

# ISTR

2017 年 4 月

期數

目錄

簡介

內容摘要

重大數據

目標式攻擊：間諜、顛覆及惡意破壞

電子郵件：惡意程式、垃圾郵件及網路釣魚

網路攻擊、工具組以及刺探攻擊線上漏洞

網路犯罪及地下經濟

勒索軟體：勒索企業及消費者

最新攻防重點：物聯網、行動裝置及雲端環境威脅

# 22



# 目錄

4	簡介	34	刺探攻擊套件	59	感染向量
6	內容摘要	35	網路攻擊	61	勒索軟體即服務的時代到來
9	重大數據	35	瀏覽器漏洞	61	全新技術：目標式攻擊和「自給自足」(living off the land)
13	目標式攻擊：間諜、顛覆及惡意破壞	36	案例研討	62	其他平台現也出現漏洞
14	簡介	36	Angler：刺探攻擊套件的興衰史	62	執法單位破獲行動
14	重要發現	36	延伸閱讀	62	延伸閱讀
16	2016 年目標式攻擊態勢	36	最佳實務準則	62	最佳實務準則
17	趨勢及分析	37	網路犯罪及地下經濟	63	最新攻防重點：物聯網、行動裝置及雲端環境威脅
17	顛覆：目標式攻擊的全新動機	38	簡介	64	物聯網
18	惡意破壞攻擊捲土重來	38	重要發現	64	重要發現
18	自給自足 (living off the land)	38	惡意程式	64	趨勢及分析
19	Shamoon 攻擊者如何使用「自給自足」戰術	39	自給自足 (living off the land)：PowerShell、巨集及社交工程	65	國家資料
20	經濟間諜	41	傀儡網路個案研究：Necurs	66	密碼
21	全新威脅浮現	42	一切向錢看：金融惡意程式	66	Mirai 傀儡網路
21	延伸閱讀	43	攻陷 Mac	67	持續演進發展
22	最佳實務準則	44	Odinaff 及 Banswift：目標式金融竊盜大行其道的一年	67	展望未來
23	電子郵件：惡意程式、垃圾郵件及網路釣魚	44	Banswift	67	最佳實務準則
24	簡介	45	Odinaff	68	行動裝置
24	重要發現	45	資料外洩及地下經濟	68	重要發現
24	趨勢及分析	45	資料外洩	68	行動裝置惡意程式趨勢
24	惡意程式威脅	45	年度回顧	69	動機與技術
25	網路釣魚	47	資料外洩原因	70	惡意程式及灰色軟體比例
26	BEC 詐騙	48	遭到暴露的產業	70	執行時期封裝工具增加
27	垃圾郵件大致持平	50	國家資料	70	行動裝置漏洞
28	個案研究/調查	51	地下經濟	70	Android 架構的強化成果
28	改變戰術	53	瓦解與破獲	72	Apple 的痛處
28	冰天雪地：雪靴 (snowshoe) 和電暴 (hailstorm) 技術	53	Avalanche	72	最佳實務準則
29	久經考驗的社交工程	53	Bayrob	72	雲端
30	社交工程及新型傳訊平台	53	Lurk/Angler	72	重要發現
30	延伸閱讀	53	Dyre	72	趨勢及分析
31	最佳實務準則	54	延伸閱讀	73	高風險業務
32	網路攻擊、工具組以及刺探攻擊線上漏洞	54	最佳實務準則	73	危險的勒索軟體
33	簡介	55	勒索軟體：勒索企業及消費者	74	物聯網與雲端：網路犯罪的潛在共犯
33	重要發現	56	簡介	74	自給自足 (living off the land)
33	趨勢及分析	56	重要發現	74	延伸閱讀
33	漏洞評估	56	趨勢及分析	74	最佳實務準則
		58	個案研究/調查	75	參與人員
		58	勒索軟體如何影響消費者	76	關於賽門鐵克
		58	勒索軟體如何影響企業	76	更多資訊
		59	勒索軟體獅子大開口		

# 目錄

## 圖片、表格及圖表

9	重大數據	35	每月攔截的網路攻擊	57	新型勒索軟體系列
13	目標式攻擊：間諜、顛覆及惡意破壞	35	最常遭刺探攻擊的網站分類	57	新型勒索軟體變種
14	2016 年重大目標式攻擊資安事端時間表	36	瀏覽器漏洞	58	每月的勒索軟體變種。
15	值得注意的目標式攻擊集團	37	網路犯罪及地下經濟	58	消費者與企業感染比例
16	零時差漏洞年度總計	38	首次偵測到的獨特惡意程式變種	58	每月的消費者與企業感染比例
16	美國總統大選：2016 年攻擊時間表	38	2016 年首見獨特惡意程式變種的每月統計數量	59	平均勒索金額
17	工業控制系統漏洞揭露	39	偵測到的獨特惡意程式變種	60	主要勒索軟體威脅
19	可能遭攻擊者濫用的最常見工具	39	2016 年獨特惡意程式變種的每月統計數量	63	最新攻防重點：物聯網、行動裝置及雲端環境威脅
20	DNC 攻擊使用的魚叉式網路釣魚電子郵件	40	惡意程式的盛行程度及趨勢	65	每個月物聯網誘捕帳號每小時遭受的攻擊數
23	電子郵件：惡意程式、垃圾郵件及網路釣魚	40	2016 年典型攻擊情境的發生步驟如下	65	賽門鐵克物聯網誘捕帳號的前十名攻擊來源國家
24	電子郵件惡意程式整體比例	41	每月偵測到的 JavaScript 下載程式數量	66	嘗試登入賽門鐵克物聯網誘捕帳號最常使用的十大密碼
25	電子郵件惡意程式每月比例	41	每月偵測到的 Office 巨集下載程式數量	67	Mirai 在 2016 年的破壞足跡
25	各產業電子郵件惡意程式比例	41	Bot 傀儡程式活動數量	68	每年行動裝置惡意程式的整體偵測數量
25	各規模企業的電子郵件惡意程式比例	42	由 Necurs 垃圾郵件傀儡網路遞送的下載程式	68	行動裝置惡意程式系列每年累計數量
25	網路釣魚整體比例	42	十大金融木馬程式	69	每個行動裝置惡意程式系列的變種
26	網路釣魚每月比例	43	金融木馬程式活動的逐月數量	69	行動惡意程式變種逐年統計數量
26	各產業網路釣魚比例	43	2014 - 2016 年 Mac 惡意程式散佈每月統計數量	69	2016 年主要行動威脅
26	各種規模企業的網路釣魚比例	44	在 OS X 端點遭到封鎖的前十大惡意程式佔總感染數的比例	70	2014-2016 年惡意程式及灰色軟體比例
27	BEC 詐騙：常見主旨行	45	2014-2016 年資料外洩	70	現場惡意行動應用程式封包的比例
27	垃圾郵件整體比例	46	2014-2016 年每月資料外洩	71	2017 年 1 月 Android 不同版本的市佔率
27	垃圾郵件每月比例	46	2014-2016 年每月遭竊身分	71	回報的行動裝置漏洞 (依據作業系統)
28	各規模企業的垃圾郵件比例	46	2016 年外洩事件的資料遺失類型	73	企業最常使用的雲端應用程式
28	各產業垃圾郵件比例	47	2016 年資料外洩十大原因		
28	每月偵測到的下載程式數量	47	2016 年身分竊取的資料外洩十大原因		
29	含有 WSF 附件的遭封鎖電子郵件	48	依據資安事端數量的十大資料外洩部門		
29	電子郵件惡意程式的典型感染程序	48	依據資安事端數量的十大資料外洩子部門		
30	惡意程式垃圾郵件攻擊所用關鍵字	49	依據身分遭竊數量的十大資料外洩部門		
30	垃圾郵件攻擊偏好使用的語言	49	依據身分遭竊數量的十大資料外洩子部門		
32	網路攻擊、工具組以及刺探攻擊線上漏洞	50	資料外洩數量前十名國家		
33	經掃描發現漏洞的網站	50	身分遭竊數量前十名國家		
33	重大漏洞比例	51	地下經濟市集價格清單		
34	十大刺探攻擊套件	52	地下市集		
		55	勒索軟體：勒索企業及消費者		
		56	全球每日偵獲勒索軟體平均數量		
		57	全球每月偵獲勒索軟體數量		
		57	各國偵獲勒索軟體比例		

# 簡介



章節

00



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™ 以最全面的方式收集網路安全威脅情報。賽門鐵克全球智慧型網路 (Global Intelligence Network) 追蹤全球 70 萬個以上的攻擊者，並記錄超過 9,800 萬起攻擊偵測器的事件。此網路結合各種賽門鐵克產品、技術及服務，包括 Symantec Endpoint Protection™、Symantec DeepSight™ Intelligence、賽門鐵克安全委外管理服務™、諾頓™ 消費性產品及其他第三方資料來源，監控超過 157 個國家及地區的威脅活動，產生 9 兆列以上的安全性資料。

此外，賽門鐵克也維護一處全球最完備的漏洞資料庫，目前存有超過 88,900 筆漏洞 (時間範圍涵蓋 20 年以上)，而這些記錄源自 24,560 家廠商的 78,900 項產品。

賽門鐵克的各項安全技術每日可處理超過 20 億封電子郵件，從中匯整垃圾郵件、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：Skeptic™、服務供應商適用的 Symantec Messaging Gateway、Symantec CloudSOC 及 Symantec Probe Network。Skeptic™ 是賽門鐵克電子郵件與網頁安全雲端™ 專屬的啟發式技術，每天可過濾 3 億 3,600 萬封以上的電子郵件，以及 24 億筆以上的網頁要求。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。

賽門鐵克雲端威脅實驗室 (Symantec Cloud Threat Labs) 透過 Symantec CloudSOC 安全性技術的資料進行開發，提供雲端型威脅及風險的詳細分析，在 2016 年保護超過 2 萬個雲端應用程式、1.76 億份雲端文件，以及 13 億封電子郵件。Symantec CloudSOC 是賽門鐵克的雲端存取安全摺客 (CASB) 解決方案，專門針對雲端型應用程式及資料提供可見度、控制及保護。

賽門鐵克的網路應用程式防火牆和反向代理技術，每日可掃描出 10 億筆未曾出現過的網頁要求。

賽門鐵克網站安全解決方案自 2004 年起，以 100% 的可用性保護了全球 140 萬台網頁伺服器。驗證基礎架構每日處理 157 億筆以上的線上憑證狀態通訊協定 (OCSP) 查詢作業，它可用來取得全球 X.509 數位憑證的撤銷狀態。

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。

# 內容摘要

章節

# 01



網路攻擊者在 2016 年展現更大野心，從事各種離奇的攻擊事件，包括數百萬美元的虛擬銀行搶劫、國家資助團體企圖破壞美國大選，以及物聯網 (IoT) 裝置組成的傀儡網路，驅動有史以來最大規模的分散式阻斷服務 (DDoS) 攻擊。

雖然網路攻擊造成前所未有的破壞，但攻擊者使用的工具與戰術通常非常簡單，即可造成重大影響。零時差漏洞和精密惡意程式的使用趨於保守，而越來越多攻擊者開始嘗試隱匿行蹤。他們仰賴各種直截了當的方法，例如魚叉式網路釣魚電子郵件，以及所謂的「自給自足」(living off the land) 戰術，使用手邊的任何工具，例如合法的網路管理軟體及作業系統功能。

Mirai 是一波重大 DDoS 攻擊幕後的傀儡網路，主要由受感染的路由器、安全攝影機及低耗電和安全措施不佳的裝置組成。如果落入惡徒之手，就算是立意良善的裝置和軟體，也可造成破壞效果。

### 目標式攻擊：顛覆與破壞就在眼前

網路間諜領域明顯開始改變，轉而從事更公開的活動，試圖顛覆及破壞遭鎖定的組織和國家。美國民主黨遭受的網路攻擊，以及後續洩漏的遭竊資訊，是美國總統大選的主要話題之一。美國情報體系將攻擊歸咎於俄羅斯，且推論對方可能認為此次是成功的行動，因此未來可能會重複使用這類戰術，在其他國家影響政治，散佈爭執。

傳統上網路攻擊很少牽涉破壞行為，不過 2016 年出現兩起獨立的攻擊事件，均牽涉到破壞性惡意程式。磁碟抹除惡意程式於 1 月對烏克蘭發動攻擊，並於 12 月再次攻擊造成電力中斷。同時磁碟抹除特洛伊木馬程式 Shamoon 在消失四年後死灰復燃，並用於攻擊沙烏地阿拉伯的多個組織。

破壞攻擊增加的同時，部分隱匿活動也隨之減少，特別是經濟間諜、智慧財產權及商業秘密的竊盜活動都減少。美國與中國在 2015 年簽訂協議後，雙方承諾不在網路空間從事經濟間諜活動，之後可能涉及中國間諜的惡意程式被偵獲的情形，就大幅下滑。不過，這並不代表經濟間諜已經完全消失，而且，其他形式的目標式攻擊也同時增加，例如顛覆或高階金融攻擊。

### 金融竊盜：網路攻擊者準備大幹一票

直到最近，網路罪犯的主要焦點還是銀行客戶，攻擊帳戶或竊取信用卡。不過全新攻擊者的野心更大，他們以銀行本身做為目標，有時嘗試在一次攻擊內就竊取數百萬美元。Carbanak 等幫派率先發難，針對美國銀行發起一系列攻擊，證明這種方式的可行性。

2016 年有另外兩個團體要求更高，發動野心更大的攻擊。Banswift 團體自孟加拉中央銀行藉由刺探攻擊銀行安全的漏洞，滲透銀行網路竊取 SWIFT 憑證，進行詐騙轉帳以竊取 8,100 萬美元。

另一個名為 Odinaff 的團體，則是針對銀行及其他金融機構從事精密攻擊。其中也使用惡意程式，隱藏執行詐騙轉帳時的相關 SWIFT 訊息等客戶記錄。

雖然 Banswift 和 Odinaff 展現技術專業，並採用與進階團體有關的戰術，但精密程度遠不如此的團體，也同樣竊取了大量金錢。企業電子郵件入侵 (BEC) 詐騙，仰賴精細編製的魚叉式網路釣魚電子郵件，持續造成重大損失，過去三年遭竊金額超過 30 億美元。

### 自給自足 (living off the land)

不論是網路罪犯，或是國家資助的團體，各種攻擊者都開始改變戰術，更頻繁利用各種作業系統功能、現貨工具及雲端服務來侵害受害者。美國大選可說是自給自足攻擊最知名的個案。簡單的魚叉式網路釣魚電子郵件，成功入侵希拉蕊柯林頓競選總幹事 John Podesta 的 Gmail 帳戶，且未使用任何惡意軟程式或漏洞。所謂「自給自足」是指使用手邊資源，而不使用惡意程式及刺探攻擊，如此能夠為攻擊者提供許多優勢。由於改良的安全性開發及通報計畫，識別並刺探攻擊零時差變得更加困難。網路攻擊工具組已經失寵，原因可能是需要維護最新的刺探攻擊及後端基礎架構。

PowerShell 和巨集等強大的程序檔編寫工具，是 Windows 及 Microsoft Office 的預設功能，可協助遠端存取及惡意程式下載，無需使用漏洞或惡意工具。Office 巨集雖然已經存在將近 20 年，但是又重新出現在威脅情境中。攻擊者利用社交工程技術，輕鬆擊敗過去用於對付巨集病毒問題的安全措施。

如果妥善執行，自給自足戰術可造成幾乎無症狀的感染，讓攻擊者隱匿行蹤。

### 電子郵件重獲青睞成為攻擊管道

各式各樣的網路攻擊在 2016 年使用惡意電子郵件，不論是國家資助的網路間諜團體，還是大量郵件勒索軟體幫派，均使用電子郵件。其中每 131 封電子郵件就有一封帶有惡意，是五年來的最高比例。

電子郵件重獲青睞有多項因素。電子郵件是證實有效的攻擊管道，不必仰賴漏洞，而是使用簡單的欺騙技巧，誘使受害者開啟附件、點擊連結，或是揭露憑證。魚叉式網路釣魚電子郵件，例如意圖讓目標重設 Gmail 密碼的詐騙電子郵件，出現於美國大選攻擊之中。

惡意電子郵件會偽裝為例行信件，例如發票或出貨通知，這些也都是散佈勒索軟體的常見方式。由於市面上可雇用垃圾郵件傀儡網路 (例如 Necurs)，讓勒索軟體集團在 2016 年從事大量郵件活動，每日發出上萬封惡意電子郵件。

### 勒索軟體提升對受害者的勒索金額

勒索軟體持續危害企業和消費者，以無差別方式傳送大量惡意電子郵件。部分情況下，組織可能會不知所措，無法處理如此大量的勒索軟體電子郵件。攻擊者向受害者要求的贖金越來越高，2016 年平均贖金已由前一年的 294 美元上升至 1,077 美元。

攻擊者持續精進商業模式，讓惡意程式隱身在無害的電子郵件之中，採用無法破解的加密技術，贖金支付方式則牽涉匿名電子加密貨幣。這種商業模式的成功，造成越來越多的攻擊者加入其中。2016 年發現的新勒索軟體系列，已經增加三倍以上達到 101 種，而賽門鐵克記錄到勒索軟體的感染比例上升 36%。

### 最新攻防重點：物聯網和雲端成為焦點

正當勒索軟體和金融詐騙團體讓一般使用者面臨最大威脅之際，其他威脅也開始浮上檯面。物聯網裝置的攻擊行動的出現只是時間問題。2016 年由 Mirai 造成的首起重大資安事端，就是由物聯網裝置 (例如路由器和安全攝影機) 組成的傀儡網路。這類裝置安全性不佳，容易成為攻擊者下手的目標，攻擊者只要打造規模夠大的傀儡網路，就可執行最大規模的 DDoS 攻擊。賽門鐵克在 2016 年期間，發現嘗試攻擊物聯網裝置的次數增加兩倍，在活動高峰期，物聯網裝置平均每兩分鐘會遭受一次攻擊。

多個 Mirai 的目標是雲端相關服務，例如 DNS 供應商 Dyn。此外於雲端託管的數百萬個 MongoDB 資料庫遭駭，也顯示雲端攻擊已經成真，更可能會在 2017 年增加。企業應關注日漸仰賴雲端服務的問題，因為這是安全性盲點。賽門鐵克發現企業組織平均使用 928 個雲端應用程式，高於年初的 841 個。不過大部分資訊長認為自家組織只使用 30 或 40 個雲端應用程式，亦即低估了風險程度，可能遭受新興威脅攻擊。

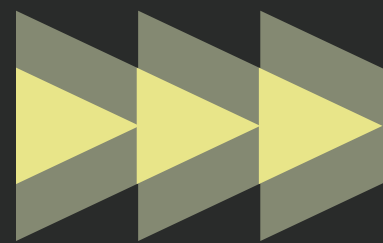


# 重大數據

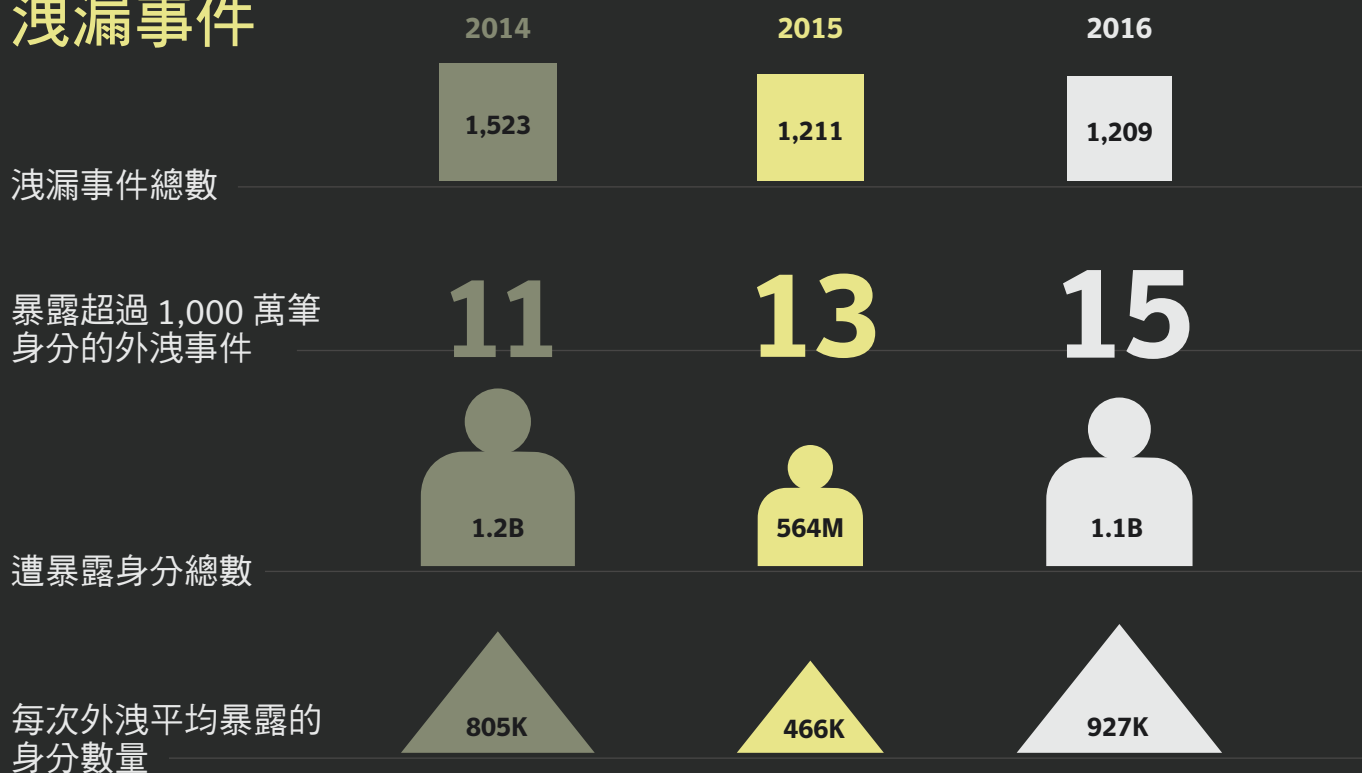
章節

352

02



## 洩漏事件

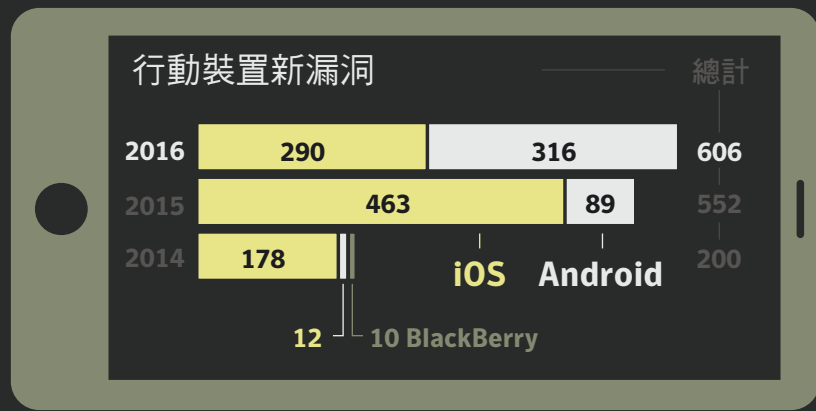


過去 8 年來，資料外洩導致超過 **71 億** 筆身分資料遭到暴露

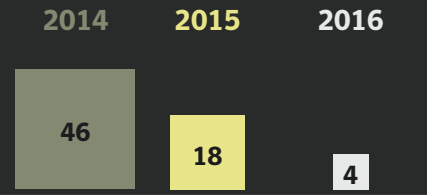
## 電子郵件威脅、惡意程式及 Bot 傀儡程式



# 行動裝置



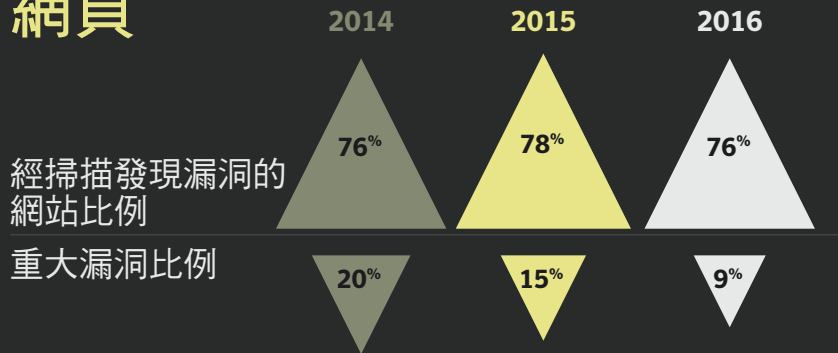
Android 行動裝置的新型惡意程式系列



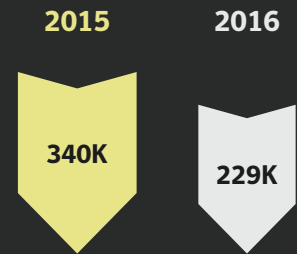
Android 行動裝置的新型惡意程式變種



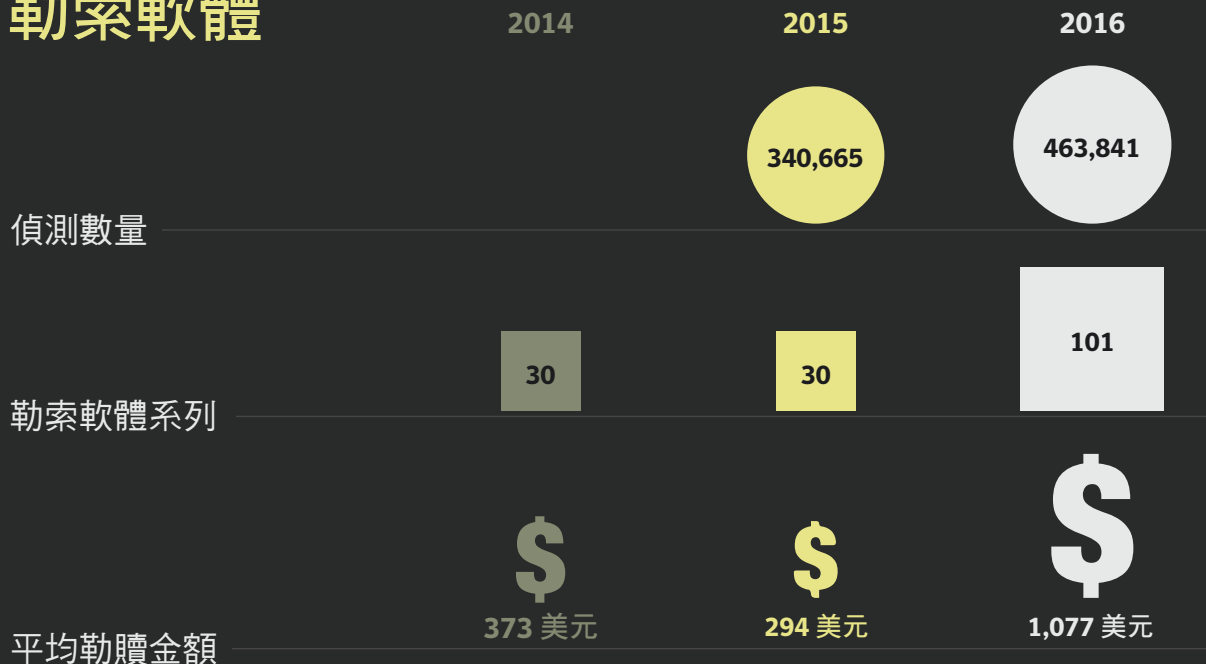
# 網頁



每天攔截的網路攻擊平均數量



# 勒索軟體



# 雲端

2015 年  
7月 - 12月

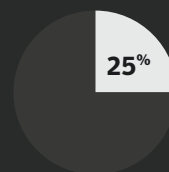
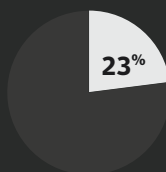
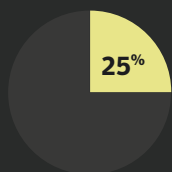
2016 年  
1月 - 6月

2016 年  
7月 - 12月

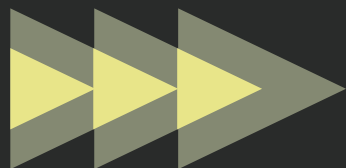
每個組織使用的  
雲端應用程式  
平均數量



廣泛共用的  
資料比例



# 物聯網

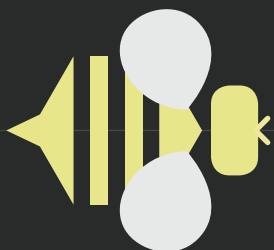


攻擊速度

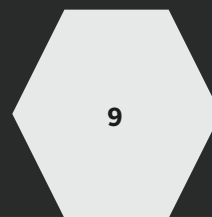
2 分鐘：  
物聯網裝置遭受  
攻擊所需的時間



賽門鐵克  
honeypot 每  
小時遭受攻  
擊的次數



2016 年|1月



2016 年|12月

# 目標式攻擊： 間諜、顛覆及惡意破壞



章節

# 03

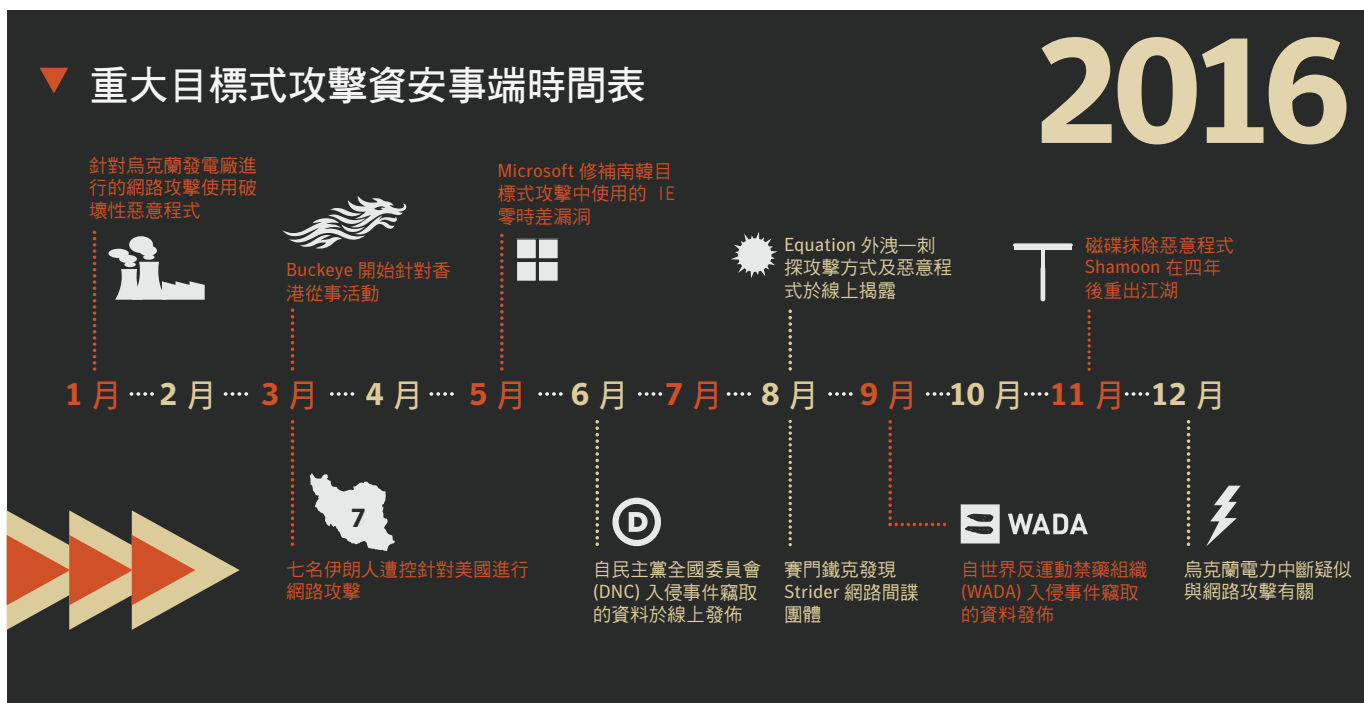


## 簡介

目標式攻擊態勢在 2016 年大幅改變，有多個集團浮出水面，公開參與政治顛覆活動。烏克蘭的持續衝突、美國大選和奧運，都有各種試圖竊取及洩漏資料的攻擊涉入其中，企圖影響公眾意見，煽動猜忌氛圍，甚至左右政治局勢。由於近期的攻擊頻頻奏效，加上 2017 年將有多國舉辦重大選舉，這類活動很可能會繼續下去。於此同時，各個團體持續精進戰術，其中許多不再使用自訂惡意程式，而更仰賴合法軟體工具來入侵遭到鎖定的網路。

