瞬息萬變的常態

趨勢科技 2020 年度網路資安報告

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。

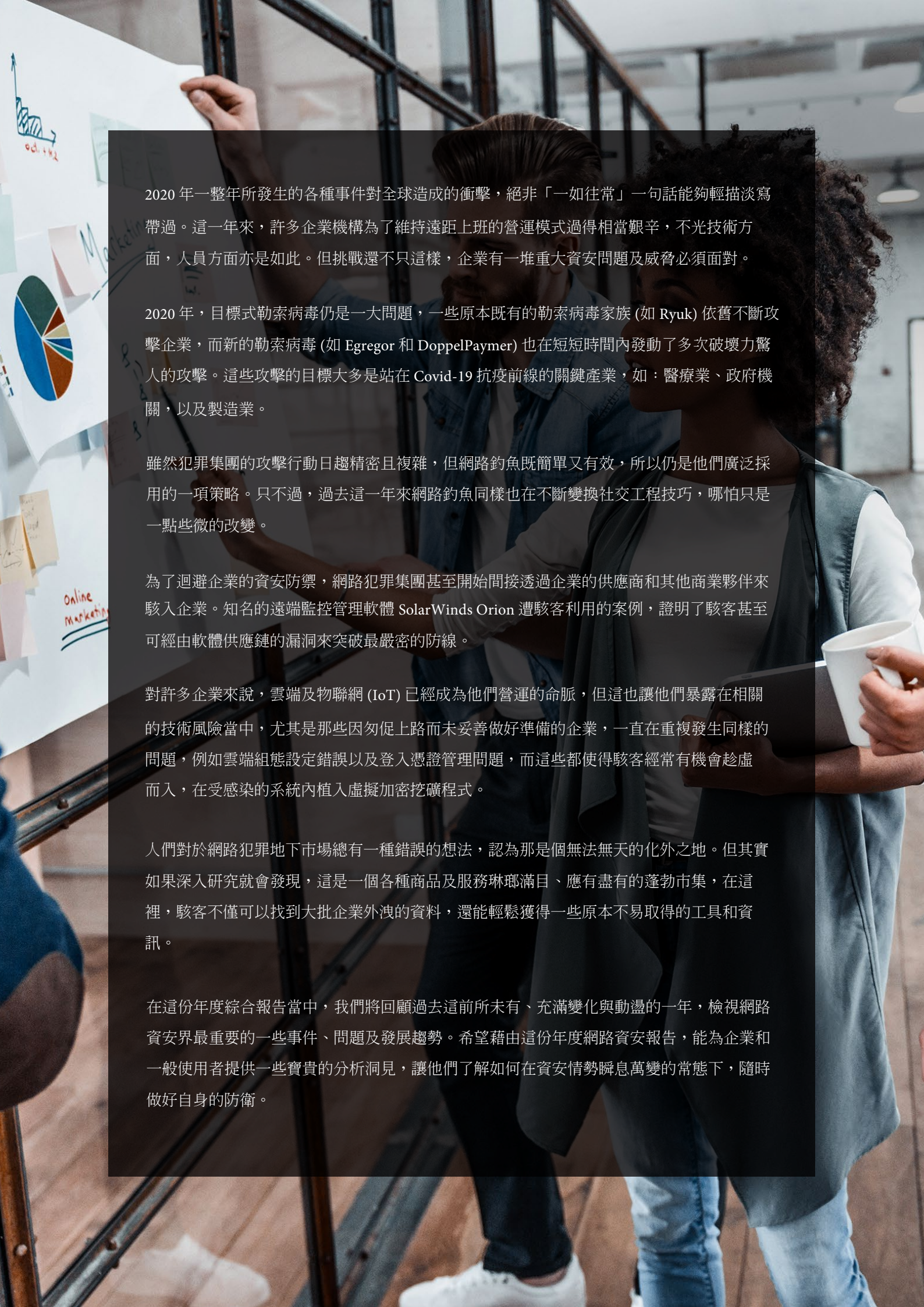
所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

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

內容



2020 年一整年所發生的各種事件對全球造成的衝擊，絕非「一如往常」一句話能夠輕描淡寫帶過。這一年來，許多企業機構為了維持遠距上班的營運模式過得相當艱辛，不光技術方面，人員方面亦是如此。但挑戰還不只這樣，企業有一堆重大資安問題及威脅必須面對。

2020 年，目標式勒索病毒仍是一大問題，一些原本既有的勒索病毒家族 (如 Ryuk) 依舊不斷攻擊企業，而新的勒索病毒 (如 Egregor 和 DoppelPaymer) 也在短短時間內發動了多次破壞力驚人的攻擊。這些攻擊的目標大多是站在 Covid-19 抗疫前線的關鍵產業，如：醫療業、政府機關，以及製造業。

雖然犯罪集團的攻擊行動日趨精密且複雜，但網路釣魚既簡單又有效，所以仍是他們廣泛採用的一項策略。只不過，過去這一年來網路釣魚同樣也在不斷變換社交工程技巧，哪怕只是一點些微的改變。

為了迴避企業的資安防禦，網路犯罪集團甚至開始間接透過企業的供應商和其他商業夥伴來駭入企業。知名的遠端監控管理軟體 SolarWinds Orion 遭駭客利用的案例，證明了駭客甚至可經由軟體供應鏈的漏洞來突破最嚴密的防線。

對許多企業來說，雲端及物聯網 (IoT) 已經成為他們營運的命脈，但這也讓他們暴露在相關的技術風險當中，尤其是那些因匆促上路而未妥善做好準備的企業，一直在重複發生同樣的問題，例如雲端組態設定錯誤以及登入憑證管理問題，而這些都使得駭客經常有機會趁虛而入，在受感染的系統內植入虛擬加密挖礦程式。

人們對於網路犯罪地下市場總有一種錯誤的想法，認為那是個無法無天的化外之地。但其實如果深入研究就會發現，這是一個各種商品及服務琳瑯滿目、應有盡有的蓬勃市集，在這裡，駭客不僅可以找到大批企業外洩的資料，還能輕鬆獲得一些原本不易取得的工具和資訊。

在這份年度綜合報告當中，我們將回顧過去這前所未有、充滿變化與動盪的一年，檢視網路資安界最重要的一些事件、問題及發展趨勢。希望藉由這份年度網路資安報告，能為企業和一般使用者提供一些寶貴的分析洞見，讓他們了解如何在資安情勢瞬息萬變的常態下，隨時做好自身的防衛。

目標式攻擊瞄準關鍵產業與最有利可圖的目標

勒索病毒犯罪集團瞄準最醒目的目標

我們經常看到，今日的勒索病毒攻擊已經不再像過去那樣採用投機性攻擊手法[1]。新式勒索病毒集團的犯案手法比以前更有章法，他們不再亂槍打鳥，而是瞄準一些關鍵產業中的高價值目標。此外，歹徒還會在攻擊中結合多種技巧，包括：攻擊尚未修補的漏洞、利用遠端桌面協定 (RDP) 的安全漏洞、在攻擊中使用其他惡意程式家族等等。

不但如此，過去企業機構只需擔心資料可能遭勒索病毒加密而無法使用，現在還得擔心萬一不遵照歹徒的要求乖乖支付贖金，資料還可能遭歹徒竊取並外流 (而且經常出現在爆料網站)[2]。

由於歹徒專門挑選高價值的重要目標，因此歹徒要求的贖金在過去幾年呈指數性翻漲。根據保險公司 Coalition 的資料，其被保險人遭歹徒勒索的金額，光 2019 至 2020 年第 1 季就翻了一倍[3]。

大家熟能詳的 Ryuk 和 Sodinokibi 就走在這波勒索病毒演化的最前端，可說是主宰了整個新式勒索病毒版圖。除此之外，也有一些相對較新的勒索病毒開始崛起，例如 Egregor 和 DoppelPaymer，兩者目前皆已占有一席之地，尤其在下半年期間。

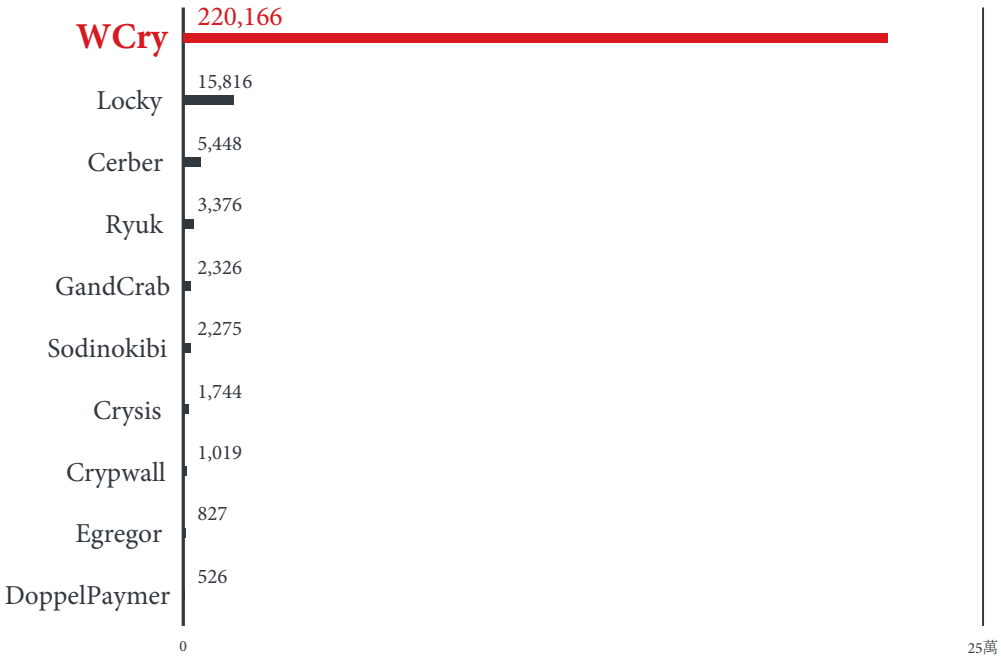


圖 1：Egregor 和 DoppelPaymer 勒索病毒雖然相對較新，但卻已擠進前 10 名：2020 年偵測數量最多的 10 大勒索病毒家族。

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

Ryuk 在 2020 年雖然沉寂了好幾個月，但仍是一些關鍵產業的惡夢，一開始就在 2 月份攻擊了美國政府承包商 Electronic Warfare Associates (EWA)[4]，隨後從 5 月至 9 月，Ryuk 都維持相對低調，直到接近年底的時候才又突然對醫療業發動一波波重大攻擊，甚至逼得美國網路資安與基礎架構安全局 (Cybersecurity and Infrastructure Security Agency，簡稱 CISA) 不得不針對它發出資安公告[5]。

Ryuk 向來習慣經由多重途徑散布，最常見的或許是利用其他惡意程式，例如：Emotet 和 Trickbot。除此之外也會使用某些工具程式，這些工具程式其實不算惡意程式，但卻經常被用於惡意用途，例如：滲透測試軟體 Cobalt Strike[6] 與 Metasploit[7]，以及漏洞攻擊後續輔助工具平台 PowerShell Empire[8]。事實上，許多這類工具都可被視為勒索病毒攻擊的前兆 (如果在初期偵測到的話)。

2020 年底，Ryuk 又增加了一項新的武器：一個名為「BazarLoader」(又稱「BazarBackdoor」) 的病毒植入程式，這是一個經由網路釣魚郵件內的附件或惡意網站連結散布的木馬程式[9]。雖然 BazarLoader 本身並不值得特別討論，但在犯罪集團不斷為 Ryuk 添加新功能的情況下，一些可能受害的產業在未來幾個月 (甚至幾年) 都應該特別提防勒索病毒攻擊。

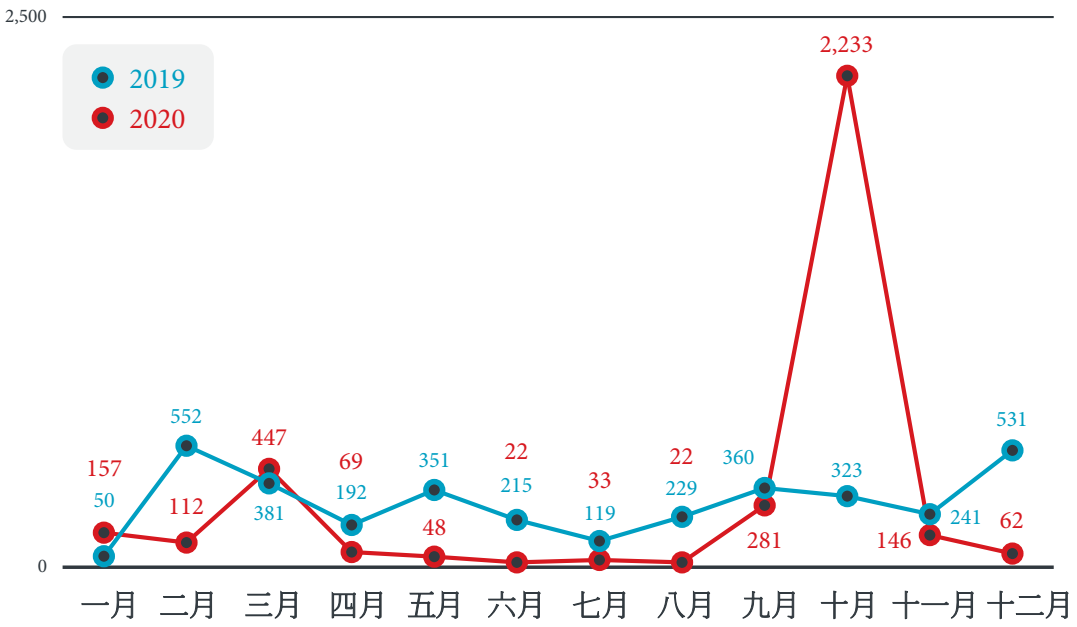


圖 2：Ryuk 的偵測數量在 2020 年 10 月突然飆高：2019 與 2020 年 Ryuk 偵測數量比較。

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

除了 Ryuk 之外，有幾個新出現的家族在 2020 年也讓人相當有感，其中較為著名的有 Nefilim 和 ColdLock，這些我們在 2020 上半年的網路資安報告當中已有詳細討論[10]。

Egregor 最早出現在 9 月，並在 12 月時針對大型零售業者發動一連串的重大攻擊[11]。Egregor 被認為有可能是從 Sekhmet 勒索病毒衍生而來[12]，因為兩者有某些共同點，此外也被視為是用來取代已退役的 Maze 勒索病毒[13]。Egregor 有一個特點是它通常隨著 Qakbot 遠端存取木馬程式 (RAT) 散布，這意味著，Egregor 和 Qakbot 背後的駭客集團之間可能有合作關係，不然就是 Egregor 其實是 Qakbot 幕後駭客集團最新採用的惡意程式[14]。

Egregor　也跟其他一些新式勒索病毒家族一樣採用雙重勒索的手法，換句話說，駭客會威脅受害機構如果不支付贖金的話就要將其資料公布在爆料網站上。面對資料外洩與資料損失的雙重壓力，受害者通常都會不得不屈服。

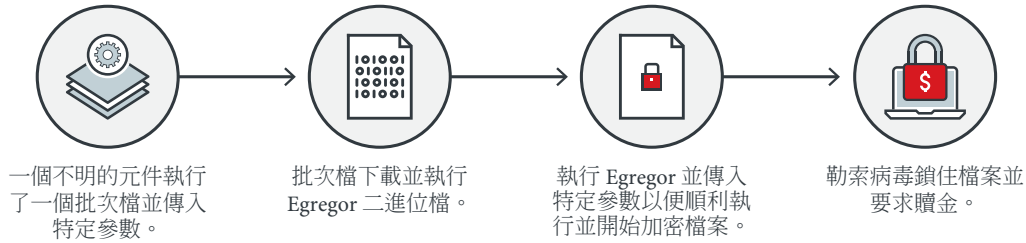


圖 3：Egregor 勒索病毒的攻擊過程。

另一個在 2020 年非常火紅的勒索病毒是 DoppelPaymer[15]。DoppelPaymer 雖然不是一個新的勒索病毒家族 (它從 2019 年即活躍至今)，但其活動卻在 2020 年底突然暴增，多到美國聯邦調查局 (FBI) 不得不發布公告來警告企業機構注意其攻擊[16]。

DoppelPaymer 據稱應該是衍生自 BitPaymer，一個專門攻擊醫療機構的舊式勒索病毒家族[17]，因為兩者在程式碼、勒索訊息、贖金支付管道方面都有相似之處。DoppelPaymer 還運用了一些進階的技巧，例如必須指定正確的指令列參數才能執行，這樣的作法應該是為了躲避資安專家的偵測及分析。此外也會使用一些像 Process Hacker 這樣的工具來停止一些服務和處理程序，避免在執行加密動作時發生存取被拒的狀況[18]。

