TWCERT/CC 資安情資電子報

2019 年 2 月份

目錄

第 1 章、 封面故事

2 月 1 日部份公共 DNS 測試其 EDNS 符合性功能，恐造成部份網站連線不正常

Google、IBM、Cloudflare 等公共 DNS (Public Domain Name System) 服務商 (https://dnsflagday.net/#supporters) 將於 2 月 1 日測試其 EDNS(Extension Mechanisms for DNS, EDNS) 符合性功能；如各網站既有使用之 DNS 無法支援 EDNS 協定時，上述公共 DNS 之使用者恐因無法順利解析 IP 位址，而造成拜訪網站時反應變慢或無法連線。因此，財團法人台灣網路資訊中心呼籲網路使用者，應檢查使用者電腦之 DNS 是否使用上述公共 DNS，對於使用公共 DNS 之不同使用者，TWNIC 提出以下建議，進行相關檢測與修正。

第一類是對網域名稱管理者及網路服務供應商 (ISP)：請先瞭解 DNS 伺服器是否完整支援 EDNS 協定，請至 https://dnsflagday.net/ 進行檢測，若經檢測有問題時，請依該網頁的說明進行修正。

第二類是對一般使用者：如果使用前述公共 DNS 之使用者，如 2 月 1 日當日發現網站無法連線時，可以將 DNS 更換為 ISP 所提供 DNS 之 IP 位址或 TWNIC 之 101.101.101.101，便可順利連線。TWNIC 所提供之 Quad101 免費公共 DNS 服務請詳 https://101.101.101.101。

TWCERT/CC (台灣電腦網路危機處理暨協調中心) 也同步透過情資分享與通報機制，將此訊息通報給國家資安資訊分享與分析中心 (N-ISAC) 、NCC 資通安全分析管理平臺 (C-ISAC) 、教育學術

資訊分享與分析中心 (A-ISAC) 、台灣 CERT/CSIRT 聯盟等，提供相關單位與企業檢測 DNS 相關的訊息，來減緩此事造成網路連線的不便。

TWCERT/CC (台灣電腦網路危機處理暨協調中心)，為非營利組織，負責與國內外各資安組織協同合作執行民間資安事故通報與應變作業，以維護台灣整體網際網路安全。

第 2 章、 國內外重要資安新聞

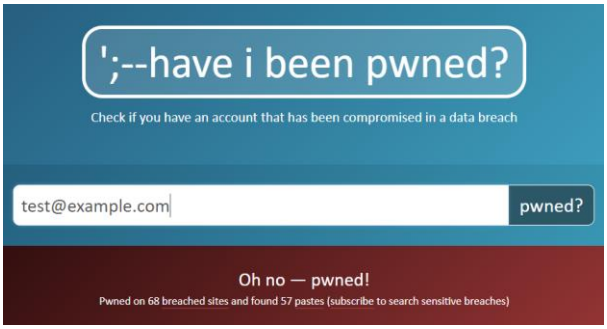
2.1、國內外資安政策、威脅與趨勢

2.1.1 史上最大個資外洩事件，多達七億七萬組 Email、2100 萬組密碼遭公開

資安研究者 Troy Hunt 日前揭露這起個資外洩事件，他指出這些帳號密碼的組合，是由過去多達兩千起以上的駭侵事件外洩資料集結而成，而且許多資料中都以明碼型態儲存在檔案中，可能也已被其他人取得。

Troy Hunt 已將這些被公開的 Email 和密碼放入查詢網站「Have I Been Pwned?」中，用戶可在此輸入自己的 Email 帳號和密碼，查詢該資料是否已經外洩，並且使用密碼管理工具針對不同網路服務，使用不同的高強度密碼，並且開啟二階段認證，以避免帳密外洩。

- *Email 外洩查詢：https://haveibeenpwned.com*
- *密碼外洩查詢：https://haveibeenpwned.com/Passwords*



圖片來源：https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

- 資料來源：
  1. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/
  2. https://www.wired.com/story/collection-one-breach-email-accounts-passwords/

2.1.2 航班訂位系統 Amadeus 重大漏洞，駭客可輕易取得、更改旅客飛行記錄

以色列資安研究人員 Noam Rotem 指出，市佔率達 44%，廣泛用於各大航空公司票務資訊的 Amadeus 系統內含重大安全漏洞。駭客只要取得旅客訂票代號，就能獲取旅客資訊；而透過操弄航空公司網站，駭客可以更改旅客的訂票記錄，例如更改座位、航班班次等等，也能輕易取得旅客的電話、Email、住址等個資。

取得旅客訂票代號的方式也很容易，許多旅客會在社群平台上分享內含加密條瑪的登機證相片，但該條碼的加密早經破解，可以輕易用手機 app 掃瞄並讀出訂票代號。

駭客甚至可以用暴力試誤法，不斷嘗試各種自己產生的訂票代號，從而對應到真實旅客身分與資料，因為該訂票代號是連續號碼，而 Amadeus 系統並未限制錯誤存取次數，甚至也未針對短期間大量存取行為設有任何限制。

圖片來源：
https://techcrunch.com/2019/01/15/amadeus-airline-booking-vulnerability-passenger-records/

- 資料來源：
  1. https://techcrunch.com/2019/01/15/amadeus-airline-booking-vulnerability-passenger-records/
  2. https://www.scmagazine.com/home/security-news/amadeus-booking-system-flaw-could-have-exposed-info-on-millions-of-travelers/

