TWCERT/CC 資安情資電子報

2019 年 5 月份

目錄

第 1 章、 封面故事

遭 ShadowHammer 供應鏈攻擊的企業，不只一家

先前華碩遭 ShadowHammer 進行攻應鏈攻擊，導致其系統更新程式成為惡意軟體的散播工具；然而另外還有多家企業也是 ShadowHammer 的受害者。

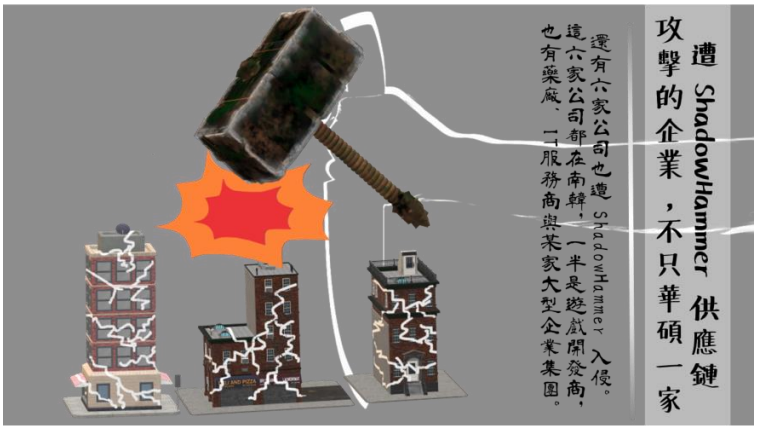
資安廠商卡巴斯基(Kaspersky)指出，除了先前遭到入侵的華碩之外，至少還有六家公司也遭到 Operation ShadowHammer 的入侵。

卡巴斯基在另外六個案例中觀測到和華碩案例十分接近的駭侵手法，包括利用多個有效的合法憑證以規避掃毒偵測，以及類似的複雜演算法。

這六家同遭感染的公司都在南韓，其中一半是遊戲開發商，另外也有藥廠、IT 服務商與某家大型企業集團。

專家同時指出，不排除有更多受害者的可能性；由於 ShadowHammer 攻擊的目標是企業後端的各種開發工具，還會將惡意程式碼注入經合法簽章的程式中，因此不但擴散力極強，還非常不容易發現。

- 資料來源：
  1. https://www.kaspersky.com/blog/details-shadow-hammer/26597/
  2. https://www.securityweek.com/kaspersky-links-shadowhammer-supply-chain-attack-shadowpad-hackers
  3. https://www.bleepingcomputer.com/news/security/shadowhammer-targets-multiple-companies-asus-just-one-of-them/



第 2 章、 資安宣導

Windows10 作業系統，下載新版讀卡機驅動程式仍可進行報稅作業

外接式讀卡機可能因為更換個人電腦、更換作業系統版本、或安裝修補軟體，導致原本可連線使用的讀卡機失效；若作業系統為 Windows10 與舊型讀卡機不合，提醒使用 Windows10 作業系統民眾，下載新版讀卡機驅動程式，仍可進行報稅作業，建議先至讀卡機廠商官網，下載安裝符合自己作業系統使用的讀卡機驅動程式，或洽詢讀卡機廠商技術服務專線。請從個人電腦裡選擇『開始 / 控制台 / 系統 / 硬體 / 裝置管理員』，確認是否有『智慧卡讀取裝置(或 Smart card reader)』，並查看讀取裝置是否有問號或驚嘆號，如有則表示未安裝成功，請將此裝置移除後再重新安裝驅動程式，重新安裝後再檢視讀卡機是否可正常使用，若仍無法使用或原廠已不支援新的驅動程式，則建議更換可與個人電腦系統環境相容的新讀卡機。

第 3 章、 資安小知識—Phishing

何謂 Phishing?

Phishing，又稱為網路釣魚，是一種有心人士透過偽裝、假冒真實的網頁，騙取受害者信任，進而達到獲取受害者個人資料、帳號密碼甚至信用卡資訊等行為。受害者可能會收到熟識的友人寄來的 email 或網址，讓使用者點選 email 或該網站，並且在受害者進入釣魚網站之後，要求使用者輸入個人的帳號密碼等資訊，就這樣將自己的資訊給了有心人士。

針對網路釣魚，又分為幾種技術—

1. 假冒網址：針對釣魚網站的網址幾個字元進行修改(1 與 l、0 與 O、m 與 rn...)，讓網址看起來容易被誤認為原本的網址，但其實已非使用者所欲前往之網站。例如 www.google.com，有心人士可將其改為 www.go0gle.com 或 www.g00gle.com，乍看之下似乎為正常網站，但實際上卻已落入假網站之陷阱中。
2. 網頁偽造：釣魚網站的排版、圖案、標示，與原本使用者所欲前往之網站極為相似或相同。因此，使用者若不小心連到假冒的釣魚網站，輸入登入之帳號密碼或個人資料，就會讓有心人士收集到受害者的個人資料。
3. 電話網釣：雖然稱作『網路釣魚』，但並非所有攻擊手法均需透過電腦完成。有心人士也可能透過電話致電到受害者家中或手機，表示自己是某家公司或銀行等受害者曾使用過的網站，並且告知受害者其帳戶有問題，要求受害者輸入或告知相關資訊。甚至有些電話網釣在撥通後，就會要求使用者鍵入自己之相關資訊，導致其個人資料和敏感資料之洩漏。而這些電話網釣，有些已不似過往會顯示『不明來電』等隱

蔽的電話系統，現已有使用假冒的相關資訊，降低受害者的戒心，進而達到更佳的詐騙率。

4. WiFi 免費熱點網釣：在人人都有智慧型手機的時代，到了咖啡廳、活動場地、甚至捷運等大眾運輸工具時，都會有免費的 WiFi 提供一般民眾連線。此時就會有駭客，開啟名稱相似相似/相同的熱點，例如台北常見的 Taipei Free 免費公共熱點，有心人士可能會於鄰近台北市的地區、將熱點名稱改為 TPE-Free，讓曾經使用該熱點的使用者，毫無戒心地使用了 TPE-Free 熱點。而此時，當受害者連入該假冒熱點，後續所瀏覽的網頁、填入的資訊、自己的帳號密碼、甚至信用卡資訊等重要資料的傳輸，若沒有經過 https 的加密，就會經由該熱點傳入網際網路，因此，有心人士只要攔截下使用者寄出之封包，便能查看裡面所有訊息，並且用於其他用途中。

☞HINT：

釣魚網站可以想做一家黑心公司，想要讓客人去到錯的店家、花費更多的錢去買類似的商品。

因此 (1)店家有可能將路上的路標進行更改，例如將鼎泰豐的名字改為頂太風，並且放置顯眼的路標，讓一般人信以為真並且前往了假冒的頂太風 (連結操控)。

(2)並且在受害者進入店家之後，其裝潢和網路上查到的照片相差無幾，除了價格的差別之外，菜單內容也和其他人士提供的一樣，因此受害者就會輕信這一家是真的鼎泰豐。並且店家可能將價格比真正店家提高之外，還可能要求受害者進行申辦會員卡或餐與優惠活動等，取得受害者資料、好進行後續的詐騙(網頁偽造)。

(3)確認會員資料過後，該假冒店家會在受害者用餐後幾天，致電給消費者，除了進行一般制式化的消費者滿意度調查以確保消費者下次的到訪外，還可能謊稱當初使用者刷的信用卡有問題，請使用者提供相關資料。而真的有前往該假冒店家用餐的使用者往往不疑有他，就將私人相關資訊

給了店家，而該店家便可以透過這些資訊做盜用、偽造、甚至轉賣個人資訊等用途賺上一筆 (電話網釣)。

(4)除此之外，該假冒店家可以告知消費者店裡有促銷活動，邀請消費者再次前往該店家用餐，並且在消費者前來之後，紀錄下消費者和友人的對話，便可以取得受害者談話中提到的個人訊息，例如交友狀況、生日、學歷、公司等資訊，甚至可以透過店家的誘導話術，取得更加隱密的其餘資訊，讓店家可以以此延伸詐騙該受害者相關人士，甚至販賣給其餘對個資有興趣之有心人士 (WiFi 免費熱點網釣)。

