Symantec™

ISTR

網路安全威脅報告

第 24 期 | 2019 年 2 月

本文件按「現狀」提供，不做任何明示或默示的條件、陳述和擔保，包括對適銷性、特定用途適用性或非侵權的默示保證，若此免責聲明在法律上無效則不在此限。

賽門鐵克公司對於本文件提供、表現或使用的附帶或後續損害概不負責。本文件所述資訊如有變更，恕不另行通知。

來自第三方的資訊理應可靠，但無法對此做出保證。

本文件中所引用的安全產品、技術服務和其他技術資料(以下稱「受管制項目」)受美國出口管制和制裁法律、法規和要求約束，並可能受其他國家或地區的進出口法規約束。

您同意謹遵這些法律、法規和要求，且確認自己有責取得可能必要之任何執照、許可或其他核准，以便將受控項目出口、再出口、國內轉運或進口。

目錄

1

重大數據

2

年度回顧

表單點擊劫持

挖礦綁架

勒索軟體

自給自足戰術和供應鏈攻擊

目標式攻擊

雲端

物聯網 (IoT)

選舉干擾

3

事實與圖表

訊息

惡意程式

行動裝置

網路攻擊

目標式攻擊

物聯網 (IoT)

地下經濟

研究方法

BIG NUMBERS

重大數據

Symantec™

惡意 URL

網路攻擊

表單點擊劫持攻擊

4,800

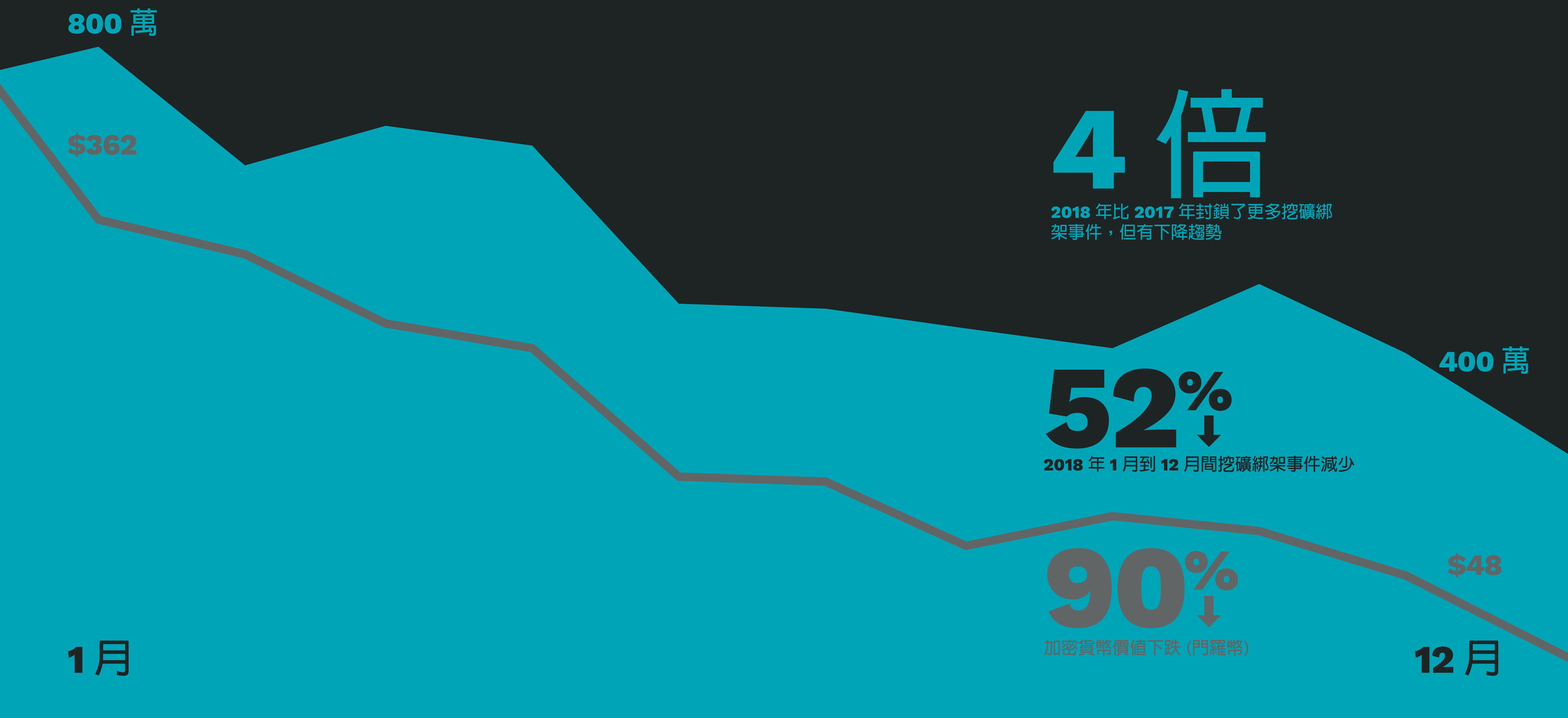
平均每月遭表單點擊劫持程式碼入侵的網站數量

已封鎖的

端點表單點擊劫持攻擊

370 萬

挖礦綁架



4 倍

2018 年比 2017 年封鎖了更多挖礦綁架事件，但有下降趨勢

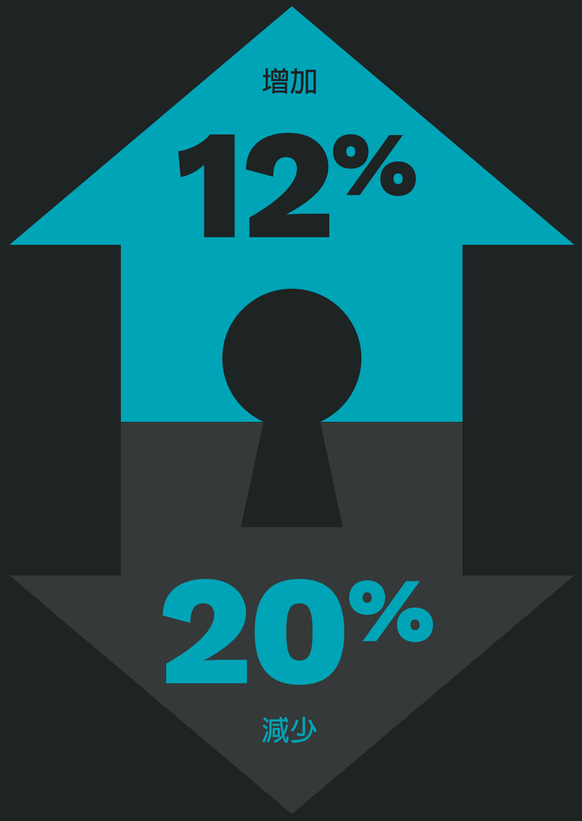
52%↓

2018 年 1 月到 12 月間挖礦綁架事件減少

90%↓

加密貨幣價值下跌 (門羅幣)

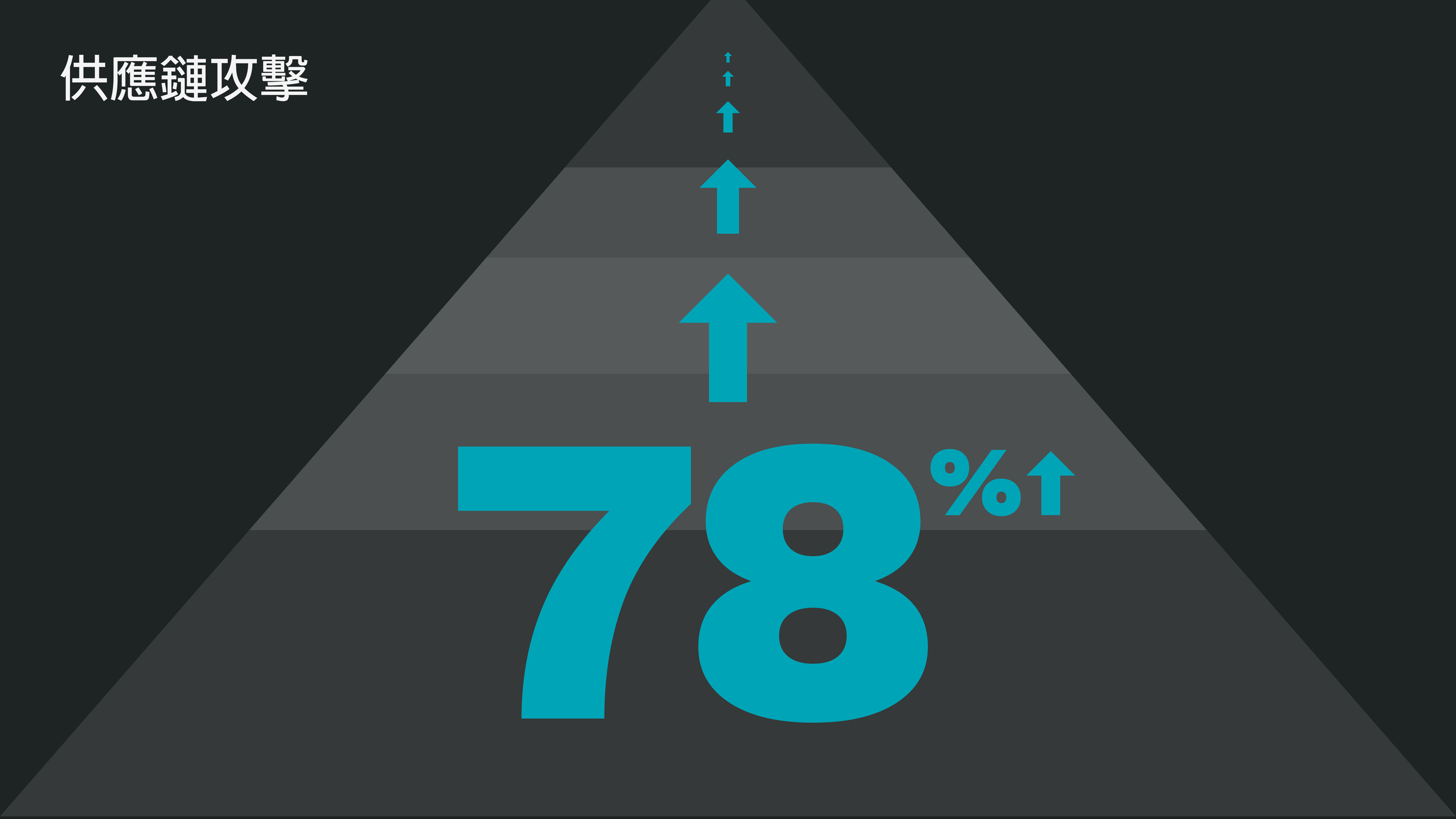
企業勒索軟體



勒索軟體總數

行動勒索軟體

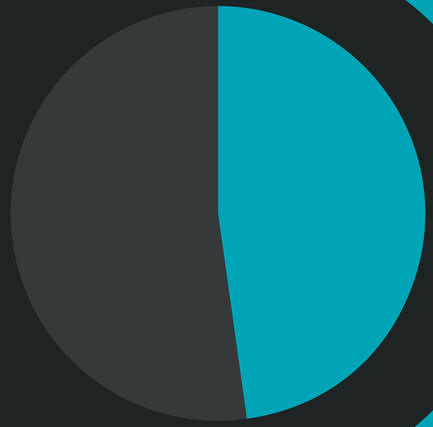
供應鏈攻擊



惡意電子郵件

48%

惡意電子郵件附件為 **Office** 檔案，從 **2017** 年的 **5%** 迅速飆升



Powershell

1000%

惡意 **PowerShell** 指令碼增加

使用破壞性惡意軟體的攻擊集團數量

平均每個攻擊集團鎖定的組織數量

YEAR IN REVIEW 2

年度回顧

Symantec™

{FORMJACKING}
表單點擊劫持

網路罪犯鎖定支付卡資料。

表單點擊劫持事件 - 使用惡意的 JavaScript 程式碼，從電子商務網站結帳網頁的付款表單，竊取信用卡詳細資料和其他資訊 - 2018 年有增加趨勢。

賽門鐵克資料顯示，2018 年每月有 4,818 個不同的網站遭表單點擊劫持程式碼入侵。每張信用卡資料在地下市場售價高達 45 美元，若每月能從受感染網站竊取 10 張信用卡，網路罪犯即可賺取高達 220 萬美元；因此，表單點擊劫持對於網路罪犯的吸引力顯而易見。

賽門鐵克在 2018 年阻止了超過 370 萬次表單點擊劫持嘗試，僅在去年最後兩個月就封鎖超過 100 萬次。表單點擊劫持在 2018 全年皆有發生，5 月活動異常激增 (僅當月就有 556,000 次嘗試)，隨後半年活動整體呈上升趨勢。

大多數表單點擊劫持可歸咎於暱稱為 Magecart 的犯罪集團，該組織由數個團體組成，其中至少有一些會彼此競爭。Magecart 據信策動了多場重大攻擊事件，目標包括英國航空公司、Ticketmaster、英國電子零售商 Kitronik 以及隱形眼鏡銷售商 VisionDirect。

這波表單點擊劫持的增加，反映出供應鏈攻擊普遍成長的趨勢，並與我們在 ISTR 23 期的分析結果相符；在許多案例中，Magecart 專挑第三方服務下手，藉此將程式碼植入目標網站。例如 Ticketmaster 遭大舉入侵的案件中，Magecart 破解了第三方聊天機器人，從而將惡意程式碼載入 Ticketmaster 網站訪客的網頁瀏覽器，藉此收集客戶的支付資料。

雖然知名品牌遭受攻擊的事件較令人矚目，但賽門鐵克的遙測資料顯示，表單點擊劫持程式碼的植入目標通常是中小型零售商網站，包括服裝、園藝設備及醫療用品等產業。這是一個全球性的問題，任何接受客戶線上付款的企業都可能受影響。

2018 年表單點擊劫持的增長趨勢，部分原因在於該年加密貨幣價值下滑，導致原本透過網站進行挖礦綁架的網路罪犯，如今可能改採表單點擊劫持的手法。就目前的行情而言，失竊信用卡個資在地下網路的價值，可能比加密貨幣更有利可圖。

CRYPTOJACKING

挖礦綁架

逐漸減少，但並未消失。

挖礦綁架 - 網路罪犯在受害者裝置暗中執行加密貨幣挖礦程式，而受害者對此一無所悉，他們還會盜用處理器 (CPU) 的運算能力來挖掘加密貨幣 - 這是 2017 年最後一季的盛行手法，也仍是 2018 年網路安全情勢的主要特徵之一。

挖礦綁架活動在 2017 年 12 月至 2018 年 2 月達到頂峰，賽門鐵克在此期間每月封鎖約 800 萬次挖礦綁架事件。我們在 2018 年封鎖的挖礦綁架事件，數目超過了 2017 年的四倍 - 在當年 12 個月內封鎖將近 6900 萬次，而 2017 年僅略多於 1600 萬次。然而，去年的挖礦綁架活動確實有所減少，自 2018 年 1 月至 12 月下降了 52%。雖然挖礦綁架活動趨減，但我們仍在 2018 年 12 月阻止了超過 350 萬次相關事件。

這仍然是一項顯著的活動，雖然加密貨幣價值在 2017 年底居於新高，成為挖礦綁架初期成長的主要驅力，但幣值隨後在 2018 年大幅下降。這可能使一些原本使用挖礦綁架的轉向表單點擊劫持等其他牟利手法，但顯然仍有大批網路罪犯看好挖礦綁架的時間報酬效益。在 2018 年，我們也發現部分挖礦綁架罪犯鎖定企業下手，採用 WannaMine(MSH.Bluwimps) 挖礦綁架指令碼，藉由 WannaCry 惡名昭彰的 Eternal Blue 刺探攻擊，大規模感染企業網路，導致特定設備因 CPU 使用率過高而停擺。

2018 年大多數的挖礦綁架活動，仍是源自瀏覽器加密貨幣挖礦程式。瀏覽器加密貨幣挖礦攻擊是透過 Web 瀏覽器發動，並採用指令碼語言來執行。如果網頁包含加密貨幣挖礦指令碼，只要訪客開啟網頁，其裝置的運算能力就會用來挖掘加密貨幣。憑藉瀏覽器加密貨幣挖礦程式，網路罪犯甚至可鎖定完全修補的裝置，並且暗中操控，而不引起受害者的注意。

我們預測，網路罪犯從事挖礦綁架的活躍程度，大致取決於加密貨幣價值是否維持高位。隨著加密貨幣價值下跌，我們也觀察到挖礦綁架事件的數量減少。然而，它們與加密貨幣價值的減幅並不相同：門羅幣 (Monero) 在 2018 年價值下跌近 90%，而挖礦綁架比例則減少約 52%。這表示一些網路罪犯仍認為此手法有利可圖，或在等待加密貨幣行情再次飆升。這個現象也顯示，挖礦綁架對於網路罪犯仍有其他誘因，例如匿名特性和較低的進入門檻。目前看來，挖礦綁架仍在網路犯罪領域中佔有一席之地。

活動開始減少，但仍是組織的挑戰。

自 2013 年以來，我們在 2018 年首次觀察到勒索軟體活動減少，端點上的勒索軟體感染總數下降了 20%。WannaCry、仿冒版本和 Petya 持續誇大了感染數據。從統計數據中刪除這些蠕蟲後，感染數量更大幅下降了 52%。

然而，在這些整體數據中，有一項戲劇性的變化。直到 2017 年，消費者受到勒索軟體重創最深，佔感染事件中的絕大多數。2017 年，資安事件的分布逐漸傾向企業，大多數感染都發生在該領域。2018 年，這項轉變加劇，在所有勒索軟體感染的事件中，企業就佔有 81%。雖然整體勒索軟體感染率下降，但 2018 年企業感染率上升了 12%。

受害者特徵的轉變，可能起因於刺探攻擊套件活動減少，這先前是挾帶勒索軟體的重要手段。在 2018 年期間，勒索軟體主要是透過電子郵件行銷活動散布。由於電子郵件仍是組織主要的通訊工具，因此企業較容易遭受電子郵件攻擊。

除此之外，愈來愈多消費者只使用行動裝置，並習慣將重要資料備份到雲端。由於主要勒索軟體系列大多仍以 Windows 電腦為目標，因此消費者受勒索軟體感染的可能性逐漸減低。

勒索軟體活動整體減少的另一項原因，在於賽門鐵克採用了電子郵件保護、行為分析和機器學習等技術，有效提高防禦效率，可在感染初期更快封鎖勒索軟體。部分網路犯罪團夥逐漸失去對勒索軟體的興趣，也導致了活動減少的趨勢。賽門鐵克觀察到，許多原本散布勒索軟體的團夥，已逐漸改用其他惡意程式，如銀行交易特洛伊木馬程式和資訊竊取程式。

但是，特定犯罪集團仍構成嚴重威脅。對於組織不利的另一項壞消息，則是 2018 年發生多起以組織為對象、具高度破壞性的目標式勒索軟體攻擊，其中許多是由 SamSam 集團犯案。在 2018 年，賽門鐵克發現 67 次 SamSam 攻擊的證據，主要針對美國境內組織；而其他使用目標式勒索軟體的犯罪集團，也隨著 SamSam 變得更加活躍。

