一網打盡：解析錯綜複雜的新舊威脅

2018 年資安總評

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

作者：
Trend Micro Research

圖片授權：Shutterstock.com

獻給 Raimund Genes (1963-2017 年)

內容

2018 年資安威脅情勢強烈反映出企業每天必須經歷的各種困難抉擇。該年最重大的一些資安事件包括：當今絕大多數電腦與運算裝置底層硬體架構所出現的 Meltdown 和 Spectre 漏洞 (即使過了一年，這些漏洞依然未獲得徹底解決)、挾帶著巨額罰鍰的歐盟通用資料保護法 GDPR 正式上路、網路釣魚之類的社交工程攻擊再度成為網路犯罪主流。對資安界來說，2018 年是一個遊戲規則改變與新舊交替的一年，充斥著各種虛擬加密貨幣挖礦惡意程式、勒索病毒以及針對已知漏洞的攻擊。

然而對於受害的企業來說，最具破壞性的莫過於資料外洩和針對性攻擊。資料外洩事件不斷登上媒體版面，而針對性攻擊則一整年都相當活躍。企業工業控制系統 (ICS)、連網裝置，以及雲端裝置與網路不斷遭到攻擊，證明資安界對連網裝置安全的呼籲似乎未獲得應有的重視，例如：歹徒駭入了大量路由器並利用這些路由器發動攻擊，此外，工業控制系統的人機介面、甚至是雲端架構軟體也出現了大量漏洞。

儘管這麼多的資安問題已經讓企業焦頭爛額，但就連最典型的傳統威脅也尚未消失。當前作業系統百家爭鳴的態勢，讓網路犯罪集團開始重新回歸到他們原本最愛的社交工程技巧，藉由「人性的弱點」來遂行其目的。這和他們先前大量運用漏洞攻擊套件與其他自動化工具的作法大相逕庭，因為這些工具必須有很多使用者都使用含有漏洞的軟體才能派上用場。

儘管時間一再證明網路犯罪集團會不斷因應資安廠商與企業所建置的最新防護而調整攻擊方式：不論是變換攻擊手法，或是調整整體攻擊行動。但直到最近，我們才明顯看到網路釣魚手法又再度成為網路犯罪主流；這樣的攻擊手法已經存在很久，也相當普遍，不過並沒有受到太多的關注。

在了解上述的情勢之後，企業應重新評估一下自己當前的資安策略，並且考慮一下是否該採取新的策略。有鑑於此，這份趨勢科技 2018 年資安總評報告將為企業點出一些企業應認真思考的重大資安問題，協助企業正確評估當前的情勢並提升自己的防護。

訊息威脅變多且形態多樣化

電子郵件是企業機構對內和對外溝通的重要工具。也因此，電子郵件已成為網路犯罪集團及駭客用來散布惡意程式或其他威脅一個非常方便的平台。儘管電子郵件威脅已經存在數十年之久，但根據 Black Hat 駭客大會 2018 年所做的一項調查，最令全球資安人員擔心的電子郵件威脅是網路釣魚攻擊：也就是利用社交工程電子郵件來詐騙身分資料[1、2、3]。這類詐騙郵件一旦躲過企業閘道防護的偵測而進入到企業內部，只要其外觀和內容都很像企業機構平常會收到的電子郵件，就很可能讓收件人受騙上當。這類郵件不論是企業標誌、內容用詞、甚至格式，都很可能模仿得幾可亂真，讓收件人很難分辨。

網路犯罪集團擴大網路釣魚範圍

當受害者點選網路釣魚郵件當中的連結，便會連上一個網路釣魚網站，這是駭客整體攻擊行動的第一步。這些網站會竭盡所能模仿正牌的網站，讓使用者不疑有詐而輸入歹徒所要求的資訊。

如同我們的 2019 年資安預測報告所提到，網路釣魚整體活動在 2018 年前三季突然大量暴增[4]。這股熱潮一直延燒至年底，我們總共攔截了 2.69 億次網路釣魚網址存取，較 2017 年成長 269%。此外，相較於前一年，我們已攔截的非重複用戶端 IP 存取網路釣魚網址的次數也增加了 82%，而這些都是原本可能受害的使用者。

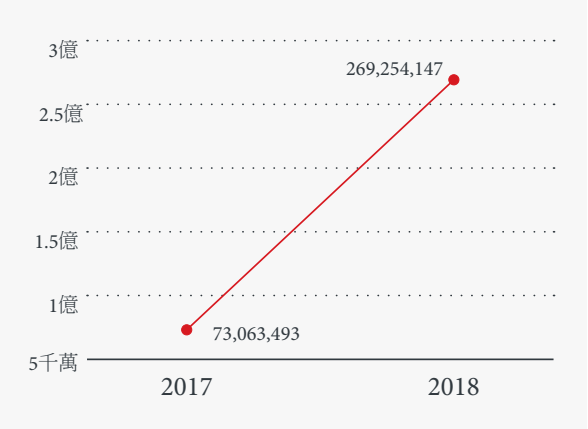

圖 1：已攔截的網路釣魚網址存取次數逐年比較 (同一個被攔截的網址若被存取三次仍算三次)：2018 年較前一年成長 269%。

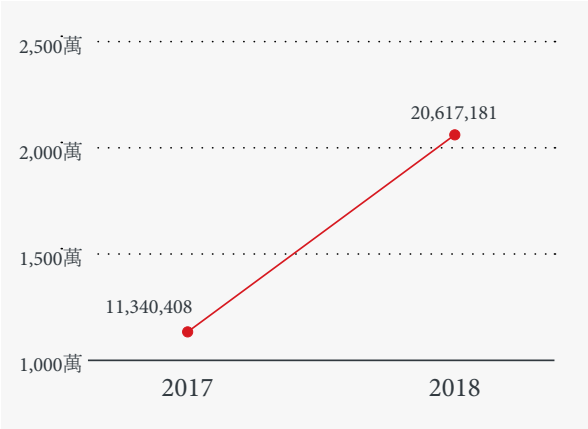

圖 2：已攔截的非重複用戶端 IP 存取網路釣魚網址次數逐年比較 (同一台電腦若存取某個連結三次則只算一次)：2018 年較前一年成長 82%。

由於網路釣魚攻擊通常需經由電子郵件來發動，所以網路犯罪集團會加強火力，發送更多的網路釣魚郵件。網路釣魚至今已存在數十年，除了電子郵件之外，甚至還衍生出網路聊天、簡訊、電話語音等不同形態的網路釣魚。網路釣魚重新成為歹徒的攻擊重心，顯示網路犯罪集團正在因應今日運算環境的重大變遷而重新調整方向。

五年前的運算環境大致上還算單一，將近 80% 的作業系統都是 Microsoft Windows，唯一的差別大概只有版本上的不同[5]。攻擊漏洞基本上能盡可能減少人的操作，不像網路釣魚攻擊需要使用者來點選連結。當漏洞攻擊可適用絕大多數的平台和瀏覽器時，網路犯罪集團將火力集中於攻擊軟體的漏洞也就相當合理。

但今日的環境已大不相同，不僅連網的裝置類型變得多樣化，一些五年前根本尚未出現或不太流行的作業系統，現在也都占有了一席之地，而且，沒有單一平台能夠囊括半數以上的電腦使用者。因此，對網路犯罪集團而言，漏洞攻擊套件的犯案效率已開始走下坡。現在已經不再有哪一種針對特定軟體版本的攻擊可以涵蓋大多數的使用者。事實上，由於使用者的瀏覽器或軟體必須要符合特定版本，漏洞攻擊套件才能派上用場，因此這類攻擊在 2018 年減少了 63%。

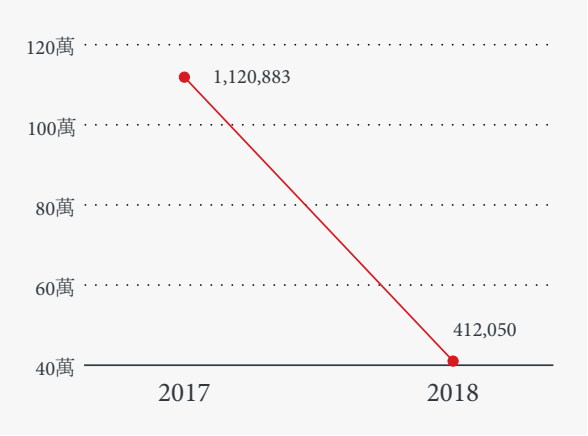

圖 3：存取漏洞攻擊套件的案例逐年比較：2018 年呈現下滑的趨勢。

網路犯罪集團為了因應這樣的現況而大費周章地不斷變換攻擊手法，倒不如調整策略，重新回歸到人類亙古不變的「人性弱點」。所以他們開始將更多心力投注在社交工程詐騙。2018 年美國有多起資料外洩事件都是因為網路釣魚攻擊而引起：某所學校員工點選了一個自稱來自區域性單位的電子郵件[6]、某個郡政府機關員工被騙點選了有關加薪的電子郵件[7]、某醫療機構人員因為收到一封自稱來自內部高層主管的電子郵件而提供了自己的登入憑證[8]。只要有一名員工遭到網路釣魚詐騙，就可能帶來嚴重的後果。

此外，2018 年也出現了一些值得關注的網路釣魚攻擊手法，包括：一個使用 AES 加密網站來誘騙 Apple ID 的攻擊[9]、一個使用國際化域名編碼 (punycode) 攻擊技巧的簡訊釣魚攻擊[10]，以及利用一個預先駭入的電子郵件帳號來回覆某電子郵件討論串的攻擊[11]。

這波逆向的發展，隨著電子郵件逐漸成為使用者網路身分的基石而變得更加危險，因為一些線上服務現在都要求使用者必須提供一個電子郵件地址來接收一些重要的帳戶相關通知與最新消息。在企業方面，辦公室軟體服務 (SaaS) 的日漸普及，使得帳號登入憑證在網路犯罪集團心中的重要性越來越高，而這些平台也因而成為網路釣魚攻擊的目標。事實上，在我們攔截的非重複網路釣魚網址當中，假冒 Microsoft Office 365 和 Outlook 服務的網址數量成長了 319%。

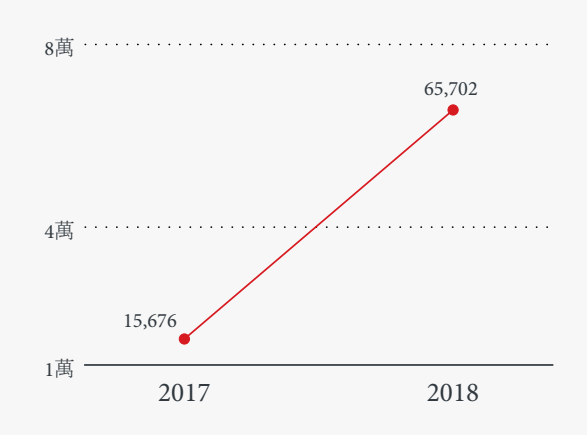

圖 4：已攔截的 Office 365 與 Outlook 非重複網路釣魚網址逐年比較：假冒 Office 365 和 Outlook 服務的網址數量較去年增加三倍以上。

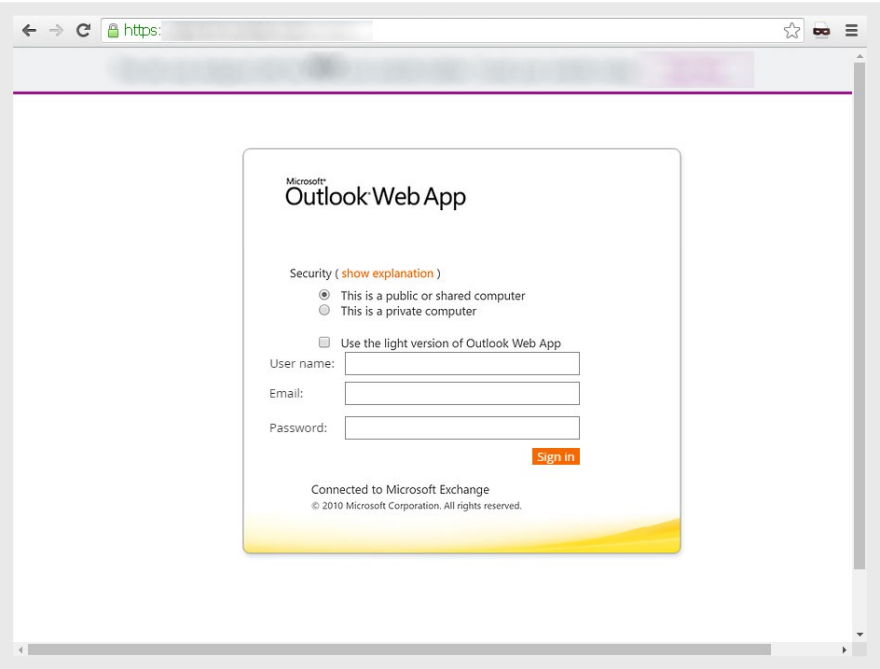

圖 5：網路犯罪集團試圖利用網路釣魚騙取辦公室軟體服務 (SaaS) 使用者的登入資訊，圖中顯示某個假冒成 Outlook Web App 登入頁面的網路釣魚網站。

網路犯罪集團利用變臉詐騙深入企業

變臉詐騙 (BEC) 是另一種形態的電子郵件威脅，執行長 (CEO) 詐騙即是一例。在典型的變臉詐騙當中，歹徒會主動聯繫公司內部具有核准出納或授權匯款權限的人員，或攔截與該人員的內部通訊。在大多數情況下，歹徒會假冒公司的執行長或具有類似權限的高階主管。

變臉詐騙在 2018 年一整年都不斷成長，且較 2017 年增加 28%，完全沒有消退的跡象。儘管這類電子郵件攻擊的整體數量不多，但其危險之處在於每一次的攻擊都有相當高的成功率。有別於網路釣魚攻擊大多針對廣大的潛在受害族群，變臉詐騙需要事先針對特定目標做足功課才能提高使用者受騙上當的機率。

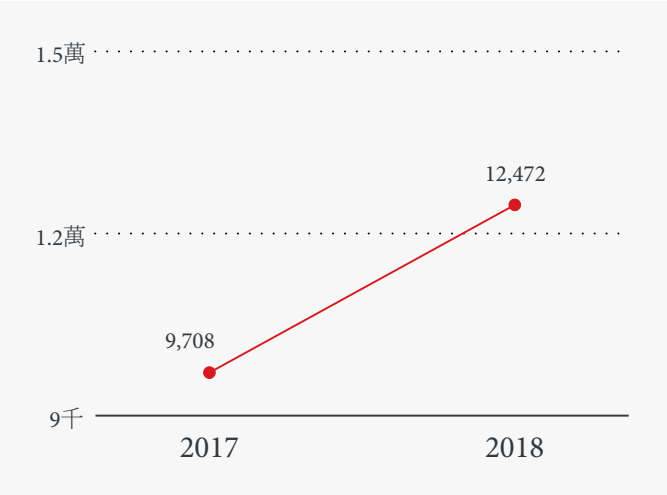

圖 6：變臉詐騙嘗試攻擊數量逐年比較：2018 年較去年增加。

註：這項資料代表偵測到的變臉詐騙所有嘗試攻擊案例，不論攻擊成功與否。

變臉詐騙包括了執行長 (CEO) 詐騙。

根據我們 2018 年的變臉詐騙嘗試攻擊樣本監控數據顯示，企業內有幾個職務是歹徒最常假冒的對象，第一名就是執行長。這一點其實不令人意外，因為執行長在大多數企業內都擁有最高的權限。

