TREND MICRO | research

持續蔓延的複雜威脅

2019 年度資安總評

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

網路資安產業以及大部分的 IT 環境在 2010 至 2019 這十年當中發生了一項重大轉變，那就是：從企業內移轉至雲端。這樣的轉變起因於各式各樣的技術創新，以及產業為了因應諸多情勢變化而做的轉型。不幸的是，網路資安威脅也跟著不斷演進，從過去單純的偶發性威脅，演變成今日複雜而持續性的威脅。在這十年結束前的最後一年所冒出來的各種知名重大威脅就是最佳證明，它們的受害對象及平台早已開始變得相當多元。

勒索病毒集團專門鎖定政府機關，其攻擊的技術、效率及恐嚇技巧都更上層樓。而知名的辦公室套裝軟體也更受到網路釣魚犯罪集團的青睞，此外，網路間諜行動似乎也有逐漸將目標轉向行動裝置的趨勢。

企業依然經常為了漏洞而拉警報，其中最聲名大噪的漏洞莫過於某個常用軟體通訊協定被發現的「可蠕蟲化」漏洞。除此之外，殭屍網路依然大量利用物聯網 (IoT) 來散播，不論新、舊漏洞都是它們的利用工具。

一起由多個駭客集團針對電子商務網站所發動的聯合攻擊，讓供應鏈攻擊頓時成為眾所矚目的焦點。而針對軟體開發工具及平台的威脅，尤其是像 DevOps 這類協同開發流程所面臨的威脅，也越來越頻繁。諷刺的是，「無檔案」惡意程式反而比「有檔案」惡意程式對相關系統及平台的威脅更大。

企業在雲端、IoT、行動及其他技術和基礎架構方面，正面臨整合及維護上的挑戰。然而企業卻不能因而疏忽了基礎架構的整體防護，尤其當外在環境日益充斥著各種可能衝擊企業營運、聲譽和生存的持續性複雜威脅。

這份年度資安總評報告深入剖析了影響 2019 年威脅情勢的一些最重要問題，讓企業了解該採取什麼樣的最佳實務原則和策略來保護自己的基礎架構，防範當前及未來的新興威脅。

勒索病毒專挑特定對象下手

政府機關飽受針對性勒索病毒危害

2019 年，勒索病毒犯罪集團改懸易轍，開始針對特定的機構進行攻擊，試圖入侵其關鍵資產、系統和服務來獲取龐大利潤[1]。策略的轉變促使他們採取一些新奇的技巧來讓他們迅速在受害者的網路內流竄，盡可能散布更多惡意程式。過去一年當中一項值得注意的駭客技巧就是入侵一些鮮少遭到攻擊的企業資源，例如：網域控制器 (Domain Controller) 和 Active Directory 目錄服務，目的是為了造成企業更嚴重的營運中斷，進而迫使企業乖乖就範，讓他們予取予求[2]。

歹徒對勒索病毒攻擊策略和方向的調整，用在政府機關身上顯然奏效，並且在 2019 年帶動了一波全球熱潮[3]。這股熱潮在美國尤其明顯，因為全球許多針對政府機關的重大勒索病毒攻擊案例都發生在美國。

去年 4 月，美屬維京群島警察局 (U.S. Virgin Islands Police Department) 遭到勒索病毒攻擊，病毒將該局的內部資料與民眾報案記錄加密[4]。去年 8 月，美國加州洛迪市 (Lodi) 政府發生了一起駭客攻擊，造成該市的財政系統與重要電話線路中斷[5]。

美國佛州彭薩科拉市 (Pensacola) 發生了一起駭客攻擊事件，揭露了一種從未見過的勒索病毒攻擊作法。這起攻擊背後的網路犯罪集團「Maze」在入侵了該市的電子郵件與電話服務系統之後，刻意從它們竊取到的 32 GB 資料中釋出 2 GB 來證明他們確實掌握了該市的資料 (而非只有將網路上的電腦加密而已)。Maze 過去即曾經將一些未在期限前支付贖金的受害者資料公開。不過在彭薩科拉市的案例中，歹徒做這動作的用意並非要對該市的官員施壓來逼迫他們支付 1 百萬美元的贖金，而是要駁斥媒體宣稱他們只不過偷了幾個檔案而已[6]。

Maze 駭客集團的攻擊之所以能夠得逞，主要是因為駭客所採用的勒索病毒 (同樣命名為「Maze」) 會自動將所有受害者的檔案複製到該集團的伺服器。這項作法會對受害者造成更大壓力：受害者不僅要應付資料被加密的問題，還要面對資料可能外洩的災難。資安專家早已指出這類手法可能嚴重衝擊企業目前的事件應變措施的執行，IT 部門現在必須與法務和其他部門密切配合來規劃一些額外的復原步驟[7]。

2019 年還有另一個重要的發展趨勢就是，勒索病毒犯罪集團開始彼此結盟。目前至少有兩個專門攻擊美國政府機關的駭客團體以及專門提供所謂「存取服務」(Access as a Service) 的不肖業者，這些業者以出租或銷售各種企業的網路存取權限來營利。這類服務的背後養了一群專門入侵企業網路的駭客，服務的價格從 3,000 至 20,000 美元不等，其中最昂貴的「套餐」包含了受害企業的系統管理主控台、伺服器以及企業 VPN 網路的完整存取權限[8]。

Ryuk 勒索病毒集團在 11 月攻擊了美國路易西安那州科技服務辦公室 (Office of Technology Services)[9]，據說就是利用了這類存取服務。根據報導，該集團租用了像 Trickbot 這類的存取服務惡意程式來非法入侵已感染該惡意程式的機構[10]。另一個與不肖存取服務業者合作的犯罪集團就是 Sodinokibi 勒索病毒 (亦稱 Sodin 或 REvil)。去年 8 月，Sodinokibi 勒索病毒背後的犯罪集團就對美國德州 22 個地方政府機關發動了一波總贖金高達 250 萬美元的聯合攻擊行動。據說勒索病毒是經由某個已遭駭入的第三方軟體散布至這些機關，因為這些市政府機關都使用了該軟體[11]。

2019 年美國至少有 110 個州政府及市政府機關和單位受到勒索病毒襲擊。儘管政府單位爆發了前所未有的大量攻擊[12]，但醫療產業依舊是勒索病毒在美國境內鎖定的首要目標，去年有超過 700 家醫療機構遭到勒索病毒攻擊。除了政府機關之外，美國的教育機構也不遑多讓，有超過 80 個大專院校和學區遭到攻擊[13]。勒索病毒犯罪集團之所以會攻擊醫療、政府和教育產業，是因為相關的損害遠遠超過受害機構本身。這些機構所服務的對象也會受到影響，由於他們提供的服務不可或缺，所以禁不起任何服務中斷或停擺的狀況發生，其影響相當深遠。

保險理賠在勒索病毒獲利當中扮演更重要角色

或許是因為許多政府機關在受害之後都願意支付贖金，所以勒索病毒犯罪集團 2019 年才會更密集地攻擊政府單位。這樣的作法很可能是從他們過去攻擊私人機構的經驗發展而來，因為之前的受害企業也都傾向於支付贖金給歹徒。例如 2017 年就有報導指出美國約有一半的受害企業至少支付了一次贖金[14]。受害的機構為了降低營業中斷所造成的損失，大多寧願與勒索病毒集團妥協並支付贖金，而非直接忽視其要求[15]。

7 月份，美國印第安納州拉波特郡 (LaPorte County) 政府發現其系統遭勒索病毒癱瘓，歹徒要求 25 萬美元的贖金。不過該郡只同意支付 132,000 美元，且其中的 10 萬美元其實是由保險公司的理賠來支付。該郡的郡委員會主席稱這是一個「經濟的抉擇」，用意是要縮短恢復營運的時間。同月，美國麻薩諸塞州新伯福市 (New Bedford) 的電腦遭駭客鎖住並索取 530 萬美金，經過討價還價之後只支付了 40 萬美元。事後，該市市長坦承雖然他一開始很猶豫要不要付款，但假使保險公司的理賠能夠承擔他們所支付的贖金，那他若不考慮循此管道來取得解密金鑰便是失職[16]。

很顯然地，保險公司的理賠能承擔勒索病毒攻擊的大部分贖金，有助於受害者加速復原被加密的檔案和被鎖住的系統。但受害機構越來越仰賴這樣的方式確實令人擔憂，因為這會變相鼓勵網路犯罪集團攻擊更多這類可能有保險理賠的機構[17]。

無怪乎美國聯邦調查局 (FBI) 對於是否該支付贖金，仍維持堅定的否定立場。該局的網路犯罪調查部門主任在 9 月建議受害者應拒絕支付贖金，因為這麼做並不保證能夠救回資料和系統。此外他也引述一個案例指出，受害者原本是希望能支付贖金來取得解密金鑰，沒想到收到的金鑰卻反而讓所有的資料被清得一乾二淨[18]。

新的勒索病毒值得注意，但新的勒索病毒家族數量卻相對減少

2019 年，我們所偵測到的勒索病毒相關威脅 (檔案、電子郵件、網址) 較以往成長。這些小幅增加的偵測數量，或許不僅反映出我們在電子郵件與網址層次主動攔截勒索病毒相關活動的方法有所提升，也反映了在勒索病毒下載之後的資安攔截技術有所改善。

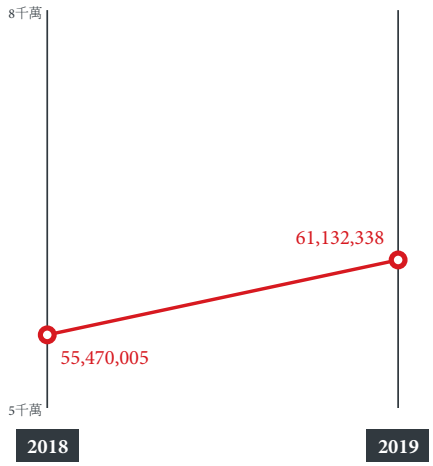

圖 1：勒索病毒相關威脅 (檔案、電子郵件、網址) 小幅增加：勒索病毒相關威脅逐年比較。

資料來源：趨勢科技 Smart Protection Network™ 全球威脅情報網。

新的勒索病毒家族數量跟去年一樣正在持續減少，2019 年新發現的數量還不到 100 個，更不到 2018 年的一半。這可能意味著歹徒或許覺得與其不斷開發新型的勒索病毒，不如挑選特定目標下手反而更有利可圖。

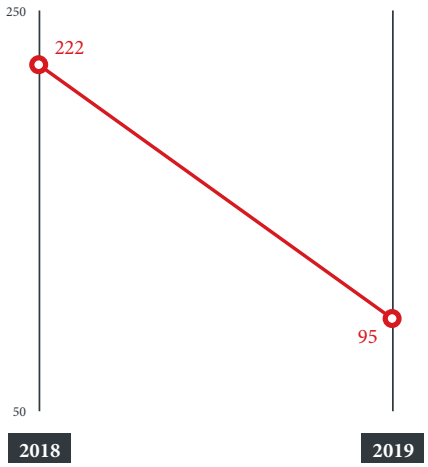

圖 2：新的勒索病毒家族數量減少：新勒索病毒家族數量脅逐年比較。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網與外部資料分析結果。

儘管如此，歹徒依然不斷推出技術高明、令人矚目的新勒索病毒家族。其中一個例子就是 Snatch 勒索病毒，該病毒首次出現於 10 月，曾被用於攻擊美國、加拿大及歐洲多個國家[19]。Snatch 會強制 Windows 電腦重新開機進入安全模式以躲避資安軟體偵測，如此就能暗中加密檔案而不被發現。歹徒開發這項功能的目的正是利用某些資安軟體無法在安全模式中執行的缺陷[20] (該模式原本是用來修復毀損作業系統和除錯)。

勒索病毒家族	入侵途徑與攻擊管道	散布方式	值得注意的特性
Maze[21]	惡意垃圾郵件、假的虛擬加密貨幣網站、漏洞攻擊套件。	已遭駭入的軟體、已遭駭入的系統架構 (如 PowerShell)、其它惡意程式變種。	將檔案外傳，然後再將電腦與網路共用磁碟加密。
Snatch[22]	暴露在外的遠端桌面連接埠。	已遭駭入的遠端桌面服務、網域控制器、已遭駭入的正常工具 (如：PsExec)。	將受感染的電腦重新開機進入安全模式來躲避偵測。
Zeppelin[23]	已遭駭入的遠端桌面控制工具、惡意廣告、已遭駭入的網站。	已遭駭入的系統架構 (如 PowerShell)。	以三重加密編碼來包裝其執行檔。
LockerGoga[24]	外洩的登入憑證、已遭駭入的 Active Directory 目錄服務[25]。	系統管理工具、滲透測試工具以及其他駭客工具，利用合法憑證來避開偵測以入侵系統。	修改受感染系統的使用者帳號密碼，不讓系統被重新開機。
Clop (CryptoMix)[26]	已遭駭入的 Active Directory 目錄服務[27]。	已遭駭入的遠端桌面服務。	使用含有合法數位簽章的執行檔來散布。

表 1：值得注意的新勒索病毒家族運用各種高效率的技術手法：2019 年出現的知名勒索病毒家族手法比較。

另一個值得注意的新勒索病毒家族是 Zeppelin，其最早發現的樣本，編譯日期可追溯至 11 月，美國和歐洲企業都出現感染案例。根據 Zeppelin 的樣本顯示，它可調整的功能很多，而且可當成 .dll 或 .exe 檔案使用或包裝在 PowerShell 載入器中。它除了會加密檔案之外，還能終止電腦上的各種處理程序。其勒索訊息有多個不同版本，從一般通用的勒索訊息，到一些較長且針對特定攻擊目標而調整的訊息[28]。

另一個引人側目的新家族是前面提過的 Maze 勒索病毒，它會自動將所有受害者的檔案複製到該集團的伺服器。該病毒幕後的犯罪集團也叫 Maze，他們會利用冒牌的虛擬加密貨幣網站、惡意垃圾郵件、甚至是漏洞攻擊套件來入侵網路[29]。當 Maze 成功入侵目標網路之後，若受害者拒絕或未能在期限內支付贖金，他們就會將受害者的資料公開到網路上。

訊息威脅依然受到駭客青睞

Office 365 的網路釣魚威脅倍增

根據我們最新的「網路資安風險指標」(Cyber Risk Index) 研究指出，網路釣魚是企業 2019 年最大的威脅，這項研究調查了美國境內上千家企業機構[30]。儘管去年仍有不少網路釣魚詐騙，但我們偵測到的活動數量已較前一年減少。2019 年已攔截的網路釣魚網址存取次數較 2018 年減少 28%，原本可能受到網路釣魚網站危害的使用者數量也因而減少。此外，已攔截的非重複用戶端 IP 存取網路釣魚網址的次數也較前一年減少 38%。這類威脅偵測的數量之所以減少，或許還有一個因素是一些新型態訊息平台 (如 Slack) 的企業用戶日漸成長，而這些平台已取代了電子郵件。

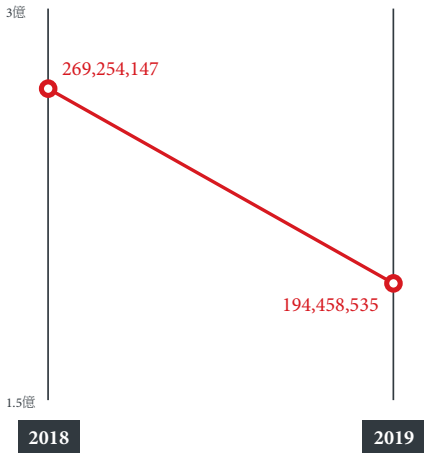

圖 3：已偵測到的網路釣魚網站試圖瀏覽次數持續減少：已攔截的網路釣魚網址存取次數逐年比較 (同一個被攔截的網址若被存取三次仍以三次計)。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

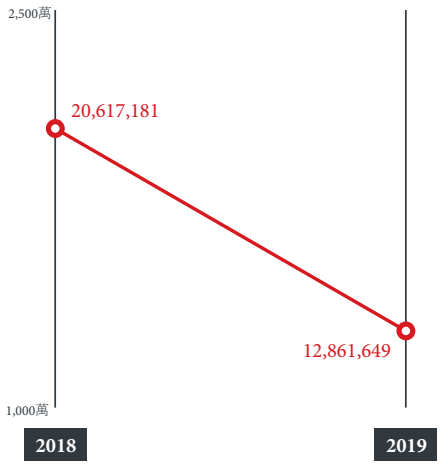

圖 4：原本可能遭網路釣魚網站感染的使用者數量減少：已攔截的非重複用戶端 IP 存取網路釣魚網址次數逐年比較 (同一台電腦若試圖存取同一個網址三次則只算一次)。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

雖然網路釣魚活動的整體數量減少，但假冒 Microsoft Office 365 (尤其是 Outlook) 的網址數量卻持續增加。2019 年已攔截的 Office 365 非重複網路釣魚網址數量較前一年翻了一倍。

