TWCERT/CC 資安情資電子報

2019 年 3 月份

目錄

第 1 章、 封面故事

防杜 DNS 攔截攻擊事件，ICANN 發文敦促技術升級

有鑒於透過 DNS 造假技術，將網路流量導向至假網站，藉以監聽網路通訊，甚至騙取帳號密碼等敏感訊息的事件愈來愈多，國際網際網路管理的最高組織 ICANN 日前發表文件，敦促和網域管理有關的各公私單位，早日升級至更安全的 DNSSEC。

DNSSEC 是能夠確認 DNS 記錄未遭竄改的安全加密技術，除了能夠完全相容於舊有的 DNS 架構外，更能防止不肖人士透過竄改 DNS 記錄，將網路流量導向到假網站。

ICANN 指出，DNSSEC 技術配合諸如 TLS（廣泛用於 https 加密協定）等安全技術，可讓終端網路用戶的資料傳輸更加安全，大幅減少「中間人攻擊」造成的風險。

ICANN 即將在三月上旬於日本神戶舉行 ICANN64 研討會，會中將更進一步地解析 DNSSEC 技術，希望能促成 DNSSEC 的早日普及。

第 2 章、 資安小知識—DNS (上)

何為網域名稱系統(DNS)?

有使用過網際網路的使用者，應該對網址(URL)不陌生，例如前往 Google，使用者可於搜尋列中輸入「https://www.google.com」，前往 Google 頁面。但對電腦本身而言，機器所認識的並非一般使用者所見之「https://www.google.com」這個字串，而是 IP 172.217.27.132。因此，為了讓電腦知道該網址所對應之 IP，網域名稱系統(Domain Name System, DNS)為此而生。

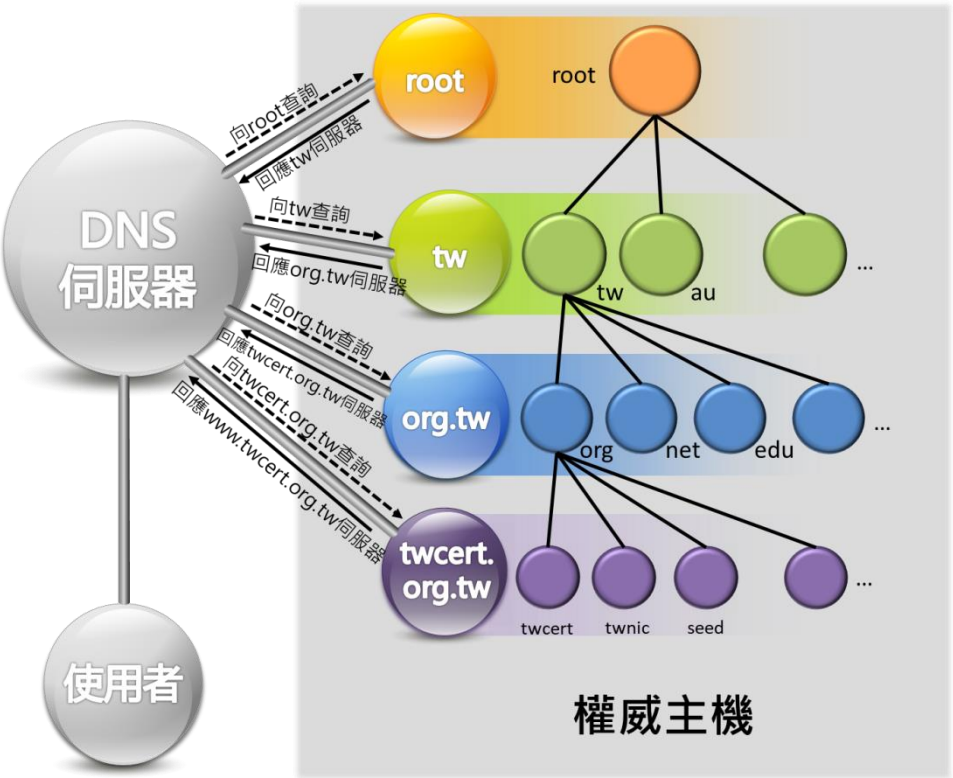
☞HINT：DNS 就像是人和電腦之間的翻譯機，因為人很難記憶 IP，電腦不認識網址，所以需要經過翻譯機的努力，才能順利連上該網站。

DNS 運作

DNS 本身可以看作一種樹狀目錄之型態，一串較長之網址，可經過層層之 DNS 主機搜尋特定部分，以減少每台 DNS 主機所需記憶之資訊。舉例而言，若一使用者欲透過瀏覽器進入 TWCERT/CC 之網站，因此鍵入「www.twcert.org.tw」。此時，電腦會向設定之 DNS 伺服器詢問，而該 DNS 伺服器，會去詢問權威主機中最上層之 root DNS 伺服器，而 root DNS 伺服器會回應「www.twcert.org.tw」中最後「tw」部分負責之 tw 伺服器；接著，會再行詢問 tw 伺服器，而 tw 伺服器會回應「www.twcert.org.tw」中「org.tw」部分負責之 org.tw 伺服器是哪台主機；並接著詢問 org.tw 伺服器過後，會取得「twcert.org.tw」負責之主機位址；最終，詢問 twcert.org.tw

伺服器過後，即可取得「www.twcert.org.tw」之對應 IP。並回應給使用者主機，供使用者主機連線至 www.twcert.org.tw 網站。

☞HINT：DNS 可以想像是政府和地方政府，一名外國人要找到台北市中正區羅斯福路二段 9 號 4 樓之 2，必須先找到台灣政府，待台灣政府引導至台北市政府後，再透過台北市政府引導至中正區.....如此一來方可找到最終目的。



DNS 資安問題一：DNS 劫持

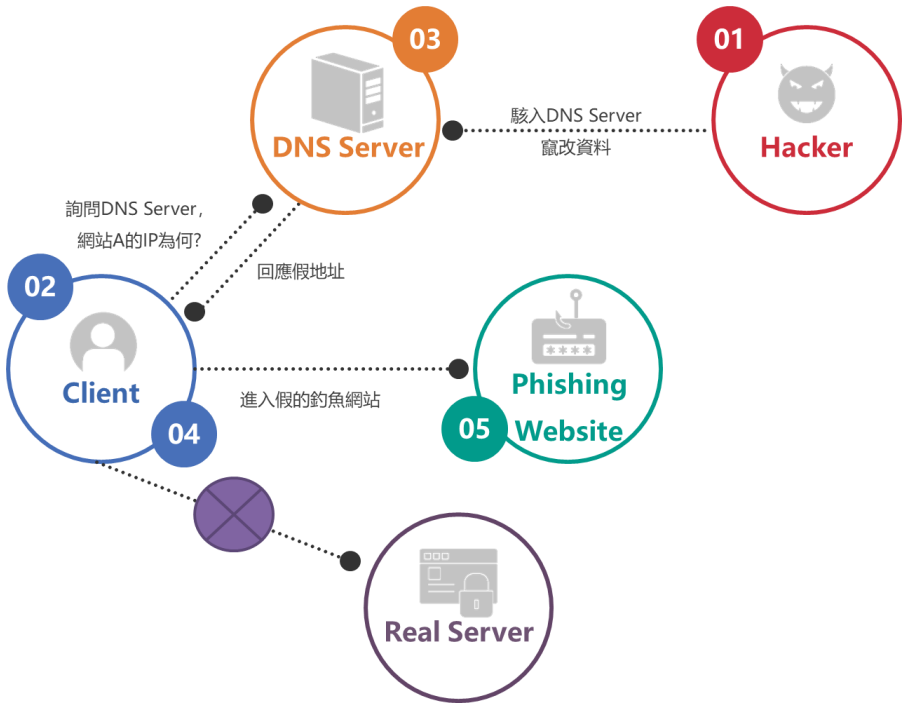
經過上述解釋後，想必大家有種感受：網路運作幾乎都仰賴 DNS 伺服器之運作而進行。在網路整體運作中，DNS 確實佔了舉足輕重之角色，因此，若 DNS 產生任何問題，將會影響使用者進行大部分之網路動作。