DoppelPaymer 也像很多其他目標式勒索病毒一樣，以關鍵產業為主要攻擊對象，例如：醫療、緊急服務、教育機構等等。

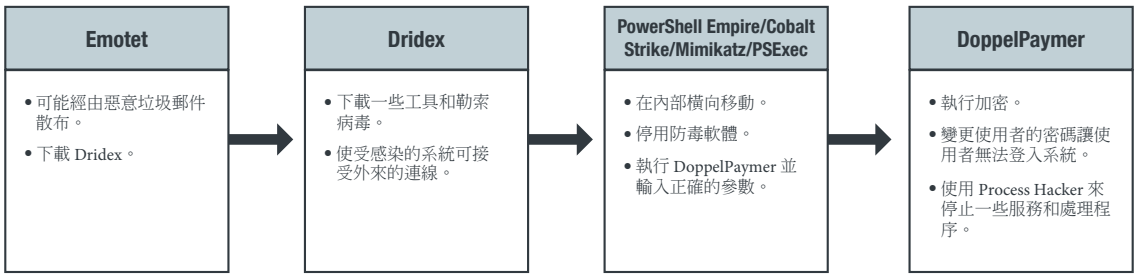


圖 4：DoppelPaymer 勒索病毒的感染過程。

從這些勒索病毒以及其他攻擊可以看出，勒索病毒集團已加強對政府及醫療等關鍵產業的攻擊力道，或許正因為這些是對抗 Covid-19 疫情的重要產業。此外，製造業同樣也是勒索病毒集團的主要目標[19]，光是一次勒索病毒攻擊，就可能為製造業受害企業帶來極其嚴重的後果，例如：營業或供應鏈中斷、產品開發設計延誤，甚至資料外洩。還有一個經常遭到攻擊的產業是銀行業，也許是因為這一行業的企業機構規模跟資金都非常龐大。

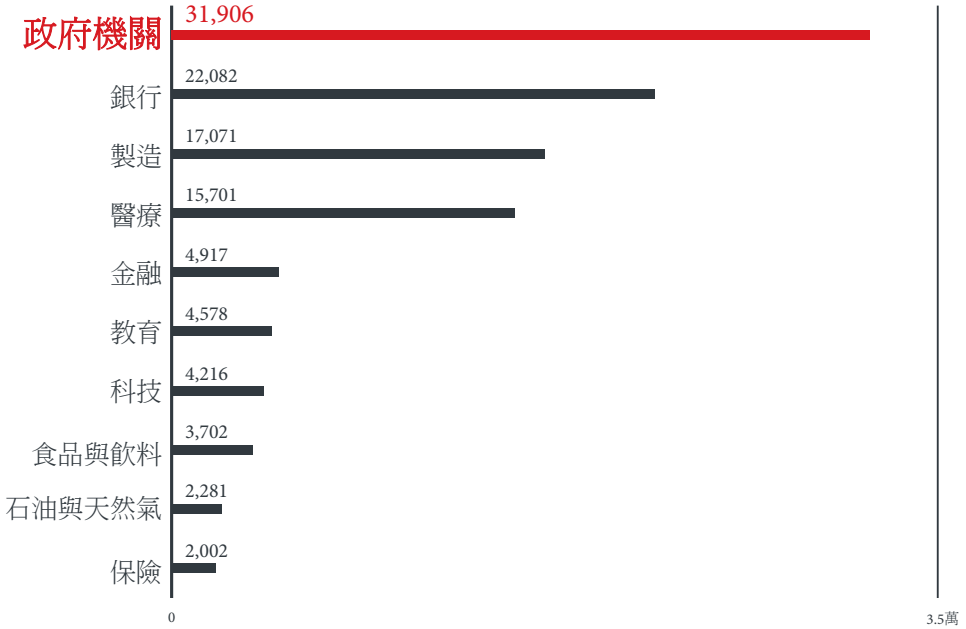


圖 5：政府、銀行、製造及醫療是遭受勒索病毒攻擊最嚴重的幾個產業：2020 年遭受勒索病毒攻擊最嚴重的 10 大產業。

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

除此之外，勒索病毒集團也將攻擊目標延伸到其他作業系統。例如，儘管 RansomExx 並未出現在 2020 年偵測數量最多的 10 大勒索病毒家族名單，但仍是一個相當值得關注的病毒，因為它的某個變種會攻擊 Linux 伺服器。根據我們的分析顯示，RansomExx 的主要攻擊目標是 VMware 的整體環境，也就是用來儲存 VMware 檔案的系統[20]。

駭客攻擊行動使用精密的工具和技巧瞄準特定族群

除了目標式勒索病毒攻擊之外，我們也觀察到不少來自新、舊駭客集團的其他攻擊行動。

從許多攻擊行動都有相當複雜的結構和程序可以看出，這些攻擊雖然很新，但幕後集團絕非新手。去年 10 月我們曾經針對一起名為「Earth Kitsune」的攻擊行動發表過研究報告，歹徒駭入了一些跟北韓有關的網站，並利用這些網站來散發惡意程式[21]。

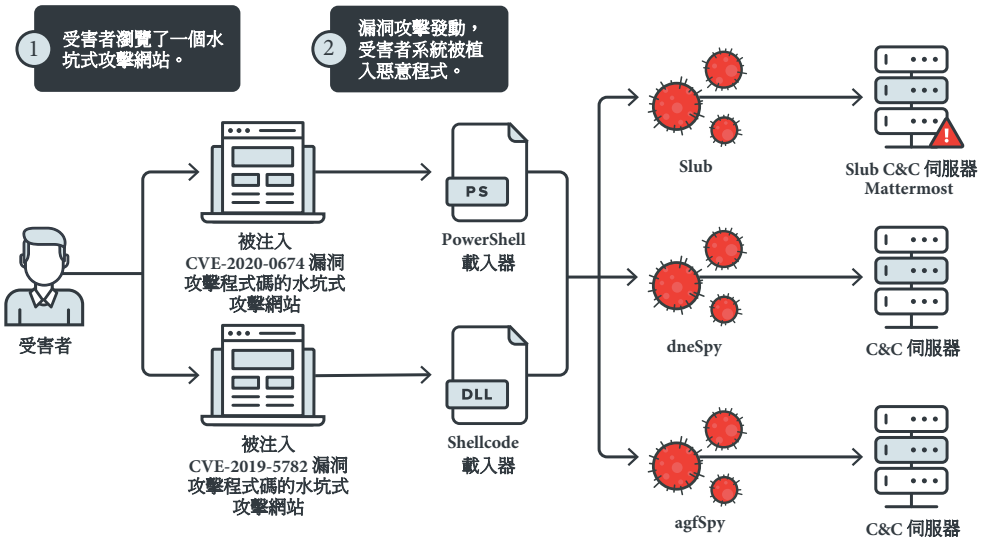


圖 6：Earth Kitsune 攻擊行動感染過程。

Earth Kitsune 運用了兩個漏洞來駭入目標網站：一個是 Google Chrome 的 CVE-2019-5782 漏洞，另一個是 Internet Explorer 的 CVE-2020-0674 漏洞。然後再搭配三個後門程式：Slub 用來將資訊傳送給駭客，agfSpy 和 dneSpy 則用來取得受害者電腦的控制權。

根據我們針對 Earth Kitsune 的追蹤研究顯示[22]，這是一起複雜而龐大的攻擊行動，結合了大型基礎架構與各式各樣的工具和漏洞攻擊手法。換句話說，這起攻擊行動並非由一般業餘人士所為，而是一群經驗跟技巧都相當豐富的高手，並且瞄準了特定的族群。

另一起我們持續追蹤的攻擊行動是「Earth Wendigo」[23]，這起攻擊與前者在主題和動機上非常相似。如同 Earth Kitsune 一樣，這起攻擊行動也是瞄準了一群特定對象，也就是那些關心西藏、新疆及香港局勢的人士，其背後的目的是要竊取使用者的信箱來獲取資訊。

Earth Wendigo 駭入系統的第一步是經由魚叉式網路釣魚郵件，郵件內含有經過加密編碼的 JavaScript 程式碼，然後再從遠端伺服器載入惡意腳本。這些腳本的用途五花八門，包括透過兩種方法來感染目標：第一種是利用網頁郵件系統的跨網站腳本 (XSS) 漏洞，第二種是利用一個名為「Service Worker」的瀏覽器功能來註冊一段惡意的 JavaScript 程式碼。在橫向移動手法部分，這起攻擊是利用惡意程式碼注入手法來修改受害者的電子郵件。

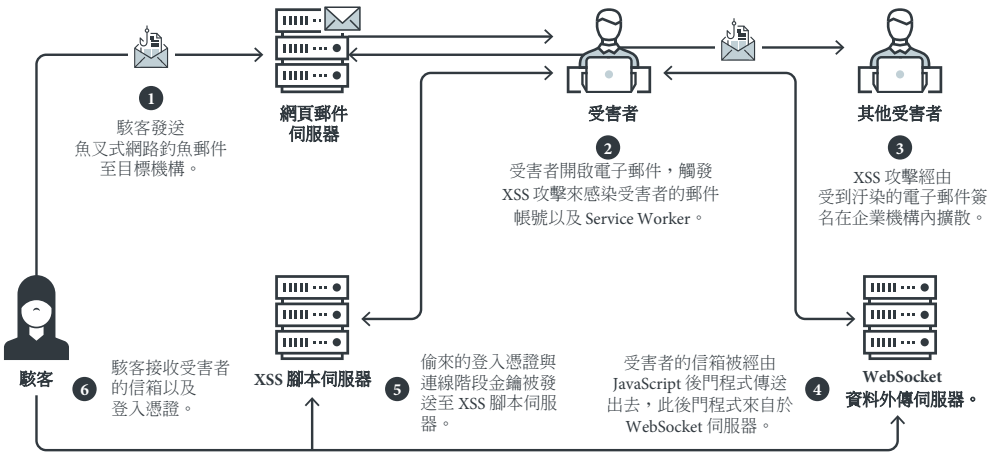


圖 7：Earth Wendigo 攻擊行動的流程。

除了這些新興駭客集團的攻擊行動之外，向來以南亞地區為主要活動範圍的 SideWinder 駭客集團，我們也追蹤到一些他們的活動。該集團在 2020 年尤其活躍，專門利用 Covid-19 相關或是涉及南亞與中國的區域紛爭以及其他外交問題的議題來發動魚叉式網路釣魚攻擊[24]。這就是 SideWinder 的主要社交工程技巧，利用熱門時事來引誘受害者瀏覽網路釣魚網頁。

由於攻擊行動日趨複雜，駭客集團也不得不開始向外尋求一些其他工具和服務作為輔助。正如我們在去年發表的一份研究報告中指出，地下市集正提供一種所謂的「存取服務」(access-as-a-service)，目前已成為網路犯罪集團入侵目標系統的一種熱門工具，這類服務專門提供一些被駭裝置與企業網路的存取權限。這些存取權限還分成各種不同等級，從單純的帳號登入憑證到整個網路的遠端桌面 (RDP) 存取權限等等[25]。Ryuk 勒索病毒集團就是這類服務的愛用者之一，此外他們還會利用他人的惡意程式 (如 Trickbot) 來進出被感染的網路[26]。

歹徒使用簡單有效的技巧

除了像 Earth Kitsune 和 Earth Wendigo 這類由技巧高超的駭客集團所發動的攻擊之外，我們發現，有些駭客集團比較偏愛單純的手法。

例如在 2004 年初試啼聲的 Pawn Storm 駭客集團，一現身便對一些重要產業造成了不小的破壞[27]，但到了 2020 年，Pawn Storm 仍不像其他駭客團體那樣紛紛採用日益複雜的攻擊策略，反而在一些攻擊行動當中選擇了較為簡單的技巧。他們會使用一些相當基礎的技巧 (如暴力登入) 來攻擊一些網際網路上的服務，

以及像 RAT 這類常見的工具[28]。事實上，要不是我們對於 Pawn Storm 所用的工具和技巧相當熟悉，否則光從我們分析到的樣本，其實很難將攻擊行動跟他們聯想在一起。

然而，技巧簡單並不意味著就因而遜色，網路釣魚就是一個很好的例子，它可說是最古老的一種詐騙技巧，但至今仍非常有效。骨子裡，網路釣魚是一種非常單純的技巧，駭客不需擁有任何技術背景或知識就能運用網路釣魚技巧，一切都只需對人性的深刻認識以及某種形式的社交工程技巧。

話雖如此，網路釣魚技巧也絕非一成不變，應該說，它們其實隨時都在演進。一個很好的例子就是我們在 2020 年所觀察到的一項趨勢：歹徒利用表單製作服務來建立網路釣魚網站 (例如問卷調查)[29]。

這類表單製作網站對歹徒的主要吸引力是，它們不像建立假冒網域或網站那麼複雜，只需具備一些基本的表單製作知識再花點時間即可。雖然利用這類表單製作服務所製作的網頁通常看起來不太專業，無法跟那些從無到有特別精心製作的假網域相比，不過卻能讓一些想要從事網路犯罪卻毫無經驗的人也能輕鬆製作出可用的網路釣魚網頁。所幸，大多數的企業機構並不會使用表單來執行一些重要的流程 (例如密碼更新或電子郵件認證)，所以這類表單式網路釣魚詐騙對於使用者來說應該不難識破。

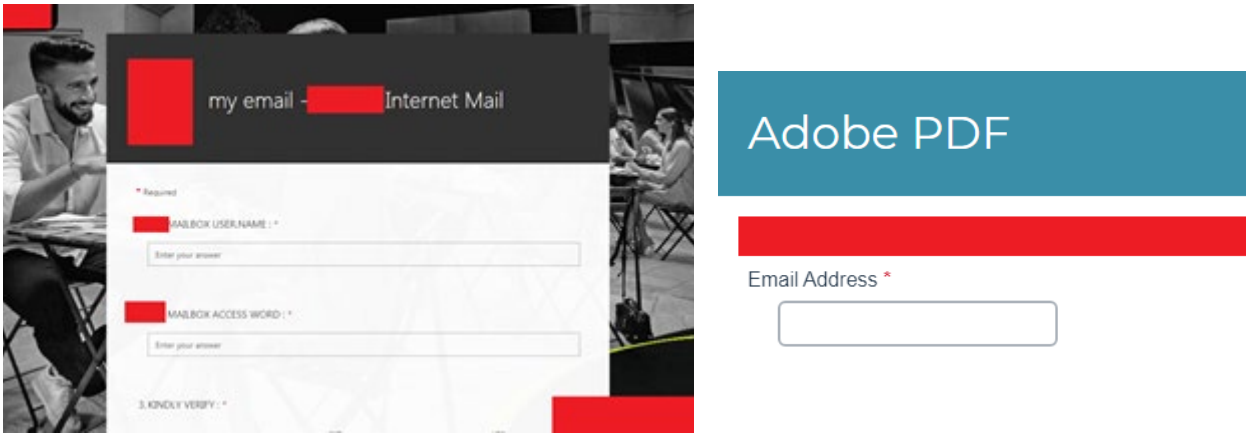


圖 8：使用表單製作的網路釣魚網頁範例：電子郵件登入憑證網路釣魚表單 (左) 以及假的 Adobe 登入畫面 (右)。

在比對過我們手上不同年度的網路釣魚偵測資料之後，我們發現了一項有趣的變化。雖然已攔截的「可重複」網路釣魚網址數量減少，但已攔截的「非重複」網路釣魚數量卻增加。其中一個原因就是，歹徒已經較少重複使用他們的網路釣魚網址，而是會針對攻擊目標另外產生特製的網址。

圖 9：已攔截的「非重複」網路釣魚網址數量增加，「可重複」的網路釣魚網址減少：2019 與 2020 年已攔截的「非重複」網路釣魚網址比較 (同一台電腦若試圖存取同一個網址三次則只算一次) 以及已攔截的「可重複」網路釣魚網址比較 (同一個被攔截的網址若被存取三次仍算三次)。

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

此外我們也發現，在已攔截的網路釣魚網址當中，假冒 Microsoft 365 (原 Office 365) 的案例從 2019 至 2020 年減少了 38%，這是全球使用最廣泛的辦公室生產力軟體之一，其中也包含了熱門的 Outlook 電子郵件軟體。不過，這不應視為歹徒已減緩攻擊力道的徵兆，有可能是因為歹徒試著擴大版圖，將目標轉移到了其他辦公室必要的工具，例如即時通訊軟體。