2.1.3 駭客透過網域註冊大廠 GoDaddy 安控疏失，以知名品牌域名大量發送勒索信件

資安廠商 KrebsOnSecurity 發表研究報告指出，近幾月兩宗大規模勒索郵件攻擊事件，都和世界最大網域註冊商 GoDaddy 的安控疏失有關。其中一起勒索信揚言放置炸彈，已造成十多間學校、商家或政府機關因而關閉。

報告指出，這兩宗和俄羅斯駭客組織相關的勒索信件攻擊，其開信率非常高，與一般亂槍打鳥的垃圾信攻擊有所不同；這表示這些垃圾信件能繞過 Email 垃圾信阻擋系統的偵測。

研究發現這些垃圾信之所以能繞過垃圾信偵測系統的原因，就在於透過知名大品牌註冊多年的網域發送；許多垃圾信的網域都來自財星五百大或一千大品牌，如麥當勞、希爾頓飯店、時代華納、特斯拉、Oath 等。

上述被用來發垃圾信的網域，大多透過 GoDaddy 註冊並管理，而駭客正是利用 GoDaddy 的安控疏失；由於 GoDaddy 並未嚴格查證任何會員對某網域所有權的主張要求，因此駭客能輕易取得這些知名品牌的網域控制權，並將 DNS 導向至旗下的垃圾信主機。

該報告統計出至少有四千個在 GoDaddy 網域透過此一疏失用來發送勒索信，GoDaddy 也承認確實存有安控疏失，也已採取行動補正。

為防制此類問題，網域管理者應隨時檢視網域設定是否遭到竄改，特別是立即刪除已不再使用的子網域。

圖片來源：https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

- 資料來源：
  1. https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/
  2. https://arstechnica.com/information-technology/2019/01/godaddy-weakness-let-bomb-threat-scammers-hijack-thousands-of-big-name-domains/
  3. https://www.itpro.co.uk/security/32822/godaddy-authentication-vulnerability-exploited-for-phishing-campaigns

2.1.4 紐西蘭總理表示，對華為的禁令相當公正客觀，並無特殊考量

路透社日前於瑞士達沃斯舉行的 2019 世界經濟論壇會議上專訪紐西蘭總理傑辛達．阿爾登，詢問紐西蘭對華為潛在資安疑慮問題；阿爾登表示，對華為設備的禁令，並不是針對華為這家公司所做出的特別決定，而是基於紐西蘭既有的資安法規架構而來。

去年十一月紐西蘭政府通訊安全局 (Government Communication Security Bureau) 裁定，以「顯著的國安風險」為由，禁止紐西蘭電信業者 Spark 採用華為 5G 網路設備，但現用於 3G 與 4G 的華為設備則不受影響。

紐西蘭是所謂「五眼聯盟」的成員國之一，此聯盟是以英國與美國為主的國際情報分享組織，另外兩名成員國為澳洲與加拿大。目前除五眼聯盟成員國外，包括德國、日本、捷克、挪威與我國台灣，都對華為祭出禁令。

圖片來源：https://www.stuff.co.nz/business/108940155/gcsb-declines-huawei-proposal

- 資料來源：
  1. https://www.reuters.com/article/us-davos-meeting-newzealand-huawei/new-zealand-pm-says-country-is-not-discriminating-against-huawei-idUSKCN1PH2IN
  2. https://www.stuff.co.nz/business/108940155/gcsb-declines-huawei-proposal
  3. https://www.wired.com/story/huawei-is-many-troubles-bans-alleged-spies-backdoors/

2.1.5 跨國大型電信業者 Vodafone 宣布核心網路停用華為設備

Vodadone CEO Nick Read 表示該公司仍會採購部分華為的 4G 與 5G 設備，但在該公司的歐洲核心網路架構中不會採用華為設備，主要原因是集中在核心網路中的資料，必須擁有最高規格的安全考量。

Nick Read 指出，目前媒體上有許多來自政界或各方對於華為安全性的議論，他認為並非所有議論都基於事實進行清楚的說明；他認為 Vodafone 在歐洲區核心網路中停用華為設備，對該公司不會造成太大的衝擊。

他同時也表示，這一政策並非受到政府或政治的壓力，但確實和目前歐洲整體的風向有關。他認為相關的討論還是必須基於事實來進行有條理的論述。Vodafone 計畫於今年年底前在多個市場推出 5G 服務。

圖片來源：
https://www.theguardian.com/business/2019/jan/25/vodafone-pauses-huawei-equipment-core-network-across-europe-security-concerns

- 資料來源：
  1. https://www.theguardian.com/business/2019/jan/25/vodafone-pauses-huawei-equipment-core-network-across-europe-security-concerns
  2. http://www.newelectronics.co.uk/electronics-blogs/vodafone-announces-pause-in-use-of-huawei-equipment/207334/