此處即舉出一 DNS 資安問題—DNS 劫持。

簡單而言，DNS 劫持即為有心人士將 DNS 伺服器中之紀錄進行修改，將使用者所連線之目的地網站改為對有心人士有力之地址。

首先，駭客會駭入 DNS 伺服器中，竄改 DNS 伺服器的資訊。並且當使用者連線至該 DNS 伺服器以詢問某網站 IP 時，DNS 伺服器會回報一個錯誤之地址，令使用者無法連線至該網頁，甚至連限制釣魚網站。如此一來，駭客便可得到所有使用者欲和真正網站溝通之訊息，例如對話、個資、訂單資訊，甚至是帳號密碼或信用卡資訊。

☞HINT：DNS 劫持可以想像如一觀光客要去購買土產，因此去詢問活動中心之服務處人員。然而，該人員已被惡劣店家置換，因此將觀光客引導至該惡劣店家。而該店家與真正的優良店家外表幾乎相同，客人難以辨別。因此，受害之觀光客在其中被迫購買既昂貴又品質差之物品外，又被盜刷信用卡、錢包手機也同時被竊盜。此手法一般人難以防範和發覺，是種相當可怕之手法。



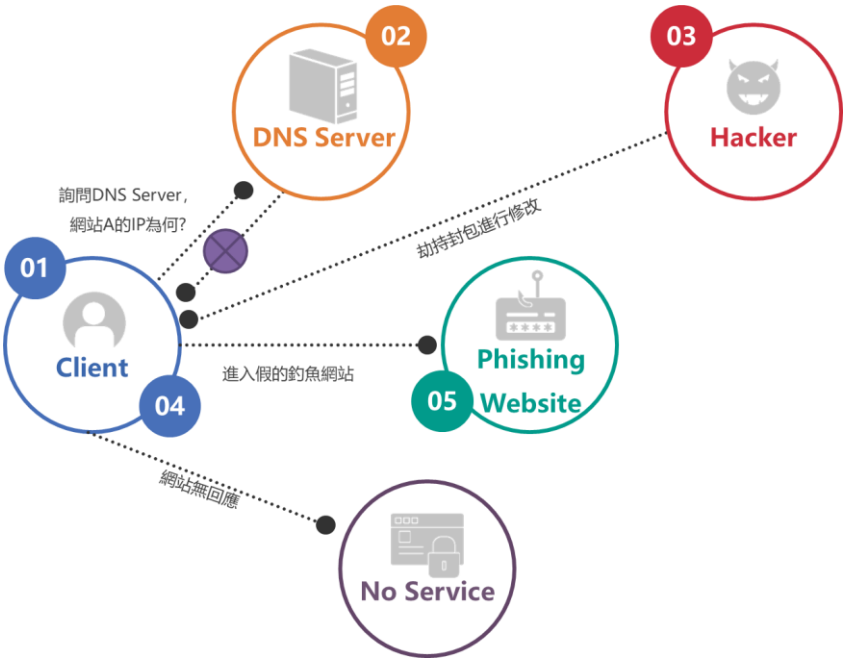
DNS 資安問題二：DNS 感染

另一種 DNS 之資安問題，稱作「DNS 感染」。

在此種手法中，駭客並非駭入 DNS 伺服器中進行修改，而是會透過監聽使用者和 DNS 伺服器之對談，將 DNS 伺服器回覆之封包擷取並偽造一個錯誤之 DNS 回應訊息給使用者，導致使用者主機認定此封包為 DNS 伺服器所發送，因此連線至錯誤之 IP 地址，導致使用者網站無法響應或是連線至錯誤之網站。

此時，使用者前往之錯誤網站，多半為釣魚網站，若使用者於該網站進行帳號密碼之輸入，或是其他購物等行為，將會將所有使用者之個人資訊全數洩漏給有心人士知道。

☞HINT：DNS 感染可以想像如當兩人聊天時，有心人士在旁偷聽，並且向兩邊傳達有心人士所捏造的不實訊息，導致聊天的兩人對對方的誤解。甚至刪除聊天二人手中對方的聯繫方式，使得兩人無法聯繫。



DNS 資安防護

自以上二篇資安問題之敘述，可歸納 DNS 本身所需之防護重點：

(1) 須保持資料之完整性：確認 DNS 伺服器所傳輸之訊息，沒有被他人劫持或被竄改。

(2) 需驗證來源正確性：需確認收到的封包確實為 DNS 伺服器所傳，而非有心人士所傳遞之假訊息。

(3) 確定網站顯示不存在是真的：須確保當網站顯示不存在時，是真正不存在，而非有心人士竄改路徑導致主機連線至錯誤之不存在位址，而非原本欲前往之網站。

為了因應以上 DNS 之問題，因此出現了網域名稱系統安全擴充(DNSSEC)之協定，詳細內容將於下月進行說明。

第 3 章、 國內外重要資安事件

3.1、資安趨勢

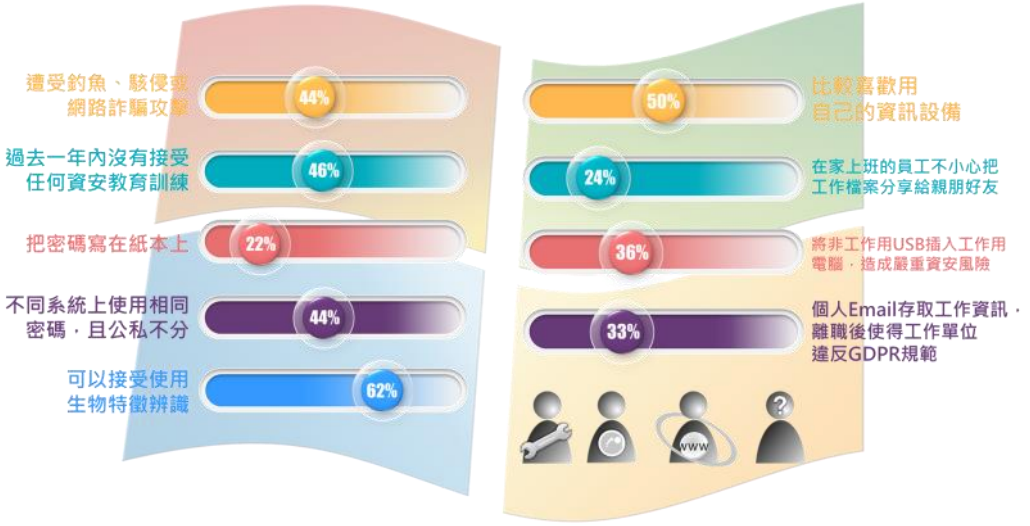
3.1.1 員工的不當使用習慣，是企業資安最大的弱點

微軟愛爾蘭分公司發表研究報告，指出員工的多項資安壞習慣，是企業維持資安的最大弱點。

在微軟委託 Amarach Research 進行的調查報告中指出，下列數種員工的不良使用習慣，對企業資安的維護造成漏洞：

- *44% 的愛爾蘭私營企業員工曾經遭受釣魚、駭侵或網路詐騙的攻擊；*
- *46% 的員工承認過去一年內沒有接受任何資安教育訓練；*
- *22% 的員工會把密碼寫在紙本上；*
- *44% 的員工在不同的系統上重覆使用相同密碼，而且公私不分；*
- *62% 的員工可以接受使用生物特徵辨識（例如指紋）；*
- *一半以上員工比較喜歡使用自己的資訊設備；*
- *24% 在家上班的員工曾經不小心把工作檔案分享給親朋好友；*
- *36% 的員工曾經將非工作用的 USB 儲存裝置插入工作用電腦，造成嚴重的資安風險；*
- *三分之一的員工使用個人 Email 來存取工作或顧客相關資訊，在離職後會造成工作單位面臨違反 GDPR 規範的風險。*

- 資料來源：
  1. https://resources.office.com/en-ie-landing-WE-M365-CNTNT-FY19-02Feb-13-Securing-the-future-MGC0003544.html?wt.mc_id=AID787879_QSG_PR_NWS_321266
  2. https://www.realwire.com/releases/New-Research-from-Microsoft-and-Amarach-Shows-Poor-Security-Habits