於此同時，其他目標式威脅也紛紛出現。涉及 Ryuk (Ransom.Hermes) 的活動在 2018 年年末顯著增加。這種勒索軟體是 12 月攻擊事件的元兇，中斷了美國多家知名報紙的印刷和發行作業。

Dharma/Crysis (Ransom.Crysis) 也經常採用目標式攻擊來入侵組織。賽門鐵克發現 Dharma/Crysis 感染次數在 2018 年增加超過兩倍，從 2017 年平均每月 1,473 次，到 2018 年的每月 4,900 次。

在 11 月間，兩名伊朗公民因涉嫌 SamSam 攻擊而在美國遭起訴。這項起訴案是否影響該集團的活動，仍有待觀察。

勒索軟體

LIVING OFF THE LAND AND SUPPLY CHAIN ATTACKS

自給自足戰術和供應鏈攻擊

仍是新興威脅態勢中的要角。

我們在上一期報告中強調，愈來愈多歹徒採用現成工具和作業系統功能發動攻擊；這種「自給自足戰術」的趨勢並無減弱跡象 - 事實上，有些活動甚至在 2018 年顯著增加。PowerShell 在網路犯罪和目標式攻擊中仍佔大宗 - 反映在 2018 年端點的惡意 PowerShell 指令碼大幅增加 1,000%。

在 2018 年，Microsoft Office 檔案佔所有惡意電子郵件附件將近半數 (48%)，遠高於 2017 年的 5%。在 2018 年，Mealybug 和 Necurs 等網路犯罪組織，仍使用 Office 檔案巨集作為散布惡意酬載的首選方法，但也嘗試使用具有 DDE 酬載的惡意 XML 和 Office 檔案。

目標式攻擊集團在 2018 年使用零時差漏洞的比例持續下降，其中僅 23% 的攻擊集團使用零時差，低於 2017 年的 27%。我們也逐漸發現，有些攻擊僅憑藉「自給自足」技術而不採用任何惡意程式碼，例如目標式攻擊組織「Gallmaker」的手法就有此轉變，他們專門利用唾手可得的工具來執行惡意活動。

自行傳播的威脅仍使企業組織頭痛不已，但新型蠕蟲有別於舊型蠕蟲，並不透過遠端刺探所發現的漏洞進行傳播。反之，諸如 Emotet (Trojan.Emotet) 和 Qakbot (W32.Qakbot) 等蠕蟲藉由從記憶體轉儲密碼或暴力存取網路共用區等簡單技術，即可在網路中橫向移動。

供應鏈攻擊仍是一項顯著的威脅態勢，2018 年的攻擊增加了 78%。供應鏈攻擊利用第三方服務和軟體來破壞最終目標，手法五花八門，包括劫持軟體更新、將惡意程式碼植入合法軟體等。開發人員仍被利用為供應鏈攻擊的來源，攻擊者的手法包括竊取版本控制工具憑證，或破壞較大軟體專案的第三方程式庫。

對於網路零售商和電商網站來說，2018 年表單點擊劫持案件激增，使得供應鏈成為更顯著的弱點。在許多表單點擊劫持的案例中，攻擊者破壞的目標是網路零售商常用的第三方服務，例如聊天機器人或客戶評論小工具。

供應鏈和自給自足戰術的攻擊，都突顯組織和個人面臨的挑戰，愈來愈多攻擊透過可信賴的通路傳播，包括使用無檔案攻擊法，或惡意濫用合法工具。雖然我們每個月平均封鎖 115,000 個惡意 PowerShell 指令碼，但這還不到 PowerShell 總體使用量的 1%。要有效識別和封鎖這些攻擊，必須使用先進的偵測方法，例如分析和機器學習。

MORE AMBITIOUS
野心更大

AND STEALTHIER
更為隱匿

目標式攻擊者在 2018 年仍對組織構成重大威脅，新的集團不斷湧現，既有團體也持續改進工具和策略。更大型、活躍的攻擊集團似乎在 2018 年加強了活動力道。賽門鐵克追蹤的 20 個最活躍的集團過去三年平均鎖定 55 個組織下手，而 2015 年至 2017 年間則為 42 個。

值得注意的趨勢在於目標的多樣化，愈來愈多團體顯然有意入侵營運用電腦，歹徒一旦得逞，即可隨意展開破壞行動。

TARGETED ATTACKS.
目標式攻擊。

這種策略是由間諜組織「Dragonfly」所開創，他們以攻擊能源公司而聞名。在 2018 年期間，我們發現「Thrip」集團入侵衛星通訊營運商並感染數台電腦，這些設備負責執行特定軟體，用於監測和控制衛星。憑藉這場襲擊，Thrip 將有能力嚴重破壞公司的營運。

我們也看到「Chafer」集團入侵了中東地區一家電信服務供應商。這間公司向當地多家電信營運商銷售解決方案，而此攻擊可能是為了加強監控這些營運商的一般使用者客戶。

已知使用破壞性惡意程式的集團數量，在 2018 年成長了 25%，這也顯示歹徒有興趣採用具有潛在破壞性的攻擊。

在 2018 年期間，賽門鐵克揭發了四個先前未知的目標式攻擊集團，這也是賽門鐵克自 2009 年以來率先揭發的第 32 個同類組織。雖然賽門鐵克在 2017 年和 2018 年個別揭發了四個新的集團，但發現他們的方式截然不同。2018 年揭發的四個新集團中，有兩個是因使用「自給自足」工具而曝光；實際上，其中一個集團 (Gallmaker) 的攻擊並未使用任何惡意程式，完全憑藉自給自足和公開可用的駭客工具。

近年來，目標式攻擊團體日漸偏好自給自足戰術，如此可在大量合法流程中隱匿惡意活動，有助於攻擊者保持低調。賽門鐵克在 2018 年開發目標式攻擊分析 (TAA) 解決方案，主要就是為了因應上述趨勢，這套解決方案採用先進的人工智慧，可偵測各種涉及目標式攻擊的惡意活動模式。在 2018 年，我們在調查中兩度揭發先前未知的目標式攻擊集團，他們就是因為「自給自足」工具被 TAA 發現而曝露行蹤。隨著自給自足工具的興起，其他較舊攻擊技術逐漸衰微。已知使用零時差漏洞的目標式攻擊集團數量為 23%，低於 2017 年底的 27%。

2018 年最引人注目的發展之一，就是美國大舉起訴國家資助的間諜嫌疑人，數量顯著高於以往。2018 年間，共有 49 名個人或組織遭起訴，而 2017 年為 4 起，2016 年為 5 起。雖然媒體大多聚焦於涉嫌 2016 年總統大選攻擊事件的 18 名俄羅斯特務嫌犯，但這類起訴案件的範圍遠大於此。除了俄羅斯公民以外，亦有 19 名中國個人或組織遭起訴，此外還有 11 名伊朗人士和一名北韓人士。

這類消息經媒體大幅披露後，可能阻撓部分遭起訴組織的行動，大幅限縮遭起訴者跨國旅行的能力，使其無法對他國目標展開行動。

安全挑戰：各種資安防線如臨大敵

從簡單的配置不當，乃至於硬體晶片漏洞等問題，我們在 2018 年注意到雲端環境的各種安全挑戰。

欠缺保護的雲端資料庫仍是組織的一大弱點。在 2018 年，S3 儲存貯體成為組織的致命傷，超過 7000 萬條記錄因配置不當而遭竊或洩露。在此之前，2017 年曾發生一連串針對 MongoDB 等開放資料庫的勒索軟體攻擊，攻擊者將內容刪除一空，要脅付款方可復原。但攻擊者並未就此止步，還鎖定容器部署系統下手，如 Kubernetes、無伺服器應用程式和其他公開 API 服務。而這些事件的共通之處，即在於不當的配置。

潛在的攻擊者會透過許多普遍可用的工具，在網路上找出配置不當的雲端資源。除非組織採取行動，妥善保護雲端資源 (例如遵循 Amazon 的建議來保護 S3 儲存貯體)，否則就會曝露在攻擊的風險中。

隨著硬體晶片出現多個漏洞，雲端環境在 2018 年面臨更加險惡的威脅。Meltdown 和 Spectter 會透過「推測執行」的流程來刺探漏洞。成功的攻擊行動讓攻擊者得以進入平常禁止存取的記憶體位置。對於雲端服務來說這個問題特別嚴重，因為雲端實例雖然有自己的虛擬處理器，卻共享記憶體群組，這表示只要一個實體系統遭成功侵入，就可能導致數個雲端實例的資料外洩。

Meltdown 和 Spectre 並非個案，這些攻擊的多種變體，在隨後的一整年間散布至公開網域。在此之後，也出現了類似的晶片層漏洞，例如 Speculative Store Bypass 和 Foreshadow，或 L1 Terminal Fault 等。這可能只是一個開端，因為研究人員和攻擊者都在關注晶片層的漏洞，表明雲端運算面臨前所未有的挑戰。

網路罪犯和目標式攻擊集團的鎖定對象

雖然蠕蟲和機器人仍佔物聯網 (IoT) 攻擊的大宗，但 2018 年出現一種新的威脅，即目標式攻擊者意圖利用物聯網作為感染媒介。

物聯網攻擊總數在 2018 年仍然偏高，相較 2017 年大致持平 (-0.2%)。路由器和連線攝影機是受感染最多的設備，分別佔攻擊事件中的 75% 和 15%。毫無疑問，路由器是最常淪為目標的裝置，它們不僅可透過網路存取，亦可提供有效的起點，也因此備受攻擊者青睞。

惡名昭彰的 Mirai 分散式阻斷服務 (DDoS) 蠕蟲仍是一項活躍的威脅，佔攻擊總數的 16%，是 2018 年第三常見的物聯網威脅。Mirai 不斷進化，變種使用多達 16 種刺探攻擊，持續增加漏洞以提高感染成功率，因為裝置通常處於未修補的狀態。這種蠕蟲也會追蹤未修補的 Linux 伺服器，藉以擴大目標範圍。另一項值得注意的趨勢，則是工業控制系統 (ICS) 遭到更多攻擊。Thrip 集團專挑衛星下手，Triton 則攻擊工業安全系統，使其容易遭到破壞或勒索攻擊，任何運算裝置都可能成為目標。

在 2018 年，VPNFilter 的出現象徵了物聯網威脅的演變。VPNFilter 是第一種散布廣泛且持久的 IoT 威脅，能在系統重啟後繼續存活，非常難以根除。有別於 DDoS 和加密貨幣挖礦等傳統物聯網威脅活動，VPNFilter 攜帶一系列強效的酬載 (例如中間人 [MitM]攻擊、資料外洩、憑證竊取及 SCADA 通訊攔截)，並且具備另一種破壞能力，可依攻擊者指令將裝置「磚化」(即無法操作) 或刪除，藉此湮滅證據。VPNFilter 出自於技能嫻熟、資源充足的威脅者之手，顯示物聯網裝置的多道防線都面臨攻擊。

ELECTION INTERFERENCE 2018

2018 年選舉干擾

由於 2016 年美國總統大選數度遭到網路攻擊 (例如對民主黨全國委員會 [DNC] 的攻擊)，因此 2018 年的期中選舉備受矚目。僅在選舉日一個月後，共和黨眾議院全國委員會 (NRCC) 證實，其電子郵件系統曾遭受不明第三方攻擊，事件發生於期中選前階段。據報導，駭客竊得四名 NRCC 資深助理電子郵件帳戶的存取權限，並可能在幾個月內蒐集數千封電子郵件。

然後在 2019 年 1 月，DNC 披露在期中選舉結束後不久，他們一度成為目標式魚叉式網路釣魚攻擊的目標，所幸對方並未得逞 。根據美國國土安全局 (DHS) 和聯邦調查局判定，俄羅斯網路間諜組織「APT29 」是上述行動的主謀。

在 2018 年 7 月和 8 月，微軟發現並關閉了多個模仿政治組織網站的惡意網域。一般認為，網路間諜組織 APT28 (經國土安全局和聯邦調查局認定為俄羅斯籍) 架設了這些網站，藉此對 2018 年期中選舉候選人展開魚叉式網路釣魚攻擊。為了反制這類網站詐騙攻擊，賽門鐵克推出了海豚計劃防詐騙服務 (Project Dolphin) ，這是一款免費安全工具，適合網站持有人使用。

2018 年，攻擊者仍專注於利用社交媒體平台來影響選民，雖然這並非新鮮事，但使用的策略更加複雜。例如一些與俄羅斯相關的帳戶透過第三方來購買社交媒體廣告，並避免使用俄羅斯 IP 位址或俄羅斯貨幣。假帳號也開始著重於宣傳活動和集會，而這類事件不像政治廣告那樣受到密切監控。

在 2018 年，社交媒體公司和政府機關更積極防治選舉干預。Facebook 成立了「戰情室」來對抗選舉干擾，並封鎖許多疑似與外國組織相關的帳號和專頁，其涉嫌企圖影響美國、英國和中南美洲的政治局勢。

Twitter 刪除了超過 10,000 個機器人，以防阻止其散播特定訊息，鼓勵人們不去投票；並且更新相關規則，以利辨別假帳號和保護選舉的公正性。Twitter 還發布了一系列推文記錄，其涉嫌接受國家資助進行政治宣傳，濫用平台傳播不實資訊，企圖影響公眾輿論。

2018 年打擊選舉干擾的其他行動包括美國網戰司令部直接聯絡俄羅斯駭客，警告對方已遭美國特務認出並追蹤；國土安全局提供各州選務機器和程序的免費安全評估；以及廣泛採用「艾伯特感應器」(Albert sensor)，這類硬體可協助聯邦政府監測任何干擾選務電腦的證據。

3 FACTS AND FIGURES

事實與圖表

Symantec™

傳達訊息

在 2018 年，小型組織的員工比大型組織的員工更容易受到電子郵件威脅攻擊，包括垃圾郵件、網路釣魚和電子郵件惡意程式。我們也發現，自 2015 年以來，垃圾郵件的氾濫程度每年持續成長，而 2018 年也不例外，有 55% 的電子郵件歸類為垃圾郵件。同時，電子郵件惡意程式比例持平，而網路釣魚電子郵件比例下降，從 2017 年的 1/2995 減至 2018 年的 1/3207。過去四年中，網路釣魚比例逐年下降。

我們也發現惡意電子郵件所使用的 URL 較少，因為攻擊者恢復以往偏好，使用惡意電子郵件附件作為主要感染媒介。2017 年，電子郵件中惡意 URL 的使用率躍升至 12.3%，但在 2018 年回落至 7.8%。賽門鐵克遙測資料顯示，Microsoft Office 使用者最容易淪為電子郵件惡意程式的受害者，Office 檔案佔惡意電子郵件附件的 48%，遠高於 2017 年的 5%。

48%

惡意電子郵件附件為 **Office** 檔案，從 **2017** 年的 **5%** 迅速飆升

電子郵件偽裝成通知，例如發票或收據

1

附件的 **Office** 檔案包含惡意指令碼

2

開啟附件執行指令碼下載惡意程式

3

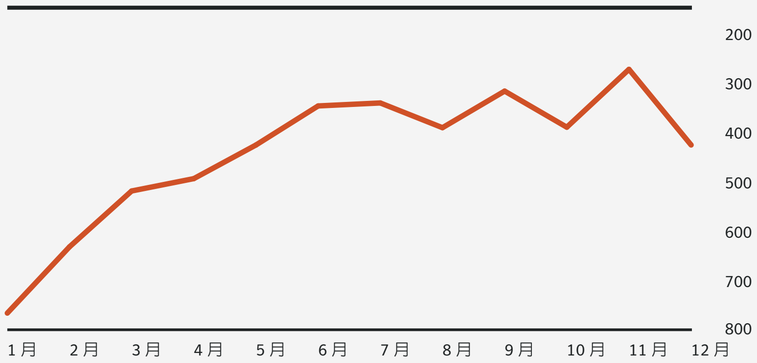
惡意電子郵件比例 (年)

2018
1/412

惡意電子郵件 URL 比例 (年)

2018
7.8%

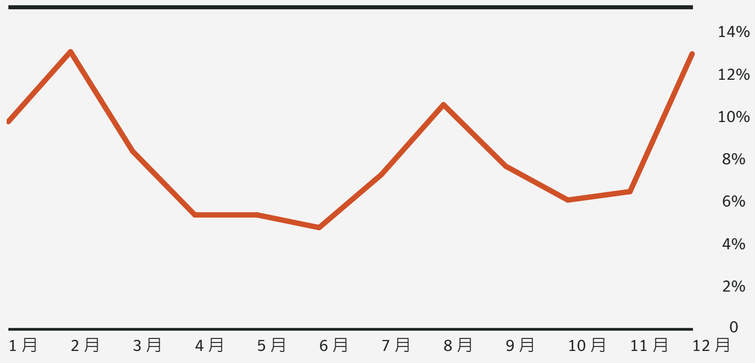
惡意電子郵件比例 (月)



惡意電子郵件比例 (1 封/每幾封)

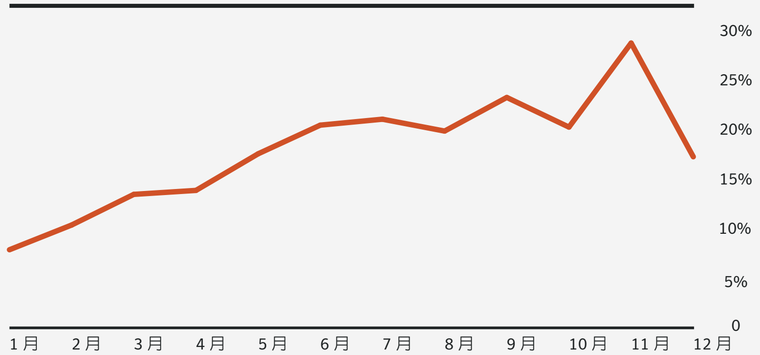
在 2018 年，遭惡意電子郵件攻擊的使用者比例有增加趨勢

惡意電子郵件 URL 比例 (月)



惡意郵件的百分比

單一使用者收到的惡意電子郵件數量 (月)



遭鎖定的使用者 (%)

各行業惡意電子郵件比例 (年)

行業	惡意電子郵件比例 (1 封/每幾封)
採礦業	258
農、林、漁業	302
公共行政	302
製造業	369
批發業	372
建築業	382
無法分類的機構	450
運輸及公用事業	452
金融、保險及不動產業	491
服務業	493
零售業	516

各行業惡意電子郵件 URL 比例 (年)

行業	電子郵件惡意程式 (%)
農、林、漁業	11.2
零售業	10.9
採礦業	8.9
服務業	8.2
建築業	7.9
公共行政	7.8
金融、保險及不動產業	7.7
製造業	7.2
無法分類的機構	7.2
批發業	6.5
運輸及公用事業	6.3

小型組織的員工比大型組織的員工更容易受到電子郵件威脅攻擊，包括垃圾郵件、網路釣魚和電子郵件惡意程式。

各行業單一使用者收到的惡意電子郵件數量 (年)

行業	遭鎖定的使用者 (%)
採礦業	38.4
批發業	36.6
建築業	26.6
無法分類的機構	21.2
零售業	21.2
農、林、漁業	21.1
製造業	20.6
公共行政	20.2
運輸及公用事業	20.0
服務業	11.7
金融、保險及不動產業	11.6

各規模組織收到的惡意電子郵件比例 (年)

組織規模	惡意電子郵件比例 (1 封/每幾封)
1-250	323
251-500	356
501-1000	391
1001-1500	823
1501-2500	440
2501+	556