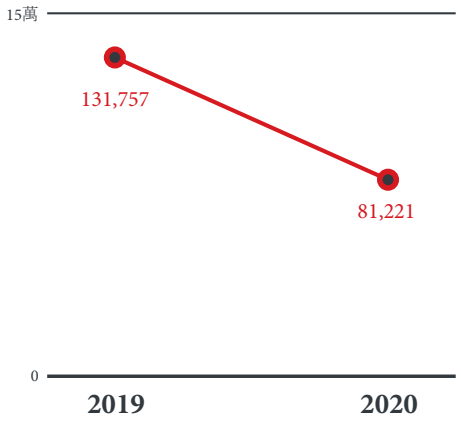


圖 10：假冒 Microsoft 365 (含 Outlook) 的「非重複」網路釣魚網址數量減少 38%：2019 與 2020 年已攔截的「非重複」Microsoft 365 相關網路釣魚網址比較。

註：資料中包含了 Office 365 相關的查詢。

資料來源：趨勢科技網站信譽評等服務。

根據我們的資料顯示，10 大網路釣魚網域每個都累積了超過一百萬次的嘗試存取記錄，證明了歹徒誘騙受害者上當的功力驚人。此外，若就「非重複」使用者的嘗試存取數量來看，這些排行榜上的網域也累積高達數十萬的非重複使用者。

網址	數量
clk.apxadtracking.net	27,722,234
apc994.com	5,558,410
157.240.2.20	4,667,619
p01.notifa.info	3,185,011
api.bdisl.com newgirlseveryday.info	2,441,834
lopw.page.link	1,831,524
kolw.page.link	1,778,225
johr.page.link	1,751,821
firebasestorage.googleapis.com	1,737,865
	1,710,295

表 1：網路釣魚 10 大網域的使用者嘗試存取記錄每個都上百萬，光第一名本身就累積了 2,700 萬次以上「可重複」的嘗試存取記錄：2020 年已攔截的「可重複」嘗試存取次數最高的 10 大網路釣魚網址 (同一個被攔截的網址若被存取三次仍算三次)。

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

網址	數量
www.vrspacely.com	241,022
apc994.com peachtrackercn.com	217,267
clk.apxadtracking.net	214,550
p01.notifa.info	167,951
api.dot-metrix.com	119,762
qwertyamerica.com	119,148
api.bdisl.com	116,230
sw.wpu.sh	116,201
d11yldzmag5yn.cloudfront.net	101,121
	97,498

表 2：就非重複的電腦數量來看，已攔截的網路釣魚網域嘗試存取次數在數十萬之譜：2020 年已攔截的「非重複」嘗試存取次數最高的 10 大網路釣魚網址 (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。

歹徒不斷經由供應鏈滲透企業

歹徒要直接攻破防禦嚴密的機構 (例如擁有極機密資料的政府機關) 不是一件容易的事，但歹徒可採用迂迴的方式試圖入侵這些機構的供應商 (因為防禦較弱)，進而間接攻擊得逞。

像這樣的供應鏈攻擊，駭客基本上就是利用企業機構與外部供應商之間的彼此信賴來入侵目標系統。這樣的攻擊非常難防，也不易偵測，原因除了企業機構大多假設供應商夥伴的產品與服務安全無虞之外，企業通常也沒有辦法主動檢查其供應鏈所暗藏的威脅，只能監控自己的系統。

2020 年由於供應鏈攻擊實在過於猖狂，美國 FBI 還特別在 2 月份發出一份資安警示，特別提到供應鏈攻擊會瞄準一些軟體公司，目的是為了駭入使用這些軟體的機構，例如採用工業控制系統的能源產業[30]。這類攻擊可透過一個名為「Kwampirs」的遠端存取工具 (RAT) 來掌控受害者的系統與網路，進一步從事其他後續行動，例如植入更多惡意元件與檔案[31]。

近年來最知名的一起供應鏈攻擊就是 SolarWinds 事件。2020 年 12 月，媒體開始陸續報導一項專門針對特定機構 (包括美國政府機關) 的精密攻擊，這項攻擊駭入了 SolarWinds 公司旗下知名 Orion 網路監控管理軟體的某次更新[32]。由於某些受害的機構相當敏感，因此可能造成深遠的影響。

根據 SolarWinds 公司所提供的資訊，駭客在某些 Orion 軟體版本當中植入了一個漏洞，好讓他們能夠入侵使用這些 Orion 軟體的伺服器[33]。換句話說，這些遭篡改的軟體更新一旦推送到客戶端，駭客就能在受害的系統上植入一個強大的後門程式，也就是「Sunburst」。一旦 Sunburst 進入系統，駭客就能隨意進出受害的網路，接著，駭客可執行一些指令來蒐集系統資訊、寫入或刪除檔案、建立或刪除系統登錄機碼、停用系統分析工具，以及其他惡意活動等等。除此之外，攻擊的第二階段還會出現一個名為「Supernova」的後門程式。駭客會使用 Supernova 來監控網路上的 HTTP 請求，然後回應適當的 HTTP 查詢字串、HTML 表單數值與 Cookie，並且利用一個特殊的 HTTP 請求格式來執行網站指令 (web shell)[34]。

Covid-19 與遠距上班造成網路資安大變革

歹徒利用全球疫情與其他重大事件

美國 2020 年選舉是駭客大肆利用的重要事件，尤其是總統選舉，他們趁著選舉的熱度來從事各種相關詐騙[35]。而且，不只一般默默無名的網路犯罪集團看上了選舉，就連一些大型進階持續性滲透攻擊 (APT) 駭客集團也盯上了總統候選人主要陣營的相關人員和單位，以及一些政治宣傳團體[36]。

除此之外，談到 2020 年的網路資安情勢，就不得不談 Covid-19 全球疫情所帶來的影響。如同我們 2020 上半年網路資安報告所云，歹徒趁著疫情期間製造了大量 Covid-19 相關的威脅[37]。

2020 年，我們偵測到 1,600 萬次 Covid-19 相關的威脅，包括：惡意網址、垃圾郵件及惡意程式，其中將近 90% 是惡意垃圾郵件。這表示垃圾郵件是歹徒的最愛，原因或許是垃圾郵件較容易取得也較為簡單，不像製作惡意網址和惡意程式需要一點技術背景和規劃。偵測數量最多的前三個國家分別是：美國、德國和法國，而這也是新冠病毒疫情最嚴重的國家。

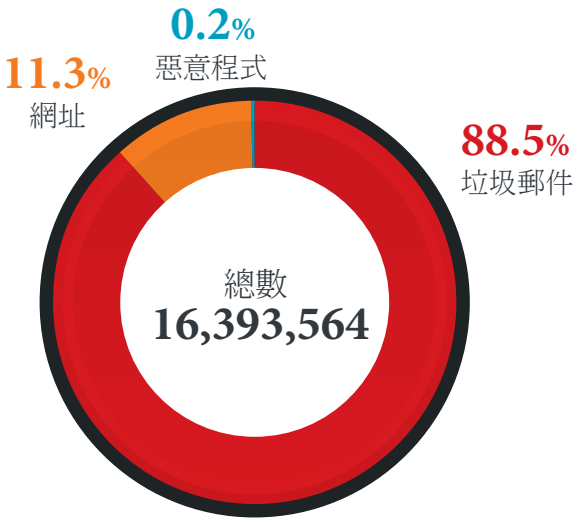


圖 11：在所有偵測到的 Covid-19 相關威脅當中，有將近 90% 是惡意垃圾郵件：2020 年 Covid-19 相關威脅分布狀況 (依類型)。

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

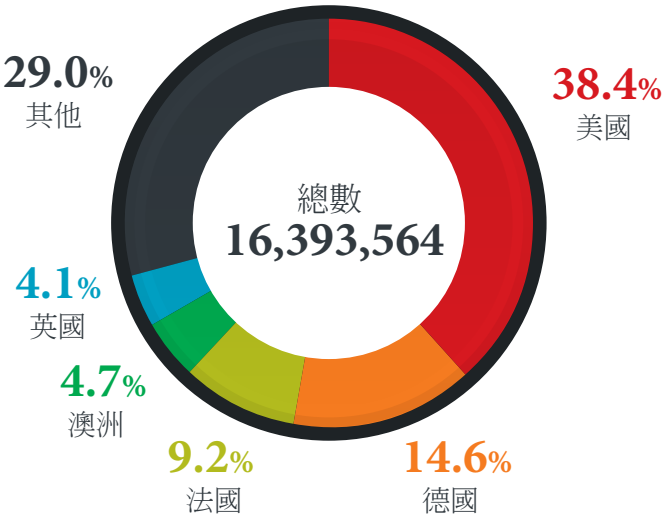


圖 12：絕大多數偵測到的 Covid-19 相關威脅都分布在美國、德國和法國：2020 年 Covid-19 相關威脅分布狀況 (依國家)。

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

上半年，Covid-19 相關威脅的主要手法是製造收件人的恐慌，或宣稱提供疫情相關資訊，例如，許多早期的垃圾郵件內容都是有關發病的症狀[38]。

而這些威脅背後的垃圾郵件集團會根據最新的發展和消息來調整技巧。比方說，當美國政府最初提供的一

波 Covid-19 經濟刺激方案申請即將截止[39]，歹徒便趁著人們對截止日期心急如焚的心情散發誘騙簡訊，表示他們已獲得補助，試圖讓受害者上當。簡訊內提供了一個連結指向一個專門騙取個人資料與金融資訊的網路釣魚網頁[40]。

另一個重大的發展是各大藥廠在下半年紛紛推出第一批 Covid-19 疫苗。而網路犯罪集團也正如預期迅速跟進，推出疫苗相關的詐騙。有些歹徒以大小不等的金額販售假疫苗，甚至架設專門的網域 (有些甚至暗藏惡意程式) 來誘騙受害者上當[41]。其他詐騙集團則是散發網路釣魚郵件，發送對象不僅包含一般大眾，而且還包含在疫苗供應鏈工作的人員[42]。

毫無意外地，變臉詐騙 (BEC) 集團也趁著這波疫情作亂， 而以 Covid-19 為主旨的郵件占所有變臉詐騙樣本的最大宗。許多郵件的主旨意義含糊，甚至與疫情毫不相干，例如提供發票或請求付款，但即使是這類郵件，也會想辦法利用「Covid」或「Covid-19」的字樣來吸引受害者注意。

“Re: COVID-19”
“Re: Covid-19 update”
“COVID-19 QUICK REPLY”
“Important Message on COVID-19”
“COVID-19...Fwd: April Invoices”
“COVID-19 Shut down”
“COVID-19 issue”
“COVID-19...Fwd: May Invoices”
“Fwd: Covid-19 update”
“Re: Covid positive donors”
“COVID-19 RESPOND”
“COVID-19/FluA+B Antigen Combo Rapid Test”
“Covid Task Force”

表 3：2020 年變臉詐騙郵件用到的一些 Covid-19 相關主旨範例。

整體而言，2020 年偵測到的變臉詐騙攻擊數量較 2019 年減少 17%。

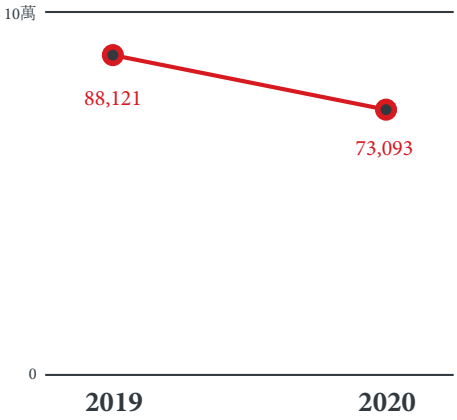


圖 13：雖然變臉詐騙攻擊整體數量減少，但變臉詐騙集團卻趁著 Covid-19 疫情作亂：2019 與 2020 年偵測到的變臉詐騙數量比較。

註：這項資料代表偵測到的變臉詐騙所有攻擊案例，不論攻擊成功與否。

執行長 (CEO) 與董事總經理/協理 (Managing Director/Director) 仍是最常被變臉詐騙假冒的職務，兩者加起來占所有案例的半數以上。至於變臉詐騙的目標，財務經理 (Finance Manager) 和財務總監 (Director of Finance) 依然是最常被詐騙的對象，兩者加起來占了將近所有攻擊案例的三分之一。至於第三名則是教授，顯然針對教育機構的詐騙依然相當猖獗。

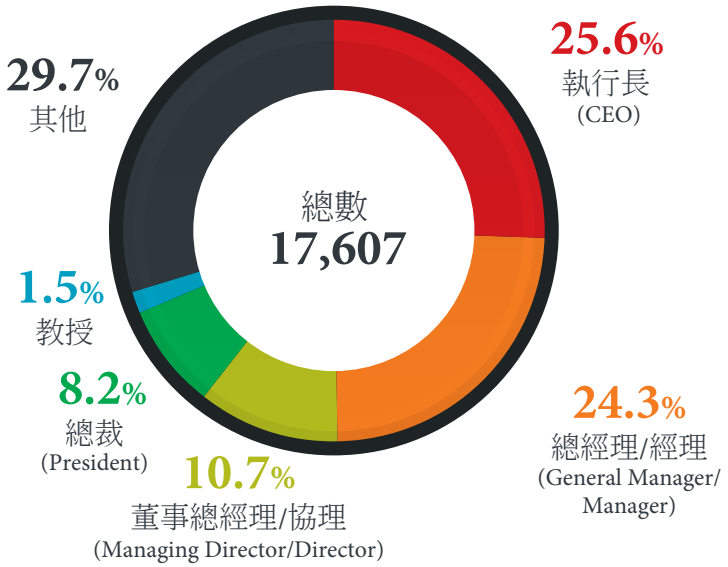


圖 14：執行長依然是變臉詐騙最常假冒的職務對象，緊跟在後的是董事總經理/董事：2020 年變臉詐騙假冒的職務對象分布。

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。

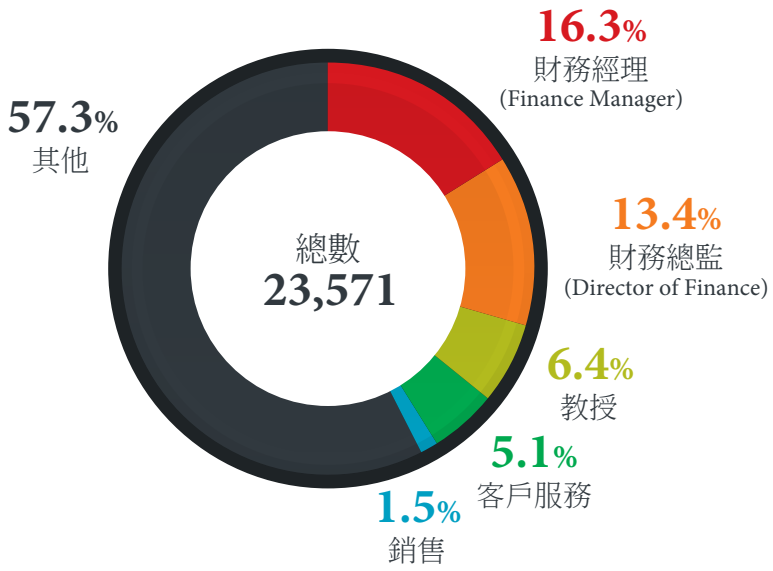


圖 15：財務經理、財務總監、教授是最常被變臉詐騙攻擊的對象：2020 年變臉詐騙攻擊目標分布情況。

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。

變臉詐騙的一項重要特點就是，歹徒不需要複雜的基礎架構就能成功發動變臉詐騙攻擊。詐騙集團甚至可採用公共的公有雲基礎架構，例如 Water Nue 變臉詐騙攻擊。這波攻擊最早始於 2020 年 3 月，專門瞄準美國和加拿大企業機構的資深高階主管，騙取他們的帳號登入憑證之後從事進一步的惡意活動。他們的帳號一旦被盜，歹徒就會假冒他們名義要求下屬匯款給歹徒。Water Nue 犯罪集團使用了像 SendGrid 這類的合法雲端電子郵件服務來散發電子郵件。雖然這聽起來很像是典型的變臉詐騙手法，但除了使用雲端服務之外，卻沒有其他值得注意的特徵。在我們進行分析的期間，Water Nue 攻擊行動前後搜刮了超過 800 筆登入憑證，這顯示就連看似平凡的變臉詐騙也可能造成嚴重損害[43]。