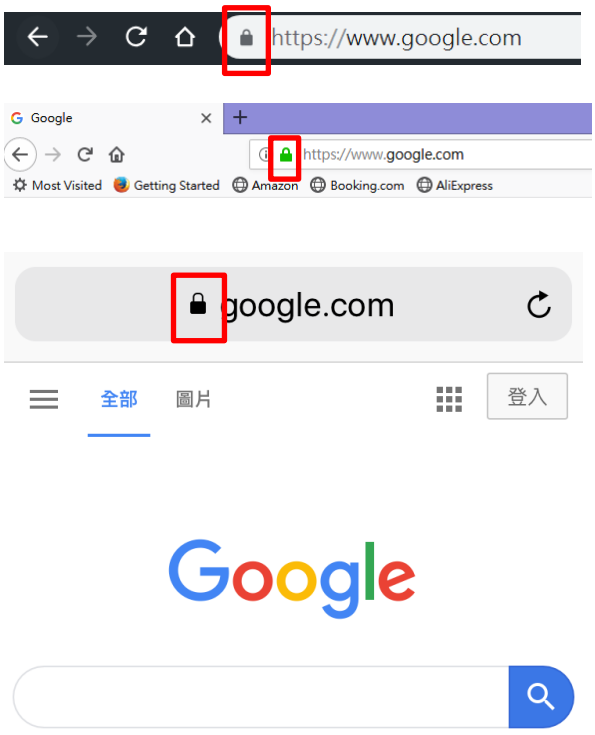
釣魚網站

在數種網路釣魚手法中，最為常見的非「網頁偽造」莫屬。亦即透過上述的技術，先製作出一假冒的相似網址，網站內不論是其色彩、放入之圖片、相關可使用之功能均與真正的網站相差無幾。甚至有些釣魚網站僅偽造首頁/登入頁，當受害者於假冒的首頁/登入頁鍵入私人資訊並登入後，釣魚網頁會將使用者導入真正的網頁，導致使用者因後續均使用真正網頁進行相關運作，因此對於被詐騙的事實毫無察覺。

當駭客架設釣魚網站後，接著可透過 Email、通訊軟體、社群媒體等方式進行散播，通知所有目標受害者宣傳釣魚網頁、誘使受害者點擊進入釣魚網站並登錄相關之個人資訊。此時，不僅僅因為受害者鍵入了自己的私人資料而導致個資的外洩，同時極有可能當受害者點擊了該網站，就使得電腦進行了惡意軟體的自動下載，使得電腦因此感染了惡意病毒等威脅。

對於一般人而言，釣魚網站的最簡單辨識方式可能是網址列上的鎖頭，有鎖頭代表著該網站的連線過程是有進行加密的，但是不代表這個網站是安全的。根據 Phishlab 於 2018/12 月的統計指出，大約有 49%的釣魚網站

一樣是有使用 https 進行加密。因此使用者也可以將滑鼠移到鎖頭上檢視，若該網站使用的憑證為公開且安全的，瀏覽器會告知使用者該網站的憑證是公開且安全的憑證，若顯示為不安全的憑證就有可能是釣魚網站，建議可經由 google 搜尋後進入該網站之官網，較容易避免進入釣魚網站。網站的安全性。



除此之外，有些有心人士本身還會自行偽造看似正常的網址列圖片，放置在網頁的頂端。即便該網站是假冒的釣魚網站，如此一來，其不僅是擁有看起來正常的鎖頭，該網站更是擁有一切正常的網址顯示。尤其是透過手機瀏覽網頁的使用者，由於手機本身有自動隱藏網址列的特性，因此對於有心人士而言，要偽造出一個讓使用者看的假網址列是非常簡單且不易被發現的事情。對於一般使用者看來，就跟正常網站並無二致，導致使用者將自己的個人資訊洩漏給釣魚網站。

小心防範釣魚網站

由於網路的發展逐漸往「簡單」、「方便」的方向發展，為了減少使用者的麻煩，網際網路上的協定和設計越來越簡潔，導致越來越容易產生的詐騙釣魚漏洞。但對於一般使用者而言，信任於網際網路給予的便利性，反而會疏於防範可能的危險，尤其是這些以假亂真的釣魚網站。因此，一般使用者須注意以下幾點，以防範落入釣魚網站的陷阱中。

1. 注意網域名稱：
   對一般使用者而言，最先能夠、也最需要注意的便是網址列上列出的網域名稱(網址)。雖然有心人士常常會用讓人容易產生混淆的網址，讓使用者在不注意的情況下落入陷阱，例如 www.twcert.org.tw 轉為 www.twecrt.org.tw 或 www.tw-cert.org.tw 等極為相近的網址。建議可以將常用的網站存成我的最愛，或是自己於網址列中輸入常用網址，都可以減少遇上釣魚網站的風險。

2. 不亂點擊來路不明的連結：
   一般使用者，在收到標題看起來聳動、吸引人，甚至看起來相識的人所寄之電子郵件或訊息時，都會因好奇心而點擊訊息中的網址連結。然而，這些通常標明「特價」、「贈品」、「公務聯繫」等訊息，多半都是利用人們的好奇心，引誘人點擊之後，蒐集個人資料之外，更有可能會讓電腦感染上惡意程式。由於 email 的寄件者是非常容易偽造的，因此看似正常的公務 email 訊息，也有可能是駭客假冒的釣魚信件，例如收到了 tw-cert@cert.org.tw 的訊息，或許看起來正常，但 tw-cert@cert.org.tw 不代表真的是由 cert 的人所發出的郵件，也曾經發生過有心人士透過假冒供應商的 email 寄信給公司業務承辦人員，要求承辦人員進行付款等作業並提供匯款帳戶作業。而處理該事

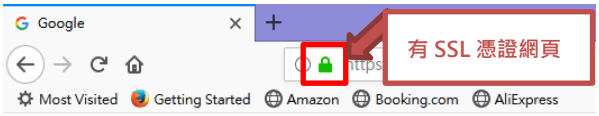
件的承辦人未仔細進行比對，因而將應付款項匯款置假帳戶中，直到合作廠商前來請款，承辦人才發現遭受有心人士詐騙。

3. 仔細觀察網站：

對於常用的網站，一般使用者就算未特別仔細觀察過，多少也會對該網站有所記憶。因此進入一網站時，可以先觀察該網站的狀況，查看是否有圖片或是字體等，和原本的網站是不同的，留心是否進入了釣魚網站，提高警覺。

4. 檢閱網站的安全鎖頭：

檢閱網址列上的網址旁是否有鎖頭出現。若該網頁沒有出現鎖頭、甚至出現了『不安全』字樣時，使用者就必須要特別注意，是否有可能落入釣魚網站。然而，正如前述所說，即便該網站有鎖頭，也不代表能夠完全信任該網站，因為鎖頭僅代表該網站有使用 HTTPS，而目前約有一半左右的釣魚網站同樣有使用 HTTPS，即便獲得了 SSL 憑證，也必須要小心進入了錯誤的釣魚網頁。



5. 安裝防毒軟體、定期更新系統：

除了以上的防範方式之外，本中心也建議使用者在電腦中安裝可信的防毒軟體或防火牆，許多防毒軟體同時都有內建惡意網頁、釣魚網頁的黑名單，當使用者連線到釣魚網頁時，防毒軟體會在瀏覽器上提出警告，同時，由於電腦系統的更新通常都是用以提升電腦的功能和防護力，因此建議定期更新電腦或手機系統，以取得最新、較為安全的作業系統，以免上了釣魚網站的當，讓電腦感染了惡意病毒，影響電腦正常的運作。

6. 定期更新瀏覽器：

現在主要的瀏覽器都有提供黑名單的功能，當使用者連線到有人通報過的釣魚網站或惡意網頁時，

都會再次提示使用者所連線之網頁可能為有問題之網頁，並再次確認是否要進行連線。

- 資料來源：

1. https://zh.wikipedia.org/wiki/%E9%92%93%E9%B1%BC%E5%BC%8F%E6%94%BB%E5%87%BB
2. https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https
3. https://chinese.engadget.com/2018/11/27/half-of-phishing-sites-now-show-as-secure/
4. https://www.inside.com.tw/article/16247-line-of-death
5. https://kknews.cc/zh-tw/tech/bxll58m.html

第 4 章、 國內外重要資安事件

4.1、資安趨勢

4.1.1 67% 的旅館網站，可能外洩房客訂房記錄與個人資料給第三方

研究指出，高達 67% 的旅館或飯店網站，會讓房客訂房記錄與個資外流；駭客甚至可以取消你的訂房。

資安公司賽門鐵克近日發表研究報告，指出 54 國、超過 1500 家以上的旅館或飯店，會將房客的訂房代碼分享給第三方廣告商或分析工具廠商；每個飯店網站都有隱私權政權，但無一提及上述行為。