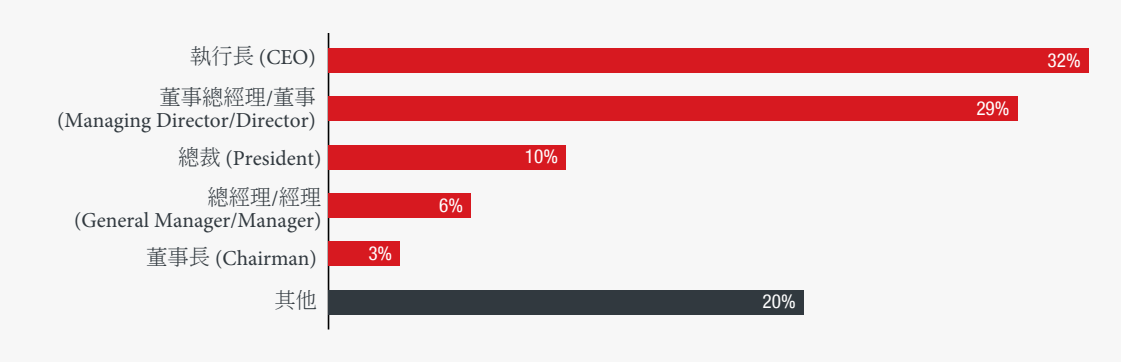

圖 7：歹徒經常假冒的公司職務：執行長是最常被假冒的職務。

註：這項資料代表偵測到的變臉詐騙所有嘗試攻擊案例，不論攻擊成功與否。

變臉詐騙包括了執行長 (CEO) 詐騙。

我們在澳洲、美國及英國的企業客戶偵測到許多變臉詐騙嘗試案例。雖然這或許跟我們的客戶分布有關，但這些國家其實也是全球商業中心，許多跨國企業的總部皆設在這些國家。因此，變臉詐騙攻擊大多集中在這些國家也就相當合理。

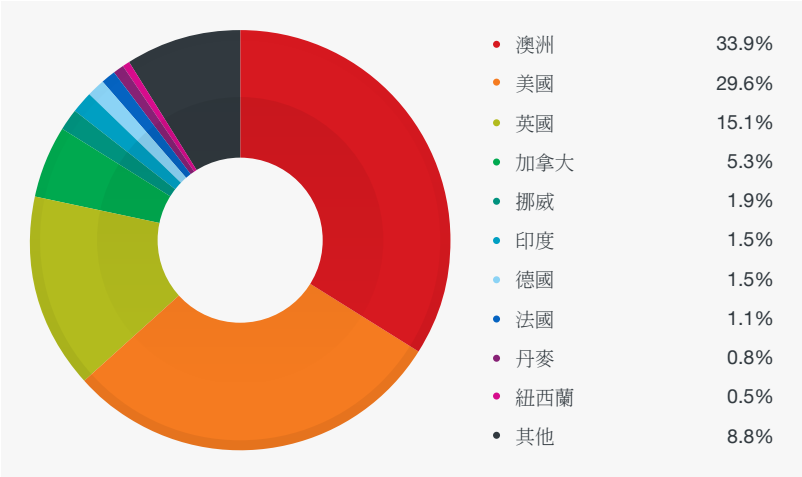

圖 8：變臉詐騙分布國家：在一些被視為全球商業中心的國家，其變臉詐騙嘗試攻擊案例也較多。

註：這項資料代表偵測到的變臉詐騙所有嘗試攻擊案例，不論攻擊成功與否。

變臉詐騙包括了執行長 (CEO) 詐騙。

在接近年底之前，美國聯邦調查局 (FBI) 發布了一項公告警告企業小心一種新的變臉詐騙手法。在這項稱為「禮物卡詐騙」的手法當中，歹徒會假冒主管來命令企業內某位員工幫執行長購買一些禮物卡或禮物，以便發給員工。由於當時正逢年節，再加上是要送禮給員工，因此這項詐騙手法從社交工程的角度來看算是相當具說服力。因此，光在美國亞利桑那州，這項禮物卡詐騙所造成的總損失就將近 9 萬美元[12]。

勒索病毒攻擊數量減少但依舊危險

勒索病毒整體偵測數量下滑，但 WannaCry 依然強勢

雖然新聞上不時會出現有關勒索病毒事件的報導，但我們發現勒索病毒相關威脅的偵測數量卻大幅減少 91%。其原因可能有以下幾點：防範勒索病毒的解決方案已有長足進步、有關這類攻擊的防範意識大幅提升，以及，在某種程度上，大眾已意識到就算乖乖支付贖金也可能徒勞無功。

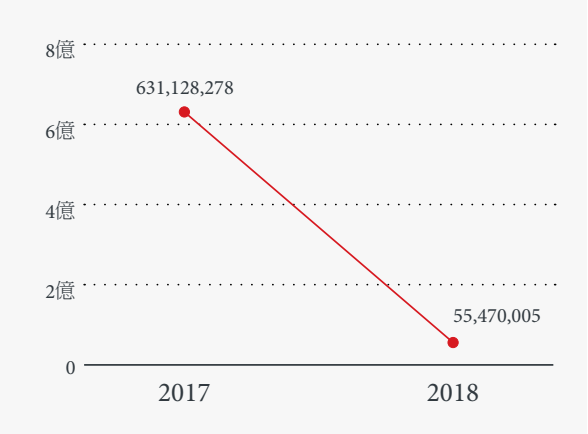

圖 9：勒索病毒相關威脅 (檔案、電子郵件、網址) 逐年比較：2018 年較去年減少。

此外，新的勒索病毒家族數量也相對減少。

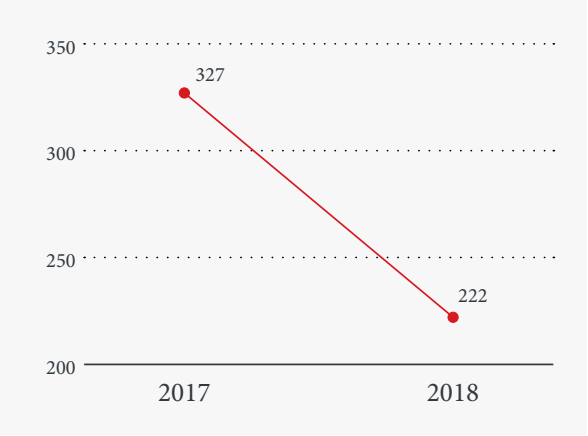

圖 10：新的勒索病毒家族數量逐年比較：2018 年較去年減少。

不過，相對於所花費的力氣，勒索病毒攻擊的報酬仍相當誘人，因此我們仍持續看到一些值得關注 (儘管不是最新) 的勒索病毒攻擊手法。在所有勒索病毒家族當中，2017 年 4 月首度現身並於 2017 年 5 月造成全球大感染[13] 的 WannaCry , 依然是 2018 年的榜首，其偵測數量高達 616,399 個。儘管已經過了一年，這數量仍大幅超越所有其他勒索病毒家族的總和。

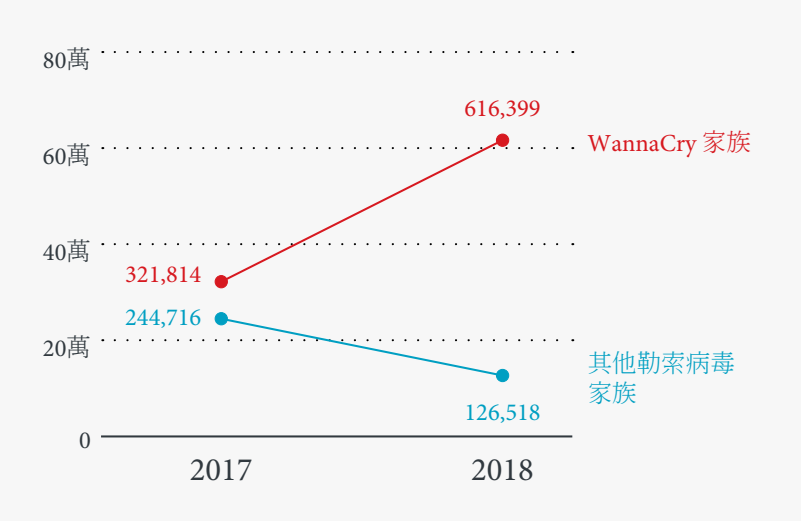

圖 11：WannaCry 數量逐年比較：WannaCry 連續兩年皆占所有勒索病毒偵測數量一半以上。

WannaCry 是經由 Microsoft Windows Server Message Block (SMB) 通訊協定的一個漏洞，並利用 EternalBlue 漏洞攻擊套件來進入含有漏洞的電腦 (此攻擊套件是由 Shadow Brokers 駭客集團散布到網路上[14])，接著，該病毒就利用其蠕蟲能力在網路上四處擴散。從 WannaCry 的偵測數量就可看出，儘管相關的漏洞早在一年多前廠商就已經修補，但全球仍有許多電腦使用者並未更新電腦，這才使得該病毒能趁虛而入。

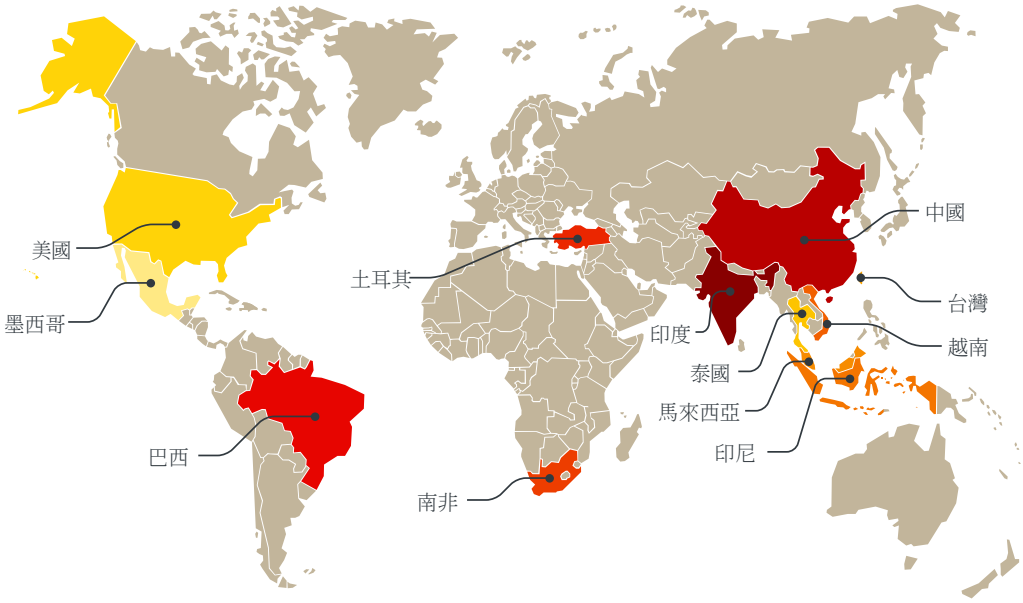

圖 12：2018 年 WannaCry 偵測數量超過 1 萬的國家：全球各地仍持續偵測到不少 WannaCry 病毒。

同時，正如 WannaCry 勒索病毒 2017 年剛現身的時候一樣[15]，偵測到 WannaCry 病毒的電腦絕大多數都還在使用 Windows 7 作業系統。這大致上符合一項事實，那就是已升級至 SMB 3.0 通訊協定的作業系統 (也就是 Windows 8 及以後的作業系統[16]) 已經沒有這項漏洞。該漏洞自 2017 年就已經有修補更新可用，但許多使用者卻至今仍未套用。

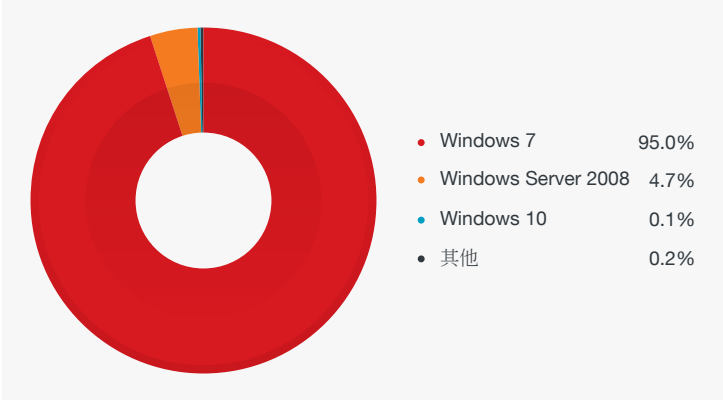

圖 13：2018 年各系統 WannaCry 偵測數量分布：Windows 7 系統上偵測到的 WannaCry 病毒占 90% 以上。

在最新發展方面，我們發現 GandCrab 家族相當活躍。在一整年當中推出了不少新的版本，增加了各種感染途徑，包括：垃圾郵件[17] 與 Fallout 漏洞攻擊套件[18]。除此之外，還會將加密後的檔案冠上不同的副檔名，並且還會散布後門程式、蠕蟲及惡意的虛擬加密貨幣挖礦程式。在針對南韓的垃圾郵件當中，其挾帶的 GandCrab 勒索病毒附件檔案採用的是 EGG 壓縮格式[19]。此外，據稱其作者在 10 月份也和某個加密服務廠商合作以躲避偵測[20]。

其他勒索病毒同樣也持續不斷演變。網路犯罪集團架設了假的軟體分享網站來散播勒索病毒，並利用彈出式廣告來將使用者導向這些網站[21]，這是一項避免使用者不敢下載執行檔或任何大型檔案的有效技巧。在另一個案例中，網路犯罪集團將勒索病毒與正常軟體包裝在一起[22]。還有另一個案例是，勒索病毒會將自己複製一份然後寄給受感染使用者的電子郵件聯絡人[23]。除此之外，我們也發現一些證據顯示勒索病毒也開始演化出反制機器學習的能力，例如：PyLocky 病毒[24]。較特別的是，Princess Evolution 病毒幕後的集團在地下論壇上表示，他們之所以沉寂了一段時間，是為了改善其勒索病毒服務 (RaaS)，提供受害者一種以加盟代替支付贖金的選擇[25]。

虛擬加密貨幣挖礦活動偵測數量超過百萬

虛擬加密貨幣挖礦活動偵測數量在 2018 年突破百萬並寫下歷史新高，較前一年增加 237%。該數字反映了我們早已觀察到的一股「掏金熱」，且一整年都有各種不同的技巧出現：濫用廣告平台[26、27]、彈出視窗[28]、伺服器漏洞攻擊[29、30]、惡意的瀏覽器附加元件[31]、手機[32]、外掛程式[33]、殭屍網路[34、35]、與正常軟體包裝在一起[36]、漏洞攻擊套件[37]，以及將原本的勒索病毒舊瓶裝新酒[38]。

網路犯罪集團對於虛擬加密貨幣的興趣顯然在於攻擊基礎架構[39]。此外，這也反映在網路犯罪地下論壇上所出現的貼文，其張貼的廣告通常都與兩種針對虛擬加密貨幣的攻擊工具和服務有關。其中，虛擬加密貨幣挖礦惡意程式的廣告占絕大多數，其次是虛擬加密貨幣竊取程式，也就是以虛擬錢包和攔截交易為目標。儘管所有證據顯示智慧型手機、路由器及其他物聯網 (IoT) 裝置都不具備太大的運算效能 (不像一般的電腦)，但地下論壇上仍不斷有利用這些裝置挖礦的相關軟體廣告[40]，歹徒或許是希望藉著數量的優勢來彌補運算效能的不足。

