TWCERT/CC 資安情資電子報

2019 年 12 月份

目錄

第 1 章、 封面故事

歐洲最大級飯店訂房系統公司近 1TB 旅客資料於網路曝光

資安研究人員發現，一家歐洲最大級飯店訂房系統公司的顧客資料庫在網路公眾伺服器上曝光，全無任何保護，受害旅客人數高達 14 萬人。

歐洲最大飯店系統，法國 AccorHotels 旗下的飯店訂房系統么司 Gekko Group，被資安研究人員發現一個曝露在 Elasticsearch 公眾伺服器上，全無保護措施且能輕鬆搜尋到的超大型旅客資料庫，檔案大小高達 1TB 以上。

該資料庫內容包括眾多透過該公司訂房顧客的各項個資，包括姓名、住家地址、投宿飯店資訊、隨行兒童個資、信用卡號碼，以及近萬筆以明文儲存的密碼資訊；受害者人數高達 14 萬人以上，包括個人、旅行團與公司行號。

更糟的是，除了該資料庫內儲存的信用卡資料可能外洩之外，資料庫內的密碼更包括世界衛生組織（WHO）差旅用的帳號與密碼；這表示駭侵者可以利用該組織的預算來訂房。

可利用 Gekko Group 訂房的飯店遍及全球，數量達到六十萬間以上；Gekko Group 的 CEO 受訪時表示已經針對該資料庫加強資安防護，並啟動對內部 IT 系統的調查作業。

- 資料來源：
  1. https://www.cnet.com/g00/news/exposed-database-left-terabyte-of-]travelers-data-open-to-the-public/?i10c.ua=4&i10c.encReferrer=&i10c.dv=15 /

第 2 章、 資安宣導

注意 E-Mail 位址！台北市政府警察局提醒小心遭到商業電子郵件詐騙

由於國內的企業，經常習慣使用電子郵件與客戶聯繫，而歹徒可能在駭入公司系統後長期潛伏，並且觀察企業與合作單位之郵件的往來，或進行網路監聽，搜集並分析該公司的相關交易資訊，並且藉由極為相似之電子郵件傳送給該公司進行詐騙。

案例：臺中市某鞋品貿易公司遭詐騙集團鎖定，掌握林姓業務與國外合作公司(下稱 A 公司)有一筆應付款項，仿照 A 公司業務的電子郵件帳號「xxxxxdaixx@163. com」，設立名稱相似的「xxxxxdeaixx@163.com」假帳號發信給該名林姓業務，謊稱原帳戶因稅務問題進行整併中，要求變更匯款帳戶至瑞典北歐斯安銀行之境外帳戶，林姓業務所屬公司因與 A 公司長期合作，遂不疑有他，直接以傳真銀行方式匯出臺幣數十萬元。孰料 5 天後，A 公司通知並未收到匯款，林姓業務連忙找出當初聯繫之電子郵件內容，發現假帳號竟多了 1 個 e 字母，「e」字之差使公司損失達數十萬元。

類詐騙手法略述如下：

(一) 詐騙集團攔截被害人公司交易信件，並申請與企業客戶電子郵件地址

相似度極高的假郵件使之混淆（如前揭案 例僅多一個字母「e」，歹徒所設立「xxxxxdeaixx@163. com」電子郵件與原本使用「xxxxxdaixx@163.com」極為相似）。

(二) 模仿原本往來郵件的語氣發信給被駭企業之客戶，騙取企業或客戶變更匯款帳戶，藉機詐騙被害人將貨款匯至詐騙集團所預設帳戶。

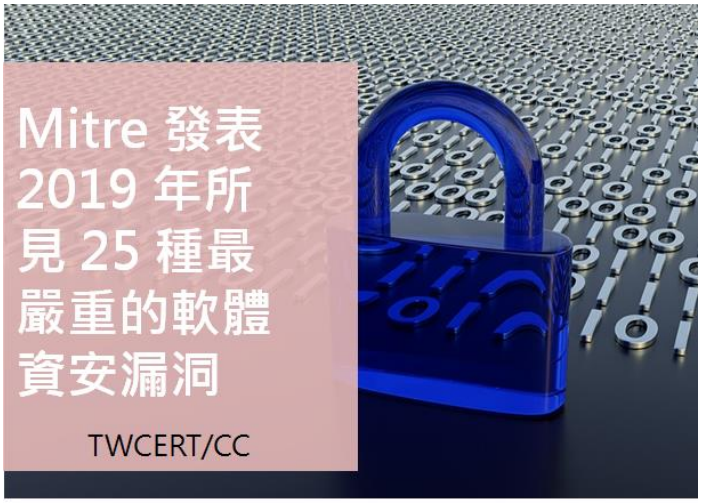
(三) 取得企業客戶的信任而匯款，俟原受款客戶反映未收到貨款時，方知受騙。

因此，請使用者務必提高警覺，面對商業上的信件，務必細心觀察及多方檢視，以免遭到詐騙！

第 3 章、 國內外重要資安事件

3.1、資安趨勢

3.1.1 Mitre 發表 2019 年所見 25 種最嚴重的軟體資安漏洞



資安漏洞統計單位 Mitre.org 列出今年的 25 種最嚴重、危險程度最高的軟體資安漏洞列表，供軟體開發與資安界列為重要資安參考指標。

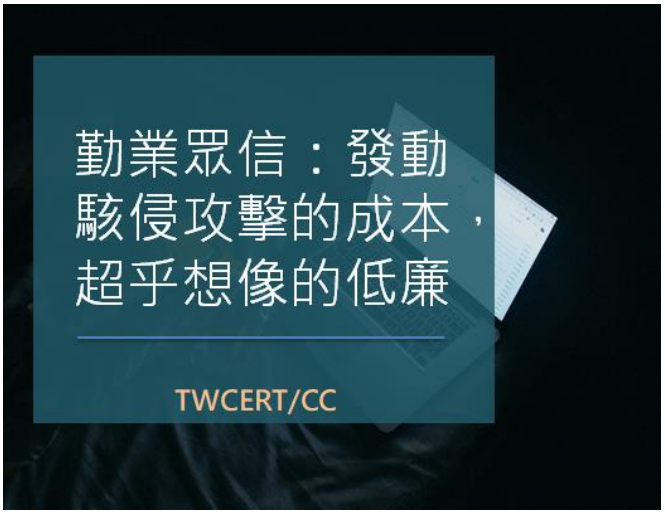
這分「常見資安弱點列表」（Common Weakness Enumeration）是 Mitre.org 綜合評估多項指標而得，包括在不同軟體間發現相同類型漏洞的次數、該漏洞被利用於駭侵攻擊的次數、因該漏洞造成的損失規模等等。