2.1.6 法國政府加強對 5G 通信設備控管

路透社報導，法國政府宣布將加強對下一代 5G 電信設備的控制，相關法案刻正研手擬之中。

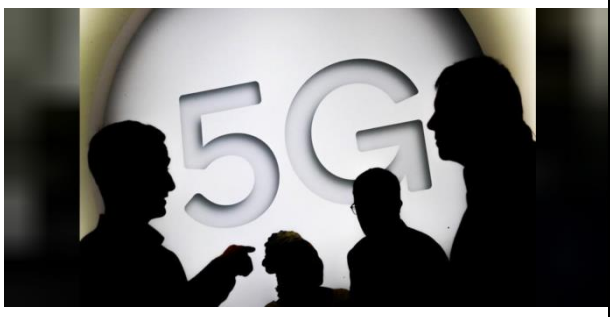
一名法國財政部官員指出，加強控管的措施並非針對特定電信設設備供應商；但華為很顯然是新法案控管的對象之一。目前包括美國、英國、澳洲、紐西蘭、德國、日本、台灣等國，都已加強對華為設備的限制。

法國外交部長 Jean-Yves Drian 於 1 月 20 表示，法國當局十分清楚華為設備可能帶來的風險，也會在需要時採取措施以防範任何資安與國安危機。

新法施行後，將會針對法律認定存有被竊聽或用於間諜活動的部分電信設備設限；業者需要先獲得政府正

式批准，才可以使用該項設備。

去年年底，法國電信業者 Orange 已經正式宣布，將不在未來的 5G 基礎建設中採用華為設備。



圖片來源：
https://www.reuters.com/article/us-france-telecom-huawei/france-tightens-5g-network-controls-amid-huawei-backlash-idUSKCN1PJ1T6

- 資料來源：
  1. https://www.reuters.com/article/us-france-telecom-huawei/france-tightens-5g-network-controls-amid-huawei-backlash-idUSKCN1PJ1T6
  2. https://www.lightreading.com/mobile/5g/orange-rules-out-huawei-for-5g-in-france/d/d-id/748274

2.1.7 調查指出，每個 PC 遊戲玩家平均遭到駭客攻擊 5 次，資安習慣仍待提升

McAfee 針對每個月以 PC 或筆電至少玩四次遊戲，而且一年在遊戲上花費超過 200 美元的美國境內遊戲玩家進行問卷調查，報告提供了一些值得參考的數字。

正面的數字包括：

- *75% 的遊戲玩家認同資安對於 PC 遊戲的未來發展，是非常重要的。*
- *64% 的遊戲玩家表示聽說過其他玩家曾遭遇網路攻擊而受影響。*
- *83% 的遊戲玩家都在電腦上裝了防毒軟體。*

但也有一些令人擔憂的數字：

- *55% 的玩家在多個遊戲中使用相同的密碼。*
- *36% 的玩家會用瀏覽器的私密瀏覽功能，但這並無助於保護電腦不受攻擊。*
- *41% 會去讀遊戲和相關服務的隱私條款，但這樣對保護電腦並無助益。*

針對如何提高遊戲玩家的資安意識，McAfee 提供以下建議：

- *每個遊戲都應分別使用不同的帳號密碼，減少被一次攻破的機會。*
- *使用防火牆阻擋不明網路入侵。*
- *按下任何連結前都要小心，以免駭客透過釣魚郵件或訊息傳送惡意軟體安裝連結，或不小心提供自己的個資。*

圖片來源：
https://www.helpnetsecurity.com/2019/01/07/the-future-of-gaming-security/

- 資料來源：
  1. https://www.helpnetsecurity.com/2019/01/07/the-future-of-gaming-security/
  2. https://www.mediaplaynews.com/mcafee-gamers-worried-about-cybersecurity/
  3. https://www.apnews.com/09212eb4c23940b3b3043c20dde467eb

2.1.8 PS4、Xbox One、微軟 Surface 等超過十億台裝置，WiFi 韌體存有遠端程式碼執行漏洞

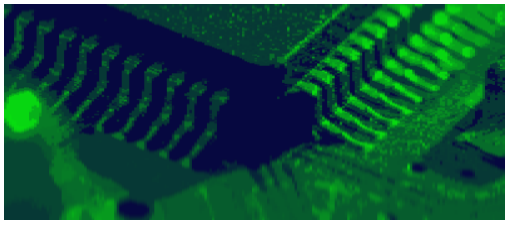
以嵌入式系統為主要研究的資安廠商 Embedi 研究人員 Denis Selianin 指出，廣泛用於各型連網設備的 Marvell WiFi 單晶片，其韌體存有安全漏洞；攻擊者能利用此漏洞，在不干擾用戶界面情形下遠端執行程式碼。

Selianin 的研究報告指稱，該漏洞出現於 Marvell Avastar 88W8897 使用的即時作業系統 ThreadX；這種即時作業系統廣泛運用在各種連網設備中。

報告指出，採用此 WiFi 晶片組因而受此漏洞影響的連網裝置，包括 Sony PlayStation 4、微軟 Xbox One、微軟 Surface 電腦系列、三星 Chromeboook 系列、三星 Galaxy J1 手機等等，總數恐多達十億台以上。

Selianin 報告中詳述了此錯誤，及可行的數種攻擊手法，其中一種可用

以攻擊所有採用 ThreadX 韌體的裝置。據 TheradX 官網資料所示，採用此韌體而可能受影響的裝置多達 62 億台。



圖片來源：https://www.zdnet.com/article/wifi-firmware-bug-affects-laptops-smartphones-routers-gaming-devices/

- 資料來源：
  1. https://www.zdnet.com/article/wifi-firmware-bug-affects-laptops-smartphones-routers-gaming-devices/
  2. https://embedi.org/blog/remotely-compromise-devices-by-using-bugs-in-marvell-avastar-wi-fi-from-zero-knowledge-to-zero-click-rce/