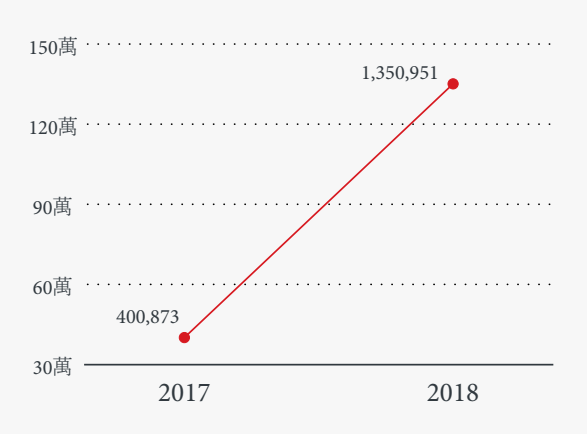

圖 14：虛擬加密貨幣挖礦活動偵測數量逐年比較：2018 年較去年成長。

無檔案式威脅在第四季增加

2018 年另一項重要的發展就是無檔案式威脅的突然崛起，這是網路犯罪集團逐漸用來躲避偵測的另一種方法。無檔案式威脅的名稱由來，正是它們不會使用獨立的二進位檔案或執行檔，而是將自己注入到現有的應用程式記憶體中，或者在正常應用程式 (如 Windows Machine Instrumentation 或 PowerShell) 當中執行腳本。為了避免使用者電腦重新開機之後惡意程式碼會不見 (因為是存在記憶體中)，歹徒也修改了一些系統登錄機碼來常駐系統內。儘管如此，我們還是可以利用一些非檔案式特徵來偵測這類無檔案惡意程式，例如特定的執行活動或行為。

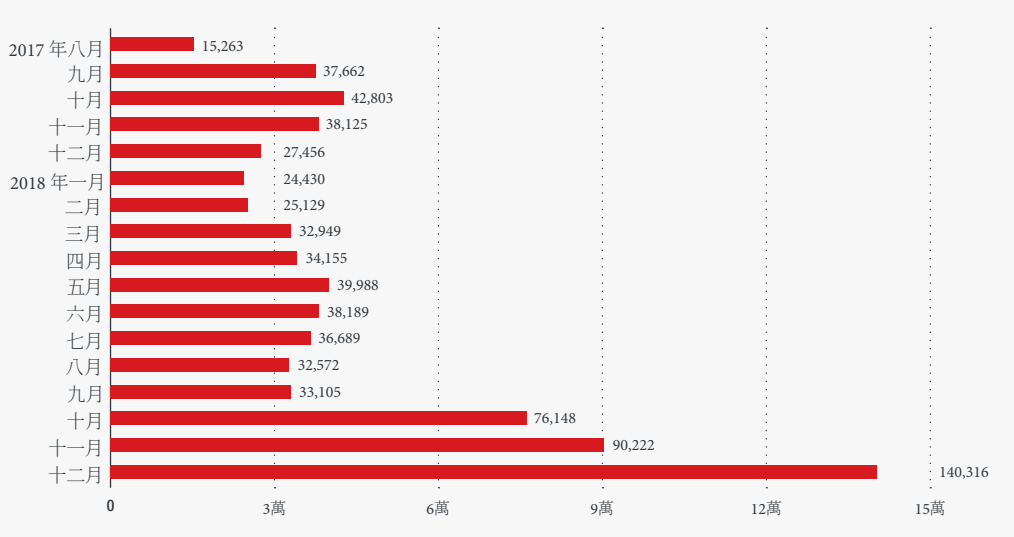

圖 15：無檔案式威脅每月攔截數量：無檔案惡意程式持續出現中。

這類威脅的活動痕跡仍可透過流量和行為監控或沙盒模擬分析來加以偵測[41]，而傳統僅仰賴惡意檔案偵測的解決方案，則無法偵測這類新興威脅。無檔案式威脅的用途非常廣泛，完全視網路犯罪集團的想像力而定。這幾年，我們曾看過這類威脅用來散布虛擬加密貨幣挖礦程式[42]、勒索病毒[43] 以及後門程式[44]。

TinyPOS 原始碼外流導致 POS 惡意程式暴增

2018 上半年，我們觀察到一大波的銷售櫃台系統 (POS) 惡意程式，主要是因為 TinyPOS 惡意程式的數量暴增。TinyPOS 惡意程式家族涵蓋了某個老舊的記憶體擷取程式變種，如 PinkKite 惡意程式，其特色是檔案很小。

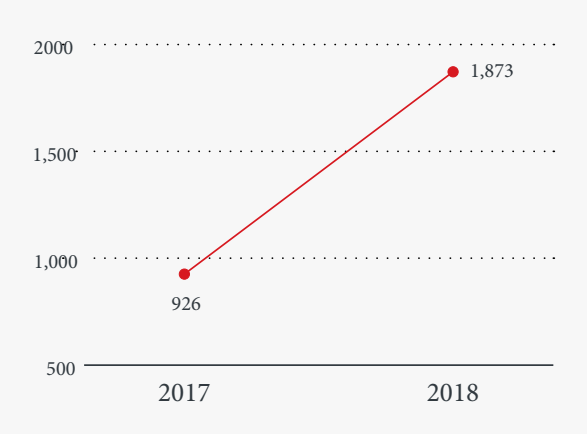

圖 16：POS 惡意程式數量逐年比較：2018 年較去年增加。

POS 惡意程式數量的高峰期出現在 5 月左右，原因是 TreasureHunter POS 的原始程式碼遭到公開[45]。每當有網路犯罪集團將惡意程式原始碼公開或外流到地下論壇，其他的犯罪集團就會加以研究、運用、改進，然後發展出更強大的武器。當這些修改過的版本經過部署、測試、調整並開始出現在網路上時，惡意程式的偵測數量就會突然暴增。這樣的情況過去也曾發生過，例如衍生自 Mirai 的 Satori 殭屍網路[46]，以及立意良善的 Hidden Tear 教學程式碼所衍生出來的一些勒索病毒[47]。

設定不當的雲端容器 API 引來虛擬加密貨幣挖礦程式

毫無疑問地，網路犯罪集團已開始將其攻擊範圍拓展至雲端。在不久前的一個案例當中，我們曾經看到 Docker 因為應用程式開發介面 (API) 暴露在外而導致雲端出現虛擬加密貨幣挖礦程式[48]。Docker 是一套開放原始碼容器化軟體，這是一種在作業系統層次而非應用程式層次的虛擬化。

這套軟體也提供了內建防護功能[49] 讓使用者保護容器。但一個重要的基本安全原則就是，由於 API 可提供雲端資產的遠端遙控功能，所以不應該開放給外部存取。然而卻因為一個小小的安全組態設定錯誤，而導致了這樁雲端管理災難。

硬體與雲端發現重大漏洞，工業控制系統 (ICS) 的漏洞亦持續增加

有多項資安相關的發現對於所有電腦使用者以及雲端採用者來說，是一記響亮的警鐘，甚至包括使用工業控制系統 (ICS) 的企業。

Meltdown 和 Spectre 的問題似乎仍無消退的跡象

2018 年一開春，電腦產業便出現了兩個超級重大的處理器漏洞：Meltdown 和 Spectre，兩者都是當代 CPU 指令預測執行設計上的漏洞。許多廠商為此特別在 1 月份緊急釋出修補更新來解決這些問題，但反而造成許多客戶電腦出現藍色當機畫面，整台電腦變得無法使用[50]。接下來的幾個月，又陸續發現更多 Meltdown 和 Spectre 漏洞的變化形態[51]。

由於 Meltdown 和 Spectre 是處理器上的漏洞，牽涉到處理器的架構設計問題，因此很難斷定影響範圍到底有多廣。這也正是為何 Meltdown 和 Spectre 漏洞的相關資安公告都列了一大串可能需要修補的對象，包括：微處理器、裝置、軟體，以及雲端服務，而非單純只侷限於某個軟體版本。

甚至到了年底，我們仍未看到廠商提出一個徹底的方法來解決這些微處理器架構上的問題，完全點出了這項問題的嚴重性[52]。然而不幸的是，這意味著未來幾年之內，在處理器底層架構徹底翻新之前，各種不同裝置在各種不同情況下都可能面臨資料外洩的風險而不自知。

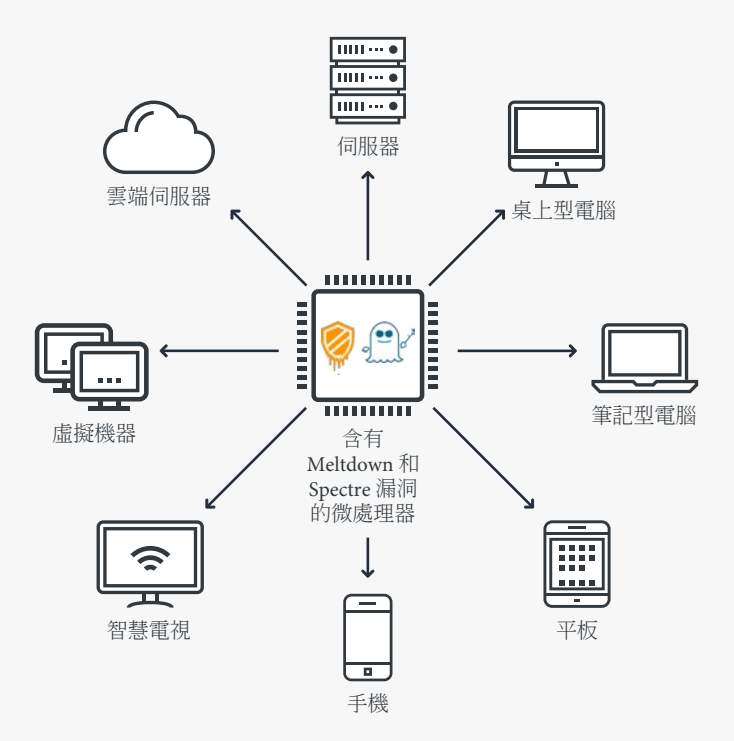

圖 17：受到 Meltdown 和 Spectre 影響的各類裝置：其漏洞影響遍及各種裝置的底層硬體。

重大雲端漏洞造成後台伺服器遭駭客存取

另一個首開先例的不幸事件是，開放原始碼雲端容器協調軟體 Kubernetes 被發現一個重大漏洞[53]。該漏洞可能讓駭客利用一個特製的網路請求，經由 Kubernetes API 伺服器連上後台伺服器[54]。結果，任何發送至後台伺服器的指令都會被照單全收、忠實執行，因為後台伺服器以為這些經由 API 所下達的指令已通過認證。雖然這項漏洞很快就獲得修正 (不像 Meltdown 和 Spectre 到現在還無法解決)，但卻也提醒了企業將資安融入開發營運 (DevOps) 的重要性，也就是所謂「開發資安營運」(DevSecOps)，因為企業未來勢必還會導入更多新的資料處理平台和技術。

針對已知和已修補漏洞的攻擊有越來越多的趨勢

以往，大約每年會出現二至三次重大的零時差漏洞攻擊，但最近卻似乎沒有任何大型的零時差漏洞攻擊出現，甚至沒有可視為零時差漏洞的案例。若有的話，也是僅用於特定的攻擊案例，且規模不大。

漏洞識別碼	零時差漏洞詳細內容
CVE-2018-4878	Flash 的零時差漏洞，僅用於 1 月出現的某些針對性攻擊案例[55]
CVE-2018-8120	Win32k 元件漏洞，5 月發現 (無進一步詳情)[56]
CVE-2018-8174	Double Kill Internet Explorer 零時差漏洞，僅用於 5 月的某些針對性攻擊[57]
CVE-2018-8341	Windows 核心漏洞，8 月發現[58]
CVE-2018-8373	僅用於 8 月的某些使用 Microsoft VBScript 的針對性攻擊[59]
CVE-2018-8414	用於 8 月某些針對 Windows Shell 的攻擊 (Adobe Acrobat 也受影響)[60]
CVE-2018-8453	用於 8 月某些針對 Windows 核心的攻擊[61]
CVE-2018-8589	用於 11 月某些針對 Windows 核心的攻擊[62]

表 1：值得注意的零時差攻擊事件：零時差漏洞攻擊在規模上已不如往年。

除此之外，我們也觀察到多起網路犯罪集團攻擊已修補漏洞的事件。這些針對已知漏洞的攻擊是所謂的「n-day」(多日) 或「1-day」(當日) 漏洞攻擊。

漏洞識別碼	詳細資訊	修補日期	2018 年攻擊出現時間
CVE-2018-7602	Drupal 漏洞，用於散布虛擬加密貨幣挖礦程式[63]	2018年4月25日	修補更新釋出後 5 小時[64]
CVE-2017-12635, CVE-2017-12636	Apache CouchDB 漏洞，用於散布虛擬加密貨幣挖礦程式[65]	2017年11月14日[66]	2018年2月15日[67]
CVE-2017-10271	Oracle WebLogic WLS-WSAT 漏洞，用於虛擬加密貨幣挖礦攻擊	2017年10月16日[68]	2018年2月26日[69]，隨後又出現在 2018 年5月11日[70]
CVE-2015-1805	可讓 Android 手機永久改機 (root) 的漏洞[71]，用於 AndroRat[72]	2016年3月16日[73]	2018年2月13日[74]

表 2：值得注意的 n-day 或 1-day 漏洞攻擊事件：針對已知和已修補漏洞的攻擊，其出現時間從修補更新釋出之後的數小時至數年不等。

犯罪集團這種先研究已公告的漏洞 (即使公告時已修補)，然後再針對漏洞開發攻擊手法的逆向操作，早已行之有年。而且看來網路犯罪集團的策略似乎奏效，因為並非所有企業機構都能適時修補其系統漏洞 (如果有修補的話)。值得注意的是，漏洞通報數量在 2017 年就已經大幅暴增[75]，到了 2018 年卻又再創新高。

至今，一些針對已修補漏洞的攻擊手法，對網路犯罪集團來說仍相當有效，例如：運用 Linux 核心權限提升漏洞 (CVE-2016-5195) 的 Dirty Cow 攻擊手法，以及利用 Windows SMB 漏洞 (CVE-2017-0144) 的 EternalBlue 攻擊手法。以 Dirty Cow 為例，儘管該漏洞在實際攻擊被發現時 (2016 年 10 月)[76] 便立即獲得修補 (但隨後在 2017 年 11 月又出現過一次，因為先前的修補有缺失)，但研究人員發現歹徒在 2018 年 10 月仍利用該漏洞來攻擊某個 Drupal 網站伺服器的後門[77]。

至於 CVE-2017-0144 則是在 2017 年 3 月就已經揭露[78]，並獲得修補[79]。但 EternalBlue 攻擊手法卻仍在 2017 年 5 月讓 WannaCry 勒索病毒全球肆虐，以及隨後出現的多起惡意程式攻擊。正如先前所說，WannaCry 勒索病毒仍是我們 2018 年經常攔截到的頭號惡意程式家族之一，而 EternalBlue 相關的網路連線也是我們偵測最多的對外攻擊活動。

PDF 閱讀器和管理程式依然不斷被發現漏洞

已知和已修補漏洞持續遭到攻擊，顯示企業應更加注意那些常用辦公室軟體的漏洞。

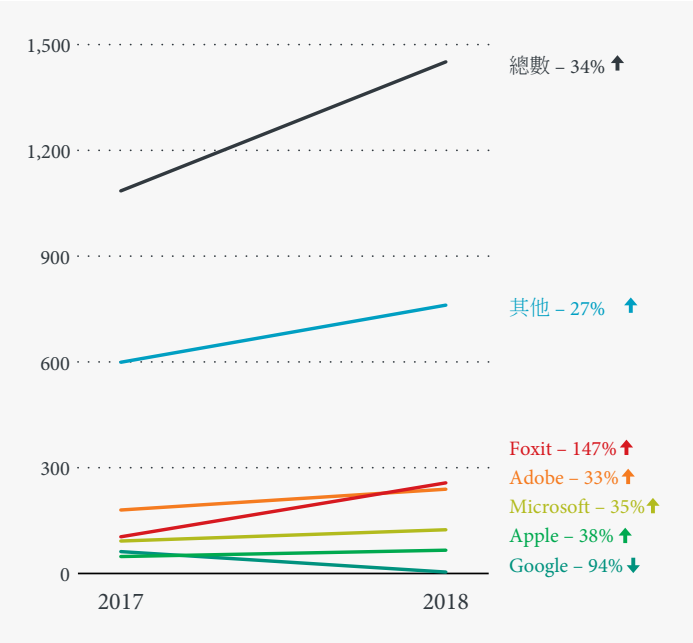

圖 18：重要軟體廠商漏洞數量逐年比較：已發現和通報的漏洞數量增加。

根據我們的資料，包括參與我們 Zero Day Initiative (ZDI) 漏洞懸賞計畫的 3,500 多名獨立研究人員所貢獻的情報[80]，Foxit 是已通報漏洞數量最多的軟體廠商 (257 個)，其次是 Adobe (239 個)。Adobe 和 Foxit 都是製作、修改、管理 PDF 檔案的軟體工具廠商。至於 Microsoft、Apple 和 Google 三巨頭的已通報漏洞數量則分別為 124、66 和 4。