除此之外，2020 年我們也發現了一種以法國企業為目標的新式犯案手法，網路犯罪集團假冒法國稅務機關的名義散發稅務詐騙電子郵件，其目的是蒐集受害者的資訊。其電子郵件當中隨附的 PDF 信件內容看起來相當真實 (因為歹徒使用了稅務機關所用的 PDF 檔為基礎來製作假冒的 PDF)，而且這封郵件的寄件地址也跟法國稅務機關的官方郵件地址長得很像。詐騙集團蒐集到所要的資訊之後，就會發送詐騙郵件給受害機構的客戶，要求更改收款人銀行帳號，讓客戶將錢匯到歹徒指定的帳號[44]。

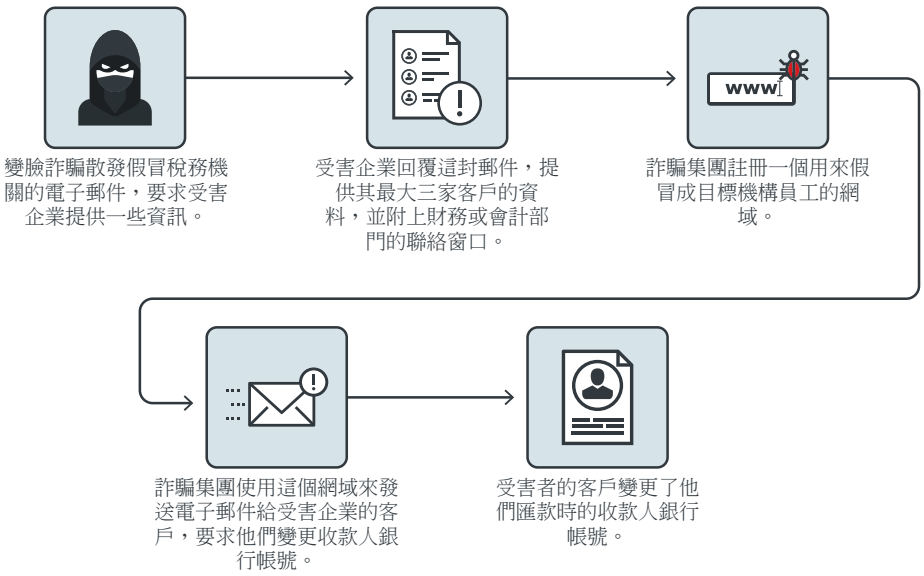


圖 16：2020 年法國變臉詐騙攻擊的犯案手法。

遠距上班為企業機構帶來各種挑戰

新冠肺炎疫情迫使大量企業機構開始從傳統的辦公室環境轉變成遠距上班模式。雖然遠距上班對企業機構及員工來說都有好處，例如可減少基礎架構支出以及通勤成本，但遠距上班也並非全無挑戰，尤其是網路資安方面的挑戰。

儘管有些企業機構或許在疫情爆發之前就已經實施了某種遠距上班措施，但要讓絕大多數的員工都改用遠距上班，意味著企業必須對其關鍵系統進行一番壓力測試，以確保即使在業務最繁忙時也能有效運作[45]。不僅如此，企業機構還必須確保員工都擁有能讓他們順利在家上班的各項支援措施及教育訓練。此外，企業該注意的還有基礎架構，為了消除資安漏洞，企業需要建置或強化一些資安措施來協助遠距上班員工確保家庭工作環境的安全。

也正因如此，虛擬私人網路 (VPN) 已成為企業保護網路連線以防止外部威脅入侵不可或缺的工具。事實上，在全球這股在家上班的風潮支撐下，VPN 的使用率在 2020 年創下了歷史新高[46]。

很重要的一點是，VPN 並非一項萬能的資安技術，VPN 也可能遭到駭客利用，變成他們的網路攻擊工具。就像任何軟體一樣，VPN 軟體也可能存在著各種漏洞，一旦遭到利用，就可能成為駭客入侵系統的管道。

一個最重要也最普遍的 VPN 漏洞就是 CVE-2019-11510，這是 VPN 軟體 Pulse Connect Secure 存在的一個重大的檔案外洩漏洞，經由這項漏洞，遠端駭客就能取得目標系統的使用者名稱與純文字密碼[47]。儘管 CVE-2019-11510 是一個新發現的漏洞，但光 2020 年就已經偵測到將近 80 萬次利用此漏洞的攻擊，而且已經出現實際攻擊案例，2020 年還曾被用於散播 Sodinokibi 勒索病毒[48]。

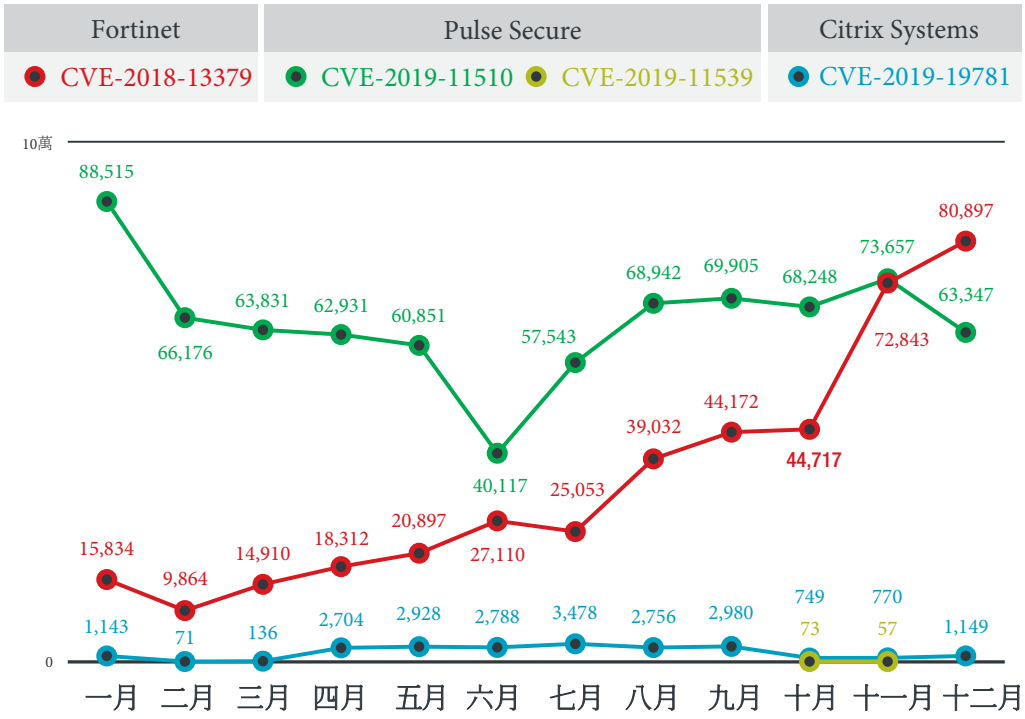


圖 17：CVE-2018-13379 偵測數量在第 4 季突然飆升，但 CVE-2019-19781 的情況剛好相反；Pulse Secure 漏洞 (CVE-2019-11510) 攻擊每月的偵測數量大致維持不變；2020 年知名 VPN 漏洞攻擊偵測數量逐月比較。

資料來源：趨勢科技 Digital Vaccine 數位疫苗過濾規則。

除了漏洞攻擊之外，駭客集團也發現了其他攻擊 VPN 的方式。2020 年 9 月，我們發表了一份事件分析報告指出，駭客在某個 VPN 軟體的安裝程式中植入了 Bladabindi 後門程式，讓駭客可從被感染電腦的蒐集資訊[49]。這樣的案例告訴我們，除了定期更新 VPN 軟體以修正所有已知漏洞之外，使用者還要特別留意自己 VPN 軟體的下載來源。

隨著遠距上班逐漸蔚為風潮，人們也越來越仰賴像 Zoom、Slack 和 Discord 這類會議通訊軟體，因而使得針對這類軟體或使用這類軟體的攻擊越來越多[50]。

例如「Zoom 轟炸」(Zoombombing) 就是一例，這是一種 Zoom 會議在進行當中遭陌生人亂入的情況，這是會議通訊軟體常見的攻擊之一。雖然 Zoom 轟炸有時會大大干擾會議的進行，但其實並無法造成太大破壞，頂多就是惱人的惡作劇而已。不過還有其他更具破壞性的 Zoom 相關攻擊，有些犯罪集團會在合法的 Zoom 安裝程式中植入惡意程式，或者明明就是惡意程式卻偽裝成 Zoom 安裝程式，目的就是要引誘使用者在電腦上安裝各種惡意程式[51]。

除了 Zoom 之外，Slack 和 Discord 也經常成為網路犯罪集團作案的工具。其中一個就是 Crypren 勒索病毒，它會利用一種獨特的方式，經由 Slack 的 webhook 將受害者的加密狀態傳送回自己的 C&C 伺服器。此外根據我們發現到的樣本指出，歹徒還會使用 Discord 來散發垃圾郵件並夾帶惡意程式，試圖感染受害者的電腦[52]。

企業面臨雲端、物聯網 (IoT) 及行動環境的威脅

雲端組態設定錯誤仍是許多企業都存在的一項問題

2020 年讓雲端變成了許多企業機構營運更不可或缺的一環，根據趨勢科技所做的 2020 年「網路資安風險指標」(Cyber Risk Index，簡稱 CRI) 顯示，雲端運算基礎架構及雲端供應商是企業最擔憂的主要領域[53]。

雲端確實已經變成企業維持正常營運的重要基石，這樣的情況在採用遠距上班的企業更加明顯。雲端式服務能為企業帶來不少效益，尤其在成本效率、靈活性及擴充性方面。不過，如果以為採用了雲端之後企業就不需操心資安問題的話，那就大錯特錯。雲端防護本身也有其特殊的挑戰[54]，雲端基礎架構當中經常被忽略的一環就是雲端資產及服務的組態設定是否正確，也正因如此，組態設定錯誤至今仍是雲端環境的一項主要風險。2020 年所見的許多事件主要都是因為雲端軟體與基礎架構組態設定錯誤所致。

傳統上，駭客會使用漏洞攻擊手法來執行遠端程式碼，這是他們入侵目標系統的一個關鍵步驟。但在過去這一年我們所觀察到的某些資安事件中，駭客反而是攻擊一些開放的 API 。在 4 月份發生的一起攻擊中，駭客經由一些組態設定不當的 Docker daemon API 連接埠，使用以 Golang 程式語言撰寫的 Golang 惡意程式在系統上植入虛擬加密貨幣挖礦程式。這就是 Kinsing 惡意程式，它最知名的能力之一就是利用 Rootkit 來隱藏惡意元件，使得受害使用者更難偵測它的活動[55]。

一個月後，我們分析了駭客團體 TeamTNT 所開發的一個殭屍程式 (bot)，該程式可執行挖礦作業並可用於發動分散式阻斷服務攻擊[56]。此殭屍程式的主要攻擊目標同樣也是開放的 Docker daemon 連接埠。

快年底的時候，我們觀察到越來越多該集團的惡意活動，而其攻擊手法也不斷持續演進。12 月份，該集團增加了自我散布能力，以及竊取 Amazon Web Services (AWS) Secure Shell (SSH) 登入憑證的能力[57]。然而，要不是被感染的系統本身就存在著某種組態設定錯誤或其他資安漏洞的話，這些攻擊都不可能發生。這些案例當中，駭客都是利用組態設定錯誤、失竊或強度不足的登入憑證，或是軟體漏洞，才有辦法在受害系統上執行遠端程式碼。

我們在 10 月份曾經披露某起因為 Docker API 暴露在網路上而遭受攻擊的案例，這起攻擊運用了 Metasploit Framework (MSF) 的 shellcode 作為惡意程式，這是我們第一次看到這樣的攻擊手法[58]。此案例之所以值得注意，是因為通常 Docker API 暴露在外而遭到攻擊的案例都是被植入挖礦程式。

網路犯罪集團利用地下市場雲端基礎架構

諷刺的是，雲端服務所帶來的效益，受惠的並非只有企業機構，根據我們的研究顯示，2020 年犯罪集團也在大量使用雲端服務。

網路犯罪地下市場上，犯罪集團之間經常會彼此互通有無、互相交易。有時候，犯罪集團之間甚至會聯合行動，例如，某個集團或某名駭客負責入侵受害者的系統，另一個集團負責提供 C&C 基礎架構，並且將地下服務商品化。而地下市場上販賣的雲端服務也是琳瑯滿目，從單純的主機代管服務到一些非常特殊的服務，例如行動裝置工作空間與電信服務，這些都是犯罪集團平常攻擊時會用到一些服務[59]。

最近我們看到一些資料遭網路犯罪集團竊取的攻擊事件，像這樣的攻擊事件，歹徒所竊取的資料通常會多到自己沒辦法完全消化利用，所以，犯罪集團就會將偷來的資料放到雲端供其他犯罪集團付費存取，這就所謂的「記錄雲」(Clouds of Logs)[60]。

這類資料服務的收費方式還會依存取等級的不同而有不同定價，其所提供的資料種類也是包羅萬象，最常見的是個人身分識別資訊 (PII)、各種雲端服務的使用者登入憑證，以及信用卡資訊。

圖 18：地下市場上販售的資料價格不等，甚至有 900 美元「終生吃到飽的會員制」。

對於網路犯罪集團來說，這類資料服務的主要好處之一是他們不需建構複雜的基礎架構就能獲得海量的資料。而這些資訊唾手可得的結果，也讓駭客變得更加敏捷且更有效率。尤其是目標式攻擊，歹徒不必再花費大量時間和精力來蒐集資料，就能找到想要的資訊。

隨著這類服務的經營模式不斷改善及演進，我們預料企業機構的資料外洩風險將越來越高，尤其有了這樣的服務之後，從資料外洩到歹徒利用資料發動攻擊的時間差將變得更短。

針對 IoT 裝置的攻擊越來越多

除了雲端之外，IoT 在許多企業轉型至遠距上班的過程當中也扮演了關鍵的角色，這一點，犯罪集團當然也注意到了。

正如我們的 2021 年資安預測報告所言，當犯罪集團在試圖尋找駭入目標機構的途徑時，家用網路將逐漸成為他們關注的焦點[61]。家用網路及裝置一旦遭到入侵，就可能成為歹徒攻擊其他裝置的跳板，幫助他們攻擊最終目標，駭入與這些裝置連接的企業網路。其中，家用路由器尤其容易遭到駭客的攻擊，因為員工

家用網路的安全性通常無法像企業網路那般嚴密。

根據我們的偵測資料，2020 年大約有 15.5% 的路由器成了駭客對內攻擊 (從網際網路攻擊家用網路) 的目標，另有 5.1% 的路由器更成了駭客對外攻擊 (從家用網路攻擊網際網路) 的跳板。

圖 19：2020 年，約有 15.5% 的路由器遭到駭客攻擊，另有 5.1% 很可能已遭到入侵。

註：根據所有偵測資料當中對內攻擊 (路由器為受害目標) 與對外攻擊 (路由器變成了攻擊者) 的百分比。

資料來源：趨勢科技 Smart Home Network 產品。

過去一年，我們也看到對內攻擊事件的數量激增，甚至超越 2019 年的三倍；至於對外攻擊的數量，則是將近 2019 年的兩倍。不僅如此，那些被偵測到可能遭遇對內攻擊以及可能已被駭客入侵而成了駭客對外攻擊跳板的連網裝置數量也雙雙增加。同時，我們也看到更多路由器 (也就是家用裝置連上網際網路的閘道) 成了對內攻擊的目標以及對外攻擊的跳板。

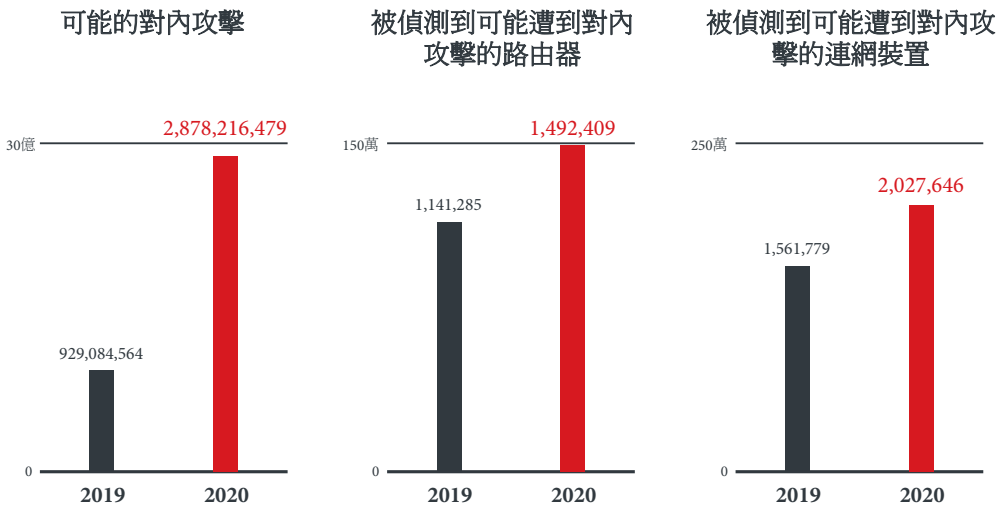


圖 20：可能的對內攻擊數量大幅增加，而且被發現可能遭到對內攻擊的連網裝置與路由器也雙雙增加：2019 與 2020 年可能的對內攻擊偵測數量與遭到攻擊的路由器與裝置數量比較。