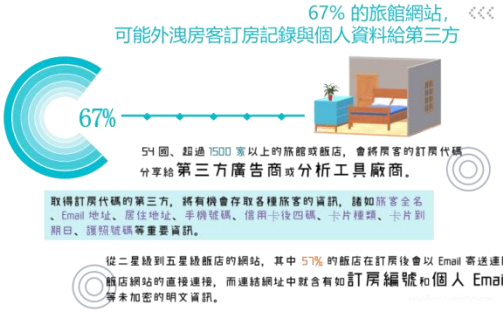
取得訂房代碼的第三方，將有機會存取各種旅客的資訊，諸如旅客全名、Email 地址、居住地址、手機號碼、信用卡後四碼、卡片種類、卡片到期日、護照號碼等重要資訊。

該報告針對從二星級到五星級飯店的網站進行廣泛測試，有些飯店隸屬於全球級連鎖飯店旗下，其中 57% 的飯店在訂房後會以 Email 寄送連回飯店網站的直接連接，而連結網址中就含有如訂房編號和個人 Email 等未加密的明文資訊。

而當旅客點擊連結開啟網頁時，平均會產生多達 176 個連線要求，許多連線要求是用以開啟各種第三方內容，例如廣告系統、社群分享工具或分析工具等等；這些工具往往可以藉此取得傳輸的資訊。

詳細可參考賽門鐵克報告全文。

- 資料來源：
  1. https://www.symantec.com/blogs/threat-intelligence/hotel-websites-leak-guest-data



3.1.2 英國政府：資料駭侵造成的企業損失，兩年來增加 41%

英國政府發表報告，針對 1500 家企業和 500 家非營利機構調查結果指出，因駭侵造成的資料外洩損失，兩年以來增加了 41%。

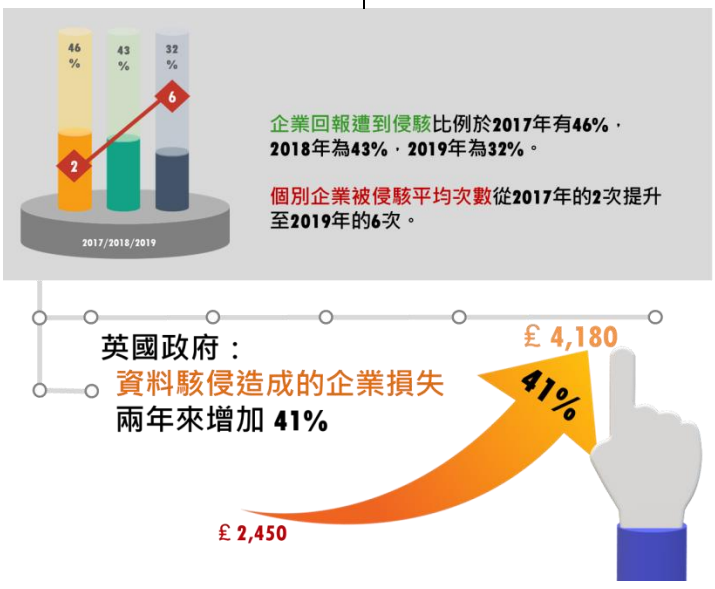
英國數位、文化、媒體與體育部（DCMS）日前發表年報，針對 1500 家大中小型企業與 500 家非營利組織，調查其資安意識與認知、資安布署情形，以及被駭侵的狀況、受影響程度等。

調查報告中有兩個重點：首先是受駭侵的企業家數較去年為少：2017 年有 46% 企業回報遭到駭侵，2018 年為 43%；2019 年的數字是 32%；但個別企業被駭平均次數則由 2017 年的 2 次提高到今年的 6 次。

其次，大多數企業均已針對 GDPR 的最新規範進行資安升級行動。

專家認為企業對資安的意識與防護行動正在逐漸提升，這可能是因為 GDPR 相關法令的嚴格規範所促成；另外駭侵行動本身也產生質變，攻擊行為逐漸集中在少數目標，而攻擊的強度也有所提升。

- 資料來源：
  1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF
  2. https://www.securityweek.com/cost-data-breach-uk-increases-more-41-two-years



3.1.3 LockerGoga 勒贖軟體分析

資安廠商 Securonix 發表研究報告，詳細解析造成全球鋁業大廠 Norsk Hydro 與其他企業近四千萬美元損失的勒贖軟體 LockerGoga，其感染途徑與運作流程。

據 Securonix 的研究報告指出，LockerGoga 為害對象是以企業內的 Windows 電腦 IT 與 OT（Operational Technology）系統為主；近期對挪威海德魯鋁業公司和其他受害企業造成的損失，約在三千五百萬到四千一百萬美金之間。

LockerGoga 的主要感染途徑，據研究指出很可能是透過夾帶惡意巨集的 MS Word 或 RTF 文件檔的釣魚郵件散布。

LockerGoga 內建多個發行商發行的合法數位簽章，因此能夠躲過某些惡意軟體入侵偵測系統；報告也指出某些 LockerGoga 的變體更包含了 taskkill 指令，能夠直接停止各種防毒防駭軟體的運作。

也有部分變體版本能夠刪除 Windows 內的事件記錄檔案。

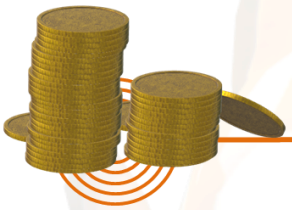
LockerGoga 也像其他惡意軟體一樣，能透過 SMB 在內部網路中尋找對象 Windows 電腦進行感染；甚至還能透過 Active Directory 在內部網路中大量散布。

一旦 Windows 電腦感染 LockerGoga 後，檔案系統內的 doc、.dot、.docx、.docb、.dotx、.wkb、.xlm、.xml、.xls、.xlsx、.xlt、.xltx、.xlsb、.xlw、.ppt、.pps、.pot、.ppsx、.pptx、.posx、.potx、.sldx、.pdf、.db、.sql、.cs、.ts、.js、py 等檔案，便會用勒贖軟體內建的 RSA-1024 公鑰來將檔案加密用的 AES-256 私鑰進行加密。遭加密的檔案其附檔名會被改為 .locked。

其餘的詳細流程可直接參考 Securonix 的研究報告。

- 資料來源：
  1. https://www.securonix.com/securonix-threat-research-detecting-lockergoga-targeted-it-ot-cyber-sabotage-ransomware-attacks/

LockerGoga 勒贖軟體分析



對受害企業造成的損失，約於
3,500萬至4,100萬之間。

LockerGoga 的主要感染途徑，據研究指出很可能是透過夾帶惡意巨集的 MS Word 或 RTF 文件的釣魚郵件散布。

Windows 電腦感染 LockerGoga 後，系統中的 doc、.dot、.docx、.docb、.dotx、.wkb、.xlm、.xml、.xls、.xlsx、.xlt、.xltx、.xlsb、.xlw、.ppt、.pps、.pot、.ppsx、.pptx、.posx、.potx、.sldx、.pdf、.db、.sql、.cs、.ts、.js、py 等文件，會被進行加密。

4.2、 國際政府組織資安資訊

3.2.1 汽車大廠 Toyota 五周以來兩度遭大規模駭侵

全球汽車生產大廠 Toyota 日前宣布其在日本的多家事業體遭到駭侵攻擊，這已經是五周以來該公司第二度遭大規模攻擊。

Toyota 指出，遭駭客攻擊的公司以其設於東京的銷售子公司為主，駭客侵入其資料庫，近三百一十萬名顧客資料遭到不當存取。

目前該公司正在調查這些資料是否外流且遭到濫用，Toyota 也指出這些資料並不包括客戶的財務資訊，但 Toyota 並未公布遭駭資料包括哪些項目。

此外，Toyota 在越南的子公司也在同一天表示該公司可能遭駭。

五周前 Toyota 澳洲分公司遭到更猛烈的駭侵攻擊，影響程度較本次事件更劇；該公司在澳洲的銷售活動遭到阻礙，甚至無法交車。資安專家懷疑主導這次駭侵行動的組織，極可能是來自越南的 APT32 (OceanLotos) 駭侵團體。有報導指出 APT32 目前集中鎖定全球大型車廠進行攻擊。

- 資料來源：
  1. https://www.infosecurity-magazine.com/news/toyota-japan-hacked-vietnam-office/
  2. https://www.zdnet.com/article/toyota-announces-second-security-breach-in-the-last-five-weeks/
  3. https://www.cyberscoop.com/apt32-ocean-lotus-vietnam-car-companies-hacked/