3.1.2 面對不同國家駭客，你有多少反應時間？

美國資安廠商推出一份有趣的研究報告，指出 2018 年不同國家的駭侵行動平均需時，其中俄羅斯的駭侵團隊最為快速，受害者只有不到二十分鐘的反應時間。

美國資安廠商 Crowdstrike 日前推出一份研究報告，比較了世界駭侵強國團隊進行駭侵時所需的平均時間，結果如下：

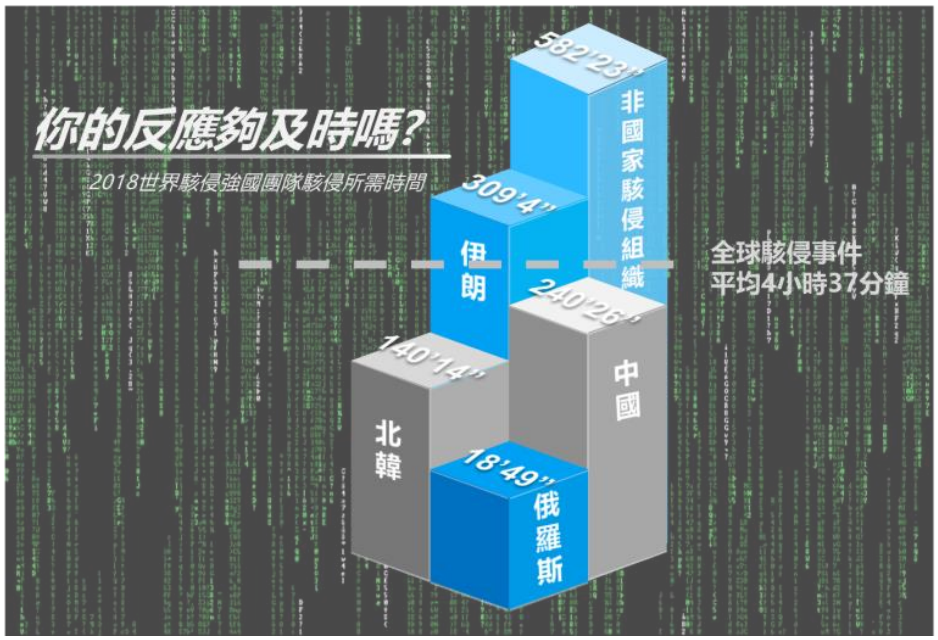
- 俄羅斯：18 分 49 秒；
- 北韓：2 小時 20 分 14 秒；
- 中國：4 小時 0 分 26 秒；
- 伊朗：5 小時 9 分 4 秒；
- 非國家駭侵組織：9 小時 42 分 23 秒。

該報告中所謂的駭侵平均需時，係從駭侵行動初步入侵受害組織的某台電腦開始計算，直到能夠存取整個區域網路資源為止；統計資料以 2018 年的多項駭侵調查報告為基礎計算。

總體計算下來，全球駭侵事件的平均需時約為 4 小時 37 分；2017 年的需時則為 1 小時 58 分。

這份資料對各種公私組織的資安防護準備工作相當重要，因為駭侵行動進展愈快速，受害單位能夠及時反應的時間壓力就愈大。

- 資料來源：
  1. https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
  2. https://www.zdnet.com/article/you-have-around-20-minutes-to-contain-a-russian-apt-attack/



3.1.3 微軟資安中心指出，0Day 攻擊比例日漸上升

微軟資安反應中心（Microsoft Security Response Center）根據駭侵事件統計資料指出，近年來利用 0Day 漏洞（指尚未出現修補程式的最新漏洞）進行攻擊的事件比例，已經高過利用已知漏洞攻擊的案例數量。

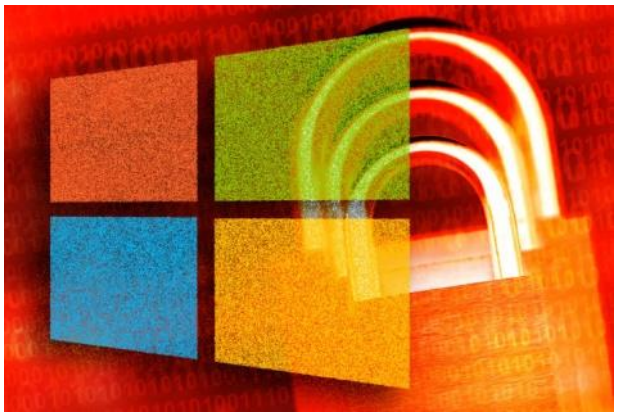
微軟資安反應中心人員於上周的 Blue Hat 資安研討會上發表研究報告，指出 2017 與 2018 兩年間，利用 0Day 漏洞進行攻擊的駭侵事件，在總數上已經超過利用已知漏洞，且修補程式發表已達 30 天者的數量。

這份報告也指出，過去五年間發現且編上 CVE 編號的各種漏洞，數量達到過去的兩倍以上；但利用這些已知漏洞的攻擊案例數量卻減為一半。

ComputerWorld 的資安專欄作家 Woody Leonhard 認為，0Day 漏洞攻

擊可能背後有國家組織的支持，且極可能是針對特定對象發動攻擊，而非針對一般不特定大眾。

- 資料來源：
  1. https://github.com/Microsoft/MSRC-Security-Research/blob/master/presentations/2019_02_BlueHatIL/2019_01%20-%20BlueHatIL%20-%20Trends%2C%20challenge%2C%20and%20shifts%20in%20software%20vulnerability%20mitigation.pdf
  2. https://www.computerworld.com/article/3339537/microsoft-watch-out-for-zero-days-deferred-patches-not-so-much.html



圖片來源：https://www.computerworld.com/article/3339537/microsoft-watch-out-for-zero-days-deferred-patches-not-so-much.html

3.2、 國際政府組織資安資訊

3.2.1 Equifax 被駭的大筆資料到哪去了？專家懷疑可能和國家組織有關

多達一億四千萬人的財務資料，一年多來完全沒出現在暗網或其他地方販售；專家開始懷疑 Equifax 駭侵事件背後有國家組織力量。

發生於 2017 年 9 月的 Equifax 駭侵事件，號稱史上最大宗駭侵事件，多達一億四千多萬美國人的財務資料被駭客竊取；但是這麼大筆的資料，一年多以來竟然消失無蹤，完全沒有出現在暗網或其他地方待價而沽。

一般駭侵事件中被竊的資料，多半很快會在暗網或其他駭客論壇中出售牟利；例如資安廠商 Sophos 指出，最近有 16 個網站的六億兩千筆個資，在暗網求售。但此件事件流失的半數美國人口個資，近年來完全沒有出現。

Equifax 事件中流出的美國民眾個資項目包括社會安全碼、駕照號碼、信用記錄和其他個資等等；以質和量來看，這些資料理論上可賣到非常好的價格，但事件發生後，竟完全沒有被販售，資安專家認為這十分不尋常。

有資安專家根據各種蛛絲馬跡，判斷這一大筆資料應是掌握在某些國家情報單位手中，可能用以進行各種情報滲透工作，甚至用於建立間諜網。

- 資料來源：
  1. https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html
  2. https://www.ftc.gov/equifax-data-breach
  3. https://boingboing.net/2019/02/13/was-that-huge-2017-equifax-dat.html
  4. https://nakedsecurity.sophos.com/2019/02/13/620-million-records-from-16-websites-listed-for-sale-on-the-dark-web

圖片來源：https://www.cnbc.com/2019/02/ 13/equifax-mystery-where-is-the-data.html

3.2.2 澳洲國會遭駭，情報單位懷疑為中國指使

澳洲情報單位指出，日前澳洲國會電腦系統遭到駭客入侵，調查人員研判攻擊者可能與中國有關。

澳洲情報單位指出，日前澳洲國會電腦系統遭到駭客入侵；雖然尚未掌握具體證據，但這次駭侵事件使用的技術十分複雜先進，調查人員研判攻擊者可能與中國有關。

調查人員指出，這次事件在初期就被掌握，目前尚未發現哪些澳洲國會系統內資料遭竊取或破壞；各系統的密碼均已重置以策安全，不過早期調查報告懷疑駭客的目標是竊取澳洲總理與國會議員間的 Email 通訊記錄。

澳洲總理表示，除國會之外，其他澳洲中央政府單位的系統都未遭入侵；目前調查正持續進行中。

- 資料來源：
  1. https://www.abc.net.au/news/2019-02-08/china-government-cyber-security-breach-parliament-hackers/10792938
  2. https://www.abc.net.au/news/2019-02-08/australian-parliament-cyber-security-breach-blame-on-china/10795010