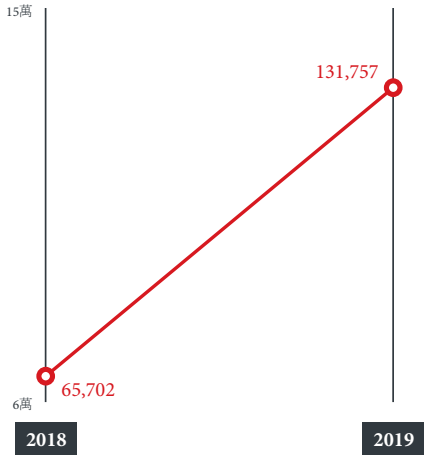

圖 5：假冒 Office 365 (含 Outlook) 的網址數量翻了一倍：已攔截的 Office 365 相關非重複網路釣魚網址逐年比較。

資料來源：趨勢科技網站信譽評等服務。

Office 365 的普及率已使得其每月活躍使用者數量在 10 月份突破 2 億大關[31]，這也是為何它一直成為網路犯罪集團覬覦的主要目標。Office 365 帳號對歹徒之所以有價值還有另一個原因，那就是用來散發垃圾郵件。網路犯罪集團看上的是 Microsoft 的電子郵件平台，包含 Hotmail、Live Mail 及 MSN Mail，因為

Microsoft 電子郵件服務的郵件地址較容易被列在白名單內，對資安軟體來說也比較難以阻擋。此外，網路犯罪集團只要駭入一個 Office 365 帳號，就能對企業機構內部進行網路釣魚攻擊，完全不必再偽造電子郵件地址，這樣的攻擊讓企業更難防範。

網路釣魚詐騙新技巧

網路犯罪集團的技巧一直在不斷精進，其偽造的電子郵件越來越真假難辨，使得電子郵件與手機簡訊的收件人更容易上當。這一點，從 2019 年網路釣魚犯罪集團所使用的一些進階手法就能看出端倪。

我們在 4 月份披露了一起採用一種最新登入憑證釣魚技巧的攻擊行動[32]，歹徒使用的是 SingleFile 這個 Google Chrome 和 Mozilla Firefox 皆支援的網頁延伸功能元件。歹徒利用這個延伸功能元件來產生與原始登入網頁一模一樣的頁面讓使用者輸入登入憑證，進而加以竊取[33]。

此外，我們也觀察到一種可破解雙重認證機制的網路釣魚技巧，它基本上是破解了一次性密碼 (OTP) 的機制。2019 年，這個手法在日本相當流行，主要攻擊目標是網路銀行用戶。歹徒所發送的網路釣魚郵件或簡訊會將使用者帶往冒牌的網路銀行登入頁面。使用者一旦在該頁面上輸入自己的登入憑證，歹徒就將使用者的登入憑證拿到網路銀行真正的登入頁面同步登入使用者的網路帳戶。此時，網路銀行會產生一次性的密碼來確認使用者的身分。當使用者收到一次性密碼之後，會將該密碼輸入假冒的登入畫面，此時歹徒就會得到密碼，並拿去輸入到真正的登入畫面當中，如此就成功駭入使用者的銀行帳戶[34]。

網路犯罪集團也成功利用類似方法來攔截使用者的網頁搜尋，將網路釣魚連結插入搜尋結果當中。2019 年，歹徒利用遭到汙染的 Google 的搜尋結果，讓受害者不小心誤入其網路釣魚網頁。此方法要能得逞，歹徒首先要重導網頁流量，將正牌網站的流量導向他們製作的網站，讓這些網站登上某些關鍵字在 Google 的熱搜排行。接著，歹徒發送含有這類 Google 熱搜網站連結的電子郵件。當受害者點選這類 Google 熱搜排行連結時，就會先連上歹徒架設的網站，然後再前往最後的網路釣魚網站[35]。

另一個在去年值得關注的網路釣魚技巧是利用自訂的「404 Not Found」(網頁找不到) 錯誤訊息頁面來發動攻擊。歹徒並非單純地製作一個網路釣魚網站，然後將受害者導向這個網站，而是先註冊一個網域，然後設定一個自訂的 404 Not Found 錯誤訊息頁面，讓這個頁面假冒成登入畫面。有了這麼一個自訂的 404 Not Found 錯誤訊息頁面，歹徒就能將網路釣魚攻擊全都導向這個網域而沒有數量限制[36]。

變臉詐騙集團跳脫傳統攻擊目標

變臉詐騙，包括：執行長詐騙、假發票詐騙、盜取帳號等等，都是一種仰賴社交工程技巧來促使受害機構員工提供敏感資訊或將款項匯出的一種網路犯罪型態[37]。根據美國聯邦調查局 (FBI) 網際網路犯罪申訴中心 (Internet Crime Complaint Center，簡稱 IC3) 指出，變臉詐騙已成為網路犯罪集團獲利最豐厚的一種犯罪形態，光 2019 年，變臉詐騙集團就在全球詐騙了將近 18 億美元[38]。

根據我們 2019 年所觀察到的趨勢顯示，變臉詐騙集團正開始跳脫傳統的企業受害目標，轉而以宗教[39]、教育[40] 和非營利[41] 等機構為目標。此外，政府機關 (尤其是美國政府機關) 也是歹徒經常攻擊的目標。

6 月份，美國喬治亞州格里芬市 (Griffin) 因變臉詐騙而損失超過 80 萬美元。變臉詐騙集團假冒成該市長期合作的一家外包商，騙過市政府承辦人員，讓兩筆款項改匯到歹徒指定的銀行帳戶。變臉詐騙集團的其中一封信要求變更銀行帳戶資訊，收件人竟不疑有他，直接遵照對方的指示進行變更。歹徒為了提高詐騙郵件的真實性，其提供的電子發票當中還特別包括了一些市政府承辦人員可查證的資訊[42]。

10 月份，美國科羅拉多州伊利鎮 (Erie) 也發生了一起類似的變臉詐騙。歹徒假冒當地某橋樑工程的承包商，誘騙該鎮承辦人員將超過 1 百萬美元的款項匯到一個假冒的帳戶[43]。

去年我們偵測到的變臉詐騙嘗試攻擊大約 13,000 次，僅較前一年成長 5%。雖然成長幅度看似平緩，但卻意味著變臉詐騙對於網路犯罪集團來說仍是高報酬的投資。而事實也的確如此，歹徒只要得逞一次就能大撈一票，就算將事前的研究規劃與其他準備工作都考慮在內，也仍舊利潤豐厚。

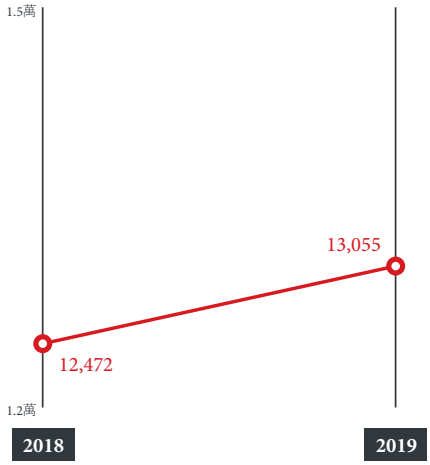

圖 6：變臉詐騙嘗試攻擊數量成長趨於平緩：變臉詐騙嘗試攻擊偵測數量逐年比較。

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。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

我們所偵測到的變臉詐騙嘗試攻擊源自許多國家，其中最多的是美國、澳洲和英國。值得注意的是，這些國家其實也是全球商業中心，很多跨國企業的總部都設在這裡。所以，雖然這些嘗試攻擊數量或許呼應了我們客戶的分布情況，但變臉詐騙攻擊大多集中這些國家也合情合理。

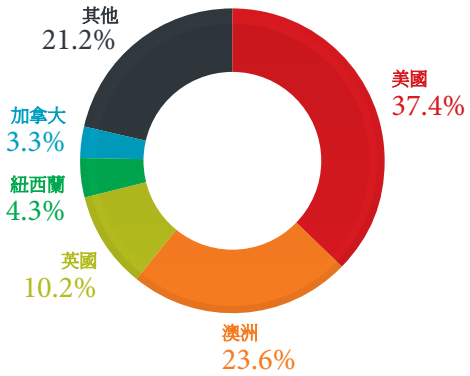

圖 7：絕大多數的變臉詐騙嘗試攻擊都集中在美國：變臉詐騙嘗試攻擊分布國家。

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。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

我們所偵測到的變臉詐騙嘗試攻擊最常鎖定的前五大目標職務當中也包括了教授和會計師。這印證了我們的 2019 年資安預測：除了企業高層主管之外，變臉詐騙也將開始鎖定企業內一些層級較低的員工[44]。這樣的情況在教育產業尤其明顯，該產業在去年即發生過多起變臉詐騙攻擊[45]。

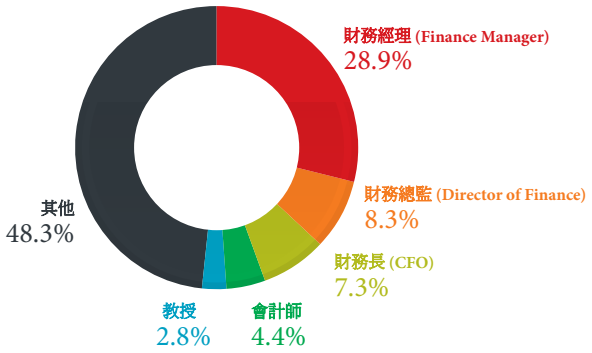

圖 8：除了企業高階主管之外，還有一些其他職務也經常遭到變臉詐騙攻擊：2019 年變臉詐騙嘗試攻擊目標分布情況。

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。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

根據我們的偵測資料，高階主管毫不意外地仍是詐騙集團最喜歡假冒的職務，尤其執行長 (CEO) 更是絕大多數變臉詐騙假冒的對象。

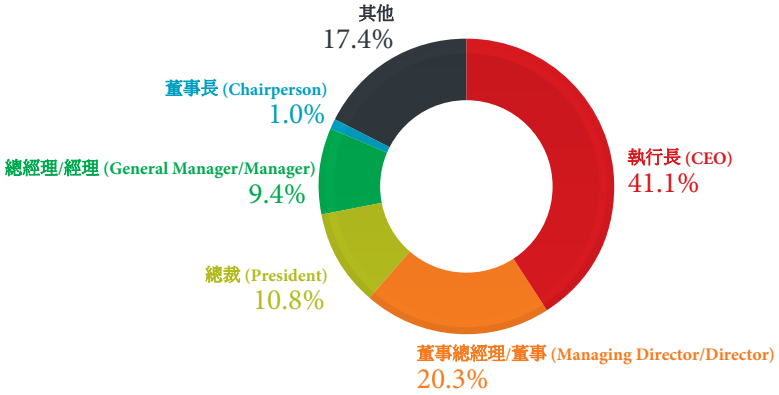

圖 9：執行長 (CEO) 依然是變臉詐騙最常假冒的對象：2019 年變臉詐騙假冒的職務對象分布。

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。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

重大漏洞對新舊系統皆同樣造成威脅

BlueKeep 漏洞讓老舊系統所面臨的風險擴大

當今及未來的新興威脅已複雜到光是一個未修補的漏洞就可能讓整家企業陷入危機。2017 年 WannaCry 勒索病毒爆發所造成的災難仍殷鑑不遠，全球 150 個國家有超過 23 萬台電腦因漏洞未修補而遭到感染，整體財務損失金額高達 40 億美元左右[46]。而那些仍在使用老舊系統的企業機構所面臨的風險甚至更高，因為他們必須面臨軟體廠商已不再修補老舊系統資安漏洞的風險。

Microsoft 在 5 月份針對其遠端桌面協定 (RDP) 中的 BlueKeep 漏洞 (CVE-2019-0708) 發出安全警示，使得一些專門針對老舊系統的威脅再度躍上檯面，尤其是針對 Microsoft 的老舊系統。受到 BlueKeep 漏洞影響的作業系統包括：Windows 7、Windows 2003、Windows Server 2008 R2、Windows Server 2008 及 Windows XP，這些都是許多企業日常營運仍在使用的老舊系統。一旦漏洞攻擊得逞，駭客就能經由 Windows 遠端桌面服務 (Remote Desktop Service) 功能從遠端執行程式碼 (Remote Code Execution，簡稱 RCE) [47] 攻擊。

由於受 BlueKeep 影響的系統可能很多，因而引起了媒體的大量報導，據報約有將近一百萬台系統將受到影響。除此之外，該漏洞特別令人關注的還有它「可蠕蟲化」的特性，這有點類似 WannaCry、Petya 與 Bad Rabbit 等勒索病毒利用 EternalBlue 漏洞攻擊手法來感染系統的方式[48、49]。不過，儘管專家表示 BlueKeep 的問題相當嚴重，但在該漏洞揭露了兩個月之後，仍有 80 萬台以上的系統尚未完成修補[50]。

犯罪集團在 9 月份開始將 BlueKeep 運用在攻擊當中，藉由下載加密編碼的 PowerShell 腳本在系統上植入虛擬加密貨幣挖礦程式並常駐系統內部。不過這些攻擊的威力還遠不及前面所提的幾個勒索病毒家族，因為這些攻擊還不具備 BlueKeep 在媒體曝光時專家們所說的自我散播能力。不過，Microsoft 在 11 月表示不能

小看未來可能出現更具破壞力的 RDP 漏洞攻擊[51]。

早在 2018 年，FBI 的網際網路犯罪申訴中心 (IC3) 就曾警告系統管理員應注意 RDP 漏洞攻擊的潛在問題。該單位在一份公告中指出，RDP 相關的惡意活動從 2016 年中期開始便一直持續增加，並且引述網路犯罪集團在地下市場公開販售遠端桌面存取權限的情況[52]。當然，RDP 漏洞相關的威脅蔚為風潮是當 Microsoft 在 2019 年 5 月針對 BlueKeep 發出資安警示之後，且隨後幾個月又揭露了更多 RDP 相關的漏洞[53]。

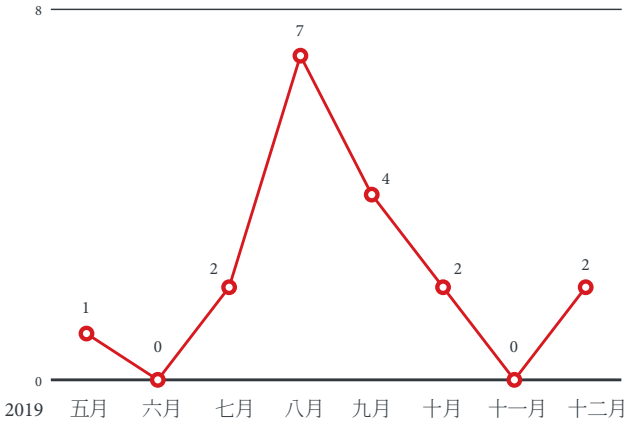

圖 10：緊接著 BlueKeep 之後又有更多 RDP 相關漏洞被揭露：2019 年 5 月至 9 月揭露的 RDP 相關漏洞數量。

資料來源：Microsoft。

遠在辦公室外的員工以及企業委外的 IT 團隊，經常會用到 RDP 來從遠端存取公司內的電腦。RDP 通訊協定讓企業員工能夠很方便地隨時一起工作而不受時空限制，同時也方便 IT 建置各種解決方案，但不可諱言地卻也為歹徒提供了一個方便的攻擊管道[54]。駭客的攻擊一旦得逞，就能透過 RDP 來接管受駭的電腦，進而存取、處理、使用電腦上的檔案。更糟的是，這些電腦將成為歹徒的跳板，進而攻擊更多電腦甚至控制整個網路，歹徒可經由 RDP 連線駭入其他相連的裝置和資源。

正因如此，企業最好不要推延系統漏洞的修補作業，而且最好將過期的老舊系統 (如 Windows 7) 升級至最新系統。2019 年，Windows 7 仍有高達三分之一左右的市場占有率[55]，但 Microsoft 對該系統的支援卻已在 2020 年 1 月終止[56]。

已揭露的高嚴重性漏洞數量翻了一倍以上

2019 年，趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫透過資安公告揭露了 1,035 個漏洞，這些是眾多獨立研究人員以及 ZDI 通報之廠商共同努力的成果[57]。

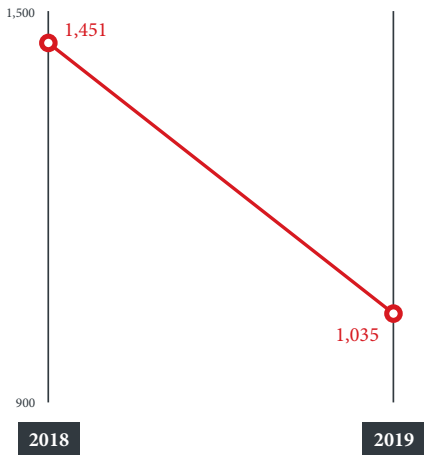

圖 11：資安公告發布數量減少：我們 ZDI 計畫揭露之漏洞數量逐年比較。

資料來源：趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫。

2019 年通報的漏洞數量比前一年幾乎減少三分之一。不過值得注意的是，2019 年所揭露的漏洞，其潛在衝擊反而更大：Common Vulnerability Scoring System (CVSS) 漏洞評分系統所評判為「高」嚴重性的漏洞比前一年增加了 171%，並且占了所有漏洞總數的一半以上。另一方面，嚴重性「重大」的漏洞較 2018 年減少了 64%，且僅占所有通報數量的 9%[58]。