2.1.9 Fortnite 遊戲平台漏洞，兩億玩家帳密與個資面臨外洩風險

資安廠商 Check Point 指出，擁有兩億全球玩家，近年來大受歡迎的線上對戰遊戲 Fortnite 存有多個安全漏洞，受害玩家的帳號密碼可能遭惡意人士竊取並用以購買遊戲中的虛擬貨幣，甚至連遊戲玩家間的語音對話記錄都可能外洩。

過去這類遊戲的惡意攻擊，通常是利用釣魚郵件等方式，以贈送遊戲虛擬貨幣或寶物、道具等為餌，誘騙玩家在假網站輸入自己的帳號密碼；但 Check Point 指出，他們發現在某些 Epic Games 的網站中存有 XSS 攻擊漏洞，用戶無需輸入帳密，只要點擊惡意連結，攻擊者就能取得受害者帳密。

Check Point 的研究文章完整說明了攻擊手法和過程，而 Epic Games 也表示他們已經修復這些漏洞。目前尚未傳出有玩家因此手法受害。

圖片來源：https://research.checkpoint.com/hacking-fortnite/

- 資料來源：
  1. https://research.checkpoint.com/hacking-fortnite/
  2. https://gamedaily.biz/article/525/epic-patches-security-hack-that-may-have-exposed-more-than-200-million-players-data
  3. http://www.gamasutra.com/view/news/334524/Epic_fixes_Fortnite_security_flaw_which_left_all_200M_players_vulnerable.php

2.1.10 美國資安與基礎建設安全局發出緊急公告，要求美國各單位加強防範 DNS 竄改攻擊

CISA 在公告中指出，該單位最近正在追蹤一系列涉及 DNS 竄攻的攻擊事件，也已通知遭攻擊單位進行必要修補措施。

CISA 同時指出，攻擊者通常先透過各種手法取得或變更 DNS 管理者的登入訊息，取得 DNS 管理權後，接下來就會竄改 DNS 中的 A、MX、NS 等重要記錄，將流量與內含資訊導向至攻擊者自有的系統中。

此外，由於攻擊者取得了 DNS 管理權，因此也能取得並控制該網域的加密憑證設定；因此攻擊者將能將導入的流量和資訊加以解密運用，而外界無法察覺異狀。

CISA 要求美國政府各單位十個工作天內採取以下措施，加強 DNS 防護：

- *全面檢視 DNS 設定與記錄，若有異常指向不明主機，應立即回報；*
- *全面更換 DNS 管理帳號之密碼；*
- *DNS 管理帳號全面實施多步驟認證，以防釣魚攻擊；無法實施者應立即向 CISA 回報主機名稱、期限內無法實施之原因，以及預定實施日期；*
- *監控網域憑證記錄檔：CISA 即日起將定期公告新增憑證資訊，各單位若發現自己並未申請該憑證，應立即回報。*

此外，CISA 也會提供美國政府各單位必要的技術支援與資訊。

圖片來源：https://boingboing.net/2019/01/22/dhs-dns.html

● 資料來源：
1. https://cyber.dhs.gov/ed/19-01/
2. https://www.cyberscoop.com/dhs-dns-directive-government-shutdown/
3. https://boingboing.net/2019/01/22/dhs-dns.html

2.1.11 伊朗疑涉入全球性 DNS 攔截綁架攻擊

近來許多中東、北非、北美和歐洲的政府組織、ISP、網路基礎設施、電信服務業者、重要商業組織紛紛遭到 DNS 攔截綁架攻擊事件；美國資安公司 FireEye 指出，有相當證據證明這些攻擊事件和伊朗政府有關。

雖然目前還無法確認攻擊者的身分，但 FireEye 發現，用來存取遭攻擊單位裝置的 IP，過去曾經用在由伊朗發動的網路攻擊事件之中。

這一連串攻擊事件中，攻擊者同時使用三種不同手法操弄 DNS，並攔截竊取受害者的網路通訊。其中一種攻擊手法是以竊得的登入資訊，進入 DNS 管理者的管理界面竄改 DNS 的 A 記錄，以便取得郵件通聯內容；另一種則是在駭入受害者的域名註冊者後更改 DNS 的 NS 記錄。

為避免遭到懷疑，入侵者使用免費的 Let's Encrypt 加密認證，因此受害者僅會感到連線稍微變慢，很難發現任何竄改跡象。

圖片來源：https://www.securityweek.com/dns-hijack-how-avoid-being-victim

● 資料來源：
1. https://www.securityweek.com/iran-linked-dns-hijacking-attacks-target-organizations-worldwide
2. https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

2.1.12 非營利青年組織 AIESEC 遭爆會員資料未加保護

自稱是全球最大由青年維運的非營利組織，分支單位跨 126 個國家，會員多達十萬人的「國際經濟學商會學生會」（AIESEC），日前遭資安研究人員發現存有嚴重的資安疏失。

獨立資安研究員 Bob Diachenko 在本月 11 日發現 AIESEC 透過 Elasticsearch 資料庫儲存的實習生申請表單，存於未以密碼保護的伺服器上。