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。

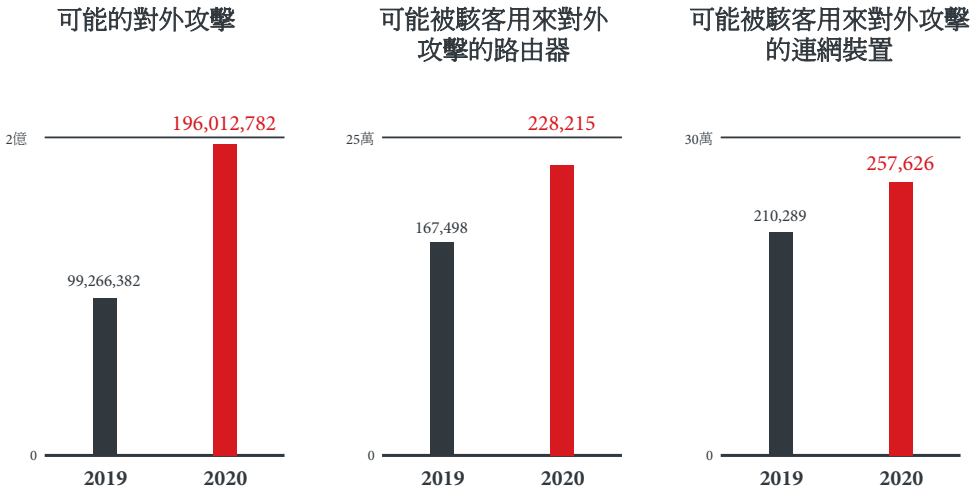


圖 21：可能的對外攻擊數量大幅增加，而且可能被駭客用來對外攻擊的連網裝置與路由器也雙雙增加：2019 與 2020 年可能的對外攻擊偵測數量與可能被駭客用來對外攻擊的路由器與裝置數量比較。

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。

在所有對內攻擊當中，暴力登入攻擊占很大一部分，顯示使用者登入憑證是 2020 年歹徒最喜愛的目標。

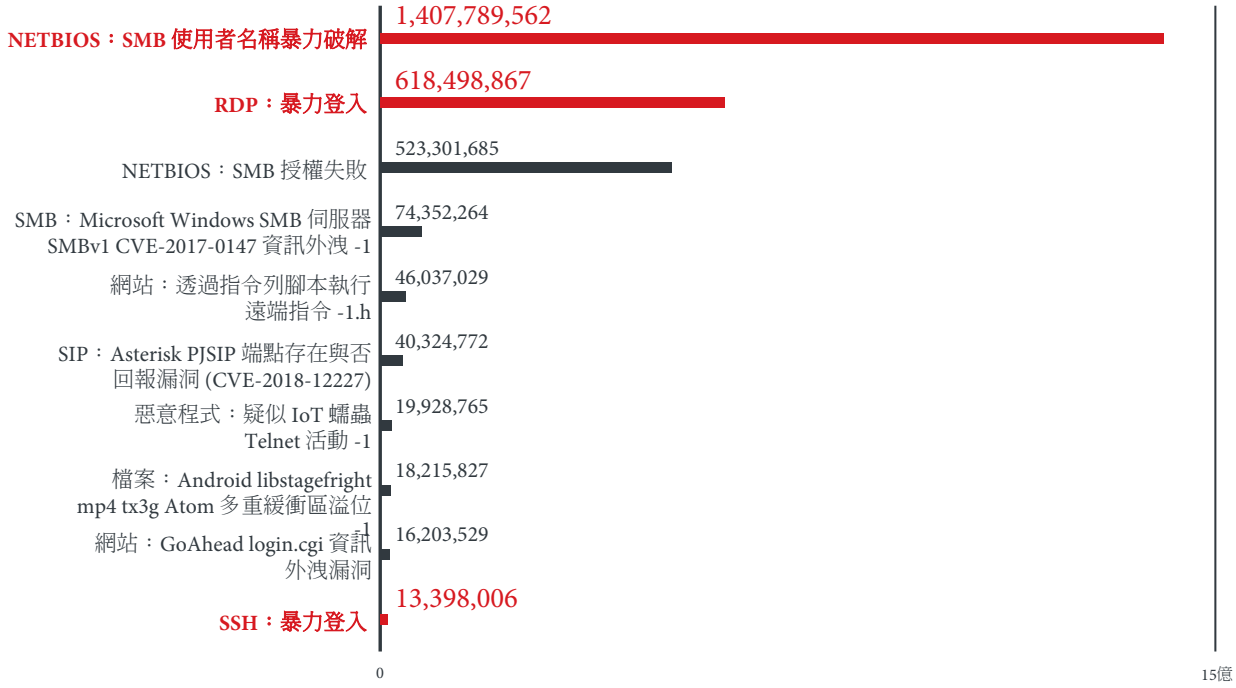


圖 22：最多的前兩種對內攻擊都屬於暴力登入攻擊：2020 年前 10 大對內攻擊偵測規則觸發事件數量比較。

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。

在對外攻擊方面也可以看到類似的情況，NetBIOS Server Message Block (SMB) 使用者名稱暴力破解所占的數量最高。Microsoft Windows SMB 攻擊 (包括 WannaCry 漏洞攻擊在內) 緊跟在後，排名第二。

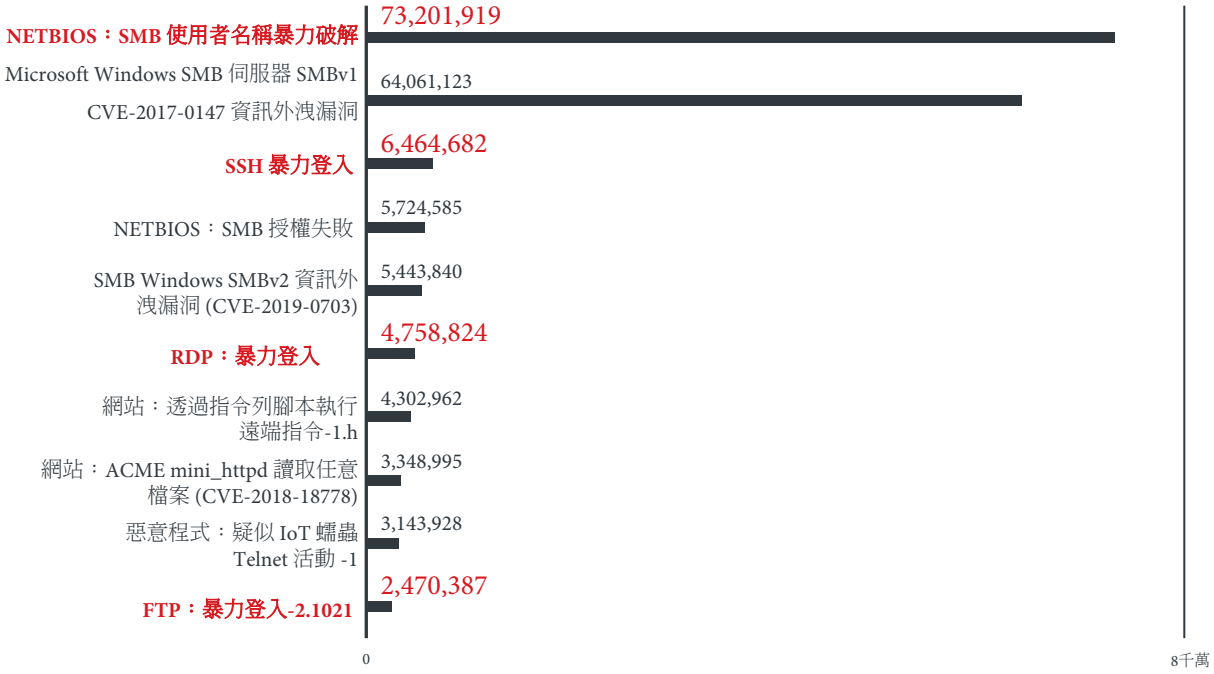


圖 23：暴力登入是對外攻擊最常見的手法：2020 年前 10 大對外攻擊偵測規則觸發事件數量比較。

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。

上半年出現了多起知名的 IoT 攻擊事件，其中有些 (如「Urgent/11」和「Ripple20」) 在我們的上半年網路資安報告中已經披露[62]。下半年，Forescout 的研究人員披露了「Amnesia:33」漏洞，這是一組共 33 個全球 IoT/IIoT 裝置開放原始程式碼 TCP/IP 軟體堆疊漏洞的總稱。這些漏洞攻擊一旦得逞，駭客就能掌控被駭裝置，利用裝置來從事各種惡意活動，例如當成入侵網路或橫向移動的跳板[63]。

Amnesia:33 之所以特別令人憂心，就在於受影響的 TCP/IP 軟體堆疊 (包括 Nut/Net、FNET、picoTCP 以及 uIP) 並非全部來自單一廠商。正因為受到影響的廠商眾多，這些漏洞很可能迅速擴散開來。此外，這些問題追蹤起來相當困難，也不易評估衝擊，因為不僅漏洞牽涉的範圍太廣，而且受到影響的系統很可能也高度模組化，或者缺乏文件說明，甚至早已不再獲得廠商支援[64]。

像 Amnesia:33 這樣的漏洞，不僅可能嚴重衝擊受影響的裝置使用者，更可能衝擊整個供應鏈。其實不難想像類似 SolarWinds 的攻擊情境也可能在 IoT 上演，駭客可能利用裝置的漏洞經由某家企業的供應商來駭入企業。

至於一般較常見的 IoT 威脅，最值得注意的是 Mirai 殭屍網路，從 2016 年至今，Mirai 殭屍網路越來越惡名昭彰[65]，去年的情況依然如此。七月份，我們發現、分析並通報了一個 Mirai 變種，此變種結合了 9 種新舊漏洞攻擊手法，最值得注意的是 CVE-2020-10173。這是一個 Comtrend VR-3033 路由器的多重已驗證指令注入漏洞[66]。該月下旬，我們又分析並通報了另一個會攻擊 CVE-2020-5902 漏洞的 Mirai 變種，這是一個 F5 BIG-IP Traffic Management User Interface (TMUI) 遠端程式碼執行漏洞[67]。

行動惡意程式雖減少但卻更隱密

相較於 2019 年，我們 2020 年所攔截的行動應用程式數量減少了 41%。然而，我們所偵測到的行動裝置相關惡意威脅樣本數量卻比前一年成長 67%。造成如此反差的原因之一很可能是駭客使用了一些應用程式以外的方法來 (直接或間接) 攻擊行動裝置，例如網路釣魚網頁、社群媒體訊息等等。

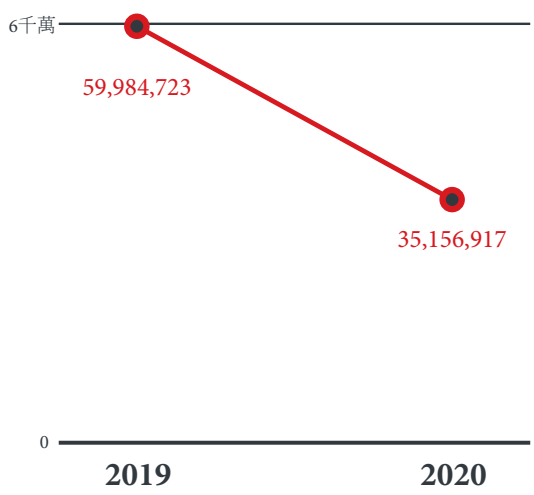


圖 24：已攔截的行動應用程式數量較去年減少 41%，這可能意味著駭客今年的重點並非在散布惡意應用程式：2019 與 2020 年已攔截的惡意 Android 應用程式數量比較。

資料來源：趨勢科技行動應用程式信譽評等服務 (MARS)。

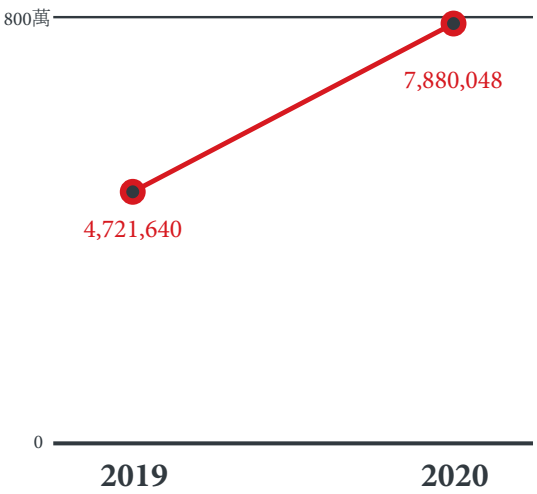


圖 25：儘管已攔截的行動應用程式數量減少，行動裝置相關惡意威脅樣本數量卻較去年成長 67%，這或許是因為駭客運用了惡意應用程式以外的方法來感染行動裝置：2019 與 2020 年已偵測到的行動裝置相關惡意威脅樣本數量比較。

資料來源：趨勢科技行動應用程式信譽評等服務 (MARS)。

雖然人們對行動裝置攻擊事件的關注度已經被其他網路資安事件所掩蓋，但去年仍有幾件值得注意的行動威脅資安事件。11 月份，我們分析了一個新的 Joker 惡意程式變種，此變種暗藏在一個 HD/4K 畫質桌布應用程式當中。此 Joker 變種值得注意的是會利用 GitHub 網頁與儲存庫 (repository) 來躲避偵測[68]。

新的變種捨棄了之前使用應用程式類別 (class) 與啟動器活動 (launcher activity) 的攻擊手法，改將程式碼注入到新的位置。此外，它使用 GitHub 的目的一方面是為了掩護惡意活動，另一方面則是用來散布惡意程式。這個變種之所以特別危險，就在於它被包含在一個正常的應用程式當中，若再搭配其他加密編碼功能，受害者很難發現自己遭到感染。

還有一點值得注意的是，Android 惡意程式的加密編碼行為正在不斷演進，經由深入的分析，我們發現 Geost 惡意程式已發展出多層式加密編碼行為，證明駭客集團一直不斷投入心力來改進惡意程式[69]。不過我們也發現駭客修正的程式碼似乎沒有提升太多加密編碼的效果，所以對躲避偵測並無太大幫助。

越來越多危險的漏洞威脅著企業安全

舊漏洞雖仍時常遭到攻擊，但更危險的新漏洞卻悄然現身

2020 年，趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫發布了 1,453 次漏洞公告，較 2019 年增加 40%。根據 Common Vulnerability Scoring System (CVSS) 的分級，其中 173 個屬於重大漏洞，983 個屬於高嚴重性漏洞[70]。重大與高嚴重性漏洞數量較 2019 年大幅增加，這些重大與高嚴重性漏洞由於對企業的風險極高，因此必須盡可能及早修補，這無形中也增加了 IT 團隊的工作負擔。

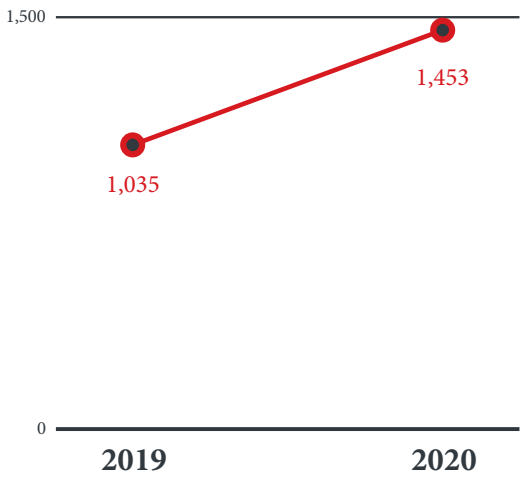


圖 26：漏洞公告發布數量較去年成長 40%：2019 與 2020 年揭露的漏洞數量比較。

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

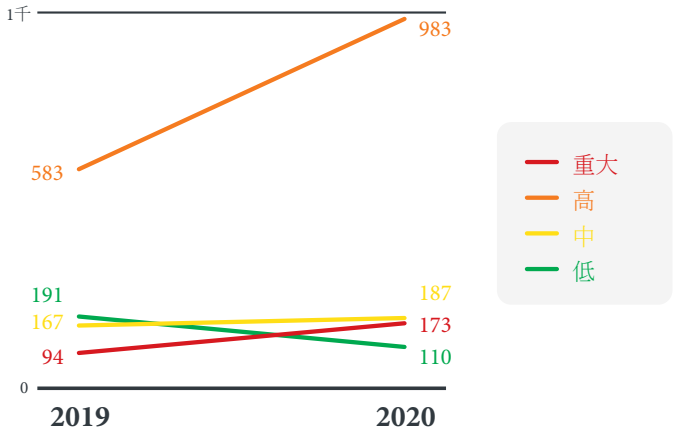


圖 27：重大與高嚴重性漏洞數量激增，這意味著，為了修補這些漏洞， IT 團隊的工作負擔將更加沉重：2019 與 2020 年不同嚴重性的漏洞數量比較 (根據 CVSS 分級)。