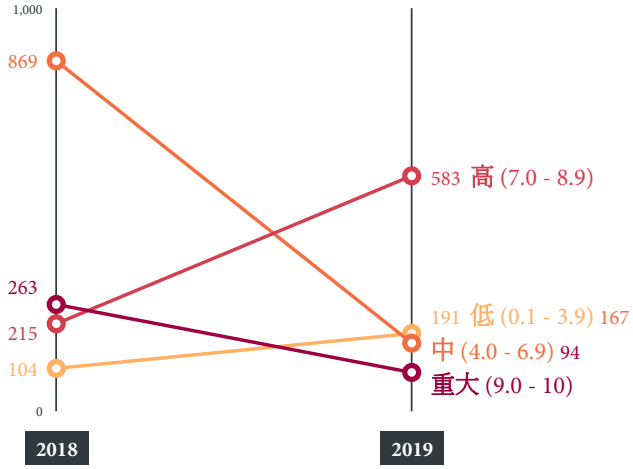

圖 12：高嚴重性漏洞成長兩倍以上：經由我們 ZDI 漏洞懸賞計畫揭露的漏洞，其嚴重性 (CVSS) 分布逐年比較。

資料來源：趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫。

工業控制系統 (ICS) 軟體相關的漏洞數量減少

2019 年，在我們 ZDI 漏洞懸賞計畫所揭露的漏洞當中，工業控制系統 (ICS) 軟體的零時差漏洞與已知漏洞 (N-Day，也就是非零時差漏洞) 的數量分別較去年減少 79% 與 11%。

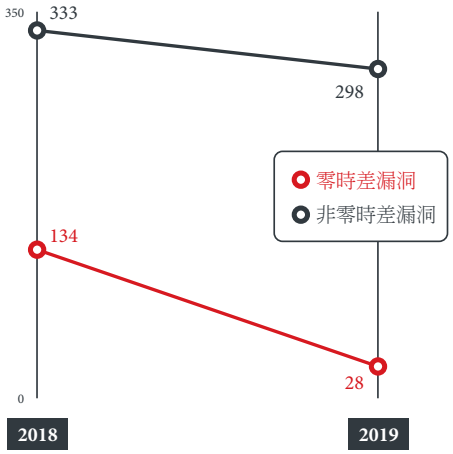

圖 13：工業控制系統 (ICS) 軟體相關零時差漏洞通報數量大幅減少：經由我們 ZDI 漏洞懸賞計畫揭露的 ICS 相關漏洞數量逐年比較。

資料來源：趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫。

這些漏洞絕大多數出現在人機介面 (HMI)，此介面是管理這些關鍵基礎架構並監控其各種操作相關控制系統的中樞。也因此歹徒很可能會藉由攻擊此介面來造成系統中斷。

未來幾年，隨著 ICS 在工業物聯網 (IIoT) 時代日益普及，保護 ICS 安全將成為擁有 ICS 環境的企業一項更迫切的工作[59]。其中一個原因就是 ICS 環境中的監控與資料擷取 (SCADA) 系統市場規模預計將在 2024 年成長至 152 億美元的規模[60]。

數起殭屍網路攻擊利用常見的 IoT 裝置漏洞

全球物聯網 (IoT) 裝置數量預計將於 2025 年成長至 220 億台[61]。這些裝置在家庭、辦公室與都市內的不斷普及，使得人人都有機會用到今日最重要的一項現代化科技。但就像任何應用廣泛的技術一樣，IoT 也已成為網路犯罪集團攻擊的一個平台。

網路犯罪集團之所以看上 IoT 裝置，正是因為這些裝置目前仍漏洞百出。而且由於 IoT 裝置的修補程序既緩慢又麻煩，因此 IoT 裝置的漏洞通常存在的時間會比傳統電腦系統更長。也因為如此而使得歹徒有機可乘， 2019 年有數個殭屍網路不斷重複利用 IoT 一些已知的老舊漏洞。

例如我們在 4 月份披露，知名 Mirai 殭屍網路的一個變種 (趨勢科技命名為：Trojan.Linux.MIRAI.SMMR1) 會利用多種漏洞攻擊手法來駭入各式各樣的路由器和其他 IoT 裝置[62]。一個月後，我們又指出另一個 Mirai 變種 (Backdoor.Linux.MIRAI.VWIPT) 同樣也是利用前者所攻擊的某些漏洞，包括 Huawei HG532 路由器一個可讓駭客執行任意程式碼的漏洞 (CVE-2017- 17215)[63]。

後面這個 Mirai 變種還會攻擊 Netgear R6400 及 R7000 路由器的一個讓駭客從遠端執行任意程式碼的漏洞 (CVE- 2016-6277)。此外，Echobot 殭屍網路的某個變種也是攻擊這項漏洞，該變種具備了 50 多種漏洞攻擊手法，專門攻擊路由器、網路連接儲存裝置 (NAS)、監視保全攝影機、智慧家庭集線器以及其他裝置[64]。

還有兩個專門使用某個常用漏洞攻擊手法的殭屍網路變種是我們分別在 7 月和 12 月披露的 Neko 和 Momentum，它們所用的是採用 Realtek SDK 的路由器所存在的一個指令執行漏洞 (CVE-2014-8361)[65、66]。

網路犯罪集團可利用暴力破解方式，也就是連續使用大量帳號密碼來試圖登入安全性不足的裝置。歹徒經常使用外洩、常見、或出廠預設的使用者名稱和密碼來嘗試暴力破解裝置的登入憑證，因為許多 IoT 使用者經常忘了修改裝置預設的登入憑證。根據我們的監測資料，包括來自第三方路由器的回報，2019 年這類嘗試暴力破解登入憑證的攻擊次數幾乎是 2018 年的三倍。

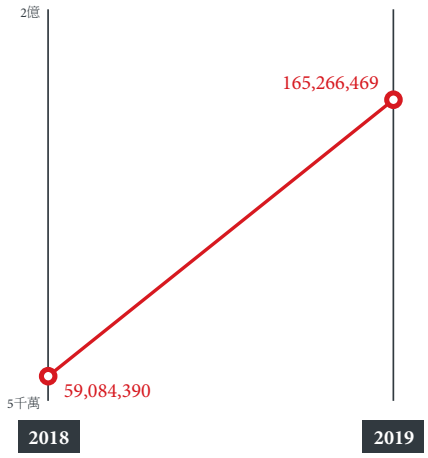

圖 14：暴力破解登入憑證的攻擊次數暴增：涉及暴力破解登入憑證的對內與對外網路事件數量逐年比較。

資料來源：趨勢科技 Smart Home Network 產品。

威脅滲透供應鏈與開發流程漏洞

Magecart 供應鏈攻擊侵襲電子商務網站

所謂的「供應鏈攻擊」是當歹徒想要攻擊某家公司或某項服務時，不直接對其攻擊，而是經由擁有該公司資料或系統存取權限的某個外部合作夥伴或第三方供應商，這類攻擊的數量在過去一年明顯增加。其中最知名的就是 Magecart 聯盟，這由數個駭客集團所組成的一個駭客聯盟，專門攻擊電子商務網站所使用的購物車系統 (如 Magento 或 OpenCart) 來竊取客戶的刷卡資訊。截至 10 月為止，不論是經由供應鏈攻擊或直接攻擊，Magecart 已駭入了 200 萬個網站以上[67]。

在我們 2019 年所觀察到的 Magecart 攻擊行動當中，有兩個行動特別引人注目，其中一個是由 Magecart Group 12 所發動。我們曾在 1 月份發現 Magecart Group 12 已駭入了 277 個電子商務網站，包括：購票、旅遊、機票訂位等網站以及服飾、化妝品、醫療等品牌的網路商店，其手法是經由第三方廣告服務來駭入這些網站。該集團會將盜卡程式碼注入到第三方廣告服務的 JavaScript 程式庫當中，如此一來就能竊取網站使用者所輸入的刷卡資訊[68]。

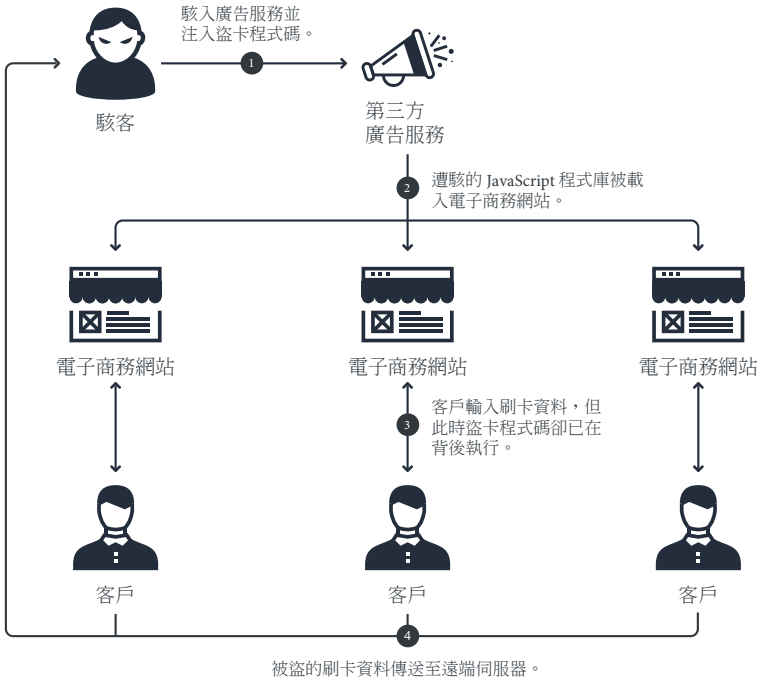

圖 15：Magecart Group 12 藉由駭入第三方廣告服務來攻擊電子商務網站：Magecart Group 12 攻擊過程。

還有另一個值得注意的網路盜卡集團是 FIN6。去年 9 月至 10 月間，該集團攻擊了某知名電子商務平台的 3,126 家網路商店。駭客將惡意程式碼注入電子商務平台提供給商家的某個 JavaScript 程式庫，接著又載入另一個存放在雲端儲存服務的 JavaScript 檔案。被載入的檔案與正常的 JavaScript 程式庫幾乎一模一樣，但卻偷偷暗藏了一段信用卡盜卡程式碼。當客戶造訪已遭感染的網站時 (絕大部分客戶來自美國)，其輸入的信用卡資訊會不知不覺地被傳送至某個資料接收伺服器[69]。

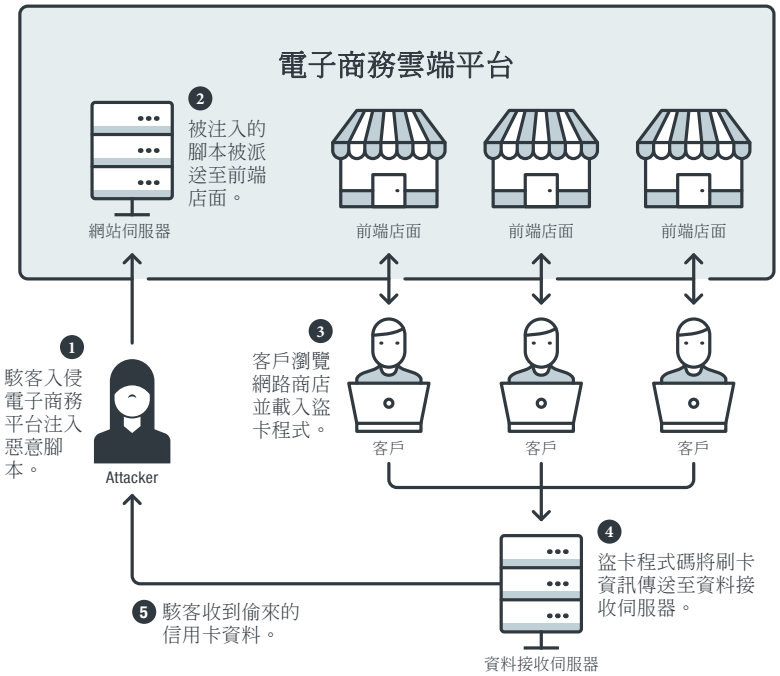

圖 16：FIN6 駭入某知名電子商務網站平台上的商店網站：FIN6 攻擊過程。

供應鏈攻擊充斥電子商務網站，突顯網站經營者必須嚴密監控其所用平台與服務內的資安漏洞，建立更嚴格的認證機制。至於使用者方面，使用者在造訪電子商務網站時應小心留意可疑徵兆，尤其在受害案例持續攀升之際。在日本，電子商務網站盜卡事件頻傳已促使該國政府在 2019 年對使用者發出警告[70]。

軟體開發工具與平台所面臨的威脅升高

DevOps 是一種簡化軟體或應用程式開發週期的方法，其中包括各式各樣的工具與文化內涵。這套方法有助於企業提升軟體開發的品質、安全及規模[71]。但儘管 DevOps 為企業提供了一種更快、更有效率的開發流程，但有時企業卻忽略了資安的層面，使得歹徒利用漏洞攻擊手法與惡意程式來駭入流程當中的元件。舉例來說，企業對外部廠商的資安要求通常不像其內部標準那麼嚴格，因此就會讓駭客有機可乘，利用篡改過的第三方程式碼來駭入企業，例如前面所說的供應鏈攻擊[72]。所以，導入 DevOps 開發流程的企業應該將這點以及其他資安問題列入考量，以避免系統遭到入侵。

要破壞企業的軟體開發流程，駭客可干擾軟體供應鏈上的某個環節，或利用 DevOps 工具和平台的資安漏洞，例如 2019 年所發生的案例。

6 月份，我們在 Docker Engine – Community 這個熱門的開放原始碼版本 DevOps 工具當中發現一個 API 組態設定錯誤，該錯誤能讓駭客入侵容器並執行 Linux 殭屍網路病毒變種「AESDDoS」。執行惡意程式之後，駭客就能接管受害主機，從遠端存取伺服器與硬體資源[73]。同月，今日相當受到歡迎的 Kubernetes 容器協調系統開發人員揭露了一個該系統指令列介面的高嚴重性漏洞 (CVE-2019-11246)。駭客可利用該漏洞來瀏覽檔案目錄，並利用一個惡意容器在受害的工作站上建立或取代檔案[74]。

7 月份，我們在 DevOps 常用的自動化伺服器 Jenkins 當中發現的一個資安漏洞，使得它可能遭到駭客攻擊。經由此漏洞，我們發現原本權限不足的帳號竟然可以取得 Jenkins 的系統管理權限，如此一來駭客就能從遠端在主機上執行程式碼。此漏洞源自於自動化伺服器安全設定中的組態設定不當[75]。此外，我們在 8 月份又披露了 4 個影響 Jenkins 外掛元件的漏洞，可能讓駭客竊取使用者的登入憑證[76]。

在過去一年當中，不安全的 Docker 主機也遭到了各式各樣的攻擊，例如 10 月份發現的虛擬加密貨幣挖礦程式。一些缺乏安全認證措施的主機因遭到攻擊而感染了該惡意程式。此事件導致 2,000 多台 Docker 主機感染某個會暗中利用這些主機來開採門羅幣 (Monero) 的蠕蟲[77]。

不良的軟體開發習慣也可能讓駭客有機會入侵 DevOps 工具和平台，進而侵害企業的實體、虛擬、雲端及容器環境。如同前面兩個案例所示，資安組態設定不當也有可能導致系統遭到入侵。此外，原始程式碼、組譯器程式庫、二進位檔案等等，若未妥善維護並驗證其一致性，也很可能讓駭客有機會感染系統[78]。

駭客利用精密元件提升隱藏能力

無檔案式威脅成為常態

採用無檔案式元件的威脅與傳統惡意程式不同，因為對這些威脅來說，惡意軟體或執行檔並不是它們感染系統的必要條件。這些威脅所使用的反倒是合法的系統管理工具或滲透測試工具，如：PowerShell、Windows Management Instrumentation (WMI)、AutoHotKey 及 PsExec，所以才能暗中活動而不被發現。儘管如此，我們還是有辦法藉由追蹤一些非檔案性指標，並透過一些端點調查及回應技術來偵測無檔案式威脅的相關活動，例如監控事件並分析哪些處理程序或事件會觸發惡意活動[79]。

過去一年，我們攔截了超過 140 萬次無檔案事件。如此龐大的數量也印證了我們過去對 2019 年的資安預測，那就是駭客越來越能「就地取材」，利用系統內建的一些應用程式和工具來發動攻擊，進而躲避偵測[80]。

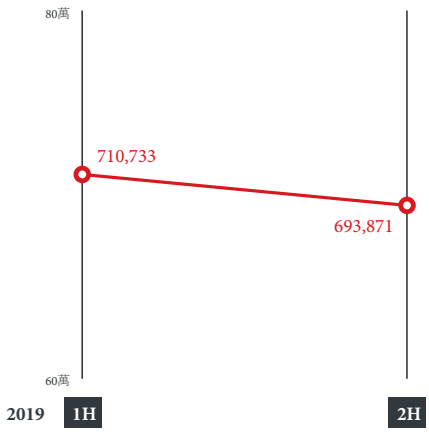

圖 17：無檔案事件攔截數量超過 140 萬：2019 年攔截的無檔案事件數量半年期比較。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