各規模組織收到的惡意電子郵件 URL 率 (年)

組織規模	惡意電子郵件 (%)
1-250	6.6
251-500	8.3
501-1000	6.6
1001-1500	8.3
1501-2500	7.3
2501+	8.6

各組織規模單一使用者收到的惡意電子郵件數量 (年)

組織規模	遭鎖定的使用者 (1 名/ 每幾名)
1-250	6
251-500	6
501-1000	4
1001-1500	7
1501-2500	4
2501+	11

各國家/地區惡意電子郵件比例 (年)

國家/地區	惡意電子郵件比例 (1 封/每幾封)
沙烏地阿拉伯	118
以色列	122
奧地利	128
南非	131
塞爾維亞	137
希臘	142
阿曼	160
台灣	163
斯里蘭卡	169
阿拉伯聯合大公國	183
泰國	183
波蘭	185
挪威	190
匈牙利	213
卡達	226
新加坡	228
義大利	232
荷蘭	241
英國	255
愛爾蘭	263
盧森堡	272
香港	294
中國	309
丹麥	311
馬來西亞	311
哥倫比亞	328
瑞士	334
巴布亞紐幾內亞	350
德國	352
菲律賓	406
比利時	406
巴西	415
南韓	418
葡萄牙	447
西班牙	510
芬蘭	525
加拿大	525
瑞典	570
紐西蘭	660
美國	674
法國	725
澳洲	728
印度	772
墨西哥	850
日本	905

各國家/地區惡意電子郵件 URL 比例 (年)

國家/地區	惡意電子郵件 (%)
巴西	35.7
墨西哥	29.7
挪威	12.8
瑞典	12.4
加拿大	11.5
紐西蘭	11.3
哥倫比亞	11.0
澳洲	10.9
法國	10.5
芬蘭	9.7
瑞士	9.5
西班牙	9.4
卡達	8.9
美國	8.9
葡萄牙	8.4
印度	8.3
菲律賓	8.1
新加坡	7.7
盧森堡	7.3
義大利	7.1
奧地利	6.7
南非	6.7
巴布亞紐幾內亞	6.5
南韓	6.5
德國	6.3
日本	6.3
比利時	6.1
英國	6.1
匈牙利	5.9
沙烏地阿拉伯	5.2
丹麥	5.1
香港	5.1
馬來西亞	5.1
中國	4.9
荷蘭	4.9
塞爾維亞	4.4
台灣	4.4
阿拉伯聯合大公國	4.2
斯里蘭卡	4.1
愛爾蘭	3.9
阿曼	3.6
泰國	3.4
希臘	3.3
波蘭	2.8
以色列	1.9

熱門電子郵件主題 (年)

主旨主題	百分比
帳單	15.7
電子郵件傳送失敗	13.3
包裹遞送	2.4
法律/執法單位	1.1
掃描文件	0.3

熱門電子郵件關鍵字 (年)

字眼	百分比
發票	13.2
郵件	10.2
寄件人	9.2
付款	8.9
重要	8.5
訊息	7.7
全新	7.2
退回	6.9
:	6.9
傳送	6.6

熱門惡意電子郵件附件類型 (年)

檔案類型	百分比
.doc、.dot	37.0
.exe	19.5
.rtf	14.0
.xls、.xlt、.xla	7.2
.jar	5.6
.html、htm	5.5
.docx	2.3
.vbs	1.8
.xlsx	1.5
.pdf	0.8

熱門惡意電子郵件附件類別 (年)

檔案類型	百分比
指令碼	47.5
可執行檔	25.7
其他	25.1

BEC 每月平均詐騙目標組織數量 (年)

平均
5,803

單一組織收到的 BEC 電子郵件平均數量 (年)

平均
4.5

熱門 BEC 電子郵件關鍵字 (年)

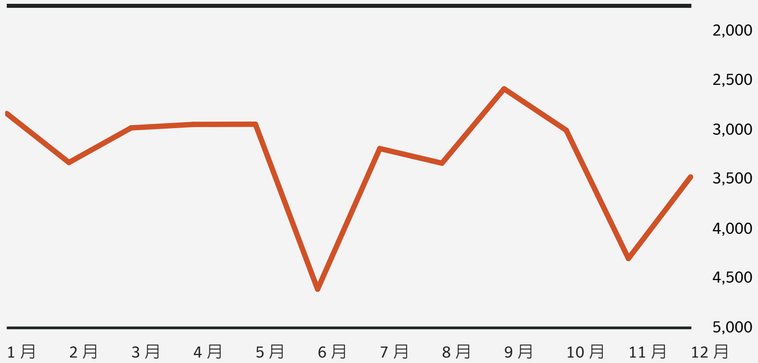
主旨	百分比
緊急	8.0
請求	5.8
重要	5.4
付款	5.2
注意	4.4
未結款項	4.1
資訊	3.6
重要更新	3.1
收件人	2.3
交易	2.3

電子郵件網路釣魚比例 (年)

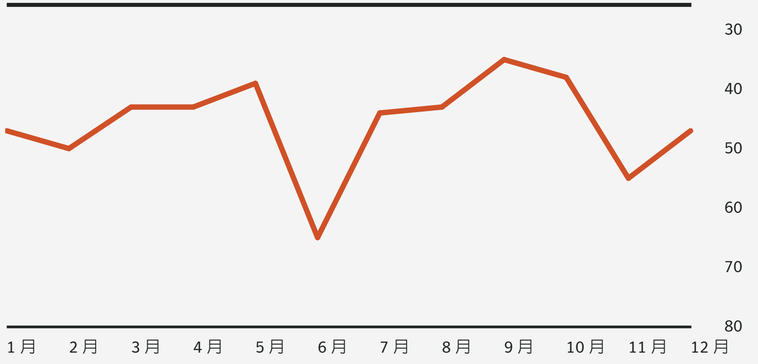
網路釣魚比例 (1 封/每幾封)
3,207

而網路釣魚電子郵件比例下降，從 2017 年的 1/2995 減至 2018 年的 1/3207。

電子郵件網路釣魚比例 (月)



單一使用者遭遇電子郵件網路釣魚比例 (月)



各行業電子郵件網路釣魚比例 (年)

行業	網路釣魚比例 (1 封/每幾封)
農、林、漁業	1,769
金融、保險及不動產業	2,628
採礦業	2,973
批發業	3,042
公共行政	3,473
服務業	3,679
建築業	3,960
零售業	3,971
製造業	3,986
無法分類的機構	5,047
運輸及公用事業	5,590

各行業單一使用者電子郵件網路釣魚比例 (年)

行業	遭鎖定的使用者 (1 名/ 每幾名)
批發業	22
農、林、漁業	28
採礦業	30
零售業	36
建築業	39
金融、保險及不動產業	46
製造業	52
無法分類的機構	53
公共行政	57
運輸及公用事業	62
服務業	64

各規模組織電子郵件網路釣魚比例 (年)

組織規模	網路釣魚比例 (1 封/每幾封)
1-250	2,696
251-500	3,193
501-1000	3,203
1001-1500	6,543
1501-2500	3,835
2501+	4,286

各規模組織單一使用者電子郵件網路釣魚比例 (年)

組織規模	遭鎖定的使用者 (1 名/ 每幾名)
1-250	52
251-500	57
501-1000	30
1001-1500	56
1501-2500	36
2501+	82

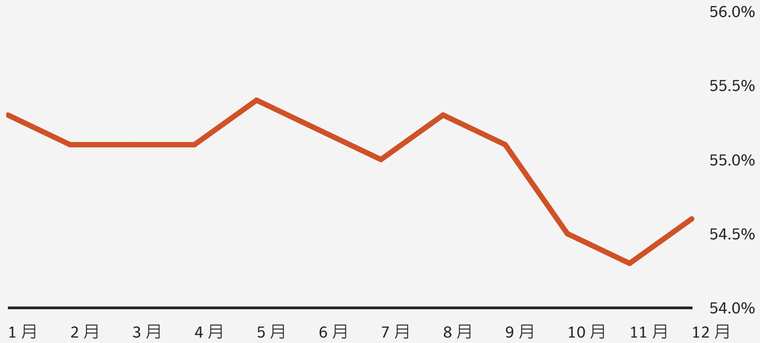
各國家/地區電子郵件網路釣魚比例 (年)

國家/地區	網路釣魚比例 (每幾封電子郵件中出現一封)
沙烏地阿拉伯	675
挪威	860
荷蘭	877
奧地利	1,306
南非	1,318
匈牙利	1,339
泰國	1,381
台灣	1,712
巴西	1,873
阿拉伯聯合大公國	2,312
紐西蘭	2,446
香港	2,549
新加坡	2,857
盧森堡	2,860
義大利	3,048
卡達	3,170
中國	3,208
美國	3,231
愛爾蘭	3,321
比利時	3,322
瑞典	3,417
澳洲	3,471
瑞士	3,627
西班牙	3,680
英國	3,722
阿曼	3,963
巴布亞紐幾內亞	4,011
斯里蘭卡	4,062
葡萄牙	4,091
菲律賓	4,241
加拿大	4,308
希臘	4,311
以色列	4,472
哥倫比亞	4,619
馬來西亞	4,687
德國	5,223
丹麥	5,312
墨西哥	5,389
法國	5,598
印度	5,707
塞爾維亞	6,376
芬蘭	6,617
日本	7,652
南韓	8,523
波蘭	9,653

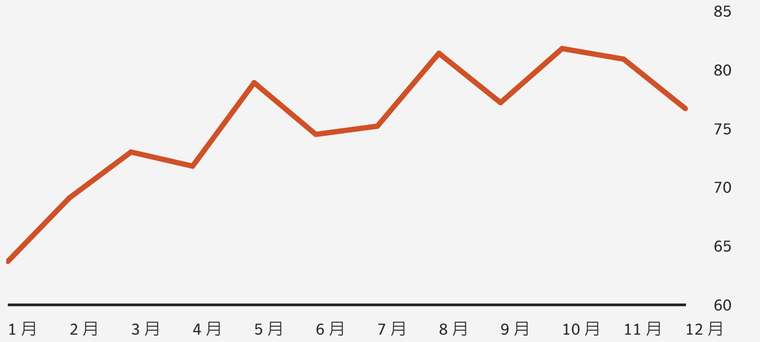
垃圾電子郵件比率 (年)

垃圾電子郵件比率 (%)
55

垃圾電子郵件比率 (月)



單一使用者垃圾電子郵件量 (月)



各行業垃圾電子郵件比率 (年)

行業	垃圾電子郵件比率 (%)
採礦業	58.3
金融、保險及不動產業	56.7
製造業	55.1
公共行政	54.9
農、林、漁業	54.6
運輸及公用事業	54.6
無法分類的機構	54.2
服務業	54.1
零售業	53.7
建築業	53.6
批發業	52.6

各行業單一使用者垃圾電子郵件量 (年)

行業	單一使用者的垃圾郵件
批發業	135
零售業	111
採礦業	109
建築業	103
無法分類的機構	97
運輸及公用事業	93
製造業	79
農、林、漁業	66
公共行政	63
金融、保險及不動產業	61
服務業	59

各行業垃圾電子郵件比率 (份)

組織規模	垃圾電子郵件比率 (%)
1-250	55.9
251-500	53.6
501-1000	54.5
1001-1500	56.9
1501-2500	53.7
2501+	54.9

各規模組織單一使用者垃圾電子郵件量 (年)

組織規模	單一使用者的垃圾郵件
1-250	55
251-500	57
501-1000	109
1001-1500	125
1501-2500	107
2501+	55

各國家/地區垃圾電子郵件比率 (年)

國家/地區	垃圾電子郵件比率 (%)
沙烏地阿拉伯	66.8
中國	62.2
巴西	60.8
斯里蘭卡	60.6
挪威	59.1
阿曼	58.6
瑞典	58.3
墨西哥	58.1
阿拉伯聯合大公國	58.1
美國	57.5
哥倫比亞	56.8
比利時	56.2
塞爾維亞	55.8
新加坡	55.4
英國	54.8
德國	54.8
台灣	54.5
奧地利	54.4
芬蘭	54.4
匈牙利	54.4
希臘	54.2
以色列	54.1
丹麥	54.1
法國	54
荷蘭	53.9
澳洲	53.9
紐西蘭	53.4
加拿大	53.4
義大利	53.4
波蘭	53.2
西班牙	52.9
卡達	52.6
南韓	52.4
葡萄牙	52.1
盧森堡	51.4
馬來西亞	51.4
泰國	51.1
愛爾蘭	51
印度	50.9
南非	50.8
瑞士	50.8
香港	50.5
巴布亞紐幾內亞	50
菲律賓	49.5
日本	48.7

惡意程式

Emotet 仍在 **2018** 年大舉擴張市佔率，佔金融特洛伊木馬程式的 **16%**，遠高於 **2017** 年的 **4%**。**Emotet** 也用於傳播 **Qakbot**，此為排名第 **7** 的金融木馬程式，佔發現總數的 **1.8%**。這兩種威脅都能自行傳播，為組織帶來更嚴峻的挑戰。

在 **2018** 年，攻擊者持續沿用「自給自足」戰術，導致惡意 **PowerShell** 指令碼的使用率激增 **1,000%**。在常見的攻擊情境中，歹徒透過 **Office** 巨集調用 **PowerShell** 指令碼，而 **PowerShell** 指令碼又會下載惡意酬載。在偵獲的下載程式當中，由 **Office** 巨集下載程式佔大宗，而 **VBS.Downloader** 和 **JS.Downloader** 的威脅則有所減少。

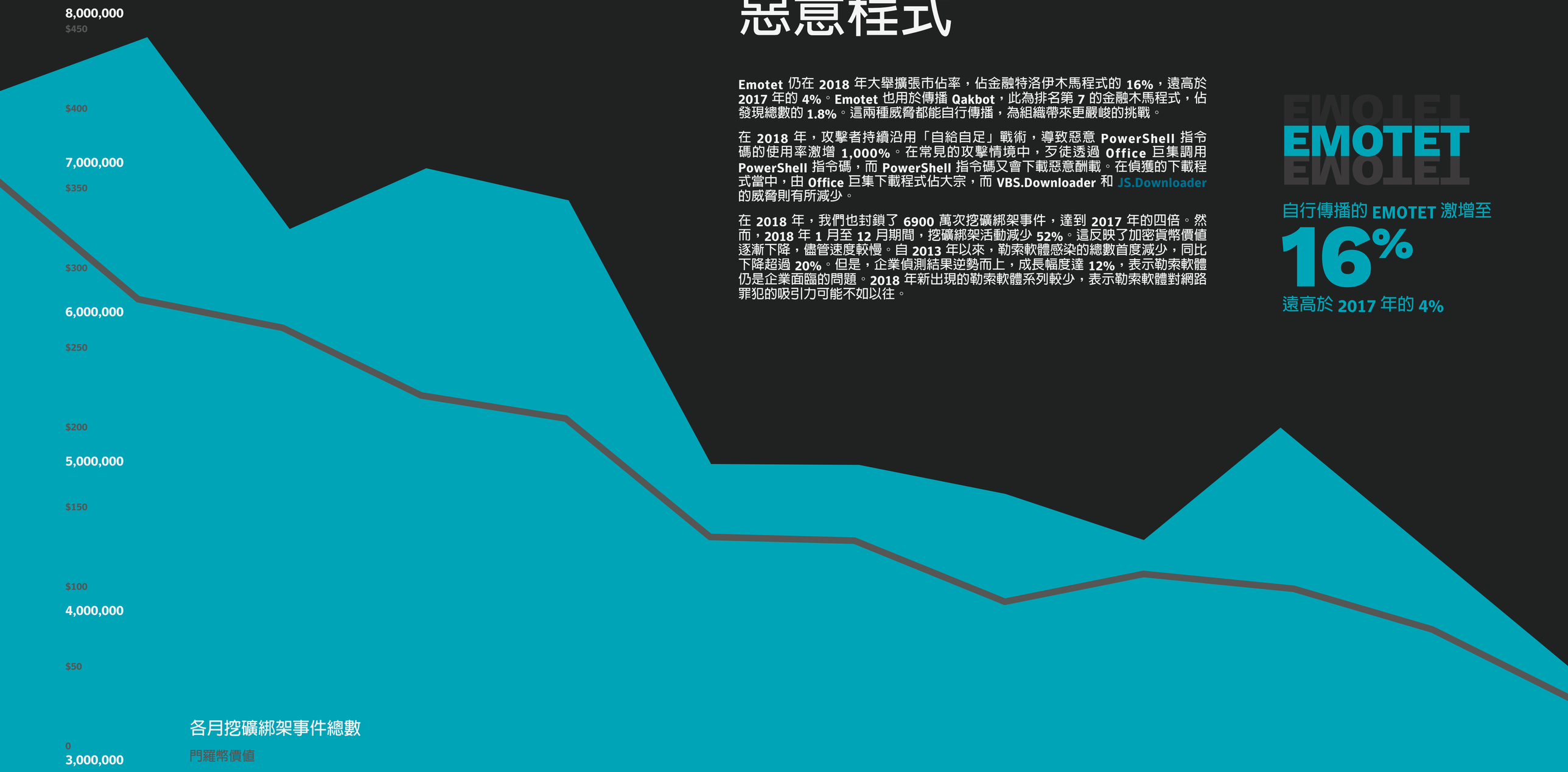
在 **2018** 年，我們也封鎖了 **6900** 萬次挖礦綁架事件，達到 **2017** 年的四倍。然而，**2018** 年 **1** 月至 **12** 月期間，挖礦綁架活動減少 **52%**。這反映了加密貨幣價值逐漸下降，儘管速度較慢。自 **2013** 年以來，勒索軟體感染的總數首度減少，同比下降超過 **20%**。但是，企業偵測結果逆勢而上，成長幅度達 **12%**，表示勒索軟體仍是企業面臨的問題。**2018** 年新出現的勒索軟體系列較少，表示勒索軟體對網路罪犯的吸引力可能不如以往。