## 重要發現

- 為了顛覆而發動的攻擊 (特別是在美國大選期間) 已成為最新手法，表示知名目標式攻擊的全新形式。
- 與破壞性惡意程式有關的目標式攻擊於部分地區有所增加，例如在中東地區捲土重來的**磁碟抹除惡意程式 Shamoon**，以及涉及 **KillDisk Trojan** 的攻擊事件，其作案目標鎖定烏克蘭。
- 經濟間諜活動 (如竊取交易或商業機密) 屬於傳統型態的目標式攻擊，數量在特定情況下有所減少。中美兩國達成不侵犯智慧財產權的協議之後，中國間諜惡意程式偵獲件數隨之銳減。不過，經濟間諜並未因此消失，而這項數據下降的同時，更出現了其他類型的目標式攻擊 (例如惡意破壞和顛覆)，而且數量正在上升。
- 零時差漏洞的重要性降低，部分攻擊者已經不再仰賴惡意程式，而是改採「自給自足」(living off the land) 策略。這是指利用手邊資源執行攻擊，包括合法的管理工具及滲透測試工具。



## 值得注意的目標式攻擊集團

<p><b>Sandworm</b> 自2014</p> <p>可能的來源地區： 俄羅斯</p> <p>別名/Quedagh、BE2 APT</p> <p><b>工具、戰術及流程 (TTP)</b> 魚叉式網路釣魚、漏洞、零時差、自訂後門程式、破壞性酬載</p> <p><b>動機</b> 間諜、惡意破壞</p> <p><b>目標類別及地區</b> 政府、國際組織、能源、歐洲、美國</p> <p><b>最新活動</b> 涉及烏克蘭媒體及能源目標的破壞性攻擊案例</p>	<p><b>Housefly</b> 自2001</p> <p>可能的來源地區： 美國</p> <p>別名/Equation</p> <p><b>工具、戰術及流程 (TTP)</b> 水坑式攻擊、感染 CD-ROM、感染 USB 金鑰、漏洞、零時差、自訂後門及資訊竊取程式、病毒程式</p> <p><b>動機</b> 間諜</p> <p><b>目標類別及地區</b> 國家級攻擊者屬意的攻擊目標</p> <p><b>最新活動</b> 於 2016 年偵破，其工具及刺探攻擊的漏洞隨之曝光。</p>
<p><b>Fritillary</b> 自2010</p> <p>可能的來源地區： 俄羅斯</p> <p>別名/Cozy Bear、Office Monkeys、EuroAPT、Cozyduke、APT29</p> <p><b>工具、戰術及流程 (TTP)</b> 魚叉式網路釣魚、自訂後門程式</p> <p><b>動機</b> 間諜、顛覆</p> <p><b>目標類別及地區</b> 政府、智庫、媒體、歐洲、美國</p> <p><b>最新活動</b> 涉及 Democratic National Committee (DNC) 攻擊案</p>	<p><b>Strider</b> 自2011</p> <p>可能的來源地區： 西方國家/地區</p> <p>別名/Remsec</p> <p><b>工具、戰術及流程 (TTP)</b> 進階偵察工具</p> <p><b>動機</b> 間諜</p> <p><b>目標類別及地區</b> 大使館、航空公司、俄羅斯、中國、瑞典、比利時</p> <p><b>最新活動</b> 賽門鐵克於 2016 年發現</p>
<p><b>Swallowtail</b> 自2007</p> <p>可能的來源地區： 俄羅斯</p> <p>別名/Fancy Bear、APT28、Tsar Team、Sednit</p> <p><b>工具、戰術及流程 (TTP)</b> 魚叉式網路釣魚、水坑式攻擊、感染儲存裝置、漏洞、零時差、自訂後門及資訊竊取程式</p> <p><b>動機</b> 間諜、顛覆</p> <p><b>目標類別及地區</b> 政府、歐洲、美國</p> <p><b>最新活動</b> 涉及 WADA 及 DNC 遭駭案</p>	<p><b>Suckfly</b> 自2014</p> <p>可能的來源地區： 中國</p> <p>別名/無</p> <p><b>工具、戰術及流程 (TTP)</b> 利用遭竊憑證登錄的自訂後門程式</p> <p><b>動機</b> 間諜</p> <p><b>目標類別及地區</b> 電子商務、政府、科技、醫療保健、金融、貨運</p> <p><b>最新活動</b> 利用多個遭竊的 Code Signing Certificate 進行目標式攻擊</p>
<p><b>Cadelle</b> 自2012</p> <p>可能的來源地區： 伊朗</p> <p>別名/無</p> <p><b>工具、戰術及流程 (TTP)</b> 自訂後門程式</p> <p><b>動機</b> 間諜</p> <p><b>目標類別及地區</b> 航空公司、電信、伊朗公民、政府、非政府組織</p> <p><b>最新活動</b> 監視伊朗境內目標及中東地區組織</p>	<p><b>Buckeye</b> 自2009</p> <p>可能的來源地區： 中國</p> <p>別名/APT3、UPS、Gothic Panda、TG-0110</p> <p><b>工具、戰術及流程 (TTP)</b> 魚叉式網路釣魚、零時差、自訂後門程式</p> <p><b>動機</b> 間諜</p> <p><b>目標類別及地區</b> 軍事、國防工業、媒體、教育、美國、英國、香港</p> <p><b>最新活動</b> 目標從西方國家/地區轉向香港</p>
<p><b>Appleworm</b> 自2012</p> <p>可能的來源地區： 北韓</p> <p>別名/Lazarus</p> <p><b>工具、戰術及流程 (TTP)</b> 魚叉式網路釣魚、DDoS 攻擊、磁碟抹除、零時差、自訂後門及資訊竊取程式、破壞性酬載</p> <p><b>動機</b> 間諜、惡意破壞、顛覆</p> <p><b>目標類別及地區</b> 金融、軍事、政府、娛樂、電子</p> <p><b>最新活動</b> 於 2016 年初受制於干擾行動。與孟加拉銀行攻擊者掛勾</p>	<p><b>Tick</b> 自2006</p> <p>可能的來源地區： 中國</p> <p>別名/無</p> <p><b>工具、戰術及流程 (TTP)</b> 魚叉式網路釣魚、水坑式攻擊、自訂後門程式</p> <p><b>動機</b> 間諜</p> <p><b>目標類別及地區</b> 科技、廣播、水下工程、日本</p> <p><b>最新活動</b> 針對日本目標的長期行動</p>

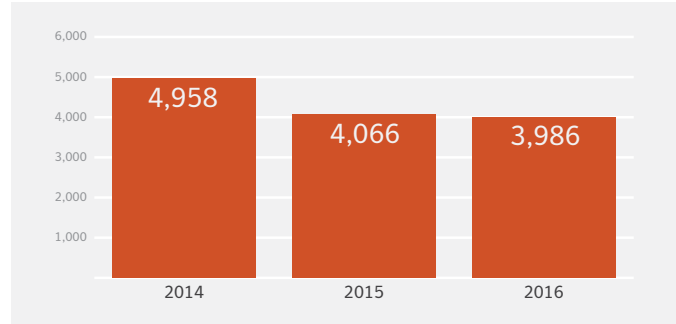
### 2016 年目標式攻擊態勢

目標式攻擊團體於 2016 年非常活躍，在歐洲、美國、亞洲及中東都發生了重大的資安事端。隨著時間進展，攻擊活動的層級似乎逐漸攀升，例如意圖顛覆美國政治的資安事端，以及鎖定沙烏地阿拉伯及烏克蘭的破壞性惡意程式。

目前有各式各樣的目標式攻擊集團正在運作。除了向來能夠進行各種網路行動的全球強權以外，區域強權也開始進軍網路空間，鎖定敵對國家和內部反對團體來發動網路間諜戰。「[值得注意的目標式攻擊集團](#)」一圖列出活躍於 2016 年並公認與國家有關的十大集團。

### 零時差漏洞年度總計

零時差漏洞 (軟體廠商未發現的漏洞) 由 2015 年的 4,066 個微幅下滑至 2016 年的 3,986 個。



前幾版的網路安全威脅研究報告著重在零時差漏洞遭到刺探攻擊的次數。今年我們決定分析零時差的總數，亦即軟體廠商未發現的漏洞。從這個指標來看，2016 年發現的零時差數量再次下降，由 4,066 個微幅下降至 3,986 個。該年度成長停滯的情形，顯示「漏洞通報獎勵」(bug bounty) 計畫日漸盛行，以及產品開發程序更加重視安全性，使攻擊者更難發現零時差漏洞，因此必須捨棄這類目標而擴大戰術範圍(請參閱以下「[自給自足](#)」(Living off the land) 戰術)。

Hacking Team 資料外洩之後，資安漏洞的地下市場在 2015 年廣受各界矚目，零時差數量也隨之下滑。這次資料外洩除了洩漏多起零時攻擊行為，也揭露這類攻擊經手的金額資訊。

## 美國總統大選：攻擊時間表

**3月**：FBI 通知民主黨全國委員會 (DNC) 其基礎架構遭到入侵

**4月**：2016 年柯林頓總統大選競選總幹事 John Podesta 收到魚叉式網路釣魚電子郵件活動

**5月**：其他魚叉式網路釣魚電子郵件傳送至 DNC 人員個人帳戶

**6月**：DNC 找出檔案及惡意程式，進而發現兩個涉嫌存取其網路的俄羅斯團體

**7月**：維基解密 (WikiLeaks) 發佈近 20,000 封 DNC 電子郵件

**7月**：民主黨國會競選委員會 (Democratic Congressional Campaign Committee; DCCC) 也遭受同一批攻擊者攻擊

**7月**：利用 Twitter 貼文宣稱入侵事件是由名為 Guccifer 2.0 的單一攻擊者進行，轉移大眾對俄羅斯團體的注意

**8月**：DNC 找出入侵者 存取，並宣稱已關閉及維護其網路安全

**8月**：由同一批攻擊者從事的兩起魚叉式網路釣魚活動，目標是政治智庫及策略非政府組織

**10月**：美國情報機構發表聲明，確信俄羅斯針對美國政治團體發動攻擊

**11月**：美國總統大選隔天，以選舉為主題的魚叉式網路釣魚電子郵件，傳送至美國聯邦政府的高階目標

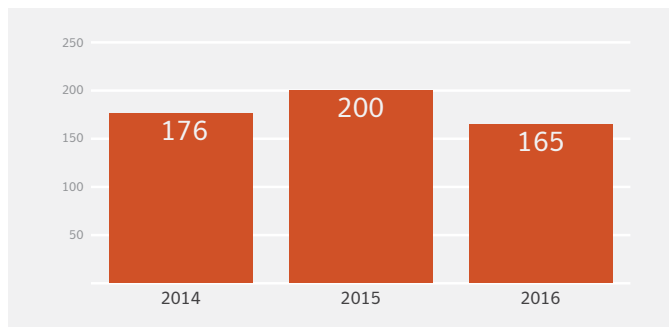
**12月**：第一批遭竊的 DNC 資料透過 BitTorrent 於線上發佈



不過 2016 年期間，仍出現多起刺探攻擊零時差漏洞的目標式攻擊。例如 Adobe 發現某個零時差漏洞遭到積極刺探攻擊之後，而在十月發佈 Flash Player 修正程式。合稱 Trident 的三項 Apple iOS 漏洞導致阿拉伯聯合大公國的人權行動者遭到網路攻擊，之後於八月遭到揭露並加以修正。五月，Microsoft 修正了在南韓的目標式攻擊中遭刺探攻擊的 Internet Explorer 零時差漏洞。

### 工業控制系統漏洞揭露

工業控制系統 (ICS) 發現的漏洞數量較 2015 年少。



同樣地，2016 年工業控制系統 (ICS) 發現的漏洞數量較 2015 年少，進一步證明攻擊者更難發現漏洞。

### 趨勢及分析

#### 顛覆：目標式攻擊的全新動機

2016 年最引人注意的發展之一，就是有越來越多的攻擊行動，是為了左右目標國家的政治事件風向。傳統上，目標式攻擊集團都將重點放在間諜活動，並維持低調以免遭到偵測，不過 2016 年有許多團體增加了公開攻擊的次數。

2016 年 8 月，涉及 Equation 網路間諜團體的一筆重大資料，就是由自稱「Shadow Brokers」的團體在線上洩漏出去，內容包含 Equation 使用的工具及攻擊套件，Shadow Brokers 聲稱這只是一小部分，其餘資料將透過競標出售。

大部分洩漏檔案都是數年前的資料 (介於 2010 至 2013 年之間)，而目前仍然不知洩漏者是如何取得。Shadow Brokers 在這些資安事端之前默默無聞，但也可能是其他團體的化名。

由於 Shadow Brokers 並未積極銷售這批遭竊資料，因此背後的主要動機似乎是想讓 Equation 團體難堪，而非從中牟利。

2016 年最知名的顛覆性資安事端，是民主黨在美國總統大選期間遭受的一連串入侵事件。美國情報體系聯手調查之後，判定這場行動牽涉兩個與俄羅斯情報機構掛勾的團體。

賽門鐵克之前就已掌握這兩個活躍多年的團體，他們參與的間諜活動，大多鎖定美國及歐洲的一系列目標。Fritillary (亦稱 APT29 及 Cozy Bear) 至少在 2010 年就開始活躍，曾經使用 Duke 系列的木馬程式攻擊目標，例如 Cozyduke (Trojan.Cozer) 及 Seaduke (Trojan.Seaduke)。Swallowtail (亦稱 APT28 及 Fancy Bear) 已活躍至少 10 年以上，通常使用 Sofacy 木馬程式 (Infostealer.Sofacy) 作為主要惡意程式工具。Fritillary 的目標是非常知名的個人及組織，涵蓋歐盟及美國的政府、國際政策及研究機構，而 Swallowtail 則主要鎖定東歐國家的軍事、政府、使館及國防承包商人員。

Swallowtail 在 9 月也涉嫌洩漏竊取自世界反運動禁藥組織 (WADA) 的醫療記錄。他們入侵系統後，發佈了美國奧運選手、英國自行車手及其他國家運動員的相關資料。

WADA 表示 Swallowtail 犯下了這起入侵事件。該團體採取罕見的做法，先使用 Fancy Bear 名稱架設自家網站再公布遭竊資料，聲稱其中含有運動員違反禁藥規範的證據。

DNC 及 WADA 入侵事件顯示以上兩個團體在戰術上的重大轉變，兩者先前未曾從事這類顛覆活動。美國情報體系針對 DNC 資料遭竊及後續的公開洩密事件提出報告，判定這是由俄羅斯政府主導的攻擊，試圖影響 2016 年美國總統大選選情。該報告的結論也指出，俄羅斯會將此次攻擊視為一項成功，可能成為往後行動的參考，繼續試圖影響政治風向。

由於這類戰術經證實可以製造爭端和混淆，因此今後極可能再度用來暗中顛覆其他國家。法國及德國今年都將進行大選，而德國國外情報單位首長 Bruno Kahl 表示該國已遭受相同類型的攻擊。他表示：「我們握有證據顯示，網路攻擊的唯一目標，就是要造成政治情勢動盪。罪犯蓄意汙名化民主程序，不在乎最終是誰受益。」

#### 惡意破壞攻擊捲土重來

2016 年再次出現惡意破壞攻擊，起初是針對烏克蘭的幾起攻擊事件，犯案工具是以磁碟抹除惡意程式為主。這些攻擊事件可能涉及另一個俄羅斯網路間諜團體（名為 Sandworm），並且動用了極具破壞力的木馬程式 (Trojan.Disakil)。烏克蘭的媒體機構和能源部門在 2015 年底及 2016 年初遭受攻擊，據傳後者造成烏克蘭電力中斷。

Disakil 於 2016 年底捲土重來，新版本偽裝成勒索軟體在外流竄。據稱這款惡意程式用於多起攻擊事件，試圖攻擊烏克蘭的金融部門。

其變種可在 Linux 電腦執行，然後加密關鍵的作業系統檔案，導致其無法使用。完成加密後，就會顯示訊息要求 222 比特幣的贖金（攻擊當時相當於 21 萬美元）。支付贖金無法解密受影響的檔案，因為受感染電腦產生的加密金鑰並未存於本機，也不是位於指令和控制 (C&C) 伺服器。這款惡意程式可能偽裝成勒索軟體，藉此誘騙受害者，導致無法徹查攻擊事件。

破壞性的攻擊也發生在其他地區，其中最知名的案件就是 Shamoon 磁碟抹除惡意程式 (W32.Distrack) 在消失五年後重出江湖。這款軟體最早於 2012 年用於攻擊沙烏地阿拉伯能源部門，新型變種 (W32.Distrack.B) 則於 2016 年 11 月及 2017 年 1 月攻擊該國境內的目標。

在第一波的新攻擊中，惡意程式設定於 11 月 17 日週四當地時間下午 8:45，啟動磁碟抹除酬載。沙烏地阿拉伯人每週的工作日為週日至週四，因此攻擊時間是在大部分員工都回家的週末進行，藉此減少遭到發現的機會，製造最大的破壞效果。

Shamoon 惡意程式會設定密碼，而密碼似乎是遭鎖定的組織竊取而來，用於讓惡意程式在組織網路中散佈。

這起攻擊事件的動機可能與政治有關。在 2012 年的攻擊事件中，受感染電腦的主要開機記錄遭到抹除，並更換為美國國旗燃燒的影像。最新攻擊使用的相片，則是 2015 年在地中海溺斃的三歲敘利亞難民 Alan Kurdi。

11 月的攻擊事件與名為「Greenbug」的團體有關，賽門鐵克在調查 Shamoon 攻擊時發現這件事。Greenbug 鎖定中東地區的一系列組織，包括航太、能源、政府、投資及教育部門的各個企業。賽門鐵克發現 Greenbug 感染的管理員電腦中，至少有一部屬於之後遭受 Shamoon 攻擊的組織。

1 月的攻擊是由名為「Timberworm」的團體執行（請參閱「Shamoon 攻擊者如何使用『自給自足』戰術」章節）。雖然 Greenbug 及 Timberworm 似乎是各自獨立的團體，但如果兩者都在散佈 Shamoon，就可能由單一團體指示進行。

#### 自給自足 (living off the land)

攻擊者開始改變戰術，擴大選用的工具種類，且不再仰賴傳統的惡意程式攻擊工具組和零時差漏洞。「自給自足」(living off the land) 並不是新技術，且越來越多團體均加以採用，使用各種作業系統功能、合法工具及雲端服務入侵網路。這種戰術可讓攻擊更難以偵測，因為相較於出現惡意程式，更難找出合法工具的惡意用途。

### Shamoon 攻擊者如何使用「自給自足」戰術

2016 年使用自給自足戰術的主要代表之一是網路間諜團體 Timberworm，他們牽涉恢復多項攻擊，包括破壞性的惡意程式 Shamoon (W32.Disttrack.B)。Shamoon 消失四年後，於 2016 年 11 月捲土重來，在沙烏地阿拉伯針對目標發動一系列攻擊。2016 年 11 月稍後又發動兩波攻擊，並於 2017 年 1 月再次犯案。

11 月攻擊與名為「Greenbug」的團體有關，而 1 月的攻擊則是由網路間諜團體 Timberworm 所發動，他們犯下了中東地區一連串的攻击案件。

為了散佈 Shamoon，Timberworm 首先鎖定目標組織中的個別人士，來傳送魚叉式網路釣魚電子郵件。部分電子郵件含有 Microsoft Word 或 Excel 附檔，其他電子郵件則包含惡意連結，一點選就會下載類似 Word 或 Excel 的檔案。

如果開啟檔案，巨集就會執行 PowerShell 程序檔供遠端存取，並且進行受害電腦的基本偵察。一旦發現屬意的電腦，他們就會安裝惡意程式 (Backdoor.Mhretreiv)。

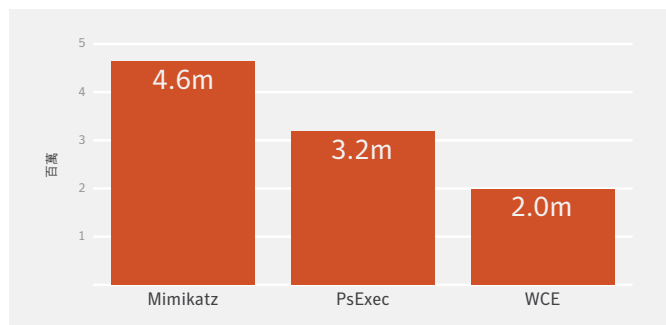
攻擊者可藉此使用各式各樣的合法管理工具和滲透測試工具，周遊在目標網路之中，並找出所要感染的電腦。其中包括：

- PsExec：由 Microsoft Sysinternals 提供的工具，可在其他系統執行程序
- PAExec：PsExec 的免費重新實作版本，由 Poweradmin 提供
- Nmap：多用途 IPv4/IPv6 網路掃描程式
- Samsync：傾印 (dump) Windows 密碼雜湊的駭客工具
- Mimikatz (Hacktool.Mimikatz)：用來取得憑證的駭客工具
- TightVNC：開放原始碼遠端桌面存取應用程式
- Plink：指令行網路連線工具，支援加密通訊
- Rar：封存公用程式，可在洩漏前壓縮檔案

一旦偵察完成，Shamoon (W32.Disttrack.B) 就會安裝於預先選定的電腦。惡意程式可以設於特定時間，在所有遭入侵的電腦觸發磁碟抹除酬載，達到最強大的攻擊效果。

### 可能遭攻擊者濫用的最常見工具

根據賽門鐵克的檔案聲譽遙測 (file reputation telemetry)，2016 年最常遭攻擊者濫用的合法工具是 Mimikatz、PsExec 及 WCE。



根據賽門鐵克的檔案聲譽遙測，2016 年最常遭攻擊者濫用的合法工具是 Mimikatz (Hacktool.Mimikatz)，這款工具能夠變更權限、匯出安全憑證，並以純文字回復 Windows 密碼；其後則為 Microsoft Sysinternals 工具 PsExec 及 Windows Credential Editor。由於實例數量急遽上升，且這三種工具都具有合法用途 (Mimikatz 甚至可用於滲透測試)，不難瞭解這類工具對攻擊者的吸引力，因為使用時不會引人注意。

惡意 PowerShell 程序檔也廣泛用於鎖定攻擊，其中攻擊者刺探攻擊架構彈性下載酬載，在入侵網路周遊，並執行偵察行動。賽門鐵克最近的研究證實，PowerShell 是一項熱門的攻擊工具。在賽門鐵克 Blue Coat 惡意程式分析沙箱內，所有 PowerShell 程序檔中，有 95.4% 具有惡意。

最近有一系列團體廣泛採用這種作法，其中的知名範例，就是先前提到的美國總統大選 DNC 遭入侵事件。FBI 表示最初的入侵點是在 2016 年 3 月 19 日，魚叉式網路釣魚電子郵件傳送至競選總幹事 John Podesta 的電子郵件帳戶。這封電子郵件看起來像是來自正式的 Gmail 管理員帳戶，其中表示 John Podesta 的電子郵件遭到入侵，引導他重設密碼。電子郵件含有縮短的 URL 網址，用於隱匿惡意 URL 網址。只要點選這個網址，受害者就會連往假的密碼重設頁面，在此偽裝成合法 Gmail 帳戶的重設頁面進行設定。執行攻擊時不需要惡意程式或刺探攻擊，而是利用簡單的社交工程取得密碼。

## DNC 攻擊使用的魚叉式網路釣魚電子郵件

2016 年柯林頓總統競選總幹事 John Podesta 收到的魚叉式網路釣魚電子郵件文字。

```
*From:* Google <no-reply@accounts.googlemail.com>
*Date:* March 19, 2016 at 4:34:30 AM EDT
*To:* ██████████@gmail.com
*Subject:* "Someone has your password"

Someone has your password
Hi John

Someone just used your password to try to sign in to your Google Account
██████████@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password
immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team
You received this mandatory email service announcement to update you about
important changes to your Google product or account.
```

另一個自給自足戰術的例子，就是可能位於伊朗的 [Chafer 網路間諜團體](#)。他們的攻擊媒介之一是入侵網頁伺服器，透過網頁掃描工具識別漏洞，並加以刺探攻擊。在最近土耳其目標遭到入侵的事件中，賽門鐵克發現 Chafer 使用名為 JexBoss 的軟體工具，識別出目標使用的 JBoss 應用程式伺服器為舊型且是未修補社群版本。該團體在伺服器部署程序檔 Web Shell，可允許遠端管理，以便複製軟體工具 Mimikatz。

如此一來，就能藉此使用 Qwinsta 及 Whoami 等原生作業系統工具，擷取入侵伺服器的相關資訊。該團體在初次入侵後 20 分鐘內，使用 Microsoft Sysinternals 工具 PsExec 擴散至目標網路的其他兩台電腦。

最近另一個使用這項戰術的則是中國團體 Tick，主要鎖定攻擊日本組織，時間至少長達 10 年之久。該團體在最近的攻擊中，[使用魚叉式網路釣魚電子郵件並入侵日本網站，以便感染目標](#)。

Tick 主要的工具之一，是自行開發的惡意程式 ([Backdoor.Daserf](#))，不過也使用其他一系列工具，例如前述的 Mimikatz、Windows Credential Editor 及 GSecdump ([GSecdump](#))。GSecdump 這款駭客工具，可由 Security Accounts Manager (SAM)、Active Directory 及使用中的登入工作程序竊取雜湊。

此外也有攻擊者使用基本雲端服務來外洩資料，而非透過指令與控制伺服器。例如攻擊 DNC 的團體之一 [Fritillary](#)，就使用約 200 個 [Microsoft OneDrive 帳戶](#) 洩漏遭竊資料。這麼做是為了在眾目睽睽之下隱匿罪證，攻擊者也可能認為，將資料移往 OneDrive 有利於偽裝成合法活動。

## 經濟間諜

美國與中國在 2015 年 9 月達成協議，[表示雙方不對彼此從事網路經濟間諜活動](#)。依據協議條款，雙方同意兩國政府都不會「從事或蓄意支援透過網路竊取智慧財產權，包括商業機密或其他機密商業資訊，也不能向公司或商業部門提供競爭優勢。」

有鑑於間諜行動的性質，要確認這項協議是否發揮作用並不容易。不過賽門鐵克分析後發現強大的證據，顯示兩國簽署協議之後，可能涉及中國團體的活動大幅減少。

賽門鐵克判定位於中國的網路間諜團體使用惡意程式系列被偵獲的情形，經過檢視之後，可針對長期活動程度提供深入見解。協議簽署後，感染數量幾乎立即大幅下降。接下來幾個月感染率持續下降，直到年底仍維持低水準。

在此同時，部分個別中國團體也展現不同的活動模式。例如，[Buckeye 團體](#) (亦稱 APT3 或 Gothic Panda) 針對美國、英國及其他國家組織從事網路間諜行動，至少長達五年以上。不過自 [美中簽訂協議之後](#)，該團體關注的焦點就開始轉變。

自 2015 年 6 月以來，該團體開始入侵香港的政治組織。到了 2016 年 3 月，Buckeye 幾乎完全將重點轉移至香港組織。雖然仍沒有證據顯示前述重點轉移是因為協議造成，不過針對其他國家目標的網路間諜活動，其整體趨勢則是出現一致的下降情形。雖然美中協議造成部分網路攻擊團體轉移焦點，但這並不表示大規模終止行動。

#### 全新威脅浮現

除了已知目標式攻擊集團持續活動，2016 年也浮現其他威脅。賽門鐵克於八月關注過去默默無名的 Strider 團體，他們針對俄羅斯、中國、瑞典及比利時的特定目標發動攻擊。

Strider 的主要工具是名為 Remsec ([Backdoor.Remsec](#)) 的隱藏木馬程式，其精密程度相當高，我們認為這主要是設計用於間諜活動。Strider 至少自 2011 年開始活動，一直維持低調，其中部分原因是他們極度慎選目標，而賽門鐵克在七個不同組織的 36 台電腦發現感染證據。

Remsec 具備高度的技術功能，含有多項進階功能，可協助規避偵測。多種元件是以可執行檔 blob (二進位大型物件) 的形式存在，更難以受到傳統以特徵為基礎的防毒軟體偵測。除此之外，大部分惡意程式功能是透過網路部署，亦即僅儲存於電腦記憶體，絕對不會儲存於磁碟，這更提升了偵測難度。