圖片來源：https://www.abc.net.au/news/ 2019-02-08/australian-parliament-cyber-security-breach-blame-on-china/10795010

3.2.3 英國提報中國相關駭侵事件證據，歐盟考慮對中國提出聯合聲明與要求

英國於上個月底向歐盟提出了與中國駭侵事件相關的軟硬體事證，歐盟考慮於近日對中國發出聯合聲明。

英國資安專家於一月 28 日在歐盟的一個技術會議上，提出了和 APT10 駭侵組織的相關軟硬體事證。據消息人士指出，歐盟正在考慮於四月和中國方面的高峰會上提出該議題。

英國提出的相關事證，焦點集中在疑似有中國政府幕後支持的駭侵團體 APT10 上；近來在美國和多個國家亦傳出與 APT10 有關的系統性駭侵行為；美國司法部認為該組織認為該組織為中國官方指使進行間諜與智財竊取行為，但遭中國否認。

歐盟若要對中國提出相關聲音，需要所有歐盟國家一致同意；但目前並非所有歐盟成員國都對此有相同看法。要明確區分攻擊行動來自國家力量或個別駭客，有其難度。

- 資料來源：
  1. https://www.bloomberg.com/news/articles/2019-02-11/eu-is-said-to-mull-response-to-china-hacking-after-u-k-evidence
  2. https://www.scmp.com/news/china/diplomacy/article/2185795/eu-says-sanctions-against-beijing-are-possible-after-uk-alleges

圖片來源：https://www.scmp.com/news/china/diplomacy/article/2185795/eu-says-sanctions-against-beijing-are-possible-after-uk-alleges

3.2.4 微軟指俄羅斯駭客入侵歐洲智庫

微軟指出，一組與俄羅斯國家情報單位有關的駭客，對歐洲智庫和研究單位進行駭侵行動，意在影響歐洲各國近期的選舉。

根據微軟的研究報告指出，該公司發現組織化的駭客，鎖定歐洲多個智庫和研究單位的一百個以上 Email 帳號發動攻擊，而這些研究單位和智庫的研究領域，多和選舉、外交與核能政策相關。

微軟報告未直接指出這些駭侵行動來源國，但指該駭客組織有時使用「Fancy Bear」名號；該組織事實上位在俄羅斯，據信和俄國情報單位有關。

接下來的幾個月內，歐盟境內將舉辦多場選舉，包括歐洲議會、愛沙尼亞國會、斯洛伐克總統、荷蘭省長、烏克蘭總統、芬蘭國會、馬其頓總統、英國地方選舉、立陶宛等等。

- 資料來源：
  1. https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/
  2. https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
  3. https://www.nytimes.com/2019/02/20/technology/russia-hack-microsoft.html

3.2.5 印度國營瓦斯公司遭爆資安漏洞，近七百萬用戶個資可用 Google 搜尋取得

資安研究者發現，印度國營瓦斯公司的用戶資料庫，可在 Google 上檢視其內容；近七百萬用戶個資都遭曝光。

法國資安研究人員 Baptiste Robert 向 TechCrunch 投書指出，根據匿名爆料者向他提供的資訊，印度國營瓦斯公司 Indane 存有資安管理漏洞。共有旗下一萬一千家經銷商，終端消費者六百七十萬人的個資遭到曝光。

報導指出，雖然 Indane 網站的的用戶資料庫頁面有帳密登入頁面，但卻能利用 Google 搜尋結果直接取得資料庫內容，並透過自行撰寫的程式將所有資料爬梳出來。

上周印度政府才被爆出疑似洩露十六萬名公務員個資的事件，而 Indane 資安漏洞的爆料者表示，由於印度政府對類似的資安危機多半予以否認，在媒體上指稱這些爆料是假新聞，同時威脅要法辦爆料者和報導媒體，因此他必須匿名。

- 資料來源：
  1. https://medium.com/@fs0c131y/indane-leaked-aadhaar-numbers-6-700-000-aadhaar-numbers-3948135239f6
  2. https://techcrunch.com/2019/02/18/aadhaar-indane-leak/

3.3、 社群媒體資安近況

3.3.1 美國 FTC 溫馨提醒：當心情人節網路詐騙

西洋情人節前夕，美國聯邦貿易委員會（FTC）提醒天下有情人，在這天要當心以情人節為名的網路詐騙。

2 月 14 日是西洋情人節，也是網路騙徒不會放過的好機會。美國聯邦貿易委員會在一篇部落格文章中指出，這天也是許多人容易上當的日子。

FTC 指出，許多詐騙者會先以美照或挑逗的圖文，以網路情人的身分吸引受害者上勾，接著再用罹患急病需要錢等理由，拐騙受害者的金錢。這些詐騙者往往會用在海外服役等理由，當作無法與受害者見面的理由。

據 FTC 的估計，每宗愛情詐騙案的平均詐騙金額約在 2,600 美元，去年大概有兩萬名美國人上當受騙，不法詐騙所得超過一億四千萬美元。

資安廠商 Avira 也指出，過往經常以提貨或待領款項誘騙用戶點按的釣魚信，在情人節期間也會改以電子情人賀卡的包裝方式來騙人。

- 資料來源：
  1. https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses
  2. https://siliconangle.com/2019/02/13/ftc-issues-warning-online-romance-scams-ahead-valentines-day/
  3. https://blog.avira.com/phishing-for-valentines-day/

圖片來源：https://siliconangle.com/2019/02/13/ftc-issues-warning-online-romance-scams-ahead-valentines-day/

3.3.2 北約軍隊資安單位透過社群網站「釣魚」，發現嚴重資安弱點

北約軍隊的資安單位在社群網站上進行測試，發現士兵透過社群網站分享的機密資訊比想像中既多且廣，形成軍隊機密和資安的嚴重漏洞。

北大西洋公約組織所屬軍隊的資安單位，日前想了解軍隊資訊是否可能在網路上傳遞，及其嚴重性，因而展開「釣魚」實驗；結果包括官兵個人姓名、駐在地、部隊移防情形、具體移防日期地點、甚至連演習進行過程與日期，都可能在社群網站上揭露。

該研究指出，實驗者甚至成功透過社群服務，誘使北約官兵擅離職守，或不執行其任務，或其他不當行為；不過北約並未透露「不當行為」內容。

該研究也發現，Facebook 造成的資安威脅最大，駭客可在 FB 上設立假的官兵個人頁面，進行釣魚或其他破壞行為；甚至包括北約高級軍事將領都在 FB 上「擁有」假的個人頁面。

- 資料來源：
  1. https://www.militarytimes.com/news/your-military/2019/02/20/nato-troops-got-catfished-honeypotted-and-revealed-how-vulnerable-they-are/
  2. https://www.nytimes.com/2019/02/21/world/europe/nato-social-media.html

3.3.3 惡意軟體安裝器 Rietspoof 透過即時通訊大量感染中

一支名為 Riesspoof 的惡意軟體安裝器，被發現透過 Facebook Messenger 或 Skype 等即時通訊軟體大量散布。

資安廠商 Avast 發表警訊指出，於 2018 年八月首次偵測到的惡意軟體安裝器 Rietspoof，自上個月起開始透過各種通訊軟體，例如 Facebook Messenger 或 Sktype 等大量散布。

據 Avast 指出，Rietspoof 這個惡意軟體本身的功能並不多，但它的為害之處主要在於會聽從駭侵者的指示，於受害者主機下載安裝各種不同的惡意軟體；而且 Rietspoof 使用多個有效數位簽章，因此往往能夠騙過受害者系統上的掃毒軟體，成功進駐系統。

Avast 的報告完整描述了 Rietspoof 的感染過程和後續駭侵動作。

要避免這類惡意軟體為害，一般使用者應該注意經常更新防毒軟體，同時避免點按透過通訊軟體傳來的不明連結。

- 資料來源：
  1. https://blog.avast.com/rietspoof-malware-increases-activity
  2. https://www.zdnet.com/article/rietspoof-malware-spreads-via-skype-spam/