這一點亦不令人意外，尤其目前已經有許多惡意程式攻擊行動開始在攻擊當中使用無檔案式元件。這些攻擊將無檔案式元件應用在躲避方法、常駐機制，以及下載和執行惡意檔案，還有攻擊程序當中的其他階段。

去年 3 月，某攻擊行動鎖定了三家巴西銀行，駭入了使用者的銀行帳號，並從使用者造訪的網站竊取其個人身分資訊以及電腦上記住的登入憑證，這些資訊可讓歹徒拿來進一步利用或販賣。該行動使用了 PowerShell 來下載一個銀行木馬程式[81]。

8 月份，我們發現了 GhostMiner 這個無檔案式數位加密貨幣挖礦惡意程式變種，它透過 WMI 物件來達成無檔案式常駐、下載檔案，並躲避資安產品。該變種原本專門攻擊 Microsoft SQL Server、phpMyAdmin 和 Oracle WebLogic Server 的多項漏洞來駭入尚未修補的伺服器[82]。

隔月，Emotet 在短暫的沉潛之後又再度現身，這次它利用大量的垃圾郵件來攻擊英文、德文、義大利文和波蘭文的使用者。這些電子郵件隨附一個內含巨集的 Microsoft Word 文件，如果使用者啟用了巨集，就會執行一個 PowerShell 腳本，該腳本會從已遭駭入的網站下載 Emotet 惡意程式[83]。同一個月，我們披露了 Purple Fox 這個檔案下載惡意程式，它使用 PowerShell 來執行無檔案式感染動作 (這應該是它首次使用這項工具) [84]。

另一個值得注意的無檔案式攻擊行動是 KovCoreG。我們在 10 月份觀察到該行動會執行某個 PowerShell 腳本來停用 Windows Defender 和 Windows Update 處理程序。除此之外，KovCoreG 也會使用 PowerShell 來執行無檔案惡意程式 Novter，後者會執行一些反制軟體除錯與分析工具的檢查，以及其他的後門指令[85]。

針對性攻擊更常採用複雜的攻擊手法

在針對性攻擊當中，駭客集團會非常積極地試圖暗中入侵並潛藏在目標機構的資訊基礎架構當中而不被發現。歹徒會利用各種攻擊手法、技巧與程序來讓他們在滲透目標網路之後還能繼續暗中行動。

2019 年，我們觀察到兩個駭客集團使用複雜的攻擊手法、技巧與程序來從事網路間諜行動，那就是「Tick」和「APT33」。Tick 駭客集團在一項名為「Operation Endtrade」的攻擊行動當中鎖定一些涉及高度機密的產業發動攻擊，尤其是國防、化學、衛星等產業，受攻擊的機構，總部大多設在日本，並且在中國設有分支機構。根據我們的分析顯示，該群組仍使用已遭駭入的合法電子郵件帳號、一些先前曾經用過的惡意程式以及加密編碼工具。不過，Tick 的攻擊配備似乎有所升級，包括一些新的惡意程式家族，能夠

偵測並終止系統上安裝的防毒軟體、檢查作業系統所用的語言是否為 Tick 集團鎖定的目標、將自身提升至系統管理員權限以順利進行攻擊，以及蒐集專屬資訊與機密資料[86、87]。

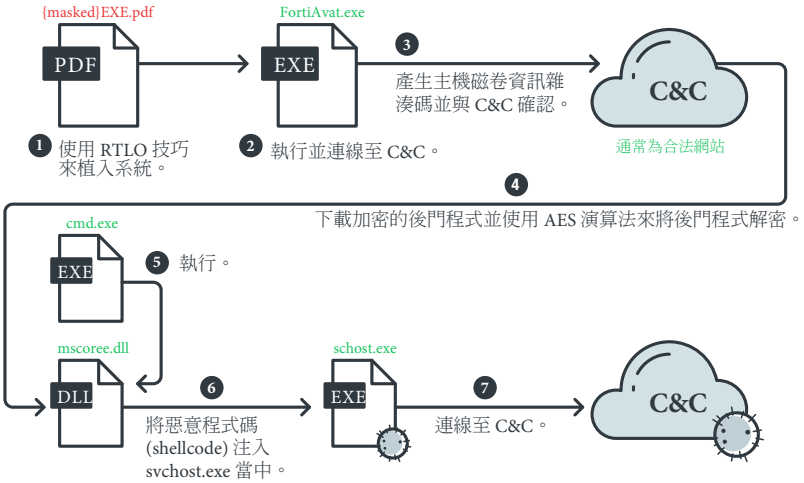

圖 18：Tick 採用可停用防毒產品的惡意程式變種：ABK 和 BBK 攻擊程序 (Tick 所使用的檔案下載器)。

註：完整的 TICK 攻擊程序 (對應 MITRE ATT&CK™ 架構) 請參閱本文「威脅情勢回顧」一節。

在 APT33 部分，我們觀察到該集團有十幾個活躍的幕後操縱 (C&C) 伺服器且攻擊目標範圍相當窄。APT33 架設了層層的掩護來保護其 C&C 伺服器，透過惡意程式來攻擊亞洲、中東及美國的機構。根據我們的分析指出，APT33 花費了很大的功夫來隱藏行蹤。其 C&C 網域通常位於雲端代理器 (proxy)，這些代理器會將來自受感染殭屍裝置的網址請求轉送至後端共用的網站伺服器，而這些伺服器上可能代管了數千個合法的網域。後端伺服器再將殭屍電腦送來的資料傳回給資料彙整與殭屍操控伺服器，這些伺服器會使用專用的 IP 位址。APT33 駭客集團會經由私人 VPN 網路連線至資料彙整伺服器，且其 VPN 出口節點 (exit node) 會經常變換。此外，APT33 駭客集團也透過這些 VPN 連線來對殭屍電腦下達指令並蒐集資料[88]。

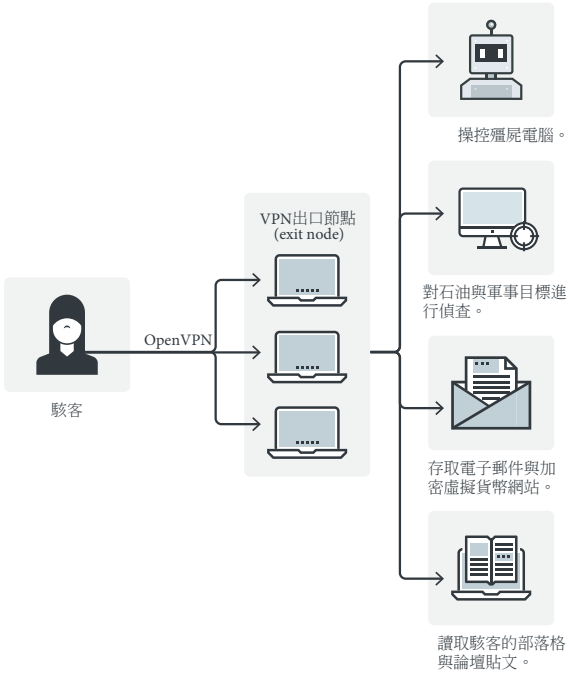

圖 19：APT33 使用一個出口節點經常變動的 VPN。

註：完整的 APT33 攻擊程序 (對應 MITRE ATT&CK 架構) 請參閱本文「威脅情勢回顧」一節。

犯罪集團持續兵分多路朝行動裝置和其他平台邁進

Android 惡意程式染指官方應用程式商店

2019 年，行動裝置 (尤其是採用 Android 作業系統的行動裝置) 仍是歹徒不變的攻擊目標。儘管我們所攔截的 Android 惡意應用程式數量從上半年至下半年持續減少，但 2019 一整年的總數還是相當可觀，將近 6 千萬。這進一步突顯出網路犯罪集團仍相當仰賴攻擊行動裝置來竊取登入憑證、發送惡意廣告、從事網路間諜活動等等。

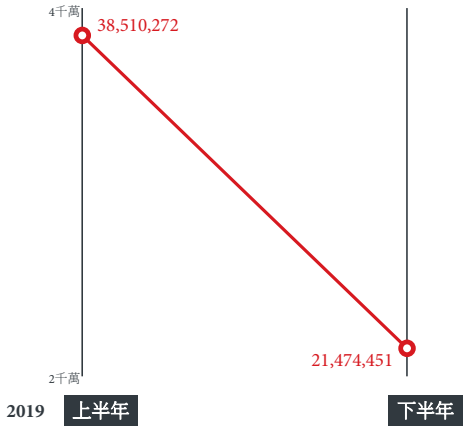

圖 20：已攔截的 Android 惡意應用程式總數將近 6 千萬：2019 年攔截的 Android 惡意應用程式數量半年期比較。

資料來源：趨勢科技行動應用程式信譽評等服務 (MARS)。

2019 年發生的最大一起行動裝置威脅事件包含多個惡意的 Android 應用程式，總共被使用者下載了一百萬次。這些應用程式假冒成美肌美顏軟體在 Google Play 官方應用程式商店上架，它們會連上遠端廣告伺服

器，進而從事網路犯罪。在我們分析到的惡意樣本中，我們發現這些應用程式很難看出有任何可疑之處。其中一個樣本在啟動之後會產生一個捷徑，但卻不會讓自己的圖示出現在應用程式清單上。此一技巧讓使用者無法解除安裝該應用程式，因為使用者根本找不到該程式，更不用說要將它刪除[89]。

另一個我們在 2019 年觀察到的有趣現象是行動網路間諜攻擊行動的數量持續攀升，這意味著駭客集團也開始將攻擊目標轉向行動裝置。過去一年當中，我們發現了 30 起類似這樣的攻擊行動，包括 Poison Carp[90]、Rana[91] 以及最知名的 MuddyWater，這個惡名昭彰的網路間諜集團向來都專門攻擊中東與亞洲國家。尤其，我們在分析 MuddyWater 攻擊活動時，發現它跟四個假冒成正常應用程式的 Android 惡意程式變種有所關連[92]，這些程式都具備竊取資訊的能力[93]。

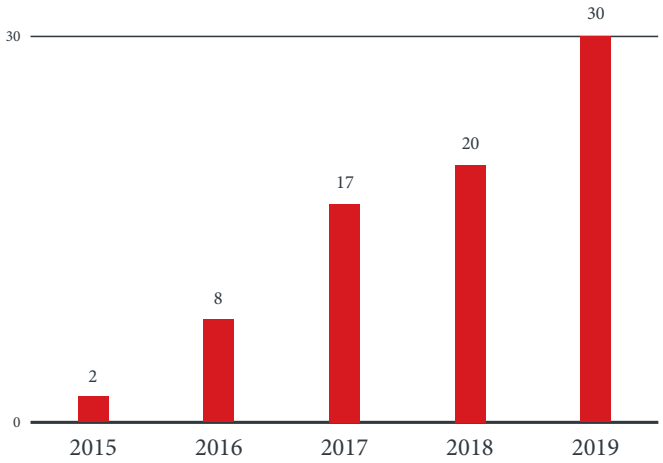

圖 21：行動裝置網路間諜行動在近五年來持續不斷增加：2015 至 2019 年行動裝置網路間諜行動數量。

資料來源：趨勢科技行動應用程式信譽評等服務 (MARS) 與外部資料分析結果。

威脅入侵 iOS 和 macOS

長久以來，Apple 的作業系統 (智慧型手機與平板的 iOS 以及桌上型與筆記型電腦的 macOS) 在安全性方面一直有很高的評價，且該公司亦不斷努力推出新的系統防護機制[94]、[95]。不過，不肖之徒仍非常積極地試圖突破這些裝置的安全機制，並在 2019 年開發出各式各樣的相關威脅。

我們發現以開發 Android 惡意程式為主的 XLoader 網路犯罪集團在去年發展出一種針對 iPhone 和 iPad 的攻擊，試圖誘騙使用者安裝一個惡意的 iOS 組態設定檔來竊取裝置上的資料[96]。同時，我們也發現歹徒運用一種使用 iOS 網址的詐騙手法會侵犯使用者的隱私、讓使用者遭遇帳單詐騙，以及不斷看到彈出式廣告[97]。

另一個我們發現的 iOS 重大威脅是有數百個博弈應用程式假扮成看似正派的應用程式來通過 Apple App Store 的審查。值得玩味的是，這些應用程式當中有些還登上了 App Store 的 100 大排行榜，其中有的還累積了 10 萬多筆評價[98]。

在 macOS 方面，我們發現的主要威脅是漏洞和惡意程式變種，例如，macOS Mojave 10.14.3 作業系統繪圖驅動程式的一個漏洞 (CVE-2019-8519) 可能因緩衝區溢位 (buffer overflow) 或記憶體區段錯誤 (segmentation fault) 而使得駭客能夠存取受保護的資訊[99]。另一個漏洞 (CVE-2019-8635) 則可能讓駭客在 macOS 裝置上將自己提升至系統管理員 (root) 權限來執行惡意程式碼[100]。

除此之外我們也發現一個 macOS 惡意程式變種會假扮成交易軟體來誘騙受害者並竊取其個人資料[101]。我們還發現一個應該是「Lazarus」網路犯罪集團所開發的 macOS 後門程式，利用含有 Microsoft Excel 巨集的試算表專門攻擊韓文使用者。此後門程式除了一般惡意功能之外，還可上傳和下載檔案[102]。

2019 年還有一個值得注意的 macOS 惡意程式是「Shlayer」，它採用圖像隱碼術 (Steganography，一種將程式碼暗藏在非加密文字或資料當中的手法) 來將一段用來下載越權廣告程式的腳本隱藏在一張圖片當中[103]。此外我們也曾發現 Shlayer 還會隨著另一個 macOS 惡意程式變種「Tarmac」植入系統當中，歹徒製作了假的軟體更新來誘騙使用者下載[104]。

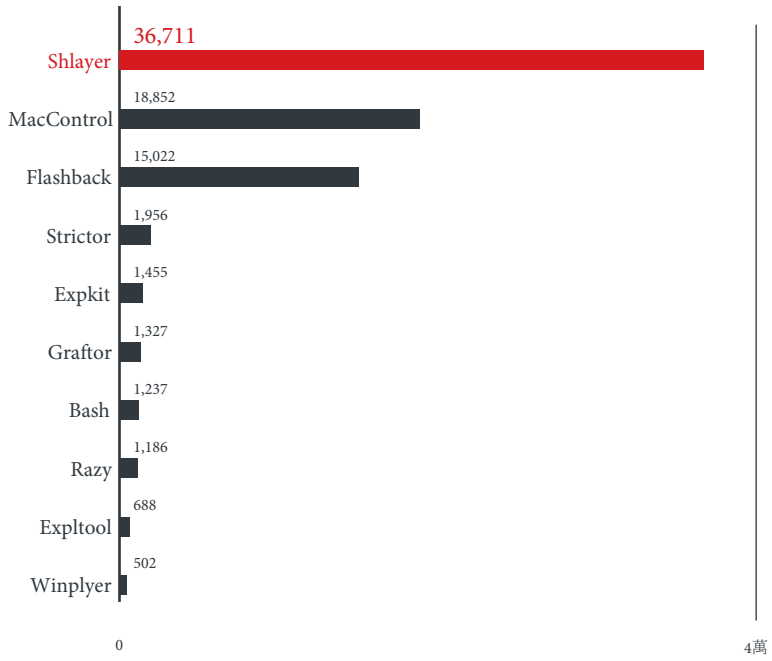

圖 22：Shlayer 是偵測數量最多的 macOS 惡意程式家族：2019 年偵測到的 macOS 惡意程式家族排行榜。

資料來源：趨勢科技 macOS 樣本資料庫。

根據我們內部蒐集和分析到的 macOS 樣本資料庫，Shlayer 是 2019 年 macOS 惡意程式家族排行榜的第一名，有超過 36,000 個非重複樣本，其中將近 30,000 個出現在美國。

多層式防護依然是最有效的威脅防禦

複雜而持續性的威脅已蔓延整個網路資安威脅版圖，令人吃驚的是它們整體上已橫跨各種不同產業、平台和裝置，而且還能充分運用新、舊系統的資安漏洞。正因如此，企業機構必須重新檢討並強化自身的網路資安防禦。

企業要防範資安威脅造成營運中斷、商譽損失以及財物損失的最佳方法就是採用一套多層式資安策略。結合各種有效、創新、方便又具成本效益的資安技術，能讓企業滿足各種不同的需求。企業應挑選能同時在閘道、網路、伺服器及端點層次偵測惡意活動的解決方案，結合機器學習、行為監控、沙盒模擬分析、入侵防護等多樣化偵測技術。除此之外，若再配合一套以偵測及回應攻擊為核心的綜合解決方案也能提供莫大幫助[105]。

企業應雙管齊下：一方面採用多層式資安防護，一方面落實業界最佳實務原則。例如，要防範勒索病毒攻擊，企業可制定一套有效的備份策略，實施網路分割來防止萬一駭客真的入侵時能避免他們在網路內四處遊走，同時監控及稽核網路流量來發掘任何異常或可疑行為。