Remsec 讓各界瞭解，國家級集團現在能夠對目標運用的技術和資源程度。由於廠商能夠更有效地找出目標式攻擊團體，因此部分團體不再使用精密工具，不過仍然有一些獨樹一格的行動。

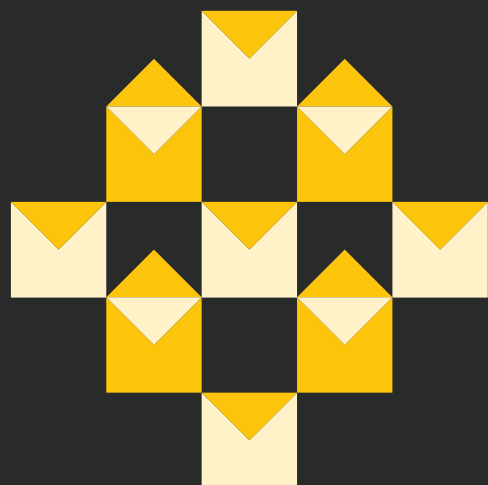
#### 延伸閱讀

- [Buckeye 網路間諜團體將目光從美國轉向香港](#)
- [Equation：秘密網路間諜團體是否曾經遭到外洩？](#)
- [Strider：網路間諜團體利用 Sauron 攻擊目標](#)
- [Patchwork 網路間諜團體擴大目標範圍，涵蓋政府乃至於各種產業](#)
- [Tick 網路間諜團體利用零時差攻擊日本](#)
- [台灣遭新型網路間諜後門木馬程式鎖定](#)
- [Suckfly：揭露 Code Signing Certificate 的祕密](#)
- [大型協同合作行動試圖再次殲滅 Lazarus](#)
- [涉及烏克蘭電力中斷的破壞性 Disakil 惡意程式，也用於攻擊媒體組織](#)
- [Shamoon：死灰復燃，依舊極具破壞性](#)
- [Greenbug 網路間諜團體鎖定中東地區，似乎與 Shamoon 有關](#)
- [Shamoon：僅針對特定目標的多階段破壞性攻擊](#)

### 最佳實務準則

- 著重多重、重複及相互支援的防禦系統，以各種特定技術或防護方式抵禦單點失敗。其中應包括部署定期更新防火牆和閘道防毒、入侵偵測或防禦系統 (IPS)、含惡意程式防護的網站漏洞，以及整個網路適用的網頁安全閘道解決方案。
- 刺探攻擊漏洞是目標式攻擊集團的常用戰術。接收各個廠商平台的新型漏洞及威脅警示，並儘速修正已知漏洞。
- 實施及執行安全政策，加密任何儲存中及傳輸中的機密資料。請務必連同客戶資料一起加密，如此能夠減輕組織內部潛在資料洩漏的損害。
- 攻擊者經常使用遭竊或預設憑證周遊網路因此要確認密碼強度夠強。重要密碼 (例如具備高度權限者) 至少應為 8 -10 個字元 (最好更長)，並混合使用字母和數字。鼓勵使用者避免在多個網站上重複使用相同的密碼，也不得向他人透露密碼。刪除未使用的憑證及設定檔，並限制建立的管理層級設定檔數量。
- 教育員工魚叉式網路釣魚電子郵件的危險性，包括小心處理陌生來源的電子郵件，也要注意開啟未經要求的附件。完整的防護架構可協助您抵禦這類電子郵件威脅，包括 [Symantec Email Security.cloud](#) 可封鎖源自電子郵件的威脅，以及 [Symantec Endpoint Protection](#) 可封鎖端點上的惡意程式。[Symantec Messaging Gateway](#) 的 Disarm 技術，也能保護電腦避免威脅，在附加文件引誘使用者之前，移除其中的惡意內容。

# 電子郵件：惡意程式、 垃圾郵件及網路釣魚



章節

# 04



## 簡介

電子郵件雖然是重要的通訊工具，也是讓一般使用者及組織遭受破壞的主要來源之一。這類破壞可能源自不必要的電子郵件（垃圾郵件），或是其他更危險的威脅，例如勒索軟體的傳播，或是針對性魚叉式網路釣魚攻擊。

所有電子郵件有一半以上（53%）是垃圾郵件，而其中含有惡意程式的比例持續提升。電子郵件惡意程式增加的主要原因，是專業化的惡意程式濫發垃圾郵件行動。惡意程式編寫者可將本身的垃圾郵件攻擊，委外給執行大量垃圾郵件攻擊的專業團體處理。電子郵件惡意程式行動規模大幅提升，顯示攻擊者從這類攻擊獲得相當豐厚的利潤，而電子郵件可能在 2017 年仍是主要的攻擊途徑之一。

## 重要發現

- 電子郵件惡意程式比例在 2016 年大幅攀升，從 2015 年每 220 封電子郵件就有一封含有惡意程式，成長為 2016 年的每 131 封就有一封含有惡意程式。主要的增加原因是傀儡網路，能夠提供與威脅有關的大型垃圾郵件攻擊，例如 Locky ([Ransom.Locky](#))、Dridex ([W32.Cridex](#)) 及 TeslaCrypt ([Ransom.TeslaCrypt](#))。
- 針對性魚叉式網路釣魚攻擊，特別是所謂的企業電子郵件入侵 (BEC) 詐騙，目前獲得攻擊者的青睞，取代過去的大量郵件網路釣魚攻擊。網路釣魚比例從每 1,846 封就有一封，下降為每 2,596 封就有一封，反映了前述情形。
- 主要電子郵件威脅團體，主要仰賴使用第一階段下載程式安裝最終酬載，一般為勒索軟體。2016 年初，含有惡意巨集的 Office 文件，是垃圾郵件攻擊最常使用的下載程式。不過 3 月出現變化，自此之後 JavaScript 下載程式就開始泛濫。

## 趨勢及分析

2016 年期間收集的電子郵件資料，證實電子郵件已經成為惡意程式傳播的主要媒介。

### 惡意程式威脅

2016 年最值得注意的趨勢，就是電子郵件惡意程式比例上升，從 2015 年的每 220 封電子郵件就有一封，增加至 2016 年的每 131 封電子郵件就有一封。

### 電子郵件惡意程式整體比例

2014	2015	2016
每 244 封就有一封	每 220 封就有一封	每 131 封就有一封

前述電子郵件惡意程式增加，可能與 2016 年大量郵件惡意程式團體持續活動有關，主要散播 Locky、Dridex 及 TeslaCrypt。惡意程式主要的散佈途徑之一，是名為 Necurs ([Backdoor.Necurs](#)) 的傀儡網路。Necurs 從事各種大型攻擊，透過 JavaScript 及 Office 巨集附件傳播惡意程式。這些下載程式之後會安裝最終酬載，在 2016 年大多為 Locky 等勒索軟體威脅。

Necurs 在 2016 年 12 月 24 日至 2017 年 3 月 20 日期間沒有活動，亦即 2017 年 1、2 月的電子郵件惡意程式比例大幅下滑。雖然惡意程式團體過聖誕節的情況並不罕見，但休息時間通常僅一週左右。Necurs 停止行動的原因至今不明，不過他們回歸之後就立即恢復大量郵件攻擊。賽門鐵克光是在 Necurs 回歸的 3 月 20 日，就封鎖將近 200 萬封的惡意電子郵件。

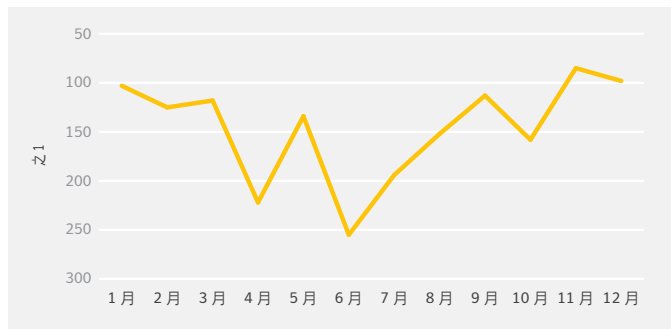
Dridex 是金融木馬程式，用於竊取一般使用者的銀行交易憑證。Dridex 幕後攻擊者是專業人士，投入許多心力持續精進惡意程式，並讓用於傳播惡意程式的電子郵件，盡可能看起來像是合法電子郵件。TeslaCrypt 及 Locky 都是勒索軟體，其中 Locky 曾經在 2016 年 2 月出現。勒索軟體是 2016 年網路安全的主要議題之一。

賽門鐵克每月收集的遙測資料顯示，電子郵件惡意程式在 2016 年初強勢出擊，在 4 月及 6 月則大幅下滑，當時 Locky、Dridex 及其他軟體的活動也減少。



### 電子郵件惡意程式每月比例

電子郵件惡意程式每月比例在 4 月及 6 月大幅下滑，可能與執法單位採取行動，對抗多個網路犯罪團體有關。



賽門鐵克認為這次活動下降，可能與執法單位採取行動有關，其中 6 月的活動下降，是在俄羅斯逮捕涉及 [Lurk 銀行交易詐騙團體](#) 的 50 人之後。

不過攻擊下降只是暫時，惡意程式垃圾郵件攻擊之後再次迅速擴展。牽涉 Dridex 及 Locky 的攻擊恢復，而 Kovter 系列威脅 ([Trojan.Kovter](#)) 資安事端於八月開始出現，一直到年底都維持成長。如需更多大量郵件勒索軟體攻擊的詳細資料，請參閱「[勒索軟體](#)」一章。

### 各產業電子郵件惡意程式比例

批發交易和農業是 2016 年最受電子郵件威脅影響的產業部門。

行業	電子郵件惡意程式比例 (每幾封電子郵件中出現一封)
無法分類的機構	103
農、林、漁業	111
批發業	111
服務業	121
製造業	130
零售業	135
採礦業	139
公共行政	141
運輸及公用事業	176
建築業	179
金融、保險及不動產業	182

2016 年每個產業的電子郵件惡意程式都上升，只有零售交易例外，其電子郵件惡意程式比例下降 (2015 年為每 74 封電子郵件就有一封，2016 年為每 135 封電子郵件就有一封)。增加幅度最高的產業為運輸 (比例從 1/338 封電子郵件升至 1/176)、金融 (比例從 1/310 封電子郵件升至 1/182) 以及礦業 (比例從 1/304 封電子郵件升至 1/139)。醫療保健服務則是從每 396 封電子郵件就有一封，躍升為每 204 封電子郵件就有一封。

電子郵件惡意程式在 2016 年襲擊所有規模的企業。不過根據我們的數據，最受影響的是中小企業 (251 至 500 名員工的公司)。

### 各規模企業的電子郵件惡意程式比例

電子郵件流量中惡意程式比例最高的，是公司規模在 251 - 500 名員工的組織，其中收到含有惡意程式的電子郵件比例為每 95 封電子郵件就有一封。

公司規模	電子郵件惡意程式比例 (每幾封電子郵件中出現一封)
1-250	127
251-500	95
501-1000	139
1001-1500	224
1501-2500	104
2501+	170

### 網路釣魚

過去幾年來，網路釣魚比例呈現下滑，並於 2016 年再次下降，由每 1,846 封電子郵件就有一封，減少至每 2,596 封電子郵件就有一封。

### 網路釣魚整體比例

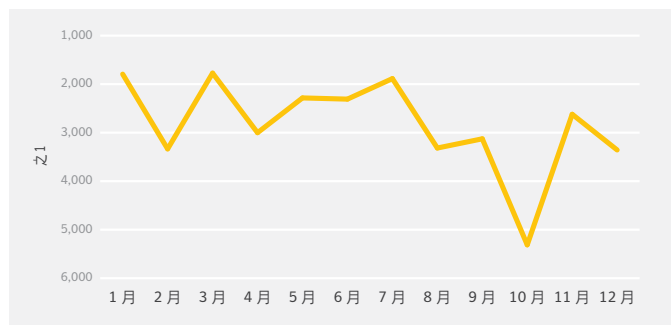
2014	2015	2016
每 965 封就有一封	每 1846 封就有一封	每 2596 封就有一封

10 月出現明顯下滑，網路釣魚比例只有 1/5,313 封電子郵件，不過 11 月則回到較為「一般」的數據，比例達到 1/2,621 封電子郵件。

10 月對資訊安全領域而言可說是多事之秋，其中包括 [Mirai 傀儡網路](#) 更加鞏固地位，針對 DNS 供應商 Dyn 採取分散式阻斷服務攻擊 (DDoS)，影響 Spotify、Netflix 及 PayPal 等眾多知名網站。此外也有報告指出 Kovter ([Trojan.Kovter](#)) 系列威脅的相關活動增加。不過並沒有明確的單一理由，能夠說明網路釣魚比例為何在該月大幅下滑。

### 網路釣魚每月比例

網路釣魚每月比例數據顯示 10 月明顯下滑，不過並沒有明確的單一理由，能夠說明該月大幅下滑的情形。



其中可能有各種原因造成網路釣魚活動減少。消費者的警覺性日漸提升，瞭解點擊不明連結或下載可疑附件的危險性，因此「標準」的無差別大量郵件網路釣魚攻擊，對詐騙者的效果每況愈下。

### 各產業網路釣魚比例

2016 年最受網路釣魚影響的產業部門為農業，每 1,815 封電子郵件就有一封嘗試進行網路釣魚。

行業	網路釣魚比例 (每幾封電子郵件中出現一封)
農、林、漁業	1815
金融、保險及不動產業	1918
採礦業	2254
公共行政	2329
零售業	2419
無法分類的機構	2498
服務業	3091
製造業	3171
批發業	4742
建築業	4917
運輸及公用事業	6176

### 各規模企業的網路釣魚比例

網路釣魚發生率最高的，是公司規模在 251 - 500 名員工的組織，其中收到嘗試網路釣魚的電子郵件比例為 1/2,554。

公司規模	網路釣魚比例 (每幾封電子郵件中出現一封)
1-250	2897
251-500	2554
501-1000	4023
1001-1500	6640
1501-2500	2610
2501+	3323

不過，魚叉式網路釣魚仍然持續成長。2016 年出現許多知名個案，例如柯林頓希拉蕊競選總幹事 John Podesta 及前美國國務卿 Colin Powell 電子郵件遭駭，其中使用的就是魚叉式網路釣魚電子郵件。

### BEC 詐騙

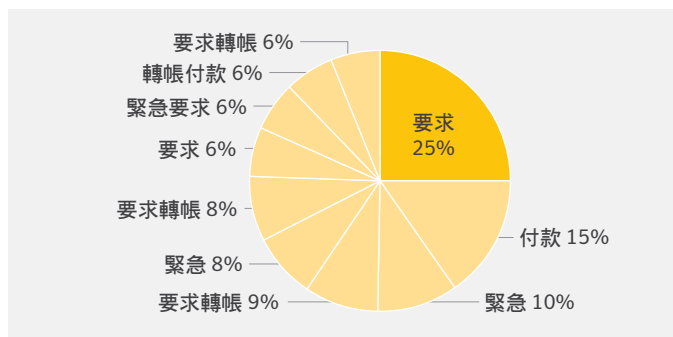
BEC 詐騙仰賴魚叉式網路釣魚電子郵件，在 2016 年的地位更加鞏固。BEC 詐騙也稱為 CEO 詐騙或「網路捕鯨」(whaling)，是一種低層級技術的金融詐騙，其中詐騙者將詐騙電子郵件傳送至金融人員，謊稱自己是執行長或資深管理階層，然後會要求轉帳大量金錢。這類詐騙可能造成重大傷害，因為其中需要的技術專業非常少，但是罪犯可獲得豐厚的金錢，而牽涉其中的公司則遭受重大損失。例如 2016 年初一家奧地利航太公司，在受到 BEC 詐騙者詐取 5 千萬美元後，解聘了公司執行長。

**賽門鐵克研究** 2016 年上半年，發現每天有 400 家以上企業遭到 BEC 詐騙鎖定，其中最主要的目標是中小企業。FBI 預估過去三年 BEC 詐騙造成 30 億美元以上的損失，全球受害者超過 22,000 個以上。

賽門鐵克研究發現，這類詐騙是由知名的奈及利亞 419 詐騙演化而來；賽門鐵克分析的電子郵件地址之中，有一半以上具有奈及利亞 IP 位址。電子郵件於週一至週五傳送，遵循標準的一週工作時間，通常包含無害的主旨行內容，出現「要求」、「付款」及「緊急」等字眼。

## BEC 詐騙：常見主旨行

BEC 詐騙電子郵件主旨行最常使用的關鍵字是「要求」，之後則是「付款」(15%) 和「緊急」(10%)。



BEC 詐騙者技術持續演進發展，以確保詐騙成功。賽門鐵克在 11 月的研究發現，詐騙者並不是立即要求轉帳，而是使用日常口語確認受害者是否在座位上，於要求現金之前找出更多資訊。

我們研究人員最近發現的新技術，是「劫持」公司傳送的合法發票，並將帳戶號碼變更為詐騙者的帳戶號碼。有些情況則是詐騙者攻擊電子郵件伺服器，變更發票上的詳細資料。其他則只是傳送假造的發票電子郵件，不需要駭入電子郵件伺服器，只要在合法發票之前傳送，就可能發揮效果。

由於 BEC 詐騙一本萬利，2017 年仍可能延續其強大趨勢。

### 垃圾郵件維持穩定

垃圾郵件比例在近幾年下滑後，於 2016 年維持穩定，達到 53%。

不過，這項數據並不表示 2016 年大部分的入埠商務電子郵件都是垃圾郵件。一般所謂的垃圾郵件，是指大批傳送未經收信人許可的電子郵件，部分情況下其中並沒有惡意威脅。垃圾郵件可能只是令人厭煩或非必要，或是可能連往執行點擊詐騙的網站。

### 垃圾郵件整體比例

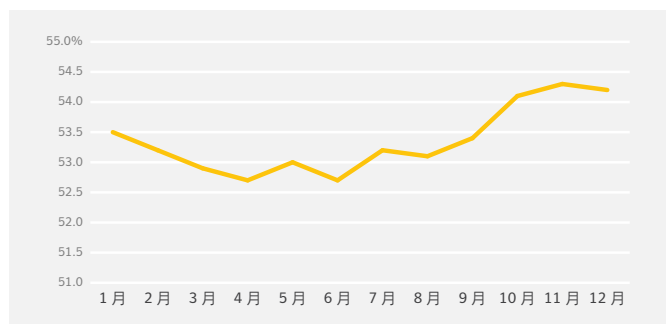
2015 及 2016 年之間的垃圾郵件比例維持穩定。

2014	2015	2016
60%	53%	53%

垃圾郵件在 2015 年跌至 2003 年以來的最低水準，並於 2016 年持續偏低。其中可能的影響因素，包括前述勒索軟體的成長，以及出現更多鎖定目標的魚叉式網路釣魚攻擊 (例如 BEC 詐騙)。以上攻擊的獲利能力，可能會讓攻擊者放棄舊式的垃圾郵件，轉為採用各種新方法。

### 垃圾郵件每月比例

垃圾郵件比例到了 2016 年底微幅上升。11 月的垃圾郵件比例達到 54.3%，是自 2015 年 3 月以來的最高比例。



雖然整體垃圾郵件比例維持停滯，不過 2016 年最後一季傳送的垃圾郵件數量達到高峰。11 月的垃圾郵件比例達到 54.3%，是自 2015 年 3 月以來的最高比例。

影響比例上升的因素有兩項。11 月初舉行的美國總統大選，造成選舉相關垃圾郵件達到高峰。賽門鐵克在 9 月中至 10 月中旬間，幾乎封鎖將近與總統選舉有關的 800 萬封電子郵件。

10 月也發生兩起重大攻擊，影響賽門鐵克客戶。於西班牙開始的成人主題垃圾郵件攻擊，影響 EMEA 地區的使用者，以多種不同歐洲語言迅速傳播。第二項攻擊則是重大的雪靴 (snowshoe) 攻擊 (請參閱「冰天雪地」章節)，傳送有關垃圾郵件產品及服務的電子郵件。攻擊者傳送少量電子郵件刺探偵測，如果訊息遭到封鎖，會在幾分鐘內中止垃圾郵件執行。

黑色星期五及網路星期一的相關垃圾郵件，也在 11 月大量出現，其中一項攻擊用於傳播 Locky 勒索軟體。12 月據報所謂的電暴 (hailstorm) 垃圾郵件技術用於散播 Dridex 及 Locky，不過垃圾郵件比例維持穩定。

垃圾郵件作者在選擇目標的公司規模時，似乎是採取無差別原則。最常遭到鎖定的小型企業，以及最少遭到鎖定的大型企業之間，差異僅略高於 1%。

### 各規模企業的垃圾郵件比例

最常及最少遭到鎖定的公司規模之間差異不大，垃圾郵件比例介於 52.6% 及 54.2% 之間。

公司規模	垃圾郵件比例 (%)
1-250	54.2
251-500	53.1
501-1000	53.4
1001-1500	53.2
1501-2500	52.6
2501+	52.8

### 各產業垃圾郵件比例

某些產業會收到比其他人的垃圾郵件，但大約只多 8% 左右。

行業	Spam Rate (%)
建築業	59.5
採礦業	57.1
零售業	54.9
製造業	54.4
農、林、漁業	54.0
無法分類的機構	53.0
服務業	53.0
金融、保險及不動產業	52.9
運輸及公用事業	52.9
批發業	52.6
公共行政	51.6

### 個案研究/調查

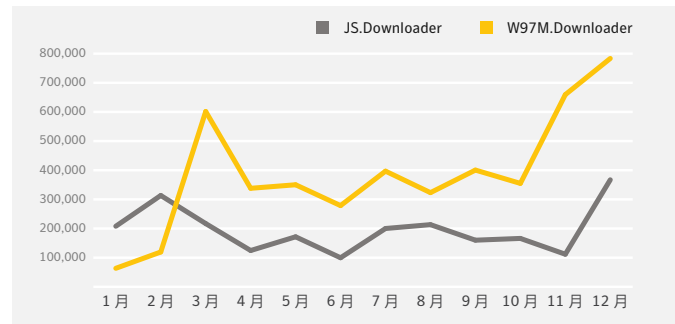
參與大量郵件攻擊的團體，持續精進戰術，以便讓自己能夠領先電子郵件安全系統。

#### 改變戰術

2016 年值得注意的趨勢，就是下載程式的類型改變，傳遞部分最前科累累的威脅。含有惡意巨集的 Office 文件 (W97M.Downloader 及變種) 在年初是最熱門的下載程式，用於傳遞 Dridex (W32.Cridex) 等各種威脅。2016 年三月期間開始出現轉變，使用 JavaScript 下載程式 (JS.Downloader 及變種) 的情形大幅增加。

### 每月偵測到的下載程式數量

Office 巨集下載程式 (W97M.Downloader 及變種) 和 JavaScript 下載程式 (JS.Downloader 及變種)，是最常用的下載程式，能夠透過電子郵件散播惡意程式。JavaScript 下載程式活動在 2016 年增加，Office 巨集則在 2016 年 12 月復甦。



賽門鐵克認為，使用 JavaScript 和 Office 巨集的濫發垃圾郵件行動，是不同的網路犯罪團體所為。惡意程式團體可聘任一(或兩者) 通路傳遞威脅。如果這是事實，那就會看到 2016 年底的這種趨勢，透過 JavaScript 下載程式從事濫發垃圾郵件行動的惡意程式團體較多。

雖然 Office 巨集下載程式的傳播情形，在一整年都維持偏低情形，賽門鐵克並不認為這種媒介將消聲匿跡。事實上，我們可以發現 W97M.Downloader 偵測數量在 12 月達到高峰，不過 JS.Downloader 仍持續居於主導地位。此高峰可能歸因於前述用於散播 Locky 及 Dridex 的電暴 (hailstorm) 攻擊 (請參閱「冰天雪地」章節)，可能是透過 Word 文件的惡意巨集傳播。

#### 冰天雪地：雪靴 (snowshoe) 和電暴 (hailstorm) 技術

雪靴 (snowshoe) 濫發垃圾郵件行動，在一系列 IP 位址散佈各種垃圾郵件，以提升入侵機會。雪靴垃圾郵件作者預期，垃圾郵件過濾器將會攔截部分電子郵件。不過這種由大量 IP 位址傳送電子郵件的技術，可增加垃圾郵件規避過濾器的機會，到達電腦使用者的收件匣。雪靴垃圾郵件作者由每個 IP 位址傳送少量垃圾郵件，以躲避偵測。

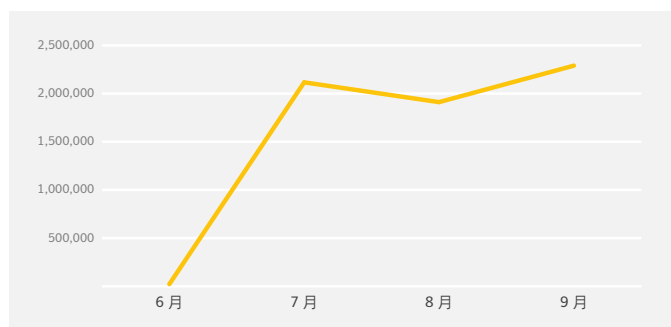
電暴 (hailstorm) 垃圾郵件技術是由雪靴演進發展而來，兩者都已存在多年。電暴垃圾郵件也是使用大量寄件者 IP 位址傳送，不過電暴活動是在非常短的時間內，傳送非常大量的垃圾郵件。電暴垃圾郵件作者能夠快速傳送數千封電子郵件，然後突然停止。部分電暴垃圾郵件攻擊在相當短的時間內進行，就算是面對最快速的傳統防垃圾郵件防禦措施，活動在其更新回應前早已結束。

在轉向 JavaScript 下載程式的過程中，賽門鐵克發現自 7 月開始，使用惡意 Windows 程序檔檔案 (WSF) 附件 (偵測為 JS.Downloader) 的情形大幅增加。WSF 檔案可讓單一檔案之中混合多種程序檔指令語言，並由 Windows Script Host (WSH) 開啟及執行。這類檔案做為惡意附件，可能是因為檔案副檔名為 .wsf，不會遭到部分電子郵件用戶端自動封鎖，並可像可執行檔一樣執行。

特別是勒索軟體，已經利用這種新戰術散佈。賽門鐵克在 2016 年下半年，封鎖一系列散佈 Locky (Ransom.Locky) 的主要攻擊，其中牽涉惡意的 WSF 檔案。

#### 含有 WSF 附件的遭封鎖電子郵件

含惡意 WSF 附件電子郵件遭到封鎖的數量，在 2016 年 7 月及 9 月之間大幅增加。



#### 久經考驗的社交工程

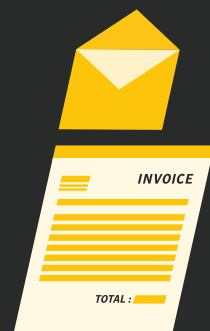
雖然垃圾郵件攻擊仰賴多種戰術散佈惡意程式，最大規模的惡意程式濫發垃圾郵件行動，傾向仰賴社交工程技術。像是 Locky 勒索軟體或 Dridex 金融木馬程式等威脅，可能透過偽裝為金融交易確認的電子郵件散佈。

賽門鐵克分析 2016 年記錄的 623 起重大惡意程式垃圾郵件攻擊後，發現「發票」是主旨行最常使用的關鍵字。「訂單」、「付款」及「帳單」等財務詞彙也名列前十名。

惡意程式垃圾郵件在這一整年期間，一直使用各種財務關鍵字，顯示攻擊者運用這類戰術相當成功。由於大部分企業會由客戶及供應商收到大量例行的正當電子郵件，如果沒有使用電子郵件安全性軟體加以封鎖，就很難避免開啟惡意電子郵件。同時消費者也可能受騙開啟這類電子郵件，因為消費者會擔心自己要為並未訂購的產品付款。

## 一般的電子郵件惡意程式感染程序

01 接收的電子郵件偽裝為例行通知，最常見的是**發票或收據**



02 包括附件(通常為 JavaScript 檔案)，或含有惡意巨集的 Office 檔案



03 開啟附件會執行 PowerShell 程序檔下載惡意程式

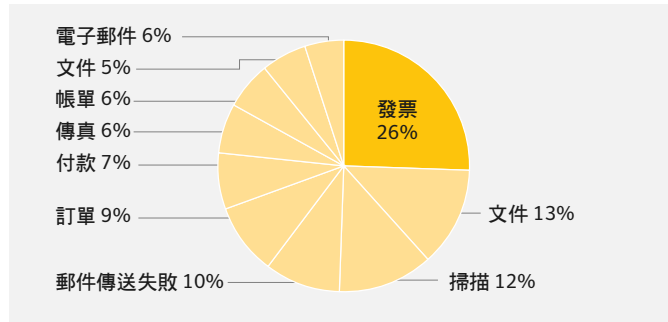


04 惡意程式下載通常為勒索軟體



## 惡意程式垃圾郵件攻擊所用關鍵字

2016 年主要惡意程式垃圾郵件攻擊的十大主旨行關鍵字。

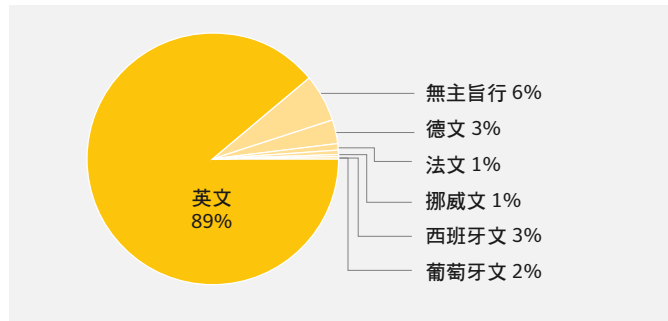


另一項常見戰術，就是將電子郵件偽裝為源自掃描器、印表機或多功能裝置 (MFD)。含有「掃描」、「文件」及「傳真」等關鍵字的電子郵件，通常會偽裝為來自這類裝置。

2016 年出現的第三種戰術，就是將惡意程式垃圾郵件攻擊，偽裝為電子郵件遞送失敗訊息。接受分析的主要垃圾郵件攻擊之中，有 10% 在主旨行使用遞送失敗訊息。

## 垃圾郵件攻擊偏好使用的語言

2016 年主要惡意程式垃圾郵件攻擊於主旨行使用的語言



接受分析的主要惡意程式垃圾郵件攻擊中，絕大部分 (89%) 都在主旨行使用英語。德語遠遠落後位居第二 (3%)，此外還有少部分的法語、挪威語、葡萄牙語及西班牙語電子郵件。有趣的是，不論語言為何，攻擊者都採取類似戰術，許多非英語攻擊也採用金融主題。例如德語攻擊最熱門的關鍵字是「Rechnung」，也就是德語的發票。