資料庫表單的欄位，包含實習申請者的姓名、性別、生日、申請原因等資料；如申請未通過，其日期與時間戳記也會記錄在資料庫中。

AIESEC 表示這個資安疏失在由 Diachenko 揭露前二十天，就已經處在未保護狀態下，可能有四十人、約五十筆資料遭不當存取；目前該問題已經修正。

由於 AIESEC 的伺服器位在歐盟境內，而非營利組織並未排除在 GDPR 的管轄之外，因此罰金可能高達兩千萬歐元，或其全球年營收的 4%。

圖片來源：
https://securitydiscovery.com/aiesec-data-breach/

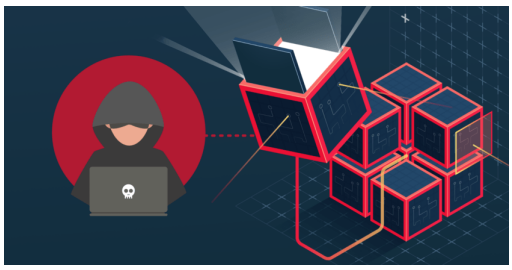
- 資料來源：
  1. http://securitydiscovery.com/aiesec-data-breach/
  2. https://blog.aiesec.org/statement-of-the-potential-security-incident-on-aiesec-platform/
  3. https://techcrunch.com/2019/01/21/aiesec-data-leak/

2.1.13 五大虛擬主機供應商後台可被輕易駭入

Website Planet 測試廣受歡迎，用戶眾多的五大虛擬主機供應商，發現各大主機商的後台都很容易駭入。

該文測試的五家虛擬主機供應商分別是 Bluehost、Dreamhost、HostGator、OVH 和 iPage。

Website Planet 委託資安專家 Paulos Yibelo 研究各虛擬主機廠商的安全漏洞，結果發現這五家廠商分別存有帳號管理權被大量取得、資訊遭竊、資安機制被破解或跳過等危險。詳細的報告詳見參考連結。



圖片來源：
https://www.websiteplanet.com/blog/report-popular-hosting-hacked/

- 資料來源：
  1. https://www.websiteplanet.com/blog/report-popular-hosting-hacked/

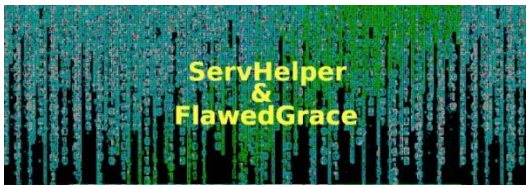
2.1.14 駭侵組織 TA505 發動新型態惡意軟體攻擊：ServHelper 與 FlawedGrace

Proofpoint 指出，ServHelper 和 FlawedGrace 分別為全新的惡意軟體。前者有兩種變體，分別用在去年 11 月的兩波 Email 攻擊事件中；以其中一波為例，ServHelper 在感染後會在宿主電腦建立反向 SSH 連結通道，讓駭侵者能透過 RDP 遠端控制受害電腦。

Proofpoint 的觀察也發現，在某些 ServHelper 的惡意軟體下載攻擊中，也出現下載另一支惡意軟體 FlawedGrace 的指令碼；根據分析，FlawedGrace 屬於遠端存取木馬，會以複雜的加密過程儲存其設定檔。

Proofpoint 指出，TA505 最近主要

的攻擊目標鎖定在金融機構。



圖片來源：
https://www.bleepingcomputer.com/news/security/ta505-group-adopts-new-servhelper-backdoor-and-flawedgrace-rat/

- 資料來源：
  1. https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
  2. https://www.bleepingcomputer.com/news/security/ta505-group-adopts-new-servhelper-backdoor-and-flawedgrace-rat/

2.1.15 IcePick-3PC 惡意軟體，鎖定媒體、電商網站，大規模竊取用戶 IP

據 Media Trust 的數位安全與營運團隊 (DSO) 指出，IcePick-3 主要以入侵廣泛用在網站頁面上的第三方插件為主，會先檢測連入用戶的 User Agent、裝置類別、是否為 Android 裝置、電池電量、裝置運動狀況與顯示橫豎方向等資訊；一旦確認該裝置為 Android 系統，便會進行 RTC P2P 連結，將受感染裝置的 IP 傳送出去。

用戶一旦遭感染，就等於門戶大開，後續將可能遭到各種各樣的攻擊。

DSO 同時指出這支惡意軟體甚至能夠穿越 VPN 連線，取得裝置的實體 IP，因此竊取規模超過所有該組織觀察到的案例；DSO 認為，以這支惡意軟體使用的先進技術來說，極可能和組織化的駭侵行動有關。

據 Media Trust 新聞稿，該公司有超過百家客戶受到 IcePick-3PC 的影響，主要集中在媒體、電商、醫療等產業。

圖片來源：
https://mediatrust.com/blog/icepick-3pc-new-malware-steals-device-ip-en-masse

- 資料來源：
  1. https://mediatrust.com/blog/icepick-3pc-new-malware-steals-device-ip-en-masse
  2. https://threatpost.com/icepick-adware-analysis/140722/
  3. https://www.infosecurity-magazine.com/news/icepick3pc-malware-strain-steals/

2.2、駭客攻擊事件及手法

2.2.1 台北市衛生局公衛系統疑遭中國駭客入侵，近三百萬筆個資外流

據台北市衛生局新聞稿指出：臺北市政府資訊局執行例行性資安檢核，於 107 年 8 月 28 日主動通知衛生局資訊系統遭不當存取，臺北市政府衛生局立即向國家資通安全會報技術服務中心進行資安通報，並協請調查局及臺北市政府警察局全力偵辦，經數月調查後，確認不當存取來源 IP 為境外；不當存取資料為北市 97 年戶政資料 298 萬餘筆，資料欄位包含姓名、生日、身分證字號、地址等。