要降低網路釣魚和變臉詐騙等這類訊息威脅，企業應定期實施網路資安意識改善計畫。反覆教育員工養成良好的資安習慣，例如：留意電子郵件是否有語法錯誤或錯字、仔細查看寄件人的名稱、遇到要求提供敏感資訊或要求匯款的電子郵件務必進一步查證，如此就能大幅降低訊息威脅的風險。

不僅如此，企業不只應該隨時注意自己的資訊平台與架構是否出現漏洞和組態設定錯誤，還要防範第三方供應商出現相關的問題。定期進行系統的全面檢查，發掘任何可能存在的缺失和錯誤，都能有助於企業防範利用外部合作夥伴為跳板的攻擊。同時，企業也應確保自己的系統和應用程式隨時更新到最新版本，預先遏止所有可能利用系統重大漏洞的威脅。若要進一步改善系統修補管理作業，企業可考慮採用虛擬修補技術來防止老舊作業系統的漏洞遭到攻擊，因為這些系統早已不再提供安全更新。

除此之外，企業還應定期檢查擁有高等權限的軟體，尤其是程式開發工具。為避免這些工具遭到濫用，系統管理員應經常更換自己的登入密碼並提高密碼強度。採用多重認證、實施最低授權原則，不需開放的權限就不要開放，這些都是防範駭客利用系統工具攻擊企業網路的不錯方法。而使用者也應透過這樣的方法來保護自己的電腦、智慧型手機、平板以及其他連網裝置。

威脅情勢回顧

2019 年，趨勢科技 Smart Protection Network™ 全球威脅情報網偵測並攔截了 520 億次以上的威脅，有效防止企業和使用者遭到各種電子郵件、檔案和網址威脅。

52,265,509,014

2019 年整體威脅攔截總數

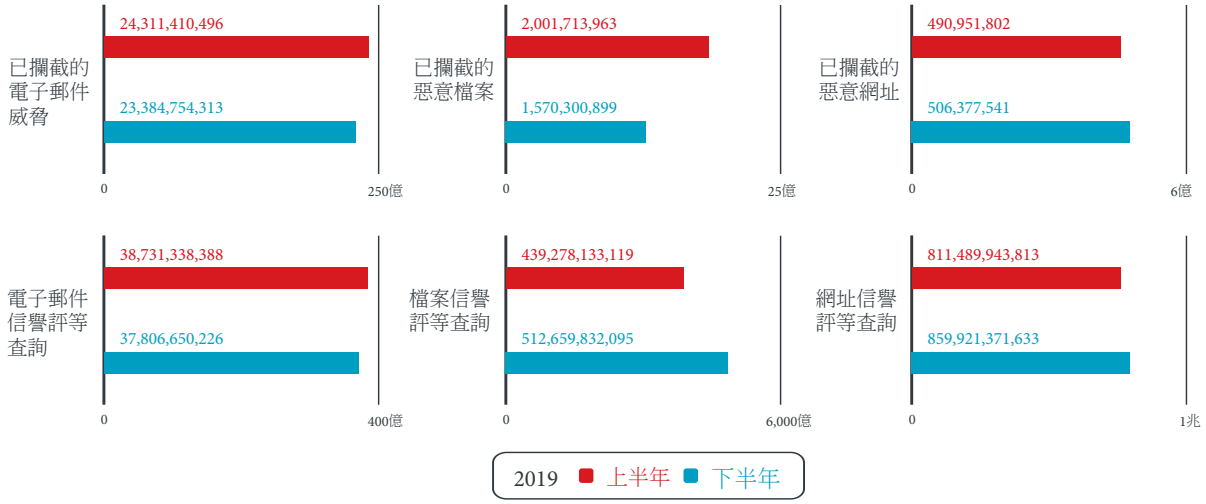

圖 23：已攔截的惡意網址稍微增加，已攔截的電子郵件威脅和惡意檔案則減少：2019 年已攔截的電子郵件、檔案與網址威脅數量半年期比較。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

儘管過去一年所偵測到的新勒索病毒家族數量相對較低，但其中卻有數個家族推出了更加精進或出現全新行為的勒索病毒。

ANATOVA	BIGBORB	BITLOCKED	BLACKROUTER	BLUEAGLE
BONE	BROWEC	BURAN CORTEX	BXCODE	CHATER
CLOP	CONTI	CRYPROTO	COSAKOS	CRAZYCRYPT
CRAZYZIP	CRYPONY	DEATHRANSOM	CRYPSPORT	CRYPTGO
CRYTEM	CYMRANSOM	EKANS FCRYPT	DEMOCRY	DMR
DOGOJOKER	ECHORAIX	GOLDENAXE	ENTSCRYPT	ERIS
EXPBOOT	FAKEWCRY	HOLA	FREEZING	FTCODE
GOJDUE	GOLANG		GOOD IMSORRY	GORGON
HERMES	HILDA			IRANSOM

JAMPER	JCRY	JUWON	LILOCKED	LOCKERGOGA
LOOCIPHER*	LOOCIPHER*	MAILTO	MAOLOA	MAZE
MEDUSALOCKER	MESPINOZA	MONGOLOCK	MONSTERRAT	MZREVENGE
NEMTY	PAPJ	PHOBOS	PONY	PURELOCKER
RABBIT	RANNOH	RAPID	REDKEEPER	ROBINHOOD
SATANA	SAVEQUEEN	SEEDLOCKER	SENJO	SEON
SHADOWCRYPTOR	SNATCH	SODINOKIBI*	SODINOKIBI*	SPARTCRYPT
SYRK	TELUDEPAS	TFLOWER	TIONE	TREE YATRON
TUNCA YFISNIFFER	VEGA	VIGRA	XCRY ZEPPELIN	ZILLA
	ZARLOCK	ZEOTICUS		

表 2：本期發現 95 個新的勒索病毒家族：2019 年偵測到的新勒索病毒家族。

**註：某個新的勒索病毒家族使用了與既有家族相同的名稱。*

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網與外部資料分析結果。

根據我們的資料，PDF 是垃圾郵件最常用的附件檔案類型，緊跟在後的是 XLS。值得注意的是，2018 年 PDF 反而是緊跟在 XLS 後面。

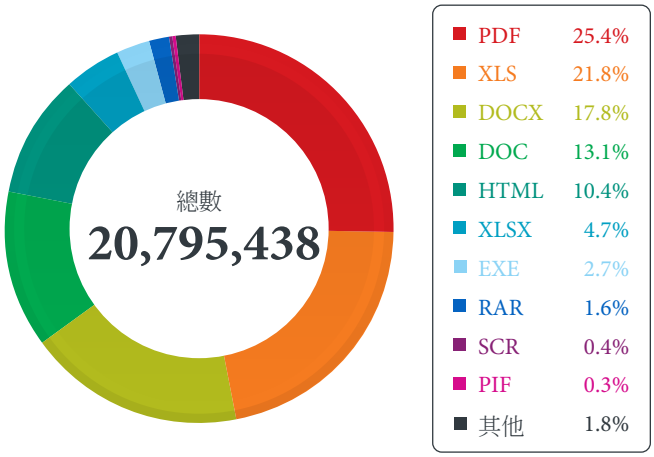

圖 24：在偵測到的電子郵件威脅當中，有四分之一的附件檔案是 PDF：2019 年偵測到的垃圾郵件附件檔案類型分布。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

在我們的 2019 年資安預測當中有一項預測是數位勒索的數量將會增加，尤其是性愛勒索[106]。而我們 2019 年也確實偵測到了大量的性愛勒索相關垃圾郵件，數量高達 1,400 多萬封，證實了這項預言。

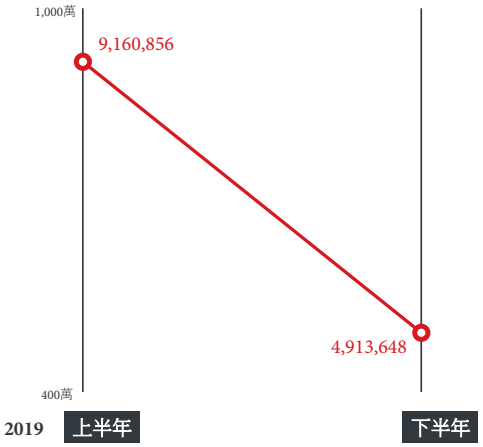

圖 25：性愛勒索相關垃圾郵件的數量從上半年至下半年呈現減少的走勢，但總數加起來卻仍超過 1,400 萬封：2019 年性愛勒索相關垃圾郵件偵測數量半年期比較。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

我們發現漏洞攻擊套件活動在 2019 年成長了 52%，顯示歹徒仍經常使用漏洞攻擊套件。

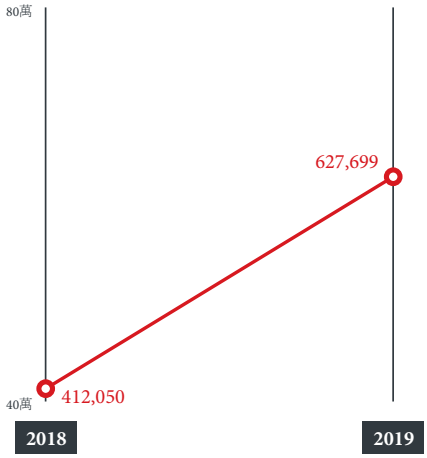

圖 26：漏洞攻擊套件活動增加：已攔截的漏洞攻擊套件散布網址存取次數逐年比較。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

GrandSoft 是 2019 年偵測數量最高的漏洞攻擊套件，超過 28 萬，幾乎占了整體總數的一半。甚至已超越 Rig，後者是前一年排行第一的漏洞攻擊套件。

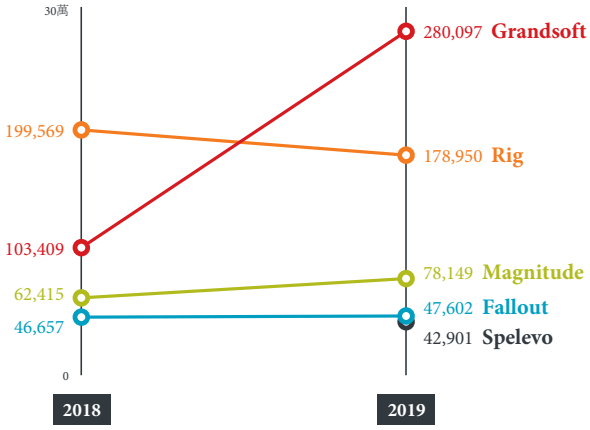

圖 27：Grandsoft 擊敗 Rig，成為偵測數量最多的漏洞攻擊套件：
已攔截的漏洞攻擊套件散布網址存取次數逐年比較。
資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

漏洞攻擊套件仍會利用已知的舊漏洞來散布惡意檔案，突顯出企業應該定期修補及更新自己的系統。

漏洞攻擊套件	攻擊的漏洞	散布的勒索病毒
GrandSoft	CVE-2018-4878 CVE-2018-8174	
Rig	CVE-2018-4878 CVE-2018-8174	Aurora、Buran、Crysis、Dharma、Eris、GandCrab、GetCrypt、Nemty、Paradise、Sodinokibi、VegaLocker
Magnitude	CVE-2019-0752 CVE-2018-4878 CVE-2018-8174	Magniber
Fallout	CVE-2018-15982 CVE-2018-4878 CVE-2018-8174	GandCrab、Hermes、Maze、Medusa、Paradise、Sodinokibi
Spelevo	CVE-2018-15982 CVE-2018-8174	Crysis、Maze、Shade、Troldash

表 3：漏洞攻擊套件仍會利用已知的舊漏洞來散布惡意檔案：2019 年前五大漏洞攻擊套件、其攻擊的漏洞，以及散布的勒索病毒。
資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

軟體廠商已通報的漏洞數量較前一年減少 29%，Microsoft 是已通報漏洞數量最多的廠商，共 190 個，其次是 Adobe，共 166 個。至於 Foxit、Apple 和 Google 的已通報漏洞數量則分別為 70、60 和 4。

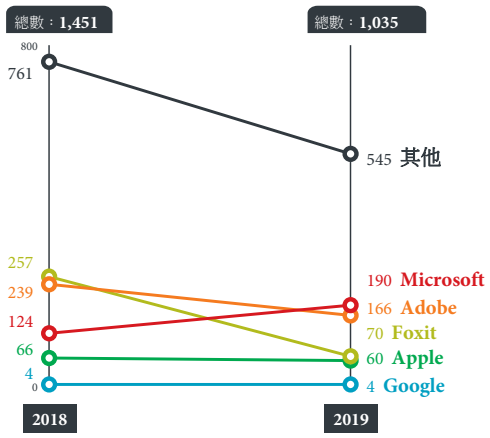

圖 28：軟體廠商已通報的漏洞數量減少：重要軟體廠商已通報漏洞數量逐年比較。

資料來源：趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫。

2019 年，殭屍網路依舊相當活躍，我們偵測到的殭屍網路連線數量總數將近 170 萬，幾乎與去年的數字相同。此外我們所偵測到的殭屍網路 C&C 伺服器數量基本上與也去年沒有太大變化，都在 15,000 個以下。

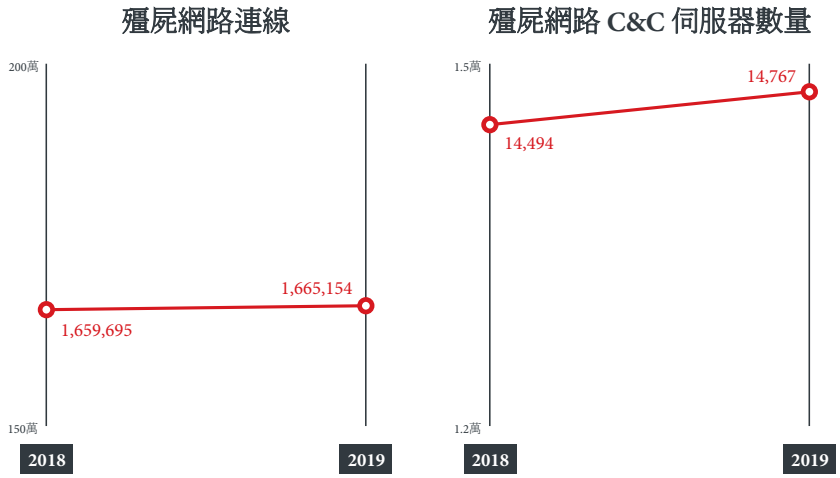

圖 29：殭屍網路連線與 C&C 伺服器數量無太大變化：殭屍網路連線與殭屍網路 C&C 伺服器偵測數量逐年比較。

註：殭屍網路 C&C 伺服器數量為端點查詢或連線的非重複且活躍的 C&C 伺服器數量；殭屍網路連線數量為向 C&C 伺服器查詢或連線的非重複端點數量。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

2019 年，Telnet 預設密碼登入活動仍是該期間觸發最多次的偵測規則，總數將近 6 億次。此一長期現象突顯出裝置登入憑證變更、更新及強化的必要。

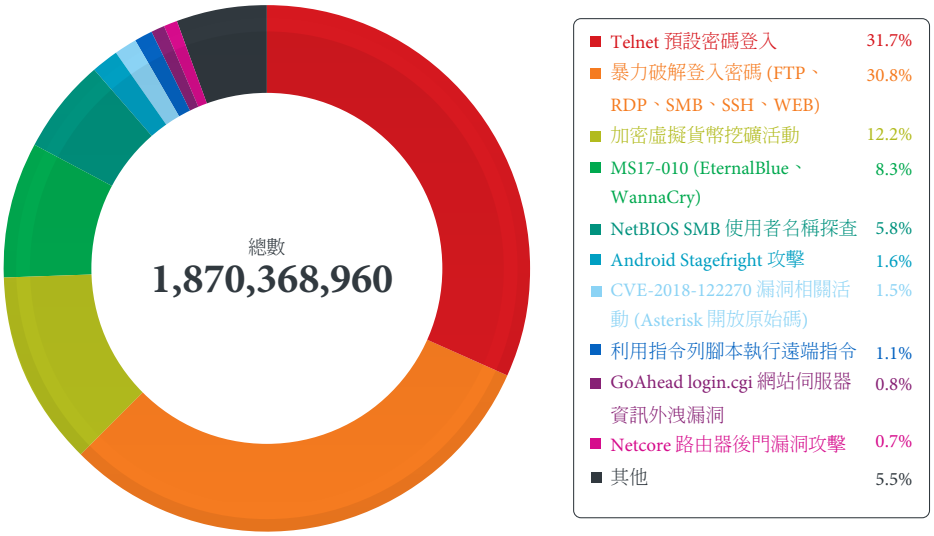

圖 30：Telnet 預設密碼登入活動仍是該期間觸發最多次的偵測規則：2019 年智慧家庭網路主要的對內與對外活動分布。

註：這些是惡意、處於灰色地帶、或可能有害的應用程式觸發偵測規則時所記錄的活動，意味著駭客攻擊或許正在發生。而與威脅活動密切關聯的事件則歸類在可能為駭客攻擊的活動。

