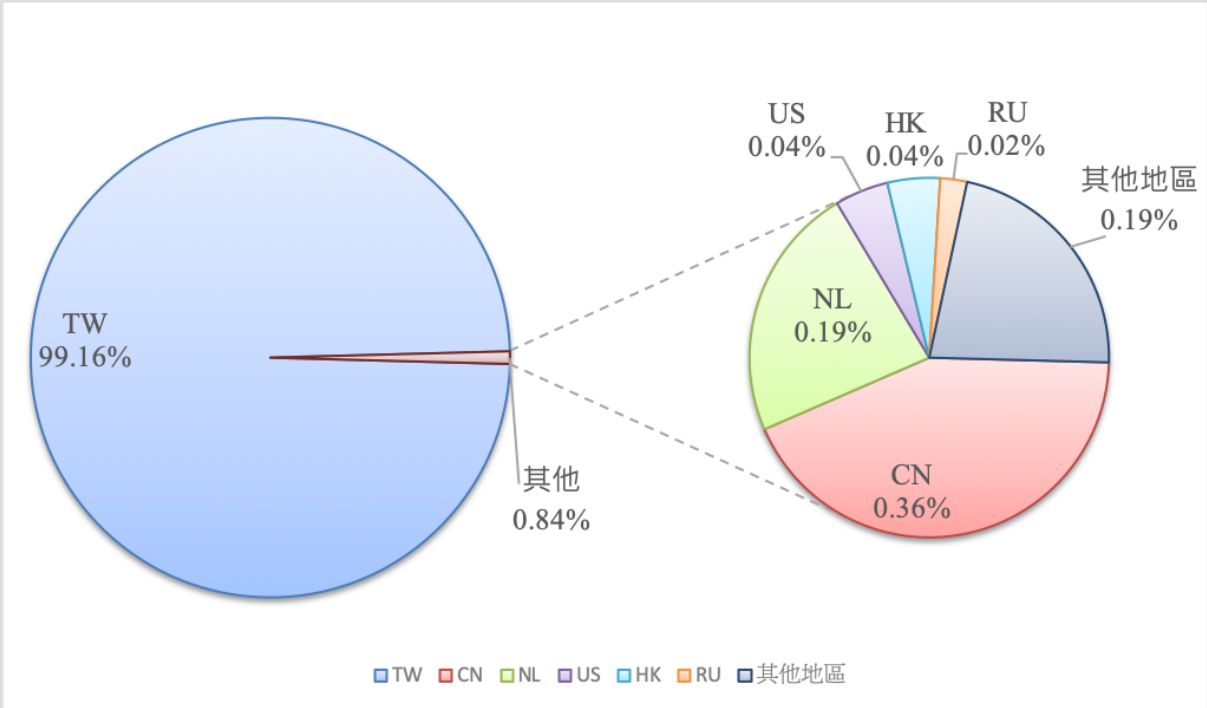


圖 1、通報地區統計圖

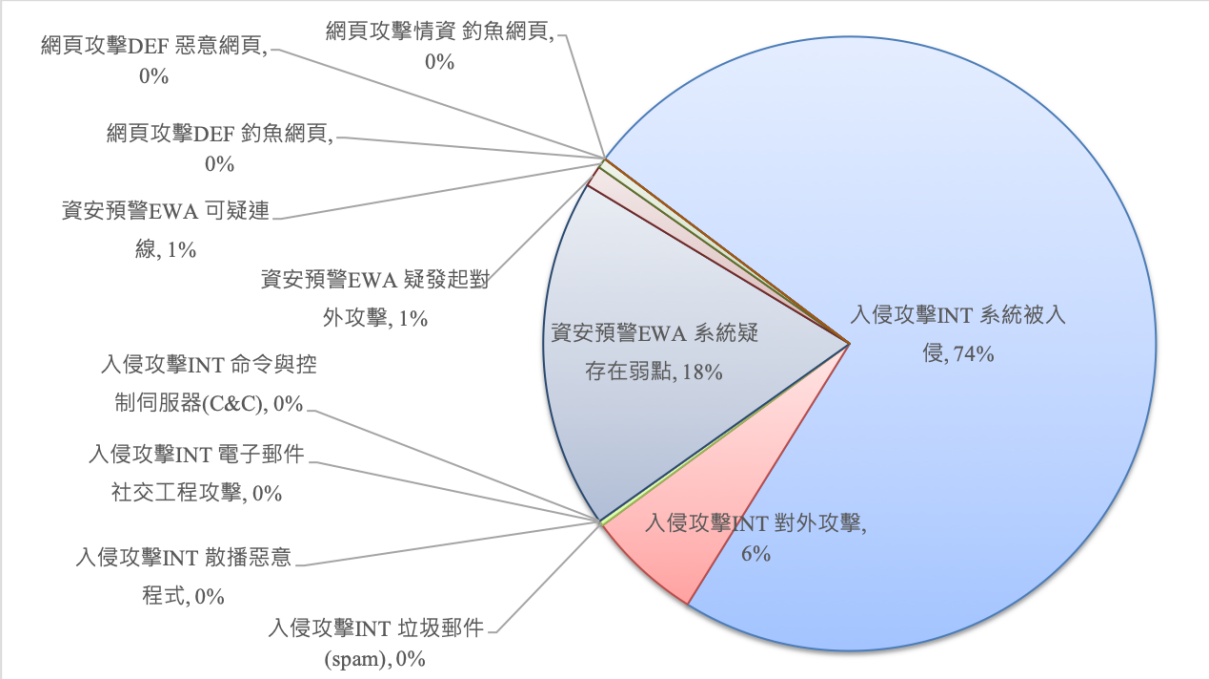

網頁攻擊DEF 惡意網頁, 0%
網頁攻擊情資 釣魚網頁, 0%
網頁攻擊DEF 釣魚網頁, 0%
資安預警EWA 可疑連線, 1%
資安預警EWA 疑發起對外攻擊, 1%
入侵攻擊INT 命令與控制伺服器(C&C), 0%
入侵攻擊INT 電子郵件社交工程攻擊, 0%
入侵攻擊INT 散播惡意程式, 0%
入侵攻擊INT 垃圾郵件(spam), 0%
資安預警EWA 系統疑存在弱點, 18%
入侵攻擊INT 系統被入侵, 74%
入侵攻擊INT 對外攻擊, 6%

圖 2、通報類型統計圖

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：2019 年 8 月 16 日

編輯：林克容、江奕昉、張洛瑀

服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官網：https://twcert.org.tw/

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

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

Twitter：@TWCERTCC