3.2.2 印度大型資訊服務外包業者遭駭，全球眾多客戶遭殃

印度大型資訊服務外包服務業者 Wipro 日前遭駭，更遭駭侵者用來攻擊其客戶。

規模大到可在紐約證交所上市的印度第三大資訊服務業者 Wipro，據信遭到疑似國家支持之駭侵行動攻擊，攻擊對象為 Wipro 的客戶。

資安專業媒體 KrebsOnSecurity 收到兩個可信賴的獨立消息來源於本月初指稱，Wipro 已經連續數月遭駭侵攻擊。攻擊者利用 Wipro 的服務系統，對其客戶發送釣魚信件；被攻擊的 Wipro 客戶多達十多家；但目前並不清楚到底是哪些 Wipro 客戶遭到攻擊。

消息來源也指出 Wipro 本身的郵件系統已遭駭客攻破，Wirpo 正在發展全新的私密郵件系統提供給其客戶使用。

Wipro 在全球只有十七萬名員工，服務對象遍及六大洲，亦包括多家財星五百大企業，行業範圍遍及醫療、金融、電信等產業。2018 年該公司的營業額突破八十億美金。

- 資料來源：
  1. https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/
  2. https://tech.economictimes.indiatimes.com/news/corporate/wipro-it-systems-may-have-been-hacked-and-used-to-attack-its-clients-report/68899479

4.3、 社群媒體資安近況

3.3.1 Facebook 偷偷承認：數百萬 Instagram 用戶密碼，亦以明文儲存

Facebook 再爆重大資安缺失，以明文儲存上百萬 Instagram 用戶的密碼。

上周 Facebook 再度傳出醜聞級重大資安缺失。Facebook 悄悄於美國復活節假期前夕，在一篇一個月前刊登於官方部落格的舊文中加上更新，指出經調查後他們也發現有數百萬 Instagram 用戶的密碼係以明文儲存。

Facebook 上個月才爆發以明文儲存眾多用戶密碼，同時在註冊時竟向用戶索取 Email 帳密的各種資安缺失；本周再度出現將 IG 密碼以明文儲存的問題。

Facebook 發布此事的時機與管道也令許多人質疑：FB 選在周五下午美股收盤後發布，避免負面消息影響隔周開盤股價表現的意圖十分明顯。媒體也指出 Facebook 經常在重要假日前夕發布負面消息，IG 密碼以明文儲存這樣的重大消息，更只用幾句話更新在舊文中，顯然有意逃避社會大眾的注意力。

- 資料來源：
  1. https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/
  2. https://edition.cnn.com/2019/04/18/tech/facebook-news-dump/

3.3.2 盜版《權力遊戲：冰與火之歌》等熱門影集，成為駭侵攻擊最佳誘餌

HBO 的《權力遊戲：冰與火之歌》最新一季掀起收視熱潮，然而不在播送區域內的全球眾多追劇網友，很可能因此成為駭侵攻擊的對象。

德國資安廠商 Zscaler 資安專家 Christopher Louie 指出，駭客可以利用像 HBO《權力遊戲：冰與火之歌》之類能帶動全球追劇風潮的熱門影集或電影，在追劇迷下載盜版內容時，同時誘使用戶下載安裝惡意軟體。

舉例來說，許多像《權力遊戲：冰與火之歌》之類的精彩影視作品，未在第一時間於全球播送；許多急著觀影的影迷，只好透過非法下載、盜版線上影音網站或 P2P 檔案分享服務來追劇。

駭侵者可以在這些網站中植入惡意軟體，攻擊用戶的瀏覽器，或是讓用戶下載打不開的影片檔，再誘騙用戶下載實際上是駭侵軟體的「專屬影片解碼器」。這樣可以輕鬆駭入大量追劇用戶的電腦或手機。

過去發生的案例中，甚至連字幕檔也可以用來攻擊系統漏洞，植入挖礦程式讓用戶幫駭客賺取加密貨幣。

- 資料來源：
  1. https://www.zscaler.de/blogs/corporate/malware-authors-have-already-won-iron-throne

4.4、行動裝置資安訊息

3.4.1WiFi 分享軟體驚傳洩漏兩百萬組連線密碼

一個廣受歡迎的 Android WiFi 熱點搜尋連線 App，被資安專家發現其連線密碼資料庫沒有任何安全措施，可任人隨意取用。

資安專家 Sanyam Jain 向科技媒體 TechCrunch 透露，一支廣受歡迎的 Android WiFi 熱點搜尋連線 App，其存有兩百萬組 WiFi 連線密碼的資料庫，竟然沒有加上任何防護措施，任何人均可自由存取，並且打包下載。

這支名為 WiFi Finder 的 Android App，疑似由中國團隊開發；在 Google Play Store 上已有超過十萬次下載，目前仍在架上。

該 App 雖然強調儲存的都是可供公眾使用的 WiFi 熱點，但實際檢視資料庫內容後發現，該資料庫也包含許多家用或私人 WiFi 路由器密碼。

專家指出，攻擊者可以透過這些密碼進入內網，進一步設法修改路由器的設定，將該區網的用戶導向至惡意網站，或是竊聽網路封包內容，進一步竊取帳密等各種資訊。

TechCrunch 試圖連絡 App 開發者，但均無回音；存放該筆資料庫的雲端服務廠商 DigitalOcean 已將此資料庫自網路上撤下。

- 資料來源：
  1. https://techcrunch.com/2019/04/22/hotspot-password-leak/

3.4.2Apple 自 App Store 中移除多支濫用企業布署機制的 App

Apple 先前移除多支家長控制 App，遭開發商抗議；Apple 發表聲明，指出這些 App 濫用企業 App 布署機制，可能造成隱私與資安問題。

Apple 日前於其 App Store 中移除多支家長控制 App。這些 App 的用途多半集中在讓家長控制子女使用 iOS 設備的時間與上網權限，並檢視使用記錄。

Apple 的下架行動遭開發商抗議，其中卡巴斯基更對 Apple 發動法律戰，在俄羅斯以反托拉斯法的罪名將 Apple 告上法院，認為 Apple 移除其 App，是為了保護自己在 iOS 中的相近功能，因而濫用其平台壟斷地位。

Apple 則在官網發表公告，說明移除這些 App 的原因，在於這批 App 違反了開發者協議，使用了 MDM 企業布署機制；這可能造成用戶的隱私與資安問題。

Apple 表示，MDM 機制是 Apple 提供給企業開發其內部 App 與管理企業用 iOS 設備的架構，管理者可以管理並監控企業內部的 iOS 設備與其使用情形：「MDM 提供第三方控制並存取裝置及其最敏感的資訊，包括使用者位置、app 使用、電子郵件帳戶、相機權限和瀏覽歷史記錄。」

Apple 在聲明中也說：「父母不應該因為擔心孩子使用裝置的狀況而需要承擔隱私和安全的風險，App Store 也不應該成為強迫接受這種選擇的平台。除了你以外，沒有人可以無限制地存取管理你孩子的裝置」。

- 資料來源：
  1. https://www.apple.com/tw/newsroom/2019/04/the-facts-about-parental-control-apps/
  2. https://www.infosecurity-magazine.com/news/apple-parental-control-apps-1/
  3. https://www.kaspersky.com/blog/apple-fas-complaint/26017/

3.4.3 iOS 版 Chrome 瀏覽器的程式錯誤，可能導致眾多 iPhone 用戶遭駭

資安專家警告，一個 iOS 版 Chrome 瀏覽器的程式錯誤，可能導致近五億 iPhone 或 iPad 用戶遭惡意廣告攻擊。

資安專家 Eliya Stein 指出，一個被稱為 eGobblers 的駭侵團體，可能利用 iOS 版 Chrome 瀏覽器尚未修補的程式錯誤，讓 iOS 用戶在瀏覽到惡意廣告時遭到駭侵攻擊。

Stein 的專文表示，當用戶瀏覽到惡意網頁時，會突然被導向到另一個廣告頁面，或是跳出一個無法關閉的廣告頁面；這些頁面看起來和大品牌的廣告無異，但實際上暗藏惡意軟體。

由於 Chrome 的軟體錯誤，該惡意軟體將可以跳過 iOS 系統的沙盒限制，並且劫持用戶的瀏覽 session。報導指稱這波攻擊主要針對美洲的 iOS 用戶，但在歐洲也觀察到駭侵事件。

也有其他資安公司指出，不只是 iOS 版 Chrome 易遭攻擊，甚至連 iOS 內建的預設瀏覽器 Safari 也可能遭駭；這使得潛在的受害層面大大擴及幾乎每一支 iOS 設備。

ThreatPost 的專文詳細描述了該駭侵攻擊的細節。

- 資料來源：
  1. https://blog.confiant.com/massive-egobbler-malvertising-campaign-leverages-chrome-vulnerability-to-target-ios-users-a534b95a037f
  2. https://threatpost.com/easter-attack-apple-ios/143901/