資料來源：趨勢科技 Smart Home Network 產品。

試圖利用舊漏洞的攻擊依然對使用者和企業造成嚴重風險。

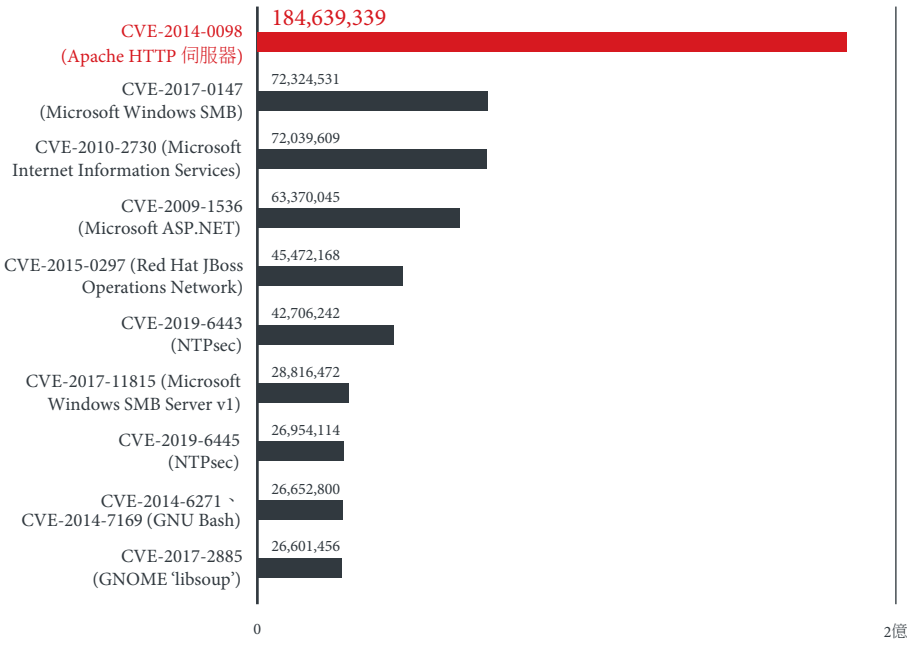

圖 31：一些老早就已釋出修補更新的舊漏洞，依然對企業造成資安風險：2019 年惡意活動偵測規則觸發次數排行榜；根據趨勢科技 Deep Security™ 解決方案回報的資料。

註：當駭客試圖攻擊某個漏洞而遭到攔截時就會觸發偵測規則。

資料來源：趨勢科技 Deep Security™ 解決方案。

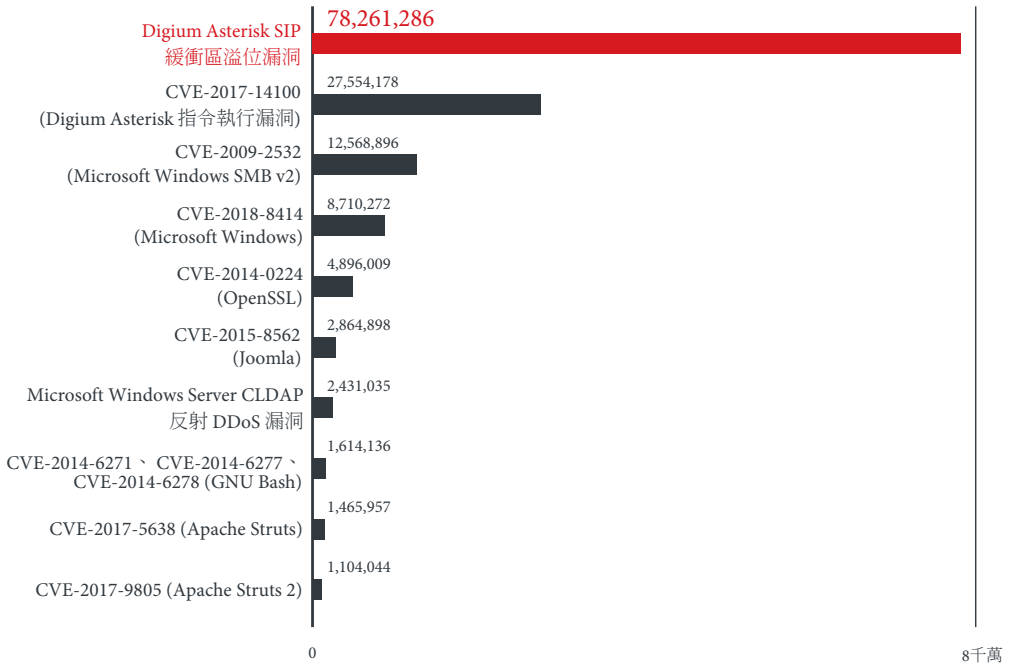

圖 32：緩衝區溢位漏洞是最常被觸發的偵測規則：2019 年偵測規則觸發次數排行榜；根據趨勢科技 TippingPoint® Threat Protection System 解決方案回報的資料。

註：當駭客試圖攻擊某個漏洞而遭到攔截時就會觸發偵測規則。

資料來源：趨勢科技 TippingPoint® Threat Protection System 解決方案。

根據我們對 Operation Endtrade 的研究資料顯示，Tick 駭客集團攻擊中國與日本企業機構的手法、技巧與程序相當精密。

手法	技巧	識別碼	說明
首次入侵	魚叉式網路釣魚附件檔案	T1193	用來發送第一階段惡意程式。
	供應鏈入侵	T1195	用來首次入侵相關子機構。
執行攻擊	利用漏洞讓用戶端執行	T1203	用來攻擊 CVE-2018-0802 和 CVE-2018-0798。
	指令列介面	T1059	讓某些被修改過的工具可使用指令列介面。
	排程工作	T1053	用來執行惡意程式。
	腳本	T1064	使用 VBScript。
	已簽署二進位檔案代理執行	T1218	用來執行惡意檔案和躲避防毒軟體偵測。
	第三方軟體	T1072	在攻擊過程中使用可公開取得的工具，如 RAR。
	使用者執行	T1204	用於初次感染。

手法	技巧	識別碼	說明
常駐系統	系統登錄的「Run」機碼或「啟動」資料夾	T1060	將自己加入系統登錄的「Run」機碼。
提升權限	避開使用者帳戶控制 (UAC) 機制	T1088	使用可避開 Windows 10 UAC 機制的工具。
躲避防禦	二進位碼填充	T1009	用於插入垃圾資料並增加檔案大小。
	避開 UAC	T1088	使用可避開 Windows 10 UAC 機制的工具。
	停用資安工具	T1089	嘗試終止防毒軟體的處理程序。
	將檔案或資訊解密/解碼	T1140	使用 TSPY_LOADVBS 來執行加密過的指令。
	檔案刪除	T1107	用於刪除用過的檔案。
	障眼法	T1036	使用從右至左書寫 (RTLO) 的技巧。
	處理程序注入	T1055	Casper 使用該手法來注入後門程式的 shellcode。
	腳本	T1064	使用 VBScript。
存取登入憑證	搜刮登入憑證	T1003	使用 Mimikatz。
搜尋	帳號搜尋	T1087	使用網路工具來進行內部偵查。
	檔案與目錄搜尋	T1083	存取共用資料夾來尋找機密資訊。
	軟體搜尋	T1518	列出已安裝的軟體。
	系統資訊搜尋	T1082	蒐集磁卷序號和其他系統資訊。
	系統服務搜尋	T1007	使用 TROJ_GETVERSION 來搜尋系統服務。
橫向移動	遠端檔案複製	T1105	透過 Windows 系統管理共用資料夾將惡意程式複製到遠端桌面。
	Windows 系統管理共用資料夾	T1077	透過 Windows 系統管理共用資料夾將惡意程式複製到遠端桌面。
蒐集	自動化蒐集	T1119	使用一個木馬程式來執行一系列搜查並將結果儲存到一個文字檔。
	來自本機系統的資料	T1005	蒐集本機和網路共用磁碟上的資料。
	來自網路共用磁碟的資料	T1039	蒐集本機和網路共用磁碟上的資料。
	螢幕截圖	T1113	可能遭竊取的 RAR 檔案含有桌面螢幕截圖。

手法	技巧	識別碼	說明
幕後操縱 (C&C)	常用連接埠	T1043	使用連接埠 80 或 443。
	客製化加密協定	T1024	用於下載或回傳資料。
	資料編碼	T1132	用於下載或回傳資料。
	資料加密編碼	T1001	用於下載或回傳資料。
	遠端存取工具	T1219	使用各種遠端存取工具 (RAT) 家族。
	遠端檔案複製	T1105	用於下載 C&C 伺服器中的檔案。
	標準應用程式層通訊協定	T1071	用於和遠端 C&C 伺服器通訊。
	標準加密協定	T1032	使用 AES。
	網站服務	T1102	用於駭入合法網站並將它當成 C&C 伺服器。
資料外傳	透過 C&C 通道將資料外傳	T1041	可能將蒐集到的資料經由 C&C 管道傳送給駭客。
	資料壓縮	T1002	使用密碼保護的 RAR。
	資料加密	T1022	使用密碼保護的 RAR。

表 4：Tick 運用了一套非常精密的攻擊程序：Tick 的 Operation Endtrade 攻擊行動所使用的手法和技巧 (對應到 MITRE ATT&CK™ for Enterprise 矩陣)[107]。

另一個我們 2019 年持續觀察的駭客集團是「APT33」，其攻擊目標橫跨全球三個大陸，其最知名的手法就是利用層層的殭屍網路來掩蓋其足跡。

手法	技巧	識別碼	說明
首次入侵	魚叉式網路釣魚連結	T1192	發送魚叉式網路釣魚郵件，內含指向 HTA 檔案的連結。
	合法帳號	T1078	使用合法帳號作為首次入侵，然後提升權限。
執行攻擊	利用漏洞讓用戶端執行	T1203	嘗試攻擊 WinRAR 的已知漏洞 (CVE- 2018-20250)。
	PowerShell	T1086	使用 PowerShell 從 C&C 伺服器下載檔案並執行各種腳本。
	使用者執行	T1204	利用魚叉式網路釣魚郵件誘騙使用者點選指向惡意 HTML 應用程式的連結。

手法	技巧	識別碼	說明
常駐系統	系統登錄的「Run」機碼或「啟動」資料夾	T1060	利用系統登錄的「Run」機碼及「啟動」資料夾在受害電腦植入多種惡意程式變種。
提升權限	排程工作	T1053	建立一個排程工作以便在一天當中讓某個 VBE 檔案執行好幾次。
躲避防禦	執行限制	T1480	在惡意程式內加入終止日期的設計來控制其執行。
	將檔案或資訊加密編碼	T1027	使用 Base64 將惡意檔案編碼。
存取登入憑證	暴力破解	T1110	嘗試利用常用密碼來試圖暴力登入大量系統。
	搜刮登入憑證	T1003	使用各種可公開取得的工具 (如：LaZagne、Mimikatz、Gpppassword、SniffPass 及 ProcDump) 來搜刮登入憑證。
搜尋	網路窺探	T1040	利用 SniffPass 來窺探網路流量以便蒐集登入憑證。
橫向移動	遠端檔案複製	T1105	從 C&C 伺服器下載其他檔案和程式。
幕後操縱 (C&C)	常用連接埠	T1043	使用連接埠 443 進行 C&C 通訊。
	資料編碼	T1132	使用 Base64 將 C&C 流量編碼。
	標準應用程式層通訊協定	T1071	使用 HTTP 來進行 C&C 通訊。
	標準加密協定	T1032	使用 AES 將 C&C 流量加密。
	不常用的連接埠	T1065	使用連接埠 808 和 880 進行 C&C 通訊。
資料外傳	資料壓縮	T1002	在資料外傳之前先使用 WinRAR 來壓縮資料。
	使用其他通訊協定來外傳資料。	T1048	使用 FTP 來外傳資料 (而非透過 C&C 管道)。

表 5：APT33 使用多種 C&C 相關技巧：APT33 所使用的手法和技巧 (對應到 MITRE ATT&CK for Enterprise 矩陣)[108]。

Trend Micro Research 在 2019 年當中不斷率先發掘各種新的威脅技巧，並且開發創新的網路資安技術。其中一項最令人訝異的發現來自於我們對無線射頻 (RF) 遙控器的研究分析，這類遙控器廣泛用於製造、營造、運輸產業以及其他工業應用。根據我們研究指出，許多知名廠商製造的 RF 遙控器都缺乏安全防護機制，因此一旦遭到攻擊就很可能導致各種嚴重的後果，如：竊盜、勒索、破壞、人身傷害等等[109]。

此外，我們也開發出一些工具來研究 Twitter 上的資料和案例，看看如何從社群媒體上蒐集有助於採取行動的威脅情報。我們的研究證明，社群媒體擁有龐大的資訊，是一個非常適合用來蒐集威脅情報以協助制定資安策略和行動的平台[110]。

我們也要再次強調將機器學習應用於威脅偵測以及搭配我們相關研究成果的重要性。在兩項由我們和澳洲聯邦大學 (Federation University Australia) 所做的研究當中，我們示範了在樣本數很少、甚至只有單一樣本時，如何運用機器學習，特別是「生成對抗自動編碼器」(generative adversarial autoencoder) 模型，來偵測和分析惡意程式[111、112]。此外，我們也展示了一項機器學習的創新運用，開發了一個採用兩階段訓練的模型來提高偵測率並降低誤判。我們將此模型命名為「TrendX Hybrid Model」，它不僅能偵測惡意程式變種，更能預測其行為[113]。

參考資料

1 趨勢科技。(2019 年 8 月 27 日)。*趨勢科技*。「2019 上半年資安總評：隱匿的威脅、瀰漫的衝擊」(2019 Midyear Roundup: Evasive Threats, Pervasive Effects)。上次存取時間 2020 年 2 月 12 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects.

2 Janus Agcaoili 與 Miguel Ang。(2019 年 6 月 6 日)。*趨勢科技*。「縮小目標、獲利更大：2019 年勒索病毒發展」(Narrowed Sights, Bigger Payoffs: Ransomware in 2019)。上次存取時間 2020 年 2 月 12 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019.

3 趨勢科技。(2019 年 11 月 5 日)。*趨勢科技*。「勒索病毒攻擊西班牙企業並癱瘓拿大領土紐納武特 (Nunavut) 政府服務」(Ransomware Attacks Hit Spanish Companies, Paralyzes Government Services in Canadian Territory of Nunavut)。上次存取時間 2020 年 2 月 6 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-attacks-hit-spanish-companies-paralyzes-government-services-in-canadian-territory-of-nunavut.

4 趨勢科技。(2019 年 7 月 4 日)。*趨勢科技*。「勒索病毒、變臉詐騙襲擊美屬維京群島政府機關」(Ransomware, BEC Attacks Strike Government Offices in the US Virgin Islands)。上次存取時間 2020 年 2 月 12 日： https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ransomware-bec-attacks-strike-government-offices-in-the-us-virgin-islands.

5 趨勢科技。(2019 年 8 月 2 日)。*趨勢科技*。「美國加州都市證實電話及金融資料系統因勒索病毒攻擊而服務中斷」(California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware.

6 Lawrence Abrams。(2019 年 12 月 24 日)。*Bleeping Computer*。「Maze 勒索病毒將美國佛州彭薩科拉市 (Pensacola) 遭竊的檔案外流」(Maze Ransomware Releases Files Stolen from City of Pensacola)。上次存取時間 2020 年 1 月 25 日：https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/.

7 Fahmida Y. Rashid。(2019 年 12 月 11 日)。*Decipher*。「Maze 讓勒索病毒事件變成資料外洩事件」(Maze Turns Ransomware Into Data Breaches)。上次存取時間 2020 年 1 月 25 日： https://duo.com/decipher/maze-turns-ransomware-incidents-into-data-breaches.

8 趨勢科技。(2019 年 10 月 21 日)。*趨勢科技*。「系統駭入專家與勒索病毒集團在地下網路結盟」(Underground Intrusion Specialists Team Up With Ransomware Groups)。上次存取時間 2020 年 1 月 30 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/underground-intrusion-specialists-team-up-with-ransomware-groups.

9 Sean Gallagher。(2019 年 11 月 22 日)。*Ars Technica*。「美國路易西安那州遭 Ryuk 襲擊，再次引發網路緊急事件」(Louisiana was hit by Ryuk, triggering another cyber-emergency)。上次存取時間 2020 年 2 月 12 日：https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-another-cyber-emergency/.

10 Lawrence Abrams。(2019 年 1 月 12 日)。*Bleeping Computer*。「Ryuk 勒索病毒與 TrickBot 合作，入侵受感染網路」(Ryuk Ransomware Partners with TrickBot to Gain Access to Infected Networks)。上次存取時間 2020 年 2 月 12 日：https://www.bleepingcomputer.com/news/security/ryuk-ransomware-partners-with-trickbot-to-gain-access-to-infected-networks/.

11 趨勢科技。(2019 年 9 月 10 日)。*趨勢科技*。「美國德州數個市政府遭 REvil/Sodinokibi 襲擊，未支付贖金，半數以上已恢復營運」(Texas Municipalities Hit by REvil/Sodinokibi Paid No Ransom, Over Half Resume Operations)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations.