在列表中排名最高分的常見軟體漏洞，是記憶體暫存區界限的不當操作限制（Improper Restric of Operations within the Bounds of a Memory Buffer）；這個漏洞讓駭侵者可以存取限制區域外的記憶體內容。

排名第二的是常見的 XSS 網頁程式漏洞，第三名則是不適當的輸入內容驗證錯誤。詳細的列表與說明，可參考 Mitre 發表的文件。

- 資料來源：
  1. https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

3.1.2 勤業眾信：發動駭侵攻擊的成本，超乎想像的低廉



駭侵攻擊與一般企業營運一樣，同樣存在營運成本、投資報酬率等財務考量。最近勤業眾信的一份調查報告指出，發動駭侵攻擊的成本其實相當低，遠低於企業的資安支出。

駭侵攻擊是不是一本萬利的工作？根據勤業眾信最近發表的調查報告，似乎確實如此。

該報告收集各種暗網上的「報價」，計入發動攻擊所需的各種資源，包括惡意網站與程式碼的 hosting、發送、攻擊對象名單等，列舉出常見攻擊形態的成本如下：

- 完整的釣魚信件攻擊服務（包括 hosting、套件）：平均一個月 500 美元，也有便宜到 30 美元月費起跳的。

- 資訊竊取攻擊，如按鍵記錄器或惡意軟體，包括 hosting 與發送，平均一個月 723 美元，最低月費 183 美元。

- 勒贖攻擊或遠端遙控木馬攻擊：平均一次 1,000 美元左右。

- 針對銀行帳戶的駭侵攻擊，起跳價約 1,400 美元，最高可達 3,500 美元。

勤業眾信也指出，最低成的的駭侵攻擊只要一個月 34 美元，但不法所得可高達 25,000 美元；更複雜的駭侵攻擊可能需要幾千美元成本，但獲利卻高達每月一百萬美元以上。

相對的，企業維持資安，通常得花大筆預算，成本遠遠高於駭侵攻擊；卡巴斯基指出一般企業一年的資安預算約為九百萬美元，和攻擊成本根本是天壤之別。

- 資料來源：
  1. https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

3.2、國際政府組織資安資訊

3.2.1 APT41 駭入電信公司機房，直接竊取簡訊通聯記錄

資安公司 FireEye 發表研究報告，指出來自中國的 APT41 駭侵組織，透過新開發的惡意軟體，駭入某電信公司用以處理簡訊通訊的 Linux 主機，直接竊取特定電話號碼使用者的 SMS 簡訊通聯記錄。

APT41 使用該組織開發的惡意軟體 MESSAGETAP，駭入該電信業者用以處理簡訊路由的 Linux 主機叢集，而且早在 2012 年起就開始這個駭侵行為，一直到日前才被發現。

MESSAGETAP 在電信機房中會監看特定對象的 SMS 對話內容，一旦發現內容符合某些關鍵字，便會將訊息內容存檔並傳回。關鍵字的內容與中國地緣政治利益相關，而被監聽的對象則包括反對中國的各國政治領袖、軍事與智庫單位的重要人物等。

FireEye 在報告中詳細描述了這個惡意軟體的運作方式，同時指控 APT41 的駭侵行為，為中國政府間諜活動的一部分。除了電信公司外，APT41 同時也針對可能存有上述人士相關活動資料的單位進行駭侵攻擊，例如大型旅行社、醫療單位等。

- 攻擊手法：利用惡意軟體駭入電信公司機房
- 關鍵字：APT41, Wiretap, Malware
- 資料來源：
  1. https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html

3.2.2 FBI 警告：駭侵組織正在鎖定美國汽車工業進行攻擊

據CNN 報導，日前美國聯邦調查局對部分美國汽車業者提出警告，指出有駭侵組織成功利用網路漏洞，入侵部分汽車業者的電腦系統。

FBI 指出，近日美國汽車業者遭到各種各樣的駭侵攻擊，包括暴力登入嘗試、釣魚郵件、軟硬體漏洞攻擊等。

這些駭侵攻擊已經成功在業者的電腦系統中植入勒贖軟體、取得資料存取權限，並竊取可辨識個人的多種資訊。

FBI 也說，由於自動駕駛汽車、連網汽車的日益普及，未來汽車工業將會面對數量更多、技術更複雜成熟、樣態更多樣、規模也更大的駭侵攻擊。

不過，到底是哪些駭侵團體攻擊汽車業者、背後有哪些國家力量支持， FBI 並未明確指出。

- 資料來源：

1. https://edition.cnn.com/2019/11/20/politics/fbi-us-auto-industry-hackers/index.html

3.2.3 PWN2OWN 東京駭客大賽落幕，多種手機、路由器、家用智慧裝置遭破解

全球知名的白帽駭客大賽「PWN2OWN」東京場剛剛結束，參賽的駭客破解多項連網裝置，多家知名品牌手機、路由器、家用智慧裝置等產品的漏洞遭參賽者突破。

2019 年十一月的 PWN2OWN 東京駭客大賽剛落幕，來自全球各地的白帽駭客與資安研究人員，今年又破解了多家廠商的各種連網產品，並且贏回高達 315,000 美元的獎金。

被參賽者破解的產品，包括 Amazon Echo Show 5、Sony X800G 智慧電視、Samsung Q60 智慧電視、Samsung Galaxy S10 手機、小米 Mi9 手機、TP-Link AC1750 無線路由器、NETGEAR R6700 無線路由器等。

也有一些廠商的產品沒有被參賽者列入駭侵目標，如 Google Nest 網路攝影機與 Facebook Portal Hub 等產品。

這些在比賽中被破解的產品，其漏洞資訊都會立即由廠商帶回，並儘快發補安全修補升級套件。

- 資料來源：
  1. https://www.zerodayinitiative.com/blog/2019/11/7/pwn2own-tokyo-2019-day-two-final-results
  2. https://threatpost.com/pwn2own-tokyo-2019-amazon-echo-hackers/150033/

3.2.4 日本經濟新聞遭企業郵件詐騙攻擊，損失超過 32 億日元

日本首屈一指的大型媒體集團日本經濟新聞(Nikkei)，日前確認於九月發生企業郵件詐騙事件，損失超過 32 億日元。

日經媒體集團的美國紐約子公司某員工，在九月時收到這封企業詐騙郵件，誤以為公司高層指示，將高達 2900 萬美元（合 32 億日元）的巨款，匯到位在香港的某家銀行帳戶。