3.4、 行動裝置資安訊息

3.4.1 色情和賭博軟體透過 Apple 企業內部軟體測試安裝機制散布

雖然 Apple App Store 對上架的 App 有相當嚴格的審查機制，但被 App Store 禁止發布的色情和賭博軟體，仍有其他管道可以散布到用戶的 iPhone 之上，即透過「企業軟體測試安裝機制」。

Apple 企業內部軟體測試安裝機制，原是 Apple 提供給企業用來對其員工發布測試與內部專用軟體的管道，但最近因 Facebook 和 Google 濫用此機制，讓一般用戶安裝流量與使用行為監控軟體，此機制因而為大眾關注。

資安廠商 Sophos 指出，由於此管道可繞過 App Store 的嚴格審查，不少色情和賭博軟體經此管道讓用戶安裝。

這些未經審查的 App 可能造成相當大的資安風險，包括用戶資料、使用行為的外流，用戶還可能曝露在惡意軟體的直接威脅。

Apple 在發現 Facebook 與 Google 濫用該機制後，曾一度取消提供給這兩家公司的憑證，使得這兩家公司的測試開發與日常運作出現混亂；在 Facebook 和 Google 移除對外部用戶發行的軟體後，Apple 恢復了憑證；不過 Sophos 指出，截至該公司發稿為止，仍有不少色情與賭博軟體尚未被 Apple 取消發行憑證。

- 資料來源：
  1. https://nakedsecurity.sophos.com/2019/02/14/apple-app-store-stuffed-with-hardcore-porn-and-gambling-apps/
  2. https://medium.com/%E6%A2%97-%E7%A7%91%E6%8A%80/facebook-reasarch-buy-user-usage-data-e0b44ea1b94a

3.4.2 歹徒藉試玩測試遊戲發錢釣魚，用戶 iPhone 遭鎖機勒贖

有台灣網友在 Facebook 上分享 iPhone 手機遭歹徒鎖機勒贖的經過，提醒其他用戶勿貪小便宜。

有台灣網友在 Facebook 上分享 iPhone 手機遭歹徒鎖機勒贖的經過，提醒其他用戶勿貪小便宜。這可算是典型的 social engineering 攻擊。

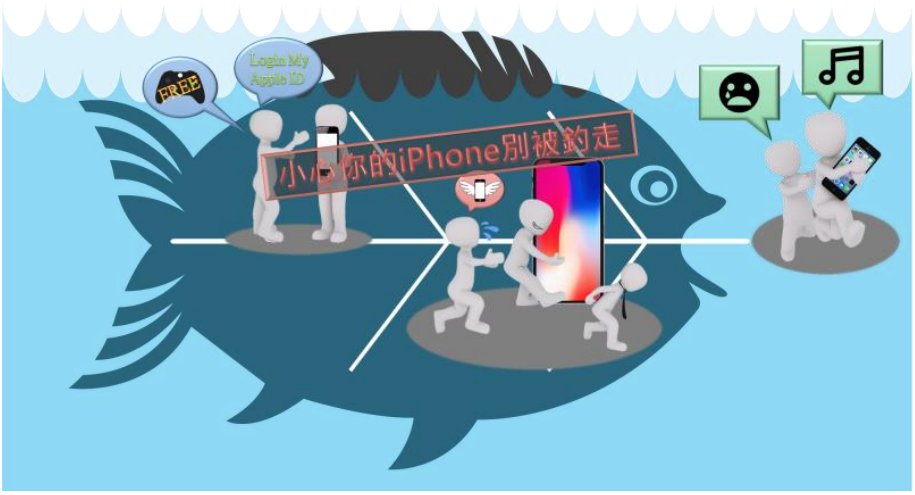
該網友的 iPhone 在 Apple 客服協助下已順利解鎖。

歹徒在 Facebook 社群發布公告，徵求遊戲試玩人員，並提供試玩費用，吸引受害者上鉤。接著，歹徒要求上鉤者改用其提供的 Apple ID 與帳號密碼登入自己的 iPhone，以便到 App Store 中下載安裝測試用軟體。

當用戶以歹徒的 Apple ID 帳密登入 iPhone 後，歹徒即利用 Find My iPhone 的鎖定功能，遠端鎖定用戶的 iPhone。

發覺 iPhone 被鎖定，受害者向歹徒詢問時，歹徒再向受害者要求贖金。

- 資料來源：
  1. https://www.facebook.com/100011208704373/posts/739904306393186



3.4.3 Google 加強對 Play Store 中惡意軟體的安全審查

Google 逐漸加強對上架於 Play Store 中 App 的審核強度。去年被拒絕上架或下架的案例大幅增加。

相對於封閉的 iOS 平台，由 Google 主導開發的 Android 由於相對開放，再加上 Google 一開始未對上架至官方軟體商店 Play Store 的 App 進行任何審核，因此造成用戶極高的資安風險。Play Store 中劣質軟體充斥，還存有不少資安風險相當高的軟體。

Google 近年來開始正視這種亂象，開始仿效 Apple App Store 的做法，逐步加強對上架軟體的審查，除了禁止有資安風險的軟體上架之外，對已經上架的問題軟體也祭出下架的手段。

Google 表示，在去年一年之中被退件的軟體上架申請案件數量上升了 55%，而被下架的軟體數量則增加了 66%。

雖然 Google 加強控管，但在 Android 平台上仍有許多第三方軟體下載安裝平台，很多平台都沒有嚴謹的安控機制；Android 用戶應避免下載這些來路不明的軟體，以避免成為惡意軟體的攻擊目標。

- 資料來源：
  1. https://android-developers.googleblog.com/2019/02/how-we-fought-bad-apps-and-malicious.html
  2. https://www.infosecurity-magazine.com/news/google-play-app-suspensions-jump-66-1/

3.4.4 你的手機上網費用老是爆表？可能是廣告詐騙作怪

軟體大廠甲骨文（Oracle）發現，一支名為 DrainerBot 的廣告詐騙軟體，藏身在許多 Android App 中，每個月會偷偷用掉用戶多達 10GB 的資料用量。

甲骨文公司指出，在多支 Android 遊戲和 App 中發現一個廣告詐騙軟體 DrainerBot 藏身，而這些 App 的下載總數可能多達一千萬次。

只要用戶安裝了含有 DrainerBot 的 App，DrainerBot 就會在用戶不知情的情形下，下載許多用戶看不到的影音廣告，用來向廣告聯播網詐騙廣告點擊費用。這是常見的一種數位廣告詐騙類型。

據甲骨文估計，DrainerBot 每個月偷偷連線產生的額外資料量多達 10GB，對非使用吃到飽資料費率的用戶來說，會造成不小的連線費用；另外也會吃掉用戶手機的電量。

甲骨文指出，一家荷蘭公司 Tapcore 涉及散布含有 DrainerBot 的軟體開發工具（SDK），該公司網頁宣稱每天能發送一億五千萬次廣告曝光，有超過三千個 Android App 使用該公司的 SDK。

- 資料來源：
  1. https://www.oracle.com/corporate/pressrelease/mobilebot-fraud-operation-022019.html

3.4.5 以隱私為餌的 Android 惡意 App，會上傳用戶各種活動記錄

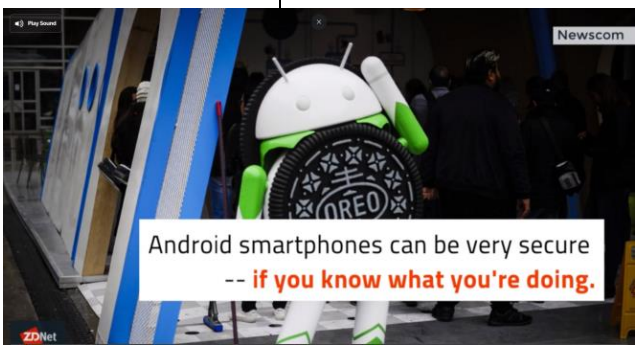
資安廠商 Bitdefender 發現在第三方 Android 應用軟體商店中，有惡意軟體假借隱私保護軟體之外，內含會竊取用戶活動資料的 Triout 惡意軟體，恐已有眾多用戶受害。

Bitdefender 指出，該公司發現內含 Triout 的這支惡意 App，係竄改自隱私保護軟體 Psiphon，會偷偷記錄並上傳用戶在其 Android 手機上的文字輸入、電話錄音、影片錄製，還會拍照並上傳 GPS 定位座標。