## 社交工程及新型傳訊平台

隨著企業及消費者移往傳統電子郵件以外的新型傳訊平台，攻擊者將可能尋求利用這類平台從事惡意用途。

越來越多企業使用協同合作工具 (例如 Slack)，進行內部通訊以及與客戶互動。WeChat 在中國的傳訊領域居於主導地位，提供各式各樣的廣泛功能，包括付款系統。只要有金融交易，網路罪犯就會如影隨形。WeChat 可能將做為其他傳訊應用程式的典範。Facebook Messenger 已經更著重於使用自動化軟體機器人，讓品牌能夠加入使用者的對話之中。

雖然一般惡意電子郵件使用的部份技術，並無法轉移至其他傳訊平台，但電子郵件攻擊的根源就是使用社交工程。各界從成功電子郵件詐騙及攻擊之中所學到的教訓，可能將應用在傳訊平台，因為這類平台受到企業及消費者採用的情形日漸廣泛。

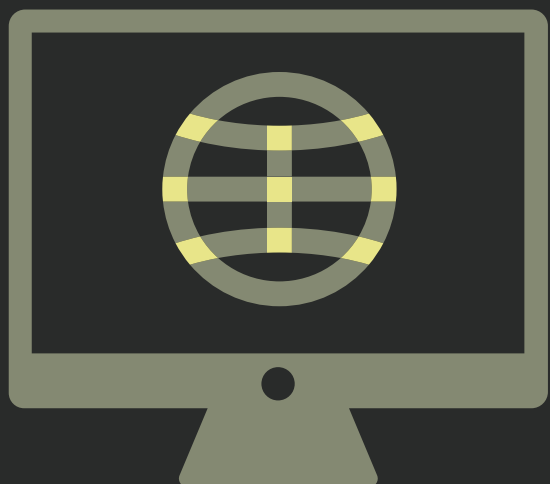
## 延伸閱讀

- [Dridex：金融木馬程式每日透過數百萬封垃圾郵件積極散佈](#)
- [Locky 勒索軟體積極尋找受害者](#)
- [Locky、Dridex 及 Angler 等網路犯罪團體活動減少](#)
- [使用惡意 WSF 附件的電子郵件攻擊興起](#)
- [Necurs：大量郵寄傀儡網路以新一波的垃圾郵件攻擊回歸](#)

### 最佳實務準則

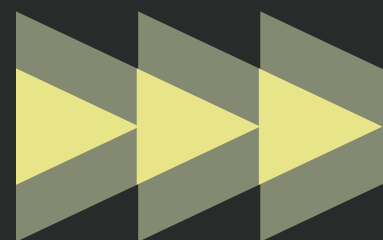
- 完整的防護架構可協助您抵禦這類電子郵件威脅。[Symantec Email Security.cloud](#) 可封鎖源自電子郵件的威脅，而 [Symantec Endpoint Protection](#) 則可封鎖端點上的惡意程式。
- 刪除任何可疑的電子郵件，尤其是含有連結或附加檔案的郵件。
- 如果有任何 Microsoft Office 電子郵件附件建議您啟用巨集以檢視信件內容，請務必小心。除非您十分確信此封信件是真的，並且來源可靠，否則請不要啟用巨集，並馬上刪除信件。
- 隨時確保您的安全軟體為最新版本，以便協助您抵禦任何最新變種惡意程式的威脅。
- 時常更新您的作業系統和其他軟體。軟體更新經常含有新發現安全漏洞的修補程式，而且這些漏洞可能為攻擊者所利用。
- 若電子郵件未依慣常程序要求您執行動作，務必保持警覺。
- 撰寫回信時，直接由企業通訊錄選取寄件者的電子郵件，而不是僅按下回信按鈕，以確保將詐騙者移除在往來的電子郵件外。
- 請勿回覆可疑的電子郵件，並且不要提供敏感資訊。
- 向適當的管理單位舉報可疑或明顯造假的電子郵件。
- 針對所有員工實施有效的密碼政策，確保密碼強度足夠，並定期更換。
- 絕對不要使用電子郵件內的連結連往網站，除非您確定連結沒有問題。直接在網址列輸入 URL 網址，確保連往正當網站，而不是網址類似的網站。

# 網路攻擊、工具組以及 刺探攻擊線上漏洞



章節

# 05





## 簡介

2016 年網路安全情勢發生明顯變化，網路攻擊數量比去年同期下降將近 1/3。其中攻擊者不再使用刺探攻擊套件作為主要感染向量，轉為使用電子郵件作為偏好的威脅遞送方式。這與 2015 年截然不同，當時網路攻擊數量是前一年的兩倍。

不過，由刺探攻擊套件轉向電子郵件的作法，可能不會永遠如此。攻擊者會定期在這兩者之間切換，並如此持續下去。

## 重要發現

- 網路攻擊數量比去年同期下降 1/3 (32%)。不過網路攻擊仍然是一大問題，2016 年平均每天遭到偵測的次數高達 22.9 萬次。2016 年網站經掃描後，有 3/4 以上 (76%) 含有漏洞，其中 9% 為重大漏洞。
- 2016 年刺探攻擊套件的惡意活動下降 60%，我們的研究指出，攻擊者現偏好以電子郵件作為主要感染向量。刺探攻擊套件活動大幅下滑，這並不一定代表攻擊者的威脅減少，而是攻擊者使用不同方法散佈威脅。
- RIG 是 2016 年底最活躍的刺探攻擊套件，佔 12 月所有網路攻擊的 35%，主要散佈 [Ransom.Cerber](#)。
- 2016 年平均每天發現 2.4 個瀏覽器漏洞，略低於 2015 年的每日平均 3 個。

## 趨勢及分析

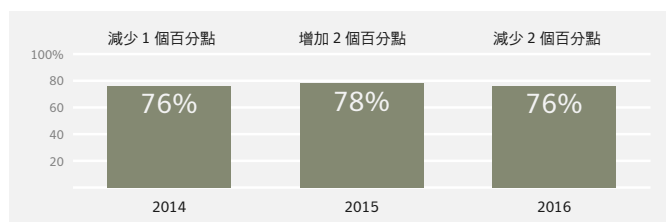
雖然網路攻擊和刺探攻擊套件數據下降，但經掃描發現漏洞的網站比例，仍然和過去幾年一樣偏高。

### 漏洞評估

我們的資料發現，經掃描發現漏洞的網站比例為 76%，這項數據與 2014 年相同，只比 2015 年降低 2%。

### 經掃描發現漏洞的網站

2016 年經掃描發現漏洞的網站比例為 76%，比 2015 年降低 2%。

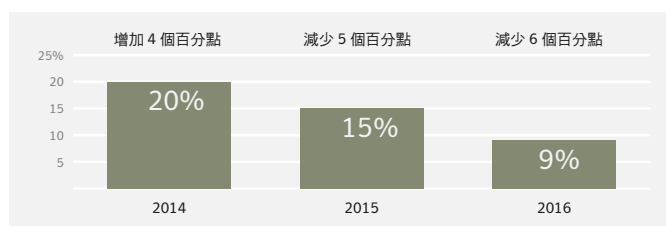


重大漏洞比去年同期降低 6%。經掃描發現重大漏洞的網站比例為 9%，低於 2014 年的 20% 及 2015 年的 15%，顯示具有重大漏洞的網站數量，呈現穩定下滑的趨勢。

重大漏洞是指，如果遭到攻擊者刺探攻擊，可能會在沒有使用者互動的情況下，就讓惡意程式碼成功執行，可能導致資料外洩，並進一步侵害受影響網站的訪客。

### 重大漏洞比例

過去三年來重大漏洞比例穩定下滑，目前為 9%。



### 刺探攻擊套件

2016 年網路威脅的最大重點，無疑是刺探攻擊套件活動顯著下滑。偵測到的刺探攻擊套件數量下降 60%，其中有一些最主要的刺探攻擊套件系列，在這一時期消聲匿跡。

偵測到的刺探攻擊套件數量降低有幾個原因。如同前述內容，以及在「[電子郵件：惡意程式、垃圾郵件及網路釣魚](#)」章節深入探討的部分，我們的資料顯示，電子郵件在 2016 年成為攻擊者偏好的感染向量。電子郵件惡意程式比例在 2016 年增加，從每 220 封電子郵件就有一封含有惡意程式，成長為每 131 封就有一封。

我們的逐月資料分析顯示，許多刺探攻擊套件也在這一年期間消聲匿跡。

2016 年偵測到的刺探攻擊套件中，比例最高的和 2015 年一樣，都屬於未分類。此類別是由許多不同、小型及不相關的刺探攻擊套件組成，且都不屬於已知攻擊套件的系列。

Angler 刺探攻擊套件持續成為 2016 年偵測次數最多的系列，於上半年居於主導地位，在五月佔所有刺探攻擊套件活動的一半以上。不過 Angler 活動在六月下滑將近 30%，並持續探底，到年底時幾乎已不存在。

Angler 活動急遽減少，與俄羅斯逮捕涉及 [Lurk 銀行交易詐騙團體](#) 的 50 人同時發生，一般推測這項破獲行動，導致這款曾經盛行的刺探攻擊套件消失。如需更多詳細資訊，請參閱 [本章稍後提出的個案研究](#)。

Angler 消聲匿跡後，Neutrino 刺探攻擊套件活動在接下來幾個月達到高峰，並在 Angler 活動減少後，Neutrino 活動立即於六月增加 10%。不過到了年底，Neutrino 活動程度大致與年初時相同。

2016 年大量減少的另外兩種工具組是 Nuclear 及 Spartan。一般認為 Nuclear 刺探攻擊套件遭到曝光，揭露其運作方式，導致其消聲匿跡。至於 Spartan 消失的原因，似乎只是因為幕後罪犯決定要讓此刺探攻擊套件「退休」。賽門鐵克遙測顯示，Spartan 在 2016 年 3 月底之前都非常活躍，因此能夠躋身年度前十名，但其實自此之後就消聲匿跡。

許多知名刺探攻擊套件消失，代表已不再是攻擊者可依賴的選項。網路罪犯可能不希望購買「刺探攻擊套件即服務」，以免還要擔心流通一個月之後就消失無蹤。

RIG 刺探攻擊套件活動在最後一季上升，可能與許多其他知名套件系列消失有關。RIG 刺探攻擊套件是 2016 年底最活躍的套件，佔 12 月所有攻擊的 35%。這些攻擊主要散佈 [Ransom.Cerber](#) 勒索軟體。

### 十大刺探攻擊套件

Angler 刺探攻擊套件是 2016 年最常使用的手法，佔所有刺探攻擊套件網路攻擊的 22%。不過 Angler 活動在六月下滑將近 30%，並持續探底，到年底時幾乎已不存在。RIG 刺探攻擊套件是 2016 年底最活躍的套件，佔 12 月所有攻擊的 35%。

排行	刺探攻擊套件	2015 年 (%)	2016 年 (%)	百分點差異
1	未分類	38.9	37.9	-1.0
2	Angler	13.3	22.2	8.9
3	Spartan	7.3	11.9	4.6
4	RIG	2.0	7.9	5.9
5	Magnitude	1.1	5.8	4.7
6	Neutrino	1.3	5.8	4.5
7	VIP	24.8	3.2	-21.6
8	Nuclear	4.0	1.6	-2.4
9	Fiesta	2.5	1.0	-1.5
10	G01 Pack	2.2	0.8	-1.4

## 網路攻擊

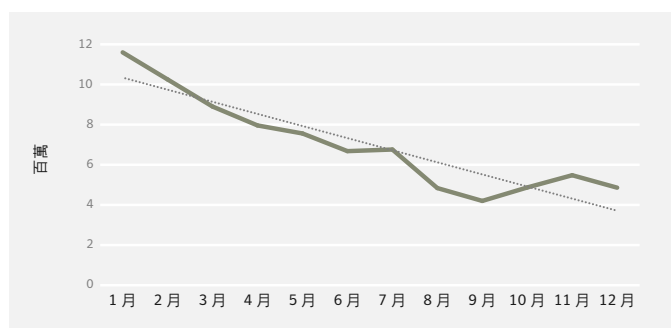
整體而言，在 2015 及 2016 年之間，網路攻擊數量下降超過 30%，原因可能是攻擊者改用電子郵件，作為主要的感染向量。如前所述，電子郵件可讓攻擊者更輕易散佈惡意程式，而且在目前的趨勢情況下，也比較穩定可靠。刺探攻擊套件需要維護後端基礎架構，而且攻擊者的工作量比傳送電子郵件還大。

但重點是，這並不代表威脅減緩，而是攻擊者選擇不同戰術來散佈威脅。

賽門鐵克遙測顯示，網路威脅在 2016 年的 12 個月內幾乎是連續下滑，在 9 月達到最低點，10 月及 11 月微幅上升，然後 12 月再次下滑。

## 每月攔截的網路攻擊

2016 年期間，每個單一系統受到的網路攻擊數穩定下滑。



雖然網路威脅活動整體呈現下滑，但仍是主要威脅，賽門鐵克 2016 年在端點電腦每天平均攔截 22.9 萬次以上的單一網路攻擊。Blue Coat Web Gateway 產品於網路層級運作，其資料顯示到了 2016 年底，攔截的網路威脅數量，比 2015 年同期上升 24%。不過相較於 2014 年至 2015 年成長 124%，這樣的增加比例是下滑的。

2016 年最常遭到刺探攻擊的網站類別，就是科技與商業相關網站。科技網站遭到刺探攻擊的次數，幾乎是商業相關網站的兩倍。搜尋網站是 2015 年最常遭到刺探攻擊的第三名，在 2016 年則掉出前十名外。

## 最常遭刺探攻擊的網站分類

2016 年科技與商業相關網站，最常被裝載惡意內容及惡意廣告。

排行	網域類別	2015 年 (%)	2016 年 (%)	百分點差異
1	科技	23.2	20.7	-2.5
2	商務	8.1	11.3	3.2
3	部落格	7.0	8.6	1.6
4	託管	0.6	7.2	6.6
5	健康	1.9	5.7	3.8
6	購物	2.4	4.2	1.8
7	教育	4.0	4.1	< 0.1
8	娛樂	2.6	4.0	1.4
9	旅遊	1.5	3.6	2.1
10	博弈業	0.6	2.8	2.2

## 瀏覽器漏洞

2016 年平均每天發現 2.4 個瀏覽器漏洞。公開宣布漏洞數量下滑的瀏覽器中，Microsoft Internet Explorer/Edge 的漏洞數量減少最多。這可能是因為 2016 年沒有推出新版 Explorer，且 Microsoft 基本上已經停止開發這款瀏覽器。Explorer 瀏覽器的使用情形也直線下滑。Microsoft 的新型瀏覽器 Edge 僅提供給 Windows 10 的使用戶，其全新安全架構讓人難以進行刺探攻擊。

Firefox 及 Safari 的漏洞數量也下滑，而賽門鐵克發現 Google Chrome 漏洞數量微幅上升。不過 2015 年發現的瀏覽器漏洞數量異常偏高，部分原因可能是該年發現大量的零時差漏洞。2016 年的瀏覽器漏洞數據，只是回到接近「正常」水準，但仍然相當高。

## 案例研討

### Angler：刺探攻擊套件的興衰史

2013 年 Blackhole 刺探攻擊套件壽終正寢之後，Angler 刺探攻擊套件於 2013 年底首次現蹤於威脅情境。這款刺探攻擊套件立即受到歡迎，不過真正一飛沖天是在 2015 年，於當時主控了刺探攻擊套件領域。

Angler 是一款精密的刺探攻擊套件，是許多技術進展成果的先驅，引領其他刺探攻擊套件在後仿效，包括使用防網路安全的反制措施。Angler 能夠由記憶體下載並執行惡意程式，無需編寫任何檔案至磁碟，藉此規避傳統安全性技術的偵測。Angler 也能夠非常快速整合零時攻擊行為，因此在 2015 年變得更加熱門。2015 年發現了許多零時差漏洞，包括 Adobe Flash Player 的漏洞在內，都是 Angler 普遍鎖定的目標。

相較於其他刺探攻擊套件，Angler 的重大優勢之一，就是能夠略過許多傳統的安全性反制措施。其中使用多項技術規避偵測，包括迅速切換主機名稱及 IP 數字，此外也使用所謂的網域掩護 (domain shadowing) 技術，註冊看起來像是正當網站的網域名稱，寄生在正當網域之中。

Angler 是 2015 年最活躍的刺探攻擊套件。賽門鐵克入侵防護系統每日要封鎖數十萬次的 Angler 攻擊。光是 2015 年，Angler 攻擊遭封鎖總數就超過 1,950 萬次以上。Angler 主要的傳遞機制是惡意廣告，主要是刺探攻擊 Adobe Flash 的漏洞，最喜愛的目標是執行 Windows 作業系統的電腦，特別是 Window 7。

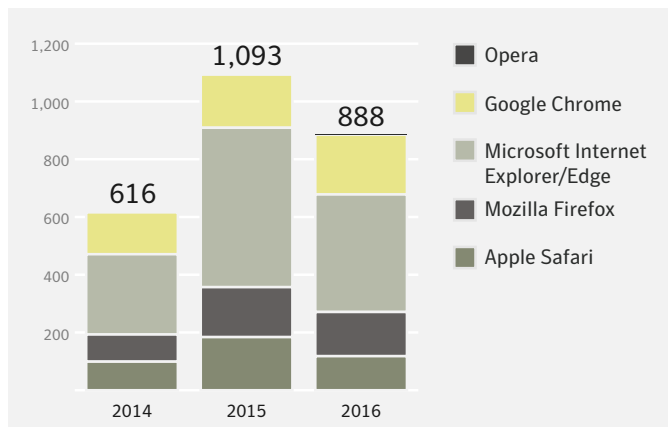
Angler 主要用於散佈勒索軟體。Angler 在 2016 年 6 月消失時，透過 Angler 散佈的 CryptXXX 勒索軟體 (Ransom.CryptXXX)，遭到偵測的數量也同時下滑。

Angler 在 2016 年初出現活動減少的情形，不過迅速再次向上攀升，直到 6 月完全消失。俄羅斯主管機關逮捕涉嫌 Lurk 銀行交易詐騙團體的 50 人之後，Angler 就消聲匿跡。各界普遍認為這項逮捕行動就是 Angler 消失的原因。

過去如此呼風喚雨的刺探攻擊套件消失，在市場上留下空缺，Neutrino 刺探攻擊套件活動順勢而起，暫時填補了這個空缺。網路罪犯絕對會在不久之後填補這個空缺。

## 瀏覽器漏洞

瀏覽器漏洞發現的數量，從 2015 年的 1,093 下降至 2016 年的 888。



瀏覽器漏洞數量下降的另一個可能原因，就是漏洞通報 (bug bounty) 計畫增加，其中有更多的安全研究人員參與，因此過去幾年已經找出並修補許多瀏覽器漏洞，讓惡意行動者過去曾經刺探攻擊的「簡易目標」不復存在。

## 延伸閱讀

[Locky、Dridex 及 Angler 等網路犯罪團體活動減少](#)

## 最佳實務準則

- 定期評估網站是否存在任何漏洞。
- 每日掃描網站是否存在惡意程式。
- 針對所有階段作業 Cookie 設定安全旗標。
- 維護網站安全，避免攔截式 (MITM) 攻擊和惡意程式感染。
- 選擇含有延伸驗證的 SSL 憑證，以驗證保護措施，並向網站使用者顯示綠色的瀏覽器位址列。
- 在網站極為明顯的位置顯示獲得認可的信任標示。
- 嚴格慎選外掛程式。用於管理網站的軟體也可能具有漏洞。使用的第三方軟體越多，攻擊表面就越大，所以請僅部署真正必要的項目。

# 網路犯罪及地下經濟



章節

# 06



## 簡介

2016 年新興網路犯罪的兩大面向。傳統大眾市場的網路犯罪集團，通常透過大規模的電子郵件活動，來散佈勒索軟體及線上銀行威脅等「現貨商品」惡意程式。雖然他們的動機與酬載大致相同，但散佈手法已由網頁式的刺探攻擊套件轉為較傳統的方式，特別是使用電子郵件附件。

網路犯罪的另一個面向，則是若干組織性的犯罪集團，犯下了多起精心策劃的金融竊盜。然而，不只專業罪犯會執行這類活動，也有證據顯示出國家等級人士的涉案跡象。

大眾市場及目標式網路犯罪集團，已經採取所謂的「自給自足」(living off the land) 戰術。這項趨勢將於「**目標式攻擊**」的章節深入探討，其中指出攻擊者透過作業系統及應用程式功能，搭配各種可公開取得的工具，來代替刺探攻擊漏洞及開發自訂工具等手法。

## 重要發現

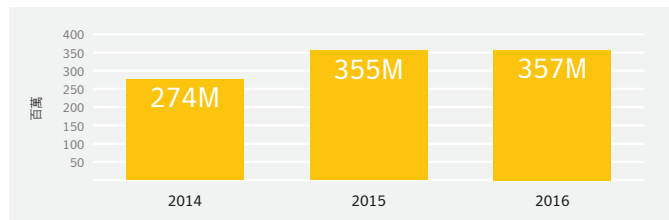
- 網路犯罪在 2016 年達到高峰，不但出現高知名度的受害者，盜取的金額也空前龐大。發生於 2016 年的 Banswift (Trojan.Banswift) 攻擊案，首次發現有國家涉入金融網路犯罪的顯著跡象。
- 即使各方努力打擊不肖行為，大眾市場網路犯罪仍然猖獗。攻擊者採用各種手法散佈傳統的網路犯罪惡意程式。其中，利用 Office 檔案的 JavaScript 和惡意巨集下載程式的方式特別泛濫，2016 年就出現超過 700 萬起意圖感染行動。
- 雖然 2016 年的資料外洩事件數量持平 (相較於 2015 年)，但遭竊身分數量則大幅攀升。2016 年有將近 11 億筆身分資料遭竊，遠高於 2015 年的 5 億 6,380 萬筆。
- 2016 年發現將近 1 億個 Bot 傀儡程式，較 2015 年增加 7%。

## 惡意程式

惡意程式仍然是各式威脅中的一大禍源，在 2016 年發現 3 億 5,700 萬以上的全新變種。不過在端點發現新惡意程式的比例，在 2016 年則首次呈現停滯，只增加 0.5%。

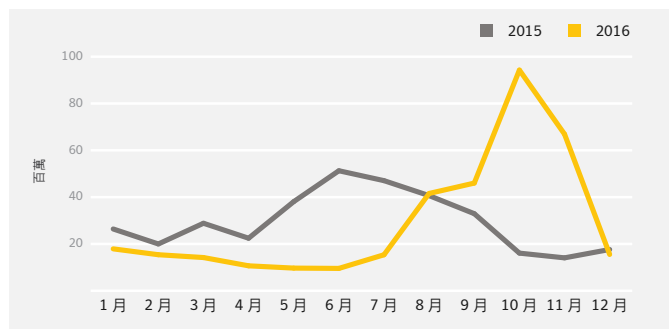
### 首次偵測到的獨特惡意程式變種

從 2015 年到 2016 年，首次偵測到的獨特惡意程式變種稍微增加 (0.5%)。



### 2016 年首見獨特惡意程式變種的每月統計數量

在這份 2016 年首見的獨特惡意程式變種逐月統計數據中，10 月出現明顯高峰。

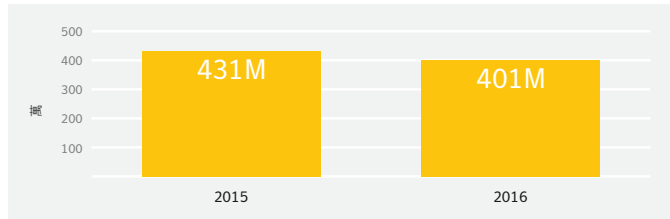


新型惡意程式變種的比例雖然在 2016 年初尚未增加，卻在下半年暴增。這主要是因為有大量的勒索軟體下載程式，由 Necurs (Backdoor.Necurs) 的傀儡網路透過電子郵件傳播，我們將在本章稍後深入討論細節。

賽門鐵克在之前的報告中，採用稍微不同的方式計算變種惡意程式數量，著重於當年度的獨特變種，而不是首見的惡意程式。如果使用舊有方式處理 2016 年資料，變種數量將稍微增加，但新變種比例則較上年同期降低 7%。

## 偵測到的獨特惡意程式變種

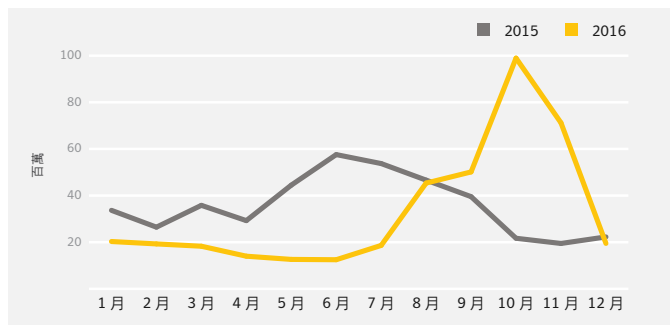
在 2015 及 2016 年間偵測到的獨特惡意程式變種數量稍微下降。



按月分析資料則發現幾乎相同的趨勢：變種數量在年底明顯上升。

## 2016 年獨特惡意程式變種的每月統計數量

獨特的惡意程式變種數量也在 10 月達到高峰。



如果單獨檢視此份資料，惡意程式問題似乎趨於穩定，甚至有所改善；不過如果綜觀全局，事實顯然並非如此。惡意程式數量的計算主要以最終或接近最終的酬載為主，但許多攻擊在攻擊鏈初期即遭封鎖，因此未計入這份數據中。我們在「[電子郵件](#)」的章節曾經提到，電子郵件是 2016 年傳播惡意程式的大宗媒介。賽門鐵克也持續攔截大量的網路攻擊。這些攻擊不會傳遞至最終酬載，因此降低了發現的變種總數。

另外一種說法是，變種威脅所造成的資安事端減少，攻擊者展開行動時，也不再那麼仰賴惡意程式。這種現象稱為「自給自足」(living off the land)。

**自給自足 (living off the land)：** PowerShell、巨集及社交工程 2016 年出現的趨勢，就是攻擊者使用合法的 Windows 程式，來下載並執行酬載。我們會在「[目標式攻擊](#)」的章節中詳細說明這種所謂的「自給自足」的戰術。不過，在網路犯罪的世界中，也發現了進階攻擊者會使用的手段。

PowerShell 是一種強大的程序檔指令語言及 Shell 架構，不但已成為感染鏈的主要傳遞方式，而且基於諸多理由，獲得了攻擊者的青睞。大部分 Windows 電腦都會預安裝 PowerShell，而多數組織並未對此啟用延伸記錄檔，因此無法察覺惡意 PowerShell 活動。程序檔也可輕易加以模糊，隱藏其惡意目的。如此可以直接從記憶體執行酬載，有利於攻擊者留下更少蛛絲馬跡。

賽門鐵克在 2016 年下旬進行分析，檢查 PowerShell 程序檔之後，發現其中 95.4% 具有惡意性質。惡意的 PowerShell 程序檔大多在初始感染階段期間作為下載程式使用，不過也可用來在網路中進行橫向移動。這種橫向移動一般發生於目標式攻擊，可讓威脅在網路內部散播的同時，還能於遠端電腦執行程式碼。在網路犯罪攻擊當中，PowerShell 則有利於促成下載，並執行最終酬載。

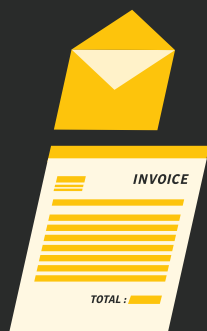
2016 年使用 PowerShell 的情形大幅增長。Blue Coat 惡意程式分析沙箱在 2016 年第三季所收到使用 PowerShell 的樣本數量，是第二季的 22 倍。這可能是因為在這段期間內，與 JavaScript 下載程式及 Trojan.Kotver 有關的活動有所增加。整體而言，我們的分析發現 PowerShell 最常搭配使用 W97M.Downloader (佔樣本 9.4%)，然後依序是 4.5% 的 Kovter (Trojan.Kotver) 及 JS.Downloader (4%)。Kovter 值得關注的原因，在於其使用 PowerShell 來產生無檔案型感染，且完全包含在登錄檔中。

2016 年也有更為進階的目標式網路犯罪集團利用了 PowerShell。[Odinaff 團體](#)使用惡意 PowerShell 程序檔攻擊金融機構。我們將在本章稍後探討這類攻擊。

惡意 Office 巨集持續成為攻擊者的熱門選擇，而證據就在於有越來越多這類活動被偵測到 (將於下文討論)。Office 巨集不會依據預設執行，所以這種攻擊必須仰賴社交工程，先說服使用者開啟 Office 附件，然後啟動巨集。使用 PowerShell 和巨集等功能的攻擊者，將無需刺探攻擊軟體漏洞或仰賴自訂工具，因為這兩者不但容易引起懷疑，也要耗費更多時間和技術來運用。

## 2016 年典型攻擊情境的發生步驟如下：

- 01** 攻擊者傳送電子郵件，通常會偽裝成發票或帳單



- 02** 電子郵件所帶有的附件，通常是 Office 檔案、JavaScript (JS) 或其他類型程序檔



- 03** 檔案啟動時，不是提示使用者執行巨集，就是啟動 PowerShell 下載及執行最終酬載



- 04** 最終酬載通常都是勒索軟體，不過也可能是 Dridex 等線上銀行威脅



此外，有些攻擊則並未仰賴任何惡意程式碼或系統功能。例如企業電子郵件入侵 (BEC) 攻擊 (我們會在「[電子郵件](#)」章節深入探討)，僅仰賴社交工程欺騙受害者，以詐取大筆金錢。

雖然這項趨勢顯示刺探攻擊及自訂工具等方式逐漸式微，不過值得注意的是，幾乎每項攻擊都含有惡意程式要素。這表示惡意程式仍是揮之不去的問題。此外，這項轉變並不代表攻擊者的手法不再縝密。事實上，這反倒顯示出他們效率提升，且有能力在眾目睽睽之下隱藏起來。

### 惡意程式的盛行程度及趨勢

2016 年在端點偵測到的最常見變種，主要都是透過變種偵測 (generic detection) 的方法所發現。

排行	偵測	感染數目
1	Heur.AdvML.B	5,648,434
2	JS.Downloader	3,487,119
3	Packed.Dromedan!Ink	2,615,857
4	W97M.Downloader	2,199,083
5	Heur.AdvML.C	2,039,212
6	SMG.Heur!cg1	1,291,550
7	W32.SillyFDC	1,019,644
8	Trojan.Startpage	908,429
9	W32.Downadup.B	814,687
10	Infostealer	753,783