日經在追查後確認這是一起企業郵件詐騙案（BEC, Business Email Compromise），但沒有說明事件發生的細節，僅在聲明中表示已循法律途徑設法追回這筆匯款。

BEC 詐騙通常是由於企業主機遭到入侵，或是重要主管的郵件帳號遭到駭入，駭入者便可利用受控的帳號來發送假命令給企業員工，發送匯款到詐騙帳戶中。

近年來 BEC 詐騙事件頻傳，除了日經之外，全球各大企業都曾受害；其中一個著名案例是一名立陶宛人假冒台灣廣達電腦名義，從 Google 和 Facebook 詐得一億美元巨款。

- 資料來源：
  1. https://www.nikkei.co.jp/nikkeiinfo/en/news/press/597.html
  2. https://www.helpnetsecurity.com/2019/11/05/nikkei-bec-scam/
  3. https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

3.2.5 英國兩大主要政黨均遭駭侵攻擊

英國兩大主要政黨，包括執政的保守黨與在野的工黨，近日均傳出遭駭侵攻擊的消息。

保守黨方面，據路透社報導，該黨的官方網站遭到不明來源的連續兩次猛烈攻擊，但未能迫使官網下線。

在工黨方面，其官方網站也兩度遭到來源不明的分散式服務阻斷攻擊（ DDoS），但攻擊未能奏效。工黨表示官網仍正常運作，且無任何資料遭到竊取。

工黨黨魁科爾賓對最近針對英國各政黨的駭侵攻擊表示憂心，他認為這些攻擊行動可能都和選舉相關。資安業者 ESET 則警告，這類針對政黨的駭侵行動將會逐漸升高，各政黨都應加強對應的相關訓練及準備工作。

- 攻擊手法：分散式服務阻斷攻擊（Distributed Denial of Service）
- 關鍵字：DDoS, UK
- 資料來源：
  1. https://www.reuters.com/article/us-britain-election-conservatives-cyber/uk-conservative-party-hit-by-cyber-attack-ahead-of-election-two-sources-idUSKBN1XM2IC
  2. https://www.telegraph.co.uk/technology/2019/11/12/cyber-attack-labour-just-beginning-warn-experts/

3.3、社群媒體資安近況

資安專家警告：「黑色星期五」之類購物狂潮，也是詐騙駭侵高峰

資安專家提出警告，許多詐騙駭侵行為，會在如「黑色星期五」之類的線上購物熱潮中趁機肆虐，用戶應特別提高警覺。

資安廠商 Check Point 的資安專家發表報告，指出各種駭侵詐騙行為，在購物熱季時會大幅上升。

報告指出，即使在如如「黑色星期五」或「網購星期一」這類線上購物大爆發的日子來到之前的十一月中，假冒促銷訊息的詐騙釣魚郵件就已經大量增加，數量甚至達到平常的 233%；而在報表發表的十一月底，這個數字甚至還提高到 275%。

典型的詐騙郵件會用極誇張的降價來引誘消費者，例如「設計師款太陽眼鏡大降 80%」這樣的文案；而這樣的詐騙連結亦可能大量出現在社群平台上，用戶必須提高警覺。

- 資料來源：
  1. hhttps://blog.checkpoint.com/2019/11/26/november-shopping-do-it-the-smart-way/
  2. https://www.forbes.com/sites/zakdoffman/2019/11/26/why-you-should-never-click-on-a-black-friday-email-deal/#61774a1941d2

3.4、行動裝置資安訊息

3.4.1 Android 表情符號鍵盤暗藏惡意訂閱詐騙機制，四千萬用戶受害

資安研究單位發現一支有四千萬次下載的 Android 表情符號鍵盤程式，內藏的惡意訂閱詐騙機制，已經造成用戶超過一千八百萬美元的損失。

資研研究單位 Secure-D 與 Upstream Systems 共同發表研究報告，指出一支名為「ai.type」的 Android 表情符號鍵盤程式，內含惡意訂閱和廣告詐騙點擊程式，除會在用戶不知情的狀況下，訂閱多個價格十分高昂的訂閱服務之外，還會進行廣告詐騙點擊。

由於這支 App 的下載次數高達四千萬次，受害者相當多，總共詐騙訂閱和廣告點擊金額，高達一千八百萬美元。

研究單位指出，ai.type 的詐騙機制十分巧妙，會偽裝成來自其他正常 Andriod App 的流量，像是 SoundCloud 的 App；提供的也是用戶真正的資料和評價，所以廣告聯播網和訂閱服務會誤以為這些都是正常點擊或訂閱。

這支 App 雖然已在今年六月遭到 Google Play Store 移除，但研究單位發現其詐騙點擊的高峰卻發生在七月；很可能是因為這支詐騙 App 仍然存在於 Android 第三方 App Store 上。

研究單位也指出，產生詐騙點擊的並不是 ai.type 本身的程式碼，而是開發者採用的程式開發框架（framework）與開發工具。

- 資料來源：

1. https://www.upstreamsystems.com/trick-treating-android-emoji-keyboard-app-makes-millions-unauthorized-purchases/
2. https://www.theregister.co.uk/2019/11/01/aitype_keyboard_malware_alert/

3.4.2 Qualcomm 晶片漏洞，致使各種 Android 手機存有個資外洩風險

資安廠商發現 Qualcomm 的手機晶片存有漏洞，可能致使攻擊者取得手機用戶的敏感個資。

資安廠商 Check Point 的研究人員發表報告，指出廣泛運用在 Android 手機中的 Qualcomm 處理器晶片漏洞，可能造成用戶個人資料外洩、手機被取得 Root 權限、Bootloader 解鎖、甚至讓駭侵者執行的程式無法被察覺。

Qualcomm 針對這些漏洞也已發表修補程式，並提供給各大手機 OEM 廠商；目前三星和 LG 已經在系統更新中加上這些修補，但其他廠商仍未釋出。

在 Check Point 的報告中，詳細描述了漏洞細節與可能的攻擊手法。

- 資料來源：

1. https://research.checkpoint.com/the-road-to-qualcomm-trustzone-apps-fuzzing/
2. https://thenextweb.com/security/2019/11/15/bugs-in-qualcomm-chips-leaked-private-data-from-samsung-and-lg-phones/