由於 Psiphon 廣受用戶歡迎，安裝次數超過五千萬，且有超過一百萬個用戶評價（多數為好評），假冒該軟體的惡意 App 恐怕也有不少受害者。另外 Bitdefender 也指出，這支惡意 App 不但功能強大，而且用戶極難發現，因此其係針對特定對象進行駭侵的可能性也相當高。

Bitdefender 指出，這支惡意軟體只在第三方 Android App 商店出現，在 Google Play 上架的正版 Psiphon 並未受感染；用戶應在 Google Play 下載自己需要的軟體，避免在來路不明的第三方 Android App 商店中下載安裝任何軟體。

- 資料來源：
  1. https://labs.bitdefender.com/2019/02/triout-android-spyware-framework-makes-a-comeback-abusing-app-with-50-million-downloads/
  2. https://www.zdnet.com/article/now-this-android-spyware-poses-as-a-privacy-tool-to-trick-you-into-downloading/



圖片來源：https://www.zdnet.com/article/now-this-android-spyware-poses-as-a-privacy-tool-to-trick-you-into-downloading/

3.5、軟體系統資安議題

3.5.1 美國 Email 服務商遭駭客刪除絕大部分資料

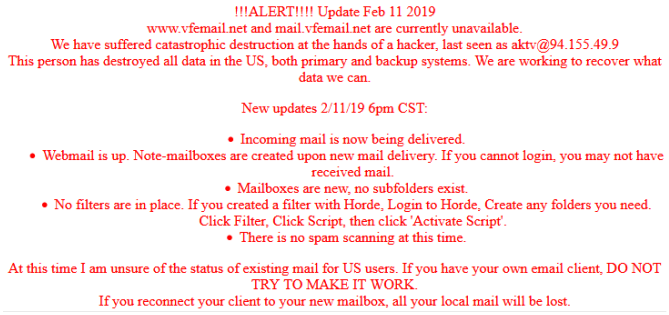
美國的 Email 服務商 VFEmail.net 於日前遭到駭客毀滅性的入侵破壞，所有其美國客戶的 Email 資料全遭刪除，公司可能因此倒閉。

VFEmail 於 2 月 11 日遭到駭客入侵，該公司伺服器的所有硬碟都遭到格式化，所有前台與備份資料庫及虛擬機器都因而遭到刪除，無一倖免。

VFEmail 表示該攻擊事件並未要求贖金，而是單純入侵與破壞。通常針對商業公司的駭侵攻擊，僅會針對該公司一部分服務進行干擾破壞，藉以要脅贖金或其他代價；像這樣一入侵就進行全面破壞的案例非常少見。

VFEmail 到底被誰攻擊？目前也沒有頭緒；該公司僅掌握一個來自保加利亞的 IP。

- 資料來源：
  1. https://www.zdnet.com/article/hackers-wipe-us-servers-of-email-provider-vfemail/
  2. https://www.vfemail.net/



圖片來源：https://www.zdnet.com/article/hackers-wipe-us-servers-of-email-provider-vfemail/

3.5.2 微軟一口氣推出 77 項產品更新修補程式

微軟於二月的「周二更新日」，一口氣推出了 77 種修補程式，修補對象從 Microsoft Edge 瀏覽器一直到 Azure IoT SDK，用戶請盡速下載安裝。

每月的某個周二是微軟大幅釋出更新程式的固定日期，二月也不例外，共有 77 個軟體錯誤或漏洞於這次大更新中獲得修補。

其中最值得注意的修補程式，是 CVE-2019-0676 的 IE 0day 漏洞更新，這個漏洞可讓駭侵者檢查檔案系統中是否存有特定檔案。

此次也包含一個 SMB 協定的重要更新，這個漏洞可讓駭客遠端執行任意程式碼，著名的勒贖軟體 WannaCry 和 NotPetya 就是透過 SMB 漏洞，於 2017 年造成大感染。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0676
  2. https://portal.msrc.microsoft.com/en-us/security-guidance
  3. https://www.zdnet.com/article/microsoft-february-patch-tuesday-fixes-77-security-flaws-including-ie-zero-day/

圖片來源：https://www.zdnet.com/article/microsoft-february-patch-tuesday-fixes-77-security-flaws-including-ie-zero-day/

3.5.3 存在 14 年的 WinRAR 安全漏洞終於修復

廣受歡迎的 WinRAR 日前宣布修復一個存在已經 14 年，可讓入侵者執行任意程式碼的安全漏洞。

WinRAR 是一套廣受用戶歡迎的老牌檔案壓縮工具，用戶多達五億；可能你的 Windows 電腦上也有安裝。日前 WinRAR 公司宣布修復一個存在已經有 14 年之久的安全漏洞。

WinRAR 這個古老安全漏洞是源自於該軟體採用的一套程式庫 UNACEV2.DLL，這個用來解壓 ACE 壓縮檔的程式庫，自 2005 年起就從未更新；資安廠商 Check Point 發現可以利用這個程式庫在 Windows 啟動目錄中放置任意執行檔。

在 Check Point 公開這個漏洞後，WinRAR 立即取消對 ACE 壓縮檔的支援，從而解決該漏洞問題。如果你的 Windows 電腦安裝了 WinRAR 程式，請盡速更新。

- 資料來源：
  1. https://research.checkpoint.com/extracting-code-execution-from-winrar/
  2. https://arstechnica.com/information-technology/2019/02/nasty-code-execution-bug-in-winrar-threatened-millions-of-users-for-14-years/

3.6、軟硬體漏洞資訊

3.6.1 Google 研究員發現駭客可利用 iOS 0day 漏洞進行駭侵，用戶應立即更新系統

Google 資安團隊 Project Zero 主任研究員 Ben Hawkes 指出，存於舊版 iOS 中的兩個 0Day 漏洞，將導致駭侵者取得系統核心權限並執行任意程式碼。

目前尚未發現有大規模利用這兩個漏洞進行惡意駭侵的情報，iOS 用戶需盡速更新至最新版的 iOS 12.1.4；這個版本同時修正了先前發現的 FaceTime 錯誤。

- CVE 編號：
  - CVE-2019-7286
  - CVE-2019-7287
- 影響產品：
  - iPhone、iPad 等 iOS 裝置
- 解決辦法：

  立即更新至 iOS 12.1.4 以上版本。
- 資料來源：
  1. https://twitter.com/benhawkes/status/1093581737924259840?ref_src=twsrc%255Etfw%257Ctwcamp%255Etweetembed%257Ctwterm%255E1093581737924259840&ref_url=https%253A%252F%252Fwww.zdnet.com%252Farticle%252Fgoogle-warns-about-two-ios-zero-days-exploited-in-the-wild%252F
  2. https://www.zdnet.com/article/google-warns-about-two-ios-zero-days-exploited-in-the-wild/
  3. https://support.apple.com/en-us/HT209520

3.6.2 MacOS 變種惡意軟體新發現，偽裝為 Adobe Flash Player 更新程式

資安廠商 Carbon Black 旗下的資安威脅研究單位發表報告指出，該單位發現了基於 Shlayer 惡意軟體的變種，偽裝為 Adobe Flash Player 安裝程式。

安裝了該惡意軟體的 Mac 電腦，部分網路連線會被攔截並重新導向至部分惡意網站。

Carbon Black 的網站詳述了該惡意軟體的運作方式與分析報告。

- 影響產品：
  - MacOS X 10.10.5 至 10.14.3
- 解決辦法：
  建議盡量不使用 BitTorrent 網站，以降低自身裝置暴露風險。
  同時若非需要，盡量不安裝 Adobe Flash Player，以避免安裝了充斥惡意軟體之假冒 Flash Player。
- 資料來源：
  1. https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/
  2. https://www.intego.com/mac-security-blog/new-osxshlayer-malware-variant-found-using-a-dirty-new-trick/

圖片來源：https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

3.7、資安研討會及活動

ICANN APAC-TWNIC Engagement Forum	
活動時間	2019/4/16 – 4/17
活動地點	臺大醫院國際會議中心
活動網站	https://forum.twnic.net.tw/2019/
活動概要	 ICANN 及 TWNIC 共同舉辦合作交流論壇 (ICANN APAC-TWNIC Engagement Forum)，集合了網路相關利害關係人與國際相關網路社群，針對域名、IP 位址及網路安全等主題，進行深入議題探討，這將是台灣與國際網路利害關係人共同面對面討論全球網路議題的最佳機會。 ICANN 及 TWNIC 建立論壇平台的目的，是讓地區內之網路相關利害關係人，可在「一個世界、一個網路」的目標下，以合作交流論壇建立一個共同合作、討論與鏈結的全球網路社群。 我們需要您的參與，為「一個世界、一個網路」共同發聲！ The ICANN APAC-TWNIC Engagement Forum is a joint effort of the two Internet organizations to bring the stakeholders of the Internet together with the local and international communities to share and discuss the latest topics on Internet policies, domain name, IP address allocation, and cybersecurity. It is the best chance to meet, discuss and share your opinions on the latest issues and know the stakeholders in Taiwan. It is also our goal to establish a platform for the communities to ignite the discussions from a variety of aspects of stakeholders and to keep pace with dynamic technologies and rapid innovation. With our goal "One World. One Internet.", facilitating we work together, discuss together, connect together under the global community as One. We need you to participate and voice out for the One Internet!