EMOTET

自行傳播的 **EMOTET** 激增至

16%

遠高於 **2017** 年的 **4%**

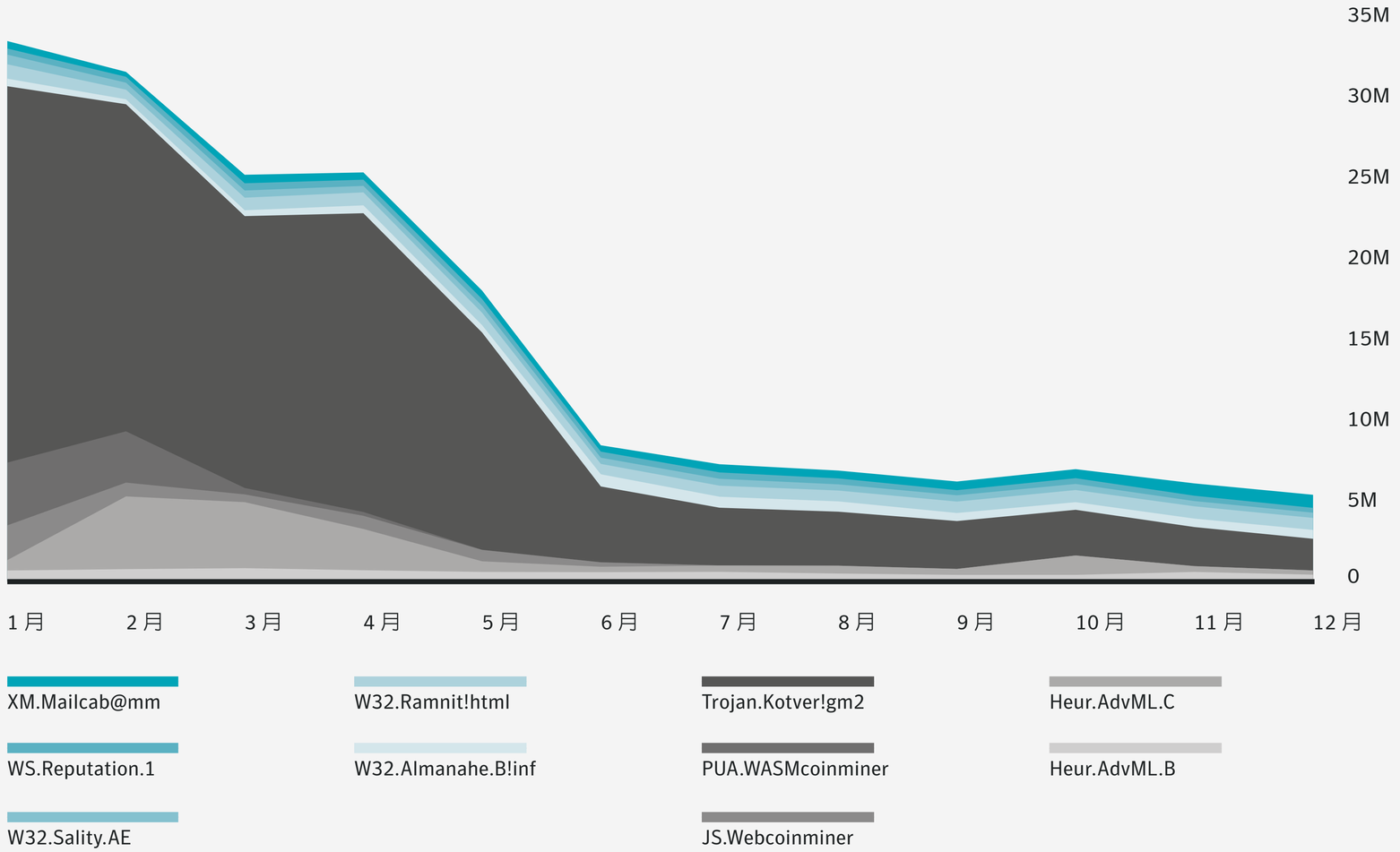


新型惡意程式變種 (年)

年	新型變種	百分比變化
2016	357,019,453	0.5
2017	669,947,865	87.7
2018	246,002,762	-63.3

Emotet 仍在 2018 年大舉擴張市佔率，佔金融特洛伊木馬程式的 16%，遠高於 2017 年的 4%。

熱門新型惡意程式變種 (月)

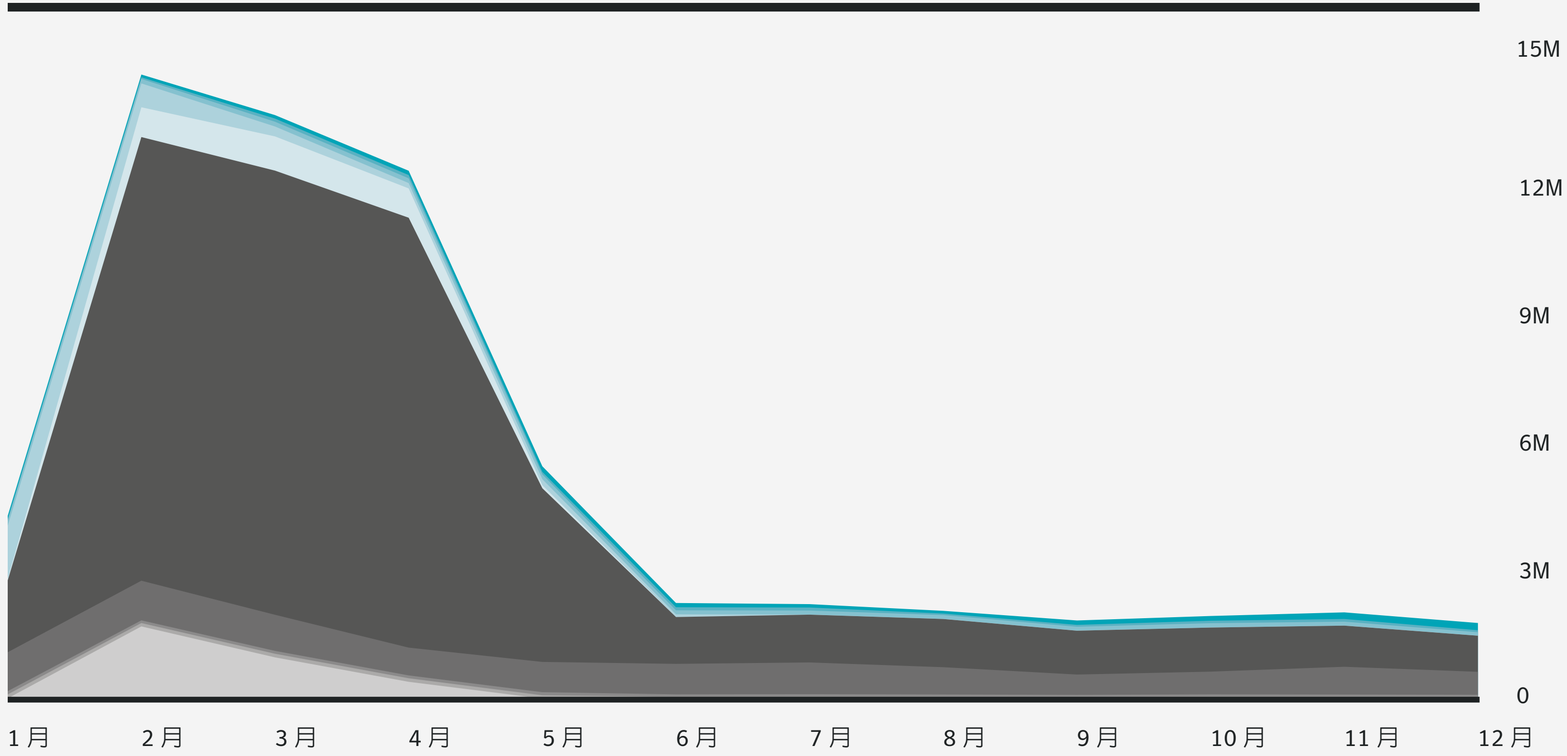


熱門惡意程式 (年)

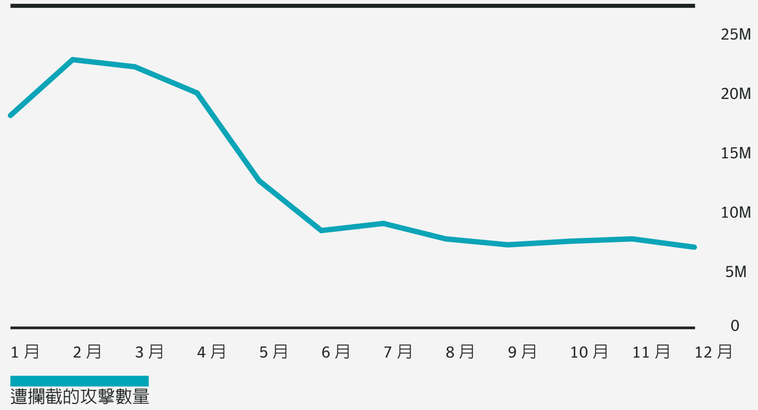
威脅名稱	遭攔截的攻擊數量	百分比
Heur.AdvML.C	43,999,373	52.1
Heur.AdvML.B	8,373,445	9.9
BloodHound.SymVT.FP	3,193,779	3.8
JS.Webcoinminer	2,380,725	2.8
Heur.AdvML.SN	2,300,919	2.7
W97M.Downloader	1,233,551	1.5
Packed.Dromedan!Ink	1,215,196	1.4
Hacktool	846,292	1.0
Hacktool.Kms	763,557	0.9
Trojan.Mdropper	679,248	0.8

在 2018 年，Mealybug 和 Necurs 等網路犯罪組織，仍使用 Office 檔案巨集作為散布惡意酬載的首選方法。

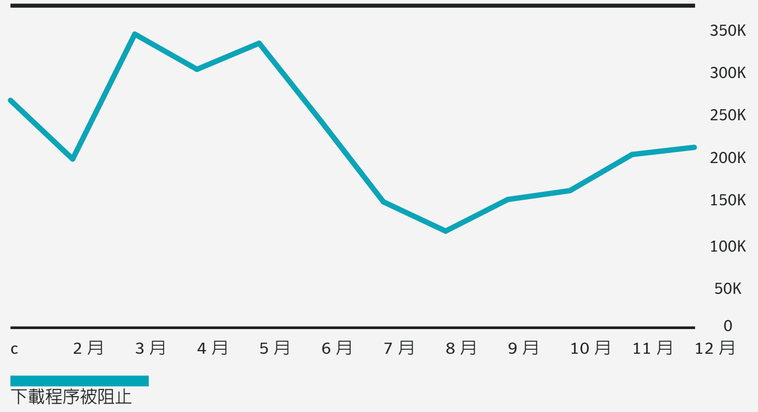
熱門惡意程式 (月)



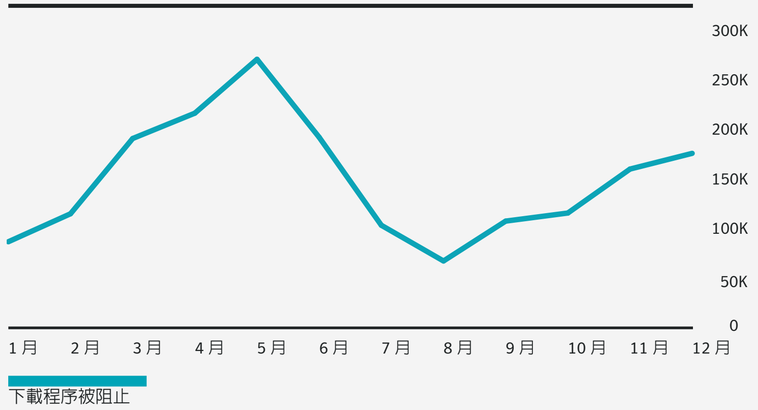
惡意程式總數 (月)



下載程式總數 (月)

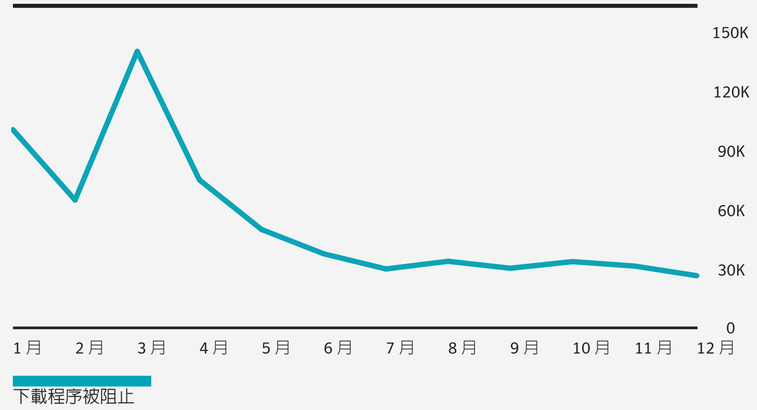


OFFICE 巨集下載程式 (月)

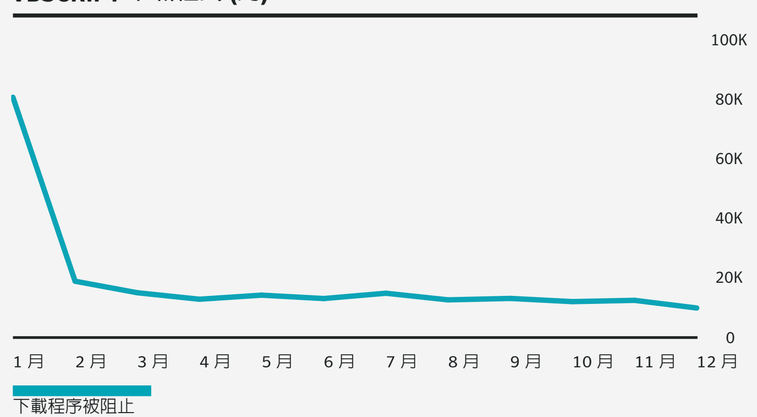


雖然 VBS.Downloader 和 JS.Downloader 威脅在 2018 年趨減，但 Office 巨集下載程式在年底漸增。

JAVASCRIPT 下載程式 (月)



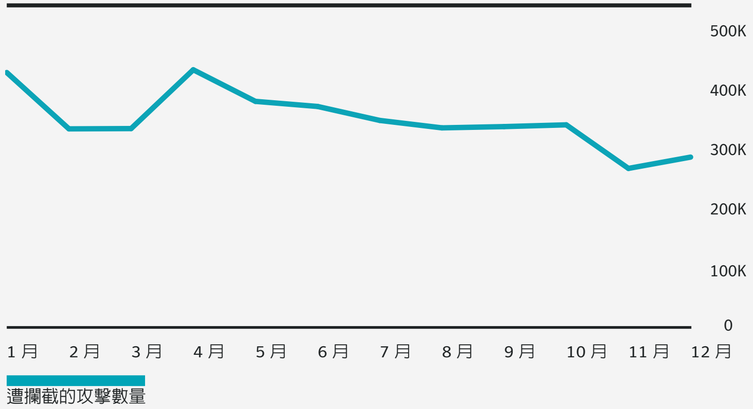
VBSCRIPT 下載程式 (月)



各作業系統惡意程式總數 (年)

年	作業系統	遭攔截的攻擊數量	百分比
2016	Windows	161,708,289	98.5
	Mac	2,445,414	1.5
2017	Windows	165,639,264	97.6
	Mac	4,011,252	2.4
2018	Windows	144,338,341	97.2
	Mac	4,206,986	2.8

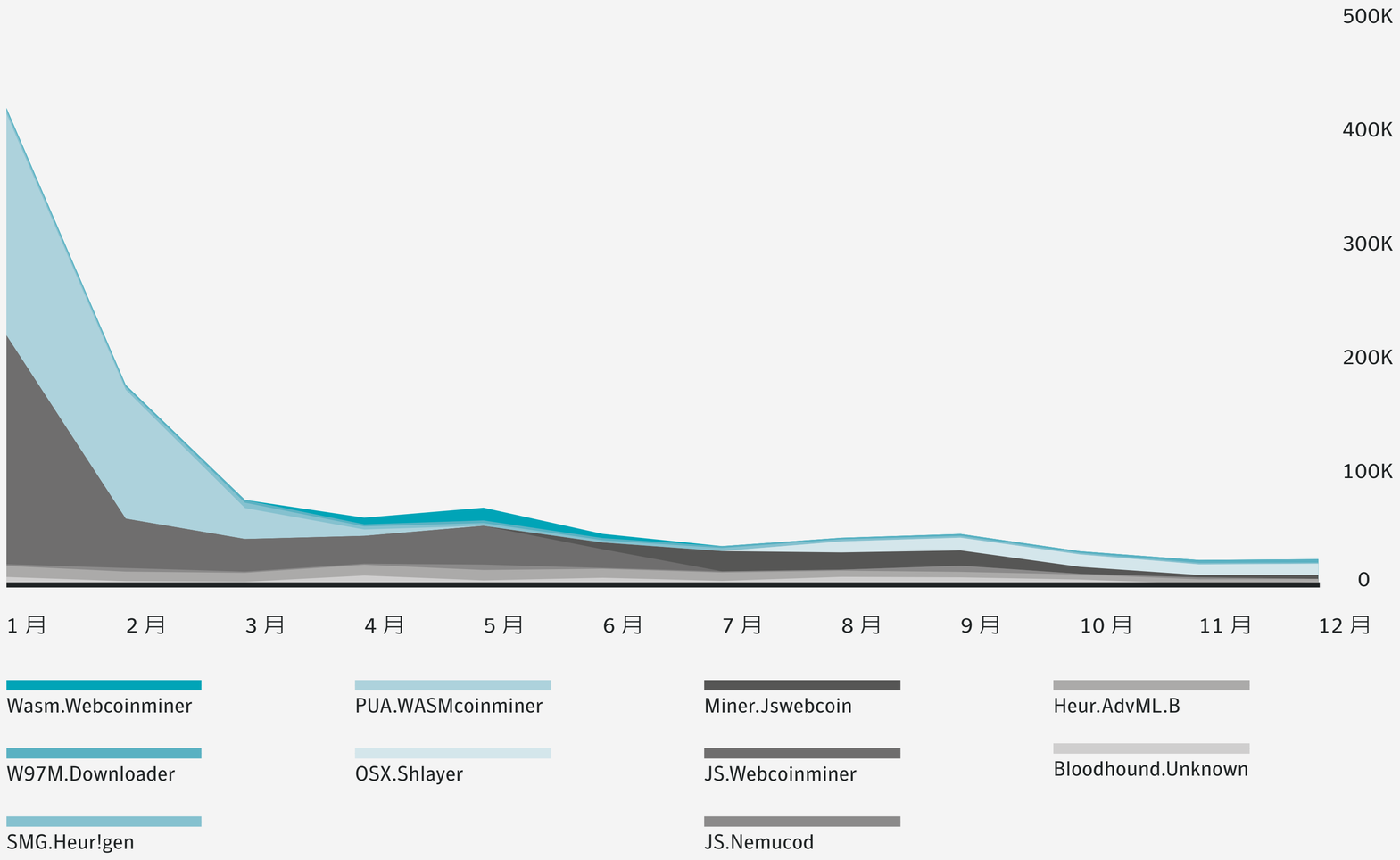
MAC 惡意程式總數 (月)



新型 MAC 惡意程式變種 (年)

年	變種	百分比變化
2016	772,018	
2017	1,390,261	80.1
2018	1,398,419	0.6

熱門新型 MAC 惡意程式變種 (月)