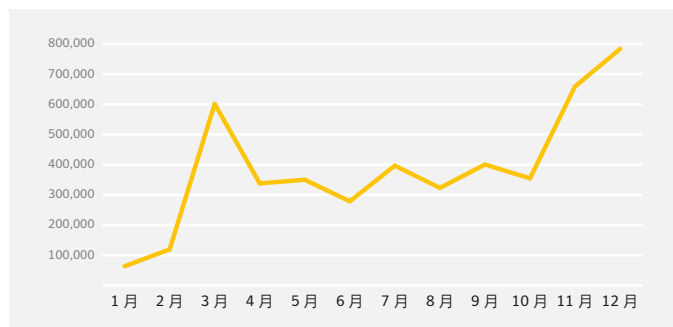
從盛行惡意程式的重點排名可以看出，變種或啟發式偵測技術的因應效果十分卓著。2016 年在端點偵測到的前十大惡意程式中，有九項是由這兩種方式所偵測。不過，要特別注意 JS.Downloader 及 W97M.Downloader 的崛起，兩者都是在 2016 年首次出現在盛行惡意程式的排行榜中。

賽門鐵克在 2016 年發現，大量電子郵件透過惡意 Office 巨集 (W97M.Downloader 及變種) 和 JavaScript 下載程式檔案 (JS.Downloader 及變種)，散佈勒索軟體及線上銀行威脅。兩者於 2016 年合計在端點被偵測到 700 萬件，成為最主要的網路犯罪威脅，情況在 2016 年下半年尤其嚴重。



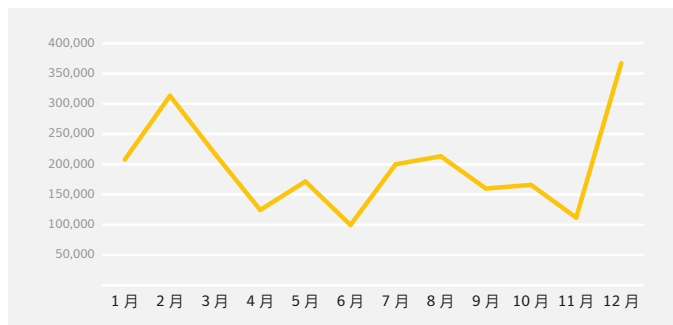
### 每月偵測到的 JavaScript 下載程式數量

JavaScript 下載程式偵測數量 (JS.Downloader 及變種) 在 2016 年下半年增加。



### 每月偵測到的 Office 巨集下載程式數量

Office 巨集偵測數量 (W97M.Downloader 及變種) 在 2016 年 12 月達到高峰。



這兩種下載程式基於諸多理由而深受攻擊者喜愛：企業不可能在電子郵件間道封鎖所有 Office 檔案，因為這樣會影響合法的電子郵件，而後者則導致 Office 巨集下載程式十分盛行。同時，由於可輕易混淆躲避偵測，JavaScript 下載程式的使用量也隨之增加。如前所述，JS.Downloader 通常使用 PowerShell 或 Visual Basic Script (VBS)，在嘗試躲避偵測的同時執行最終酬載。

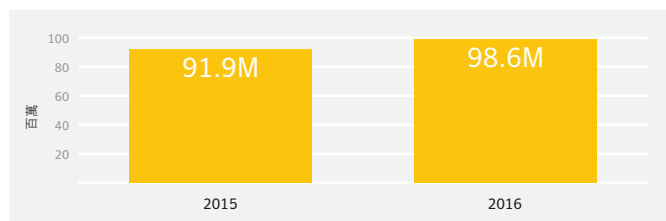
賽門鐵克研發中心指出部分團體偏好 W97M.Downloader，其他團體則偏好 JS.Downloader。W97M.Downloader 相關活動在 2016 年下半年減少，不過賽門鐵克認為，使用這種下載程式的集團可能會再度猖獗起來。事實上，在 2016 年的最後一個月，W97M.Downloader 的偵測數量就有所增加。

其中許多威脅的主要傳播管道，則是垃圾郵件傀儡網路。

賽門鐵克發現，Bot 傀儡程式在 2016 年的數量也有提升，從 9,190 萬增加到 9,860 萬個 Bot 傀儡程式，構成各種不同的傀儡網路。

### Bot 傀儡程式活動數量

賽門鐵克發現 2016 年的 Bot 傀儡程式數量，比 2015 年多出 6,700 萬個。



部分惡意程式採取進一步的預防措施，因而隱藏得更好。目前有 20% 的惡意程式，能夠定期偵測並識別虛擬機器環境，而這項比例高於 2015 年的 16%。

Blue Coat 的惡意程式分析沙箱追蹤發現，使用 SSL 通訊協定與指令和控制項 (C&C) 伺服器通訊的情形增加，因此更難以檢查網路流量。前述行為增加了 79%，在 2016 年底達到 3.1%。這可能是因為 SSL 憑證在 2016 年更容易取得，且攻擊者也發現：使用 SSL 加密更有利於通過閘道而不被偵測。此外，與雲端服務的通訊加倍成長，在 2016 年達到 4%。

所有威脅當中的 1% 使用了 Tor 網路，主要是由勒索軟體用來下達付款指示。

### 傀儡網路個案研究：Necurs

Necurs 傀儡網路是 2016 年主要的惡意程式散佈者之一，並透過大量電子郵件活動散佈 JavaScript、VBS 及 Office 巨集下載程式。Necurs 在 2016 年的主要酬載為 [Ransom.Locky](#)。由賽門鐵克所發現的其他主要傀儡網路，大多用來傳播 Dridex ([W32.Cridex](#))、Cerber ([Ransom.Cerber](#)) 及 Kotver ([Trojan.Kotver](#)) 和 Locky 等威脅。

Necurs 是 2016 年散佈惡意程式最活躍的傀儡網路之一。Necurs 的操作者固定在一般週間行動，並在週一至週五散佈威脅，週末則很少活動。

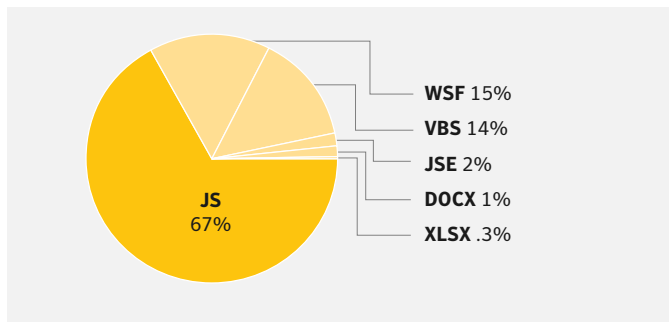
如果只檢視一天的 Necurs 活動，可發現明確的規模比例。在 2016 年 11 月 24 日，Necurs 發動了五場垃圾郵件攻擊，其中兩項傳遞 JavaScript 下載程式，另兩項傳遞 .wsf 附件，其餘一項則是 VBS 附件。這五場垃圾郵件攻擊傳送超過 230 萬封的垃圾郵件，其中超過 180 萬封使用 JS 下載程式，使用 VBS 的則不到 465,000 封。

賽門鐵克研究 2016 年最後一季 Necurs 執行的 146 次電子郵件攻擊，發現 Necurs 在每次電子郵件攻擊中，平均送出 525 個獨特惡意程式樣本。

研究團隊檢視了大多涉及 JS、VBS 及 WDF 下載程式的垃圾郵件後，發現 JavaScript 下載程式是 Necurs 所散佈最熱門的下載程式類型。

### 由 Necurs 垃圾郵件傀儡網路遞送的下載程式

在賽門鐵克觀察的期間，Necurs 發起的垃圾郵件攻擊大多涉及了 JS.Downloader。



10 月底開始研究 Necurs 時，威脅主要是透過 VBS 散佈，不過到了 11 月及 12 月，則是由 JavaScript 下載程式取得主導地位。

這種使用不同下載程式的方式，顯示 Necurs 是由不同的攻擊團體所使用的「雇用傀儡網路」。

有趣的是，賽門鐵克發現 Necurs 活動自 12 月底，消失了幾乎三個月的時間，最後一次垃圾郵件活動是在 12 月 22 日開始，於 12 月 24 日結束。我們起初認為，這可能只是 Necurs 幕後集團放假去了，不過這個傀儡網路直到 2017 年 3 月 20 日都沒有動靜。

Necurs 消聲匿跡，造成 2016 年底及 2017 年初的惡意電子郵件數量大幅下降，其消失的原因至今仍然成謎。賽門鐵克在 Necurs 恢復活動的 3 月 20 日，封鎖將近 200 萬封的惡意電子郵件。事實上，Necurs 恢復活動之後，就能恢復大量的垃圾郵件活動，顯示不論其消失的原因為何，並沒有喪失任何功能。

### 一切向錢看：金融惡意程式

金融惡意程式是專門鎖定線上銀行的威脅，一直以來都是網路犯罪的強大驅動因素。不過在幾次逮捕及破獲行動後，再加上勒索軟體持續成功，代表金融惡意程式的地位已經式微。

感染資料顯示有五大系列主宰此領域，因此五大系列以外的活動可忽略不計。

### 十大金融特洛伊木馬程式

從十大金融特洛伊木馬程式名單看來，2016 年的態勢是由少數金融特洛伊木馬程式所主宰。

排行	金融威脅	受影響的機器總數
1	Ramnit	460,673
2	Bebloh	310,086
3	Zbot	292,160
4	Snifula	121,624
5	Cridex	23,127
6	Dyre	4,675
7	Shylock	4,512
8	Pandemiya	3,330
9	Shifu	2,177
10	Spyeye	1,480

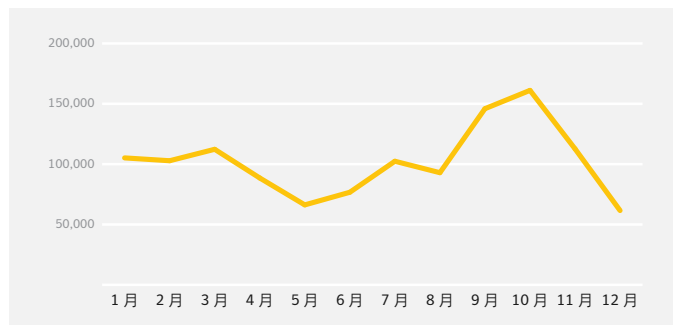
Ramnit (W32.Ramnit) 在 2016 年強勢回歸金融詐騙世界。Ramnit 自 2010 年起開始運作，不過在賽門鐵克的協助下，於 2015 年 2 月破獲其幕後的網路犯罪集團，一般認為這波行動阻止了傀儡網路運作。據傳在破獲當時，這幫傀儡網路是由 35 萬台電腦組成。Ramnit 消失了一段時間，不過在 2015 年 12 月發現新變種。

Ramnit 在 2016 年持續主宰金融特洛伊木馬程式，一整年都維持高度的偵測頻率。有趣的是，雖然 Ramnit 過去經常透過 Angler 攻擊套件散佈，但是 Angler 於年中消失後，Ramnit 的活動並未減少。這表示其幕後的行動者，可能已經調整感染技術，此外也有報告指出，Ramnit 在英國透過電子郵件傳播。部分 Ramnit 變種會自我複製，因而助長了其盛行情況。

Bebloh (Trojan.Bebloh) 名列金融特洛伊木馬程式名單的第二位；而 2016 年的報告指出，這項程式在日本積極活動，鎖定小型銀行及信用合作社為目標。Bebloh 也在 9 月和 10 月大幅提升了金融特洛伊木馬程式活動。Avalanche 惡意程式主控網路的一部分採用 Bebloh，於 2016 年遭到破獲，因此 Bebloh 在 11 月及 12 月的活動大幅下滑。

### 金融特洛伊木馬程式活動的逐月數量

2016 年 10 月之後活動下滑，是由於受到多起轟動的破獲行動所影響。



Neverquest 銀行惡意程式是賽門鐵克所偵測的 Trojan.Snifula，其幕後的駭客於 2017 年 1 月遭到逮捕。以上所有因素，可能讓 2017 年底的五大金融特洛伊木馬程式截然不同。

破獲行動的影響 (本章稍後將詳細探討)，具體呈現在 2016 年 10 月之後的感染數量下滑。Dridex (於 2015 年主宰威脅領域)、Dyre 及 Shylock (Trojan.Shylock) 的活動大幅下滑，都可歸功於破獲行動。

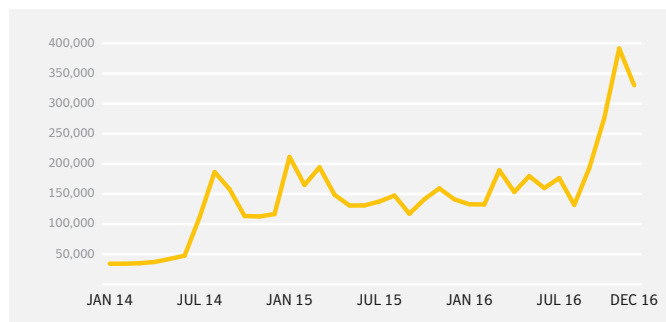
### 攻陷 Mac

過去 Apple 作業系統似乎堅不可摧，不過在 2016 年期間，在其中發現的惡意程式數量持續增加。

在 Mac 電腦發現的惡意程式，從 9 月開始穩定成長，一直持續到 2016 年的最後一季。2016 年 11 月的惡意程式偵測數量，幾乎是該年初的三倍。

### 2014 - 2016 年 Mac 惡意程式散佈每月統計數量

Mac 惡意程式在 2016 年下半年的成長相當顯著。



然而，這些數據並未必表示鎖定 Mac 生態系統的攻擊者有增加的趨勢。

深入檢視在 OS X 端點遭到封鎖的惡意程式，會發現 JavaScript 下載程式 (JS.Downloader) 和 Office 巨集下載程式 (W97M.Downloader) 是主要的兩個感染媒介，在前五名當中佔了三位。JS.Nemucod 遞送 Locky 勒索軟體，也名列前十名。

Mac 使用者遭到感染，比較可能是透過使用 JS.Downloader、W97M.Downloader 及 JS.Nemucod 散佈威脅的電子郵件，並不是因為越來越多的威脅行動者鎖定 Mac 使用者。

Mac 惡意程式偵測數量在 11 月和 12 月上升時，與 JS.Downloader 及 W97M.Downloader 相關的資安事端也同時增加，這兩者之間的關係顯而易見。

其他偵測到的前五名包括 OSX.Malcol 及 OSX.Malcol.2。這是變種偵測，能夠保護許多個別但變種的 OS X 特洛伊木馬程式。

## 在 OS X 端點遭到封鎖的前十大惡意程式佔總感染數的比例

JS.Downloader 及 W97M.Downloader 均名列 2016 年在 OS X 端點封鎖的惡意程式前五名。

排行	偵測	總感染率 (%)
1	OSX.Malcol	6.88
2	JS.Downloader	5.76
3	OSX.Malcol.2	5.73
4	W97M.Downloader	5.11
5	JS.Downloader.D	1.87
6	JS.Nemucod	1.09
7	VBS.Downloader.B	1.04
8	VBS.Downloader.Trojan	0.83
9	Trojan.Malscript	0.59
10	SMG.Heur!cg1	0.57

## Odinaff 及 Banswift：目標式金融竊盜大行其道的一年

雖然網路犯罪威脅多為無差別的大規模攻擊，但 2016 年卻有更精明幹練的網路犯罪團體浮出水面，或捲土重來。傳統網路犯罪採取的手法比較像「強取豪奪」，而菁英罪犯通常採用進階目標式攻擊的技術。由於執行這類攻擊需要資源、耐心及虛張聲勢，顯示網路犯罪可能已經進入全新時代。

其中出現兩個團體，鎖定國際金融系統的內部運作，而傳統線上銀行威脅則開始式微，顯示金融機構將在 2017 年面對截然不同的威脅。

### Banswift

2016 年初於孟加拉中央銀行發生的網路搶劫，是有史以來最膽大妄為的銀行搶劫案。罪犯成功帶走 8,100 萬美元，不過由於打錯字，加上負責監督的銀行官員起疑，否則遭劫金額可能高達 10 億美元。

罪犯刺探攻擊孟加拉銀行的安全性漏洞，滲透進入系統竊取銀行 SWIFT 憑證，以便從事詐騙交易。

之後罪犯使用惡意程式隱藏蹤跡。惡意程式能夠竄改孟加拉銀行的書面交易確認訊息，以便延遲發現詐騙的時間。攻擊者也選擇在孟加拉的長週末執行攻擊，進一步降低遭到發現的機會。

罪犯使用從孟加拉銀行竊取的 SWIFT 憑證，向紐約聯邦儲備局提出多項轉帳要求，以便將孟加拉銀行的款項轉帳至其他地方，主要是位於菲律賓及斯里蘭卡。其中四筆轉帳要求成功，總計轉出 8,100 萬美元至菲律賓的實體，不過有一筆要求轉帳至斯里蘭卡非營利「基金會」的 2,000 萬美元款項，因為基金會這個字拼錯而引起懷疑。轉帳因此遭到終止，並向孟加拉釐清情況，進而發現詐騙。不過已經損失了 8,100 萬美元，主要匯入與菲律賓賭場相關的帳戶。

其中大部份款項尚未追回，不過，有一間菲律賓賭場在 11 月將 1,500 萬美元歸還給孟加拉中央銀行。

這次攻擊所使用的手法，特別是對 SWIFT 系統的深入瞭解，以及掩飾攻擊的各項步驟，都顯示行動者是高度幹練的專家。這令人吃驚的大膽駭客行徑，也是首次明確顯示了國家等級人士涉入金融網路犯罪的跡象。這次攻擊與北韓的國家級行動者有關。

賽門鐵克分析這次攻擊孟加拉銀行使用的惡意程式 (Trojan.Banswift) 後，發現此惡意程式與 Lazarus 使用的工具之間，出現程式碼共用的情形，FBI 據此證據宣稱這與北韓政府有關。Lazarus 團體於 2014 年涉及聲名狼藉的 Sony 駭客事件，並與 2009 年起一連串對付美國及南韓的攻擊有關。

這個團體也牽涉其他兩起銀行搶劫，鎖定以 SWIFT 網路進行轉帳的銀行，不過 SWIFT 網路本身並未在任何這類攻擊中遭到侵害。

越南先鋒銀行 (Tien Phong Bank) 表示，曾經在 2015 年第四季攔截一筆 100 萬美元以上的詐騙轉帳。賽門鐵克研究也發現，另一家銀行也在 2015 年 10 月遭到相同團體鎖定。

第三家銀行是厄瓜多的 Banco del Austro 銀行，也提報損失 1,200 萬美元，由攻擊者使用詐騙 SWIFT 交易竊取，不過其中並沒有發現與亞洲攻擊事件的明確連結。

賽門鐵克認為 Lazarus 團體可能在 2017 年捲土重來，進一步攻擊金融機構。

#### Odinaff

2016 年發現牽涉 Trojan.Odinaff 的活動，將目標鎖定在全球金融機構。利用 Odinaff 的攻擊事件相當精明，顯然是由專業的網路犯罪幫派執行。雖然也鎖定 SWIFT 的使用者，但並沒有證據顯示這些攻擊與 Banswift 攻擊有關。

賽門鐵克研究指出，使用 Odinaff 的活動於 2016 年 1 月開始，將重點放在銀行、保全、貿易及薪資部門等組織。Odinaff Trojan 通常部署於攻擊的第一階段，以便在網路中取得立足之地。

牽涉 Odinaff 的攻擊事件非常精密，需要大量實機操作，並在特別鎖定的電腦上，依序部署一系列的輕量型後門及特定用途工具。

含有惡意巨集的文件最常部署特洛伊木馬程式，其中也使用傀儡網路進行部署。所有攻擊都是縝密管理，威脅行動者在目標組織網路維持低調，僅於必要時下載及安裝新工具。

Odinaff 攻擊使用的工具，具有 Carbanak 這個惡名昭彰團體的特徵，他們自 2013 年起鎖定金融部門。

Carbanak 活動於 2014 年底遭到發現，一般認為該團體已經鎖定多國的上百家銀行。部分網路安全社群成員預估，該團體可能已經竊取 10 億美元。賽門鐵克在 Carbanak 與 Odinaff 攻擊者之間發現多項連結，不過交叉分析基礎架構後並不符合規則，亦即 Odinaff 如果不屬於廣泛的 Carbanak 組織，就可能與 Carbanak 存在鬆散的合作關係。

雖然 2016 年許多攻擊者重拾現有的工具和技術，但 Odinaff 及 Banswift 的攻擊顯示，仍然有一群極為精明的網路罪犯，能夠部署進階活動以大撈一票。

## 資料外洩及地下經濟

### 資料外洩

過去 8 年來，資料外洩導致超過 70 億筆的身分資料遭到竊取，幾乎等於地球上每個人都遭竊一筆資料。

在 2016 年，資料外洩遭竊的身分達到 11 億筆，幾乎是 2015 年遭竊數量的兩倍（當時為略高於 5 億 6,300 萬筆身分資料），而且這兩年間的資料外洩次數，其實是從 1,211 次降低至 1,209 次。

2016 年平均每次外洩遭竊的身分數量，大幅上升至將近 100 萬筆，是過去三年最高的平均數字。

2016 年發生了 15 起大型外洩事件。大型外洩事件是指遭竊身分數量超過 1,000 萬筆的外洩事件，2016 年的次數高於 2014 年的 11 起及 2015 年的 13 起。

### 2014-2016 年資料外洩

雖然 2016 年的資料外洩事件數量大致持平，但遭竊身分數量則大幅攀升。

年	洩漏事件	遭竊身分	每次洩漏平均數	大型洩漏事件
2014	1523	1,226,138,929	805,081	11
2015	1211	563,807,647	465,572	13
2016	1209	1,120,172,821	926,528	15

資料外洩也在 2016 年登上頭條新聞，主要的原因是 Yahoo。Yahoo 在 9 月揭露 2014 年的外洩事件，當時導致 5 億個使用者帳戶遭到侵害。之後 Yahoo 於 12 月揭露 2013 年 8 月發生的事件，有 10 億個使用者帳戶受到侵害，成為史上最大規模的資料外洩事件。

Yahoo 表示這兩起外洩事件十分相關，且攻擊事件是由國家資助。揭露這兩起事件對 Yahoo 造成嚴重後果，當時 Yahoo 正在出售給 Verizon，其市值因此大幅下滑。

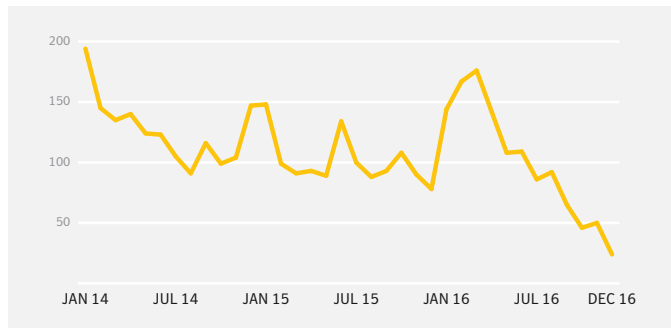
### 年度回顧

雖然 Yahoo 資料外洩消息於 2016 年爆發，但並未列入賽門鐵克 2016 年的遙測中，因為賽門鐵克是記錄資料外洩發生的時間，而不是提報的時間。

2016 年每月外洩數量在年初達到最高峰，然後一路下滑至年底。這是資料外洩的常見情形，因為資料外洩發生與提報之間通常有時間差距，Yahoo 資料外洩就是很明顯的例子，所以 2016 年底發生的資料外洩事件，可能根本尚未提報。

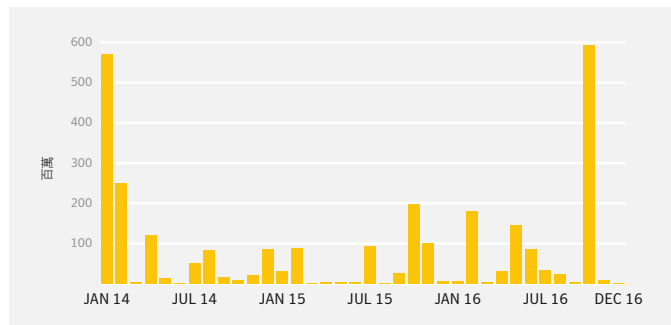
### 2014-2016 年每月資料外洩

每月資料外洩數量在 2016 年底一路下滑，可能是因為 11 月及 12 月發生的資料外洩事件尚未提報。



### 2014-2016 年每月遭竊身分

遭竊身分數量在 2016 年 10 月達到高峰，主要是因為 Friend Finder Networks 外洩事件造成。



雖然資料外洩數量一路下滑至 2016 年底，但遭竊身分數量卻在 10 月達到高峰，增加至將近 6 億筆。這種上升情形主要的因素為 Friend Finder Networks 的資料外洩事件，其中 4 億 1,200 萬個使用者帳戶的隱私詳細資料遭到暴露。

Friend Finder Networks 是成人約會及色情網站公司，營運網站包括 Adult Friend Finder、Cams.com 及一些其他較小的網站。該公司也曾經營運 Penthouse.com，並於 2016 年 2 月將其出售。儘管如此，Adult Friend Finder 仍存有 Penthouse.com 的使用者詳細資料，因此這些資料也在這次外洩事件中遭到暴露。

外洩的資料包括電子郵件地址、密碼 (以一般可見格式或 SHA1 雜湊儲存)、上次造訪日期、瀏覽器資訊、IP 位址及網站會員狀態。這是該公司在短短一年內第二次遭駭。

### 2016 年外洩事件的資料遺失類型

個人識別資訊仍是 2016 年最普遍遺失的資料，不過個人金融資訊緊追在後。

類型	2015 年 (%)	2016 年 (%)	百分點差異
個人識別資訊 (PII)	54.5	42.9	-11.6
個人金融資訊 (PFI)	32.9	39.2	6.3
其他資訊	1.6	11.1	9.5
個人健康資訊 (PHI)	11.0	6.8	-4.2

2016 年資料外洩所遺失的資訊中，將近 40% 為個人金融資訊，其中可能包括信用卡或簽帳卡詳細資料，或是銀行金融記錄。這項數據比 2015 年增加了六個百分點以上。資料外洩若暴露金融資料，是相當嚴重的事件，如果該資料遭到刺探攻擊，就會對受影響者產生財務損失的直接風險。

**資料外洩原因**

在 2015 及 2016 年，資料竊取都是資料外洩的第一大原因 (2016 年的比例為 36%)，之後依序為不當使用資料、未分類或其他原因 (無法判定原因) 及網路釣魚、詐騙或社交工程。

**2016 年資料外洩十大原因**

資料竊取是 2016 年資料外洩主要原因的第一名，比例超過 1/3。

排行	原因	2015 年 (%)	2016 年 (%)	百分點差異
1	資料竊取	42.4	36.2	-6.2
2	使用資料不當	20.4	19.3	-1.1
3	未分類或其他原因	11.9	19.2	7.3
4	網路釣魚、詐騙或社交工程	21.8	15.8	-6.0
5	意外資料遺失	1.7	3.2	1.5
6	裝置遺失或遭竊	0.6	3.1	2.5
7	IT 錯誤導致資料遺失	0.5	1.6	1.1
8	網路破壞或 DDoS	0.3	1.6	1.3
9	敲詐、勒索或破壞	0.1	0.2	0.1
10	身分竊取或詐騙	0.1	0	-0.1

就資料外洩數量而言，有 1/3 以上的原因是竊取資料，不過如果以遭竊身分數量衡量，其比例將高達 91%。

**2016 年身分竊取的資料外洩十大原因**

2016 年身分竊取的發生原因，絕大多數都是為了竊取資料。

排行	原因	2015 年 (%)	2016 年 (%)	百分點差異
1	資料竊取	85.3	91.6	6.3
2	網路釣魚、詐騙或社交工程	9.8	6.4	-3.4
3	意外資料遺失	1.1	1.0	-0.1
4	IT 錯誤導致資料遺失	< 0.1	0.9	0.9
5	網路破壞或 DDoS	< 0.1	< 0.1	< 0.1
6	使用資料不當	3.3	< 0.1	-3.3
7	裝置遺失或遭竊	< 0.1	< 0.1	< -0.1
8	未分類或其他原因	0.4	< 0.1	-0.4
9	敲詐、勒索或破壞	< 0.1	< 0.1	< 0.1
10	身分竊取或詐騙	< 0.1	0	< -0.1

**遭到暴露的產業**

2016 年最受資料外洩影響的產業為服務業，將近有 45% 的外洩事件發生在服務業，之後則依序為金融、保險及不動產的 22%，與 2015 年的前兩名相同。如果更詳細分析探討子部門，商業服務產業的資料外洩比例最高 (24%)，然後是健康服務產業 (11%)。

由於健康服務產業能夠揭露的資訊非常機密，因此舉報資料外洩時受到嚴密規範，這可能是其名列前茅的原因。

**依據資安事端數量的十大資料外洩部門**

2016 年最受資料外洩影響的產業為服務業。

排行	行業	洩漏事件	百分比
1	服務業	452	44.2
2	金融、保險及不動產業	226	22.1
3	製造業	116	11.3
4	零售業	84	8.2
5	運輸及公用事業	75	7.3
6	批發業	32	3.1
7	建築業	20	2.0
8	採礦業	8	0.8
9	公共行政	6	0.6
10	無法分類的機構	3	0.3

**依據資安事端數量的十大資料外洩子部門**

商業服務是最受影響的子部門，之後則是健康服務。

排行	行業	洩漏事件	百分比
1	商業服務	248	24.2
2	醫療服務業	115	11.2
3	存款機構	71	6.9
4	非存款機構	62	6.1
5	通訊業	42	4.1
6	保險人	41	4.0
7	工程及管理服務	38	3.7
8	雜貨零售	34	3.3
9	批發業 - 耐用商品	25	2.4
10	控股及其他投資辦事處	23	2.2



依據身分遭竊數量所列出的資料外洩前十大部門及子部門，大致反映前述數據，其中服務業 (90%) 是部門名單的第一名，商業服務 (78%) 則在子部門名列第一。

在以身分遭竊數量探討資料外洩時，健康服務所佔的比例大幅降低，是子部門的第九名，其中遭竊身分的比例不到 1%。

#### 依據身分遭竊數量的十大資料外洩部門

在 2016 年遭竊的身分中，服務部門外洩的數量佔 90% 以上。

排行	行業	遭竊身分	百分比
1	服務	914,382,512	90.1
2	製造業	56,782,089	5.6
3	零售業	13,173,167	1.3
4	採礦業	9,758,832	1.0
5	建築業	7,963,470	0.8
6	運輸及公用事業	6,243,712	0.6
7	金融、保險及不動產業	3,554,225	0.4
8	批發業	2,051,635	0.2
9	公共行政	1,198,971	0.1
10	無法分類的機構	685	< 0.1