12 Matthew Rosenberg、Nicole Perlroth 與 David E. Sanger。(2020 年 1 月 10 日)。*The New York Times*。「製造混亂：2020 年俄羅斯駭客與酸民將更加隱匿」('Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020)。上次存取時間 2020 年 2 月 7 日：https://www.nytimes. com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

13 Emsisoft Malware Lab。(2019 年 12 月 12 日)。*Emsisoft Blog*。「美國勒索病毒現況：2019 年報告與統計數據」(The State of Ransomware in the US: Report and Statistics 2019)。上次存取時間 2020 年 1 月 25 日：https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

14 SentinelOne。(2018 年 3 月 27 日)。*SentinelOne*。「SentinelOne：2018 年全球勒索病毒研究」(SentinelOne: Global Ransomware Study 2018)。上次存取時間 2020 年 1 月 31 日：https://go.sentinelone.com/rs/327-MNM-087/images/Ransomware%20Research%20Data%20Summary%202018.pdf.

15 Kathleen Foody。(2019 年 9 月 20 日)。*AP News*。「保險理賠可能進一步助長勒索病毒攻擊」(Payouts from insurance policies may fuel ransomware attacks)。上次存取時間 2020 年 1 月 25 日：https://apnews.com/234360e2e36b424b8849e51e57fe53c5.

16 Kathleen Foody。(2019 年 9 月 20 日)。*AP News*。「保險理賠可能進一步助長勒索病毒攻擊」(Payouts from insurance policies may fuel ransomware attacks)。上次存取時間 2020 年 1 月 25 日：https://apnews.com/234360e2e36b424b8849e51e57fe53c5.

17 Kathleen Foody。(2019 年 9 月 20 日)。*AP News*。「保險理賠可能進一步助長勒索病毒攻擊」(Payouts from insurance policies may fuel ransomware attacks)。上次存取時間 2020 年 1 月 25 日：https://apnews.com/234360e2e36b424b8849e51e57fe53c5.

18 James Leggate。(2019 年 9 月 3 日)。*Fox Business*。「遭到勒索病毒襲擊嗎？看看 FBI 怎麼建議」(Hit by ransomware? Here's what the FBI says you should do)。上次存取時間 2020 年 1 月 25 日：https://www.foxbusiness.com/technology/ransomware-fbi-paying-cyber-criminals.

19 Andrew Brandt。(2019 年 12 月 9 日)。*Sophos News*。「Snatch 勒索病毒讓電腦重新開機進入保護模式來躲避資安防護」(Snatch ransomware reboots PCs into Safe Mode to bypass protection)。上次存取時間 2020 年 1 月 25 日：https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/.

20 趨勢科技。(2019 年 12 月 12 日)。*趨勢科技*。「最新勒索病毒總整理：Snatch 和 Zeppelin 勒索病毒」(Ransomware Recap: Snatch and Zeppelin Ransomware)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-snatch-and-zeppelin-ransomware.

21 趨勢科技。(2020 年 1 月 6 日)。*趨勢科技*。「最新勒索病毒總整理：Clop、DeathRansom 和 Maze 勒索病毒」(Ransomware Recap: Clop, DeathRansom, and Maze Ransomware)。上次存取時間 2020 年 2 月 10 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-clop-deathransom-and-maze-ransomware.

22 Andrew Brandt。(2019 年 12 月 9 日)。*Sophos News*。「Snatch 勒索病毒讓電腦重新開機進入保護模式來躲避資安防護」(Snatch ransomware reboots PCs into Safe Mode to bypass protection)。上次存取時間 2020 年 2 月 10 日：https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/.

23 Alon Groisman。(2019 年 12 月 18 日)。*Morphisec*。「ConnectWise Control 又遭駭客利用，散布 Zeppelin 勒索病毒」(ConnectWise Control Abused Again to Deliver Zeppelin Ransomware)。上次存取時間 2020 年 2 月 10 日：https://blog.morphisec.com/connectwise-control-abused-again-to-deliver-zeppelin-ransomware/.

24 趨勢科技。(2019 年 3 月 20 日)。*趨勢科技*。「有關 LockerGoga 勒索病毒您該知道的事」(What You Need to Know About the LockerGoga Ransomware)。上次存取時間 2020 年 2 月 12 日：https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/.

25 Andy Greenberg。(2019 年 3 月 25 日)。*Wired*。「了解癱瘓工業設施的 LockerGoga 勒索病毒」(A Guide to LockerGoga, the Ransomware Crippling Industrial Firms)。上次存取時間 2020 年 2 月 12 日：https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/.

26 Lawrence Abrams。(2019 年 3 月 5 日)。*Bleeping Computer*。「CryptoMix Clop 表示其攻擊的目標是網路而非電腦」(CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers)。上次存取時間 2020 年 2 月 10 日：https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/.

27 Lee Tae-woo、Kim Byoung-jae、Kim Dong-wook、Ryu So-joon、Shim Jae-hong 與 Eunju Pak。(日期不詳)。*Korea Internet & Security Agency*。「勒索病毒透過 AD Server 在內部網路散布的個案研究」(Analysis on Cases of Distribution of Internal Network Ransomware through Exploiting AD Server)。上次存取時間 2020 年 2 月 12 日：https://www.boho.or.kr/filedownload.do?attach_file_seq=2235&attach_file_id=EpF2235.pdf.

28 趨勢科技。(2019 年 12 月 12 日)。*趨勢科技*。「最新勒索病毒總整理：Snatch 和 Zeppelin 勒索病毒」(Ransomware Recap: Snatch and Zeppelin Ransomware)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-snatch-and-zeppelin-ransomware.

29 趨勢科技。(2020 年 1 月 6 日)。*趨勢科技*。「最新勒索病毒總整理：Clop、DeathRansom 和 Maze 勒索病毒」(Ransomware Recap: Clop, DeathRansom, and Maze Ransomware)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-clop-deathransom-and-maze-ransomware.

30 Business Wire。(2019 年 12 月 19 日)。*Business Wire*。「2019 年趨勢科技網路資安風險指標 (Cyber Risk Index) 上升」(Trend Micro Cyber Risk Index Increased in 2019)。上次存取時間 2020 年 1 月 25 日：https://www.businesswire.com/news/home/20191219005130/en/Trend-Micro-Cyber-Risk-Index-Increased-2019.

31 Tony Redmond。(2019 年 10 月 24 日)。*Office 365 for IT Pros*。「Office 365 每月活躍用戶數量突破 2 億」(Office 365 Hits 200 Million Monthly Active Users)。上次存取時間 2020 年 2 月 6 日：https://office365itpros.com/2019/10/24/office-365-hits-200-million-monthly-active-users/.

32 趨勢科技。(2019 年 3 月 4 日)。*趨勢科技*。「趨勢科技 2018 年 Cloud App Security 報告：針對進階電子郵件威脅的進階防禦」(Trend Micro Cloud App Security Report 2018: Advanced Defenses for Advanced Email Threats)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/advanced-defenses-for-advanced-email-threats.

33 Samuel P Wang。(2019 年 4 月 4 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「網路釣魚攻擊使用瀏覽器擴充元件 SingleFile 來將惡意登入網頁加密編碼」(Phishing Attack Uses Browser Extension Tool SingleFile to Obfuscate Malicious Log-in Pages)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-attack-uses-browser-extension-tool-singlefile-to-obfuscate-malicious-log-in-pages/.

34 Katsuyuki Okamoto。(2019 年 10 月 24 日)。*トレンドマイクロ セキュリティブログ*。「国内ネットバンキングの二要素認証を狙うフィッシングが激化」。上次存取時間 2020 年 1 月 30 日：https://blog.trendmicro.co.jp/archives/22696.

35 Office 365 Threat Research Team。(2019 年 12 月 11 日)。*Microsoft Security*。「網路釣魚暗中演化」(The quiet evolution of phishing)。上次存取時間 2020 年 1 月 25 日：https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/.

36 Office 365 Threat Research Team。(2019 年 12 月 11 日)。*Microsoft Security*。「網路釣魚暗中演化」(The quiet evolution of phishing)。上次存取時間 2020 年 1 月 25 日：https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/.

37 趨勢科技。(2018 年 1 月 18 日)。*趨勢科技*。「深入變臉詐騙的世界」(Delving into the World of Business Email Compromise [BEC])。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/delving-into-the-world-of-business-email-compromise-bec.

38 Federal Bureau of Investigation Internet Crime Complaint Center (IC3)。(日期不詳)。*Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*。「2019 年網際網路犯罪報告」(2018 Internet Crime Report)。上次存取時間 2020 年 2 月 20 日：https://pdf.ic3.gov/2019_ IC3Report.pdf.

39 趨勢科技。(2019 年 5 月 2 日)。*趨勢科技*。「變臉詐騙集團從美國俄亥俄州某教會騙取 175 萬美元」(BEC Scammers Steal US$1.75 Million From an Ohio Church)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scammers-steal-us- 1-75-million-from-an-ohio-church.

40 Oregon Live。(2019 年 8 月 19 日)。*Oregon Live*。「美國奧勒岡州波特蘭公立學校 (Portland Public Schools) 遭詐騙近 290 萬美元」(Portland Public Schools nearly scammed out of $2.9 million)。上次存取時間 2020 年 2 月 26 日：https://www.oregonlive.com/education/2019/08/portland-public-schools-nearly-scammed-out-of-29-million.html.

41 趨勢科技。(2019 年 16 月 4 日)。*趨勢科技*。「新的變臉詐騙手法利用自動轉帳竊取員工薪資」(New Business Email Compromise Scheme Reroutes Paycheck by Direct Deposit)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-business-email-compromise-scheme-reroutes-paycheck-by-direct-deposit.

42 趨勢科技。(2019 年 7 月 12 日)。*趨勢科技*。「變臉詐騙集團使用偽造發票詐騙美國喬治亞州格里芬市 (Griffin City) 超過 80 萬美元」(Fake Invoices Used by BEC Scammers to Defraud Griffin City, Georgia of Over US$800,000)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-invoices-used-by-bec-scammers-to-defraud-griffin-georgia-us-800-000.

43 Sergiu Gatlan。(2020 年 1 月 3 日)。*Bleeping Computer*。「美國科羅拉多州城鎮匯了 100 萬美元以上給變臉詐騙集團」(Colorado Town Wires Over $1 Million to BEC Scammers)。上次存取時間 2020 年 1 月 25 日：https://www.bleepingcomputer.com/news/security/colorado-town-wires-over-1-million-to-bec-scammers/.

44 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 2020 年 2 月 7 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.

45 Lindsey O'Donnell。(2019 年 3 月 5 日)。*Threatpost*。「RSA Conference 2019：變臉詐騙集團瞄準童子軍團與其他非營利機構」(RSA Conference 2019: BEC Scammer Gang Takes Aim at Boy Scouts, Other Nonprofts)。上次存取時間 2020 年 2 月 7 日：https://threatpost.com/rsac-2019-bec-scammer-gang-takes-aim-at-boy-scouts-other-nonprofts/142302/.

46 Charles Cooper。(2018 年 5 月 16 日)。*Symantec Blogs*。「WannaCry：一年來給我們什麼教訓」(WannaCry: Lessons Learned 1 Year Later)。上次存取時間 2020 年 1 月 25 日：https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later.

47 Microsoft。(2019 年 5 月 14 日)。*Microsoft MSRC*。「CVE-2019-0708 | 遠端桌面服務遠端程式碼執行漏洞 」(CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability)。上次存取時間 2020 年 1 月 25 日：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708.

48 趨勢科技。(2019 年 5 月 29 日)。*趨勢科技*。「BlueKeep 可蠕蟲化漏洞 (CVE-2019-0708) 影響將近百萬台系統」(Nearly 1 Million Systems Affected By 'Wormable' BlueKeep Vulnerability [CVE-2019-0708])。上次存取時間 2020 年 2 月 6 日：https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/nearly-1-million-systems-affected-by-wormable-bluekeep-vulnerability-cve-2019-0708.

49 Danny Palmer。(2017 年 10 月 27 日)。*ZDNet*。「研究人員證實 Bad Rabbit 勒索病毒利用美國國家安全局外洩的 EternalRomance 漏洞攻擊手法散布」(Bad Rabbit ransomware spread using leaked NSA EternalRomance exploit, researchers confirm)。上次存取時間 2020 年 2 月 7 日：https://www.zdnet.com/article/bad-rabbit-ransomware-spread-using-leaked-nsa-eternalromance-exploit-researchers-confirm/.

50 Rob Wright。(2019 年 7 月 17 日)。*SearchSecurity*。「BlueKeep 災難：仍有超過 80 萬台電腦至今仍未修補」(BlueKeep blues: More than 800,000 systems still unpatched)。上次存取時間 2020 年 1 月 25 日：https://searchsecurity.techtarget.com/news/252466932/BlueKeep-blues-More-than-800000-systems-still-unpatched.

51 Microsoft Defender ATP Research Team。(2019 年 11 月 7 日)。*Microsoft Security*。「Microsoft 與研究人員合作偵測及防範最新的 RDP 漏洞攻擊」(Microsoft works with researchers to detect and protect against new RDP exploits)。上次存取時間 2020 年 1 月 25 日：https://www.microsoft.com/security/blog/2019/11/07/the-new-cve-2019-0708-rdp-exploit-attacks-explained/.

52 Federal Bureau of Investigation Internet Crime Complaint Center (IC3)。(2018 年 9 月 27 日)。*Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*。「網路駭客越來越常利用遠端桌面通訊協定來從事惡意活動」(Cyber Actors Increasingly Exploit the Remote Desktop Protocol to Conduct Malicious Activity)。上次存取時間 2020 年 1 月 25 日：https://www.ic3.gov/media/2018/180927.aspx.

53 Microsoft。(日期不詳)。*Microsoft MSRC*。「安全更新指南」(Security Update Guide)。上次存取時間 2020 年 1 月 29 日：https://portal.msrc.microsoft.com/en-us/security-guidance.

54 趨勢科技。(2018 年 10 月 31 日)。*趨勢科技*。「InfoSec Guide: 遠端桌面通訊協定 (RDP)」(InfoSec Guide: Remote Desktop Protocol [RDP])。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/infosec-guide-remote-desktop-protocol-rdp.

55 Net Market Share。(日期不詳)。*Net Market Share*。「作業系統版本市占率分布」(Operating System Share by Version)。上次存取時間 2020 年 1 月 25 日：https://netmarketshare.com/operating-system-market-share.aspx?id=platformsDesktopVersions.

56 Microsoft。(2020 年 1 月 14 日)。*Microsoft*。「Windows 7 支援已於 2020 年 1 月 14 日終止」(Windows 7 support ended on January 14, 2020)。上次存取時間 2020 年 1 月 25 日：https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020.0.

57 Brian Gorenc。(2020 年 1 月 30 日)。*Zero Day Initiative*。「ZDI 漏洞懸賞計畫 2019 年回顧」(LOOKING BACK AT THE ZERO DAY INITIATIVE IN 2019)。上次存取時間 2020 年 2 月 3 日：https://www.zerodayinitiative.com/blog/2020/1/30/looking-back-at-the-zero-day-initiative-in-2019.

58 Brian Gorenc。(2020 年 1 月 30 日)。*Zero Day Initiative*。「ZDI 漏洞懸賞計畫 2019 年回顧」(LOOKING BACK AT THE ZERO DAY INITIATIVE IN 2019)。上次存取時間 2020 年 2 月 3 日：https://www.zerodayinitiative.com/blog/2020/1/30/looking-back-at-the-zero-day-initiative-in-2019.

59 趨勢科技。(2019 年 6 月 27 日)。*趨勢科技*。「IIoT 攻擊面：威脅與資安解決方案」(The IIoT Attack Surface: Threats and Security Solutions)。上次存取時間 2020 年 2 月 6 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions.

60 Markets and Markets。(2019 年 4 月)。*Markets and Markets*。「監控與資料擷取 (SCADA) 系統市場」(SCADA Market)。上次存取時間 2020 年 1 月 25 日：https:// www.marketsandmarkets.com/Market-Reports/scada-market-19487518.html.

61 Randal Kenworthy。(2019 年 11 月 18 日)。*Forbes*。「5G 和 IoT 革命即將來臨：看看有什麼值得期待」(The 5G And IoT Revolution Is Coming: Here's What To Expect)。上次存取時間 2020 年 1 月 25 日：https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/#7cc557756abf.

62 趨勢科技。(2019 年 4 月 4 日)。*趨勢科技*。「Mirai 變種使用多種漏洞攻擊手法瞄準各類型路由器」(Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers.

63 Augusto Remillano II 與 Jakub Urbanec。(2019 年 5 月 23 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「新的 Mirai 變種使用多種漏洞攻擊手法瞄準路由器和其他裝置」(New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/.

64 趨勢科技。(2019 年 8 月 8 日)。*趨勢科技*。「從 Mirai 衍生的 Echobot 殭屍網路具備 50 多種漏洞攻擊手法」(Mirai Spawn Echobot Found Using Over 50 Different Exploits)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-spawn-echobot-found-using-over-50-different-exploits.