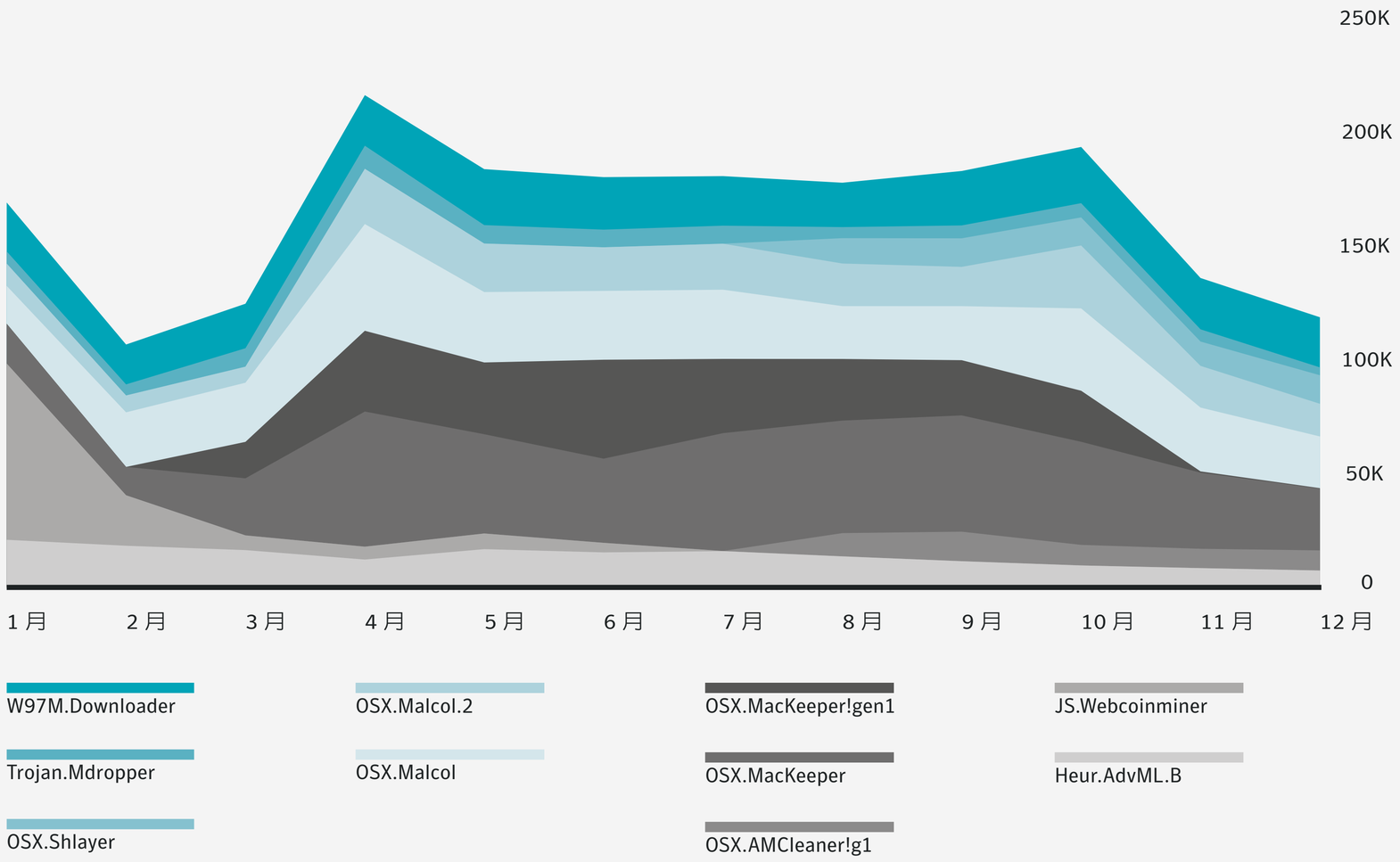


熱門 MAC 惡意程式 (年)

威脅名稱	遭攔截的攻擊數量	百分比
OSX.MacKeeper	452,858	19.6
OSX.Malcol	338,806	14.7
W97M.Downloader	262,704	11.4
OSX.Malcol.2	205,378	8.9
Heur.AdvML.B	166,572	7.2
JS.Webcoinminer	122,870	5.3
Trojan.Mdropper	77,800	3.4
OSX.Shlayer	59,197	2.6
OSX.AMCleaner!g1	49,517	2.1
JS.Downloader	40,543	1.8

在 2018 年，賽門鐵克封鎖了 6900 萬次挖礦綁架事件，達到 2017 年的四倍。

熱門 MAC 惡意程式 (月)



SSL 啟用惡意程式百分比 (年)

年	使用 SSL 的惡意程式百分比
2017	4.5
2018	3.9

勒索軟體總數 (年)

年	總計
2018	545,231

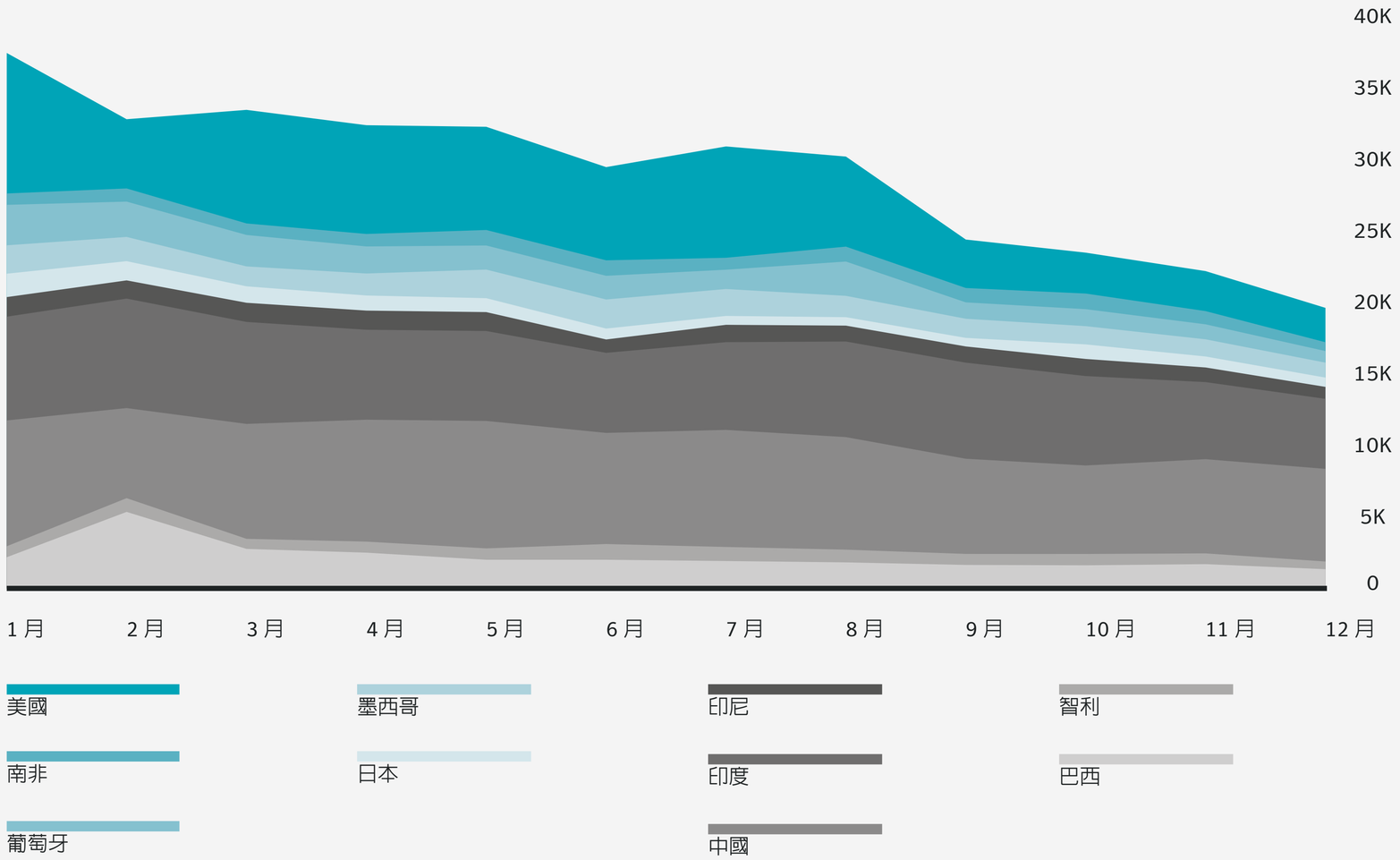
各市場勒索軟體 (年)

市場	總計
消費類	100,907
企業	444,259

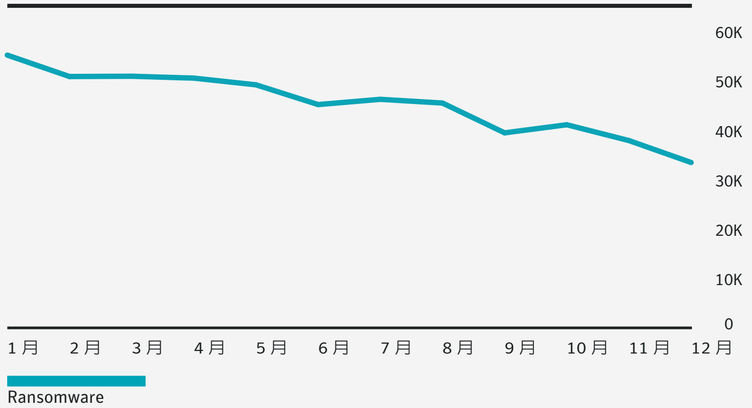
各國家/地區熱門勒索軟體 (年)

國家/地區	百分比
中國	16.9
印度	14.3
美國	13.0
巴西	5.0
葡萄牙	3.9
墨西哥	3.5
印尼	2.6
日本	2.1
南非	2.1
智利	1.8

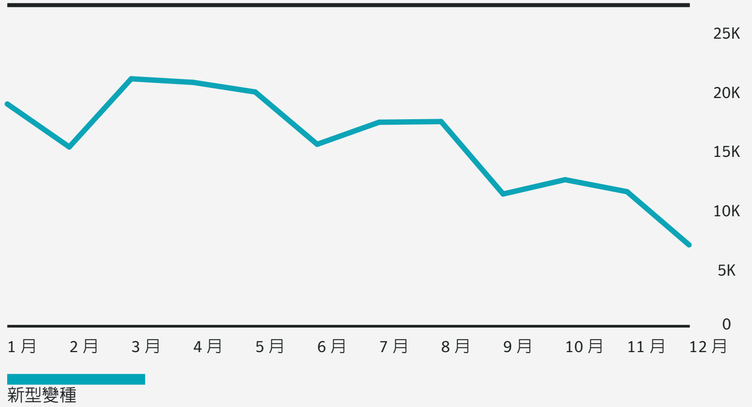
各國家/地區勒索軟體 (月)



勒索軟體總數 (月)



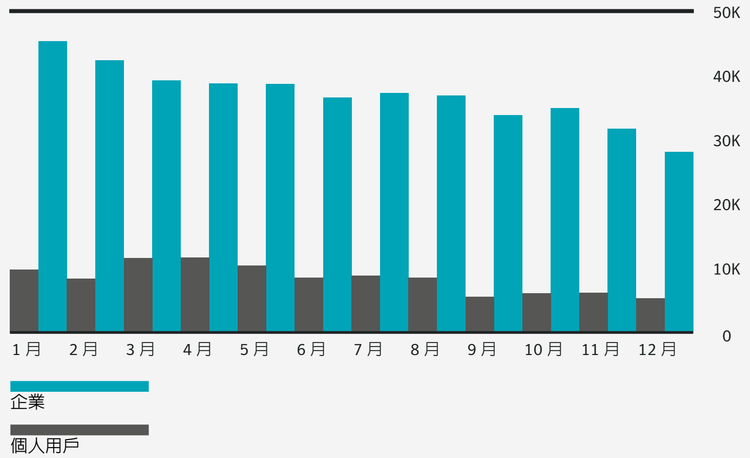
新型勒索軟體變種 (月)



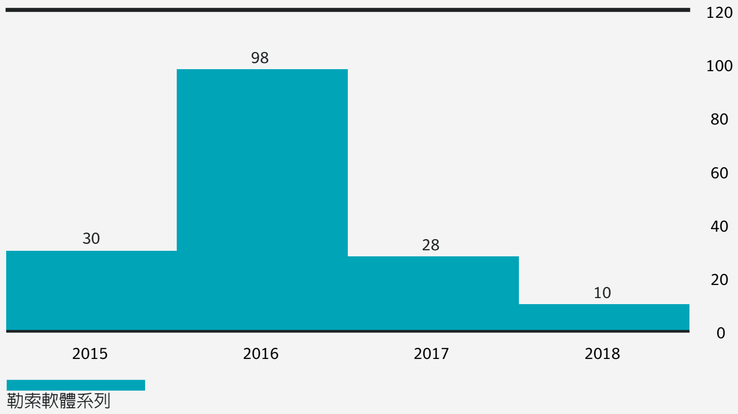
新型勒索軟體變種 (年)

年	總計
2018	186,972

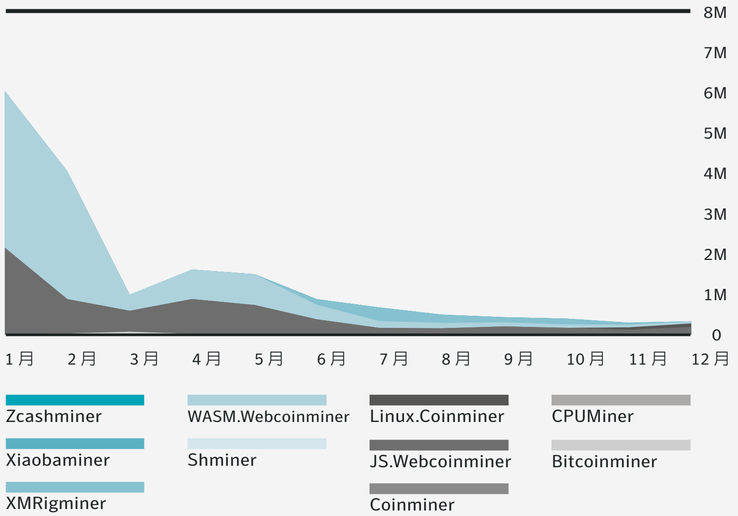
各市場勒索軟體 (月)



新型勒索軟體系列 (年)

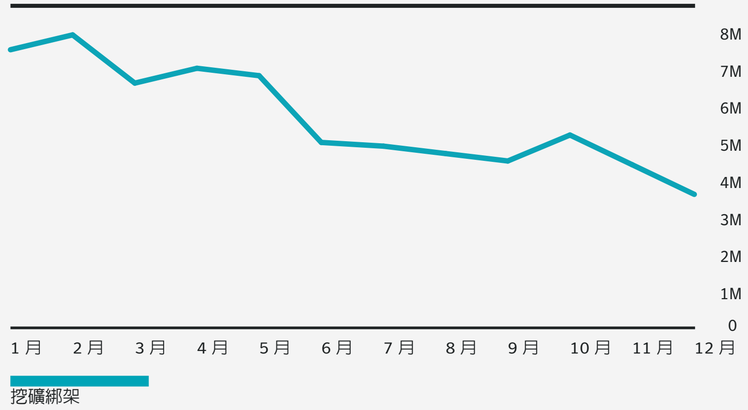


惡意程式：熱門加密貨幣挖礦程式變種 (月)



勒索軟體感染總數減少，同比下降超過 20%。但是，企業偵測結果逆勢而上，成長幅度達 12%，表示勒索軟體仍是企業面臨的問題。

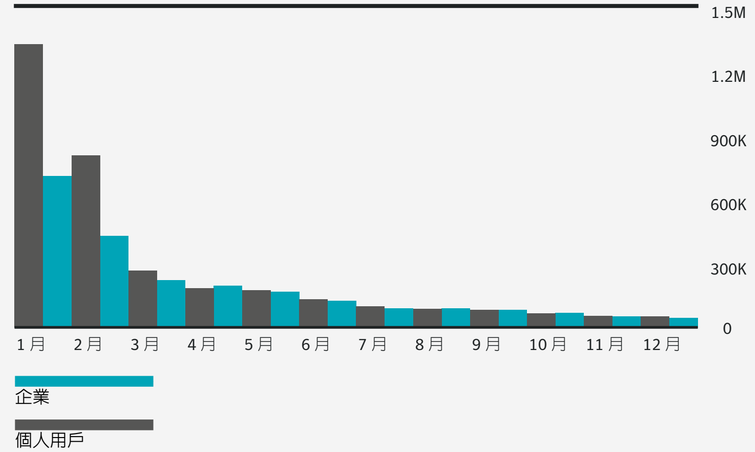
挖礦綁架總數 (月)



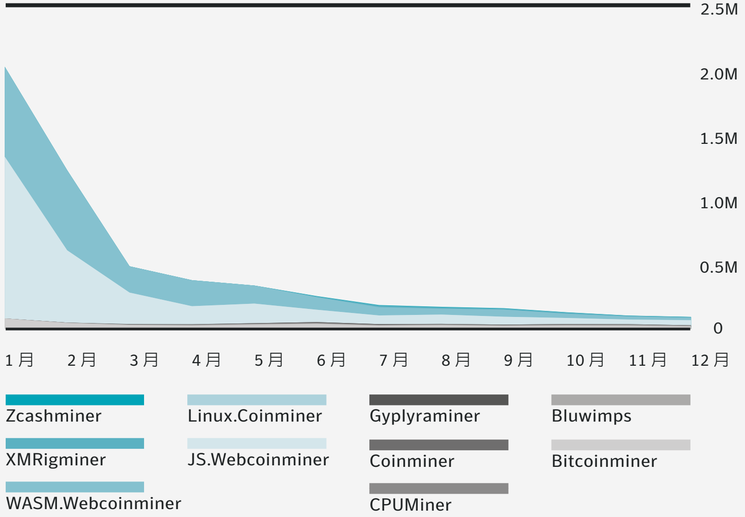
熱門加密貨幣挖礦程式 (年)

威脅名稱	遭攔截的攻擊數量	百分比
JS.Webcoinminer	2,768,721	49.7
WASM.Webcoinminer	2,201,789	39.5
Bitcoinminer	414,297	7.4
Bluwimps	58,601	1.1
XMRigminer	58,301	1.0
Coinminer	38,655	0.7
Zcashminer	13,389	0.2
Gyplyraminer	5,221	0.1
CPUMiner	3,807	0.1
Linux.Coinminer	3,324	0.1

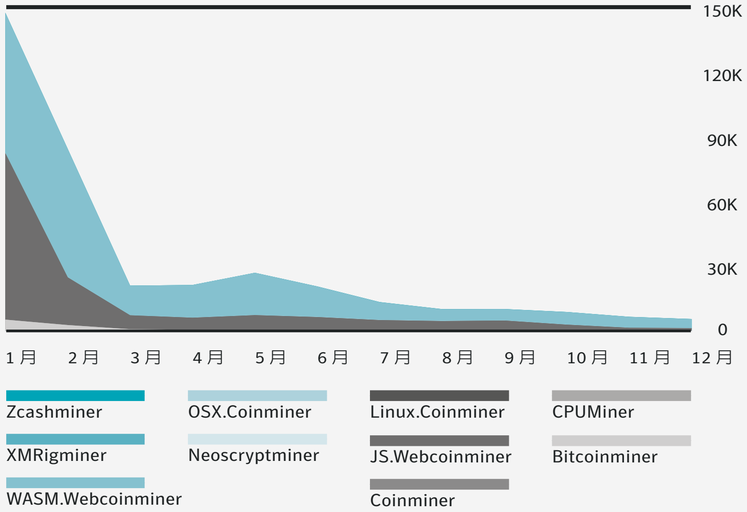
各市場加密貨幣挖礦程式 (月)



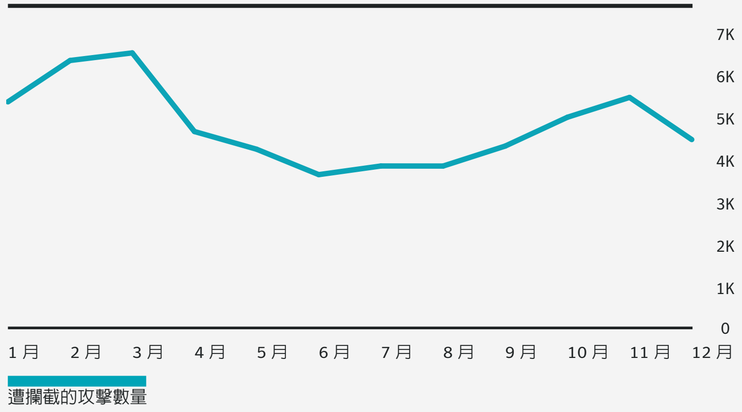
熱門加密貨幣挖礦程式 (月)