#### 依據身分遭竊數量的十大資料外洩子部門

在身分遭竊方面受影響最大的子部門是商業服務，外洩數量佔將近 78%。

排行	行業	遭竊身分	百分比
1	商業服務	786,918,569	77.5
2	電影	85,200,000	8.4
3	印刷與出版	49,299,205	4.9
4	個人服務	27,001,398	2.7
5	雜貨零售	10,694,512	1.1
6	煤礦業	9,746,241	1.0
7	工程及管理服務	8,216,181	0.8
8	特殊交易承包商	7,932,817	0.8
9	醫療服務業	6,838,017	0.7
10	通訊業	5,304,054	0.5

在這份子部門的名單中有一項值得關注的數據：在名列第二的影片 (Motion Pictures) 類別中，有 8,520 萬筆身分 (8%) 遭竊。這項數據的原因是單一資料外洩事件，也就是法國線上影片分享網站 [Dailymotion](#) 遭駭，而這類網站是分類在影片類別。

Dailymotion 資料外洩於 10 月發生，不過直到 12 月才對外公佈。該公司系統在這次外洩中，暴露了 8,520 萬筆不同的電子郵件地址及使用者名稱。不過其中約有 1/5 的帳戶，其相關密碼以強大的 Bcrypt 雜湊功能進行編碼，因此難以破解。

**國家資料**

美國在外洩事件數量以及身分遭竊數量方面，都名列各國第一。這並不令人意外，其中有多項原因。美國人口眾多，採用科技的比率高，且有許多公司總部位在美國。美國在提報資料外洩方面也制定嚴格法律規範。在沒有法律規範的地區，通常資料外洩的情形會少報。

**資料外洩數量前十名國家**

美國在 2016 年是受到資料外洩影響最大的國家。

排行	國家/地區	洩漏事件
1	美國	1023
2	英國	38
3	加拿大	19
4	澳洲	15
5	印度	8
6	愛爾蘭	8
7	日本	7
8	以色列	6
9	德國	5
10	泰國	5

**身分遭竊數量前十名國家**

美國在 2016 年也是身分遭竊數量最多的國家。

排行	國家/地區	遭竊身分
1	美國	791,820,040
2	法國	85,312,000
3	俄羅斯	83,500,000
4	加拿大	72,016,746
5	台灣	30,000,051
6	中國	11,344,346
7	南韓	10,394,341
8	日本	8,301,658
9	荷蘭	6,595,756
10	瑞典	6,084,276

如果探討美國身分遭竊的問題，有一項有趣發現，就是身分暴露主要都發生在大型外洩事件。其中光是八項大型外洩事件，就暴露了 90% 的美國遭竊身分。

法國在 2016 年只有四起資料外洩事件，不過在身分遭竊數量則名列第二，原因為之前談到的 Dailymotion 外洩事件，造成 8,500 萬筆以上身分遭竊。

同樣地，俄羅斯的兩起資料外洩事件，也暴露了大量身分。這兩起外洩事件都發生在 Mail.Ru。其中一次外洩揭露了 5,700 萬筆電子郵件地址，第二次外洩則有 2,500 萬筆線上討論區的使用者帳戶遭到侵害。

### 地下經濟

雖然地下經濟一般與信用卡詳細資料及竊取個人資訊有關，不過賽門鐵克研究人員發現，網路罪犯越來越有興趣販售 Netflix 及 Spotify 等媒體帳戶，每個帳戶的價格從 10 美分到 10 美元不等。雖然前述帳戶可收取的價格不高，不過如果攻擊者入侵裝置，就可能取得此帳戶資訊，因此會嘗試進行銷售，試圖從中獲得最大利益。

2016 年地下經濟應有盡有：從 1 美元的叫車服務應用程式 (如 Uber 帳戶)，到可能需要花上 1,000 美元的分散式阻斷服務 (DDoS)。

餐廳禮品卡、飯店預訂以及航空公司常客哩程，都在銷售服務的範圍內。其中也銷售線上銀行帳戶以及 PayPal 帳戶，此外還有 Amazon 和 Walmart 的零售購物帳戶。

在惡意程式方面，勒索軟體工具組要價可能高達 1,800 美元，且通常以犯罪軟體即服務 (CaaS) 方式販售，而 Android 銀行特洛伊木馬程式的價格則為 200 美元。

賽門鐵克發現轉帳服務方案增加，其銷售金額為本身價值的 10%，例如以比特幣支付 100 美元，換取轉帳 1,000 美元。這顯示竊取金錢的洗錢程序，仍然是網路罪犯最難克服的難關。

在公開的地下討論區及黑市網頁 Tor 網站發現的價格，自 2015 年以來維持穩定。信用卡仍是地下討論區銷售最多的數位商品。

信用卡價格差異幅度相當大，需視其發卡國家 (歐盟信用卡比美國信用卡貴)、公司、等級 (金卡、白金卡等等) 及提供的額外資訊而定。擁有完整詳細資料的信用卡，價格高於沒有完整詳細資料的卡，如果其中包含個人識別資訊 (PIN)，價格就會高上 10 倍。

### 地下經濟市集定價表

支付卡	價格
單一信用卡	0.5 - 30 美元
單一信用卡含完整詳細資料 (Fullz)	20 - 60 美元
轉儲磁條磁軌 1&2 及 PIN	60 - 100 美元
惡意程式	
基本銀行交易特洛伊木馬程式含支援	100 美元
竊取密碼特洛伊木馬程式	25 - 100 美元
Android 銀行交易特洛伊木馬程式	200 美元
Office 巨集下載程式產生器	5 美元
惡意程式加密器服務 (使其難以遭到偵測)	20 - 40 美元
勒索軟體套件	10 - 1800 美元
服務	
媒體串流服務	0.10 - 10 美元
旅館獎勵計畫帳戶 (10 萬點)	10 - 20 美元
航空公司常客哩程帳戶 (1 萬英哩)	5 - 35 美元
計程車應用程式帳戶含餘額	0.5 - 1 美元
線上零售禮品卡	面值的 20% - 65%
餐廳禮品卡	面值的 20% - 40%
航空公司機票及旅館預訂	面值的 10%
DDoS 服務 (1 小時內、中型目標)	5 - 20 美元
DDoS 服務 (24 小時以上、中大型目標)	10 - 1000 美元
專屬防彈主機 (每月)	100 - 200 美元
轉帳服務	
提取現金服務	10% - 20%
帳戶	
線上銀行帳戶	帳戶餘額的 0.5% - 10%
零售商帳戶	20 - 50 美元
雲端服務供應商帳戶	6 - 10 美元
身分	
身分 (姓名、SSN 及 DOB)	0.1 - 1.5 美元
掃描護照及其他文件 (例如水電瓦斯帳單)	1 - 3 美元

# 地下市集



勒索軟體  
工具組

\$10 - \$1,800



短期 DDoS  
(< 1hr)

\$5 - \$20



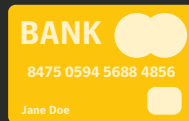
文件  
(密碼、水電瓦斯帳單)

\$1 - \$3



Android 銀行交易木馬程式

\$200



信用卡

\$0.5 - \$30



雲端服務帳戶

\$6 - \$10



禮品卡

20%- 40%  
(面值)



提取現金服務

10%- 20%  
(帳面價值)

這裡的一切  
都有價格

## 瓦解與破獲

雖然網路犯罪持續有利可圖，不過幾次重大的瓦解破獲行動，有助於減少活動並提出警告訊息。

### Avalanche

**Avalanche 破獲行動**重重打擊了網路犯罪社群，破獲至少 17 個惡意程式系列使用的基礎架構。這項破獲行動在多個國際執法單位、多位檢察官與包含賽門鐵克在內的安全及 IT 企業共同努力下，查扣了 Avalanche 網路幕後犯罪組織所使用的 39 台伺服器與數十萬個網域。

賽門鐵克自 2012 年起開始研究 Avalanche 網路，當時賽門鐵克曾發佈研究報告，探討主要鎖定德國、奧地利及部分瑞士地區的德語人士的勒索軟體。同時，德國警方則調查名列賽門鐵克研究中的 Bebloh 惡意程式 (Trojan.Bebloh)。賽門鐵克研究人員提供技術協助警方調查，在各方通力合作下，發現了 Avalanche 傀儡網路。Avalanche 運作範圍龐大，負責控制全球大量遭入侵的電腦。

調查行動在 2016 年 11 月 30 日進入尾聲，最後關閉了至少為 17 種惡意程式系列提供支援的基礎架構，並逮捕多位涉嫌參與行動的罪犯。

### Bayrob

**Bayrob 破獲行動**是 FBI 調查八年所累積的成果，賽門鐵克也從中協助。相關行動逮捕並引渡了三名羅馬尼亞人前往美國，他們多年來從受害者身上竊取高達 3,500 萬美元。

Bayrob (Trojan.Bayrob) 幕後的職業網路罪犯，一開始是建立假的線上車輛拍賣，向受害者詐欺數萬美元，然後擴大範圍從事其他詐騙及惡意程式行動，包括信用卡竊盜及電子加密貨幣探勘等等。

賽門鐵克在調查期間，發現多種版本的 Bayrob 惡意程式收集情報資料，並見證 Bayrob 由線上詐騙轉型為 30 萬台以上電腦的傀儡網路，從事電子加密貨幣探勘。賽門鐵克成功揭露這幫惡徒行動，深入掌握其中的關鍵人物、戰術、惡意程式，以及所從事的犯罪活動和其影響。

賽門鐵克於 2007 年首次撰文介紹 Bayrob 幫，揭露其高度精密的假汽車銷售 eBay 騙局。不過即使獲得大眾關注，仍沒有遏止網路罪犯，這幫人持續從事犯罪活動，進行更多線上拍賣詐騙，並將觸角伸入信用卡詐騙。他們也在美國及歐洲招募錢駝網路組織，以便將詐騙所得送回羅馬尼亞。

近年來，該團體將焦點轉移至建構傀儡網路進行電子加密貨幣探勘，其傀儡網路到了 2016 年，已經成長到超過 30 萬台電腦。

多年來，賽門鐵克持續監控這個團體的活動，以便加強對客戶的保護，同時協助 FBI 從事調查。這項合作最終在 2016 年底逮捕嫌犯。

### Lurk/Angler

俄羅斯安全部隊於 2016 年 6 月破獲 Lurk 銀行交易集團，在莫斯科逮捕 50 名嫌犯。

Lurk 銀行交易特洛伊木馬程式鎖定俄羅斯的金融機構，一般認為其幕後集團從多家俄羅斯金融機構，竊取了超過 2,500 萬美元的款項。

逮捕以上嫌犯後，多個威脅團體的活動也同時下降，包括 Locky、Dridex 及 Angler 攻擊套件。不過，雖然 Locky 及 Dridex 活動在 2016 年下半年再次復甦，Angler 並未回歸。這讓各界推測 Lurk 銀行交易特洛伊木馬與 Angler 攻擊套件，是由相同的幕後人士負責操控。

自 Lurk 逮捕事件後，Angler 就在各種威脅中消聲匿跡，我們將於「網路攻擊」的章節詳細探討相關發展。

### Dyre

2016 年初的重大破獲案之一，就是 Dyre 金融詐騙特洛伊木馬程式。

根據 2 月份的報導，俄羅斯執法單位在 2015 年 11 月採取行動，同時幾乎消弭了金融特洛伊木馬程式的相關活動。賽門鐵克遙測證實了此項活動減少的情形。Dyre (Infostealer.Dyre) 是透過電子郵件垃圾郵件活動散佈，自 2015 年 11 月 18 日後，賽門鐵克就沒有再發現 Dyre 相關的垃圾郵件活動。

Dyre 破獲行動十分重大，因為 Dyre 已經成為最活躍的金融詐騙工具之一。Dyre 鎖定 Windows 電腦竊取銀行交易及其他憑證，也可用於以其他類型惡意程式的感染受害者，將其加入垃圾郵件傀儡網路中。

Dyre 垃圾郵件活動包含惡意附件，如果開啟，就會在受害者電腦安裝 Upatre 下載程式 (Downloader.Upatre)。Upatre 遭到偵測的數量，於 2015 年 7 月達到高峰，超過 25 萬。Upatre 及 Dyre 遭到偵測的數量，在 2015 年 11 月之後大幅下滑。

目前破獲 Dyre 的相關情況並不明確，並沒有任何決定性事物顯示其中的逮捕對象或人數。2016 年底的報導宣稱新型的銀行交易特洛伊木馬程式 Trojan Trickbot (Trojan.Trickybot)，是重新編寫的 Dyre。Fidelis 研究人員表示，他們有「一定程度的信心」認為，有一位以上的 Dyre 原始開發人員參與 Trickbot。

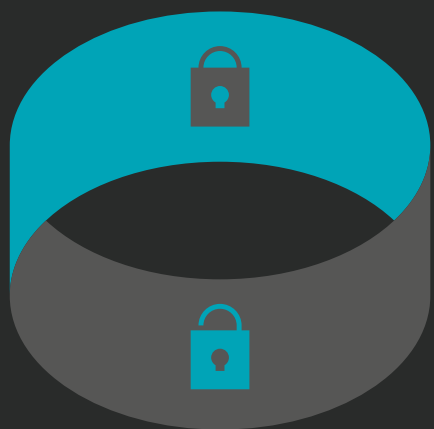
### 延伸閱讀

- [SWIFT 攻擊者所用的惡意程式涉及更多起金融攻擊事件](#)
- [Odinaff：新型特洛伊木馬程式用於高階金融攻擊事件](#)
- [執法單位一舉破獲並重創「雪崩行動 \(Avalanche\)」惡意程式網路](#)
- [Bayrob：三位嫌犯引渡前往美國受審](#)
- [PowerShell 威脅興起：95.4% 分析過的程序檔為惡意](#)
- [Necurs：大量郵寄傀儡網路以新一波的垃圾郵件活動回歸](#)

### 最佳實務準則

- 定期備份電腦或任何其他裝置儲存的任何檔案。
- 隨時確保您所有裝置內的安全軟體為最新版本，包括行動裝置在內，以便協助您抵禦任何最新變種惡意程式的威脅。
- 時常更新您的作業系統和其他軟體。軟體更新經常含有新發現安全漏洞的修補程式，而且這些漏洞可能為攻擊者所利用。
- 刪除任何可疑的電子郵件，尤其是含有連結或附加檔案的郵件。
- 如果有任何 Microsoft Office 電子郵件附件建議您啟用巨集以檢視信件內容，請務必小心。除非您十分確信此封信件是真的，並且來源可靠，否則請不要啟用巨集，並馬上刪除信件。
- 使用行動裝置時，請不要由不熟悉的網站下載應用程式，只能由信賴來源安裝應用程式。此外也請特別留意應用程式請求的權限。
- 確保您在線上帳戶使用的密碼獨一無二且強度足夠。請勿在多個帳戶重複使用相同密碼，並啟用雙因素驗證功能 (如有)。
- 註冊接收銀行警示，一旦您的帳戶出現任何可疑交易，就可以獲得警示。

# 勒索軟體： 勒索企業及消費者



章節

# 07



## 簡介

在 2016 年，勒索軟體成為個人及組織最重大的威脅之一。攻擊者不斷精良其利用勒索軟體的犯案手法，使用強化加密、匿名比特幣支付及大規模垃圾郵件攻擊，建立危險且影響廣泛的惡意程式。新型勒索軟體系列持續增加，顯示越來越多攻擊者加入這個行列。雖然勒索軟體對消費者構成較高的風險 (佔所有感染事件的 69%)，但今年也有證據顯示勒索軟體攻擊者勢力擴張，並開發更縝密的攻擊手法，例如鎖定企業發動的目標式勒索軟體攻擊，包括初始入侵 (initial compromise) 及網路走訪 (network traversal)，皆可造成多部機器遭到加密。勒索軟體將持續成為 2017 年全球的主要資安隱憂。

## 重要發現

- 勒索軟體的盛行率及破壞性，使其在 2016 年成為消費者及企業面臨的最危險網路犯罪威脅。
- 平均勒索金額由 2015 年的 294 美元激增 266%，來到 1,077 美元。攻擊者顯然認定，可以從受害者身上詐取更多暴利。
- 2016 年偵獲的勒索軟體增加 36%。

## 趨勢及分析

2016 年偵獲的勒索軟體數量增加 36%，從 2015 年的 34 萬上升至 2016 年的 46.3 萬。2016 年每日由防毒工具偵獲的勒索軟體數量也有所提升，年初每日平均約為 846 個，年底則上升至每日超過 1,539 個。

其中值得注意的是，以上偵測數據僅佔賽門鐵克所封鎖的勒索軟體極小比例，因為多數攻擊都在感染程序初期即遭封鎖。

勒索軟體會以多種不同方式散佈。一般而言，感染過程包含多個不同階段，且在任何階段都可以封鎖攻擊。例如電子郵件散佈的勒索軟體，大部分攻擊 (每日數十萬) 都由防垃圾郵件的防禦機制所封鎖。大部分勒索軟體電子郵件都含有下載程式，隱藏在惡意附件中。下載程式可用來將勒索軟體下載並安裝到受害者電腦，許多攻擊會在此階段遭到封鎖，亦即勒索軟體下載到目標電腦之前。

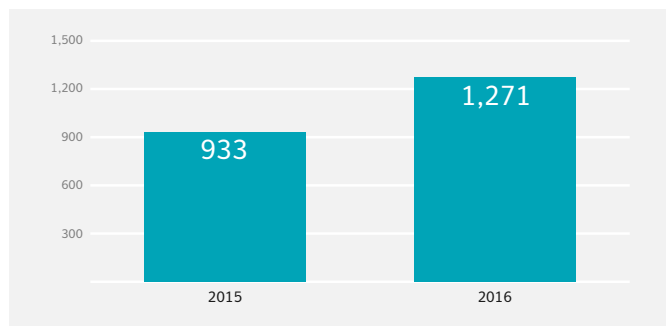
就網路攻擊而言，許多勒索軟體會透過刺探攻擊套件來發動攻擊，或利用惡意網頁刺探攻擊受害者電腦的漏洞，藉此植入惡意程式。許多勒索軟體攻擊在此階段遭到封鎖，亦即勒索軟體植入受害者電腦之前。

除了在感染程序初期封鎖的攻擊以外，變種偵測技術也常偵獲並封鎖勒索軟體，因其能夠識別惡意程式常見的惡意行為。

雖然由防毒工具偵獲的勒索軟體，只佔整體攻擊數量的一小部分，但由於此數據在 2016 年顯著上升，表示此期間的勒索軟體活動有所增加。

## 全球每日偵獲勒索軟體平均數量

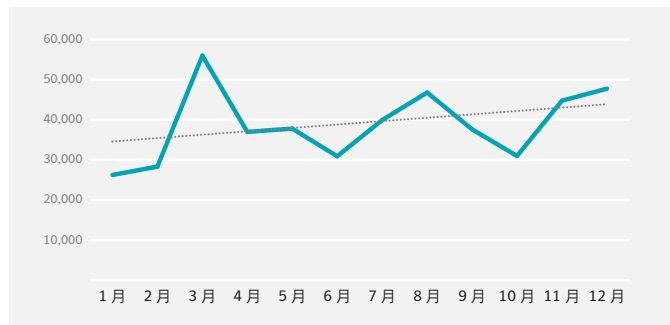
由防毒工具偵獲的勒索軟體數量增加 36%，從 2015 年平均每日 933 個，增加到 2016 年的 1,270 個。





## 全球每月偵獲勒索軟體數量

每月遭防毒工具偵獲的勒索軟體數量，在 2016 年期間逐步增加，年初約為每月平均 3.5 萬個，年底則上升至 4 萬個。

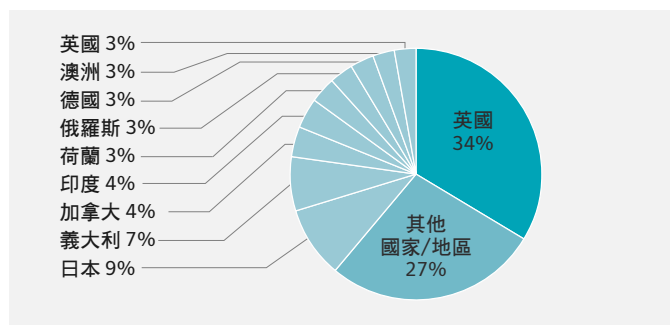


在 2016 年記錄的所有感染事件中，超過 1/3 發生於美國，成為勒索軟體影響最嚴重的地區。日本 (9%)、義大利 (7%)、加拿大 (4%) 及印度 (4%) 也是重度受創地區。荷蘭 (3%)、俄羅斯 (3%)、德國 (3%) 及英國 (3%) 是感染數據偏高的歐洲國家。另一個名列前十的國家為澳洲 (3%)。

這項統計數據顯示，攻擊者多將目標放在局勢穩定的已開發經濟體。

## 各國偵獲勒索軟體比例

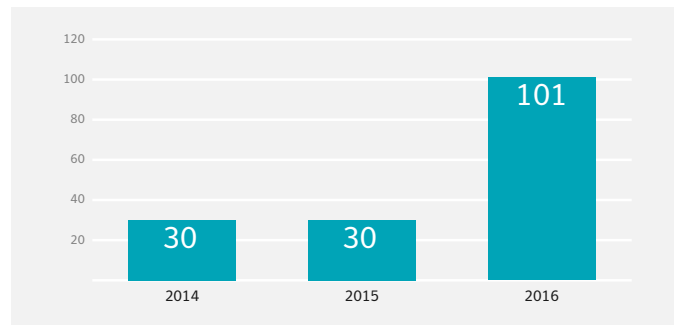
2016 年防毒工具偵獲勒索軟體的各國比例。美國持續成為勒索軟體最盛行的地區。



2016 年出現的新型勒索軟體系列大幅增加。2014 及 2015 年各出現 30 種新系列，2016 年則成長超過 2 倍而達到 101 種。這項趨勢顯示，越來越多攻擊者加入勒索軟體的行列，開發各種新型勒索軟體系列，或是修改現有系列。

## 新型勒索軟體系列

各年發現的新型勒索軟體系列數量。2016 年數據成長 3 倍而達到 101 種，顯示更多攻擊者加入勒索軟體的行列。

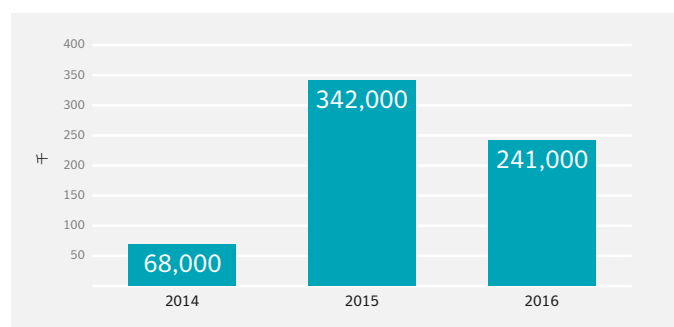


勒索軟體變種數量 (即勒索軟體系列的獨特變種) 較去年同期下降，由 2015 年的 34.2 萬種減少 29% 至 2016 年的 24.1 萬種。新型勒索軟體變種的逐月統計數量也反映出這項下滑趨勢，從 1 月平均超過 2 萬個下降到年底的 2 萬個以下。

新變種的數量是整體勒索軟體活動的另一項指標，攻擊者希望能夠迴避偵測，因此要建立全新的威脅變種。若要瞭解變種數量下滑的原因，就必須一併考量新型勒索軟體系列在 2016 年大幅增加的情形。其中顯示，較多攻擊者偏好從零開始做出全新的勒索軟體系列，而不是創造新變種來調整現有系列。

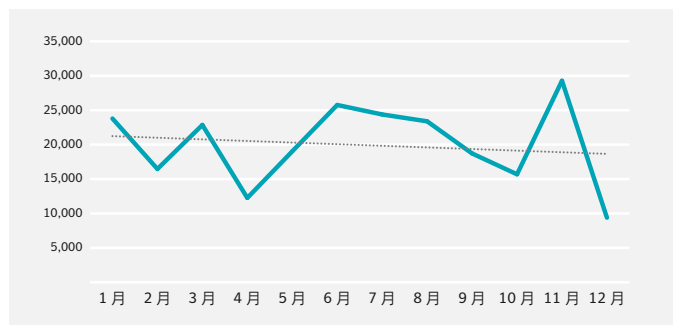
## 新型勒索軟體變種

各年新型勒索軟體變種 (獨特個案) 數量。新變種數量下滑 29%，從 2015 年的 34.2 萬種下降至 2016 年的 24.1 萬種。



### 每月的勒索軟體變種

每月的新型勒索軟體變種。平均數量由 2016 年 1 月的超過 2 萬，減少至年底的 2 萬以下。

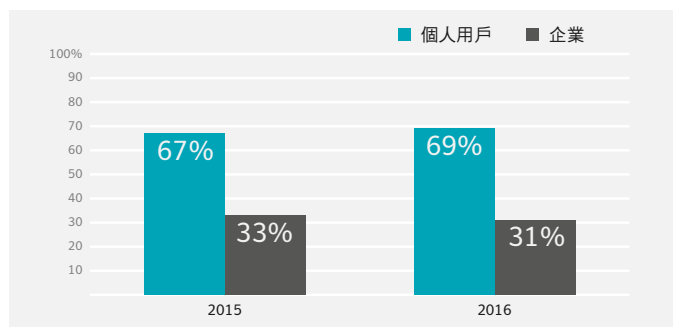


2016 年的勒索軟體主要感染目標為消費者電腦 (69%)。這項數據略高於 2015 年，當時消費者電腦感染勒索軟體的比例為 67%。

消費者感染比例與企業及其他組織的對照結果，在 2016 年大致相對穩定，其中每月的消費者感染比例介於 59% 及 79% 之間。唯一例外是 2016 年 12 月，當時兩者之間的比例幾乎相同，消費者感染的比例下降至 51%。

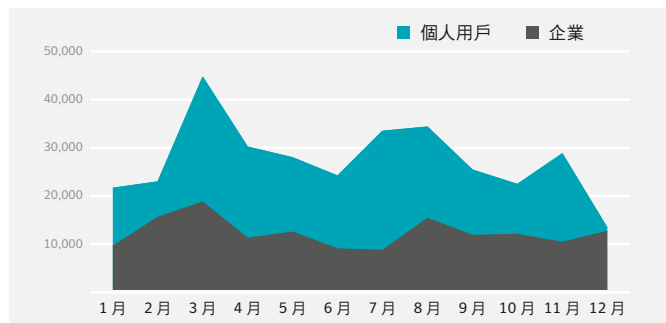
### 消費者與企業感染比例

企業與消費者感染勒索軟體的比例。2016 年的勒索軟體主要感染目標為消費者電腦。消費者感染比例 (69%) 僅略高於 2015 年的 67%。



### 每月的消費者與企業感染比例

消費者感染比例與企業及其他組織的對照結果，在 2016 年大致相對穩定。



### 個案研究/調查

#### 勒索軟體如何影響消費者

目前有數百種不同的勒索軟體系列以各種方式散佈；不過 2016 年最活躍的勒索軟體威脅，則是透過電子郵件散佈。在許多情況下，受害者會收到垃圾郵件，看起來就像公司的發票或收據。這類電子郵件通常會精心撰寫，設法誘騙收件者開啟惡意附件，例如「這是您最近的購物明細，請詳見附件收據」。

開啟附件後，就會啟動一連串感染流程。這可能會執行惡意程式的一小部分，亦即所謂的下載程式，以便將勒索軟體下載並植入受害者的電腦。一旦遭到安裝，勒索軟體就會開始在電腦加密預先編程範圍的檔案 (特定資料夾檔案及/或特定副檔名檔案)。大部分新型的勒索軟體系列都採用強化加密，亦即受害者若沒有加密金鑰，就完全無法開啟遭加密的檔案。

通常受害者一開始都渾然不覺，直到畫面出現勒索訊息才驚覺大事不妙。訊息通常說明受害者檔案發生了什麼情形，以及贖金的支付方式，贖金通常是透過網站或匿名 Tor 網路支付。

#### 勒索軟體如何影響企業

大部分勒索軟體的威脅對受害者「一視同仁」，企業及消費者的感染經驗也類似。不過有少數團體開始特別針對企業，透過專門設計的勒索軟體攻擊，僅感染單一網路內的多部電腦，並加密寶貴資料。

SamSam ([Ransom.SamSam](#)) 案例中，攻擊者的初始進入點是公開的網頁伺服器。他們刺探攻擊未修補的漏洞入侵伺服器，並在受害者網路取得立足之地，藉此使用 Microsoft Sysinternals 等多用途工具，周遊於受害者網路中。如此一來，攻擊者就能在組織網路中，對應每台可存取的電腦，並識別大部分的寶貴資產。

攻擊者之後使用名為 f.bat 的批次程序檔，在每台電腦部署 SamSam 及公開加密金鑰。程序檔也會從電腦刪除磁碟區陰影複本，讓電腦無法在感染之後回復任何檔案。攻擊者散佈一種名為 sqlsrvtmgl.exe 的工具。這種可執行檔會搜尋任何執行中的備份程序，並將其停止，此外也會刪除發現的任何備份相關檔案。

最後一個階段就是散佈另一種名為 reg.bat 的批次程序檔。這個檔案會在每台受感染的電腦開始加密程序。SamSam 可加密數百種不同類型的檔案，一旦加密完成，勒索軟體就會自刪，留下遭加密的檔案，以及桌面上的勒索通知。通知要求受害者前往特定網站，為每台遭入侵的電腦支付 1.5 比特幣 (撰寫本文時約為 1,587 美元) 的贖金。

#### 勒索軟體獅子大開口

2016 年，攻擊者要求的平均贖金大幅成長。贖金在 2015 年略微下滑後，2016 年新系列勒索軟體要求的平均贖金，由 294 美元提升至 1,077 美元。

平均贖金要求增加，部分原因是 2016 年所出現的最大額贖金。當時 MIRCOP 勒索軟體 ([Ransom.Mircop](#)) 要求異常高額的贖金，達到 28,730 美元。不過，即使不計算 MIRCOP 的贖金要求，平均贖金仍然翻倍達到 678 美元。攻擊者顯然認為可以從受害者身上榨取更多錢財。