3.4.4 內藏詐騙廣告機制，中國大型開發者 App 遭 Google 大批移除

中國大型 App 開發商 Do Global 有 46 支 App，因內含詐騙廣告機制，遭 Google 自 Play Store 中下架。

由中國網路巨人百度公司持股 34% 的 App 軟體公司 Do Global，遭美國媒體 Buzzfeed News 踢爆，其開發的多支 Android App 內含惡意廣告詐騙機制；Google Play Store 隨即祭出鐵腕，將該公司上架的 46 支 App 下架。

Google 除了將這些 App 下架外，也將 Do Global 自旗下的 AdMob 廣告聯播網中除名，因此該公司未來也無法自 Google AdMob 廣告播放中獲利。

資安廠商 Check Point 先前發現六支來自 Do Global 的 Android App，內含詐騙廣告機制；即使用戶沒有開啟 App，這些 App 也會暗中點擊廣告。這不但造成用戶手機連線費用增加、電力下降、速度變慢、手機升溫、提高故障率，更造成 Google 在廣告刊登費用的巨額損失。

據報導，Do Global 在 Play Store 中上架了近百支各式 App，每月活躍用戶超過兩億五千萬人，總下載次數超過六億次；但調查發現並非每支 App 都標示為 Do Global 發行。有些 App 標示為其他開發者發行，這也增加調查難度。

- 資料來源：
  1. https://research.checkpoint.com/preamo-a-clicker-campaign-found-on-google-play/
  2. https://www.buzzfeednews.com/article/craigsilverman/google-ban-play-store-do-global-baidu

3.4.5 多支 Android App 內含廣告軟體，大量耗電並用光連線頻寬

資安廠商發現多達 50 支 Google Play Store 中的 Android App 暗藏廣告軟體，不但破壞用戶體驗，更會造成電力或可用上網額度快速耗盡等問題。

資安廠商 Avast 發表研究報告指出，該公司在 Google Play Store 中發現至少 50 支各式 Android App，內含有問題的廣告軟體，會造成用戶各種困擾。

一但用戶安裝了這些 App，不但手機經常會自動跳出全螢幕廣告，還會要求用戶點按安裝特定 App；而用戶的手機速度會明顯變慢，電池電力會快速耗盡，可用上網額度也會被占用；對沒有上網吃到飽的用戶來說，可能造成上網費用暴增。

據 Avast 統計，這些 App 個別下載量從五千次到五百萬次不等，整體下載量可能超過三千萬次；而 App 所屬領域相當多元，從小遊戲、健身、相片編修、音樂等都有。目前多數廣告 App 均已遭下架。

由於這些 Android App 都曾在 Google Play 合法上架，因此用戶難以

識別；Avast 建議 Android 手機用戶應該安裝值得信任的防毒軟體，在下載前也應先仔細閱讀 App 說明與用戶意見回饋。類似的不良 App 應會有用戶提供負面反應，只要細讀即可察覺。另外對於要求過多權限的 App，也應提高警覺。

- 資料來源：
  1. https://blog.avast.com/adware-plagues-google-play
  2. https://docs.google.com/spreadsheets/d/1T2zy8lTtkYj45psdTyOZw6GVe1WI7LQuU8k42tHeiuM/edit#gid=1186582891

3.4.6 新發現的高通晶片設計瑕疵，可能導致眾多 Android 裝置面臨密鑰外洩風險

新發現的高通（Qualcomm）手機晶片設計瑕疵，讓駭客得以取得存在晶片中的加密密鑰。Android 手機機用戶請盡速更新系統。

資安研究單位 NCC Group 的研究員 Keegan Ryan 近日發表研究報告，指出高通的手機晶片由於設計瑕疵，駭侵者可用其分支預測與快取中取得資訊，並且據以解開儲存於晶片中的 224、256 位元 ECDSA 加密密鑰。

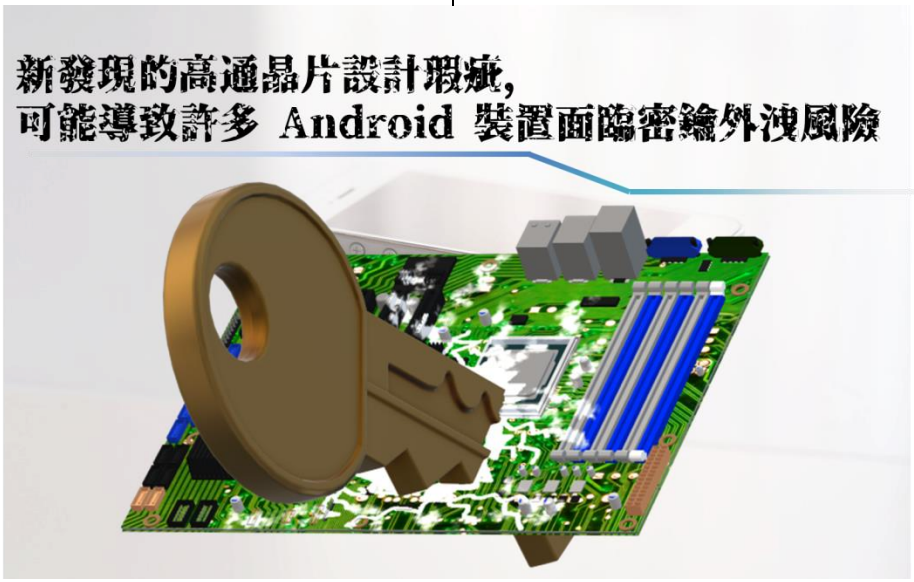
研究報告稱一供有 36 種高通手機晶片有此安全問題，包括廣泛使用在各型熱銷 Android 手機中的 SnapDragon 820、835、845 與 855 型晶片。

採用這些晶片的市場熱銷手機包

括 Samsung Galaxy 系列、Sony Xperia 系列、小米 Mi 系列和 LG V50、中興 Axon 等。

Qualcomm 在今年四月時針對此漏洞推出修補程式，而 Google 隨後也發表 Android 系統更新；然而各廠家推出針對旗下 Android 手機系統更新軟體的進度不一，有些較舊手機甚至完全無法更新。建議 Android 手機用戶盡可能安裝最新版作業系統。

- 資料來源：
  1. https://www.nccgroup.trust/us/our-research/private-key-extraction-qualcomm-keystore/
  2. https://threatpost.com/qualcomm-critical-flaw-private-keys-android/144112/
  3. https://www.qualcomm.com/company/product-security/bulletins



3.4.7 義大利公司疑似散布間諜軟體，Google Play 緊急下架二十五支 App

Google Play 日前緊急移除二十五支 App，這些 App 遭到一支被稱為 Exodus 的間諜軟體感染；資安研究單位指散布該 App 的是一家名稱 eSurv 的義大利公司，而該公司亦承包義大利政府標案，目前正接受司法調查。

非營利資安研究單位「無邊界安全」（Security Without Borders）指出，

這些 App 偽裝成義大利各電信業者的服務用軟體。

一旦感染後，手機中的各種資訊，包括 IMEI、手機號碼、安裝的 App 清單、撥號與通聯記錄、簡訊內容、手機所在地的座標、網頁瀏覽記錄、行事曆中的行程、通訊錄等敏感個資都會遭到不當存取。

無邊界安全同時指出，Exodus 可能已經感染數百到上千支 Android 手機。

散布該 App 的義大利公司 eSurv 的主要業務是錄影監視系統、無人機監視、面孔與車牌辨識等安保範圍；在此事遭揭發後 eSurv 的網站即無法讀取，該公司的多個社群帳號亦被清空。

那不勒斯的義大利檢調單位已針對此案展開調查行動。報導指出，三星期前 eSurv 的辦公室即遭到搜索，所有可疑電腦設備均遭調查單位查扣。

- 資料來源：
  1. https://securitywithoutborders.org/blog/2019/03/29/exodus.html
  2. https://threatpost.com/google-play-boots-italian-spyware-apps-that-infected-hundreds/143308/
  3. https://www.securityweek.com/exodus-android-spyware-possible-links-italian-government-analyzed
  4. https://www.vice.com/en_us/article/eveeq4/prosecutors-investigation-esurv-exodus-malware-on-google-play-store

4.5、 軟體系統資安議題

3.5.1 最新 WiFi 加密標準 WPA3 存有安全漏洞，攻擊者可取得密碼

研究報告指出，最新的 WiFi 加密標準 WPA3 仍存有安全漏洞，駭客可藉以取得無線網路的加密密碼。

由資安專家 Mathy Vanhoef 和 Eyal Roene 發表的研究報告指出，最新的 WPA3 無網網路加密協定，仍然存有一系列的安全漏洞；駭客可以透過這些漏洞取得無線網路密碼。