2019 臺灣資安大會	
活動時間	2019/3/19 – 3/21
活動地點	臺北國際會議中心 & 世貿一館 2 樓
活動網站	https://cyber.ithome.com.tw/
活動概要	2019 臺灣資安大會邀請您與我們一起參與臺灣年度資安盛事，為期一週的 2019 臺灣資安大會 (CYBERSEC 2019) 在此集結 180 家以上的國際及臺灣在地知名資安夥伴，展示最新與最適切的資安產品與服務，提供超過 180 堂資安全面向的議程，探討 80 種以上最熱與最廣泛的資安議題與技術。除了豐富的資安對策，更可與來自臺灣與亞太地區的 6,000 位與會者進行交流，拓展專業人脈成為未來工作的助力。 現今面對的攻擊已非單一人、單一部門乃至於單一企業可以有效防守，孤軍奮戰難以抗衡全球日漸壯大且有組織的縝密攻擊。不論您來自業界、專家學者、法務人士、公部門或企業用戶等，都歡迎與我們一同在此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。期許大家除了將資安意識與知識帶回組織中，從上至下凝聚共識與成長，並與資安產業的夥伴們偕同防禦，共同在資安戰場更加壯大，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。 ● 2019 臺灣資安大會特色： ✓ 臺灣最大規模資安會議 ✓ 技術研討、主題論壇、實機操作、攻防演練一應俱全 ✓ 從技術到策略、從最新趨勢到日常營運 ✓ 產官學研齊聚一堂共商資安對策 ✓ 實戰演練資安攻防，提升實務防禦與鑑識能力 ✓ 最大規模的資安展覽，有效找到最適資安產品與服務 ✓ 凝聚共識與成長，偕同資安夥伴建構更強力防禦

Black hat 2019 年亞洲大會	
活動時間	2019/3/26 – 3/29
活動地點	新加坡濱海灣金沙會展中心
活動網站	https://ubm.io/2zZu87q
活動概要	**blackhat ASIA –針對亞洲社群資安發展需求，發表產業最新資安訊息與因應技術** ● blackhat Asia 為網路安全(Cyber Security)專業會議暨展會，提供最新資安教育訓練、產業趨勢簡報會暨產品展示，吸引多國政府機構、企業資安人員、系統整合代理商、經銷商等專業人員與會。 ✓ 為亞洲資安發展量身訂做專業議題，邀集「亞洲區資安委員會」，收集最新議題技術 ✓ 新加坡為國際政治中立國家，順利邀集歐、美、中東、亞太等重要講者。 ✓ 亞洲市場資安需求量逐漸上升，亞太企業開始重視人員培訓與資安環境建置。 **趨勢簡報會議(Briefings)–匯集全球資安專家談亞太資安議題與解決方案** ● 趨勢簡報會：為各行業從事資安相關人員提供一個學習亞太地區網路安全風險與趨勢的平台；邀請資安行業中頂尖人士主講，熱門議題包含：IOS & Andorid、車控系統、物聯網、虛擬貨幣、支付系統、加密系統運用、企業軟體漏洞、國際資安政策等漏洞攻防主題； ● 2019 年講師與簡報主題詳請請見：https://ubm.io/2rN2NRq (完整議題預計於 2019 年 2 月公布) ● 2019 年趨勢簡報會主題範疇：應用程式安全、密碼學、數據鑑識/事件應變、企業、資安漏洞發展、硬體/內嵌、網路防禦、人為因素、物聯網、惡意軟體、平台安全、資安開發週期、逆向工程、政策 **商業大會(Business Hall) - 全球資安產品品牌拓展亞太市場的國際平台** ● 2019 年指標展廠： Infoblox CONTROL YOUR NETWORK　QUALYS ON DEMAND SECURITY　POLYSWARM　ANOMALI　hackerone efficient iP DEFINING SMART DDI　Lockpath　eLearnSecurity Forging security professionals　wolfSSL　CASHSHIELD

	2018 會議與展會規模 ● 來自 60 個國家，超過 2,200 名專業人士與會，亞太區 88%、美國 6%、歐洲 3%、中東 3%。 ● 邀集 57 名資安權威，舉辦 33 場專業簡報、10 場教育訓練與 30 場產品展示，18 家國際媒體出席。 **匯聚 60 國，跨越醫療、軍警、金融、電信、資安的產官學決策代表與會** ● 系統整合商： M Tech!、Netpoleon、Westcon Comstor、Pacific Tech、Quantiq International ● 醫療保健：IHis、MSD International Gmbh、新加坡保健集團、陳篤生醫院 ● 金融服務：2C2P Pte Ltd、Allianz Asia Pacific、FinIQ Consulting Pte Ltd、歐力士亞洲有限公司 ● 電信服務：CommzGate、Ericsson Telecommunications、華為技術有限公司、LGA Telecom Pte Ltd ● 資訊服務：CTC Global Pte Ltd、Deskera Singapore、ITOCHU Techo-solutions、NCS Pte Ltd ● 政府單位：新加坡中央公積金、香港警務處、新加坡資訊通信媒體發展局、新加坡內政部 ● 電腦製造商：Garhi Japan、三菱電機公司、三星公司、索尼電子公司 ● 公民與軍事防衛：DSTA、Jupiter Protection Pte.Ltd、MINDEF、S-fifteen Space Systems ● 資訊安全:Attila CybertechPte Ltd、CDNetworks Singapore、Horangi、VenusTech

2019 亞太資訊安全論壇暨展會	
活動時間	2019/5/8 – 5/10
活動地點	台北世貿南港展覽館
活動網站	https://secutechinfosecurity.tw.messefrankfurt.com/taipei/zh-tw/visitors/welcome.html
活動概要	2019 年第十八屆(年) 亞太資訊安全論壇暨展會，《資安人》媒體，將於三天展覽會會場上，從四個主軸出發深入探討資訊安全議題: 觀念：與法規同步，與協同合作夥伴共同推動資安關鍵角色的重要性。 ● 組織：企業組織設立專職單位與專職資訊安全人員。 ● 管理：採用工具的評估讓觀念具體呈現其效力。

	● 技術：新型態網路部署規劃，建置。 **3 天論壇，10 個關鍵資安主題，50 場演講 + 攤位展示。** ● 資安議題方向： ✓ 資安管理與法規 (Security Management and Compliance) ✓ 網際威脅 (Cybersecurity) ✓ 雲端與行動安全 (Cloud & Mobile Info Security) ● 資安與監控安防聯網 ✓ 資安議題：Infra Security、Endpoint、Application Security、Wireless、Cloud、Mobile Security、SIEM、Incident Response、Identity Management ..... 歡迎各界、資安領域廠商們參與，展現您們的優秀產品與高品質的服務。

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 4 章、 2019 年 2 月份事件通報統計

本中心每日透過官方網站、電郵、電話等方式接收資安情資通報，2019 年 2 月情資總計 67,043 筆，以下為各項統計數據，分別為通報來源統計圖、通報對象統計圖及通報類型統計圖。