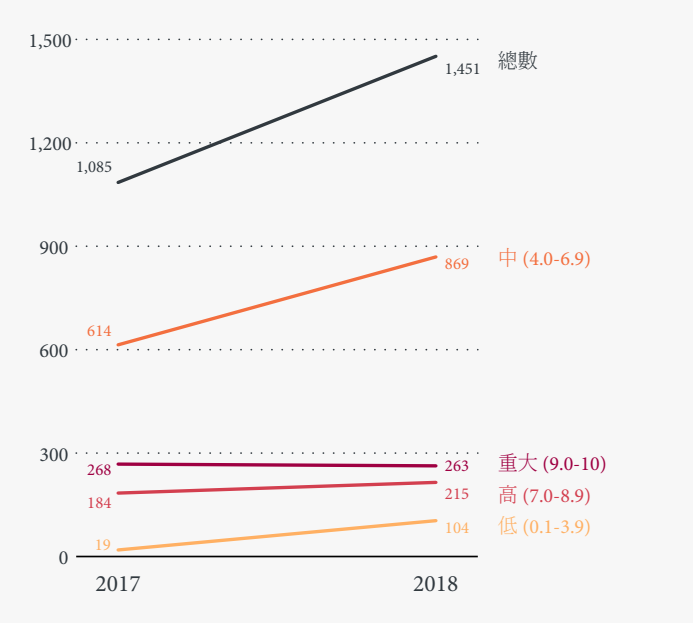

圖 19：各種嚴重等級的漏洞數量逐年比較：重大等級的漏洞從 25% 減少至 18%。

在所有 2018 年揭露的漏洞當中，有 60% 為中嚴重等級漏洞，較 2017 年增加 3 個百分點。所幸，重大等級的漏洞從 2017 年的 25% 減少至 2018 年的 18%。

工業控制系統人機介面軟體的漏洞數量依然令人擔憂

在所有已通報的漏洞當中，有相當比例是工業控制系統 (ICS) 軟體的漏洞。Advantech 和 Wecon 兩家公司的軟體就各占了一百多個漏洞。這些漏洞大多發生在工業控制系統以及監控與資料擷取 (SCADA) 系統的人機介面 (HMI) 軟體。HMI 是使用者監控、管理、設定廠房設施各種流程狀態的主要介面，一般皆認為不會對設備和裝置造成直接影響。然而，不幸的是，這些系統除了能為駭客在進行針對性攻擊時提供寶貴的偵查資訊之外，還有可能讓駭客實質影響設備的功能。尤其，如果有某個漏洞能讓駭客修改特定設備或裝置的門檻值的話。

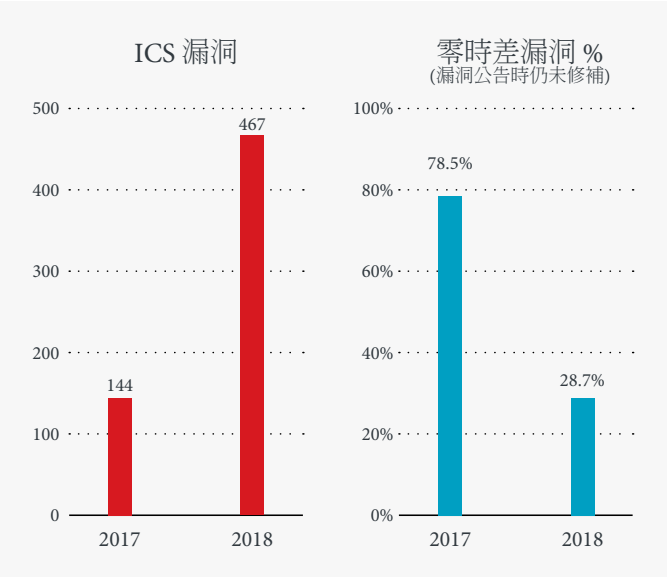

圖 20：ICS 漏洞數量逐年比較：儘管 ICS 的漏洞數量增加，但漏洞公告時仍未完成修補的比例卻降低。

此外，相較於其他軟體廠商，HMI 廠商的整體回應速度也無明顯改善。在 2018 年通報的所有零時差漏洞當中，有 85% 是歸類在 ICS 底下[81]。

IoT 資安事件突顯智慧家庭安全問題

儘管經由感染大量路由器來發動分散式阻斷服務 (DDoS) 攻擊的 Mirai[82] 和 Satori[83] 兩個病毒的作者皆已受到法律制裁，但針對路由器的攻擊卻絲毫不減。全球各地的路由器依然持續受到 Mirai 衍生的病毒攻擊[84]。此外，VPNFilter 這個功能更上層樓的路由器惡意程式 (增加了偵查與長期潛伏能力) 更是為路由器殭屍網路開啟了 DDoS 攻擊以外的運用手法[85]。正如我們的上半年資安總評報告指出[86]，路由器殭屍網路的運用正朝多樣化發展，例如：虛擬加密貨幣挖礦與網址嫁接 (Pharming) 攻擊[87]。

網路犯罪集團充分運用路由器的弱點

在巴西，MikroTik 廠牌的路由器因其使用的 RouterOS 作業系統隨附的遠端管理軟體含有一個已修補的漏洞，因而遭到網路犯罪集團駭入並用於虛擬加密貨幣挖礦。駭客將開採門羅幣 (Monero，XMR) 的惡意 Coinhive 腳本注入使用者造訪的每個網頁，但最後卻只有在使用者遇到 HTTP 錯誤時才會載入挖礦程式碼以避免立即被發現[88]。正如先前所述，智慧裝置本身通常沒有太大的運算效能來開採足夠的虛擬加密貨幣，但儘管如此，網路犯罪集團還是將路由器列為鎖定對象。

除此之外，我們也深入研究了一個名為 Novidade 的漏洞攻擊套件[89]。它會藉由跨站請求偽造 (CSRF) 手法來篡改路由器的網域名稱系統 (DNS) 設定，讓使用者接下來的上網活動都會被導向駭客掌控的伺服器。例如，倘若使用者的路由器遭到感染，接下來當使用者要連上自己的網路銀行時，就會被帶往歹徒偽造的銀行網頁。除非使用者的觀察敏銳，能夠瞬間發覺任何異樣，否則很可能就會直接在偽造的銀行網頁上輸入自己的帳戶登入名稱和密碼，而這等於直接將帳戶拱手交給了網路犯罪集團。

Windows SMB 通訊協定漏洞相關活動占路由器惡意對外連線大宗

根據趨勢科技 Smart Home Network 解決方案所回報的資料顯示 (其中也包含第三方路由器廠牌的回報資料)，以下是網路流量活動排行 (包含正常連線) 和分布圖。從 Telnet 預設密碼登入活動就可看出使用者並未修改裝置出廠設定的密碼。這樣的作法就好像買了個保險箱來保管一些重要財產，卻並未更換原廠預設的密碼組合一樣，等於為盜賊開啟方便之門。

此外，我們也發現針對 Microsoft Windows SMB 漏洞的 EternalBlue 活動相當多。

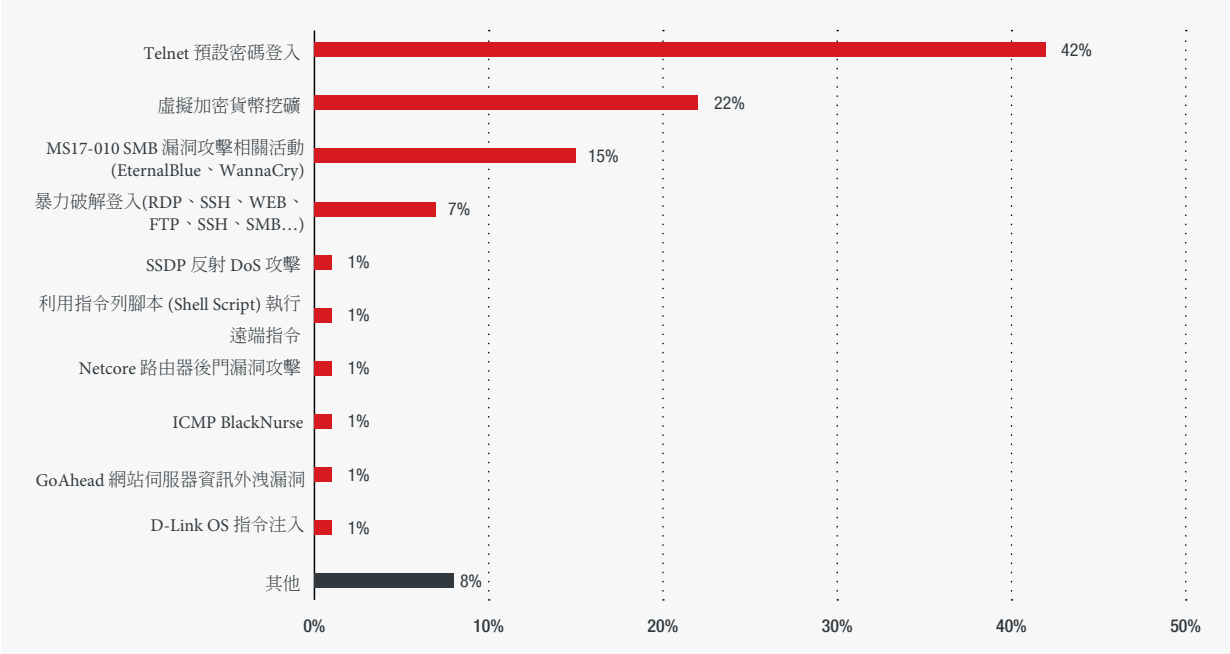

圖 21：2018 年惡意活動偵測規則觸發比例分布：Telnet 預設密碼登入是最常偵測到的活動。

為了更進一步深入研究，我們將範圍縮小至對外連線活動，因為這可反映出路由器是否遭到入侵並試圖向駭客回報。我們發現，疑似 WannaCry 相關的活動占了對外通訊一半以上，此外還有其他各種不同的洪水攻擊 (ICMP 和 TCP SYN) 與暴力破解攻擊等等。這也呼應了前述有關勒索病毒的威脅情勢，那就是：縱然 WannaCry 所攻擊的漏洞早已有修補更新可用，但該病毒依然到處橫行。

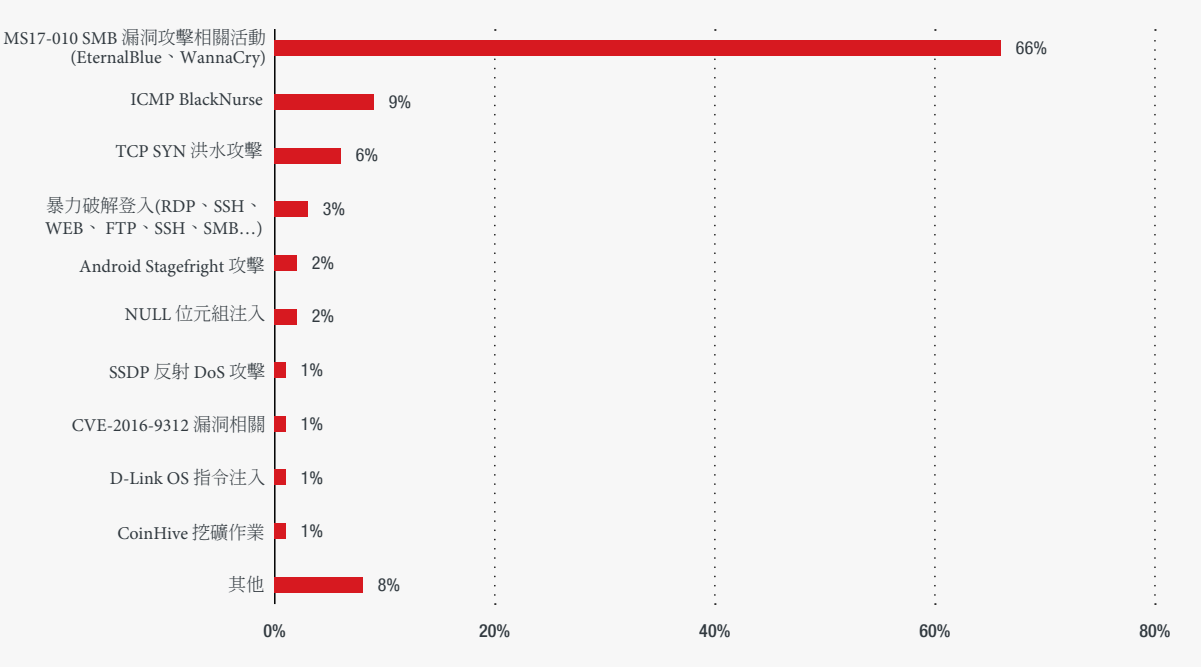

圖 22：2018 年對外連線活動比例分布：WannaCry 相關的活動數量最多。

前述連線來自許多不同國家，但絕大部分皆來自亞洲。

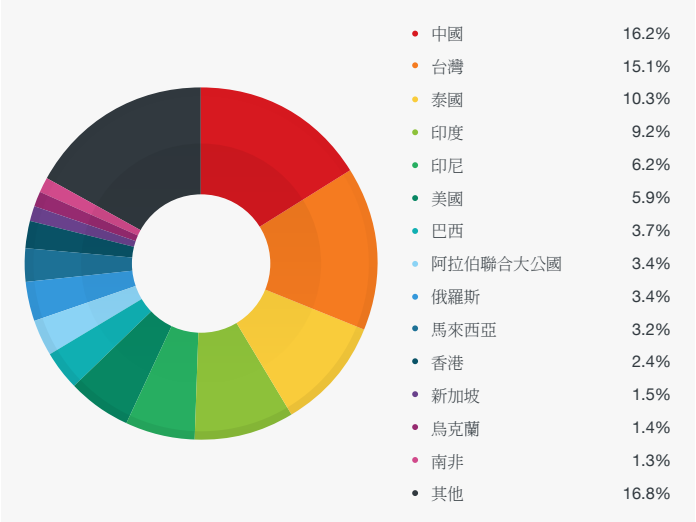

圖 23：2018 年路由器相關事件分布國家：絕大多數對外連線活動皆來自亞洲國家。

隨著越來越多家庭使用者開始擔任起「智慧家庭網路系統管理員」，這些使用者必須確實了解並落實家用路由器安全原則，以免讓路由器成為駭客的入口。由於路由器只是整個網際網路的一個小小環節，因此很容易被人忽略。但它卻扮演著各類裝置與網際網路連線的門戶，因此必須獲得妥善保護。

超大型資料外洩持續攀升，隱私權的問題與因應更加重要

資料隱私法規全面上路

歐盟通用資料保護法 (General Data Protection Regulation，簡稱 GDPR) 在 2018 年 5 月正式上路，而大量的通報和釋疑案件也開始湧入歐盟辦公室，因為各國監理單位已開始對違規者發出警告[90]。事實上，在該法規上路的同一天，美國的一些大型企業就被隱私權團體點名投訴[91]。但直到年底左右，監理單位才開始真正祭出罰鍰：奧地利一起涉及監視保全錄影相關的違規案件遭罰 5,280 歐元[92]、德國某社群網站因採用未加密文字方式儲存使用者密碼而遭罰 2 萬歐元[93]、葡萄牙某醫院因發生重大醫療資料違規而被重罰 40 萬歐元[94]。