據媒體報導，該批資料已在暗網上待價而沽；但駭客取得的是十年前的舊資料，而非新的個資。

亦有媒體報導，同一批駭客也攻擊國內外各公私單位，已成功入侵全球 38 個國家共 1509 個網站，手中握有多達九十億個資；而國內有近四十個政府機關、公立醫院、上市公司網站等都曾被同一批駭客入侵。

攻擊手法

據媒體報導，調查局指出駭客先鎖定資安防護較差的中小企業網站，植入「一句話木馬」程式，取得管理權後，透過這些網站做為跳板，於 2014 年及 2017 年間二度攻擊北市衛生局電腦主機，竊取 298 萬筆個資。

圖片來源：https://health.gov.taipei/News_Content.aspx?n=BB5A41BA1E6CA260&sms=72544237BBE4C5F6&s=5D7AE3A66E3B0D65

- 資料來源：
  1. https://health.gov.taipei/News_Content.aspx?n=BB5A41BA1E6CA260&sms=72544237BBE4C5F6&s=5D7AE3A66E3B0D65
  2. http://news.ltn.com.tw/news/society/breakingnews/2659779
  3. https://www.businesstoday.com.tw/article/category/80392/post/201809130028/北市衛生局公衛系統遭駭%20上百萬筆個資恐外洩

2.2.2 德國上千政治人物個資遭竊，連首相也無法倖免

德國傳出重大駭侵事件，超過一千名以上的德國各級政治人物個資遭到駭客竊取，受害者甚至包括德國首相梅克爾在列。

根據報導，這些政治人物被竊取的資料，包括個人的 email 地址、身分證上的大頭照、手機號碼、通聯記錄、財務記錄等等。一個 ID 為 G0D 的 Twitter 帳號在網路上散布這些資料。

德國政府對這起資料駭侵事件十分重視，目前除積極調查外，也尋求美國的協助。

2015 年德國國會亦曾遭駭，當時德國國會的資訊訊統遭到入侵，共有 16GB 的資料遭竊；資安廠商趨勢科技認為該次事件幕後駭客組織 Pawn Storm 可能和俄羅斯有關。

攻擊手法

本次攻擊事件可能是典型的「社交工程」(social engineering) 型駭侵手法。駭客先取得受害者的 Facebook 和 Twitter 密碼，然後透過社群網路進一步散布並擴大駭侵範圍。

圖片來源：
https://www.bloomberg.com/news/articles/2019-01-06/germany-seeks-u-s-assistance-after-hacking-breach-bild-reports

- 資料來源：
  1. https://www.bloomberg.com/news/articles/2019-01-06/germany-seeks-u-s-assistance-after-hacking-breach-bild-reports
  2. https://www.forbes.com/sites/daveywinder/2019/01/05/russia-or-the-far-right-who-hacked-german-politics/#210ffcef12c1
  3. https://www.thelocal.de/20190104/personal-details-of-politicians-revealed-in-huge-hack-on-bundestag-mps

2.2.3 美國西岸數家大報因惡意軟體而延遲出報

來自美國境外的惡意軟體攻擊，造成美國數家大型報社出報遭到阻礙，因而延遲出報。

因攻擊而延遲出報的報紙，主要以《洛杉磯時報》和《聖地牙哥聯合論壇報》的周末版為主，另外透過《洛杉磯時報》印刷廠印製的西岸版《紐約時報》和《華爾街日報》也遭波及。

《洛杉磯時報》引述知情人士指稱，「我們認為這次攻擊的目的是要癱瘓我們的基礎設施，特別是伺服器，而非竊取資料。」

通常 Ryuk 的勒索金額從 15 到 50 個比特幣不等，資安公司 Check Point 指出 Ryuk 在去年八月的攻擊中獲得約六十萬美元的不法利益；而這次攻擊事件中該惡意軟體向論壇報系勒索多少金額，目前還不清楚。

攻擊手法

據調查，此攻擊事件和一支名為 Ryuk 的綁架軟體有關。此軟體攻擊論壇報系位於芝加哥總部的伺服器，致使旗下多家報紙印製作業受到影響。

據資安公司 Sophos 和 Check Point 調查指出，其名稱來自知名漫畫《死亡筆記本》；不像其他惡意軟體透過大量擴散感染，Ryuk 主要針對特定對象，受害者多為製造業或醫療產業等。

Ryuk 主要鎖定安全防護較弱的遠端桌面遙控協定(RDP)密碼進行攻擊，取得控制權限後即關閉資安防護軟體，加密本機檔案，並感染其他系統。

圖片來源：https://www.securityweek.com/ryuk-ransomware-suspected-us-newspaper-attack

- 資料來源：
  1. https://www.securityweek.com/ryuk-ransomware-suspected-us-newspaper-attack
  2. https://www.securityweek.com/cyberattack-hits-us-newspaper-deliveries-report
  3. http://www.govtech.com/security/Ryuk-Malware-Tailor-Made-for-Maximum-Disruption.html

2.2.4 資料竊取惡意軟體 FormBook 再次透過免費檔案儲存空間肆虐

一支早在 2016 年就被發現，會竊取用戶 Windows 電腦中各種帳號密碼的惡意軟體 FormBook，最近被資安研究人員發現再次透過免費檔案空間活躍；目前北美地區已有眾多受害者。