通報來源統計圖為各國遭受網路攻擊事件，屬於我國疑似遭利用發起攻擊或被攻擊之 IP，向本中心進行通報之次數，如圖 1 所示；通報對象統計圖為本中心所接獲之通報中，針對通報事件責任所屬國家之通報次數，如圖 2 所示；通報類型統計圖則為本中心所接獲的通報中，各項攻擊類型之筆數，如圖 3 所示。

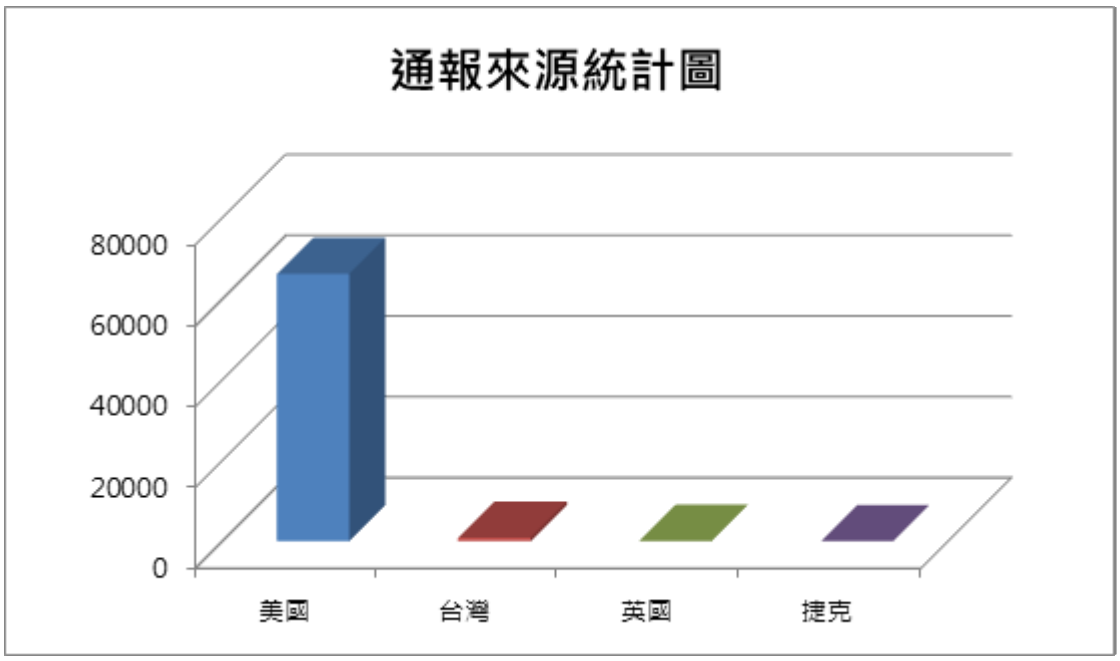


圖 1、通報來源統計圖

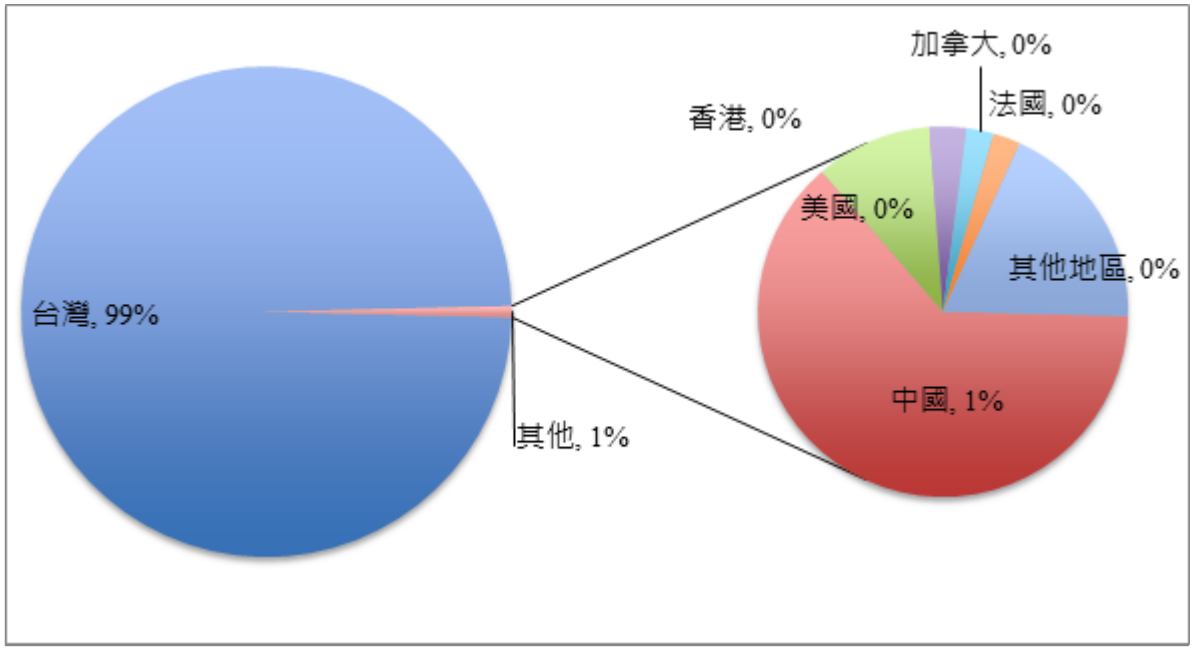


圖 2、通報對象統計圖

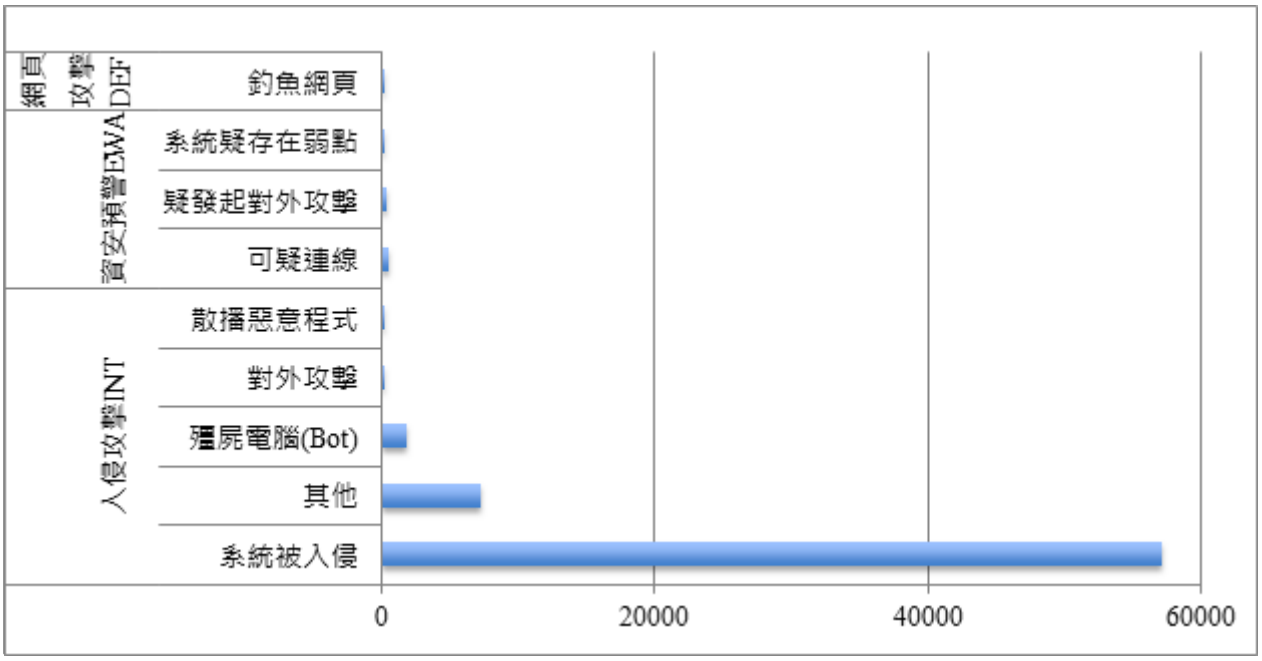


圖 3、通報類型統計圖

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 3 月 12 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/

電子報線上閱覽：https://blog.twnic.net.tw/