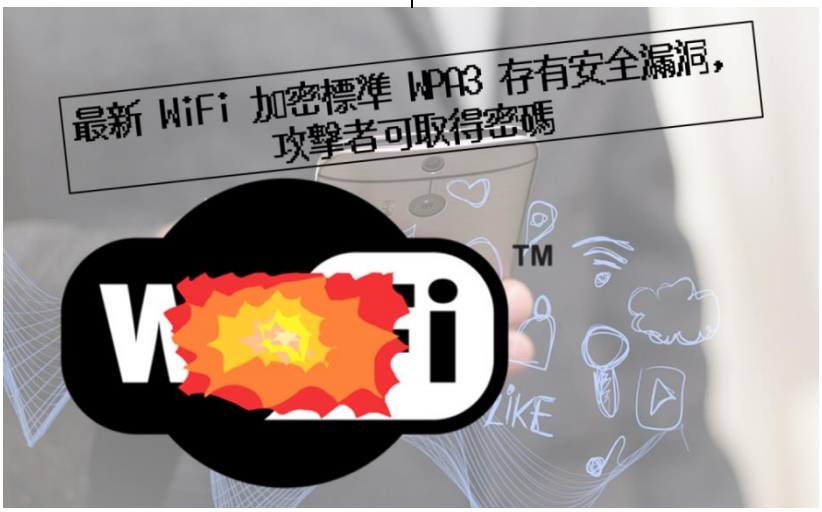
報告指出，推出才一年的 WPA3，當初是為了補強 WPA2 的弱點而推出，例如離線字典攻擊與前向保密（Forward secrecy）；然而 WPA3 本身也有一些設計缺陷。

該報告透過理論分析與實際模擬，指出駭客可以利用時間差或鄰近頻道的快取攻擊來取得 WiFi 密碼。

報告也指出，他們找到的安全漏洞，能夠以非常簡單的軟體更新加以解決。

詳細的漏洞分析與攻擊模擬結果，可參照報告原文。

- 資料來源：
  1. https://papers.mathyvanhoef.com/dragonblood.pdf
  2. https://www.computing.co.uk/ctg/news/3074010/security-flaws-in-wpa3-allow-attackers-to-hack-passwords



3.5.2 駭侵組織鎖定 D-Link、TOTOLINK 等家用路由器進行 DNS 劫持

近三個月來有駭侵團體鎖定家用路由器進行 DNS 劫持攻擊，遭入侵的多為 D-Link 和 TOTOLINK 的產品，總數接近兩萬台。

資安公司 Bad Packets 指出，該公司自去年十二月起觀察到至少三波大規模家用路由器劫持攻擊事件，而攻擊行動目前仍持續進行中。

駭侵團體透過路由器韌體的安全漏洞，竄改路由器的 DNS 伺服器設定，將用戶的網路連線導向至假的 DNS 伺服器，以讓用戶進入假網站，誘使用戶輸入帳號密碼或其他重要資訊。

據報導，受害者會被導至的假網站包括 Netflix、Google、PayPal 等，以及巴西多家銀行的官方網站。

目前已知受害的路由器廠牌型號與受感染台數分列如下：

- D-Link DSL-2640B - 14,327
- D-Link DSL-2740R - 379
- D-Link DSL-2780B - 0
- D-Link DSL-526B - 7
- ARG-W4 ADSL routers - 0
- DSLink 260E routers - 7
- Secutech routers - 17
- TOTOLINK routers - 2,265

如果你發現自己的路由器 DNS 被設定為以下四個 IP 之一，請立即更正，並儘快更新路由器韌體。

- 66.70.173.48
- 144.217.191.145
- 195.128.126.165
- 195.128.124.131

- 資料來源：
  1. https://badpackets.net/ongoing-dns-hijacking-campaign-targeting-consumer-routers/
  2. https://twitter.com/stefant/status/1114190053226549248
  3. https://en.wikipedia.org/wiki/DNSChanger
  4. https://www.zdnet.com/article/hacker-group-has-been-hijacking-dns-traffic-on-d-link-routers-for-three-months/#ftag=RSS-03-10aaa0a

3.5.3 Windows 7 更新後無法啟動，微軟暫停對 Sophos 防毒用戶推送四月分更新

微軟暫停推送本月的 Windows 7 與 Windows 8.1 更新給 Sophos 防毒軟體用戶，因為有眾多用戶回報更新後電腦即無法啟動。

發生更新後無法啟動問題的，主要是在 Windows 7 和 Windows 8.1 上安裝 Sophos Endpoint Security and Control 以及 Sophos Central Endpoint Standard/Advanced 防毒軟體的電腦；同樣的問題也出現在 Windows Server 2008 R2 和 Windows Server 2012 之上。

微軟在周二推送了四月分的軟體更新，主要解決的問題包括 KB4493467、KB4493446、KB4493448、KB4493472、KB4493450 和 KB4493451。

Sophos 已經對其用戶發出通知，暫勿安裝微軟四月份系統更新；已經安裝且發生問題的用戶，可以用安全模式啟動電腦後關閉 Sophos 防毒並移除更新程式，就能再度啟動 Windows 並重新啟用 Sophos 防毒。

其他消息來源指出，Avast 防毒同樣受這次更新影響，但微軟尚未確認。

- 資料來源：
  1. https://community.sophos.com/kb/en-us/133945
  2. https://www.zdnet.com/article/windows-7-problems-microsoft-blocks-april-updates-to-systems-at-risk-of-freezing/

3.5.4 微軟推出 Tamper Protection 新功能，防止惡意軟體關閉掃毒

微軟公司在其防毒產品 Microsoft Defender Advenced Threat Protection 中新增「Tamper Protection」功能，可預防惡意軟體試圖關閉系統的資安監測功能。

有許多惡意軟體會試圖關閉作業系統上運作中的駭侵監控功能，例如有個叫做 DoubleAgent 的惡意軟體，會搜尋並關閉諸如 Avast, AVG、Avira、Bitdefender、Trend Micro、Comodo、ESET、F-Secure、Kaspersky、Malwarebytes、McAfee、Panda、Norton 等知名防毒軟體。

微軟新推出的 Tamper Protection 功能，會在其防駭系統中新增一個稱為「Tampert Protectoion」的選項；開啟後即可防止惡意軟體修改系統核心設定，避免駭侵監控功能遭到關閉。

微軟表示，啟用該功能後，系統駭侵監視功能被關閉的機會將會大幅降低。

該功能也會防止惡意軟體試圖刪除已安裝的安全更新修補程式，並阻止惡意軟體關閉微軟的雲端防駭監控功能。微軟認為這樣能大幅減少系統被 0-day 惡意軟體攻擊的風險。

這項新功能目前仍在測試，未來

正式推出的日期未定。

- 資料來源：
  1. https://techcommunity.microsoft.com/t5/Windows-Defender-ATP/Tamper-protection-in-Microsoft-Defender-ATP/ba-p/389571
  2. https://www.zdnet.com/article/windows-security-microsoft-defender-av-can-now-stop-malware-from-disabling-it/

3.5.4 微軟客服帳號遭駭，Outlook、Hotmail、MSN 等雲端郵件內容可能外洩

微軟承認由於客服管理用帳號密碼遭駭客取得，包括 Outlook.com、MSN 和 Hotmail 等非企業用郵件帳號，可能遭到不當存取。

TechCrunch 日前報導，擁有近七億七千三百萬個郵件帳號的微軟雲端郵件服務，其客服管理工具的帳號密碼遭駭客取得，造成眾多郵件用戶面臨郵件內容和敏感訊息外洩的風險。

微軟表示，可能外洩的資料類型，包括 Email 地址、資料夾名稱、Email 主旨、通訊對象的 Email 地址或連絡人名稱；微軟說約有 6% 的上述雲端郵件用戶可能遭駭，微軟也已分別寄出通知信信給這些用戶。

微軟否認 Email 內容和附加檔案被駭侵的可能性，但資訊新聞網站 Motherboard 報導說他們收到匿名人士提供管理工具各種功能的螢幕截圖，顯示駭客可以透過該工具取得郵件內

文。

這起駭侵事件發生於今年一月一日至三月二十八日，微軟表示已經停用被取得的管理工具帳號；不過各界對微軟的風控漏洞多所指責，更有不少聲音批評微軟竟然能夠以內部工具存取客戶的郵件內容，簡直不可思議。

- 資料來源：
  1. https://techcrunch.com/2019/04/13/microsoft-support-agent-email-hack/
  2. https://www.vice.com/en_us/article/ywyz3x/hackers-could-read-your-hotmail-msn-outlook-microsoft-customer-support