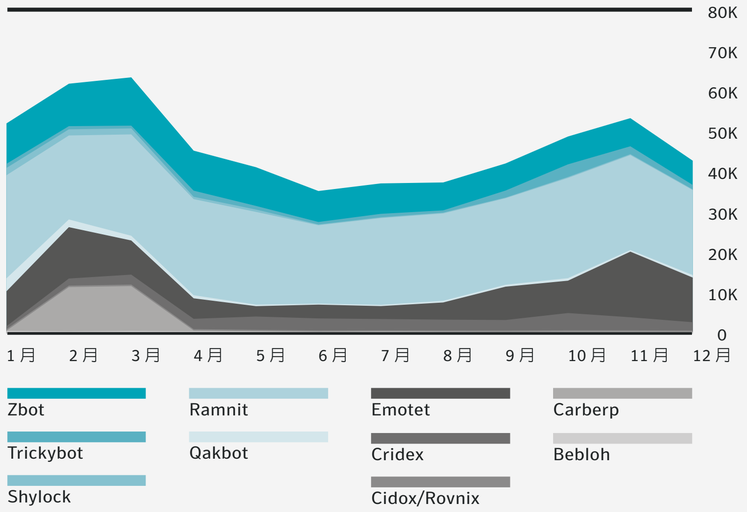
熱門 MAC 加密貨幣挖礦程式 (月)



金融特洛伊木馬程式總數 (月)



熱門金融特洛伊木馬程式 (月)

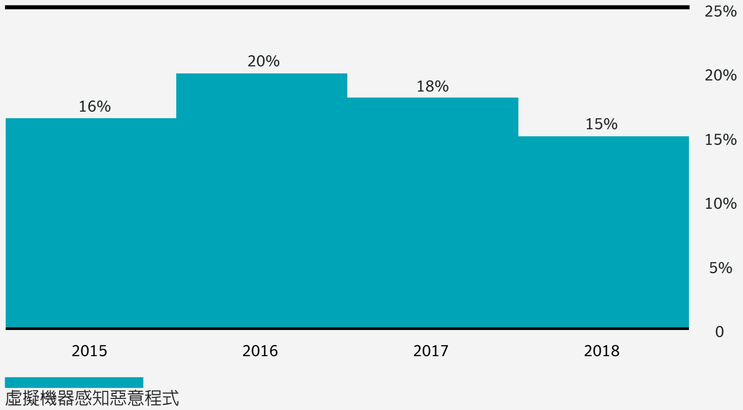


熱門金融特洛伊木馬程式 (年)

金融特洛伊木馬程式	遭攔截的攻擊數量	百分比
Ramnit	271,930	47.4
Zbot	100,821	17.6
Emotet	92,039	16.0
Cridex	31,539	5.5
Carberp	22,690	4.0
Trickybot	14,887	2.6
Qakbot	10,592	1.8
Shylock	7,354	1.3
Bebloh	5,592	1.0
Cidox/Rovnix	3,889	0.7

在 **2018** 年，攻擊者持續沿用「自給自足」戰術，導致惡意 **PowerShell** 指令碼的使用率激增 **1,000%**。

虛擬機器感知惡意程式 (年)



POWERSHELL 偵獲數量 (月)

日期	惡意 POWERSHELL 指令碼百分比	比例
1 月	0.1	1/1,000
2 月	0.5	1/200
3 月	2.5	1/40
4 月	0.4	1/250
5 月	1.3	1/77
6 月	0.9	1/111
7 月	1.4	1/71
8 月	0.8	1/125
9 月	1.0	1/100
10 月	1.0	1/100
11 月	0.7	1/143
12 月	0.7	1/143

POWERSHELL 偵獲數量 (年)

年	惡意程式總計百分比	比例	惡意指令碼增加百分比
2017	0.9	1/111	
2018	0.9	1/111	998.9

行動裝置

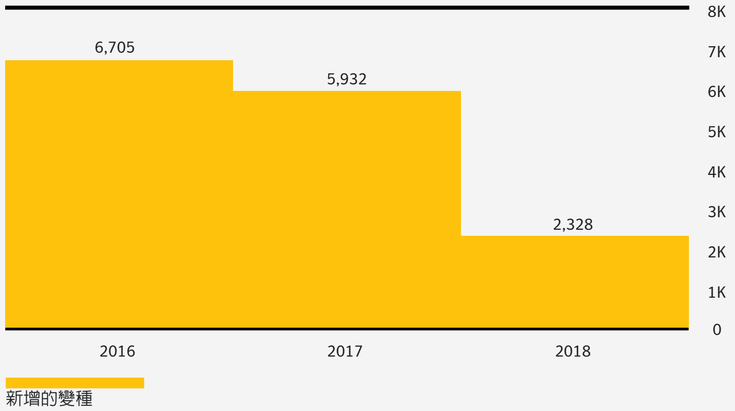
雖然行動惡意程式感染總數在 2018 年減少，但行動裝置遭勒索軟體感染數量遽增，較 2017 年增加三分之一。美國遭行動勒索軟體影響最嚴重，佔感染總數的 63%。其次是中國 (13%) 和德國 (10%)。

行動裝置安全的管理仍是組織的一大挑戰。組織在 2018 年所使用的裝置當中，每 36 種就有一種歸類為高風險。這包括經過 JB 破解、Root，或極可能植入惡意程式的裝置。

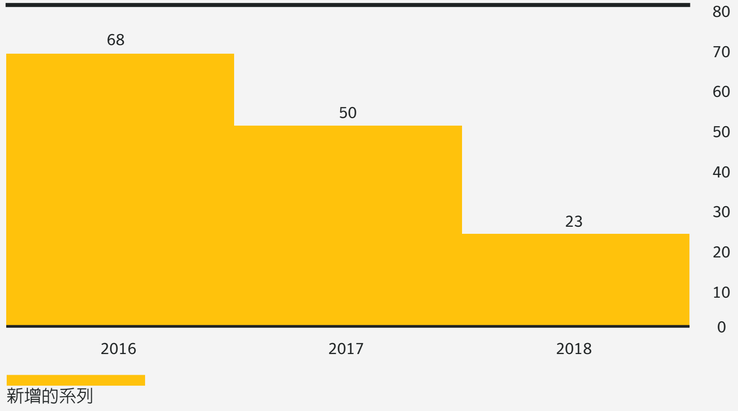
行動裝置安裝了
高風險應用程式

行動勒索軟體
數量高於
2017 年

新型行動惡意程式變種 (年)



新型行動惡意程式系列 (年)



在 2018 年，賽門鐵克平均每天封鎖 10,573 個惡意行動應用程式。工具 (39%)、生活品味 (15%) 和娛樂 (7%) 是最常見的惡意應用類別。

遭攔截的行動應用程式數量 (年)

每天
10,573

每月平均行動勒索軟體數量 (年)

每月
4,675

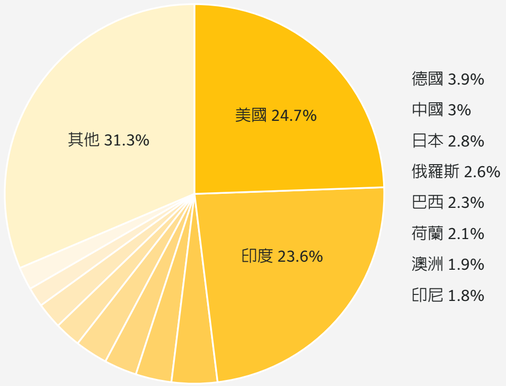
熱門惡意行動應用程式類別 (年)

類別	百分比
工具	39.1
生活品味	14.9
娛樂	7.3
社交與通訊	6.2
音樂和音訊	4.3
益智解謎遊戲	4.2
照片和影片	4.2
街機和動作遊戲	4.1
書籍和參考資料	3.2
教育	2.6

熱門行動惡意程式 (年)

威脅名稱	百分比
Malapp	29.7
Fakeapp	9.1
MalDownloader	8.9
FakeInst	6.6
Mobilespy	6.3
HiddenAds	4.7
Premiumtext	4.4
MobileSpy	2.8
HiddenApp	2.5
Opfake	2.0

行動惡意程式盛行國家/地區 (年)



遭 JB 破解或 ROOT 的行動裝置比例 (年)

使用族群	比例
Android 消費者	1/23
Android 企業	1/3,890
iOS 消費者	1/828
iOS 企業	1/4,951

各市場經密碼保護的行動裝置 (年)

使用族群	百分比
消費類	97.9
企業	98.4

行動裝置的網路威脅曝險時間長度 (年)

面臨網路攻擊的裝置	百分比
1 個月後 (開發完成 1-4 個月的裝置)	15.1
2 個月後 (開發完成 2-5 個月的裝置)	21.8
3 個月後 (開發完成 3-6 個月的裝置)	27.4
4 個月後 (開發完成 4-7 個月的裝置)	32.2

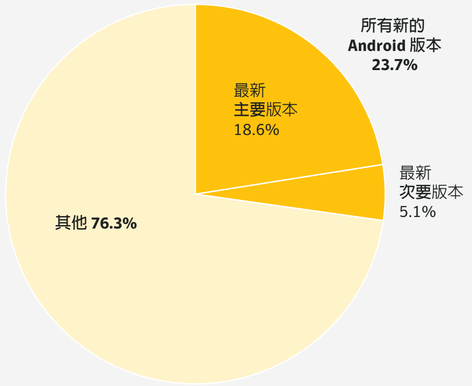
未啟用加密的裝置 (年)

使用族群	百分比
消費類	13.4
企業	10.5

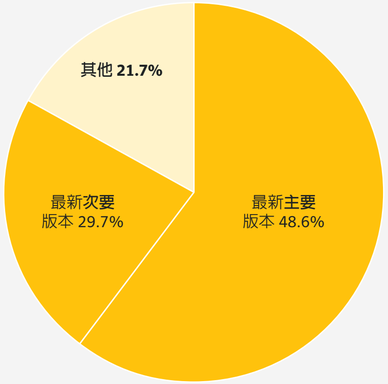
裝置風險等級 (年)

裝置風險等級	比例
極低	1/2
低	1/4
中	1/4
高 (包括經過 Root /JB 破解/極可能植入惡意應用程式的裝置)	1/36

執行最新 ANDROID 版本的裝置 (年)



執行最新 IOS 版本的裝置 (年)



所有新的 iOS 版本 78.3%

使用侵入式廣告技術的行動應用程式百分比有所下降。**2017** 年的比率為 **30%**，**2018** 年降至 **26%**。

存取高風險資料的應用程式比例 (年)

年	存取高風險資料的應用程式 (%)	比例	變化 (PP)
2016	7.2	1/13.9	
2017	8.9	1/11.3	1.7
2018	6.9	1/14.5	-2

含有硬編碼憑證的應用程式比例 (年)

年	含有硬編碼憑證的應用程式 (%)	比例	變化 (PP)
2016	0.8	1/124.5	
2017	1.1	1/91.0	0.3
2018	1.0	1/99.1	-0.1

使用緊急修補程式的應用程式比例 (年)

年	使用緊急修補程式的風險應用程式 (%)	比例	變化 (PP)
2016	0.7	1/142.1	
2017	0.35	1/285.1	-0.35
2018	0.01	1/7,146.0	-0.34

存取健康資料的應用程式比例 (年)

年	存取健康資料的應用 (%)	比例	變化 (PP)
2016	0.2	1/427.3	
2017	1.7	1/57.6	1.5
2018	2.2	1/46.3	0.5

使用侵入式廣告的應用程式比例 (年)

年	使用侵入式廣告的應用程式百分比	比例	變化 (PP)
2016	19.4	1/5.2	
2017	30.5	1/3.3	11.1
2018	26.4	1/3.8	-4.1

因應用程式存取健康資料而受影響的組織百分比 (年)

年	具有 1 個以上應用程式的組織：健康資料 (%)	比例	變化 (PP)
2016	27.6	1/3.6	
2017	44.9	1/2.2	17.3
2018	39.0	1/2.6	-5.9

因應用程式存取高風險資料而受影響的組織百分比 (年)

年	經發現其應用程式存取高風險資料的組織百分比	比例	變化 (PP)
2016	63	1/1.6	
2017	54.6	1/1.8	-8.4
2018	46	1/2.2	-8.6

因應用程式含有硬編碼憑證而受影響的組織百分比 (年)

年	經發現其應用程式含有硬編碼憑證的組織百分比	比例	變化 (PP)
2016	47.3	1/2.1	
2017	42.9	1/2.3	-4.4
2018	34.3	1/2.9	-8.6

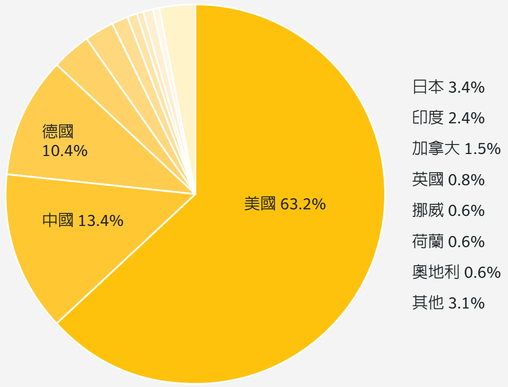
因應用程式使用緊急修補程式而受影響的組織百分比 (年)

年	經發現其應用程式使用緊急修補程式的組織百分比	比例	變化 (PP)
2016	31.3	1/3.2	
2017	11.7	1/8.5	-19.6
2018	6.8	1/14.7	-4.9

因應用程式使用侵入式廣告而受影響的組織百分比 (年)

年	經發現其應用程式使用侵入式廣告的組織的百分比	比例	變化 (PP)
2016	19.4	1/5.2	
2017	30.5	1/3.3	11.1
2018	26.4	1/3.8	-4.1

行動勒索軟體盛行國家/地區 (年)

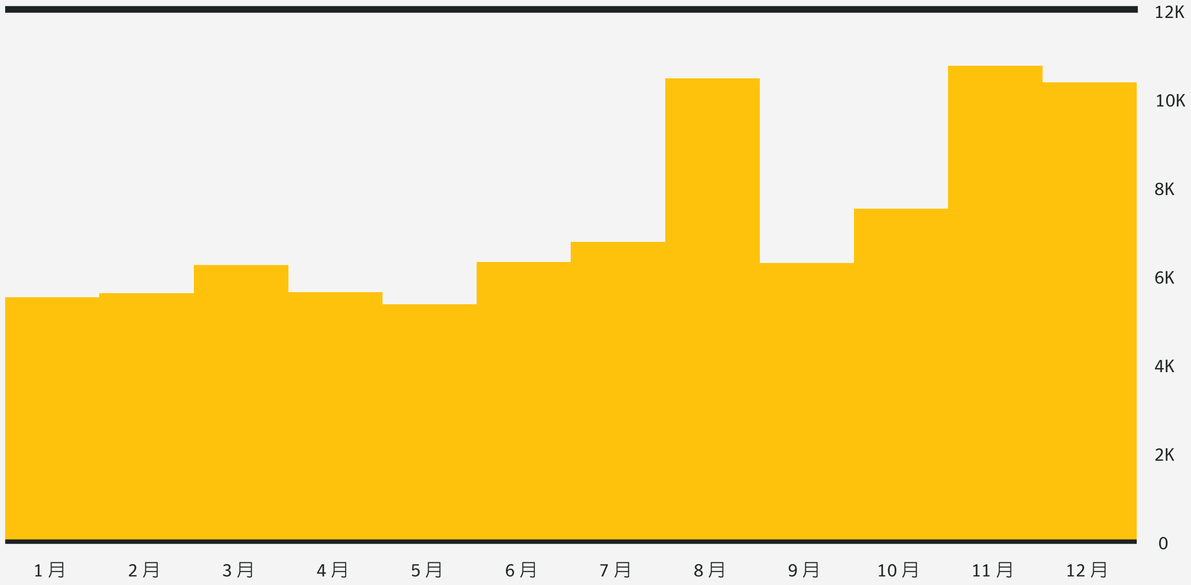


行動裝置感染勒索軟體的數量在 2018 年明顯增加，較 2017 年增加三分之一。

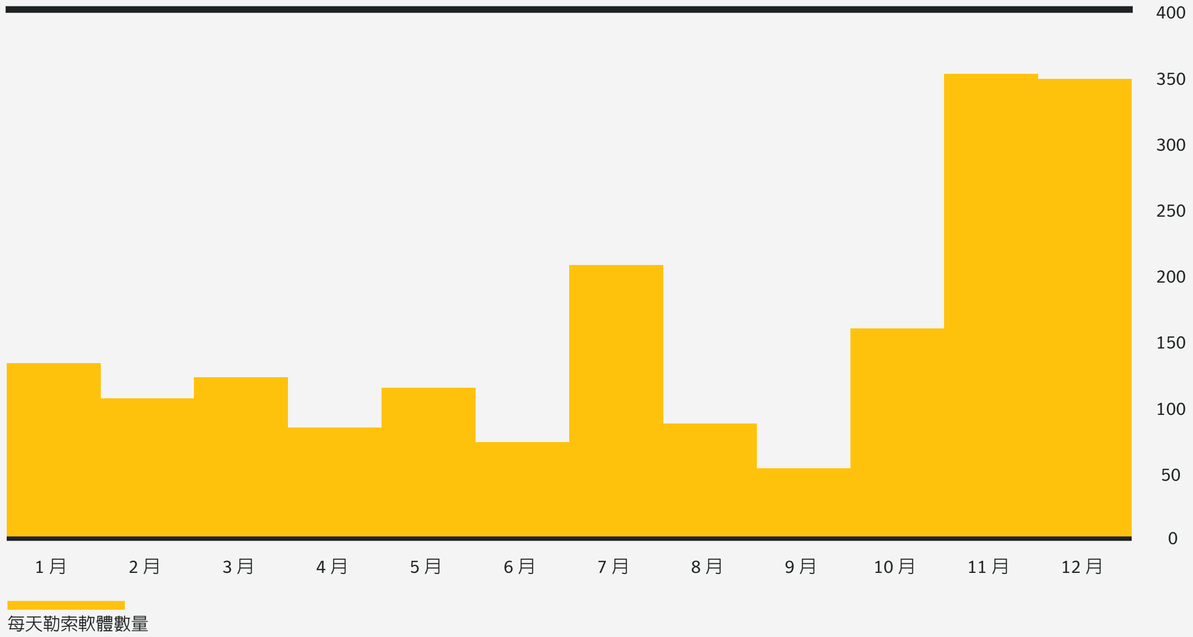
熱門行動勒索軟體 (年)

威脅名稱	百分比
Simplocker	59.3
Lockdroid.E	26.2
LockScreen	7.1
Simplocker.B	2.8
Ransomware	2.7
Ransomeware	1.0
Lockdroid.F	0.7
Android.WannaLocker	<0.1
WannaLocker	<0.1
Lockdroid.G	<0.1

遭攔截的行動惡意程式數量 (月)