此外，一些其他國家也在 2018 年，實施或推出了自己的隱私權法規。例如，澳洲的「應通報之資料外洩」(Notifiable Data Breaches) 規範已從 2 月開始生效[95]，加拿大也隨後跟進，在四月實施更多強制性資料外洩通報法規[96]。英國的「資料保護法案」(Data Protection Bill) 也在三月通過公開委員會審查，不僅在脫歐之後依然能夠落實 GDPR 規範，並且將取代原有的「1998 年資料保護法」(Data Protection Act of 1998)[97]。在美國，「2018 年加州消費者隱私法」(California Consumer Privacy Act of 2018) 在六月無異議通過[98]，該法案的主要適用對象為企業 (不像 GDPR 廣泛涵蓋所有處理資料的機構)，而主要保護對象也是從客戶蒐集而來的資料 (不像 GDPR 涵蓋歐盟人民的所有資料)。日本的個人資訊保護法也在 7 月正式宣告與 GDPR 具備同等效力，且雙方互相承認兩法律具備同等約束力，並允許雙邊跨境傳輸資料[99]。

然而，前述某些國家 (澳洲、加拿大、英國、美國以及紐西蘭) 同樣也是 Five Eyes 情報聯盟的會員，該聯盟規定資訊與通訊企業有義務協助執法機關。這些會員國宣稱，在取得保護人民的資訊時若遭到任何阻礙，將透過「技術、立法與其他強制手段來達成合法存取的目的」[100]。然而，加密若是能被破解就不算是安全的加密，因此，當企業面臨政府的強制要求時，無可避免將面臨艱難抉擇。

資料外洩創新高

2018 年，資料外洩通報筆數再創新高，美國至少有 22 起資料外洩其通報的外洩筆數突破百萬。整體而言，根據 Privacy Rights Clearinghouse (隱私權情報交換所) 的資料，美國總共有 807 件資料外洩通報，較前一年增加 46%[101]。雖然這有一部分的原因或許是由於法規更加嚴格而使得通報數量增加，但卻不失為一項指標，顯示企業在資料隱私和安全方面仍有許多需要改進之處。

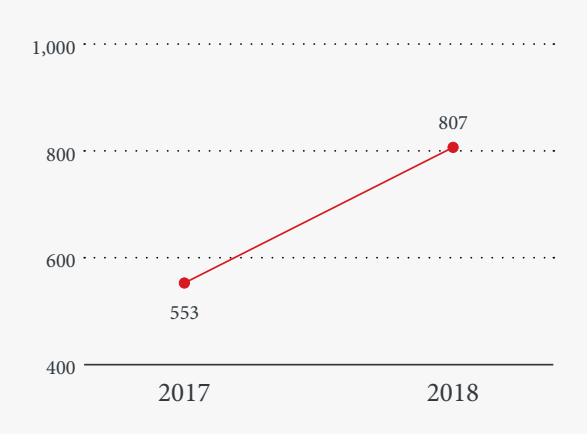

圖 24：資料外洩通報數量逐年比較：美國資料外洩事件變多。

在美國以外地區，除了我們在上半年資安總評報告當中所指出的之外，一些重大的資料外洩事件還包括：一家連鎖飯店[102] 以及一家航空公司[103] 分別外洩了 1.3 億與 940 萬名使用者資料。

對於網路犯罪集團來說，這些遭到外洩的資料可說是協助他們發動攻擊的最佳養分。外洩的資料通常會以原始方式在深層網路論壇上販賣，或者經過整理之後賣到更好的價錢，至於買家則通常是其他犯罪集團。購買資料的犯罪集團會利用這些資料來發動網路攻擊：從網路釣魚到針對性攻擊等等，而這些攻擊會再造成更多資料外洩，進而形成一種惡性循環。事實上，2018 下半年，我們在監控深層網路時就曾發現某個疑似與前述連鎖飯店外洩資料相關的貼文[104]，而這也讓我們一窺個人身分資訊 (PII) 非法交易的供應鏈樣貌。

機器學習解決方案、跨領域研究以及執法行動出現重大斬獲

機器學習的應用進一步強化資安解決方案

趨勢科技研究機構 Trend Micro Research 向來強調機器學習在網路資安所扮演的角色與重要性[105]，並且透過我們的解決方案示範了如何運用機器學習技巧來偵測惡意活動。我們的解決方案採用機器學習技術已有一段時日，只不過這項技術近來突然大受矚目，好像一項新的技術。但其實不然，機器學習技術存在已久，只不過由於特性使然，機器學習必須仰賴大量的優質訓練資料，才能變得更強、更精準。

也因為這樣的緣故，機器學習在網路防護上的應用非常廣泛。例如 2018 年，我們即曾說明我們如何運用機器學習來減少使用者下載不明軟體的情況[106]、偵測憑證濫用的情況[107]、利用惡意網路流量叢集技巧來協助偵測惡意程式攻擊行動[108]，以及偵測惡意詆毀網站的攻擊行動[109]。

除了惡意程式和網路流量之外，我們也利用人工智慧專家系統來模仿資安人員辨識可疑電子郵件的方式，研發出一套可偵測變臉詐騙 (BEC) 電子郵件的解決方案[110]。除此之外，我們也利用人工智慧開發出所謂的「Writing Style DNA」(寫作風格 DNA) 技術，藉由與寄件人先前的電子郵件寫作風格進行比對來防範假冒郵件。Writing Style DNA 技術會分析並結合眾多個人寫作風格的特徵，包括：句子長度、重複字詞、標點符號，以及其他數千種特徵。

不僅如此，我們也預料網路犯罪集團將想盡辦法刻意避開資安防護中的機器學習技術。為了應付這樣的情況，我們藉由產生敵對樣本的方式，來讓機器學習系統更趨完善[111]。

上述這些發展，證明了機器學習的應用無窮無盡，而且能用於網路與裝置防護的各種面向。此外，機器學習也不應被單純視為資安產品的額外附加功能。

醫院和工業控制系統網路資產暴露在外

想要創造一個安全的資訊交換世界，需從多方面下手，其中很重要的一點就是深入掌握當前威脅情勢的發展。例如，雖然公家機關的設備和系統在連網之後可以提升效率，但相對地卻也增加了風險。

Trend Micro Research 針對醫療產業曾做過一份詳盡的風險分析[112]，主要針對暴露在外的醫療裝置以及供應鏈相關的攻擊。我們在結論中指出，基於醫療產業所儲存的資料特殊，再加上其網路及供應鏈的資安現況，該產業非常容易遭到攻擊，尤其是連網的醫院。

此外，我們的研究人員也發現石油、天然氣、生質氣體、電力、自來水等公共事業有許多暴露在外的人機介面 (HMI) 系統，這些系統的控制台在操作與檢視時都不需經過太多認證 (甚至不需認證)[113]。由於這些公共事業提供了民生必需的服務，因此這項發現令人相當擔憂。例如，萬一自來水廠遭到攻擊，很可能會帶來嚴重的後果，甚至引發連鎖效應。

我們對物聯網 (IoT) 整體以及工業物聯網 (IIoT) 的資安問題研究甚至更加深入。我們提出了幾種針對業界兩大主流通訊協定：Message Queuing Telemetry Transport (MQTT) 和 Constrained Application Protocol (CoAP) 暴露在外所可能衍生的攻擊情境[114]。希望能藉此喚起業界正視採用預設組態來運作的風險，以及強制加密和認證的必要性。

公私部門合作破獲網路犯罪集團

與網路犯罪集團或其他犯罪分子的對抗，是一場永無止境的戰鬥，不論對所有電腦使用者、資安人員以及執法機關皆然。所幸，每隔一陣子，正義的一方就會出現重大斬獲，不僅終結了網路犯罪集團的營運，更將網路犯罪分子繩之以法。例如，知名的防毒反制服務 Scan4You 遭到破獲就是一起重大的成功案例。該服務在 2017 年被關閉[115]，其中一名長期犯罪成員被判決 14 年徒刑[116]，而這一切要歸功於趨勢科技與 FBI 的長期密切合作。

長久以來，趨勢科技一直在透過公私部門合作計畫與全球各地的執法機關密切配合[117]。這樣的合作之所以重要，就在於雙方能夠截長補短。當然，資安廠商不可能將網路犯罪集團繩之以法，但執法機關有時也缺乏足夠的威脅情報蒐集能力 (甚至完全沒有)，尤其是跨境犯罪。正因如此，這樣的聯合行動才能發揮綜效，有效遏止數位地下網路的組織性犯罪。

雖然我們的威脅研究主要是為了保障我們的客戶安全，但這些資訊對緝捕網路犯罪分子卻非常有用。未來，趨勢科技仍將與執法單位繼續保持合作，因為從過去的案例證明，這類合作確實有助於遏止犯罪，進而創造一個更安全的運算環境。

全方位多層式防護最適合應付今日的威脅情勢

企業應嚴肅看待 2018 年出現的各種資安問題與挑戰，並重新檢視當前的資安策略。今日各種豐富的科技所帶來的整合、功能、便利與成本效益，為企業開創了拓展業務與成長的契機。但卻也擴大了歹徒的攻擊面，讓網路暴露在新的風險當中。每當企業在推行新的計畫 (例如雲端移轉或建置現代化工業控制系統) 或者重新檢討當前的政策時，資安都應該是企業優先考量的一項重點。

本報告所指出的大多數資安問題，都能藉由多層式防護來解決，包括可在閘道、網路、伺服器以及端點上偵測威脅的解決方案，然後再結合多樣化偵測技術，如：行為偵測、沙盒模擬分析、入侵防護等等。尤其像無檔案式威脅更需要這類多層式防護，因為，即使是最微小的網路流量或系統登錄異常，系統管理員都應該收到相關的警示，因為這可能意味著有攻擊正在進行。

社交工程攻擊是任何企業皆應正視的問題，而且要在企業文化當中培養防範能力，因為這類攻擊技巧是網路犯罪集團和其他犯罪分子一項很重要的武器。企業應定期舉辦資安意識提升計畫，此外，也應透過不斷的演練來培養員工的良好習慣，並定期測試員工在日常上網時的警戒心。

家庭使用者應採用一些能夠妥善保護電腦、平板、智慧型手機以及其他連網裝置與裝置內資料的防護技術。除此之外，使用者也應定期更換密碼、避免在不同的帳號使用相同密碼、盡可能啟用多重認證功能，或者使用一套密碼管理工具來妥善保護自己的各種帳號密碼。智慧家庭的系統管理員應採用能在路由器層次攔截威脅的資安防護，讓連上路由器的裝置都能受到保護。

威脅情勢回顧

2018 年，趨勢科技 Smart Protection Network™ 全球威脅情報網總共幫使用者攔截了480 億次以上的威脅，包含各式各樣網路犯罪攻擊所用到的電子郵件、檔案和網址。

48,387,151,118

2018 年整體威脅攔截總數

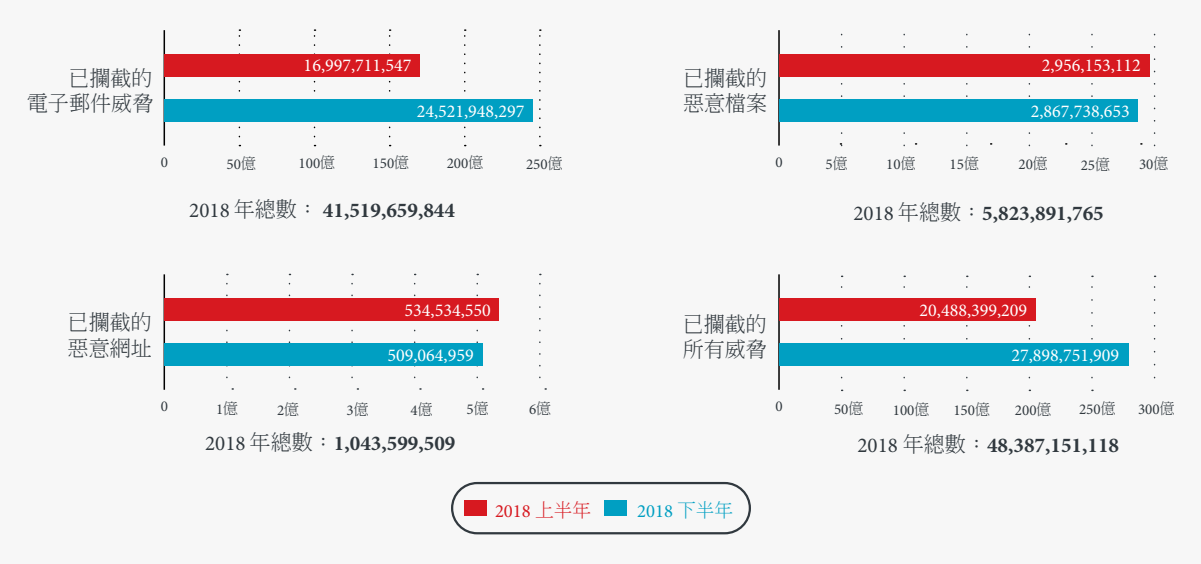

圖 25：趨勢科技 Smart Protection Network™ 已攔截的電子郵件、檔案與網址半年期比較：已攔截的電子郵件威脅增加。

整體上，勒索病毒威脅的數量減少，但新的勒索病毒家族依然不斷出現。其中有許多都出現新的行為或功能上的優化，並且較前一代更強。

ACKNYS	DEATHNOTEBATCH	GOODRABBIT	MINOTAUR	STINGER
ADAMLOCKER	DEDWARE	GRUJARSORIUM	MONEROPAY	STOP
ANIMUS	DEFENDER	GUILLOTINE	MRDEC	STUPJ
ANNABELLE	DELPHIMORIX	GUSLOCKER	NECNE	SURESOME
ARGUS	DESKLOCKER	HAKNATA	NEGOZI	SURI
ARMAGE	DESKTOP	HARROS	NIKSEAD	SYMMYWARE
AURORA	DEUSCRYPT	HAXLOCKER	NMCRYPT	SYSTEM
AUSIV	DGER	HEARTBLEED	NOTOPEN	TALINSLOCKER
AUTISMLOCKER	DIRCRYPT	HERMES	NOWORI	TBLOCKER

AUTOCRYPT	DISKDOC	HIDDENBEER	NOZELESN	TEARDROP
AVCRYPT	DISTRICT	HIGUNIEL	OUTSIDER	TEERAC
BANACRYPT	DONUT	HOLA	PABGEE	TERMITE
BHOOD	DOTZERO	HONOR	PACTELUNG	THANATOS
BIRBWARE	DWORRY	HORSUKE	PAIN	TK
BLACKEYE	DYAR	ICRYPT	PEDCOT	TQV
BLACKHEART	EBOLA	INSANECRYPT	PESOJ	TROLDESH
BLACKRUBY	ELGOSCARE	INSTALADOR	PEWDIEPIE	TRON
BLACKWORM	EMBRACE	ITBOOK	POSIONFANG	USELESS
BLANK	ENCODER	JEFF	POTTIEQ	VAPOR
BLOODJAWS	ENYBENY	KASITOO	PYLOCKY	VBRSCARE
BORSCH	EOEO	KATYUSHA	RANCIDLOCKER	VENDETTA
BOSLOKI	EPAR	KCTF	RANDOMLOCKER	VERTUN
BYTELOCKER	EVERBE	KILLMBR	RAPID	VIBOROT
CARDSOME	EXOCRYPT	KILLRABBIT	RARA	WADHRAMA
CCP	FAKEKILLBOT	KINGBOROS	REDEYE	WANNAPEACE
CDLLM	FBLOCKER	KRAKATOWIS	RONT	WARRIOR
CESLOCKER	FILECODER	KRAKEN	RSAUTIL	WHITEROSE
CREAMPI	FILECRYPTOR	KYMERA	RUSSENGER	WHOOPSIE
CRUSIS	FILEF	LADON	RYUK	WINLOCK
CRYAR	FILESLOCKER	LAZAGNECRYPT	SAR	WISE
CRYBRZ	FLKR	LEBANA	SATURN	WYVERN
CRYPT	FLYTERPER	LIGMA	SATWANCRYPT	XBASH
CRYPTG	FOREIGN	LILFINGER	SATYR	XEROWARE
CRYPTOLITE	FORMA	LIME	SEPSIS	XLOCKR
CRYPTOLOOT	FURY	MAFYA	SEQUR	XUY
CRYPTOPAL	GAMEOVER	MAGICIAN	SHRUG	YAMI
CRYPTOR	GANDCRAB	MARYAH	SIGMA	ZENIS
CRYPWALKER	GANDCRYPT	MCRANSOM	SIGRUN	ZGAMES
CSGO	GARRANTYDECRYPT	MCRYPT	SKIDDY	ZLOCKER
CYPEN	GEGLOCKER	MEDUZA	SKULL	ZOLDON
CYRLOCKER	GERBER	MEGACRYPTOR	SKYFILE	ZYKA
CYSEARCHER	GHOST	MEINE	SNEAKYJ	ZZZ
DABLIO	GLOBIM	MIMICRY	SNOWPICNIC	
DATAKEEPER	GODCRYPT	MINDCRYPT	SOBACHKA	
DEADCRYPT	GOLDEN	MINDLOST	STACUS	