65 Augusto Remillano II 與 Jakub Urbanec。(2019 年 8 月 13 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「一連串的攻擊行動：Neko、Mirai 及 Bashlite 惡意程式變種利用各式各樣漏洞攻擊手法駭入多種路由器和裝置」(Back-to-Back Campaigns: Neko, Mirai, and Bashlite Malware Variants Use Various Exploits to Target Several Routers, Devices)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/back-to-back-campaigns-neko-mirai-and-bashlite-malware-variants-use-various-exploits-to-target-several-routers-devices/.

66 Aliakbar Zahravi。(2019 年 12 月 16 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「DDoS 和 IoT 漏洞攻擊：Momentum 殭屍網路最新活動」(DDoS Attacks and IoT Exploits: New Activity from Momentum Botnet)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet/.

67 Dark Reading Staff。(2019 年 10 月 7 日)。*Dark Reading*。「在 2 百萬個網站上發現 Magecart 盜卡程式碼」(Magecart Skimmers Spotted on 2M Websites)。上次存取時間 2020 年 1 月 25 日：https://www.darkreading.com/endpoint/magecart-skimmers-spotted-on-2m-websites/d/d-id/1336011.

68 Chaoying Liu 與 Joseph C. Chen。(2019 年 1 月 16 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「新的 Magecart 攻擊經由網路廣告供應鏈來散布惡意程式」(New Magecart Attack Delivered Through Compromised Advertising Supply Chain)。上次存取時間 2020 年 1 月 30 日：https://blog.trendmicro. com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.

69 Joseph C. Chen。(2019 年 10 月 9 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「FIN6 利用 Magecart 攻擊手法在數千個網路商店注入信用卡盜卡程式」(FIN6 Compromised E-commerce Platform via Magecart to Inject Credit Card Skimmers Into Thousands of Online Shops)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/.

70 Katsuyuki Okamoto。(2020 年 1 月 10 日)。**トレンドマイクロ セキュリティブログ。「2019年『法人』と『個人』のサイバー脅威動向：サイバー犯罪が覆す『安全』の常識」**。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.co.jp/archives/23409.

71 趨勢科技。(日期不詳)。*趨勢科技*。「開發營運」(DevOps)。上次存取時間 2020 年 2 月 6 日：https://www.trendmicro.com/vinfo/us/security/definition/devops.

72 Tony Bradely。(2018 年 8 月 1 日)。*Forbes*。「網路犯罪集團專門瞄準脆弱的環節使得供應鏈攻擊變多」(Supply Chain Attacks Increase As Cybercriminals Focus On Exploiting Weak Links)。上次存取時間 2020 年 2 月 6 日：https://www.forbes.com/sites/tonybradley/2018/08/01/supply-chain-attacks-increase-as-cybercriminals-focus-on-exploiting-weak-links/#2661edfd3519.

73 David Fiser、Jakub Urbanec 與 Jaromir Horejsi。(2019 年 6 月 14 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「AESDDoS 殭屍網路病毒經由暴露在外的 Docker API 滲透容器」(AESDDoS Botnet Malware Infiltrates Containers via Exposed Docker APIs)。上次存取時間 2020 年 2 月 5 日：https://blog.trendmicro.com/trendlabs-security-intelligence/aesddos-botnet-malware-infiltrates-containers-via-exposed-docker-apis/.

74 趨勢科技。(2019 年 6 月 26 日)。*趨勢科技*。「Kubernetes 因先前漏洞的安全更新不完整而被發現 CVE-2019-11246 漏洞」(Kubernetes Vulnerability CVE-2019-11246 Discovered Due to Incomplete Updates from a Previous Flaw)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/kubernetes-vulnerability-cve-2019-11246-discovered-due-to-incomplete-updates-from-a-previous-flaw.

75 David Fiser。(2019 年 6 月 17 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「Jenkins 系統管理員：採用預設值設定可能讓 Master 電腦暴露於遠端程式碼執行漏洞攻擊的風險」(Jenkins Admins: Relying on Default Settings Could Put Master at Risk of Remote Code Execution Attacks)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro. com/trendlabs-security-intelligence/jenkins-admins-relying-on-default-settings-could-put-master-at-risk-of-remote-code-execution-attacks/.

76 David Fiser。(2019 年 8 月 30 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「隱藏在純文字中：Jenkins 外掛漏洞」(Hiding in Plain Text: Jenkins Plugin Vulnerabilities)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/hiding-in-plain-text-jenkins-plugin-vulnerabilities/.

77 趨勢科技。(2019 年 10 月 17 日)。*趨勢科技*。「超過 2,000 台不安全的 Docker 主機感染門羅幣挖礦蠕蟲」(Monero-mining Worm Infects Over 2,000 Unsecure Docker Hosts)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/monero-mining-worm-infects-over-2-000-unsecure-docker-hosts.

78 Mohamad Mokbel。(2019 年 22 月 4 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「分析軟體供應鏈攻擊中的 C/C++ 執行時期程式庫篡改手法」(Analyzing C/C++ Runtime Library Code Tampering in Software Supply Chain Attacks)。上次存取時間 2020 年 2 月 5 日： https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks/.

79 趨勢科技。(2019 年 7 月 29 日)。*趨勢科技*。「檯面下的風險：認識無檔案式威脅」(Risks Under the Radar: Understanding Fileless Threats)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats.

80 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 2020 年 2 月 7 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.

81 Henry Alarcon, Jr. 與 Raphael Centeno。(2019 年 3 月 4 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「無檔案式銀行木馬程式攻擊巴西銀行，可能下載殭屍網路病毒與資訊竊取程式」(Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/.

82 Carl Maverick Pascual。(2019 年 9 月 19 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「無檔案虛擬加密貨幣挖礦程式 GhostMiner 利用 WMI 物件為武器，終止其他挖礦程式」(Fileless Cryptocurrency-Miner GhostMiner Weaponizes WMI Objects, Kills Other Cryptocurrency-Mining Payloads)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-cryptocurrency-miner-ghostminer-weaponizes-wmi-objects-kills-other-cryptocurrency-mining-payloads/.

83 趨勢科技。(2019 年 9 月 18 日)。*趨勢科技*。「Emotet 終結 Hiatus，發動新的垃圾郵件行動」(Emotet Ends Hiatus with New Spam Campaigns)。上次存取時間 2020 年 1 月 25 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-ends-hiatus-with-new-spam-campaigns.

84 Johnlery Triunfante 與 Earle Earnshaw。(2019 年 9 月 9 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「Rig 漏洞攻擊套件現在會利用 PowerShell 來散布含有 Rootkit 元件的 Purple Fox 無檔案惡意程式」('Purple Fox' Fileless Malware with Rookit Component Delivered by Rig Exploit Kit Now Abuses PowerShell)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/purple-fox-fileless-malware-with-rookit-component-delivered-by-rig-exploit-kit-now-abuses-powershell/.

85 Jaromir Horejsi 與 Joseph C. Chen。(2019 年 10 月 1 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「KovCoreG 惡意廣告行動散布新的無檔案殭屍網路 Novter」(New Fileless Botnet Novter Distributed by KovCoreG Malvertising Campaign)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-fileless-botnet-novter-distributed-by-kovcoreg-malvertising-campaign/.

86 Joey Chen、Hiroyuki Kakara 與 Masaoki Shoji。(2019 年 11 月 29 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「Operation ENDTRADE：追查 TICK 網路間諜集團的多重階段後門程式」(Operation ENDTRADE: Finding Multi-Stage Backdoors that TICK)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/.

87 Joey Chen、Hiroyuki Kakara 與 Masaoki Shoji。(2019 年)。*趨勢科技*。「Operation ENDTRADE：TICK 網路間諜集團利用多重階段後門程式攻擊不同產業並竊取機密資料」(Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data)。上次存取時間 2020 年 2 月 6 日： https://documents.trendmicro. com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

88 Feike Hacquebord、Cedric Pernet 與 Kenney Lu。(2019 年 12 月 12 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「層層掩護下的十多個 APT33 殭屍網路鎖定攻擊極少數特定目標」(More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting)。上次存取時間 2020 年 1 月 25 日：https://blog. trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/.

89 Lorin Wu。(2019 年 1 月 30 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「Google Play 上多款相機修圖軟體會發送色情內容，並將使用者重導至網路釣魚網站以蒐集其照片」(Various Google Play 'Beauty Camera' Apps Send Users Pornographic Content, Redirect Them to Phishing Websites and Collect Their Pictures)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/various-google-play-beauty-camera-apps-sends-users-pornographic-content-redirects-them-to-phishing-websites-and-collects-their-pictures/.

90 Bill Marczak、Adam Hulcoop、Etienne Maynier、Bahr Abdul Razzak、Masashi Crete-Nishihata、John Scott-Railton 與 Ron Deibert。(2019 年 9 月 24 日)。*The Citizen Lab*。「失落的環節：西藏團體遭到行動裝置單次點選漏洞攻擊」(Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits)。上次存取時間 2020 年 2 月 13 日：https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.

91 ClearSky Cybersecurity。(2019 年 5 月)。*ClearSky Cyber Security*。「伊朗國家 APT 駭客團體 Black Box 資料外洩」(Iranian Nation-State APT Groups 'Black Box' Leak)。上次存取時間 2020 年 2 月 13 日：https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf.

92 Daniel Lunghi 與 Jaromir Horejsi。(2019 年 6 月 10 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「MuddyWater 再度現身，採用多重階段的後門程式 POWERSTATS V3 與新的漏洞攻擊後續工具」(MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/.

93 Daniel Lunghi 與 Jaromir Horejsi。(2019 年)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「發現 MuddyWater 駭客集團新活動：使用多重階段後門程式、新的漏洞攻擊後續輔助工具、Android 惡意程式等等」(New MuddyWater Activities Uncovered: Threat Actors Used Multi-Stage Backdoors, New PostExploitation Tools, Android Malware, and More)。上次存取時間 2020 年 2 月 7 日：https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf.

94 Kari Paul。(2019 年 1 月 6 日)。*MarketWatch*。「Apple 還是 Android？以下是您能買到最安全的手機」(Apple or Android? Here is the most secure phone you can get)。上次存取時間 2020 年 1 月 25 日：https://www.marketwatch.com/story/apple-or-android-here-is-the-most-secure-phone-you-can-get-2018-10-10.

95 Eric Zeman。(2018 年 9 月 29 日)。*Fortune*。「看看 Apple iOS 12 如何強化您 iPhone 的安全性」(Apple iOS 12 Fortifies Your iPhone's Security. Here's How)。上次存取時間 2020 年 1 月 25 日：https://fortune.com/2018/09/29/apple-ios-12-iphone-security/.

96 Hara Hiroaki、Lilang Wu 與 Lorin Wu。(2019 年 2 月 4 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「新版 XLoader 偽裝成 Android 應用程式；某 iOS 設定檔內含指向 FakeSpy 的新連結」(New Version of XLoader That Disguises as Android Apps and an iOS Profile Holds New Links to FakeSpy)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/.

97 Lilang Wu、Yuchen Zhou 和 Moony Li。(2019 年 7 月 12 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「iOS URL Scheme 可能遭到挾持」(iOS URL Scheme Susceptible to Hijacking)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/.

98 行動裝置威脅應變團隊。(2019 年 9 月 26 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「賭博應用程式暗中登上百大排行榜：數以百計的假應用程式如何在 iOS App Store 和 Google Play 應用程式上散布」(Gambling Apps Sneak into Top 100: How Hundreds of Fake Apps Spread on iOS App Store and Google Play)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/gambling-apps-sneak-top-100-hundreds-fake-apps-spread-app-store-google-play/.

99 Juwei Lin。(2019 年 8 月 4 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「macOS 三月份更新：修正可能洩漏機密資訊以及讓駭客執行任意程式碼的漏洞」(Patch With March macOS Updates: Vulnerabilities May Expose Restricted Information, Enable Arbitrary Code Execution)。上次存取時間 2020 年 1 月 25 日：https://blog. trendmicro.com/trendlabs-security-intelligence/patch-with-march-macos-updates-vulnerabilities-may-expose-restricted-information-enable-arbitrary-code-execution/.

100 Moony Li 與 Lilang Wu。(2019 年 6 月 21 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「CVE-2019-8635：Apple macOS 重複釋放記憶體漏洞讓駭客提升其系統權限並執行任意程式碼」(CVE-2019-8635: Double Free Vulnerability in Apple macOS Lets Attackers Escalate System Privileges and Execute Arbitrary Code)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-8635-double-free-vulnerability-in-apple-macos-lets-attackers-escalate-system-privileges-and-execute-arbitrary-code/.

101 Luis Magisa。(2019 年 9 月 20 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「Mac 惡意程式假冒交易應用程式，竊取使用者資訊並上傳至網站」(Mac Malware that Spoofs Trading App Steals User Information, Uploads it to Website)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/mac-malware-that-spoofs-trading-app-steals-user-information-uploads-it-to-website/.

102 Gabrielle Joyce Mabutas。(2019 年 11 月 20 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「可能與 Lazarus 集團有關的 Mac 後門程式瞄準韓國使用者」(Mac Backdoor Linked to Lazarus Targets Korean Users)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/trendlabs-security-intelligence/mac-backdoor-linked-to-lazarus-targets-korean-users/.

103 Eliya Stein。(2019 年 1 月 24 日)。*Confiant*。「Confiant 與 Malwarebytes 披露使用圖像隱碼術 (Steganography) 的廣告會在 Mac 使用者的電腦上植入 Shlayer 木馬程式」(Confiant & Malwarebytes Uncover Steganography Based Ad Payload That Drops Shlayer Trojan On Mac Users)。上次存取時間 2020 年 1 月 30 日：https://blog.confiant.com/confiant-malwarebytes-uncover-steganography-based-ad-payload-that-drops-shlayer-trojan-on-mac-cd31e885c202.

104 Taha Karim。(2019 年 9 月 25 日)。*Confiant*。「OSX/Shlayer 出新招... OSX/Tarmac 現身」(OSX/Shlayer new Shurprise.. unveiling OSX/Tarmac)。上次存取時間 2020 年 1 月 31 日：https://blog.confiant.com/osx-shlayer-new-shurprise-unveiling-osx-tarmac-f965a32de887.

105 Greg Young。(2019 年 8 月 8 日)。*趨勢科技 Simply Security 部落格*。「XDR 為何正夯，它與 SIEM 及所謂的「平台」又有何不同」(Why XDR Is A Big Deal, and Is Different from SIEM and Platforms)。上次存取時間 2020 年 1 月 25 日：https://blog.trendmicro.com/why-xdr-is-a-big-deal-and-is-different-from-siem-and-platforms/.

106 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 2020 年 2 月 7 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019.

107 Joey Chen、Hiroyuki Kakara 與 Masaoki Shoji。(2019 年)。*趨勢科技*。「Operation ENDTRADE：TICK 網路間諜集團利用多重階段後門程式攻擊不同產業並竊取機密資料」(Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data)。上次存取時間 2020 年 2 月 7 日：https://documents.trendmicro. com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

108 MITRE ATT&CK。(2018 年 18 月 4 日)。*MITRE ATT&CK*。「APT33」。上次存取時間 2020 年 1 月 25 日：https://attack.mitre.org/groups/G0064/.

109 Jonathan Andersson、Marco Balduzzi、Stephen Hilt、Philippe Lin、Federico Maggi、Akira Urano 與 Rainer Vosseler。(2019 年)。*趨勢科技*。「工業用無線射頻遙控器資安分析」(A Security Analysis of Radio Remote Controllers for Industrial Applications)。上次存取時間 2020 年 1 月 30 日：https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf.

110 Vladimir Kropotov 與 Fyodor Yarochkin。(2019 年 7 月 30 日)。*趨勢科技*。「在 Twitter 上追蹤威脅：如何運用社群媒體來蒐集可採取行動的威脅情報」(Hunting Threats on Twitter: How Social Media Can Be Used to Gather Actionable Threat Intelligence)。上次存取時間 2020 年 1 月 30 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter.

111 Sean Park、Iqbal Gondal、Joarder Kamruzzaman 和 Jon Oliver。(2019 年)。*趨勢科技*。「生成模型惡意程式疫情爆發偵測」(Generative Malware Outbreak Detection)。上次存取時間 2020 年 1 月 30 日：https://documents.trendmicro.com/assets/white_papers/GenerativeMalwareOutbreakDetection.pdf.

112 Sean Park、Iqbal Gondal、Joarder Kamruzzaman 及 Leo Zhang。(2019 年)。*趨勢科技*。「採用時空同構動態特徵的一次性惡意程式爆發偵測」(One-Shot Malware Outbreak Detection Using Spatio-Temporal Isomorphic Dynamic Features)。上次存取時間 2020 年 1 月 30 日：https://documents. trendmicro.com/assets/white_papers/one-shot-malware-outbreak-detection-using-spatio-temporal-isomorphic-dynamic-features.pdf.

113 Dr. Spark Tsao。(2019 年 11 月 8 日)。*趨勢科技*。「利用預判式機器學習技術交叉關聯靜態與動態行為特徵，實現更快、更精準的惡意程式偵測」(Faster and More Accurate Malware Detection Through Predictive Machine Learning: Correlating Static and Behavioral Features)。上次存取時間 2020 年 1 月 30 日：https://www.trendmicro.com/vinfo/us/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.

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.com

TREND MICRO™ | research