3.4.3 兩支 Android App 使用 Facebook、Twitter 登入機制竊取數百名用戶個資

Facebook 和 Twitter 近日發布公告，指出有兩支在 Google Play 上架的 Android App 利用不適當的權限，透過這兩家公司的登入機制竊取用戶個資。

這兩家公司表示，並非該公司的資安機制有問題，而是這兩支 App 使用的開發架構 OneAudience，會讓 App 與其開發者取得登入用戶的個資；會被存取的資訊包括用戶的 Email、用戶名稱、最近發布的推文內容。

被點名的 Android App 為 Giant Square 與 Photofy，據信因此導致個資外洩的受害用戶約有數百名。

Twitter 與 Facebook 均表示已經開始個別通知受害用戶，同時也已通報兩大行動平台業者 Google 與 Apple。

- 資料來源：
  1. https://help.twitter.com/en/sdk-issue
  2. https://www.cnbc.com/2019/11/25/facebook-and-twitter-says-users-gave-improper-access-to-personal-data.html

3.5、軟體系統資安議題

3.5.1 Firefox 瀏覽器 Bug 遭利用於勒贖詐騙

廣受歡迎的開源瀏覽器 Firefox 傳出遭多個詐騙網站利用於勒贖攻擊，威脅用戶撥打某支電話，否則就會將用戶的電腦鎖死。

資安廠商 MalwareBytes 的研究人員發現 Firefox 的這個 bug，已經被駭侵人員用於詐騙活動；用戶造訪某些假冒的技術支援網站時，其 Firefox 就會跳出假的警告視窗，指用戶使用盜版軟體，如不在五分鐘內撥打某支電話，其電腦將被鎖死。

這個惡意網站同時會鎖定用戶的 Firefox 瀏覽器，無法進行任何操作，只能透過作業系統強制關閉；但重新啟動 Firefox 後，如果不立即關閉先前開啟的惡意網站標籤頁，Firefox 又會再次被鎖定。

目前 Mozilla 已經開始處理這個問題，預計在下一版 Firefox 中會予以解決。用戶如果發現自己的瀏覽器亦遭鎖定，務必保持冷靜，絕對不要按照駭侵者指示操作，撥打該電話。

- 資料來源：
  1. https://bugzilla.mozilla.org/show_bug.cgi?id=1593795
  2. https://arstechnica.com/information-technology/2019/11/scammers-are-exploiting-an-unpatched-firefox-bug-to-send-users-into-a-panic

3.5.2 GitHub 上的惡意軟體，意圖竊取加密貨幣

資安廠商發現某個惡意軟體 dropper，感染後會從 GItHub 上下載惡意軟體，意圖竊取受害者的加密貨幣。

Deep Instanct 最近發現一個全新的惡意 dropper，大小僅有 30KB，一但感染後，會從 GitHub 下載安裝另一個惡意軟體，會試圖竊取受害者擁有的加密貨幣。

將惡意軟體放置在 GitHub，這種做法並不多見。該公司也已通報 GitHub。

會被這段惡意軟體竊取的加密貨幣，包括比特幣、萊特幣等多種常見加密貨幣，種類高達三百種。

在 Deep Instince 的報告中，詳述了這個 dropper 和惡意程式碼的運作過程。

- 資料來源：
  1. https://www.deepinstinct.com/2019/11/12/malware-on-github-wants-your-crypto-currencies/

3.5.3 MacOS 以明文儲存加密郵件，Apple 展開調查

專家發現 MacOS 的郵件程式存有重大錯誤，原本應以 S/MIME 加密儲存的郵件，在部分用戶的 MacOS 郵件資料庫中，竟以明文儲存。

這位蘋果 IT 專家 Bob Gandler 表示，當他正在研究 Siri 和 MacOS 作業系統如何向用戶推薦欲通訊的聯絡人與相關資料時，發現了這個漏洞。

Gandler 在其文章中指出，他發現 MacOS 會把可能會讓 Siri 用來推薦的郵件內容，以明文儲存在某個資料庫中，而且理應經過 S/MIME 加密過的郵件，也一樣以明文儲存；即使把 Siri 關掉，該資料庫的內容仍然是未經加密的。

Gandler 在六月底時將此問題通報 Apple，Apple 隔了三個月以上才回覆 Gandler，表示目前正在調查漏洞成因。Gandler 也說，這個問題似乎也並非發生在所有用戶身上。

Gandler 在其報告中提供了多種暫時對應方式，例如透過 MacOS 內建的 FileVault 功能把整個系統磁碟完全加密。

3.5.4 QNAP NAS 遭 QSnatch 感染，QNAP 已提出安全建議以清除惡意程式

根據 QNAP PSIRT 資訊，自 10/23 起，其陸續接獲德國及荷蘭的使用者通報其 ISP 偵測到有異常的網路行為。根據德國 CERT-Bund 公布的數據，在德國就已有 7,000 起之案例，其 ISP 已針對受害之用戶進行隔離處理。

經 QNAP 調查，此次事件主要是源於一被稱作 QSnatch 的惡意程式所造成。該惡意程式在感染了 NAS 系統後，會將惡意程式碼注入於受害系統中，並且修改系統設定以防止其韌體更新，以及關閉 QNAP 的防毒軟體 Malware Remover，並定期將資訊回傳給 C&C 伺服器，可能造成個資或機敏資料的外洩。

而 QNAP 為處理該事件，其提供了刪除該惡意程式之規則，且目前已推出最新版本之 Malware Remover 3.5.4.0/4.5.4.0，可以協助用戶清除 QSnatch 惡意程式，並提出以下建議：

1.將 QTS 更新至最新版本

2.安裝 Security Counselor，並更新至最新版本

3.安裝 Malware Remover，並更新至最新版本

4.應使用高強度的管理者密碼

5.應啟用 IP 以及帳戶存取防護，以避免遭受暴力攻擊

6.若非需要，應盡量關閉 SSH 與 Telnet 連線

7.應避免使用默認的 443 與 8080 埠。

- 資料來源：
  1. https://preview.qnap.com/en/security-advisory/nas-201911-01
  2. https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware

3.5.5 史上最大級資料外洩事件，12 億人個資未經保護對外曝光

資安研究人員發現史上最大級個資資料庫，未經任何保護，可借任何人自由存取；資料庫內含 12 億名以上不重覆用戶個資。

發現這個資料庫的資安研究人員是 Bob Diachenko 和 Vinny Troia。他們在一個未經保護的 Elasticsearch 伺服器發現這個資料庫，檔案大小高達 4TB，內含 40 億筆用戶資料，不重覆用戶人數高達 12 億人以上。