表 3：2018 年新出現的勒索病毒家族：本期發現
222 個新的勒索病毒家族。

漏洞攻擊套件活動較 2017 年減少，許多漏洞攻擊套件都已消失不見，取而代之的也不多。

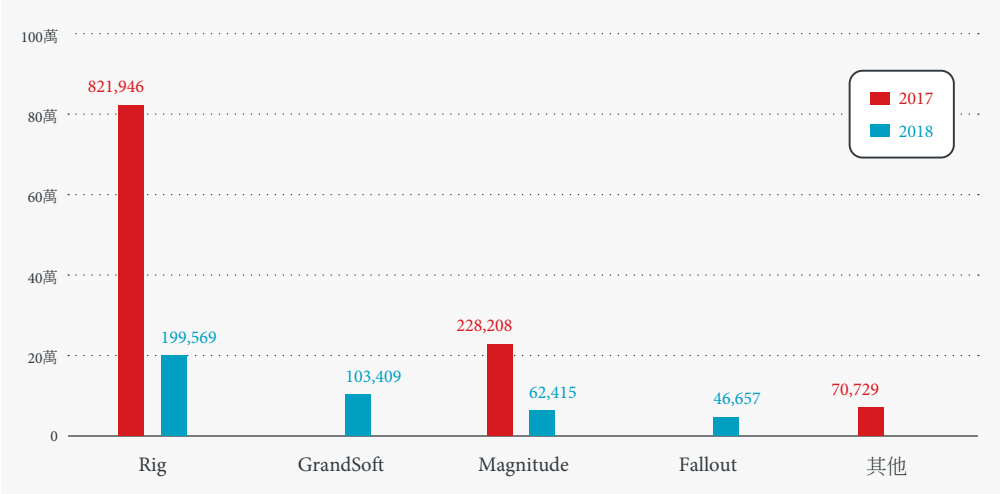

圖 26：漏洞攻擊套件活動逐年比較：Rig 和 Magnitude 依然活躍，一些不再活躍的套件則被新的所取代。

根據我們的資料，XLS 依然是垃圾郵件附件最常用的檔案類型，但 EXE (執行檔) 也緊跟在後。

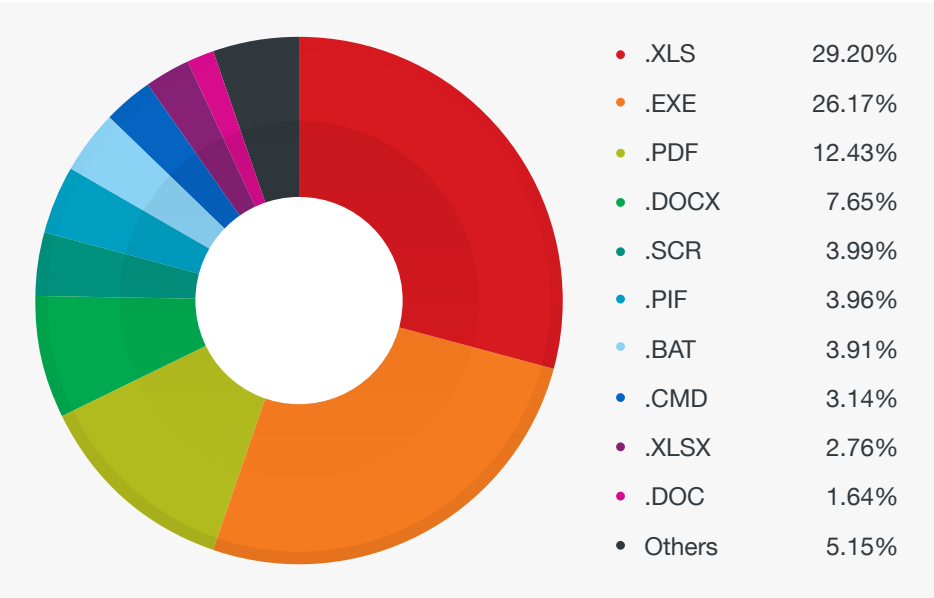

圖 27：2018 年垃圾郵件附件檔案類型分布：XLS 和 EXE 是垃圾郵件附件最常用的檔案類型。

參考資料

1. Black Hat USA 2018。(2018 年 6 月)。*Black Hat*。「2018 年美國 Black Hat 駭客大會與會者問卷調查：網路資安現況」(The 2018 Black Hat USA Attendee Survey: Where Cybersecurity Stands)。上次存取時間 2019 年 1 月 28 日： https://www.blackhat.com/docs/us-18/black-hat-intel-where-cybersecurity-stands.pdf.
2. Black Hat Europe 2018。(2018 年 11 月)。*Black Hat*。「2018 年歐洲 Black Hat 駭客大會與會者問卷調查：歐洲網路資安挑戰」(The 2018 Black Hat Europe Attendee Survey: Europe's Cybersecurity Challenges)。上次存取時間 2019 年 1 月 28 日：http://images.blackhat.com/Web/UBMAmericasTech/%7Bc0e36393- 4267-48d4-b493-0c963173c732%7D_BH_EU18_Report.pdf.
3. Black Hat Asia 2018。(2018 年 3 月)。*Black Hat*。「2018 年亞洲 Black Hat 駭客大會與會者問卷調查：亞洲網路資安風險」(The 2018 Black Hat Asia Attendee Survey: Cybersecurity Risk in Asia)。上次存取時間 2019 年 1 月 28 日：https://www.blackhat.com/docs/us-18/Cybersecurity_Risk_In_Asia.pdf.
4. 趨勢科技。(2018 年 12 月 11 日)。*趨勢科技*。「映對未來：對抗無所不在的持續性威脅」(Mapping the Future: Dealing With Pervasive and Persistent Threats)。上次存取時間 2019 年 2 月 22 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.
5. StatCounter。*Statcounter Global Stats*。「2013 年 1 月至 12 月全球作業系統市場占有率」(Operating System Market Share Worldwide, Jan-Dec 2013)。上次存取時間 2019 年 1 月 28 日：http://gs.statcounter.com/os-market-share#monthly-201301-201312.
6. Cathy Jett。(2018 年 5 月 8 日)。*Fredericksburg.com*。「駭客入侵美國德州 Fredericksburg 學校體系的電子郵件與檔案系統」(Hackers break into Fredericksburg school system's emails, file system)。上次存取時間 2019 年 1 月 28 日：https://www.fredericksburg.com/news/local/fredericksburg/hackers-break-into-fredericksburg-school-system-s-emails-file-system/article_d2b4e537-83ae-5160-8d6c-bbccf705e75a.html.
7. Andy Mannix。(2018 年 8 月 9 日)。*Star Tribune*。「網路駭客滲透美國明尼蘇達州 Hennepin 郡員工電子郵件」(Cyberattackers infiltrate Hennepin County workers' e-mails)。上次存取時間 2019 年 1 月 29 日：http://www.startribune.com/cyber-attackers-infiltrate-hennepin-county-workers-e-mails/490508031.
8. Unity Point Health。(2018 年)。*Unity Point Health*。「資安公告常見問題集」(Security Notice Frequently Asked Questions)。上次存取時間 2019 年 1 月 28 日：https://www.unitypoint.org/security-faq.aspx.
9. Jindrich Karasek。(2018 年 5 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「出現新的網路釣魚詐騙使用 AES 加密並騙取 Apple ID」(New Phishing Scam Uses AES Encryption and Goes After Apple IDs)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-phishing-scam-uses-aes-encryption-and-goes-after-apple-ids.
10. 趨勢科技。(2018 年 6 月 5 日)。*趨勢科技資訊安全新聞*。「使用國際化域名編碼 (punycode) 技巧的簡訊釣魚攻擊」(SMiShing Attacks Leverage Punycode Technique)。上次存取時間 2019 年 1 月 28 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/smishing-attacks-leverage-punycode-technique.
11. Erika Mendoza、Anjali Patil 與 Jay Yaneza。(2018 年 10 月 9 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「網路釣魚行動利用預先駭入的電子郵件帳號，以回覆電子郵件對話串的方式散發 URSNIF 惡意程式」(Phishing Campaign Uses Hijacked Emails to Deliver URSNIF By Replying to Ongoing Threads)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/.
12. Jill McCabe。(2018 年 12 月 11 日)。*FBI*。「FBI Tech Tuesday：變臉詐騙 (BEC) 禮物卡詐騙」(FBI Tech Tuesday: Business Email Compromise (BEC)-Gift Card Fraud)。上次存取時間 2019 年 1 月 28 日：https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-business-email-compromise-bec-gift-card-fraud.
13. 趨勢科技。(2017 年 5 月 13 日)。趨勢科技資訊安全新聞。「WannaCry/WCRY 勒索病毒該如何防範」(WannaCry/WCRY Ransomware: How to Defend against It)。上次存取時間 2019 年 1 月 28 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it.
14. 趨勢科技。(2017 年 12 月 6 日)。*趨勢科技商務支援*。「使用趨勢科技產品來防範 WannaCry 勒索病毒」(Preventing WannaCry (WCRY) ransomware attacks using Trend Micro products)。上次存取時間 2019 年 1 月 28 日：https://success.trendmicro.com/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products.

15. Andy Patrizio。(2017 年 5 月 23 日)。*Network World*。「WannaCry 是一種 Windows 7 現象」(WannaCry was a Windows 7 Phenomenon)。上次存取時間 2019 年 1 月 28 日： https://www.networkworld.com/article/3197762/microsoft-subnet/wannacry-was-a-windows-7-phenomenon.html.

16. Russell Brandom。(2017 年 5 月 15 日)。*The Verge*。「網際網路有史以來最大的勒索病毒攻擊應該怪罪 Microsoft 嗎？」(Is Microsoft to blame for the largest ransomware attacks in internet history?) 上次存取時間 2019 年 1 月 28 日： https://www.theverge.com/2017/5/15/15641198/microsoft-ransomware-wannacry-security-patch-upgrade-wannacrypt.

17. 趨勢科技。(2018 年 4 月 30 日)。*趨勢科技資訊安全新聞*。「最新 GandCrab 勒索病毒變種利用垃圾郵件散布各種惡意檔案」(New GandCrab Variants, Varied Payloads Delivered via Spam Campaign)。上次存取時間 2019 年 1 月 28 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-gandcrab-variants-varied-payloads-delivered-via-spam-campaign.

18. 趨勢科技。(2018 年 9 月 13 日)。*趨勢科技資訊安全新聞*。「新的 Fallout 漏洞攻擊套件散布 Gandcrab 勒索病毒」(New Exploit Kit Fallout Delivering Gandcrab Ransomware)。上次存取時間 2019 年 1 月 28 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-exploit-kit-fallout-delivering-gandcrab-ransomware.

19. Donald Castillo。(2018 年 8 月 20 日)。*趨勢科技資訊安全新聞*。「針對南韓使用者的垃圾郵件挾帶 .EGG 檔案散布 GandCrab v4.3 勒索病毒」(.EGG Files in Spam Delivers GandCrab v4.3 Ransomware to South Korean Users)。上次存取時間 2019 年 1 月 28 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-egg-files-in-spam-delivers-gandcrab-v4-3-ransomware-to-south-korean-users.

20. Charlie Osborne。(2018 年 10 月 12 日)。*ZDNet*。「GandCrab 勒索病毒犯罪集團與加密服務廠商合作」(GandCrab ransomware operators team up with crypter service)。上次存取時間 2019 年 1 月 28 日：https://www.zdnet.com/article/gandcrab-ransomware-teams-up-with-crypter-service/.

21. Joseph C. Chen。(2018 年 3 月 22 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「彈出式廣告與上百個網站正在幫忙散布殭屍網路病毒、虛擬加密貨幣挖礦程式以及勒索病毒」(Pop-up Ads and Over a Hundred Sites are Helping Distribute Botnets, Cryptocurrency Miners and Ransomware)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/.

22. Raphael Centeno。(2018 年 5 月 1 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「正派工具程式 AnyDesk 遭新勒索病毒變種利用」(Legitimate Application AnyDesk Bundled with New Ransomware Variant)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/.

23. Raphael Centeno 與 Noel Llimos。(2018 年 9 月 21 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Viro 殭屍網路勒索病毒出現重大突破」(Viro Botnet Ransomware Breaks Through)。上次存取時間 2019 年 1 月 28 日： https://blog.trendmicro.com/trendlabs-security-intelligence/virobot-ransomware-with-botnet-capability-breaks-through/.

24. Ian Kenefick。(2018 年 9 月 10 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「PyLocky 勒索病毒深入研究」(A Closer Look at the Locky Poser PyLocky Ransomware)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/.

25. Joseph C. Chen。(2018 年 8 月 9 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Princess Evolution 勒索病毒服務徵求業務夥伴」(Ransomware as a Service Princess Evolution Looking for Affiliates)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-as-a-service-princess-evolution-looking-for-affiliates/.

26. Joseph C. Chen。(2018 年 1 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「惡意廣告行動利用 Google DoubleClick 散布加密虛擬貨幣挖礦程式」(Malvertising Campaign Abuses Google's DoubleClick to Deliver Cryptocurrency Miners)。上次存取時間 2019 年 1 月 28 日： https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/.

27. Joseph Chen 與 Chaoying Liu。(2018 年 4 月 4 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「AOL 廣告平台遭注入虛擬加密貨幣網頁挖礦腳本」(Cryptocurrency Web Miner Script Injected into AOL Advertising Platform)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-web-miner-script-injected-into-aol-advertising-platform/.

28. Joseph C. Chen。(2018 年 3 月 22 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「彈出式廣告與上百個網站正在幫忙散布殭屍網路病毒、虛擬加密貨幣挖礦程式以及勒索病毒」(Pop-up Ads and Over a Hundred Sites are Helping Distribute Botnets, Cryptocurrency Miners and Ransomware)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/.

29. Hubert Lin。(2018 年 5 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「虛擬加密貨幣挖礦程式嘗試攻擊已修補的 2017 年 Oracle WebLogic 漏洞，導致連接埠 7001 上的惡意流量暴增」(Malicious Traffic in Port 7001 Surges as Cryptominers Target Patched 2017 Oracle WebLogic Vulnerability)。上次存取時間 2019 年 1 月 28 日：https://blog. trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/.

30. Hubert Lin。(2018 年 1 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「駭客利用 Struts 和 DotNetNuke 漏洞來入侵伺服器以從事虛擬加密貨幣挖礦」(Struts and DotNetNuke Server Exploits Used For Cryptocurrency Mining)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/struts-dotnetnuke-server-exploits-used-cryptocurrency-mining/.

31. Joseph C. Chen。(2018 年 30 月 4 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「FacexWorm 攻擊虛擬加密貨幣交易平台，利用 Facebook Messenger 散布」(FacexWorm Targets Cryptocurrency Trading Platforms, Abuses Facebook Messenger for Propagation)。上次存取時間 2019 年 1 月 28 日： https://blog.trendmicro. com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/.