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

根據我們 2017 至 2020 年最常被攻擊的漏洞統計資料顯示，一些最遠可追溯至 2005 年的漏洞至今仍經常遭到攻擊。這表示，企業千萬別對老舊的漏洞掉以輕心，以為系統應該都能應付舊的漏洞，反倒是應該勤於修補軟體，讓軟體常保更新。

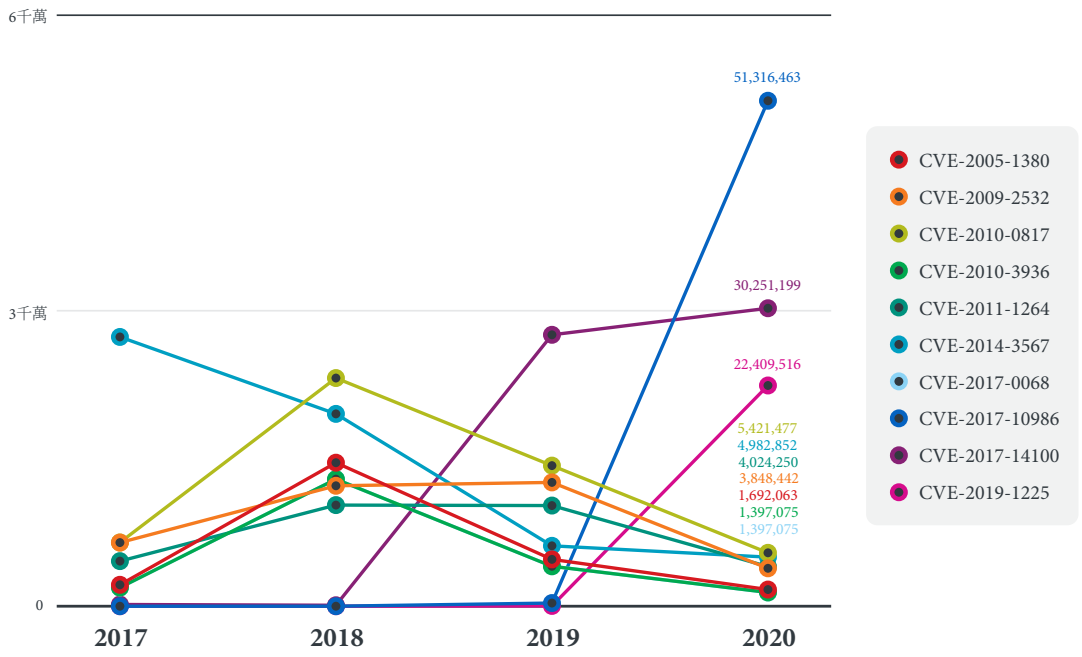


圖 28：對駭客來說漏洞的新舊並不重要，就連一些可追溯至 2005 年的老舊漏洞至今仍是最常遭到攻擊的漏洞：2017 至 2020 年 10 大最常遭到攻擊的漏洞偵測數量比較。

註：偵測 CVE-2010-3936 與 CVE-2017-0068 的過濾規則 ID 相同，因此兩者的偵測數量相同。

資料來源：趨勢科技 Digital Vaccine 數位疫苗過濾規則。

Zerologon 漏洞的出現讓駭客有機會掌控整個網路

2020 年最重大的一個漏洞就是 Zerologon 漏洞 (CVE-2020-1472)[71]，該漏洞存在於 NT Lan Manager (NTLM) 伺服器中的登入程序，該程序所用的一個數值原本應該是隨機數字，但卻因為 Zerologon 漏洞的關係而使用了四個「零」作為數值，所以被稱作 Zerologon 漏洞[72]。

Zerologon 是一個相當危險的漏洞，目前已經出現了概念驗證 (POC) 攻擊，其嚴重性在 CVSS 分級上是最高等級 (10/10)。駭客在發動漏洞攻擊時會利用 Microsoft Active Directory (AD) Netlogon Remote Protocol (MS-NRPC) 通訊協定的一個漏洞來登入使用 NTLM 的伺服器[73]。由於 MS-NRPC 通訊協定也用於傳輸帳號變更資訊和密碼，所以問題才會變得棘手。

Zerologon 可讓駭客取得網域控制器的控制權、變更或移除網域控制器上某個服務的帳號密碼，接著駭客就能執行各種惡意行為，例如：發動阻斷服務攻擊，甚至接管整個網路。駭客利用網路上公開的概念攻擊程式碼，甚至可以做出一些更具破壞性的行為，例如讓受害的電腦感染勒索病毒[74]。

Microsoft 在 2020 年 8 月釋出初步的 Zerologon 修補更新，接著在 2021 年 2 月又釋出第二次修補更新[75]。第一次更新是為了防止網域控制器使用無安全性的遠端程序呼叫 (PRC) 通訊，第二次更新則是強迫網域控制器在預設情況下防止不合規定的裝置與其連線[76]。

新式威脅需要完整的防禦策略與多層式防護技術

面對無時無刻不在試圖利用各種可用工具和技巧來發動攻擊的駭客集團，企業隨時都面臨著重大的資安風險。再加上許多企業目前正遭遇一個特殊的情況，必須在全球疫情的環境下同時兼顧實體與虛擬工作環境的安全。

今日複雜的工作環境，家庭與辦公室的界線已經開始模糊，因此必須有一些適當的技術來構築一套強大的資安防禦。企業不能再仰賴各自為政的個別防護層來分別保護不同的基礎架構環節，企業需要的是一套強大的多層式防護。這套解決方案必須提供廣泛的防護功能 (包括偵測、調查及回應)，同時還要提供涵蓋整個系統的全方位防護，從電子郵件和端點，到伺服器、網路，甚至是雲端工作負載。

除了技術的因素與問題考量之外，疫情也大大影響了資安營運中心 (SOC) 的執行能力。資安團隊除了必須確保企業建置適當的技術來保護工作環境之外，還要妥善處理越來越多的工作量以免過勞[77]。一套良好的多層式解決方案，應該要讓 IT 人員和資安團隊深入掌握他們所面臨的威脅性質。此外，像機器學習與行為監控這樣的技術，也能讓企業只需處理最重要的資安問題，而不需整天應付一大堆的監控資料。

企業應結合這些技術與正確的資安策略和政策。即使每天都有更加精密的攻擊手法出現，但絕大多數駭客常用的感染技巧，依然是網路釣魚和社交工程技巧，從業餘的新手到最有經驗老手皆是如此。因此，企業應考慮投入一些教育訓練成本，讓員工認識一些最常見的網路釣魚和社交工程技巧[78]。

此外，企業也應定期執行一些資安檢查來確保其實體和雲端基礎架構沒有任何組態設定錯誤，以及其他資安弱點。還有，企業應定期掃瞄資料來偵測一些早期警訊，例如駭客的第一階段惡意程式與工具程式，這些通常是實際攻擊的前兆。

不僅如此，有鑑於供應鏈攻擊正逐漸成為一種常態，企業很重要的一點就是妥善評估其供應商及其他合作夥伴的資安狀況，可能的話，和他們共同建立一些強大的防禦來防範這類攻擊。

即時而有效率的修補更新管理，其重要性亦不在話下。如同 Zerologon 漏洞所證明，在修補更新釋出之後盡快套用更新，才是修補更新的最佳時機。然而殘酷的現實是，修補更新沒有表面上看起來容易，企業需花費相當的時間來完成整套系統的更新，再加上還有可能出現零時差漏洞，使得問題更加複雜。為了解決這樣的困境，企業可考慮採用虛擬修補技術，在修補更新的過程當中或者等待修補更新釋出的期間，防止漏洞遭到攻擊[79]。

大多數企業或多或少都已經讓員工離開原本的辦公室而改在家中上班，所以大部分企業目前最迫切需要的是一方面要維持營運，另一方面又要兼顧技術、資安與人性，盡可能面面俱到。

威脅情勢回顧

2020 年，趨勢科技 Smart Protection Network™ 全球威脅情報網總共幫使用者攔截了 620 億次以上的威脅，包含電子郵件威脅、惡意檔案以及惡意網址。

62,637,731,995

(2020 年攔截的威脅總數)

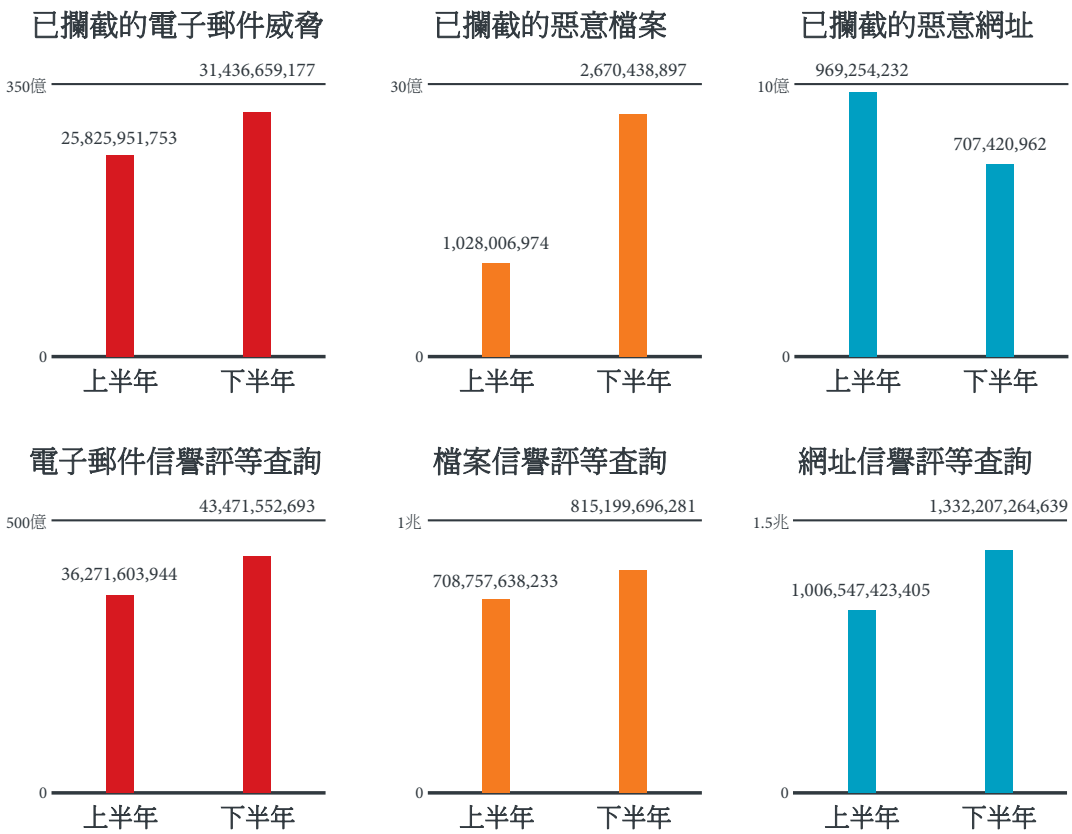


圖 29：從上半年至下半年，幾乎所有已攔截威脅的數據和信譽評等查詢數量都增加，但已攔截的惡意檔案增加數量尤其驚人：2020 上半年及下半年，已攔截的電子郵件、檔案與網址威脅數量，以及電子郵件、檔案與網址信譽評等查詢數量比較。

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

2020 年偵測數量最多的 10 大惡意程式家族，排行前三名的都是一些老面孔：WannaCry、挖礦程式與 Emotet。WannaCry 除了是第一大惡意程式家族之外，同時也是名單當中唯一的勒索病毒。所有虛擬加密貨幣挖礦程式加起來占據第二名，顯示這類惡意程式的氾濫程度。在這 10 大惡意程式家族名單中，大部分都是一些老舊家族，這些家族儘管歷史久遠，但仍囊括了大多數的感染案例。

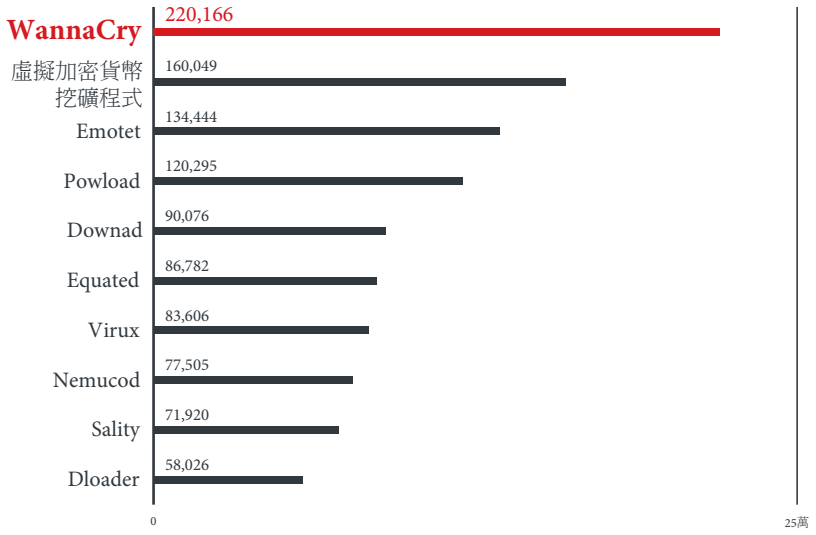


圖 30：WannaCry 勒索病毒依然是最大的威脅，其次是所有的虛擬加密貨幣挖礦程式：2020 年偵測數量最多的 10 大惡意程式家族。

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

根據我們 2020 年偵測的 10 大虛擬加密貨幣挖礦程式資料顯示，光前三名加起來的偵測數量就超過 12 萬。

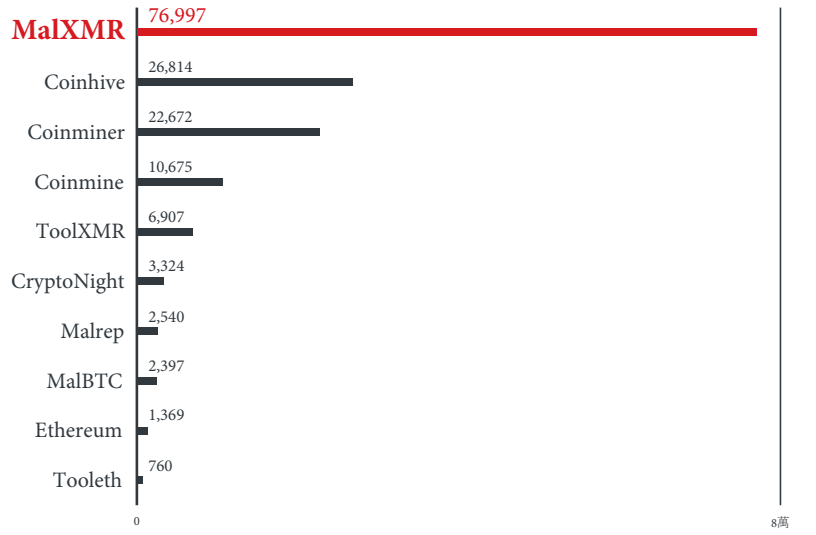


圖 31：MalXMR、Coinhive 與 Coinminer 是偵測數量最多的虛擬加密貨幣挖礦程式，三者加起來超過 12 萬：2020 年偵測數量最多的 10 大虛擬加密貨幣挖礦程式。

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

2020 年，我們偵測到超過 230 萬個與 C&C 伺服器通訊的端點裝置，而我們偵測到的殭屍網路 C&C 伺服器數量約 10 萬多一點。伺服器數量之所以這麼多，有可能是很多駭客集團的攻擊行動都會用到 C&C 伺服器，也有可能是他們所使用的 C&C 基礎架構日益複雜。另一方面，光從我們的感測器所偵測到的殭屍網路連線數量，就能推斷潛在的受害者數量應該超過百萬。