在這個資料庫中包含的用戶個資欄位，包括姓名、Email 地址、電話號碼、 LinkedIn 與 Facebook 帳號資訊等。

值得注意的是，這個龐大資料庫的個資，係來自兩家不同的資料收集處理業者 People Data Labs 和 OxyData.io；研究人員比對了自己在 People Data Labs 的資料與該外洩資料庫的資料，發現兩者完全吻合。

這個資料庫代管於 Google 雲端服務，目前不知道是誰把資料庫放上去的，也不清楚為何兩家公司的資料庫會被合併。

- 資料來源：
  1. https://www.dataviper.io/blog/2019/pdl-data-exposure-billion-people/

3.5.6 微軟發表惡意軟體警訊，至少八萬台電腦遭挖礦軟體劫持

微軟資安團隊 Microsoft Defender ATP Reserach Team 表示，至少八萬台電腦近來遭到一個名為 Dexphot 的惡意軟體入侵，利用 CPU 的運算能力挖礦。

研究人員是在去年十月首次發現這個惡意軟體，在今年七月觀察到活動最高峰。

研究人員表示，這個惡意軟體的感染過程中，採用非常多種匿蹤手法，甚至還會偵測系統上是否安裝防毒防駭軟體，並且定期自我更新。

微軟發布的報告中，詳細說明了這個惡意軟體的感染方式與運作流程。

- 關鍵字：Malware, cryptocurrency
- 資料來源：
  1. https://www.microsoft.com/security/blog/2019/11/26/insights-from-one-year-of-tracking-a-polymorphic-threat/
  2. https://threatpost.com/dexphot-malware-cryptocurrency/150634/

3.5.7 資安人員發現 BlueKeep 漏洞首宗大規模攻擊事件，用以安裝挖礦程式

由微軟在五月份公開的 Windows RDP 嚴重資安漏洞 BlueKeep（CVE-2019-0708），日前有資安研究單位截獲大規模全球駭侵攻擊。

資安研究人員架設陷阱，捕獲試圖攻擊此漏洞的駭侵活動，並發現駭侵者在駭入系統後，試圖安裝挖礦程式。

目前尚未發現該惡意攻擊有竊取任何資料的行為，也沒有發現自我散布的跡象。

據今年八月份的估計，全球還有約 735,000 台 Windows 伺服器主機仍有 BlueKeep 漏洞，尚未更新修補。

- 攻擊手法：透過 Windows BlueKeep RDP 漏洞安裝挖礦程式
- 關鍵字：BlueKeep, Windows RDP, Malware, Crypto, Miner
- 資料來源：
  1. https://twitter.com/GossiTheDog/status/1190654984553205761
  2. https://fossbytes.com/first-windows-bluekeep-attacks-spotted-installing-cryptocurrency-miners/

3.6、軟硬體漏洞資訊

3.6.1 Internet Explorer 再遭發現遠端執行 0-day 漏洞

資安研究單位 Resecurity 發現微軟 Internet Explorer 瀏覽器存有一個嚴重漏洞，可讓攻擊者遠端執行任意程式碼。

這個漏洞位於 IE 的 Jscript 垃圾收集機制中，駭侵者可利用記憶體崩潰錯誤，以和登入使用者相同的權限執行任意程式碼；如果用戶以系統管理者權限登入，攻擊者便可以系統管理者的權限，取得受害系統的控制權，包括安裝軟體、檢視、增刪並改寫檔案或用戶帳號。

Resecurity 於十月二十日將此漏洞向微軟通報，微軟已在十一月十二日推出安全修補軟體，請所有仍在使用 Internet Explorer 的 Windows 用戶，儘速安裝安全修補軟體。

- CVE 編號：CVE-2019-1429
- 影響產品(版本)：IE 6 到 IE 11 所有版本
- 解決方案：安裝微軟最新推出的修補軟體
- 資料來源：

1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1429
2. https://www.resecurity.com/article/resecurity-discovered-0-day-rce-vulnerability-in-internet-explorer

3.6.2 WhatsApp MP4 影音檔處理漏洞，遭駭客用以遠端執行任意程式碼

Facebook 表示在 WhatsApp 中發現相當嚴重的資安漏洞，駭侵者可藉由傳送 MP4 影音檔案，入侵受害者的手機，並執行任意程式碼。

Facebook 雖然沒有透露太多技術細節，但指出漏洞存在於 WhatsApp 處理 MP4 影音檔時發生的堆疊暫存溢位錯誤。駭侵者可用以遠端執行任意程式碼，或發動 DDoS 攻擊。

Facebook 指出，使用舊版 WhatsApp 的用戶，應即刻更新至最新版本，以修補漏洞。

- CVE 編號：CVE-2019-11931
- 影響產品(版本)：WhatsApp Android 2.19.274 之前、iOS 2.19.100 之前、WhatsApp Business Android 2.19.104 之前、iOS 219.100 之前；企業客戶端 2.25.3 之前、WhatsApp for Windows Phone 2.18.368 之前版本。
- 解決方案：更新至最新版本
- 資料來源：

1. https://www.facebook.com/security/advisories/cve-2019-11931
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11931
3. https://www.zdnet.com/article/attackers-using-whatsapp-vulnerability-triggered-by-video-files-can-remotely-execute-code/

3.6.3 卡巴斯基確認 Google Chrome 瀏覽器的嚴重 0-day 漏洞，已遭駭侵者大規模運用

卡巴斯基確認 GOOGLE CHROME 瀏覽器的嚴重 0-DAY 漏洞，已遭駭侵者大規模運用

TWCERT/CC

卡巴斯基發表最新警訊，指出一個存在於 Google Chrome 瀏覽器的 0-day 漏洞，已遭駭侵組織大規模使用。

卡巴斯基說，這個漏洞被用來進行典型的水坑式攻擊。駭侵組織駭入韓國某新聞網站，在該網站中植入一段惡意 JavaScript 程式碼，用戶若使用 Google Chrome 瀏覽該站首頁，就會引發一連串後續的惡意軟體攻擊，導致用戶電腦被用來執行任意程式碼。