32. Lorin Wu。(2018 年 3 月 28 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Android 門羅幣挖礦惡意程式 HiddenMiner 可能導致裝置故障」(Monero-Mining HiddenMiner Android Malware Can Potentially Cause Device Failure)。上次存取時間 2019 年 1 月 28 日： https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure/.

33. 趨勢科技網路資安解決方案團隊。(2018 年 3 月 21 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「虛擬加密貨幣挖礦程式經由 PHP Weathermap 漏洞散布，鎖定 Linux 伺服器。」(Cryptocurrency Miner Distributed via PHP Weathermap Vulnerability, Targets Linux Servers)。上次存取時間 2019 年 1 月 28 日：https://blog. trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-distributed-via-php-weathermap-vulnerability-targets-linux-servers/.

34. 趨勢科技。(2018 年 11 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Outlaw 犯罪集團散布殭屍網路病毒從事虛擬加密貨幣挖礦、掃瞄與暴力破解攻擊」(Outlaw Group Distributes Botnet for Cryptocurrency-Mining, Scanning, and Brute-Force)。上次存取時間 2019 年 1 月 28 日： https://blog.trendmicro.com/trendlabs-security-intelligence/outlaw-group-distributes-botnet-for-cryptocurrency-mining-scanning-and-brute-force/.

35. Jindrich Karasek 與 Loseway Lu。(2018 年 6 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「虛擬加密貨幣挖礦殭屍病毒經由疑似詐騙網站攻擊啟用 SSH 服務的裝置」(Cryptocurrency-Mining Bot Targets Devices With Running SSH Service via Potential Scam Site)。上次存取時間 2019 年 1 月 28 日：https://blog. trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-bot-targets-devices-with-running-ssh-service-via-potential-scam-site/.

36. Janus Agcaoili 與 Gilbert Sison。(2018 年 11 月 8 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「虛擬加密貨幣挖礦惡意程式運用各種躲避技巧來入侵系統，包括 Windows Installer」(Cryptocurrency-Mining Malware uses Various Evasion Techniques, Including Windows Installer, as Part of its Routine)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-uses-various-evasion-techniques-including-windows-installer-as-part-of-its-routine/.

37. 趨勢科技網路資安解決方案團隊。(2018 年 7 月 26 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「新的 Underminer 漏洞攻擊套件經由加密的 TCP 通道散布 Bootkit 和虛擬加密貨幣挖礦惡意程式」(New Underminer Exploit Kit Delivers Bootkit and Cryptocurrency-mining Malware with Encrypted TCP Tunnel)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-underminer-exploit-kit-delivers-bootkit-and-cryptocurrency-mining-malware-with-encrypted-tcp-tunnel/.

38. Don Ladores 與 Angelo Deveraturda。(2018 年 4 月 17 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「XIAOBA 勒索病毒改頭換面，變成檔案感染程式與虛擬加密貨幣挖礦程式」(Ransomware XIAOBA Repurposed as File Infector and Cryptocurrency Miner)。上次存取時間 2019 年 1 月 28 日： https://blog.trendmicro. com/trendlabs-security-intelligence/ransomware-xiaoba-repurposed-as-file-infector-and-cryptocurrency-miner/.

39. Gertrude Chavez-Dreyfuss。(2019 年 1 月 29 日)。*Yahoo! Finance*。「2018 年報告：虛擬加密貨幣竊盜、詐騙金額高達 17 億美元」(Cryptocurrency thefts, scams hit $1.7 billion in 2018: report)。上次存取時間 2019 年 1 月 29 日：https://finance.yahoo.com/news/cryptocurrency-thefts-scams-hit-1-7-billion-2018-143345592.html.

40. Fernando Merces。(2018 年 5 月)。*Trend Micro Research*。「地下市場上的虛擬加密貨幣挖礦惡意程式」(Cryptocurrency-Mining Malware in the Underground)。上次存取時間 2019 年 1 月 28 日：https://documents.trendmicro.com/assets/research_brief_Cryptocurrency-Mining_Malware_in_the_ Underground.pdf.

41. Marvin Cruz。(2017 年 6 月 1 日)。*趨勢科技資訊安全新聞*。「資安基礎觀念：利用 PowerShell 的無檔案式威脅開始崛起」(Security 101: The Rise of Fileless Threats that Abuse PowerShell)。上次存取時間 2019 年 1 月 28 日：https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-the-rise-of-fileless-threats-that-abuse-powershell.

42. 趨勢科技。(2018 年 7 月 30 日)。*趨勢科技資訊安全新聞*。「專門攻擊企業系統的 PowerGhost 無檔案惡意程式」(Fileless Malware PowerGhost Targets Corporate Systems)。上次存取時間 2019 年 1 月 28 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fileless-malware-powerghost-targets-corporate-systems.

43. Buddy Tancio。(2017 年 6 月 15 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「SOREBRECT：會注射程式碼的無檔案式勒索病毒」(Analyzing the Fileless, Code-injecting SOREBRECT Ransomware)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/.

44. Michael Villanueva。(2017 年 8 月 2 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「純無檔案式惡意程式 JS_POWMET 初探」(A Look at JS_POWMET, a Completely Fileless Malware)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/.

45. Jai Vijayan。(2018 年 5 月 10 日)。*Dark Reading*。「POS 惡意程式 TreasureHunter 的作者公開其原始程式碼」(Author of TreasureHunter PoS Malware Releases Its Source Code)。上次存取時間 2019 年 1 月 28 日：https://www.darkreading.com/vulnerabilities---threats/author-of-treasurehunter-pos-malware-releases-its-source-code-/d/d-id/1331778.

46. 趨勢科技。(2018 年 1 月 3 日)。*趨勢科技資訊安全新聞*。「IoT 殭屍網路 Satori 原始程式碼在 Pastebin 上公開」(Source Code of IoT Botnet Satori Publicly Released on Pastebin)。上次存取時間 2019 年 1 月 28 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/source-code-of-iot-botnet-satori-publicly-released-on-pastebin.

47. Francis Antazo、Byron Gelera、Jeanne Jocson、Ardin Maglalang 與 Mary Yambao。(2018 年 8 月 25 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「從 Hidden Tear 和 EDA2 衍生而來的最新開放原始碼勒索病毒可能以企業為目標」(New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-open-source-ransomwar-based-on-hidden-tear-and-eda2-may-target-businesses/.

48. Hubert Lin、Fyodor Yarochkin 與 Alfredo Oliveira。(2018 年 10 月 25 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「組態設定錯誤導致容器被用於散布虛擬加密貨幣挖礦惡意程式」(Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware)。上次存取時間 2019 年 1 月 28 日：https://blog.trendmicro.com/trendlabs-security-intelligence/misconfigured-container-abused-to-deliver-cryptocurrency-mining-malware/.

49. Docker。*Docker 說明文件*。「安全引擎」(Secure Engine)。上次存取時間 2019 年 2 月 13 日：https://docs.docker.com/engine/security/.

50. Woody Leonhard。(2018 年 1 月 9 日)。*Computer World*。「Microsoft 撤掉問題重重的 AMD 電腦 Windows Meltdown/Spectre 漏洞修補更新」(Microsoft yanks buggy Windows Meltdown/Spectre patches for AMD computers)。上次存取時間 2019 年 1 月 28 日：https://www.computerworld.com/article/3246188/microsoft-windows/microsoft-yanks-buggy-windows-meltdown-spectre-patches-for-amd-computers.html.

51. Claudio Canella、Jo Van Bulck、Michael Schwarz、Moritz Lipp、Benjamin von Berg、 Philipp Ortner、Frank Piessens、Dmitry Evtyushkin 與 Daniel Gruss。(2018 年 11 月 13 日)。*ArXiv*。「以系統性方式評估暫態執行攻擊與防禦」(A Systematic Evaluation of Transient Execution Attacks and Defenses)。上次存取時間 2019 年 1 月 28 日： https://arxiv.org/pdf/1811.05441.pdf.

52. Lily Hay Newman。(2019 年 1 月 3 日)。Wired。「Intel 菁英團隊仍在試圖解決 Meltdown 和 Spectre 漏洞」(The Elite Intel Team Still Fighting Meltdown and Spectre)。上次存取時間 2019 年 1 月 29 日：https://www.wired.com/story/intel-meltdown-spectre-storm/.

53. Steven J. Vaughan-Nichols。(2018 年 12 月 3 日)。*ZDNet*。「Kubernetes 被發現第一個重大資安漏洞」(Kubernetes' first major security hole discovered)。上次存取時間 2019 年 1 月 29 日： https://www.zdnet.com/article/kubernetes-first-major-security-hole-discovered/.

54. Jordan Liggitt。(2018 年 11 月 26 日)。*Github*。「CVE-2018-1002105：kube-apiserver 的 Proxy 請求處理方式可能造成 TCP 連線出現漏洞」(CVE-2018-1002105: proxy request handling in kube-apiserver can leave vulnerable TCP connections)。上次存取時間 2019 年 1 月 28 日： https://github.com/kubernetes/kubernetes/issues/71411.

55. 趨勢科技。(2018 年 2 月 2 日)。*趨勢科技資訊安全新聞*。「北韓駭客據稱利用 Adobe Flash Player 漏洞 (CVE-2018-4878) 攻擊南韓目標」(North Korean Hackers Allegedly Exploit Adobe Flash Player Vulnerability [CVE-2018-4878] Against South Korean Targets)。上次存取時間 2019 年 1 月 28 日：https://www.trendmicro. com/vinfo/us/security/news/vulnerabilities-and-exploits/north-korean-hackers-allegedly-exploit-adobe-flash-player-vulnerability-cve-2018-4878-against-south-korean-targets.

56. Chris Williams。(2018 年 5 月 9 日)。*The Register*。「都 2018 年了，您的 Windows PC 還是可能因為一個網頁而中毒，而應用程式也能跳出 Hyper-V 虛擬環境」(It's 2018, and a webpage can still pwn your Windows PC – and apps can escape Hyper-V)。上次存取時間 2019 年 1 月 29 日：https://www.theregister.co.uk/2018/05/09/microsoft_windows_hyperv_patch_ tuesday/.

57. 趨勢科技。(2018 年 5 月 31 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Rig 漏洞攻擊套件現在會利用 CVE-2018-8174 來散布門羅幣挖礦程式」(Rig Exploit Kit Now Using CVE-2018-8174 to Deliver Monero Miner)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/rig-exploit-kit-now-using-cve-2018-8174-to-deliver-monero-miner/.

58. Charlie Osborne。(2018 年 8 月 15 日)。*ZDNet*。「Microsoft 每月定期更新：解決了 60 個漏洞，包括兩個正遭受攻擊的漏洞」(Microsoft Patch Tuesday: 60 vulnerabilities resolved including two active exploits)。上次存取時間 2019 年 1 月 29 日：https://www.zdnet.com/article/microsoft-patch-tuesday-60-vulnerabilities-resolved-including-two-active-exploits/.

59. Catalin Cimpanu。(2018 年 11 月 12 日)。*ZDNet*。「Internet Explorer 的腳本引擎成了 2018 年北韓進階持續性滲透攻擊的最愛」(Internet Explorer scripting engine becomes North Korean APT's favorite target in 2018)。上次存取時間 2019 年 1 月 29 日：https://www.zdnet.com/article/internet-explorer-scripting-engine-becomes-north-korean-apts-favorite-target-in-2018/.

60. Dustin Childs。(2018 年 8 月 14 日)。*Zero Day Initiative*。「2018 年 8 月份資安更新評析」(The August 2018 Security Update Review)。上次存取時間 2019 年 1 月 29 日：https://www.zerodayinitiative.com/blog/2018/8/14/the-august-2018-security-update-review.

61. Catalin Cimpanu。(2018 年 10 月 9 日)。*ZDNet*。「Microsoft 2018 年 10 月定期更新修正了 FruityArmor 進階持續性滲透攻擊所利用的零時差漏洞」(Microsoft October 2018 Patch Tuesday fixes zero-day exploited by FruityArmor APT)。上次存取時間 2019 年 1 月 29 日：https://www.zdnet.com/article/microsoft-october-2018-patch-tuesday-fixes-zero-day-exploited-by-fruityarmor-apt/.

62. 趨勢科技。(2018 年 11 月 14 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「11 月份定期更新修正了另一個 Win32k 零時差漏洞與其他公開漏洞」(November Patch Tuesday Fixes Another Zero-Day Win32k Bug, Other Public Vulnerabilities)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/november-patch-tuesday-fixes-another-zero-day-win32k-bug-other-public-vulnerabilities/.

63. 趨勢科技 Smart Home Network 與 IoT 信譽評等服務團隊。(2018 年 6 月 21 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「駭客利用 Drupal (CVE-2018-7602) 漏洞散布門羅幣挖礦惡意程式」(Drupal Vulnerability [CVE-2018-7602] Exploited to Deliver Monero-Mining Malware)。上次存取時間 2019 年 1 月 29 日： https://blog.trendmicro.com/trendlabs-security-intelligence/drupal-vulnerability-cve-2018-7602-exploited-to-deliver-monero-mining-malware/.

64. Catalin Cimpanu。(2018 年 25 月 4 日)。*Bleeping Computer*。「駭客不讓網站管理員有修補的機會：新的 Drupal 漏洞公開幾小時後即開始發動攻擊」(Hackers Don't Give Site Owners Time to Patch, Start Exploiting New Drupal Flaw Within Hours)。上次存取時間 2019 年 1 月 29 日：https://www.bleepingcomputer.com/news/security/hackers-dont-give-site-owners-time-to-patch-start-exploiting-new-drupal-flaw-within-hours/.

65. Hubert Lin。(2018 年 2 月 15 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Apache CouchDB 漏洞為門羅幣挖礦程式開啟了大門」(Vulnerabilities in Apache CouchDB Open the Door to Monero Miners)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-apache-couchdb-open-door-monero-miners/.

66. Jan Lehnardt。(2017 年 11 月 14 日)。*Apache Mail Archives*。「檢視電子郵件 #6c405bf3f8358e6314076be9f48c89a2e0ddf005...(與回覆)」(Viewing email #6c405bf3f8358e6314076be9f48c89a2e0ddf005...[and replies])。上次存取時間 2019 年 1 月 29 日：https://lists.apache.org/thread.html/6c405bf3f8358e6314076be9f48c89a 2e0ddf00539906291ebdf0c67@%3Cdev.couchdb.apache.org%3E.

67. Hubert Lin。(2018 年 2 月 15 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Apache CouchDB 漏洞為門羅幣 (Monero) 挖礦程式開啟了大門」(Vulnerabilities in Apache CouchDB Open the Door to Monero Miners)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-apache-couchdb-open-door-monero-miners/.

68. Oracle Technology Network。(2017 年 10 月)。*Oracle*。「2017 年 10 月份 Oracle 重大修補更新公告」(Oracle Critical Patch Update Advisory - October 2017)。上次存取時間 2019 年 1 月 29 日： https://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html.

69. Johnlery Triunfante 與 Mark Vicente。(2018 年 2 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Oracle 伺服器漏洞遭駭客用來散布門羅幣 (Monero) 挖礦程式」(Oracle Server Vulnerability Exploited to Deliver Double Monero Miner Payloads)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro. com/trendlabs-security-intelligence/oracle-server-vulnerability-exploited-deliver-double-monero-miner-payloads/.

70. Hubert Lin。(2018 年 5 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「虛擬加密貨幣挖礦程式嘗試攻擊已修補的 2017 年 Oracle WebLogic 漏洞，導致連接埠 7001 上的惡意流量暴增」(Malicious Traffic in Port 7001 Surges as Cryptominers Target Patched 2017 Oracle WebLogic Vulnerability)。上次存取時間 2019 年 1 月 29 日：https://blog. trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/.

71. Veo Zhang。(2016 年 3 月 29 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「CVE-2015-1805 重大漏洞可能讓大多數 Android 手機被永久改機 (root)」(Critical 'CVE-2015-1805' Vulnerability Allows Permanent Rooting of Most Android Phones)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/critical-cve-2015-1805-vulnerability-allows-permanent-rooting-android-phones/.