攻擊手法

FormBook 的典型攻擊手法，是透過詐騙郵件進行。用戶點開了詐騙郵件中含有惡意指令的 RTF 或 PDF 檔後，該惡意指令便會利用 Office 的指令執行漏洞（CVE-2012-0158 與 CVE-2017-11882），從一個才開站一周，叫做 DropMyBin 的檔案下載服務中下載 FormBook，並安裝於用戶的 Windows 系統中，成為開機自動背景執行的軟體。

一旦 FormBook 成功安裝並開始執行，就會盡可能竊取用戶電腦中的各種帳號密碼，例如瀏覽器、Email 和 FTP 軟體記錄的登入資訊，同時還會記錄並傳送用戶的按鍵動作，甚至還會偷拍用戶畫面截圖，將資料上傳至其伺服器。

資安廠商 DeepInstinct 完整描述了該惡意軟體的運作流程與特徵碼。

圖片來源：
https://www.technadu.com/security-researchers-report-formbook-malware-spike/56235/

- 資料來源：
  1. https://www.deepinstinct.com/2019/01/27/info-stealer-formbook-continues-activity-and-uses-a-new-malware-friendly-file-hosting-service/
  2. https://www.technadu.com/security-researchers-report-formbook-malware-spike/56235/

2.3、軟硬體漏洞資訊

2.3.1 MSHTML 引擎遠端程式碼執行漏洞

微軟 MSHTML 引擎驗證輸入過程中，被發現存有遠端程式碼執行漏洞。微軟已透過系統更新更改 MSHTML 引擎驗證輸入的方式，從而修補此一漏洞。

圖片來源：https://www.exefiles.com/zh-tw/dll/mshtml-dll/

- CVE 編號：CVE-2019-0541

- 影響產品：
  - IE 9、IE 10、IE 11
  - MS Office 365 ProPlus、MS Office 2016、MS Office 2019
  - MS Office 2010 SP 2、MS Office 2013 RT SP1、MS Office 2013 SP1
  - MS Excel Viewer 2007 SP3、MS Office Word Viewer

- 解決辦法：
  透過系統更新自動完成漏洞修補。

- 資料來源：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0541
  2. https://www.securityfocus.com/bid/106402/info
  3. https://www.cvedetails.com/cve/CVE-2019-0541/

2.3.2 D-Link 路由器部分產品發現可進行遠端執行程式碼漏洞

資安研究單位 CyCarrier CSIRT 研究員 Harry Huang 發現部分 D-Link 路由器產品內含兩種安全漏洞，D-Link 已經提供修補漏洞用之更新版本韌體。

圖片來源：https://www.bhphotovideo.com/c/product/971699-REG/d_link_dir_820l_ac1000_dual_band_cloud.html

- CVE 編號：CVE-2018-20674

- 影響產品：
  - DIR-850L Rev. A 所有版本
  - DIR-805L Rev. B 所有版本
  - DIR-880L Rev.A 所有版本
  - DIR-822 Rev. C1
  - DIR-822-US Rev. C1

- 解決辦法：
  用戶可檢視路由器產品之標籤，確認產品型號是否名列受影響列表，並進行韌體更新以修補漏洞。

- 資料來源：
  1. https://securityadvisories.dlink.com/announcement/publication.aspx?name=SAP10101
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20674

2.4、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。

第 3 章、 2019 年 1 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 1 月情資總計 75,278 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。