卡巴斯基已在第一時間通報 Google，Google 也已釋出安全修補程式，建議所有 Chrome 用戶都能儘快安裝修補程式，避免受害範圍進一步擴大。

卡巴斯基的報告詳述了該惡意攻擊的流程；其惡意程式碼與先前的 Lazarus 攻擊有部分相似之處；而受害者也和早先一起稱為 DarkHotel 的攻擊行動接近。

- CVE 編號：CVE-2019-13720
- 影響產品(版本)：Google Chrome 78.0.3904.87 for Windows, Mac, Linux 之前版本
- 解決方案：安裝 Google 釋出之安全修補程式，或更新至 Chrome 版本 78.0.3904.87
- 資料來源：
  1. https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/
  2. https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

3.6.4 微軟 Outlook for Android 遭發現 XSS 資安漏洞

資安廠商 Cybersecurity Help 發現，微軟 Outlook for Android 存有資安漏洞，駭侵者可透過傳送 Email，以網頁 XSS 攻擊用戶手機，並進一步發動各種攻擊，例如竊取用戶手機中的資訊、下載任意程式碼、寄送釣魚郵件等。。

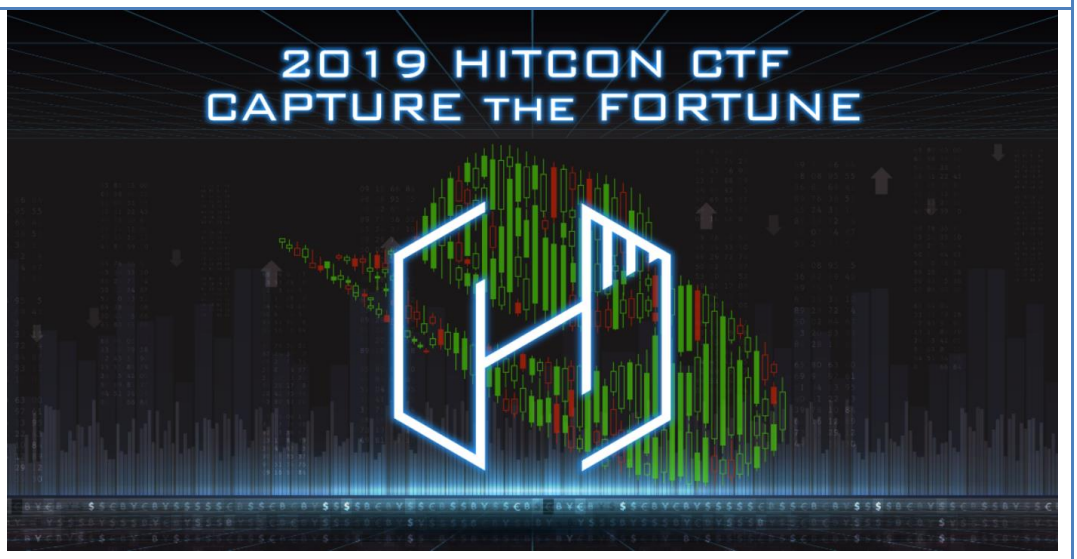
這個資安漏洞的嚴重程度達到「重要級」的 5.6 分，10 分為最嚴重的等級。

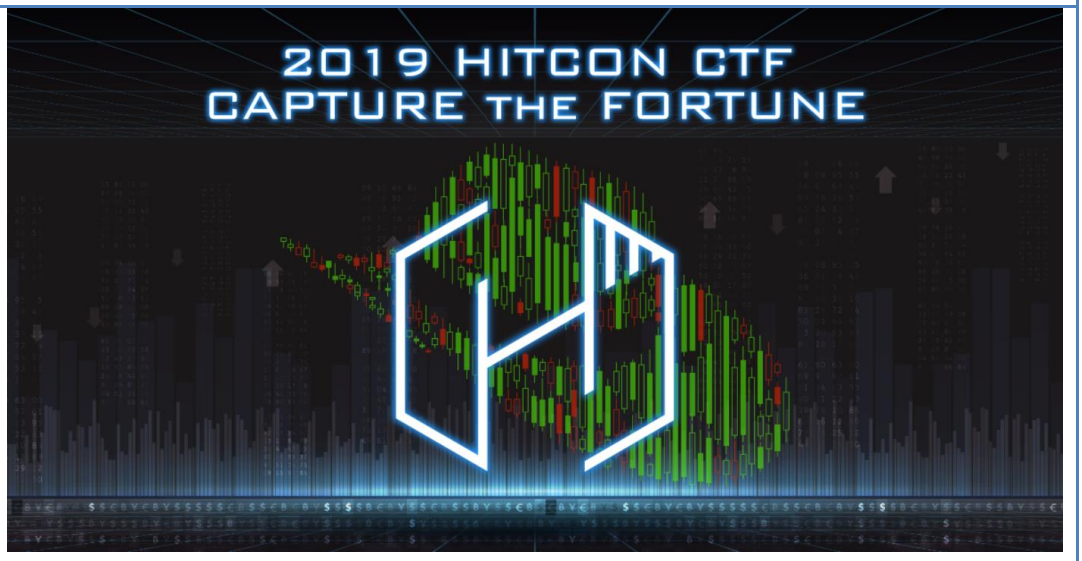
微軟表示這個錯誤存在於 Outlook for Android 分析處理網頁時的錯誤，攻擊者可以用登入使用者的權限進行各種操作；微軟建議該 App 的用戶立即更新至最新版本，同時開啟自動更新功能。

- CVE 編號：CVE-2019-1460
- 影響產品(版本)：Outlook for Android
- 解決方案：更新至最新版本
- 資料來源：

1. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1460#ID0EA
2. https://www.tenforums.com/windows-10-news/144873-cve-2019-1460-outlook-android-spoofing-vulnerability.html#post1774661
3. https://threatpost.com/microsoft-outlook-android-bug-xss/150528/

第 4 章、 資安研討會及活動

2019 HITCON CTF Forum	
活動時間	2019/12/14 (六) 10:00-17:00
活動地點	台北文創 6 樓 BC 廳 (台北市信義區菸廠路 88 號 6 樓)
活動網站	http://surl.twcert.org.tw/4kgkL
活動概要	 美國 DEF CON CTF vs 日本 CODE BLUE vs 日本 TrendMicro CTF 臺灣 AIS3 、 Balsn CTF 、神盾盃網路奪旗賽 經驗分享與交流 全球駭客及國內資安圈最引頸期盼的競賽 2019 HITCON CTF 將於 12 / 14 - 15 於台北文創舉行，今年度包含：美國、俄羅斯、日本、匈牙利、波蘭、越南、台灣、中國 8 個國家共 14 個隊伍參與決賽，並角逐前往美國 2020 DEF CON CTF 決賽資格門票。 今年特別邀請美國 DEF CON CTF 主辦人及日本 CODE BLUE 主辦人、TrendMicro CTF 負責人來台與國內 CTF 與資安團隊進行經驗分享與交流，歡迎來解密。