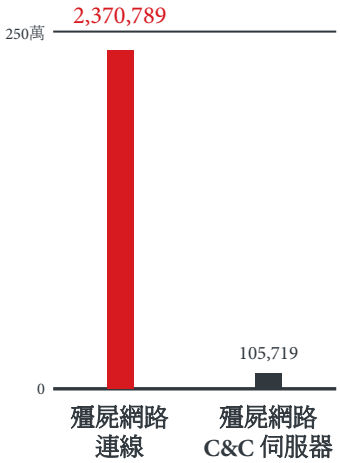


圖 32：我們偵測到超過 230 萬次殭屍網路連線，以及超過 10 萬台的殭屍網路 C&C 伺服器：2020 年偵測到的殭屍網路連線數量與 C&C 伺服器。

註：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；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。

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

2020 年發現了 127 個新的勒索病毒家族，較 2019 年的 95 個成長 34%[80]。9 月份才開始現身的 Egregor 一下子就竄升到 2020 年 10 大勒索病毒家族之一 (參見圖 1)。

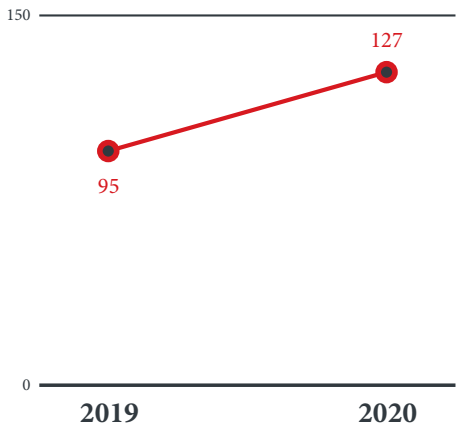


圖 33：新勒索病毒家族數量較去年成長 34%：2019 與 2020 年新勒索病毒家族數量比較。

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

一月	二月	三月	四月	五月	六月
AkoLocker	Antefrigus	BB	Ballistic BearCrypt	PonyFinal	Zorab
Avest	Balaclava	Corvina	Coronawinlocker	GonnaCry	WorldCry
BitPyLocker	Cai CrypenCode	Mado	Creepy CryLock	CoronaLock	SuchCrypt
Keslan	Cryptopxj Crytox	Nefilim	Geminice	ColdLock	Sapphire
Zeoticus	DemonCrypt	Pysa	Jest	BlueCheeser	QrnaLock
	FTCode	Triplem	Lbkut OnaLocker		PowLock
	Ledif	WannaRen	Ooglego Sadogo		Locment
	Makop		Sfile2		LickyAgent
	Morrisbatchcrypt		Upper		Krygo
	OnyxLocker		Void		Funicorn
	Ragnarok		Wreath		Freefil
	Ranscrape				Escal
	Trsomware				CyberThanos
	WannaCash				Chimera
	WannaScream				BlackMoon
	Wilboy				BlackKingdom
					BlackClaw
					Avaddon

七月	八月	九月	十月	十一月	十二月
Xinof	Tappif SunCrypt	Aidsnt BitMiner	Doowtar	Hiddeneargdarmerie	AgeLocker
WhoLocker	Silvertor	BlackKnight	EyeCryLocker	RanzyLocker WoodRat	Alol
Wastedlocker	RagnarLocker	BlackSquid	Hibuniel		BacuCrypt
ThiefQuest	GiveMeTheKey	CoronaCryptor	JarCrypt		Dusk
StrongPity	FlyingShip	DogeCrypt	LeakTheMall		Erica
Pojie	Exorcist	Egregor	Pay2Key		Godra
Panther	DarkSide	Exx	RegretLocker		Hwru
Lolkek	CryptoLock	Gav HexaCrypt	SantaCrypt		RedRoman
JosephNull	BigLock	MountLocket			StingJar
EvilQuest		ReadMan			Vaggen
CryCryptor		Thanos			
Bead		Vashsorena			
		Viluciware Zhen			

表 4：本期發現 127 個新的勒索病毒家族：2020 年偵測到的新勒索病毒家族。

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。

在 2020 年偵測到的垃圾郵件所用的 1,100 多萬個附件檔案的類型分布中，PDF 占了將近半數。此外，XLSX 與 HTML 也占了相當大的偵測量。

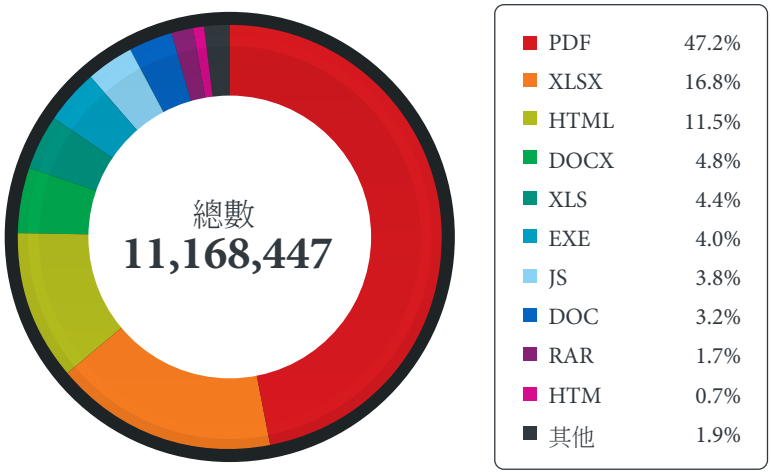


圖 34：PDF 檔案占了將近所有垃圾郵件附件的半數：2020 年垃圾郵件附件檔案類型分布。

資料來源：趨勢科技電子郵件信譽評等服務。

雖然，在所有感染惡意程式的電腦中，採用 Windows 作業系統的仍占絕大多數，但 macOS 和 Linux 電腦也有不少電腦感染了惡意程式。

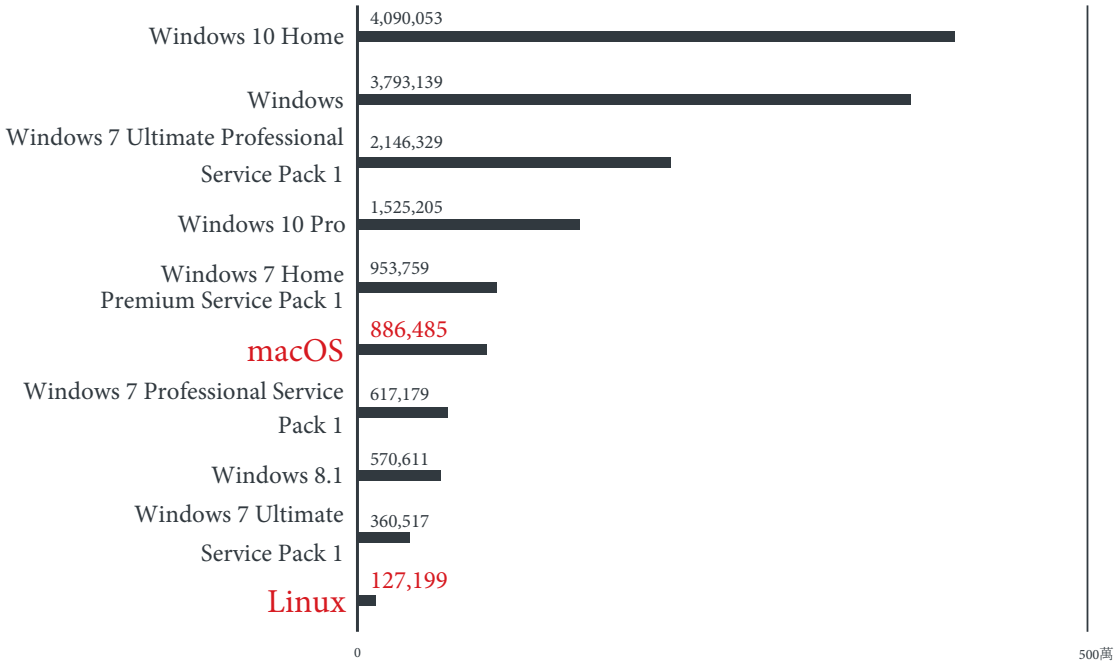


圖 35：macOS 和 Linux 也有不少電腦感染了惡意程式，其中 macOS 甚至還高於某些 Windows 版本：2020 年感染惡意程式最多的 10 大作業系統。

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

參考資料

1 趨勢科技。(2020 年 9 月 15 日)。*趨勢科技*。「提升破壞力來達成獲利：持續演變的目標式勒索病毒攻擊手法」(Boosting Impact for Profit: Evolving Ransomware Techniques for Targeted Attacks)。上次存取時間 2021 年 1 月 15 日： https://www.trendmicro.com/en_us/research/20/i/boosting-impact-for-profit-evolving-ransomware-techniques-for-targeted-attacks.html.

2 Catalin Cimpanu。(2020 年 4 月 21 日)。*ZDNet*。「看看這份名單：哪些勒索病毒集團會在您不支付贖金時竊取並公開您的資料」(Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay)。上次存取時間 2021 年 1 月 15 日：https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay.

3 Coalition, Inc. (日期不詳)。*Coalition*。「網路攻擊保險理賠報告」(Cyber Insurance Claims Report)。上次存取時間 2021 年 1 月 15 日：https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf.

4 趨勢科技。(2020 年 4 月 4 日)。*趨勢科技資訊安全新聞*。「Ryuk 勒索病毒感染美國政府外包商」(Ryuk Ransomware Infects US Government Contractor)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-ransomware-infects-us-government-contractor.

5 Cybersecurity & Infrastructure Agency。(2020 年 11 月 2 日)。*Cybersecurity & Infrastructure Agency*。「鎖定醫療與公衛產業的勒索病毒活動」「Ransomware Activity Targeting the Healthcare and Public Health Sector)。上次存取時間 2021 年 1 月 15 日：https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

6 HHS Cybersecurity Program。(2020 年 11 月 11 日)。*HHS Cybersecurity Program*。「TrickBot、Ryuk 與醫療公衛體系」(TrickBot, Ryuk, and the HPH Sector)。上次存取時間 2021 年 2 月 3 日：https://www.hhs.gov/sites/default/files/trickbot-ryuk-and-the-hph-sector.pdf.

7 Greg Foss。(2020 年 10 月 30 日)。*Carbon Black*。「TAU 威脅公告：美國醫療與公衛體系迫切面臨的勒索病毒威脅」(TAU Threat Advisory: Imminent Ransomware threat to U.S. Healthcare and Public Health Sector)。上次存取時間 2021 年 2 月 3 日：https://www.carbonblack.com/blog/tau-threat-advisory-imminent-ransomware-threat-to-u-s-healthcare-and-public-health-sector.

8 趨勢科技。(2019 年 3 月 14 日)。*趨勢科技*。「從託管式偵測及回應服務的角度看 Ryuk 勒索病毒」(Examining Ryuk Ransomware Through the Lens of Managed Detection and Response)。上次存取時間 2021 年 2 月 3 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response.

9 趨勢科技。(2020 年 11 月 4 日)。*趨勢科技*。「Ryuk 2020：利用 TrickBot 與 BazarLoader 散播勒索病毒」(Ryuk 2020: Distributing Ransomware via TrickBot and BazarLoader)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader.

10 趨勢科技。(2020 年 8 月 26 日)。*趨勢科技*。「保護因疫情而改變的工作環境」(Securing the Pandemic-Disrupted Workplace)。上次存取時間 2021 年 2 月 8 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report.

11 趨勢科技。(2020 年 12 月 14 日)。*趨勢科技*。「Egregor 勒索病毒在 2020 年底前發動一波波重大攻擊」(Egregor Ransomware Launches String of High-Profile Attacks to End 2020)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html.

12 Tomas Meskauskas。(2020 年 10 月 29 日)。*Security Boulevard*。「Egregor：Sekhmet 的表親」(Egregor: Sekhmet's Cousin)。上次存取時間 2021 年 1 月 15 日：https://securityboulevard.com/2020/10/egregor-sekhmets-cousin.

13 CISO Mag。(2020 年 11 月 3 日)。*CISO Mag*。「我們真的脫離險境了嗎？勒索病毒集團宣布退休。」(Are We Really Out of the Maze? The Ransomware Gang Announces Retirement)。上次存取時間 2021 年 2 月 8 日：https://cisomag.eccouncil.org/maze-ransomware-retires.

14 趨勢科技。(2020 年 12 月 14 日)。*趨勢科技*。「Egregor 勒索病毒在 2020 年底前發動一波波重大攻擊」(Egregor Ransomware Launches String of High-Profile Attacks to End 2020)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html.

15 趨勢科技。(2020 年 1 月 5 日)。*趨勢科技*。「DoppelPaymer 勒索病毒簡介」(An Overview of the DoppelPaymer Ransomware)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html.

16 Federal Bureau of Investigation, Cyber Division。(2020 年 12 月 10 日)。*網際網路犯罪申訴中心 (Internet Crime Complaint Center)*。「DoppelPaymer 勒索病毒攻擊關鍵基礎架構並衝擊關鍵服務」(DoppelPaymer Ransomware Attacks on Critical Infrastructure Impact Critical Services)。上次存取時間 2021 年 1 月 15 日： https://www.ic3.gov/Media/News/2020/201215-1.pdf.

17 趨勢科技。(2020 年 8 月 13 日)。*趨勢科技*。「BitPaymer 惡意程式資訊」(BitPaymer Malware Information)。上次存取時間 2021 年 1 月 24 日：https://success.trendmicro.com/solution/000261855.

18 Process Hacker。(日期不詳)。*Process Hacker*。「Process Hacker」。上次存取時間 2021 年 1 月 15 日：https://processhacker.sourceforge.io.

19 Ryan Flores。(2020 年 12 月 1 日)。*趨勢科技*。「現代勒索病毒對製造業網路的衝擊」(The Impact of Modern Ransomware on Manufacturing Networks)。上次存取時間 2021 年 1 月 19 日：https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html.

20 Leandro Froes。(2021 年 1 月 6 日)。*趨勢科技*。「擴大範圍並提升速度：RansomExx 的策略」(Expanding Range and Improving Speed: A RansomExx Approach)。上次存取時間 2021 年 2 月 4 日：https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed-a-ransomexx-approach.html.

21 Nelson William Gamazo Sanchez 等人。(2020 年 10 月 19 日)。*趨勢科技*。「Operation Earth Kitsune：追蹤 SLUB 的最新動態」(Operation Earth Kitsune: Tracking SLUB's Current Operations)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations.

22 Nelson William Gamazo Sanchez 等人。(2020 年 10 月 28 日)。*趨勢科技*。「Operation Earth Kitsune：兩個新的後門共舞」(Operation Earth Kitsune: A Dance of Two New Backdoors)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html.

23 趨勢科技。(2021 年 1 月 5 日)。*趨勢科技*。「Earth Wendigo 在 Service Worker 中注入 JavaScript 後門程式來竊取信箱」(Earth Wendigo Injects JavaScript Backdoor to Service Worker for Mailbox Exfiltration)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html.

24 Joseph C Chen、Jaromir Horejsi 與 Ecular Xu。(2020 年 12 月 9 日)。*趨勢科技*。「SideWinder 利用南亞衝突議題發動魚叉式網路釣魚及行動裝置攻擊」(SideWinder Uses South Asian Issues for Spear Phishing, Mobile Attacks)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html.

25 Mayra Rosario Fuentes。(2020 年 5 月 26 日)。*趨勢科技*。「網路犯罪地下市場變遷」(Shifts in Underground Markets)。上次存取時間 2021 年 2 月 5 日：https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf.

26 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 2021 年 2 月 8 日：https://www.bleepingcomputer.com/news/security/ryuk-ransomware-partners-with-trickbot-to-gain-access-to-infected-networks/.

27 趨勢科技。(2016 年 1 月 16 日)。*趨勢科技*。「Pawn Storm 攻擊行動重點摘要與最新發展」(Operation Pawn Storm: Fast Facts and the Latest Developments)。上次存取時間 2021 年 1 月 15 日：https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts.

28 Feike Hacquebord 與 Lord Alfred Remorin。(2020 年 12 月 17 日)。*趨勢科技*。「Pawn Storm刻意採取非精密攻擊的策略」(Pawn Storm's Lack of Sophistication as a Strategy)。上次存取時間 2021 年 1 月 18 日：https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html.

29 Paul Miguel Babon。(2020 年 9 月 3 日)。*趨勢科技*。「奸詐的網路釣魚表單」(Tricky 'Forms' of Phishing)。上次存取時間 2021 年 1 月 18 日：https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html.

30 Catalin Cimpanu。(2020 年 10 月 4 日)。*ZDNet*。「FBI 警告企業機構小心針對軟體供應鏈的持續攻擊」(FBI warns about ongoing attacks against software supply chain companies)。上次存取時間 2021 年 2 月 10 日：https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/.