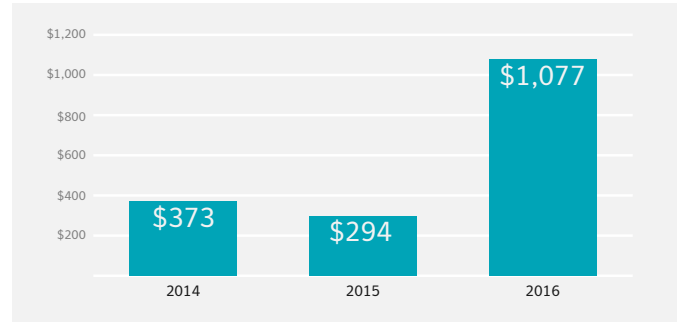
根據 Norton Cyber Security Insight 團隊的研究，有 34% 的受害者會支付贖金，美國地區的比例更高達 64%，顯示出美國是非常熱門的目標。願意支付贖金是勒索要求金額增加的主要原因。

贖金付款也變得更容易。為了鼓勵受害者付款，攻擊者目前通常會支援付費管道，並與更多的付費捐客服務合作，簡化了比特幣的使用方式，更何況現在比特幣的名氣也逐漸上升。

不過，支付贖金並不保證能夠解密受害檔案。根據 Norton Cyber Security Insight 團隊的資料，支付贖金的受害者中，只有 47% 取回檔案。

#### 平均勒索要求金額

2016 年發現的新系列勒索軟體，其平均贖金要求金額成長為三倍以上，從 294 美元上升至 1,077 美元。



攻擊者也透過更有創意的方式，試圖從受害者身上榨取更多錢財。多種新型勒索軟體系列，就會運用變化多端的勒索要求。例如 Cerber ([Ransom.Cerber](#))，如果五天後仍未支付贖金，就會將贖金由 1.25 比特幣 (1,255 美元) 加倍為 2.5 比特幣。

此外也有一些證據顯示，勒索軟體攻擊者開始依據加密的資料類型及數量，進行不同的勒索要求。據報 HDDCryptor ([Ransom.HDDCryptor](#)) 幕後的攻擊者，向受害者舊金山市運輸局 (San Francisco's Municipal Transportation Agency) 要求 7 萬美元贖款，導致舊金山市的輕軌服務完全停擺 (我們計算平均贖金時，並未將這類「客製化」贖金要求列入其中)。

#### 感染媒介

勒索軟體是以多重感染媒介散佈，其中最常用的媒介就是垃圾電子郵件，這也是 2016 年部分廣泛威脅的散佈手法，例如 Locky ([Ransom.Locky](#)) 就是以這種方式散佈。

大規模的垃圾郵件攻擊可能包含數百萬封電子郵件，幾乎每日都會發生，並以傀儡網路作為傳遞媒介。傀儡網路是一群遭入侵的電腦，規模可從數百台至數百萬台電腦。大部分攻擊使用社交工程技巧，誘使收件者開啟電子郵件及附件，例如將電子郵件偽裝成發票或出貨通知。

## 主要勒索軟體威脅



### Locky

大約贖金：

**\$965**

搜尋：

2016 年 2 月

傳播媒介：

- 電子郵件活動
- Neutrino 刺探攻擊套件
- Nuclear 刺探攻擊套件
- RIG 刺探攻擊套件

○ 2016 年最廣泛散佈的勒索軟體威脅之一

○ 透過 Necurs 傀儡網路的大量電子郵件活動傳播

○ Locky 盛行率於 2017 年初大幅下滑，因為 Necurs 活動自 2016 年 12 月底開始減少



### Cerber

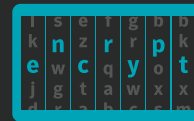
**\$1,200**

2016 年 3 月

- 電子郵件活動
- RIG 刺探攻擊套件
- Magnitude 刺探攻擊套件

○ 在 2016 年底散佈非常廣泛，原因包括大量電子郵件及 RIG 刺探利用套件活動

○ 電子郵件活動主要使用 JavaScript 及 Office 巨集，不過也可能附加為 zip 檔案



### CryptXXX

**\$500**

2016 年 4 月

- Angler 刺探攻擊套件
- Neutrino 刺探攻擊套件

○ Angler 於六月初消聲匿跡，造成活動減少

○ 於 2017 年初重現江湖，透過 Neutrino 刺探攻擊套件傳遞

○ 初期變種使用可破解的脆弱加密。新型變種採用增強的加密，不可能解密

最常見的感染方法就是含有下載程式的惡意附件，通常是 JavaScript 下載程式 ([JS.Downloader](#)) 或 Word 巨集下載程式 ([W97M.Downloader](#))，一旦點開將下載並安裝勒索軟體。有些情況則未使用下載程式，而是由惡意附件直接安裝勒索軟體。此外，有些垃圾郵件含有刺探攻擊套件的連結，啟動後會將勒索軟體植入收件者電腦。部分連結並不會連往刺探攻擊套件，而是直接連往下載程式或勒索軟體酬載。

刺探攻擊套件本身是另一種主要感染媒介，用於散佈常見的勒索軟體威脅，例如 Cerber ([Ransom.Cerber](#)) 及 CryptXXX ([Ransom.CryptXXX](#))。刺探攻擊套件攻擊者通常會入侵第三方網頁伺服器，將惡意程式碼置入其中託管的網頁，如此可將瀏覽器引導至刺探攻擊套件伺服器。

除了透過垃圾郵件攻擊或社交媒體貼文散佈連結，攻擊者還可利用多種其他方式，重新將流量重新導向至刺探攻擊套件伺服器，例如惡意廣告，或從流量分佈服務進行重新導向。

刺探攻擊套件須透過漏洞來發揮作用。執行過期或未修補軟體的使用者風險最高。擁有最新軟體的使用者，只有在刺探攻擊套件攻擊零時差漏洞時，才會遭到暴露。到了 2016 年底，賽門鐵克每日封鎖的刺探攻擊套件攻擊約 38.8 萬次。

雖然垃圾郵件攻擊及刺探攻擊套件是主要的感染媒介，但仍有其他散佈勒索軟體的戰術，其中包括：

- 二次感染：在部分情況下，已經感染電腦的惡意程式，可用來下載更多惡意程式，包括勒索軟體。例如原始的 [CryptoLocker](#) 勒索軟體，部分受害者表示是在感染其中一種傀儡網路後遭到感染。
- 暴力攻擊密碼：部分系列的勒索軟體會針對伺服器使用的軟體，透過暴力攻擊登入憑證進行散佈。例如 Bucbi ([Ransom.Bucbi](#)) 就是使用此方法，在遠端桌面通訊協定 (RDP) 伺服器找到擴張的據點。

- 刺探攻擊伺服器漏洞：部分勒索軟體集團鎖定在伺服器上執行的脆弱軟體，藉此存取組織網路。SamSam 勒索軟體 ([Ransom.SamSam](#)) 的幕後集團，發現並刺探攻擊漏洞，透過網路散佈他們的惡意程式。
- 自我傳播：部分 Android 勒索軟體的行為類似病毒，會透過 SMS 擴散至所有聯絡人，而 2016 年則首見使用自我傳播的 Windows 勒索軟體。ZCryptor ([W32.ZCrypt](#)) 會感染所有抽取式磁碟機，在開始加密之前複製自己，提升擴散至其他電腦的機會。
- 第三方應用程式商店：部分行動裝置勒索軟體可能透過不受信任的第三方應用程式商店散佈。例如 [Android.Lockdroid.E](#) 就是在第三方應用程式商店，以色情影片播放器的方式出現。

#### 勒索軟體即服務的時代到來

2016 年勒索軟體活動增加的因素之一，就是勒索軟體即服務 (RaaS) 的出現，例如惡意程式開發人員建立的勒索軟體套件，即可輕易用來建立及自訂新型勒索軟體變種。開發人員通常會向攻擊者提供套件，並收取一定比例的利潤。

其中一項 RaaS 的案例是 Shark ([Ransom.SharkRaaS](#))，出現於 2016 年。Shark 透過自家的網站散佈，允許使用者自訂贖金和所要加密的檔案。款項會自動直接交付 Shark 的製作者，製作者拿取其中的 20%，然後將剩餘款項送交給攻擊者。

#### 全新技術：目標式攻擊和「自給自足」(living off the land)

雖然目前的勒索軟體攻擊大多為無差別攻擊，不過有證據顯示，攻擊者針對組織利用目標式攻擊的意圖持續提升。雖然數量遠不及大量郵件威脅，不過對受感染的組織而言，這可能造成毀滅性影響，導致數百台電腦遭到加密。

這種新型目標式攻擊最危險的範例之一，就是 SamSam ([Ransom.SamSam](#))。SamSam 鎖定的伺服器，通常執行於舊型的未修補社群版本 JBoss 應用程式伺服器。攻擊者使用可自由取得的工具，例如開放原始碼測試工具 JexBoss，識別有漏洞的伺服器。

一旦有一部伺服器遭到入侵，攻擊者就可能竊取憑證，並使用多種可公開取得的工具（例如 Microsoft Sysinternals 公用程式），在受害者的網路中周遊。發現適合感染的電腦時，攻擊者就會使用批次程序檔，在每台電腦部署 SamSam 及公開加密金鑰。程序檔也會由電腦刪除磁碟區陰影複本，讓電腦無法在感染之後回復任何檔案，另外，也會搜尋任何執行中的備份程序加以終止，並刪除任何發現的備份相關檔案。

SamSam 攻擊所用的技術較常見於網路間諜活動，並顯示出某些勒索軟體集團的專業程度。這類目標式攻擊雖然較難執行，但可能在受害組織中感染上千部電腦，造成大規模的破壞效果。

#### 其他平台現也出現漏洞

到目前為止，勒索軟體攻擊者大都鎖定 Windows 使用者，不過受威脅平台的範圍正逐漸擴大。目前已出現多種 Android 威脅，其中包括一款 Android 的加密勒索軟體，也就是俄語版 Simplocker ([Android.Simplocker](#)) 及其英語版變種 ([Android.Simplocker.B](#))。Android 裝置中，不只是行動裝置可能會受到勒索軟體侵襲。賽門鐵克研究發現，執行 Android 的智慧型電視也可能受到感染。

2016 年一種名為 KeRanger ([OSX.Keranger](#)) 的威脅，成為第一個廣泛散佈、鎖定 Mac 使用者的勒索軟體。KeRanger 透過破解版的 Transmission BitTorrent 用戶端安裝程式，在短期間內散佈。

有許多款勒索軟體變種不只是專為單一作業系統設計的威脅，而且還能使用 JavaScript 進行設計，亦即可感染多種平台，例如 [Ransom.Nemucod](#) 和 [Ransom.Ransom32](#)。

#### 執法單位破獲行動

2016 年的多場執法任務影響了一些規模較小的勒索軟體集團。荷蘭警方在 8 月查扣 WildFire 集團 ([Ransom.Zyklon](#)) 的指令和控制 (C&C) 基礎架構。

賽門鐵克於 12 月協助破獲 [Avalanche](#) 惡意程式主控網路，查扣犯罪組織使用的 39 台伺服器與數十萬個網域，這些設備散佈至少 17 種惡意程式系列，其中包括 [Trojan.Ransomlock.P](#) 勒索軟體。

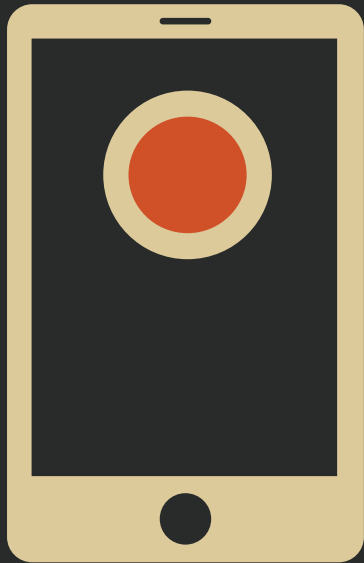
#### 延伸閱讀

- [2016 年勒索軟體及企業](#)
- [Locky 勒索軟體積極尋找受害者](#)
- [KeRanger：第一款 Mac OS X 勒索軟體](#)
- [SamSam 預示了目標式攻擊勒索軟體的新趨勢](#)

#### 最佳實務準則

- 新型勒索軟體變種會定期出現。請將安全軟體更新到最新版本，確保自己不受勒索軟體侵襲。
- 時常更新您的作業系統和其他軟體。軟體更新經常含有新發現安全漏洞的修補程式，這些漏洞將可能為勒索軟體攻擊者所利用。
- 電子郵件是其中一大感染途徑。刪除所有收到的可疑電子郵件，尤其內含連結和/或附件的郵件。
- 如果有任何 Microsoft Office 電子郵件附件建議您啟用巨集以檢視信件內容，請務必小心。除非您十分確信此封信件是真的，並且來源可靠，否則請不要啟用巨集，並馬上刪除信件。
- 為重要資料進行備份，這是打擊勒索軟體感染唯一的最有效方法。攻擊者透過加密受害者極有價值的檔案，並讓其無法存取，藉此對受害者予取予求。如果受害者有備份，只要確定清除感染，即可還原檔案。
- 使用雲端服務有助於減輕勒索軟體感染的影響，因為許多人會保留舊版檔案，可藉此「回復」到未加密的狀態。

# 最新攻防重點： 物聯網、行動裝置及 雲端環境威脅



章節

# 08



以數量上來說，攻擊傳統桌上型電腦和伺服器仍然主宰威脅情境，不過威脅行動者已經積極準備好鎖定其他平台。

普遍使用的行動裝置，以及主流採用的雲端和物聯網 (IoT) 技術，使得各種全新平台及使用者成為攻擊者鎖定的目標。2016 年可能會出現多種新興威脅，鎖定上述三項漸受矚目的領域。

## 物聯網

物聯網裝置安全剖析在 2016 年急速增加，這並不令人意外。賽門鐵克在 2015 年的 ISTR 報告中，就曾提過「物聯網內的危險因子」。不過當時很難預測物聯網及其安全性，在 2016 年最後一季獲得或缺少的關注程度。

其中原因只有一個，就是 Mirai。Mirai 傀儡網路是由物聯網裝置組成，直到 2016 年底，已發起許多知名的分散式阻斷服務 (DDoS) 攻擊事件。

判定究竟多少裝置受到 Mirai 感染十分困難，不過從許多數據看來，數量相當驚人。[Incapsula](#) 研究發現有將近 50,000 個獨一無二的 IP，主控受到 Mirai 感染的裝置，嘗試在其網路發動攻擊。[Level 3](#) 表示已經識別約 493,000 個 Mirai Bot 傀儡程式：發佈原始程式碼之前有 213,000 個，2016 年最後幾個月則有 280,000 個。

賽門鐵克於 2015 年底建立的物聯網 honeypot，能夠追蹤對物聯網裝置的攻擊嘗試。此誘捕帳號收集的資料顯示物聯網攻擊的動力來源，以及物聯網裝置在攻擊者眼中的堅固程度。

## 重要發現

- 從 2016 年 1 月到 12 月，賽門鐵克物聯網誘捕帳號的攻擊事件數量幾乎加倍成長。在 1 月時，平均每小時有將近 4.6 個獨一無二的 IP 位址攻擊 honeypot，到了 12 月平均則超過 8.8 次。在活動高峰時刻，也就是 Mirai 迅速擴展的時候，honeypot 每兩分鐘就會出現一次攻擊。
- 在 2016 年，物聯網裝置牽涉到史上最大規模的 DDoS 攻擊事件。法國主控公司 OVH 遭受攻擊，最高峰達到 1 Tbps，是史上最大規模的 DDoS 攻擊事件，主要是由 Mirai 傀儡網路發動。
- 預設密碼仍是物聯網裝置最大的安全漏洞。攻擊者最常嘗試的密碼為「admin」。

## 趨勢及分析

什麼是物聯網？在許多人的想像中，物聯網是智慧型恆溫控制器，或是回應語音指令的虛擬助理，不過物聯網主要是由各種常用裝置組成。像是家用路由器、數位錄影機及連網攝影機，這些裝置構成部分的物聯網，且是最常受到 Mirai 傀儡網路鎖定的目標。

傀儡網路就像是連網裝置的「傀儡大軍」，受到惡意程式感染，並在其擁有者不知情的狀況下，以團體方式遭到控制。攻擊者可使用遭到控制的裝置執行惡意活動，例如 DDoS 攻擊或垃圾郵件活動。物聯網裝置吸引傀儡網路作為目標的原因有三：

- 01 裝置製造商通常並未將安全性視為優先事項，導致各種不良實務作法，例如使用預設密碼及開放連接埠，而使用者不會或不能加以變更。
- 02 其中通常沒有內建機制接收自動韌體更新，造成沒有修補漏洞。
- 03 此外這類裝置安裝後通常就遭到遺忘。這代表其擁有者不瞭解裝置何時會被用於惡意用途，而且幾乎不願意套用韌體更新。

雖然 Mirai 的唯一目的是從事 DDoS 攻擊，不過一般相信無線路由器的惡意程式可竊取個人資訊，包括使用者名稱、密碼及金融資料。受感染的物聯網裝置，也可作為墊腳石，攻擊其他私有網路中的裝置。這也代表您的裝置，也可能成為全球傀儡網路的一份子，扮演攻擊網站或服務的角色。

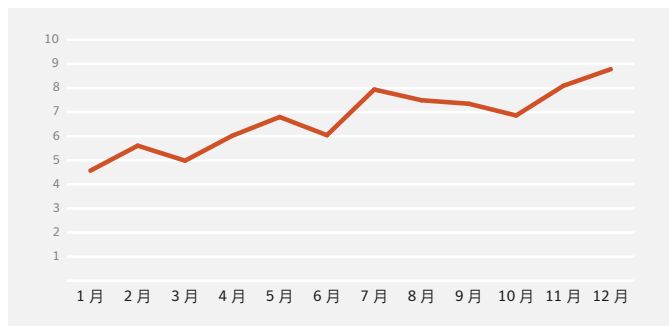


賽門鐵克於 2015 年建立的物聯網誘捕帳號 (honeypot)，能夠觀察對物聯網裝置的攻擊情形。Honeypot 是以開放路由器的形式出現，會記錄嘗試連線至系統的行為，並加以分析。在 2016 年 1 月至 12 月之間，鎖定誘捕帳號的獨特 IP 位址數量幾乎加倍成長。

在 1 月時，掃描誘捕帳號的獨特 IP，平均數量為每小時將近 4.6 個，12 月時則成長為平均 8.8 個以上。攻擊誘捕帳號的大部分 IP 為其他物聯網裝置。

### 每個月物聯網誘捕帳號每小時遭受的攻擊數量

從 1 月到 12 月，賽門鐵克誘捕帳號每小時遭受的攻擊數量明顯增加，在這一年期間幾乎加倍成長。



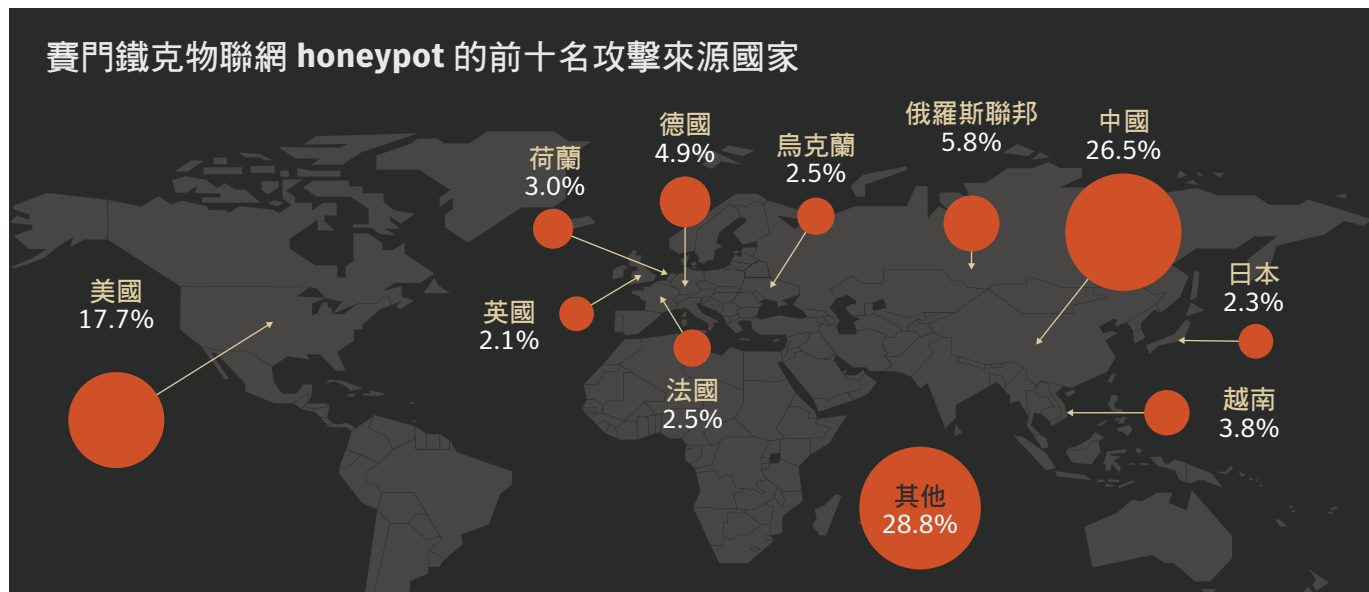
雖然 7 月到 10 月的趨勢略微下滑，但攻擊事件在 11 月及 12 月急遽上升。Mirai 傀儡網路的原始程式碼於 9 月最後一天公佈，可能對前述數據上升有所影響。

Mirai 原始程式碼是由名為 Anna-senpai 的使用者，於駭客活動討論區公佈。雖然無法斬釘截鐵確定 Mirai 的幕後主使者，但專門報導安全性議題的記者 Brian Krebs (首批傀儡網路受害者之一)，撰寫了一篇[詳細文章](#)，說明他調查 Anna-senpai 身分的結果。

10 月 21 日對 DNS 供應商 Dyn 發動的大規模攻擊，獲得廣泛的媒體關注，並提升了 Mirai 的知名度。這個事件顯示，建立大型傀儡網路並破壞主要網站是多麼輕而易舉。目前尚未找出從事 Dyn 攻擊的犯罪者，不過一般認為這應該是所謂的「腳本小子」(script kiddies，是指自居駭客但技術有限的初學者)，而不是精密的駭客團體。Dyn 攻擊也向整個世界揭露 Mirai，而且根據後續的[媒體報導](#)，有所謂的「遊民駭客」(skid) 在駭客活動討論區要求教學資料，以便學習如何使用 Mirai 原始程式碼。

### 國家資料

分析誘捕帳號資料，也表示能夠判定誘捕帳號攻擊是源自哪些國家。



攻擊主要是來自中國 (26.5%) 及美國 (17.7%)，而俄羅斯 (5.8%)、德國 (4.9%) 及越南 (3.8%) 則為三至五名。

衡量各國情形的以上數據，是以攻擊裝置的 IP 位址為依據，這並不代表攻擊者本身位於這些國家。

## 密碼

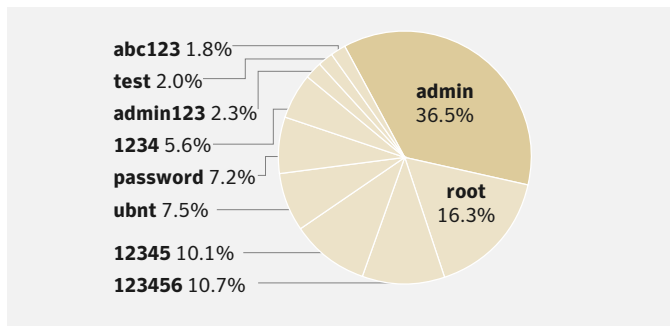
分析物聯網惡意程式嘗試登入裝置時使用的密碼後，結果並不令人意外，顯示物聯網裝置的預設使用者名稱及密碼通常從未變更。

其中有許多原因。部分物聯網裝置使用硬式編碼的使用者名稱及密碼，無法輕易變更。許多使用者可能不瞭解預設憑證的危險性，因此不太可能加以變更。

傳統的最佳實務準則規定，使用者應在所有物聯網裝置使用唯一的使用者名稱及密碼組合，而線上帳戶也應比照辦理。不過，除非製造商及供應商實施變更，強迫使用者選擇唯一密碼，則密碼仍將持續成為安全性漏洞。

## 嘗試登入賽門鐵克物聯網誘捕帳號最常使用的十大密碼

在登入賽門鐵克誘捕帳號時使用的十大密碼中，以預設密碼為主。



「Admin」(37%) 及「root」(16%) 是最主要用於登入賽門鐵克誘捕帳號的密碼，此外還有其他常見的「123456」、「12345」、「1234」及「password」等等。Ubiquiti 品牌路由器的預設密碼「ubnt」也名列前十名之中。Ubiquiti 路由器遭到鎖定，是因為 2016 年 5 月時，其路由器的舊有漏洞遭到揭露，可讓病蟲鎖定內嵌裝置，並在執行過期韌體的眾多 Ubiquiti 網路路由器中擴散。

雖然 Ubiquiti 於 2016 年中發佈韌體更新修補此項漏洞，病蟲仍然能在未下載更新韌體的裝置，刺探攻擊這項漏洞。

## Mirai 傀儡網路

如前所述，Mirai 這款傀儡網路在 Brian Krebs 網站進行大規模 DDoS 攻擊，因此於 9 月獲得大眾關注。該次攻擊高峰達到 620 Gbps，成為當時史上最大規模的 DDoS 攻擊。不過幾天後出現報導，表示先前法國主控公司 OVH 遭到的攻擊，高峰達到 1 Tbps。

不過，DNS 公司 Dyn 在 10 月遭到的 DDoS 攻擊，才真正讓 Mirai 成為熱門焦點。Dyn 攻擊事件破壞全球許多主要網站，包括 Netflix、Twitter 及 Paypal。

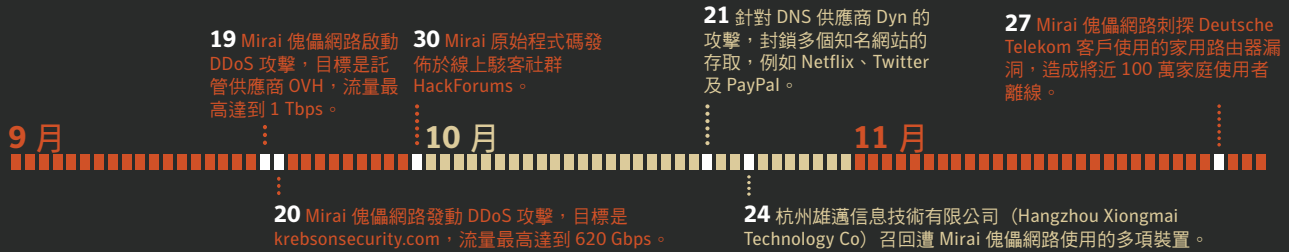
這次攻擊顯示使用物聯網裝置的 DDoS 攻擊極為強大，也開始讓各界質疑，如果攻擊者決定鎖定工業控制系統或重要國家基礎設施時，可能會發生什麼情形。

Mirai 的運作方式，是持續掃描可透過網際網路存取的物聯網裝置，且這些裝置都是使用工廠預設或硬式編碼的使用者名稱及密碼。之後 Mirai 會利用惡意程式進行感染，迫使裝置聽命於中央控制伺服器，使其成為 Bot 傀儡程式，從事 DDoS 攻擊。目前至少還有其他 17 種物聯網惡意程式系列，積極地侵害裝置。

Gartner 預測全球在 2020 年的物聯網裝置將超過 200 億個，因此解決安全性問題非常重要，否則將出現更大規模的 Mirai 及類似活動。此外，物聯網裝置的形象也可能改變。隨著連網汽車及連網醫療裝置逐漸普遍，攻擊者動機也可能隨之變化。

使用物聯網裝置攻擊，也降低了網路罪犯的入門門檻。對攻擊者而言，嘗試接手控制物聯網裝置時，需要克服的安全性問題少了許多。桌上型電腦或筆記型電腦通常都會安裝防毒軟體，並接收自動安全更新，但物聯網裝置的唯一保護措施，可能就是能夠輕易猜測的預設使用者名稱及密碼。就目前而言，安全性不佳的物聯網裝置，正讓網路罪犯的日子更輕鬆。

## ▼ Mirai 在 2016 年的破壞足跡



### 持續演進發展

Mirai 的原始程式碼在 9 月底公諸於世。如前所述，這是由名為 Anna-senpai 的使用者，於 9 月 30 日公布在 HackForums 駭客討論區。一如預期，原始程式碼公布之後，產生了其他 Mirai 變種。

到了 11 月底，一種 Mirai 變種在德國癱瘓將近 100 萬個家用網際網路使用者的存取能力。這種變種攻擊可由裝置遠端存取 TCP 連接埠 7547 的路由器，同時也會刺探攻擊 CPE WAN 管理通訊協定的漏洞。愛爾蘭公司 Eir 使用的相似路由器，在相同攻擊下可能也不堪一擊。

這款首次出現的變種，在原始程式碼公佈後兩個月內問世，可以合理假設這只是冰山一角。

### 展望未來

物聯網裝置數量持續成長，可能會讓各界更加要求制定物聯網產業法規，作為因應安全性問題的唯一方法。如果可以制定法規，接下來的問題就是：應該在產業層級實施，或是在政府層級實施？

總部位於美國的 Dyn 所遭受的 DDoS 攻擊，其主要是透過中國電子公司「雄邁信息技術有限公司」(XiongMai Technologies) 生產的網路攝影機執行，突顯了規範物聯網裝置的困難之處。

雖然沒有單一方式能夠修正如此複雜的問題，不過風險導向的基準安全性標準可作為一部分的解決方案。各國應考慮採取最低限度的安全性法規，特別是針對關鍵用途進行規範，以確保安全性成為物聯網設計及製造時的核心考量因素。

當然，市場上產品的安全性方面，製造商應扮演主導角色。他們應該提供消費者一定的透明度，瞭解物聯網裝置的安全性，以便在購買時做出明智決策。如此也可讓安全性成為裝置的固有特色，讓優質的製造商藉此基礎，打造出差異化產品。

無論如何，物聯網安全性將持續在 2017 年成為熱議話題。

### 最佳實務準則

- 在購買前研究物聯網裝置的能力和安全性功能。
- 請稽核要用於您網路的物聯網裝置。
- 變更裝置的預設憑證。為裝置帳號和 Wi-Fi 網路設定高強度的唯一密碼。不要使用「123456」或「password」等常見且容易猜測的密碼。
- 使用強化加密法設定 Wi-Fi 網路存取 (WPA2)。
- 許多裝置都有各種預設啟用的服務。請停用不需要的功能和服務。
- 儘可能停用 Telnet 登入而改用 SSH。
- 依據個人需求修改物聯網裝置的預設隱私權及安全性設定。
- 不需要時，應停用或保護物聯網裝置的遠端存取功能。
- 儘可能使用有線連線而非無線連線。
- 定期查看製造商網站的韌體更新。
- 確保硬體停機不會導致裝置處於不安全的狀態。