2019 HITCON CTF Final	
活動時間	2019/12/14（六）09:00-18:00 & 2019/12/15（日）09:30-19:00
活動地點	臺北文創 14 樓 (台北市信義區菸廠路 88 號 14 樓)
活動網站	http://surl.twcert.org.tw/4kgkL
活動概要	 HITCON CTF 已連續第 5 年成為美國 DEF CON CTF 種子賽國家，也是亞洲與臺灣重要指標性資安競賽，全球最頂尖駭客將齊聚一堂。 2019 HITCON CTF (Capture The Fortune) 將帶你進入國際證券交易所.... 每個隊伍就代表一支股票，分數的漲跌如同股價，除了牽動排名，也對應可獲得的獎金。 來自美國、俄羅斯、日本、匈牙利、波蘭、越南、台灣、中國、歐盟等共 14 個隊伍參與決賽，將角逐前往美國拉斯維加斯 2020 DEF CON CTF 決賽資格門票。 每年 HITCON CTF 在視覺和感官上都有不同的震撼，今年 First Blood 有什麼驚喜? 哪個隊伍可以前進美國拉斯維加斯？歡迎報名導覽親身體驗。

台灣駭客年會 HITCON Winter Training 2019	
活動時間	2019/12/16 09:30 - 12:30, 14:00 - 17:00
活動地點	台北市境內，如已達開課人數標準，主辦單位將儘快公布地點。
活動網站	http://surl.twcert.org.tw/PMsw2
活動概要	 **左移！自動化資安測試** 票價：NTD 17,000 課程介紹：課程著重在 DevSecOps 其中的資安測試部分：CI/CD 導入資安測試的方法和實作，包含靜態安全測試（SAST）、動態安全測試（DAST）、軟體組建分析（SCA）等測試方法。 從介紹 DevSecOps 的概念、引入自動化開源工具、部署時的環境安全分析，到掃描結果的弱點管理，帶大家實際感受將資安測試「左移」的體驗。 **當工業控制系統（ICS/SCADA）遇上駭客** 票價：NTD 17,000 課程介紹：當工業控制系統遇上駭客，究竟會蹦出什麼樣的火花，駭客到底是如何對工業控制系統造成無法挽回的傷害呢？ 本課程將深入淺出地說明工業控制系統的概念，以及該如何對工業控制系統造成傷害。

	Web Exploitation and Evasion Techniques 票價：NTD 17,000 課程介紹：This course will focus on advanced vulnerability identification, exploitation, and evasion techniques which are actually used and exploited in the real world. We'll try out the evasions, explain and dive into the rationale step by step. Several hands-on practices demonstrating different possible scenarios will be given while we go through the course. Hence, attendees will gain experience when trying their best to carry out the attack they just learned. Tough environments will be presented so as to push every audience to the limit of one's ability to figure out the possible ways out from the challenges.

台灣駭客年會 HITCON Winter Training 2019	
活動時間	2019/12/16 & 2019/12/17 09:30 - 12:30, 14:00 - 17:00
活動地點	台北市境內，如已達開課人數標準，主辦單位將儘快公布地點。
活動網站	http://surl.twcert.org.tw/PMsw2
活動概要	 **區塊鏈與智能合約攻防** 票價：NTD 33,000 課程介紹：本課程除了將介紹區塊鏈概念的基礎知識外，將藉由實作包含真實事件， DApp 與 CTF 類型題目，以及了解近期智能合約攻擊向量來強化投入區塊鏈相關應用的開發者之資安意識，了解駭客的攻擊思維與方式，就能對自己的區塊鏈開發產品有更好的保護。

	揣摩軟體安全 - 學習系統攻防 票價：NTD 33,000 課程介紹：本課程非常適合有程式基礎，且有心想要學習資安入門，卻又苦於不知該從何著手的學員，課程內容濃縮自講者自身的資安學習經驗，透過詼諧有趣的軟體修改實戰過程，從零開始一步步的學習系統底層知識與駭客記憶體攻擊手法，期望能培養出讓學員有獨立逆向分析 & 撰寫底層攻防程式的能力。

台灣駭客年會 HITCON Winter Training 2019	
活動時間	2019/12/17 & 2019/12/18 09:30 - 12:30, 14:00 - 17:00
活動地點	台北市境內，如已達開課人數標準，主辦單位將儘快公布地點。
活動網站	http://surl.twcert.org.tw/PMsw2
活動概要	 **物聯網安全實務剖析** 票價：NTD 33,000 課程介紹：萬物聯網的時代，物聯網的應用已成為人們生活中密不可分的一部分，相對其資安威脅也日益增長。本課程將由淺入深逐步說明物聯網概念、架構及相關攻擊面向與攻擊手法，讓學員可一窺物聯網安全的世界。

	本課程有相當多的實作時間，適合想要被手把手教學的學員們報名。 **Practical Web Hacking and Exploitation** 票價：NTD 33,000 課程介紹：This course will focus on advanced vulnerability identification and exploitation techniques and allow attendees to get familiar with some tricky but decent ways that were actually used and exploited in the real world. Several hands-on practices demonstrating different possible scenarios will be given while we go through the course. Hence, attendees will gain experience when trying their best to carry out the attack they just learned. There will be some new techniques shown during the course exclusively, which can give attendees insight into the problems of vulnerability. **Windows APT Warfare** 票價：NTD 33,000 課程介紹：本課程將盤點近年實用網軍釣魚技術 與 完整 Windows 編譯器技術：包含 PE 結構完整操作攻擊/繞過手段解析、Windows Shellcode 開發、程式感染技術 與防毒繞過技巧、UAC 提權細節分析與作業系統服務逆向工程，將在課程中打下扎實的 Windows 系統知識與結構體基礎、帶學員動手做出一些有趣的研究並理解其中駭客攻擊的原理。

台灣駭客年會 HITCON Winter Training 2019	
活動時間	2019/12/18 09:30 - 12:30, 14:00 - 17:00
活動地點	台北市境內，如已達開課人數標準，主辦單位將儘快公布地點。
活動網站	http://surl.twcert.org.tw/PMsw2
活動概要	 **Windows Filter Driver - 核心層攔截情資工具開發與實務應用** 票價：NTD 11,000 課程介紹：對資安人員所使用在 Windows 系統上開發防禦腳本執行及其他病毒載入的工具── Windows Filter Driver 做基本概述。 介紹在 Windows 系統核心層級獲取 I/O 指令與內容並修改或紀錄的方法，以及相關開發除錯。