3.5.6 挖礦蠕蟲「Beapy」對亞洲企業造成嚴重威脅

Symantec 資安研究人員發現一支全新的惡意挖礦蠕蟲「Beapy」，正對亞洲各國的企業造成嚴重威脅，特別是中國境內企業受害最深。

這支前所未見的惡意挖礦軟體，係透過釣魚郵件進行散播；一但成功感染，就會透過已知的兩個 Windows 漏洞 EternalBlue 與 DoublePulsar，對感染者的內網發動大規模攻擊，利用受感染電腦進行挖礦。

被這類挖礦蠕蟲感染的電腦，除了速度會變慢，造成使用者生產力下降外，也容易因為過熱導致系統提前損壞，造成企業電費和 IT 維護支出增加；如果感染的是雲端主機，雲端的使用費也會增加，更有可能造成重要

資料外洩。

據 Symantec 觀察，Beapy 主要感染對象 98% 都是企業設備；受害者以中國企業最多，占 83%，次多的是日本與南韓企業，台灣企業也有 2% 左右遭駭。

- 資料來源：
  1. https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china
  2. https://www.scmagazine.com/home/security-news/new-cryptomining-worm-beapy-targets-asian-enterprises-while-ignoring-consumers/

第 5 章、 資安研討會及活動

「網路社群與數位合作」專家座談會	
活動時間	2019/5/13
活動地點	IEAT 會議中心 8F 國貿講堂
活動網站	https://twnic-icann.kktix.cc/events/108-3
活動概要	全球社會在數位時代中面臨了如安全、公平、道德和人權等問題，而當前的國際合作方式與合作程度仍不足以因應這些挑戰。國內外的社群成員面對這些新的科技發展議題衝擊時所形成的意見與想法也需要表達及參與討論的管道。在多方利害關係人的模式下，鼓勵各個層面的利害關係人積極參與網路治理議題的討論，即為促進利害關係人合作、瞭解相關議題，並建立對議題共識的方法之一，本次座談旨在鼓勵臺灣的網路社群作為利害關係人，一同探討國內科技發展、數位發展以及需要優先行動的領域所產生的議題。 藉由提出議題，與相關領域（學界、網路組織、公民社會等）之其他利害關係人代表交換數位科技發展情形、可協同合作的形式等方面的意見，幫助臺灣的網路社群瞭解國內網路公共政策議題可能的影響，同時提升對數位合作相關議題的認知。 

TANET 2019 - 臺灣網際網路研討會 資訊展望 X 5 新啟航	
活動時間	2019/9/25 – 2019/9/27
活動地點	高雄國際會議中心
活動網站	https://tanet2019.nsysu.edu.tw/index.php
活動概要	TANET2019 臺灣網際網路研討會以「資訊展望、5 新起航」為主題。因科技的日新月異，使物聯網絡擴大成熟，經濟和生活將迎來重大變革，同時影響智慧校園的發展，也為教學形式上碰撞出新的火花。本次大會圍繞著五大主軸「物聯新通訊、智慧新生活、雲端新服務、資安新防護、軟體新應用」擴展，全方面探討物聯網絡時代帶來的關鍵課題。 5 新議題延伸的子議題涵蓋 5G 網路通訊、人工智慧及其應用、前瞻資安研發、網路規劃建置、物聯網(IOT)、深度學習、網際網路技術、區塊鏈、軟體工程等多達 55 個領域，將徵求各方資訊從業人員於本次大會發表優質論文，進行深度探索，交流切磋。大會也將邀請產、官、學界資深專家進行精彩的專題演講，以及各類議題討論、論壇分享、資安體驗營、戶外參訪等活動，藉由不同交流形式，共覽學術面及實務面的最新技術發展，使與會者從 5 新啟航，激發創意思維，共同展望智能時代的美麗新境界。


TANET 2019
TANET2019
臺灣網際網路研討會
Taiwan Academic Network Conference
暨資訊工程X智慧計算學門成果發表會
資訊展望、5新啟航
會議日期：2019/9/25-27
會議地點：高雄國際會議中心ICCK
TANET2019臺灣網際網路研討會以「資訊展望、5新起航」為主題。因科技的日新月異，使物聯網絡擴大成熟，經濟和生活將迎來重大變革，同時影響智慧校園的發展，也為教學形式上碰撞出新的火花。本次大會圍繞著五大主軸「物聯新通訊、智慧新生活、雲端新服務、資安新防護、軟體新應用」擴展，全方位探討物聯網絡時代帶來的關鍵課題。
5新議題延伸的子議題涵蓋5G網路通訊、人工智慧及其應用、前瞻資安研發、網路規劃建置、物聯網(IOT)、深度學習、網際網路技術、區塊鏈、軟體工程等多達55個領域，將徵求各方資訊從業人員於本次大會發表優質論文，進行深度探索，交流切磋。大會也將邀請產、官、學界資深專家進行精彩的專題演講，以及各類議題討論、論壇分享、資安體驗營、戶外參訪等活動，藉由不同交流形式，共覽學術面及實務面的最新技術發展，使與會者從5新啟航，激發創意思維，共同展望智能時代的美麗新境界。
活動網站：
https://tanet2019.nsysu.edu.tw
指導單位：教育部、科技部
主辦單位：國立中山大學
協辦單位：財團法人臺灣網路資訊中心
國家高速網路與計算中心
中華民國資訊安全學會
科技部工程司工程科技推展中心

Taiwan Cloud Edge 台灣	
活動時間	2019/5/15
活動地點	台北國際會議中心 (TICC)
活動網站	https://cloudsummit.ithome.com.tw/index.html
活動概要	● **把握數位轉型的決勝之年**

隨著 5G 商轉在即，可望加速邊緣運算起飛，密集催生大量的創新產品與服務，順勢揭開下一波市場淘汰賽的序幕。面對生存保衛戰，企業不容遲疑觀望，急需武裝自己、提高競爭力；透過本活動，您可深入了解混合雲、DevOps、IoT、AI...等數十種雲端技術內涵，進一步理解如何活用它們，快速強化數位創新能量。

- **將資安內化於數位創新**

  不少企業因懼怕遭受網路攻擊，延緩數位轉型的腳步。有鑑於此，本活動不僅引領您躍上雲端、擁抱科技融匯的 IT 新世界，也不忘帶您掌握企業雲端應用安全邊界，知道如何將資訊安全融入數位發展戰略，在業務創新、風險控制天平兩端之間建立最佳平衡。

- **結合案例分享，創造臨場體驗**

  臺灣雲端大會處在新技術浪潮尖端，屢屢放送包括 Cloud Native Computing、AI、IoT、Edge Computing、DevOps、Microservices、Serverless、Blockchain…等大量新知；難能可貴的是，大會不只關切技術理論，更重視管理與應用實務，因而致力規劃案例分享議程，使學員得以增加臨場感，更懂得將新技術運用在企業 IT 發展實務。

- **互動 Hands-on Lab，練就實戰功力**

  一直以來，「實機體驗課」（Hands-on Lab, HOL）始終是臺灣雲端大會的一大亮點，2019 活動現場也不例外！除了特別設計互動式實機環境外，更搭配專業講師的教學引導，帶學員深入了解雲端新技術或新服務的應用環境，學習相關設定、流程或指令，透過做中學、不空談，把這份能力帶回企業工作崗位。

- **新世代雲端資料中心**

  邁向新世代雲端機房，實現雲端運算理念，滿足企業雲端商務應用！雲端主導未來新商業模式的創新與發展，資料中心則是現代數位經濟的核心能力。新世代雲端資料中心議程，旨揭分享各產業且不同規模的企業所需要的雲端資料中心專業案例。

DEF CON 27	
活動時間	2019/8/8 – 8/11
活動地點	Paris Las Vegas Las Vegas, NV 89109, US
活動網站	https://www.defcon.org/
活動概要	● **The DEF CON 27 Theme: 'Technology's Promise'**： DEF CON 26 was about the inflection point between disorder and dystopia - the moment before the point of no return. The DEF CON 27 theme, in a way, responds to '1983' with new questions. What does it look like when we make the better choice? What kind of world do we hack together in the sunniest timeline? How does our real best-case scenario compare to the future we've been dreaming of for generations? Extra consideration will be granted for submissions that tie into this year's theme. We want you to hear about your hacks and research, and how will it relate to the discussions below. 1) **Cypherpunk and "engineering out of the problem".**： Tim May was once quoted saying anonymity online would "alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret." At the time his manifesto was for "both a social and economic revolution" and so began the newly formed "Cypherpunks". Cypherpunks invented cryptography with the aim of abolishing big brother, but 30 years later we have big corporations in their place. Large corporations have insured that the 21st century hasn't come without compromises. Crypto-anarchism is still alive and well today in well known examples like Tor, Freenet, cryptocurrencies, etc. Tell us what you're doing now to circumvent the future we're living in? Corporations are developing advanced facial recognition and becoming "the new big brother". Social media is exchanging a false sense of freedom at the expense of a total removal of anonymity. The Cypherpunk ethos will have to adapt now that we have merged the "instagram-able" life, biometrics, ML, IOT, and micro-targeting. To build a future that doesn't limit our love of modern technology and socialization at the expense of freedom will require decentralization and anonymity technology breakthroughs. What are you doing to engineer your way out of these problems? 2) **"Keep InfoSec out of Hacking"**： DEF CON wants to support the culture of hacking. Between the TV interviews and the assessments we are still the same people with funny names threading the eye of the needle to make the next breakthrough.