## 行動裝置

賽門鐵克發現行動裝置相關的惡意活動持續增加，這是因為網路罪犯使用經過測試且受信任的方法，能夠透過攻擊牟利。Android 仍然是最常受到鎖定的行動平台。不過在 2015 年受到的攻擊量暴增之後，隔年的攻擊成長率首次減緩，因為攻擊者正在整併勢力，試圖對付改良後的安全性架構。

### 重要發現

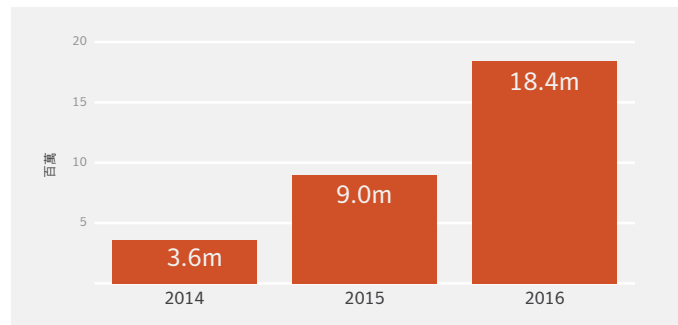
- Android 作業系統仍然是行動威脅的主要目標。不過，Android 架構的安全性經過強化，因此更難以感染行動電話，即使成功感染，也經常無利可圖。
- 針對 iOS 作業系統的攻擊事件仍然相當罕見。不過 2016 年 iOS 有三個零時差漏洞遭到刺探攻擊，這是由於 Pegasus 惡意程式發動目標式攻擊而感染了行動電話。
- 惡意 Android 應用程式的整體數量，在 2016 年大幅成長 105%。不過，相較於前一年惡意應用程式增加 152%，2016 年的成長率已經減緩。
- 賽門鐵克在 2016 年總共封鎖了 1,840 萬次行動裝置惡意程式的感染意圖。受賽門鐵克保護的行動裝置資料顯示，2016 年每 20 部裝置之中，就有一部曾遭蓄意攻擊而受感染。這項比例與 2015 年相近。

### 行動裝置惡意程式趨勢

行動裝置的整體威脅偵測數量 (包括賽門鐵克雲端技術的統計資料) 於 2016 年翻倍，共偵測到 1,840 萬個行動裝置惡意程式。不過即使越來越多人使用智慧型手機，2016 年 105% 的成長率仍遠低於前一年的 152%。這顯示行動威脅的態勢，正由爆炸性成長轉移到攻擊者整併勢力的階段，而他們也逐漸掌握 Android 採取的安全措施。

### 每年行動裝置惡意程式的整體偵測數量

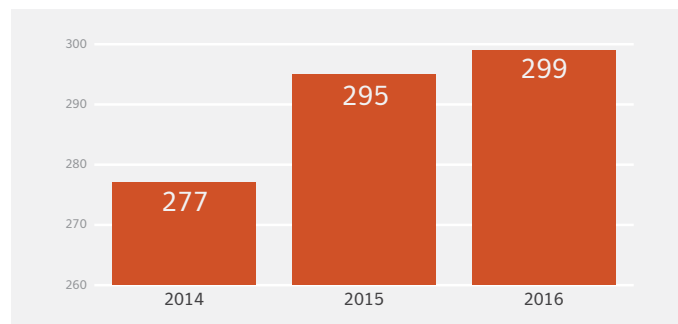
賽門鐵克 2016 年行動裝置惡意程式的偵測數量總計高達 1,840 萬，比 2015 年增加了 105%。



檢視各個類別的威脅系列，將可進一步證實攻擊者正在整併勢力。威脅系列是指將相同或類似的攻擊集團分為一組。賽門鐵克於 2016 年記錄了 4 種新的行動威脅系列，遠低於 2015 年的 18 個新系列。不過值得注意的是，諸如啟發式、機器學習及雲端偵測等新型偵測技術，大多傾向採取變種偵測的方式，可能無法揭露新系列的存在。深入分析行動威脅特性之後，發現 2016 年出現 61 種獨特的新型威脅叢集。相較於 2015 年發現 75 個叢集，這次下降幅度將近 19%，再次顯示行動威脅態勢成長或創新的速度趨緩。

### 每年行動裝置惡意程式系列的累計數量

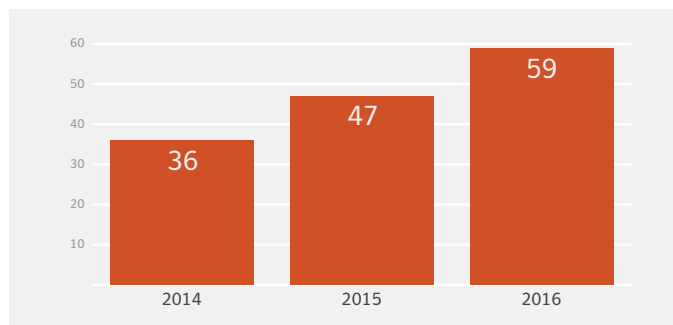
賽門鐵克在 2016 年發現四種新的行動裝置惡意程式系列，遠低於 2015 年發現的 18 種新系列。



深入探討各系列的個別威脅變種後，發現每個系列的惡意行動應用程式變種數量，在 2016 年成長 25% 以上，略低於 2015 年的 30%。

### 每個系列的行動惡意程式變種數量

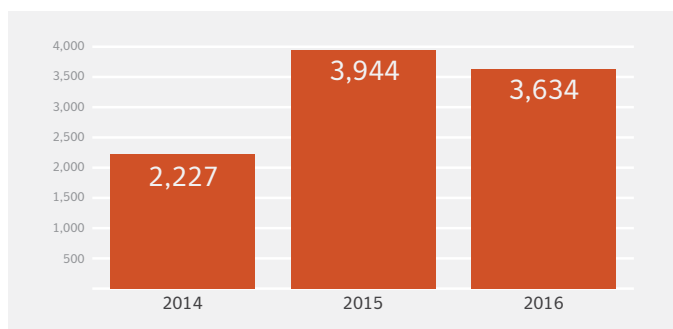
每個系列的行動惡意程式變種數量，在 2016 年成長 25% 以上，略低於 2015 年的 30%。



綜觀全局，偵測到的惡意行動應用程式變種整體數量略減，在 2015 年及 2016 年之間下滑 8%。在 2014 年及 2015 年間偵測到的惡意行動應用程式變種數量則大幅攀升，增加超過 75%。此年度的數據顯示，變種的活動量開始趨於穩定。

### 行動惡意程式變種逐年統計數量

2016 年遭偵測的行動惡意程式變種數量減少，顯示其中的活動量開始趨於穩定。



整體而言，由上可知攻擊者正在改善及修正現有惡意程式系列及類型，而不是開發新型獨特的威脅類型。

### 動機與技術

行動惡意程式的動機向來都是金錢，使用各種經測試過且受信任的方式牟利，例如傳送中獎簡訊、廣告點擊詐騙、勒索軟體等。

偵測到的惡意程式類型經分析發現，前兩名的 **Android.Malapp** 及 **Android.MalDownloader** 佔 2016 年總偵獲數量的一半以上。這些是透過變種偵測所發現，這種技術是用來偵測多種個別（但未經分類）的威脅。

偵測到的前十名中，最值得注意的是第三名 **Android.Opfake**。**Opfake** 可偵測傳送中獎簡訊的惡意程式，因為中獎簡訊一直是行動威脅攻擊者的金雞母。偵獲的第二個中獎簡訊則是第五名的 **Android.Premiumtext**。**Android** 作業系統已經新增警告訊息，會在中獎簡訊傳送時出現，讓威脅行動者更難隱藏其活動。前十名的其他惡意程式 (**Android.HiddenAds** 及 **Android.Fakeapp**) 使用點擊詐騙方法，以此牟利並規避警告訊息。

2016 年偵測到的前 20 名項目中，也出現用於散佈勒索軟體、或嘗試竊取受害者銀行交易資訊的惡意程式。

### 2016 年主要行動威脅

最常見的兩款行動裝置惡意程式偵測工具都是變種偵測名稱，用於封鎖各式各樣未分類的 **Android** 威脅。

行動威脅	百分比
Android.Malapp	39.2
Android.MalDownloader	16.1
Android.Opfake	5.2
Android.HiddenAds	4.8
Android.Premiumtext	4.1
Android.MalDropper	2.1
Android.Mobilespy	1.9
Android.Downloader	1.7
Android.Dropper	1.7
Android.Fakeapp	1.7
Android.Smsstealer	1.7
Android.Rootnik	1.6
Android.Lotoor	1.4
Android.SmsBlocker	1.4
Android.MobileSpy	1.3
Android.RegSMS	1.2
Android.FakeInst	1.2
Android.SMSblocker	0.9
Android.HiddenApp	0.8
Android.Lockdroid.E	0.8

## 惡意程式及灰色軟體比例

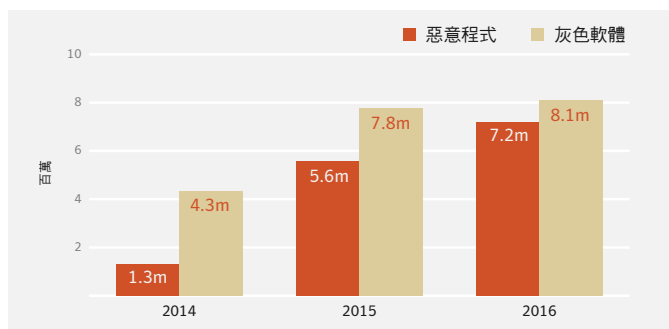
賽門鐵克會主動匯集整理含有灰色軟體或惡意程式的行動應用程式。

灰色軟體的程式並不包含惡意程式，也不具明顯惡意，但可能對使用者造成困擾及傷害，例如駭客工具、非法存取軟體、間諜程式、廣告程式、撥號木馬程式和惡作劇程式。

惡意程式及灰色軟體應用程式在 2014 及 2015 年間都顯著成長，不過兩者在 2016 年皆大致持平。灰色軟體在 2016 年僅增加 4%，惡意程式則增加約 29%，遠低於 2015 年增加的 300%。2016 年發現的灰色軟體及惡意程式數量則相去不遠。

### 2014-2016 年惡意程式及灰色軟體比例

惡意程式及灰色軟體在 2014 及 2015 年成長後，2016 年的數量持平。



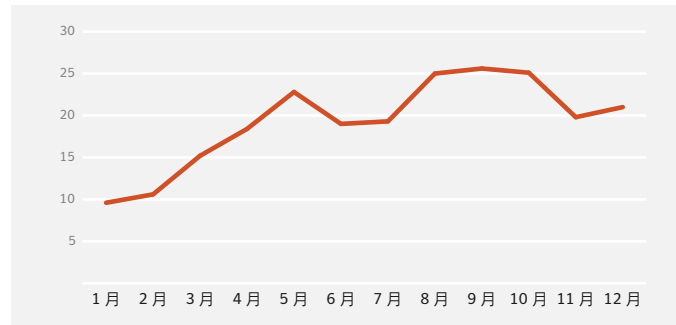
## 執行時期封裝工具增加

在威脅活動類型方面，雖然行動裝置攻擊者並未展現大幅創新，但他們採用的技術會提升感染成功率及壽命。越來越多行動裝置攻擊者採用執行時期封裝工具來隱匿惡意程式，這種作法從 2016 年初到年底幾乎翻倍。

執行時期封裝工具會讓惡意程式難以偵測，而且傳統惡意程式已使用此手法多年。這種手法可讓惡意應用程式重新封裝許多次而掩藏其惡意性質，然後再於執行時期部署其惡意活動。

## 現場惡意行動應用程式封包的比例

2016 年執行時期封裝工具的使用情形增加，從 1 月到 12 月之間成長超過一倍。



## 行動裝置漏洞

2016 年值得注意的變化，就是 Android 提報的行動裝置漏洞數量超越 iOS。這與前幾年的情形截然不同：過去 iOS 提報的行動裝置漏洞數量都遠超過 Android。這項變化的部分原因，可能是由於 Android 架構持續加強安全性，或是研究人員持續關注於行動平台。

## Android 架構的強化成果

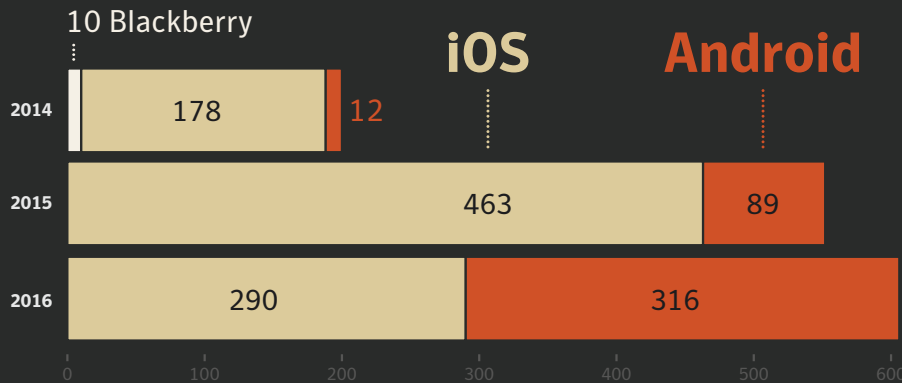
Android 持續修改其架構，以期提升安全性。這也對網路罪犯造成影響，使其難以成功在行動電話安裝惡意程式。即使成功在受害者行動電話安裝惡意程式，Android 的各種開發及強化成果，也讓攻擊者難以從中牟利。

賽門鐵克的資料顯示，網路攻擊者若要利用行動惡意程式賺錢，中獎簡訊仍是最有效的方式。不過 Android 4.2 (Jelly Bean) 在 2012 年進行更新，瓦解了當時十分猖獗的中獎 SMS 木馬程式攻擊。更新之後，如果有人嘗試傳來中獎訊息，該行動電話就會出現警示，大幅降低這類詐騙的效果。

Android 3.1 (Honeycomb) 於 2011 年採用的自動啟動限制功能，也形成了攻擊者的阻礙，因為封鎖了無聲自動啟動功能，讓木馬程式在沒有前端活動的情況下，無法無聲啟動。這種方式雖然有效，但攻擊者也另有對策來擺脫限制。

## 回報的行動裝置漏洞 (依據作業系統)

Android 2016 年回報的行動裝置漏洞數量超越 iOS。



此外，Android 5.0 (Lollipop) 及 Android 6.0 (Marshmallow) 發佈的部分更新，也讓攻擊者更難部署行動銀行交易惡意程式。行動銀行交易惡意程式會建立覆蓋植入程序，以釣魚方式攻擊目前執行的應用程式，但這些更新可以取代 `getRunningTasks()` API，讓惡意程式無法找到目前執行的作業。自此之後，攻擊者就尋找各種規避方式，試圖克服上述的額外安全措施。

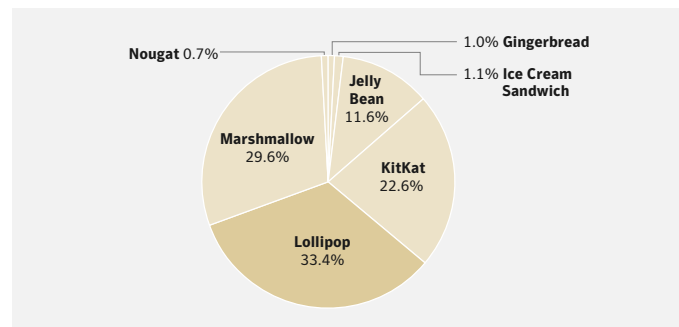
Marshmallow 更新也試圖解決行動勒索軟體的問題。更新後的全新權限模式，可讓勒索軟體編寫者難以鎖定 Marshmallow，而無法要求使用者向勒索軟體提供明確權限，並藉此鎖定裝置，然後順利啟動惡意程式。

雖然以上更新及安全強化成果令人欣慰，但是使用者必須能夠於裝置下載最新版的 Android，才能持續發揮效果，但情況並非總是如此。

有些製造商出產的手機從不安裝最新版的 Android，或是最新版發佈時間與手機上市時間的間隔過久。Android 本身的統計數據顯示，在 2017 年初，其最新版作業系統 Nougat 的市佔率非常低，因為尚未開放給 Google 生態系統以外的大部分手機使用。至於第二新的版本 Marshmallow 也不是市佔率最高的作業系統，前一代的 Lollipop 市佔率還高了 4%。缺乏更新的狀況，可能成為網路攻擊者的大好機會，鎖定過時的行動裝置作業系統下手。

### 2017 年 1 月 Android 不同版本的市佔率

Android 最新版作業系統 Nougat 市佔率非常低。



多數人仍然使用舊版作業系統，代表攻擊者不需更新舊有技術，即可持續發動攻擊，即使無法攻擊最新作業系統也無妨。

這可能是行動裝置攻擊者很少進行更新或繼續擴張的部分原因，因為他們的運作模式仍然有效。

## Apple 的痛處

針對 iOS 設計的惡意程式並不多。不過在 2016 年 8 月，iOS 發現三個零時差漏洞 (名為 Trident) 遭到目標式攻擊的刺探攻擊，企圖將 Pegasus 惡意程式植入受害者手機。Pegasus 是一種間諜程式，可存取訊息、電話及電子郵件，也可從應用程式收集資訊，包括 Gmail、Facebook、Skype 及 WhatsApp 等程式。

這種攻擊是透過簡訊，將連結傳送給受害者。如果受害者點擊連結，手機就會遭到 JB 破解，Pegasus 就可入侵從事間諜活動。

其中一個可供攻擊的漏洞位於 Safari WebKit，如果使用者點選連結，核心就會洩漏資訊，造成核心記憶體損毀，進而遭到 JB 破解，讓攻擊者入侵裝置。

這類攻擊是一位人權倡議人士收到可疑簡訊後，將手機交給 Cirizen Lab 而曝光。以上漏洞似乎只在少數的目標式攻擊中遭到刺探攻擊。

Pegasus 是由以色列公司 NSO Group 開發的間諜程式，據說這家公司只向各國政府銷售軟體。Apple 在 iOS 版本 9.3.5 修補了這三個漏洞。

這次攻擊顯示雖然 iOS 遭受的攻擊相當少，但系統並非無懈可擊。

## 最佳實務準則

- 讓您的軟體維持在最新狀態。
- 請不要由不熟悉的網站下載應用程式，只能由信賴來源安裝應用程式。
- 特別留意應用程式請求的權限。
- 安裝適當的行動安全應用程式，例如諾頓產品，以保護您的裝置與資料。
- 經常備份重要資料。

## 雲端

企業及消費者使用雲端已成主流趨勢，自然也吸引更多攻擊者。雖然雲端攻擊仍處於剛起步的階段，但 2016 年發生首次造成大規模雲端服務中斷的阻斷服務 (DoS) 攻擊，這警示了雲端服務有多麼容易遭受惡意攻擊。

## 重要發現

- 企業廣泛採用雲端應用程式，以及具有高度風險的使用者行為 (企業可能根本沒意識到)，都讓雲端攻擊的範圍持續擴大。2016 年底，企業組織平均使用 928 個雲端應用程式，高於年初的 841 個。不過大多數的資訊長 (CIO) 都認為自家組織只使用 30 或 40 個雲端應用程式。
- Symantec CloudSOC 分析發現，所有的不明資料 (未經 IT 同意或知情而儲存於雲端的商業資料) 當中，有 25% 受到「廣泛共用」，而提高了曝光的風險。在這「廣泛共用」的資料中，有 3% 涉及法規遵循事務。
- 2016 年多起知名的攻擊和活動，都將目標鎖定雲端相關服務，其中包括 Mirai 傀儡網路對 DNS 供應商 Dyn 發動的分散式阻斷服務 (DDoS) 攻擊，以及雲端服務託管的 MongoDB 資料庫所遭受的攻擊事件。

## 趨勢及分析

Symantec CloudSOC 在 2016 年下半年收集的資料顯示，雲端應用程式及服務的使用和濫用，以及藉此分享和儲存的資料，都在逐漸增加。

分析對象包括 2 萬個以上的雲端應用程式、1.76 億份雲端文件，以及 13 億封電子郵件。從中發現，企業平均使用 928 個雲端應用程式，比 2016 年上半年的 841 個增加了 87 個。

以上數據看似非常大量，然而請謹記，其中包括各式各樣的常用服務，例如 Office 365、Google、Dropbox，以及 Salesforce 等所有雲端應用程式。事實上，Office 365、Google 及 Dropbox 在 2016 年的上、下半年，都是企業最常採用及使用的前三名協同合作應用程式。



## 企業最常使用的雲端應用程式

企業內部的系統平均使用 928 個雲端應用程式，不過大部分資訊長認為自家公司只使用 30 或 40 個。

協同合作	
2016 上半年	2016 下半年
Office 365	Office 365
Google	Google
Dropbox	Dropbox
Box	Evernote
Evernote	Box
業務輔助	
2016 上半年	2016 下半年
Salesforce	GitHub
GitHub	Salesforce
Zendesk	Zendesk
ServiceNow	ServiceNow
Amazon Web Services	Amazon Web Services
個人用戶	
2016 上半年	2016 下半年
Facebook	Facebook
Twitter	LinkedIn
LinkedIn	YouTube
YouTube	Twitter
Pinterest	Pinterest

若缺乏雲端服務的使用政策及程序來規範組織內部使用者，雲端應用程式的使用風險將會提高。這項分析發現，大部分資訊長認為自家組織只使用 30 或 40 個雲端應用程式，但大部分企業平均採用 928 個，兩項認知之間差距超過 2000%。

Symantec CloudSOC 分析發現，所有的不明資料 (未經 IT 同意或知情而儲存於雲端的商業資料) 當中，有 25% 受到「廣泛共用」，亦即是在內部、外部或公開分享。

更令人擔憂的是，這 25% 廣泛共用的資料中，有 3% 含有法規遵循相關資料，例如個人識別資訊 (PII)、支付卡資訊 (PCI) 或受保護的醫療資訊 (PHI)。如果以上機密資料外洩，受害公司可能必須面臨嚴重的法規遵循罰款並負擔補救成本。限制員工只

能使用 Office 365 及 Box 等安全且熱門的檔案分享應用程式，並無法充分降低員工濫用資料或駭客入侵帳戶的相關風險。執行各種智慧型雲端資料治理實務，例如識別、分類及監控所有雲端資料的使用情形，是預防資料遺失的關鍵重點。

令人擔憂的是，Symantec CloudSOC 發現雲端中有 66% 的高風險使用者活動，皆顯示出洩漏資料的意圖。蓄意洩漏資料的跡象包括：經常性的分享帳戶、大量下載以及預覽文件等行為。頻繁地預覽文件之所以是洩漏活動的徵兆，在於攻擊者可從螢幕擷圖中取得資料。使用者行為分析 (UBA) 不但是識別高風險使用者的關鍵，也可識別及預防刺探攻擊的活動，例如資料洩漏、資料破壞及帳戶入侵等。

### 高風險業務

組織及其員工使用雲端服務的情形增加，表示公司的資料治理成效降低，並容易受到組織外的漏洞所影響。

這可能造成非常嚴重的後果。賽門鐵克分析發現，有 76% 的網站含有漏洞，其中 9% 屬於重大漏洞。我們將在「[網路攻擊](#)」一章詳細探討這項統計數據。

先前在本章「物聯網」一節介紹的 Dyn 攻擊事件，就說明了攻擊者如何鎖定單一組織，卻能波及大量企業的服務，其中包括 Amazon Web Services、SoundCloud、Spotify 及 GitHub。這突顯出企業使用雲端服務時所承擔的風險。

### 危險的勒索軟體

多起針對雲端服務的勒索軟體攻擊事件，都顯示了雲端資料多麼容易遭受網路犯罪攻擊。近期的知名個案，就是[成千上萬的 MongoDB 開放原始碼資料庫遭到劫持並勒索贖金](#)。這起資安事端起因於使用者在預設組態的設定中，讓舊型 MongoDB 資料庫維持開啟狀態。

雖然 MongoDB 本身沒有安全漏洞，公司也已警告使用者這項問題，但線上仍有無數舊型實作未套用最佳安全性實務準則，據報有超過 27,000 個資料庫遭到劫持。這類攻擊突顯使用者必須維持警戒，確保自己使用的任何開放原始碼軟體安全無虞。

2016 年初曾有報告指出，加州一間企業透過受管雲端解決方案公司來營運所有業務。結果其中一位員工開啟垃圾電子郵件後，全公司都無法存取儲存於雲端的 4 千多個檔案，

使該公司成為勒索軟體 TeslaCrypt ([Ransom.TeslaCrypt](#)) 的受害者。還好雲端供應商每天都有備份，不過仍花費一週時間才回復公司檔案。這只是勒索軟體對企業造成重大干擾的其中一個例子。

### 物聯網與雲端：網路犯罪的潛在共犯

急著讓所有裝置上線，通常表示事後才會考慮安全性問題。CloudPets 這款有連網功能的泰迪熊產品，就是很明顯的例子。Spiral Toys 的 CloudPets 是一款絨毛布偶，可讓孩童與父母錄下訊息，並透過網際網路交流。不過研究人員 [Troy Hunt](#) 發現，該公司將客戶資料儲存於未受保護的 MongoDB，可輕易在線上搜尋取得。這起事件暴露了 80 萬筆以上的客戶憑證，包括電子郵件及密碼，以及超過 200 萬則的錄製訊息。Hunt 表示，雖然憑證受到 Bcrypt 的安全雜湊功能保護，但仍有大量密碼強度不足，可能遭到解密。

這個例子說明，物聯網結合雲端之後，是多麼容易將客戶資料置於風險之中。許多物聯網裝置會蒐集個人資料，並仰賴雲端服務，將其儲存於線上資料庫中。如果資料庫不夠安全，客戶的隱私和安全也隨之面臨風險。

### 自給自足 (living off the land)

雲端服務的用量增加，也催生了本報告另外探討的一項趨勢，就是攻擊者採用「自給自足」(living off the land) 策略，而不是自行開發專屬的攻擊基礎架構。

2016 年最著名的兩項個案，就是 [希拉蕊柯林頓 \(Hillary Clinton\)](#) 競選總幹事 John Podesta 的 Gmail 帳戶以及 [世界反運動禁藥組織 \(World Anti-Doping Agency; WADA\)](#) 遭駭，兩者都是因為使用雲端服務而造成。攻擊者透過社交工程的手法取得了 John Podesta 的 Gmail 密碼。此外，據傳攻擊者也利用雲端服務來洩漏失竊資料，而並未特地建置一套自訂的基礎架構。這兩起知名事件將於「[目標式攻擊](#)」的章節詳細介紹。

雲端對於攻擊者頗具吸引力 (視其使用方式和組態而定)，這種環境有利於攻擊者略過本機安全措施；相較於本機伺服器儲存的資料，放在雲端的資料更容易竊取。鎖定雲端服務下手，攻擊者也能以極小的代價，造成最大的破壞，就像 DNS 供應商 Dyn 遭遇的 DDoS 攻擊那樣。

隨著雲端服務日漸普遍，可合理推斷這類服務將更常遭受攻擊。

### 延伸閱讀

2016 半年期《[影子資料報告](#)》：企業的協作程度、安全性和雲端用量均空前大幅提升

### 最佳實務準則

- 刪除任何可疑的電子郵件，尤其是含有連結或附加檔案的郵件。
- 如果有任何 Microsoft Office 電子郵件附件建議您啟用巨集以檢視信件內容，請務必小心。除非您十分確信此封信件是真的，並且來源可靠，否則請不要啟用巨集，並馬上刪除信件。
- 留意您使用的任何開放原始碼軟體是否發佈任何更新或修正程式。軟體更新經常含有新發現安全漏洞的修補程式，而且這些漏洞可能為攻擊者所利用。
- 請確保您使用的雲端服務會定期備份檔案，確保可因應遭勒索軟體綁架的不時之需。
- 在您的企業中實作智慧型的資料治理實務，確切掌握儲存於雲端服務的商業資料。

---

**參與人員****團隊**

Kavitha Chandrasekar  
Gillian Cleary  
Orla Cox  
Hon Lau  
Benjamin Nahorney  
Brigid O Gorman  
Dick O'Brien  
Scott Wallace  
Paul Wood  
Candid Wueest

**撰寫人**

Shaun Aimoto  
Tareq AlKhatib  
Peter Coogan  
Mayee Corpin  
Jon DiMaggio  
Stephen Doherty  
Tommy Dong  
James Duff  
Brian Fletcher  
Kevin Gossett  
Sara Groves  
Kevin Haley  
Dermot Harnett  
Martin Johnson  
Sean Kiernan  
Bhavani Satish Konijeti  
Gary Krall  
Richard Krivo  
Yogesh Kulkarni  
Matt Nagel  
Gavin O'Gorman  
John-Paul Power  
Nirmal Ramadass  
Rajesh Sethumadhavan  
Ankit Singh  
Tor Skaar  
Dennis Tan  
Suyog Upadhye  
Parveen Vashishtha  
William Wright  
Tony Zhu

## 關於賽門鐵克

賽門鐵克公司 (NASDAQ : SYMC) 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。

同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。若想瞭解更多資訊，請造訪 [www.symantec.com.tw](http://www.symantec.com.tw)。


## 更多資訊

賽門鐵克全球網站：<https://www.symantec.com/zh/tw>

ISTR 及 Symantec 情報資源：<https://www.symantec.com/zh/tw/security-center/threat-report>

Symantec 安全中心：[https://www.symantec.com/zh/tw/security\\_response/](https://www.symantec.com/zh/tw/security_response/)

Norton 安全中心：<https://tw.norton.com/security-center>



台灣賽門鐵克股份有限公司  
地址：台北市信義路五段 7 號  
台北 101 大樓 13 樓 A 室

電話：(02) 8726-2000  
傳真：(02) 8726-2199

[symantec.com/zh/tw](http://symantec.com/zh/tw)

Copyright © 2017 Symantec Corporation. 版權所有 © 2017 賽門鐵克公司。

All Rights Reserved. 保留所有權利。Symantec、Symantec 標誌和打勾標誌是賽門鐵克公司或其子公司在美國及其他國家或地區的商標或註冊商標。其他名稱可能是其各自擁有者的商標。

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。

**04/17**