思科線上風雲會「擁抱 5G 打造資安無限大未來 」	
活動時間	2019/12/19(四) 下午 14:40-16:10 (下午 14:30 開放登入)
活動地點	線上活動
活動網站	http://surl.twcert.org.tw/5zcgi
活動概要	 4G 改變生活、5G 改變社會。迎向 5G 新時代，未來 5G 網路將覆蓋手機、智慧家居、自駕汽車、遠程醫療服務、智慧城市服務體系等領域，而隨著物聯網(IoT)、車聯網(V2X) 、遠距醫療等 5G 應用科技的實現，全球資安將面臨更強大的挑戰。 誠摯邀請參與 12 月 19 日「擁抱 5G 打造資安無限大未來」，此次思科線上風雲會，特別邀請新加坡思科亞太區通路事業群總監與台灣首席資安顧問，進行線上對談，除了解析 5G 資安三大挑戰，也將分享企業如何結合 AI 建立滴水不漏的資安防禦機制，攜手打造資安無限大未來。 講師：Ben Ng 思科亞太區通路事業群總監 & Allen Yu 游証硯 思科台灣首席資安顧問 活動聯絡人：思專員 02-2721-1070

第 5 章、 2019 年 11 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。

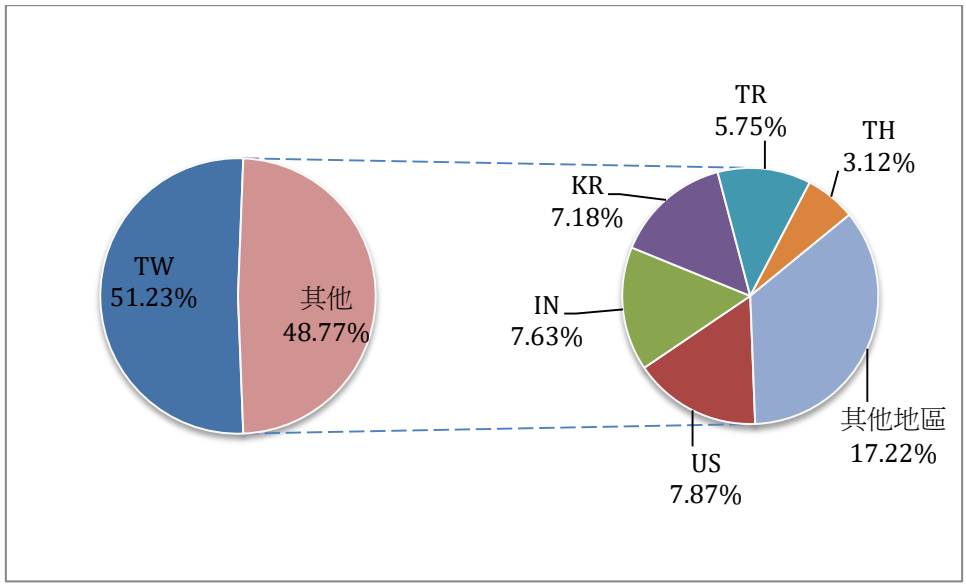


圖 1、通報地區統計圖

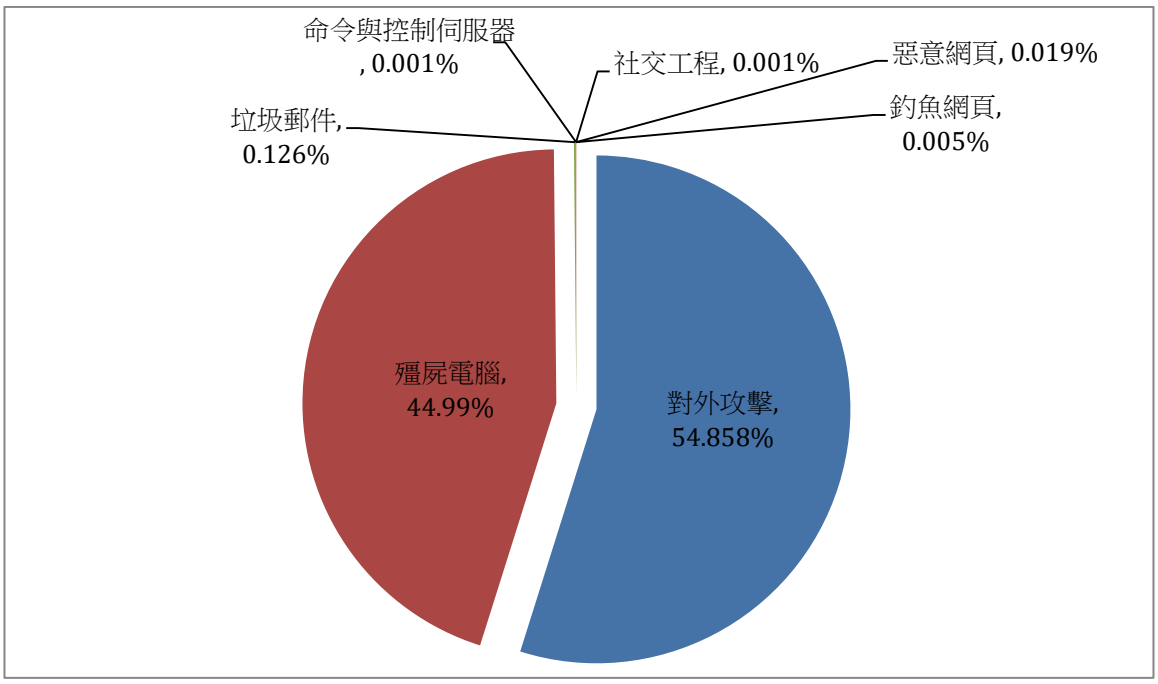

命令與控制伺服器
, 0.001%
社交工程, 0.001%
惡意網頁, 0.019%
垃圾郵件,
0.126%
釣魚網頁,
0.005%
殭屍電腦,
44.99%
對外攻擊,
54.858%

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 12 月 12 日

編輯：林克容、江奕昉、洪彩馨

服務電話：0800-885-066

電子郵件：twcert@cert.org.tw

官網：https://twcert.org.tw/

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

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

Twitter：@TWCERTCC