Hackers have become mainstream, seemingly to leave the underground to make a "legitimate" living. The industry has developed policies for ethical hacking, multimillion dollar pentesting orgs, bug bounty programs, and set the foundations of security for behemoth corporations. Being paid for hacking was the dream, but now it is an industry unto itself that focuses predominantly on enterprise.

DEF CON is a hacker con, not an InfoSec conference. Hackers are more focused on the joy of discovery, irreverence, novel if impractical approaches. InfoSec is more focused on enterprise, frameworks, and protecting the interests of share holders. There is great value in both types of content, but our con is a hacker con by design.

Activities that enable the hacker mindset and demonstrate how to master a certain technique are always going to be selected over a great enterprise InfoSec talk. DEF CON has always tried to provide a way to amplify the work of hackers, to create a venue for research that allows for others to grow. The idea that technology should be free was written into the subtext of "The Hacker Manifesto" and is just as valid today as it was 33 years ago.

3) **We want the computer from Star Trek, what we're getting is HAL 9000.** :

At DEF CON 24 we hosted DARPA's Grand Cyber Challenge, a challenge to the innovation community with a $2M prize to build a computer that can hack and patch software with no one at the keyboard. This was a lot of fun, and yet there were whispers among us of a future where artificial intelligence will render some human jobs irrelevant. We can see ourselves approaching an event horizon of automation. This technology is not without a price, but how do we get to the utopian world where we ask a computer to make us a cup of earl grey without landing ourselves in a black mirror dystopia? Engineers are developing smart home devices with disembodied voices, while hackers are quick to shout tropes of "NSA listening devices". Is the reckless misuse of technology leading us to a dark future? What can hackers do to help achieve the sunniest timeline?

Above are some suggested topics that loosely align with the theme, we consider all talk subjects. If your talk doesn't fit in one of these topics don't worry, the suggested themes are just a starting point. We've dozens of speaking slots, the tracks will be filled with a clustering of subjects; hardware hacking, lock picking, mobile hacking, reverse engineering, legalities of hacking, and more.

第 6 章、 2019 年 4 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。

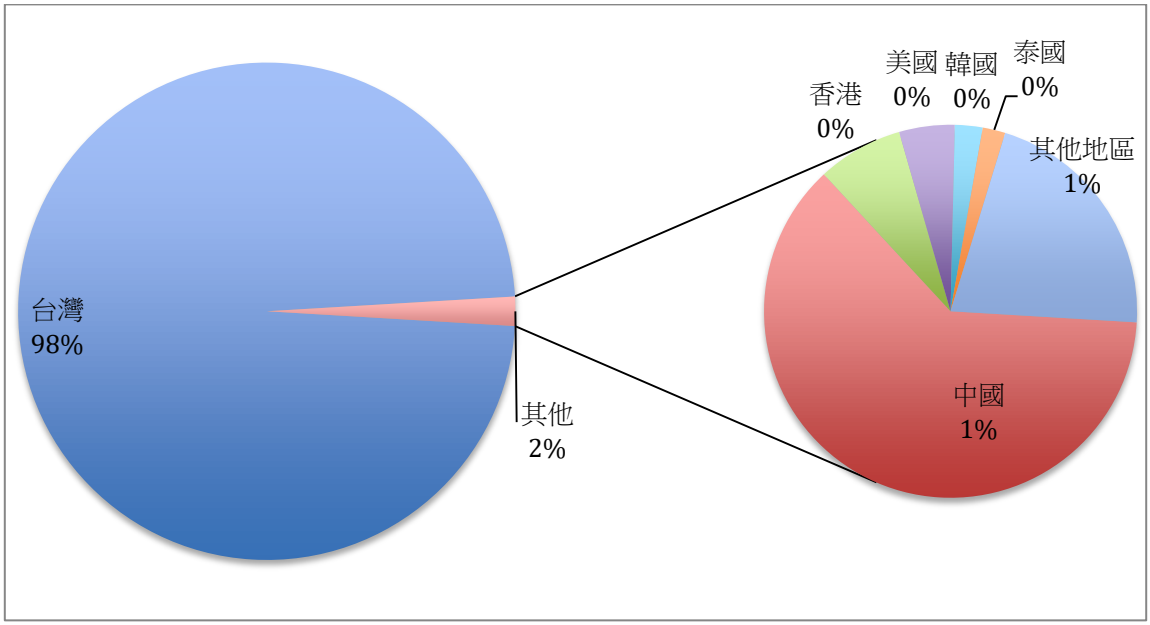


圖 1、通報地區統計圖

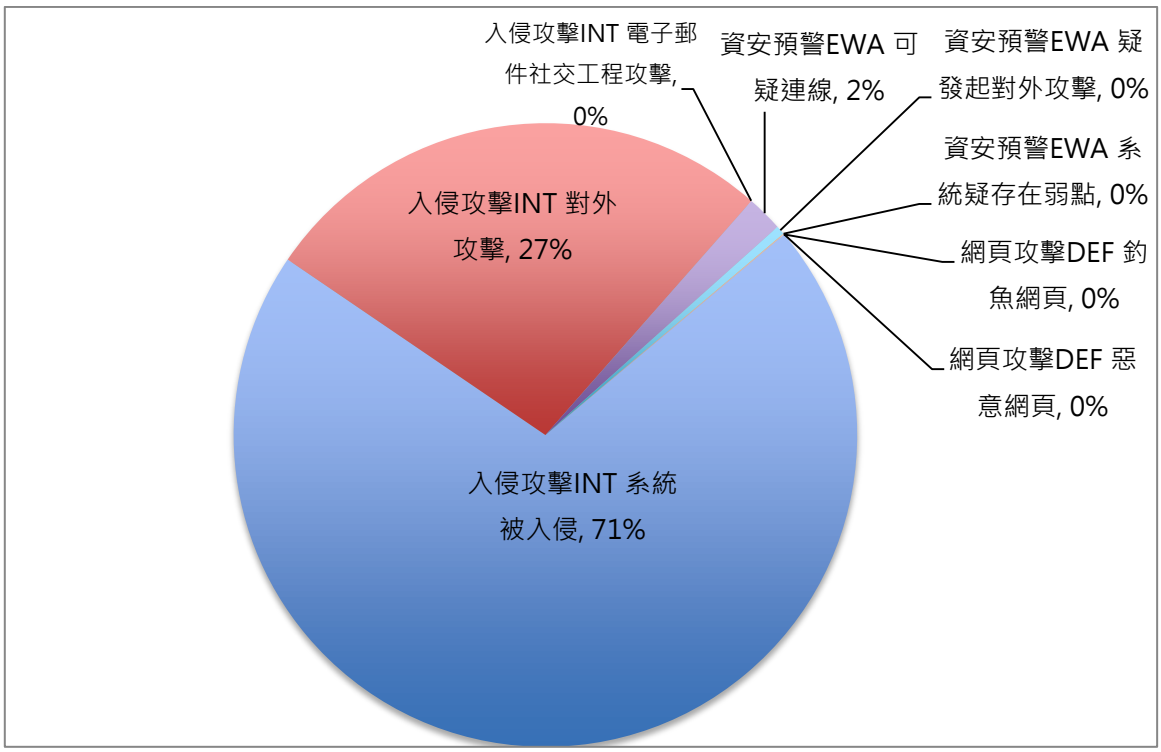

入侵攻擊INT 電子郵件社交工程攻擊, 0%
資安預警EWA 可疑連線, 2%
資安預警EWA 疑發起對外攻擊, 0%
資安預警EWA 系統疑存在弱點, 0%
網頁攻擊DEF 釣魚網頁, 0%
網頁攻擊DEF 惡意網頁, 0%
入侵攻擊INT 對外攻擊, 27%
入侵攻擊INT 系統被入侵, 71%

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 5 月 10 日

編輯：林克容、黃耀輝、江奕昉

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

電子報線上閱覽：https://blog.twnic.net.tw/