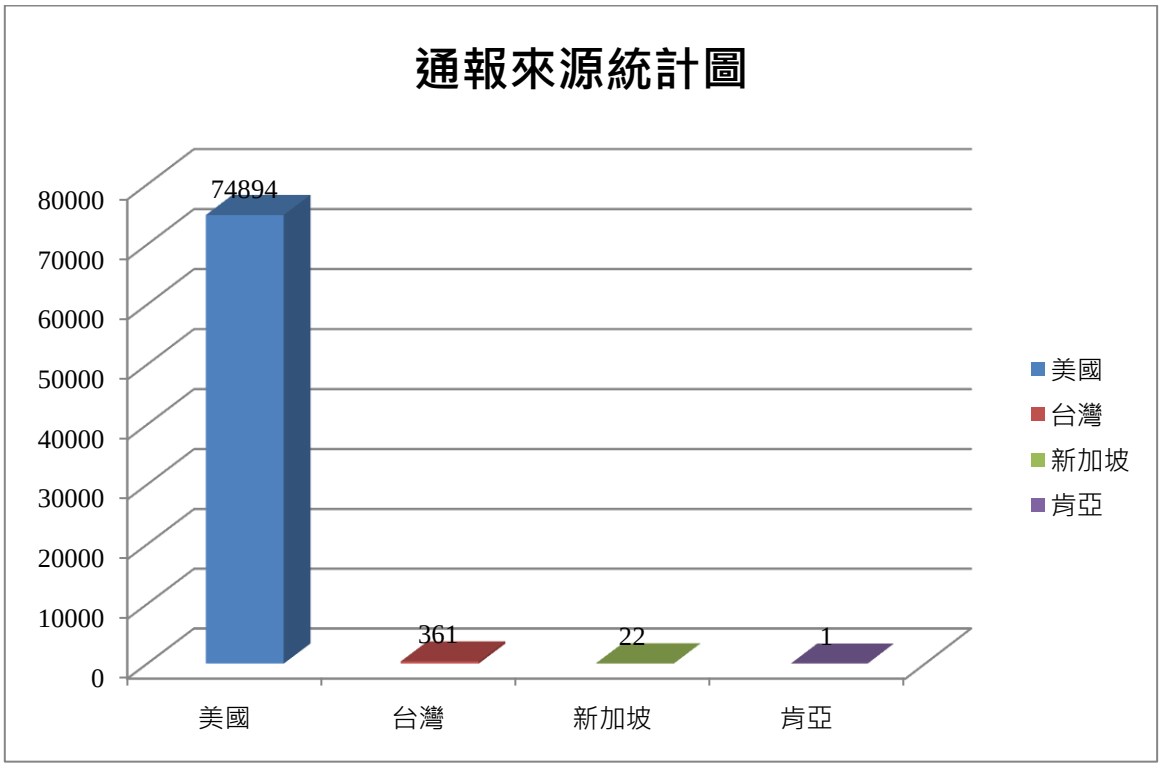


圖 1、通報來源統計圖

圖 2、通報對象統計圖

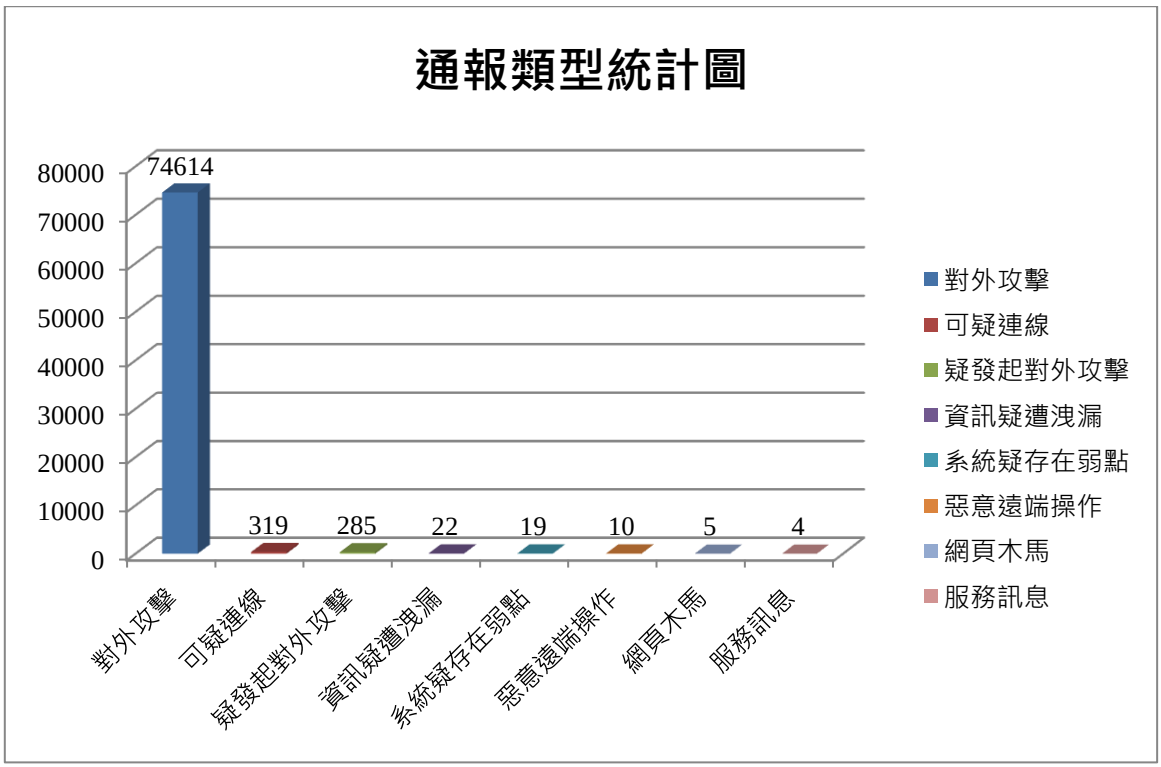


圖 3、通報類型統計圖

本中心近期接獲通報，有大量網頁使用者之帳號密碼外洩，除台灣之使用者外，國際他國同樣有網站及其使用者之帳號密碼被公開於某網頁上。

本中心已調查此些帳號密碼之網域所屬單位，並進行相關之通報，告知各負責單位恐有資料外洩疑慮，應盡速進行處理。而截至目前已有數家單位回報已進行處理並公告，請諸位使用者放心。

此通報並未說明如何取得此些資料，僅是由某資安單位於某國際網頁中發現此統合之帳號密碼清單。

因此，本中心在此提醒系統管理員，請定期檢查單位內資訊設備是否遭受惡意程式感染；若資訊設備已遭入侵，建議重新安裝作業系統，並更新至最新修補程式，同時安裝防毒軟體並更新至最新版本，亦注意病毒碼須持續更新。

對一般使用者而言，本中心呼籲使用者應定期更新密碼，並且應使用高強度之密碼，建議至少由 8 個以上字元組成，並混合英、數、以及特殊字元，並盡量不使用有意義之單詞，以免容易遭有心人士以猜測或暴力破解之方式取得該密碼。

- 參考連結：
  1. https://support.google.com/accounts/answer/32040?hl=zh-Hant

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 1 月 17 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/