遭攔截的行動勒索軟體數量 (月)



雖然 2018 全年行動惡意程式感染總數減少，但感染數量在該年第四季再度成長。

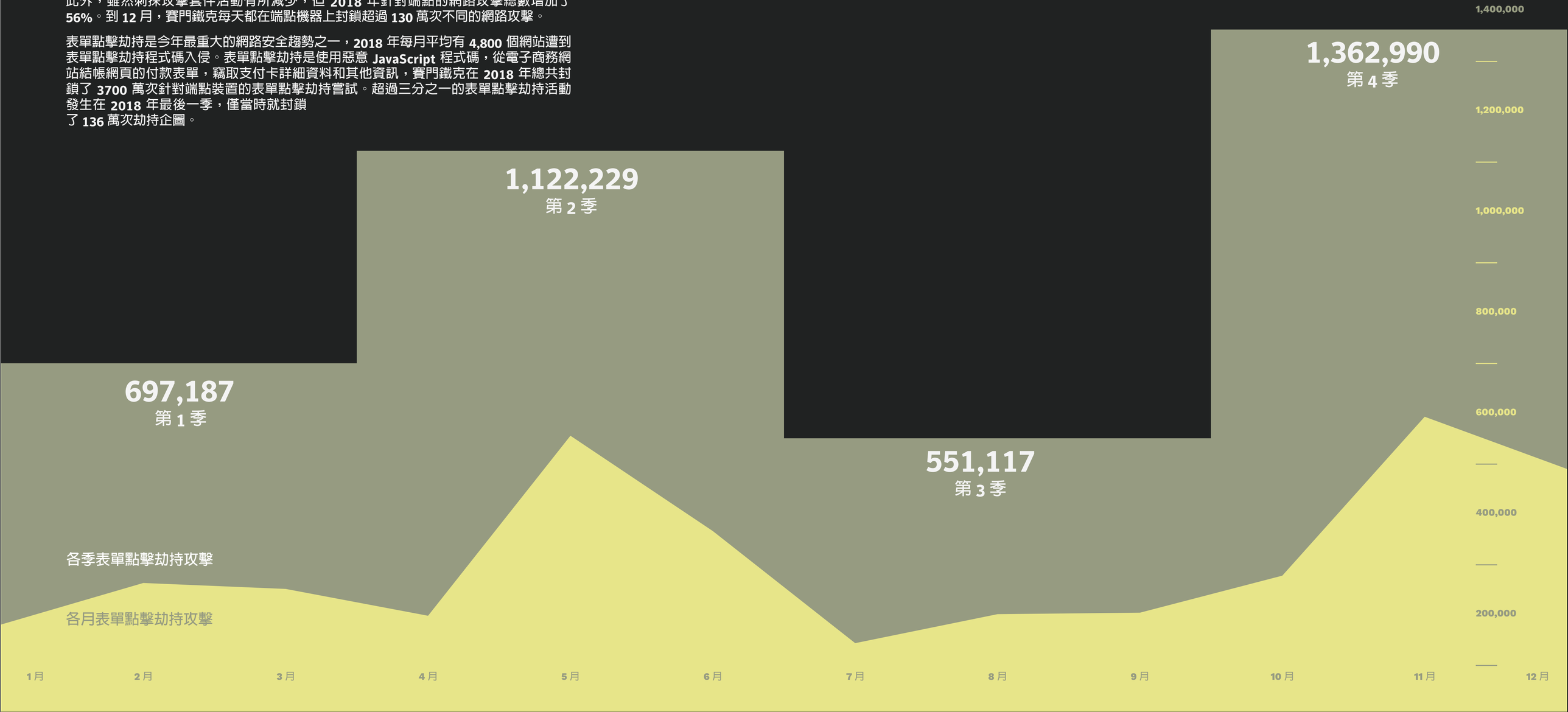
網路攻擊

在 2018 年，每分析 10 個 URL 就有 1 個經識別為惡意性質，多於 2017 年的 1/16。此外，雖然刺探攻擊套件活動有所減少，但 2018 年針對端點的網路攻擊總數增加了 56%。到 12 月，賽門鐵克每天都在端點機器上封鎖超過 130 萬次不同的網路攻擊。

表單點擊劫持是今年最重大的網路安全趨勢之一，2018 年每月平均有 4,800 個網站遭到表單點擊劫持程式碼入侵。表單點擊劫持是使用惡意 JavaScript 程式碼，從電子商務網站結帳網頁的付款表單，竊取支付卡詳細資料和其他資訊，賽門鐵克在 2018 年總共封鎖了 3700 萬次針對端點裝置的表單點擊劫持嘗試。超過三分之一的表單點擊劫持活動發生在 2018 年最後一季，僅當時就封鎖了 136 萬次劫持企圖。

表單點擊劫持活動

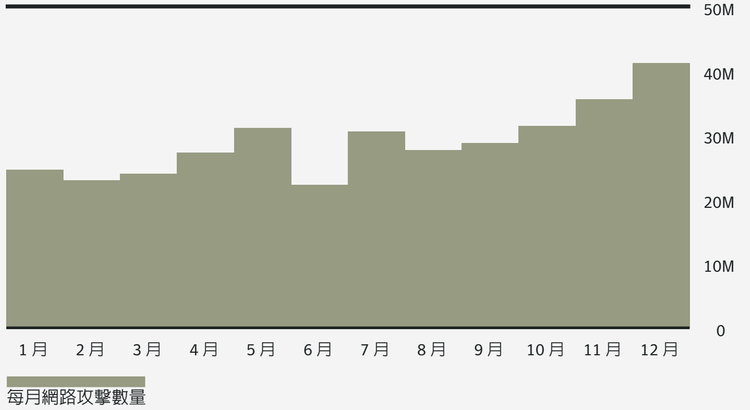
超過三分之一的表單點擊劫持活動發生在 2018 年最後一季。



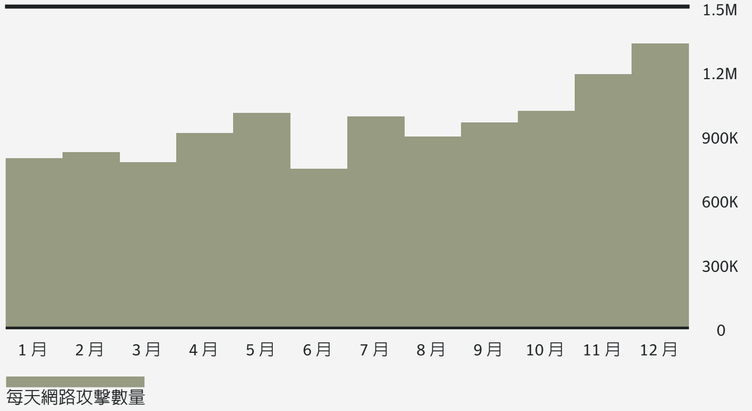
網頁攻擊 (年)

遭攔截的網頁攻擊總數	每日封鎖的網頁攻擊平均次數
348,136,985	953,800

網頁攻擊 (月)



網頁攻擊 (日)



最常遭入侵網站類別 (年)

網域類別	2017 年 (%)	2018 年 (%)	百分點差異
動態 DNS	15.7	16.6	0.8
博弈	7.9	16.3	8.4
託管	8.2	8.7	0.5
技術	13.6	8.1	-5.5
購物	4.6	8.1	3.6
商務	9.0	7.2	-1.7
色情內容	3.2	5.2	2.1
醫療	5.7	4.5	-1.2
教育	3.7	3.9	0.2
內容傳送網路	2.1	2.6	0.6

惡意網址 (年)

年	總計百分比	比例	百分點變化
2017	6.4	1/16	
2018	9.9	1/10	3.4

殭屍網路 URL (年)

年	所有 URL 的百分比	比例	惡意 URL 的百分比	比例	百分比變化	百分點變化
2017	1.2	1/85	18.2	1/5		
2018	1.8	1/54	18.7	1/5	57.6	0.7

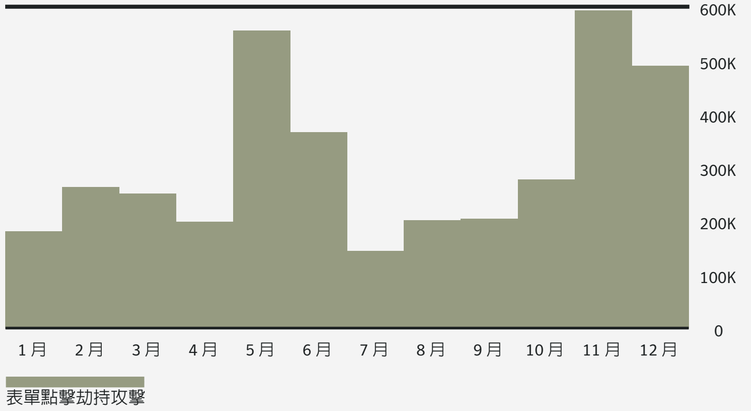
網路釣魚 URL (年)

年	所有 URL 的百分比	比例	惡意 URL 的百分比	比例	百分比變化	百分點變化
2017	0.4	1/235	6.6	1/15		
2018	0.6	1/170	5.9	1/17	38.1	0.2

表單點擊劫持攻擊 (年)

年	表單點擊劫持攻擊
2018	3,733,523

表單點擊劫持攻擊 (月)



表單點擊劫持網站平均數量 (月)

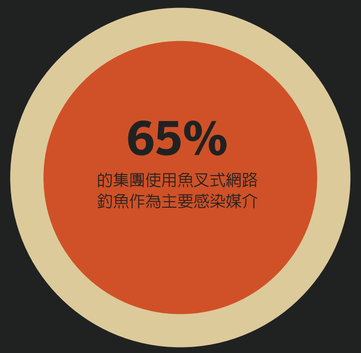
年	每月網站平均數量
2018	4,818

目標式攻擊

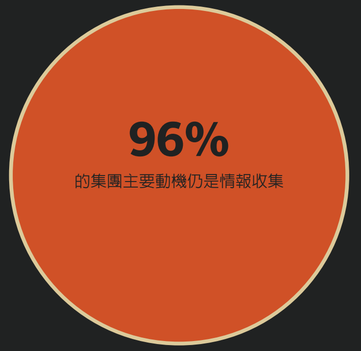
雖然去年目標式攻擊總數有所下降，但最活躍的集團加強活動力道，過去三年平均攻擊 55 個組織，而 2015 年至 2017 年間則為 42 個。魚叉式網路釣魚電子郵件仍然是最受歡迎的攻擊途徑，65% 的已知集團使用這種媒介。對組織發動目標式攻擊的最可能因素是情報收集，這也是 96% 的集團的犯案動機。

隨著自給自足戰術逐漸普及，零時差漏洞利用率在 2018 年有所下降，僅 23% 的集團採用零時差攻擊，低於 2017 年的 27%。雖然仍是小眾領域，但破壞性惡意程式的使用率持續成長。已知有 8% 的集團使用破壞性工具，較 2017 年增加 25%。

魚叉式網路釣魚



情報收集



2015-2017: 每個集團平均鎖定 42 個組織
(20 個最活躍的集團)

2016-2018: 每個集團平均鎖定 55 個組織
(20 個最活躍的集團)

↓ 23%
利用零時差
漏洞的集團

↑ 8%
利用破壞性惡
意程式的集團

美國政府起訴的間諜活動

5

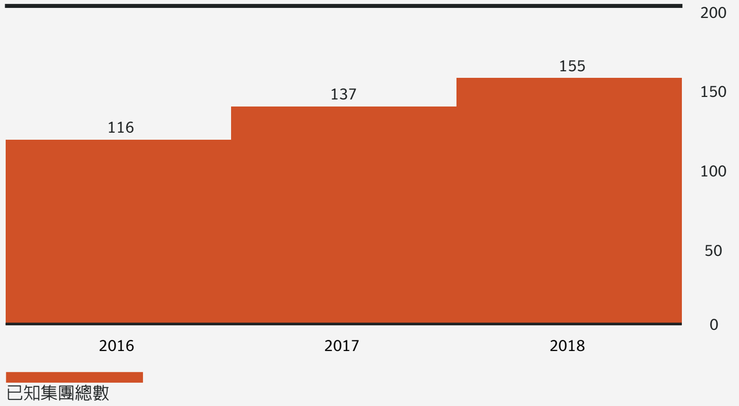
2016

4

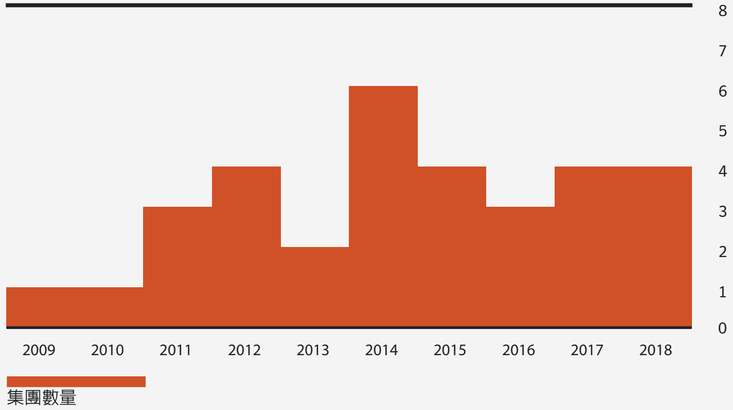
2017

2018

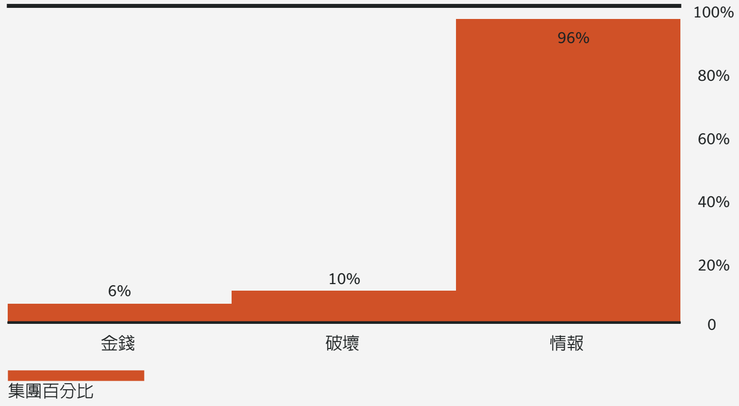
已知目標式攻擊集團 (年)



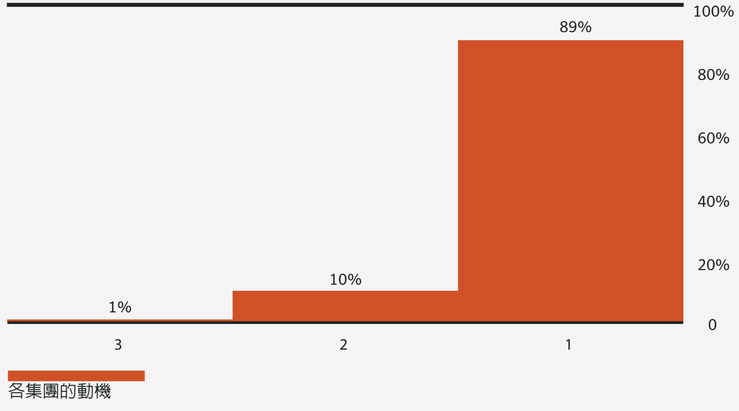
賽門鐵克發現的目標式攻擊集團 (年)



目標式攻擊集團動機 (所有時間)



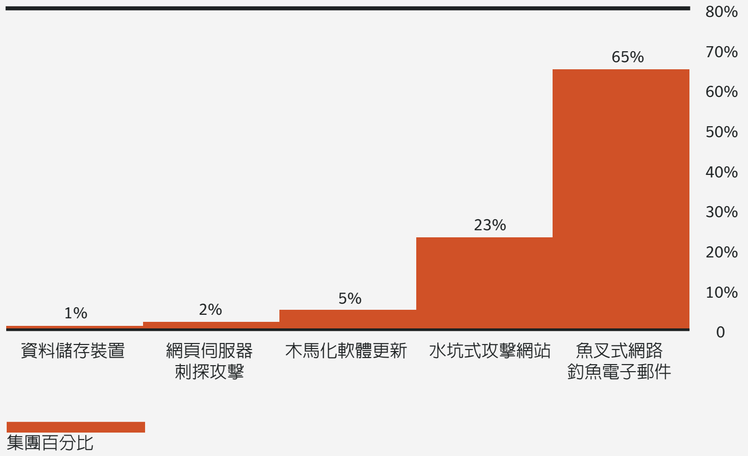
各目標式攻擊集團動機 (所有時間)



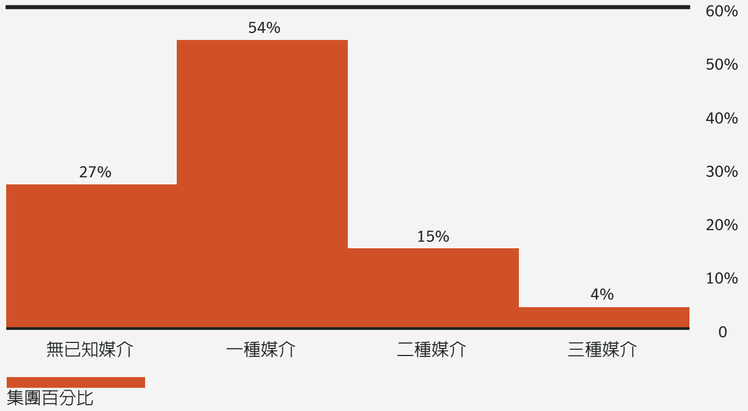
對組織發動目標式攻擊的最可能因素是情報收集，這也是 96% 的集團的犯案動機。

魚叉式網路釣魚電子郵件仍然是最受歡迎的攻擊途徑，65% 的已知集團使用這種媒介。

目標式攻擊集團感染媒介 (所有時間)



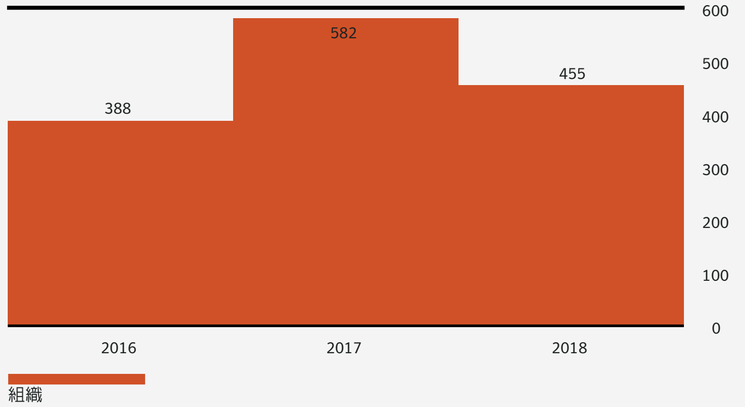
各目標式攻擊集團感染媒介 (所有時間)



受目標式攻擊集團影響的主要國家 (2016-2018)

國家/地區	攻擊
美國	255
印度	128
日本	69
中國	44
土耳其	43
沙烏地阿拉伯	42
南韓	40
台灣	37
阿拉伯聯合大公國	30
巴基斯坦	28

受目標式攻擊影響的組織數量 (年)



20 個最活躍集團使用的工具數量 (2016-2018)