31 Federal Bureau of Investigation, Cyber Division。(2020 年 3 月 30 日)。*SANS Internet Storm Center*。「Kwampirs 惡意程式被用於針對全球產業供應鏈的持續性網路攻擊，醫療產業也在攻擊之列」(Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector)。上次存取時間 2021 年 2 月 10 日：https://isc.sans.edu/diaryimages/Kwampirs_PIN_20200330-001.pdf.

32 Jake Williams。(2020 年 12 月 15 日)。*SANS Institute*。「有關 SolarWinds 供應鏈攻擊您該知道的事」(What You Need to Know About the SolarWinds Supply-Chain Attack)。上次存取時間 2021 年 1 月 19 日：https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack.

33 SolarWinds。(2020 年 12 月 31 日)。*SolarWinds*。「SolarWinds 安全公告」(SolarWinds Security Advisory)。上次存取時間 2021 年 1 月 19 日：https://www.solarwinds.com/securityadvisory.

34 趨勢科技。(2020 年 12 月 15 日)。*趨勢科技*。「最新 Sunburst 目標式攻擊簡介」(Overview of Recent Sunburst Targeted Attacks)。上次存取時間 2021 年 1 月 19 日：https://www.trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html.

35 David Klepper。(2020 年 10 月 17 日)。*Associated Press News*。「詐騙集團趁著美國選舉期間做亂，但他們要的並不是選票」(Scammers seize on US election, but it's not votes they want)。上次存取時間 2021 年 1 月 19 日：https://apnews.com/article/election-2020-virus-outbreak-joe-biden-senate-elections-media-f3 2410451f45102ddd4a82ebec8ac746.

36 Tom Burt。(2020 年 9 月 10 日)。*Microsoft*。「針對美國選舉的新式網路攻擊」(New cyberattacks targeting U.S. elections)。上次存取時間 2021 年 1 月 19 日：https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/.

37 趨勢科技。(2020 年 8 月 26 日)。*趨勢科技*。「保護因疫情而改變的工作環境」(Securing the Pandemic-Disrupted Workplace)。上次存取時間 2021 年 1 月 19 日：https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf.

38 趨勢科技。(2020 年 11 月 11 日)。*趨勢科技*。「發展中的疫情：COVID-19 遭網路攻擊利用」(Developing Story: COVID-19 Used in Malicious Campaigns)。上次存取時間 2021 年 1 月 19 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

39 Andrew Duehren 與 Kristina Peterson。(2020 年 11 月 25 日)。*The Wall Street Journal*。「Covid-19 補助與振興方案：哪些快要過期，哪些正在進行」(Covid-19 Aid and Stimulus: What's Expiring Soon and What's in the Works)。上次存取時間 2021 年 1 月 19 日：https://www.wsj.com/articles/coronavirus-aid-whats-expiring-soon-and-whats-in-the-works-11606311697.

40 美國國稅局 (IRS)。(2020 年 12 月 8 日)。*Internal Revenue Service*。「IRS 警告人們注意 COVID 相關的詐騙簡訊」(IRS warns people about a COVID-related text message scam)。上次存取時間 2021 年 1 月 19 日：https://www.irs.gov/newsroom/irs-warns-people-about-a-covid-related-text-message-scam.

41 Check Point。(2021 年 1 月 12 日)。*Check Point*。「Covid-19 疫苗在黑暗網路上只賣 250 美元」(Covid-19 'Vaccines' Touted for Just $250 on Darknet)。上次存取時間 2021 年 1 月 19 日：https://blog.checkpoint.com/2020/12/11/covid-19-vaccines-touted-for-just-250-on-darknet/.

42 Claire Zaboeva 與 Melissa Frydrych。(2020 年 12 月 3 日)。*IBM Security Intelligence*。「IBM 發現瞄準 COVID-19 疫苗冷鏈的全球網路釣魚攻擊行動」(IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain)。上次存取時間 2021 年 1 月 19 日： https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain.

43 Marshall Chen 等人。(2020 年 8 月 6 日)。*趨勢科技*。「Water Nue 網路釣魚攻擊高階經理的 Office 365 帳號」(Water Nue Phishing Targets Execs' Office 365 Accounts)。上次存取時間 2021 年 1 月 22 日：https://www.trendmicro.com/en_us/research/20/h/water-nue-phishing-targets-execs-office-365-accounts.html.

44 Cedric Pernet。(2020 年 10 月 6 日)。*趨勢科技*。「法國企業遭遇狡猾的變臉詐騙攻擊」(French companies Under Attack from Clever BEC Scam)。上次存取時間 2021 年 1 月 22 日： https://www.trendmicro.com/en_us/research/20/j/french-companies-under-attack-from-clever-bec-scam.html.

45 趨勢科技。(2020 年 10 月 7 日)。*趨勢科技*。「CSO 觀點：DataBank 資安長 Mark Houpt 討論如何放眼未來在新的常態下保護基礎架構安全 」(CSO Insights: DataBank's Mark Houpt on Looking Beyond Securing Infrastructures in the New Normal)。上次存取時間 2021 年 1 月 19 日： https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-databank-mark-houpt-on-looking-beyond-securing-infrastructures-in-the-new-normal.

46 Yahoo!。(2020 年 11 月 24 日)。*Yahoo! Finance*。「2020 年虛擬私人網路 (VPN) 市場報告：VPN 用量激增創下 27.1% 的歷史新高 — 至 2027 年的全球預測」(Virtual Private Network (VPN) Market Report 2020: VPN Usage Spirals to an all Time High of 27.1% - Global Forecast to 2027)。上次存取時間 2021 年 1 月 19 日：https://finance.yahoo.com/news/virtual-private-network-vpn-market-100300294.html.

47 Common Vulnerabilities and Exposures。(日期不詳)。*Common Vulnerabilities and Exposures*。「CVE-2019-11510」。上次存取時間 2021 年 1 月 19 日：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510.

48 Eduard Kovacs。(2020 年 1 月 6 日)。*Security Week*。「Pulse Secure VPN 漏洞遭駭客用來散布勒索病毒」(Pulse Secure VPN Vulnerability Exploited to Deliver Ransomware)。上次存取時間 2021 年 1 月 19 日： https://www.securityweek.com/pulse-secure-vpn-vulnerability-exploited-deliver-ransomware.

49 Raphael Centeno。(2020 年 9 月 21 日)。*趨勢科技*。「網路犯罪集團利用 VPN 安裝程式散布後門程式」(Cybercriminals Distribute Backdoor With VPN Installer)。上次存取時間 2021 年 2 月 5 日：https://www.trendmicro.com/en_us/research/20/i/cybercriminals-distribute-backdoor-with-vpn.html.

50 趨勢科技。(2020 年 11 月 16 日)。*趨勢科技*。「駭客瞄準 Zoom、Slack、Discord 等常用的應用程式」(Malicious Actors Target Comm Apps such as Zoom, Slack, Discord)。上次存取時間 2021 年 1 月 19 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord.

51 Raphael Centeno、Bren Matthew Ebriega 與 Llalum Victoria。(2020 年 5 月 21 日)。*趨勢科技*。「冒牌 Zoom 安裝檔暗藏後門程式與 Devil Shadow 殭屍網路」(Backdoor, Devil Shadow Botnet Hidden in Fake Zoom Installers)。上次存取時間 2021 年 2 月 5 日： https://www.trendmicro.com/en_us/research/20/e/backdoor-devil-shadow-botnet-hidden-in-fake-zoom-installers.html.

52 趨勢科技。(2020 年 11 月 16 日)。*趨勢科技*。「駭客瞄準 Zoom、Slack、Discord 等常用的應用程式」(Malicious Actors Target Comm Apps such as Zoom, Slack, Discord)。上次存取時間 2021 年 1 月 19 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord.

53 趨勢科技。(2020 年)。*趨勢科技*。「2020 年網路資安風險指標涵蓋全球」(The 2020 Cyber Risk Index Goes Global)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/en_us/research/20/l/2020-cyber-risk-index-global.html.

54 趨勢科技。(2020 年 5 月 14 日)。*趨勢科技*。「雲端安全：重要概念、威脅與解決方案」(Cloud Security: Key Concepts, Threats, and Solutions)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions.

55 趨勢科技。(2020 年 4 月 7 日)。*趨勢科技*。「組態設定錯誤的 Docker Daemon API 連接埠遭 Kinsing 惡意程式的駭客集團攻擊」(Misconfigured Docker Daemon API Ports Attacked for Kinsing Malware Campaign)。上次存取時間 2021 年 2 月 5 日： https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/misconfigured-docker-daemon-api-ports-attacked-for-kinsing-malware-campaign.

56 Augusto Remillano II 與 Jemimah Molina。(2020 年 5 月 6 日)。*趨勢科技*。「Coinminer、DDoS 殭屍網路攻擊 Docker Daemon 連接埠」(Coinminer, DDoS Bot Attack Docker Daemon Ports)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/coinminer-ddos-bot-attack-docker-daemon-ports.

57 David Fiser。(2020 年 12 月 18 日)。*趨勢科技*。「TeamTNT 正在散布具備 DDoS 攻擊能力的 IRC 殭屍病毒 TNTbotinger」(TeamTNT Now Deploying DDoS-Capable IRC Bot TNTbotinger)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html.

58 Alfredo Oliveira 與 David Fiser。(2020 年 10 月 12 日)。*趨勢科技*。「Metasploit shellcode 攻擊暴露在外的 Docker API」(Metasploit Shellcodes Attack Exposed Docker APIs)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/en_us/research/20/j/metasploit-shellcodes-attack-exposed-docker-apis.html.

59 Vladimir Kropotov、Robert McArdle 和 Fyodor Yarochkin。(2020 年 9 月 1 日)。*趨勢科技*。「網路犯罪基礎架構商品化：探索地下網路犯罪服務市場」(Commodified Cybercrime Infrastructure: Exploring the Underground Services Market for Cybercriminals)。上次存取時間 2021 年 1 月 20 日：https://www. trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals.

60 Vladimir Kropotov 與 Fyodor Yarochkin。(2020 年 11 月 16 日)。*趨勢科技*。「網路犯罪『記錄雲』」(Cybercriminal 'Cloud of Logs')。上次存取時間 2021 年 1 月 24 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-cloud-of-logs-the-emerging-underground-business-of-selling-access-to-stolen-data.

61 趨勢科技。(2020 年 12 月 8 日)。*趨勢科技*。「扭轉潮流：趨勢科技 2021 年資安預測」(Turning the Tide: Trend Micro Security Predictions for 2021)。上次存取時間 2021 年 1 月 22 日：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021.

62 趨勢科技。(2020 年 8 月 26 日)。*趨勢科技*。「保護因疫情而改變的工作環境」(Securing the Pandemic-Disrupted Workplace)。上次存取時間 2021 年 1 月 21 日：https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf.

63 Amine Amri 等人。(2020 年)。*Forescout*。「AMNESIA:33 IoT、OT 及 IT 裝置 TCP/IP 堆疊重大漏洞是怎麼來的」(AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices)。上次存取時間 2021 年 1 月 22 日：https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices.

64 Amine Amri 等人。(2020 年)。*Forescout*。「AMNESIA:33 IoT、OT 及 IT 裝置 TCP/IP 堆疊重大漏洞是怎麼來的」(AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices)。上次存取時間 2021 年 1 月 22 日：https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices.

65 趨勢科技。(2016 年 9 月 13 日)。*趨勢科技*。「Linux 安全：深入探討最新 Linux 威脅」(Linux Security: A Closer Look at the Latest Linux Threats)。上次存取時間 2021 年 2 月 9 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-security-a-closer-look-at-the-latest-linux-threats.

66 Augusto Remillano II 與 Jemimah Molina。(2020 年 7 月 8 日)。*趨勢科技*。「最新 Mirai 變種功能更強，攻擊 CVE-2020-1017 漏洞」(New Mirai Variant Expands, Exploits CVE-2020-1017)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/en_us/research/20/g/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173.html.

67 Fernando Merces、Augusto Remillano II 與 Jemimah Molina。(2020 年 7 月 28 日)。*趨勢科技*。「Mirai 殭屍網路利用 CVE-2020-5902 漏洞攻擊 IoT 裝置」(Mirai Botnet Attack IoT Devices via CVE-2020-5902)。上次存取時間 2021 年 1 月 20 日：https://www.trendmicro.com/en_us/research/20/g/mirai-botnet-attack-iot-devices-via-cve-2020-5902.html.

68 Zhengyu Dong。(2020 年 11 月 9 日)。*趨勢科技*。「Joker 惡意程式新伎倆：使用 Github 來隱藏惡意檔案」(An Old Joker's New Tricks: Using Github To Hide Its Payload)。上次存取時間 2021 年 1 月 21 日：https://www.trendmicro.com/en_us/research/20/k/an-old-jokers-new-tricks--using-github-to-hide-its-payload. html.

69 Vit Sembera。(2020 年 12 月 3 日)。*趨勢科技*。「從 Geost 到 Locker：監控 Android 惡意程式加密編碼技術的演變」(From Geost to Locker: Monitoring the Evolution of Android Malware Obfuscation)。上次存取時間 2021 年 1 月 21 日：https://www.trendmicro.com/en_us/research/20/l/from-geost-to-locker-monitoring-the-evolution.html.

70 National Institute of Standards and Technology。(日期不詳)。*National Vulnerability Database*。「漏洞數據」(Vulnerability Metrics)。上次存取時間 2021 年 2 月 5 日：https://nvd.nist.gov/vuln-metrics/cvss.

71 Common Vulnerabilities and Exposures。(日期不詳)。*Common Vulnerabilities and Exposures*。「CVE-2020-1472」。上次存取時間 2021 年 1 月 22 日：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472.

72 Ophtek, LLC.。(日期不詳)。*Ophtek*。「Zerologon 是最新的 Microsoft 漏洞」(Zerologon is the Latest Microsoft Vulnerability)。上次存取時間 2021 年 2 月 10 日： https://ophtek.com/zerologon-is-the-latest-microsoft-vulnerability.

73 趨勢科技。(日期不詳)。*趨勢科技*。「何謂 Zerologon？」(What is Zerologon?)。上次存取時間 2021 年 1 月 22 日：https://www.trendmicro.com/en_us/what-is/zerologon.html.

74 趨勢科技。(日期不詳)。*趨勢科技*。「何謂 Zerologon？」(What is Zerologon?)。上次存取時間 2021 年 1 月 22 日：https://www.trendmicro.com/en_us/what-is/zerologon.html.

75 Microsoft。(2020 年 8 月 8 日)。*Microsoft*。「Netlogon 權限提升漏洞 (CVE-2020-1472)」(Netlogon Elevation of Privilege Vulnerability [CVE-2020-1472])。上次存取時間 2021 年 1 月 22 日： https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472.

76 Lindsey O'Donnell。(2021 年 1 月 15 日)。*Threatpost*。「Microsoft 實作 Windows Zerologon 漏洞『強制模式』」(Microsoft Implements Windows Zerologon Flaw 'Enforcement Mode')。上次存取時間 2021 年 2 月 10 日：https://threatpost.com/microsoft-implements-windows-zerologon-flaw-enforcement-mode/163104/.

77 FireEye, Inc 與 Ponemon Institute LLC.。(2021 年)。*Respond Software*。「資安營運中心經濟第二屆年度研究：達成有效成果的真實成本為何？」(Second Annual Study on the Economics of Security Operations Centers: What is the True Cost for Effective Results?)。上次存取時間 2021 年 1 月 19 日：https://d53g0hkpcf8eh. cloudfront.net/wp-content/uploads/2021/01/Ponemon-Institute-FireEye-Second-Annual-Study-Economics-of-the-SOC-2021. pdf.

78 趨勢科技。(2017 年 10 月 4 日)。*趨勢科技*。「最佳實務原則：分辨與防範網路釣魚攻擊」(Best Practices: Identifying and Mitigating Phishing Attacks)。上次存取時間 2021 年 1 月 24 日：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/best-practices-identifying-and-mitigating-phishing-attacks.

79 趨勢科技。(2018 年 10 月 25 日)。*趨勢科技*。「虛擬修補：在漏洞遭到攻擊之前預先加以修補」(Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited)。上次存取時間 2021 年 1 月 22 日：https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited.

80 趨勢科技。(2020 年 25 月 4 日)。*趨勢科技*。「持續蔓延的複雜威脅」(The Sprawling Reach of Complex Threats)。上次存取時間 2021 年 1 月 21 日：https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf.

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

©2021 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、Trend Micro Smart Protection Network、Trend Micro Smart Home Network 以及 Trend Micro Zero Day Initiative 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。