72. 行動裝置威脅應變團隊。(2018 年 2 月 13 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新的 AndroRAT 攻擊老舊的權限提升漏洞讓 Android 手機被永久改機 (root)」(New AndroRAT Exploits Dated Privilege Escalation Vulnerability, Allows Permanent Rooting)。上次存取時間 2019 年 1 月 29 日： https://blog.trendmicro.com/trendlabs-security-intelligence/new-androrat-exploits-dated-permanent-rooting-vulnerability-allows-privilege-escalation/.

73. Android。(2016 年 3 月 18 日)。*Android*。「2016-03-18 Android 資安公告」(Android Security Advisory—2016-03-18)。上次存取時間 2019 年 1 月 29 日： https://source.android.com/security/advisory/2016-03-18.html.

74. 行動裝置威脅應變團隊。(2018 年 2 月 13 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新的 AndroRAT 攻擊老舊的權限提升漏洞讓 Android 手機被永久改機 (root)」(New AndroRAT Exploits Dated Privilege Escalation Vulnerability, Allows Permanent Rooting)。上次存取時間 2019 年 1 月 29 日： https://blog.trendmicro.com/trendlabs-security-intelligence/new-androrat-exploits-dated-permanent-rooting-vulnerability-allows-privilege-escalation/.

75. CVE Details。(2018 年)。*CVE Details*。「按時間瀏覽漏洞」(Browse Vulnerabilities by Date)。上次存取時間 2019 年 1 月 29 日：https://www.cvedetails. com/browse-by-date.php.

76. Dan Goodin。(2016 年 10 月 21 日)。*Ars Technica*。「有史以來最嚴重的 Linux 權限提升漏洞正遭到猛烈攻擊 (消息更新)」(Most serious" Linux privilege-escalation bug ever is under active exploit [updated])。上次存取時間 2019 年 1 月 29 日：http://arstechnica.com/security/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/.

77. Robert Abel。(2018 年 11 月 19 日)。*SC Magazine*。「DirtyCOW 再度現身針對 Drupal 網站伺服器的後門攻擊」(DirtyCOW is back in backdoor attack targeting Drupal Web Servers)。上次存取時間 2019 年 1 月 29 日：https://www.scmagazine.com/home/security-news/dirtycow-is-back-in-backdoor-attack-targeting-drupal-web-servers/.

78. Zach Whittaker。(2017 年 14 月 4 日)。*ZDNet*。「美國國家安全局 (NSA) 的 Windows 駭客工具遭到外流」(NSA's arsenal of Windows hacking tools has leaked)。上次存取時間 2019 年 1 月 29 日： https://www.zdnet.com/article/shadow-brokers-latest-file-drop-shows-nsa-targeted-windows-pcs-banks/.

79. Charlie Osborne。(2018 年 9 月 17 日)。*ZDNet*。「為何『已經修正』的 Windows EternalBlue 漏洞依然不死」(Why the 'fixed' Windows EternalBlue exploit won't die)。上次存取時間 2019 年 1 月 29 日：https://www.zdnet.com/article/why-the-fixed-windows-eternalblue-exploit-wont-die/.

80. Zero Day Initiative。(2018 年)。*Zero Day Initiative*。「已發布的資安公告」(Published Advisories)。上次存取時間 2019 年 1 月 29 日：https://www. zerodayinitiative.com/advisories/published/2018/.

81. Zero Day Initiative。(2019 年 1 月 17 日)。*Zero Day Initiative*。「ZDI 漏洞懸賞計畫 2018 年回顧」(The ZDI 2018 Retrospective)。上次存取時間 2019 年 1 月 29 日： https://www.thezdi.com/blog/2019/1/17/the-zdi-2018-retrospective.

82. Garrett Graff。(2018 年 9 月 18 日)。*Wired*。「Mirai 殭屍網路設計者現在正與 FBI 共同打擊犯罪」(The Mirai Botnet Architects are Now Fighting Crime with the FBI)。上次存取時間 2019 年 1 月 29 日： https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing/.

83. Catalin Cimpanu。(2018 年 10 月 28 日)。*ZDNet*。「Satori 殭屍網路作者違反開庭前假釋規定再度入獄」(Satori botnet author in jail again after breaking pretrial release conditions)。上次存取時間 2019 年 1 月 29 日：https://www.zdnet.com/article/satori-botnet-author-in-jail-again-after-breaking-pretrial-release-conditions/.

84. 趨勢科技 IoT 信譽評等服務團隊。(2018 年 4 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「偵測到疑似 Mirai 病毒掃瞄網路的活動來自中國並鎖定巴西境內目標」(Mirai-like Scanning Activity Detected From China, With Targets in Brazil)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro. com/trendlabs-security-intelligence/mirai-like-scanning-activity-detected-from-china-targets-in-brazil/.

85. 趨勢科技。(2018 年 5 月 24 日)。趨勢科技資訊安全新聞。「重開您的路由器：VPNFilter 感染了全球 50 多萬台路由器」(Reboot Your Routers: VPNFilter Infected Over 500,000 Routers Worldwide)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/reboot-your-routers-vpnfilter-infected-over-500-000-routers-worldwide.

86. 趨勢科技。(2018 年 8 月 28 日)。*趨勢科技資訊安全新聞*。「看不見的威脅，即將引爆的損失」(Unseen Threats, Imminent Losses)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unseen-threats-imminent-losses.

87. Joseph C. Chen。(2018 年 12 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新的漏洞攻擊套件 Novidade 正在攻擊家用與 SOHO 族路由器」(New Exploit Kit 'Novidade' Found Targeting Home and SOHO Routers)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/.

88. 趨勢科技。(2018 年 8 月 3 日)。*趨勢科技資訊安全新聞*。「超過 20 萬台 MikroTik 遭駭客入侵用來挖礦」(Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign.

89. Joseph C. Chen。(2018 年 12 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新的漏洞攻擊套件 Novidade 正在攻擊家用與 SOHO 族路由器」(New Exploit Kit 'Novidade' Found Targeting Home and SOHO Routers)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/.

90. Foo Yun Chee。(2018 年 10 月 10 日)。*Reuters*。「獨家：歐盟隱私權主管預料新法規將於年底祭出第一波違規罰鍰」(Exclusive: EU privacy chief expects first round of fines under new law by year-end)。上次存取時間 2019 年 1 月 29 日：https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY.

91. Chris Foxx。(2018 年 5 月 25 日)。*BBC News*。「Google 與 Facebook 被指控違反 GDPR 規定」(Google and Facebook accused of breaking GDPR laws)。上次存取時間 2019 年 1 月 29 日：https://www.bbc.com/news/technology-44252327.

92. European Data Protection Board。(2018 年 9 月 12 日)。*European Data Protection Board*。「奧地利第一張罰單：監視攝影機涵蓋範圍 — 摘要」(First Austrian Fine: CCTV Coverage – Summary)。上次存取時間 2019 年 1 月 29 日： https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_en.

93. Ionut Ilascu。(2018 年 11 月 23 日)。*Bleeping Computer*。「德國第一張 GDPR 罰單針對調情聊天平台開罰 2 萬歐元」(First GDPR Sanction in Germany Fines Flirty Chat Platform EUR 20,000)。上次存取時間 2019 年 1 月 29 日：https://www.bleepingcomputer.com/news/security/first-gdpr-sanction-in-germany-fines-flirty-chat-platform-eur-20-000/.

94. HIPAA Journal。(2018 年 12 月 7 日)。*HIPAA*。「第一張針對醫院的 GDPR 罰單：葡萄牙某醫院需支付 40 萬歐元罰款」(First Hospital GDPR Violation Penalty Issued: Portuguese Hospital to Pay €400,000 GDPR Fine)。上次存取時間 2019 年 1 月 29 日：https://www.hipaajournal.com/first-hospital-gdpr-violation-penalty-issued-portuguese-hospital-to-pay-e400000-gdpr-fine/.

95. 趨勢科技。(2018 年 5 月 4 日)。*趨勢科技資訊安全新聞*。「澳洲『應通報之資料外洩』規範：為 GDPR 資料外洩通報暖身」(Australia's Notifiable Data Breaches Scheme: Prelude to GDPR's Data Breach Notification)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/online-privacy/australia-s-notifiable-data-breaches-scheme-prelude-to-gdpr-s-data-breach-notification.

96. 趨勢科技。(2018 年 5 月 9 日)。*趨勢科技資訊安全新聞*。「加拿大實施自己的資料外洩通報規範」(Canada to Impose Own Data Breach Notification Regulations)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/online-privacy/canada-to-impose-own-data-notification-regulations.

97. 趨勢科技。(2018 年 4 月 2 日)。*趨勢科技資訊安全新聞*。「英國的資料保護法：超越 GDPR 規範」(UK's Data Protection Bill: Beyond GDPR Compliance)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/online-privacy/uk-s-data-protection-bill-beyond-gdpr-compliance.

98. Issie Lapowsky。(2018 年 6 月 28 日)。*Wired*。「加州無異議通過歷史性的隱私權法規」(California Unanimously Passes Historic Privacy Bill)。上次存取時間 2019 年 2 月 13 日： https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

99. 趨勢科技。(2018 年 7 月 24 日)。*趨勢科技資訊安全新聞*。「EU-JEPA 完成簽署，日本資料保護法與 GDPR 雙邊效力互相承認」(EU-JEPA Inked, Reciprocal Adequacy of Japan Data Protection Law and the GDPR Finalized)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/online-privacy/eu-jepa-inked-reciprocal-adequacy-of-japan-data-protection-law-and-the-gdpr-finalized.

100. Stilgherrian。(2018 年 9 月 2 日)。ZDNet。「Five Eyes 聯盟國家政府對加密的態度更加強硬」(Five Eyes governments get even tougher on encryption)。上次存取時間 2019 年 1 月 29 日：https://www.zdnet.com/article/five-eyes-governments-get-even-tougher-on-encryption/.

101. Privacy Rights Clearinghouse。(2018 年)。*Privacy Rights Clearinghouse*。「資料外洩。」(Data Breaches)。上次存取時間 2019 年 1 月 15 日： https://www.privacyrights.org/data-breaches.

102. Daniel Ren。(2018 年 8 月 29 日)。*South China Morning Post*。「上海警方著手調查 1.3 億筆飯店客戶資料外洩並在黑暗網路上以 8 彼特幣代價兜售的事件」(Shanghai police investigate data leak of 130 million hotel clients available on dark web for 8 bitcoin)。上次存取時間 2019 年 1 月 29 日： https://www.scmp.com/business/companies/article/2161800/shanghai-police-investigate-data-leak-130-million-hotel-clients.

103. Raymond Zhong。(2018 年 10 月 25 日)。*The New York Times*。「國泰航空外洩 940 萬旅客資料」(Cathay Pacific Data Breach Exposes 9.4 Million Passengers)。上次存取時間 2019 年 1 月 29 日： https://www.nytimes.com/2018/10/25/business/cathay-pacific-hack.html.

104. 趨勢科技前瞻威脅研究團隊。(2018 年 9 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「中國連鎖飯店遭竊資料與其他不法產品在深層網路論壇上兜售」(Stolen Data from Chinese Hotel Chain and Other Illicit Products Sold in Deep Web Forum)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/we-uncovered-personally-identifiable-information-pii-stolen-from-a-china-based-hotel-chain-being-sold-on-a-deep-web-forum-we-were-monitoring/.

105. 趨勢科技。(2017 年)。*趨勢科技資訊安全新聞*。「機器學習」(Machine Learning)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/definition/machine-learning.

106. Marco Balduzzi。(2018 年 4 月 12 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「採用人類可讀機器學習技術發掘未知威脅」(Uncovering Unknown Threats With Human-Readable Machine Learning)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-unknown-threats-with-human-readable-machine-learning/.

107. Jon Oliver。(2018 年 6 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「機器學習技巧如何協助我們發現 BrowseFox 大量濫用憑證」(How Machine Learning Techniques Helped Us Find Massive Certificate Abuse by BrowseFox)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/how-machine-learning-techniques-helped-us-find-massive-certificate-abuse-by-browsefox/.

108. Joy Nathalie Avelino、Jessica Patricia Balaquit 與 Carmi Anne Loren Mora。(2018 年 11 月 13 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「利用機器學習來叢集 Gh0st RAT 變種的惡意網路流量」(Using Machine Learning to Cluster Malicious Network Flows From Gh0st RAT Variants)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/using-machine-learning-to-cluster-malicious-network-flows-from-gh0st-rat-variants/.

109. 趨勢科技。(2018 年 8 月 9 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「機器學習如何協助偵測惡意詆毀網站的攻擊行動」(How Machine Learning Can Help Identify Web Defacement Campaigns)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/how-machine-learning-can-help-identify-web-defacement-campaigns/.

110. 趨勢科技。(2018 年 4 月 16 日)。*趨勢科技資訊安全新聞*。「利用人工智慧和機器學習來遏止變臉詐騙」(Curbing the BEC Problem Using AI and Machine Learning)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/curbing-the-bec-problem-using-ai-and-machine-learning.

111. Weimin Wu。2018 年 8 月 2 日。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「藉由產生對抗樣本來讓機器學習系統更加完善」(Adversarial Sample Generation: Making Machine Learning Systems Robust for Security)。上次存取時間 2019 年 1 月 29 日：https://blog.trendmicro.com/trendlabs-security-intelligence/adversarial-sample-generation-making-machine-learning-systems-robust-for-security/.

112. 趨勢科技。(2018 年 4 月 5 日)。*趨勢科技資訊安全新聞*。「暴露在外的裝置與供應鏈攻擊：遭忽略的醫療網路風險」(Exposed Devices and Supply Chain Attacks: Overlooked Risks in Healthcare Networks)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/exposed-medical-devices-and-supply-chain-attacks-in-connected-hospitals.

113. 趨勢科技。(2018 年 10 月 20 日)。*趨勢科技資訊安全新聞*。「關鍵基礎架構暴露在外並引來風險：能源與自來水產業」(Critical Infrastructures Exposed and at Risk: Energy and Water Industries)。上次存取時間 2019 年 1 月 29 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.

114. 趨勢科技。(2018 年 12 月 4 日)。*趨勢科技資訊安全新聞*。「MQTT 與 CoAP：IoT 與 IIoT 通訊協定安全與隱私問題」(MQTT and CoAP: Security and Privacy Issues in IoT and IIoT Communication Protocols)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols.

115. 趨勢科技。(2018 年 5 月 16 日)。*趨勢科技資訊安全新聞*。「Scan4You 的興衰」(The Rise and Fall of Scan4You)。上次存取時間 2019 年 1 月 29 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-rise-and-fall-of-scan4you.

116. Mathew J. Schwartz。(2018 年 9 月 25 日)。*Information Security Group*。「Scan4You 經營者被判 14 年徒刑」(Scan4You Operator Gets 14-Year Prison Sentence)。上次存取時間 2019 年 1 月 29 日： https://www.bankinfosecurity.com/scan4you-operator-gets-14-year-prison-sentence-a-11554.

117. 趨勢科技。(2018 年 10 月 29 日)。*趨勢科技資訊安全新聞*。「網路犯罪的演進」(Evolution of Cybercrime)。上次存取時間 2019 年 1 月 29 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolution-of-cybercrime.

TREND MICRO™ RESEARCH
趨勢科技為網路資安解決方案全球領導廠商，致力建立一個安全的資訊交換世界。

Trend Mico Research 背後擁有一群熱情的專家為後盾，他們熱衷發掘最新威脅、分享重要分析情報、全力為遏止網路犯罪而努力。我們的全球團隊每天都協助客戶偵測數以百萬計的威脅，為業界漏洞研究揭露的先驅，經常發表有關最新威脅偵測技巧的創新研究。我們不斷鑽研並預測最新威脅，發表令人深思的研究。

www.trendmicro.tw

TREND MICRO™ | research

©2019 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro、t 字球形標誌與 Trend Micro Smart Protection Network 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。