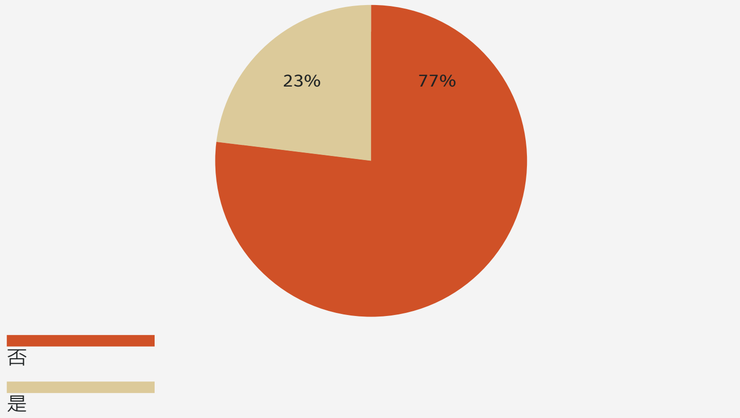
最少	最多	平均
1	18	5

20 個最活躍集團鎖定的組織平均數量 (2016-2018)

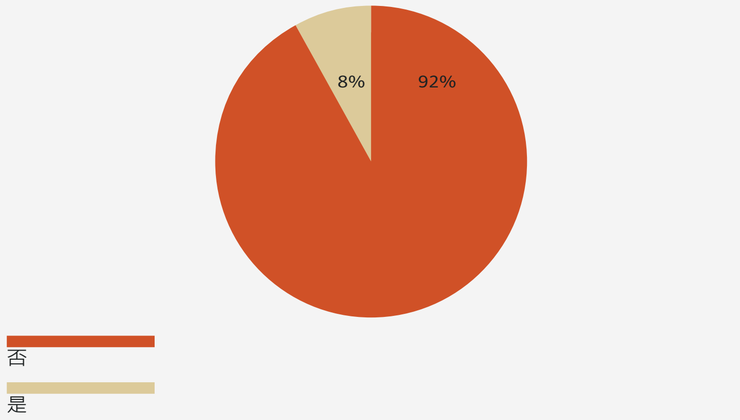
2016-2018
55

雖然仍是小眾領域，但破壞性惡意程式的利用率持續成長。已知有 **8%** 的集團使用破壞性工具，高於 **2017** 年底的 **6%**。

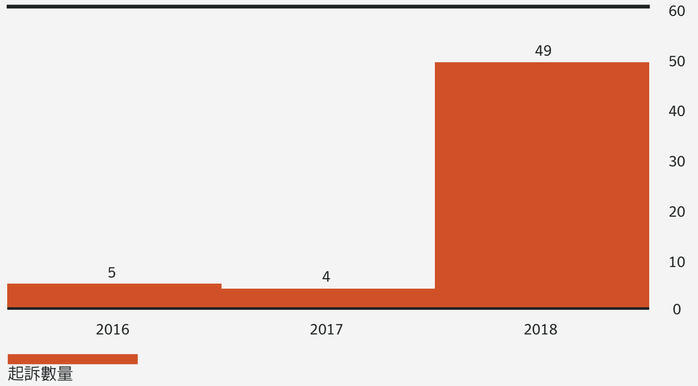
已知利用零時差漏洞的集團百分比 (所有時間)



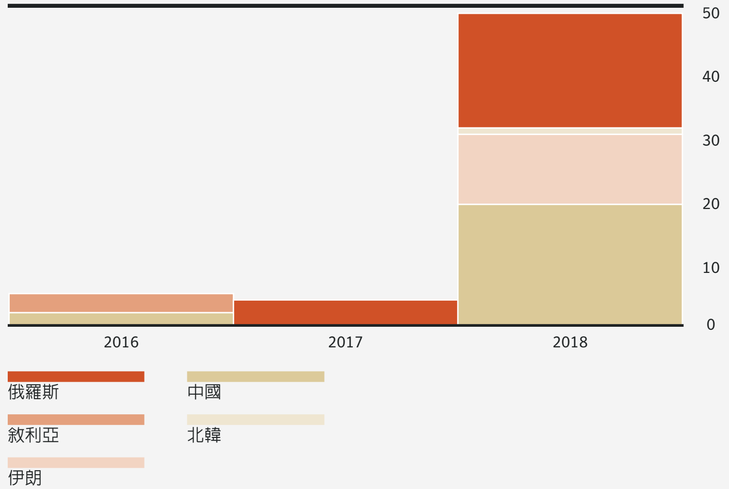
已知利用破壞性惡意程式的集團百分比 (所有時間)



美國政府起訴總數 (年)



各國遭美國政府起訴數量 (年)



IOT

物聯網 (IoT) 攻擊在 2017 年一度激增，隨後在 2018 年趨於穩定，當時賽門鐵克的物聯網 Honeypot 每月平均受到 5,200 次攻擊。到目前為止，路由器和連線攝影機是物聯網攻擊的主要來源，佔 Honeypot 所受攻擊的 90% 以上。2018 年，用於發動攻擊的受感染攝影機比例大幅增加。連線攝影機佔攻擊目標的 15%，高於 2017 年的 3.5%。攻擊者也逐漸著重使用 Telnet 作為攻擊途徑。在 2018 年，Telnet 佔攻擊嘗試的比例超過 90%，遠高於 2017 年的 50%。

涉及連線攝影機的攻擊從 2017 年的 3.5% 增加到 2018 年的 15%

路由器和連線攝影機

是 IOT 攻擊的主要來源

佔超過

90%

的活動

物聯網裝置每月平均遭受 5,200 次攻擊

物聯網攻擊的主要來源國家/地區 (年)

國家/地區	百分比
中國	24.0
美國	10.1
巴西	9.8
俄羅斯	5.7
墨西哥	4.0
日本	3.7
越南	3.5
南韓	3.2
土耳其	2.6
義大利	1.9

物聯網攻擊使用的熱門密碼 (年)

密碼	百分比
123456	24.6
[BLANK]	17.0
system	4.3
sh	4.0
shell	1.9
admin	1.3
1234	1.0
password	1.0
enable	1.0
12345	0.9

物聯網攻擊使用的熱門使用者名稱 (年)

使用者名稱	百分比
root	38.1
admin	22.8
enable	4.5
shell	4.2
sh	1.9
[BLANK]	1.7
system	1.1
enable	0.9
> /var/tmp/.ptmx&& cd/var/tmp /	0.9
> /var/.ptmx&& cd/var /	0.9

最常見的物聯網威脅 (年)

威脅名稱	百分比
Linux.Lightaidra	31.3
Linux.Kaiten	31.0
Linux.Mirai	15.9
Trojan.Gen.2	8.5
Downloader.Trojan	3.2
Trojan.Gen.NPE	2.8
Linux.Mirai!g1	1.9
Linux.Gafgyt	1.7
Linux.Amnesiark	1.1
Trojan.Gen.NPE.2	0.8

惡名昭彰的 **Mirai** 分散式阻斷服務 **(DDoS)** 蠕蟲仍是一項活躍的威脅，佔攻擊總數的 **16%**，是 **2018** 年第三常見的物聯網威脅。

路由器和連線攝影機是受感染最多的設備，分別佔攻擊事件中的 75% 和 15%。

最常遭物聯網威脅攻擊的通訊協定 (年)

目標式服務	百分比
Telnet	90.9
http	6.6
https	1.0
smb	0.8
ssh	0.6
ftp	<0.1
snmp	<0.1
cwmp	<0.1
upnp	<0.1
modbus	<0.1

最常遭物聯網威脅攻擊的通訊埠 (年)

TCP 通訊埠號	說明	百分比
23	Telnet	85.0
80	全球資訊網 HTTP	6.5
2323	Telnet (替代)	5.8
443	基於 SSL/TLS 的 HTTP	1.0
445	Microsoft 目錄服務	0.8
22	Secure Shell (SSH) 協定	0.6
8080	HTTP (替代)	0.1
2223	Rockwell CSP2	<0.1
2222	Secure Shell (SSH) 協定 (替代)	<0.1
21	檔案傳輸協定 [控制]	<0.1

用於執行物聯網攻擊的熱門裝置類型 (年)

裝置類型	百分比
路由器	75.2
連線攝影機	15.2
多媒體裝置	5.4
防火牆	2.1
PBX 電話系統	0.6
NAS (網路附加儲存裝置)	0.6
VoIP 電話	0.2
列印機	0.2
警訊系統	0.2
VoIP 變壓器	0.1

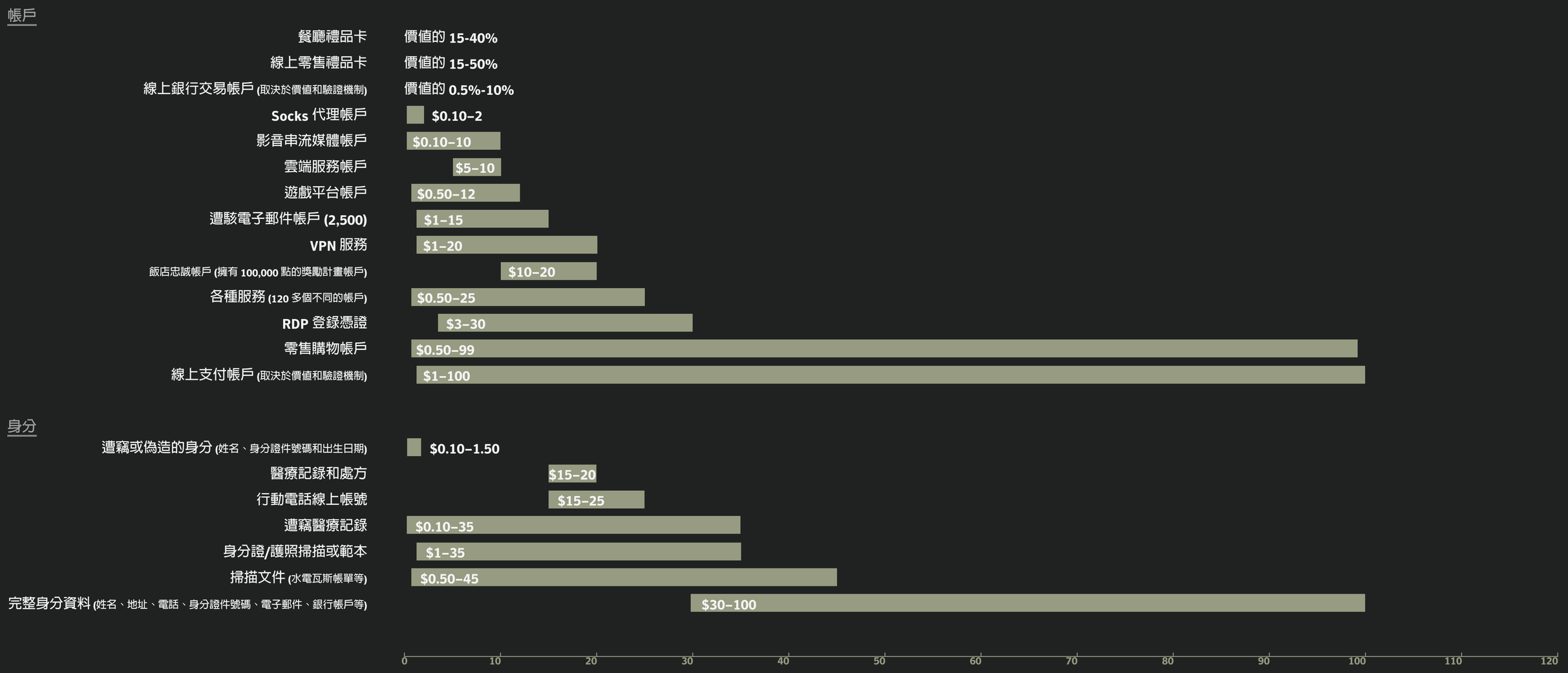
針對物聯網裝置的攻擊 (年)

年	攻擊總數	百分比變化
2017	57,691	
2018	57,553	-0.2

針對物聯網裝置攻擊平均數量 (月)

每月
5,233

地下經濟


帳戶
餐廳禮品卡
價值的 15-40%
線上零售禮品卡
價值的 15-50%
線上銀行交易帳戶 (取決於價值和驗證機制)
價值的 0.5%-10%
Socks 代理帳戶
$0.10–2
影音串流媒體帳戶
$0.10–10
雲端服務帳戶
$5–10
遊戲平台帳戶
$0.50–12
遭駭電子郵件帳戶 (2,500)
$1–15
VPN 服務
$1–20
飯店忠誠帳戶 (擁有 100,000 點的獎勵計畫帳戶)
$10–20
各種服務 (120 多個不同的帳戶)
$0.50–25
RDP 登錄憑證
$3–30
零售購物帳戶
$0.50–99
線上支付帳戶 (取決於價值和驗證機制)
$1–100
身分
遭竊或偽造的身分 (姓名、身分證件號碼和出生日期)
$0.10–1.50
醫療記錄和處方
$15–20
行動電話線上帳號
$15–25
遭竊醫療記錄
$0.10–35
身分證/護照掃描或範本
$1–35
掃描文件 (水電瓦斯帳單等)
$0.50–45
完整身分資料 (姓名、地址、電話、身分證件號碼、電子郵件、銀行帳戶等)
$30–100
0
10
20
30
40
50
60
70
80
90
100
110
120

地下經濟

身分 (續)

偽造健保卡	$50–220
包裹投遞箱	$70–240
偽造身分證、駕照、護照等	$25–5,000

轉帳服務

為銀行帳戶提供現金轉匯服務	價值的 .1-15%
為線上支付系統提供現金轉匯服務	價值的 1-5%
以比特幣支付 100 美元，即可獲得 1,000 美元轉帳	$100
現金轉匯服務	價值的 5-20%

惡意程式

Office 巨集下載程式產生器	$5–10
DDoS Bot 傀儡網路軟體	$1–15
間諜軟體	$3–50
加密貨幣竊盜惡意程式	$4–60
加密貨幣挖礦程式 (例如門羅幣)	$10–200
勒索軟體工具套件	$0–250
常見銀行交易特洛伊木馬程式含支援	$10–1,500

地下經濟

服務

航空公司機票及旅館預訂	價值的 10%
洗錢服務 (現金或加密貨幣)	4–40%
提取現金服務 (銀行帳戶、ATM 卡、假身分證)	$350
受僱駭客	$100+
自訂網路釣魚頁面服務	$3–12
DDoS 服務，短時間 <1 小時，防護等級中等的目標	$5–20
DDoS 服務，持續時間 >24 小時，防護等級中上的目標	$10–1,000

支付卡

單一信用卡	$0.50–20
單一信用卡含完整詳細資料 (Fullz)	$1–45
轉儲磁條 1/2 磁軌資料 (例如來自側錄)	$5–60

社交媒體

社交媒體平台 100 個讚	$0.10–3
社交媒體粉絲 500 人	$2–6
社交媒體影片觀看 100,000 次	$200–250

以下價格是取自可公開存取的地下論壇和暗網 TOR 網站。封閉式私人論壇的價格往往更低，我們無法驗證商品是否確實按提出的價格出售，其中可能有假造交易。

METHODOLOGY 研究方法

賽門鐵克已經建立全球最大的民間威脅偵蒐網路，並透過 Symantec Global Intelligence Network (GIN) 以最全面的方式收集網路安全威脅情報。

賽門鐵克 GIN 包含超過 1.23 億個攻擊偵測器，每秒記錄數千個威脅事件，並包含超過 9PB 的安全威脅資料。全球超過 30 萬間企業和組織倚賴賽門鐵克提供保護，並透過此網路監控威脅活動。賽門鐵克威脅防護產品組合具備遙測技術，協助我們 3,800 名網路安全研究人員和工程師掌握主要趨勢，洞悉威脅態勢的發展。

賽門鐵克的各項電子郵件安全技術每日可處理超過 24 億封電子郵件，從中彙整垃圾郵件、網路釣魚及電子郵件惡意程式的趨勢分析資料，這些技術包括：Symantec Messaging Gateway for Service Providers、Symantec Email Security.cloud、Symantec Advanced Threat Protection for Email、Symantec CloudSOC™ 服務及 Symantec Probe Network。賽門鐵克也透過企業、安全廠商及合作夥伴構成的廣大防詐騙社群，來收集各種網路釣魚資訊。

賽門鐵克專屬 Skeptic™ 技術每天過濾超過 322 億封電子郵件和超過 1.5 億次網頁請求，同時也是 Symantec Email Security.cloud 和 Web Security.cloud™ 服務的基礎，利用進階機器學習、網路流量分析和行為分析，偵測最為隱匿持續的威脅。此外，賽門鐵克的 Advanced Threat Protection for Email 透過加入雲端沙箱、額外的魚叉式網路釣魚防護、獨特的目標式攻擊識別功能，找出進階電子郵件攻擊。

賽門鐵克的 Secure Web Gateway 解決方案每月處理和分析數十億個網址，前述解決方案包括 ProxySG™、Advanced Secure Gateway (ASG) 和 Web Security Solution (WSS)，且皆以即時 WebPulse Collaborative Defense 技術和 Content Analysis 系統為後盾，進而識別並防止惡意酬載和控制敏感的網頁內容。

賽門鐵克 Endpoint Protection Mobile (SEPM) 提供行動威脅情報，可用於預測、偵測和防範各式各樣的既有和未知威脅。SEPM 的預測式技術採用多層式方法，運用大規模的使用者社群威脅情報，加上裝置和伺服器分析，主動為行動裝置提供防護，免於惡意軟體、網路威脅和應用程式、作業系統漏洞刺探利用的侵害。此外，Appthority 的行動技術可搭配 SEPM 運用，從而分析行動應用程式的惡意功能、不安全和不良的行為，例如漏洞、敏感資料遺失風險和侵犯隱私的行徑。

這些資源賦予賽門鐵克分析師無與倫比的資料來源，以利辨識、分析、並針對網路攻擊、惡意程式碼活動、網路釣魚及垃圾郵件等新興趨勢，提供資訊豐富的專業見解。以上成果彙整成為一年一度的賽門鐵克網路安全威脅研究報告™，提供一般企業、小型企業及消費者各種基本資訊，協助他們從現在到未來皆能有效保護系統安全。

參與人員

團隊

Brigid O'Gorman

Candid Wueest

Dick O'Brien

Gillian Cleary

Hon Lau

John-Paul Power

Mayee Corpin

Orla Cox

Paul Wood

Scott Wallace

撰寫人

Alan Neville

Alex Shehk

Brian Duckering

Chris Larsen

Christian Tripputi

Dennis Tan

Gavin O'Gorman

Parveen Vashishtha

Pierre-Antoine Vervier

Pravin Bange

Robert Keith

Sean Kiernan

Sebastian Zatorski

Seth Hardy

Shashank Srivastava

Shaun Aimoto

Siddhesh Chandrayan

Tor Skaar

Tyler Anderson

Yun Shen

INTERNET SECURITY THREAT REPORT

網路安全威脅研究報告

Symantec™

台灣賽門鐵克股份有限公司
地址：台北市信義區忠孝東路
5 段 68 號 29 樓
電話：+886 2 8729 9277
傳真：+886 2 8729 9257

www.symantec.com/zh/tw

如需任何分公司和聯絡電話的相關資訊，請造訪我們的網站。美國地區客戶如需產品資訊，請洽免付費電話 1 (800) 745 6054。

02/19