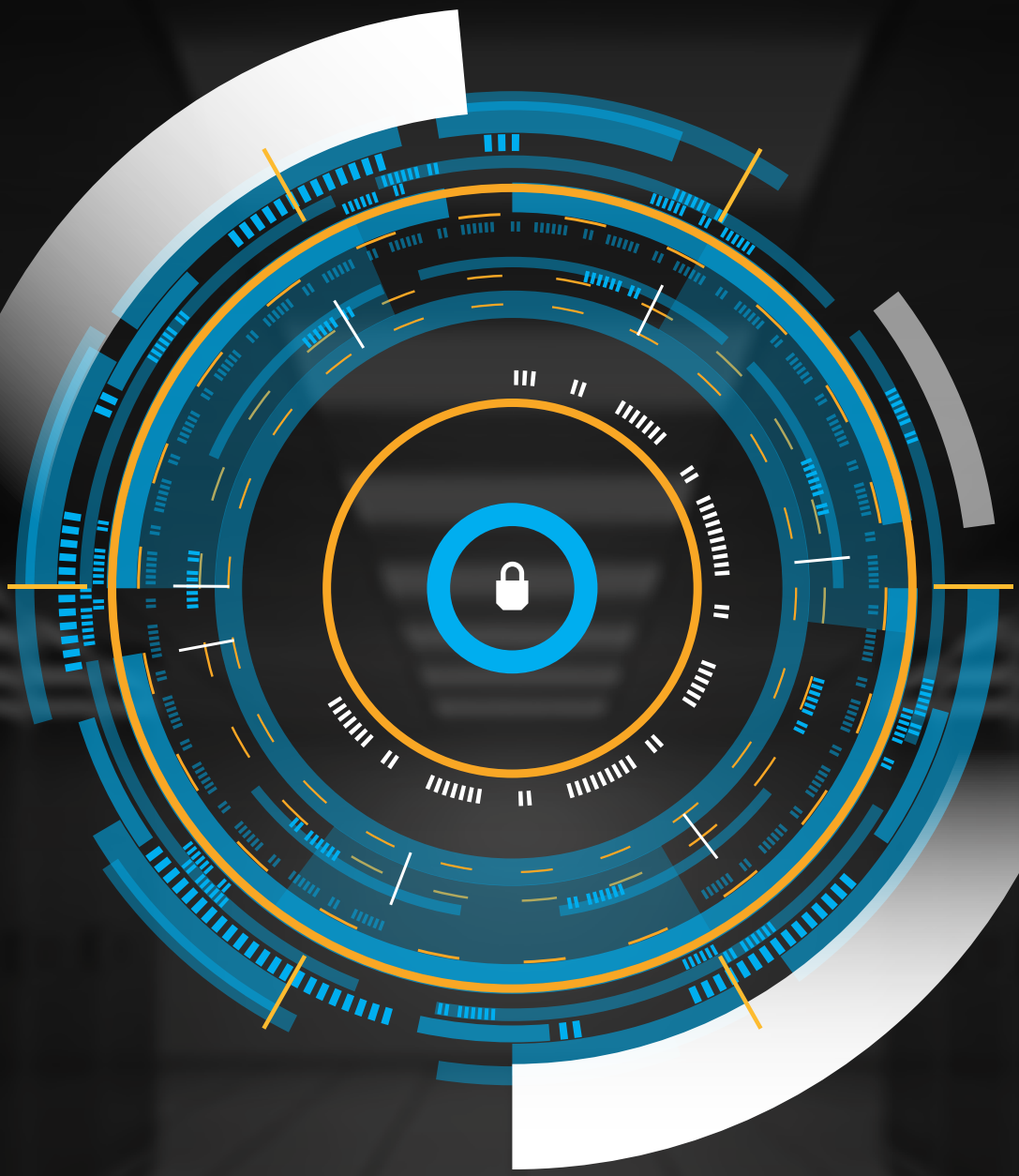


ISTR

網路安全威脅研究報告

第 21 期，2016 年 4 月發佈

Symantec

目錄

圖表和表格

簡介

透過賽門鐵克全球智慧型網路(Symantec™ Global Intelligence Network)，賽門鐵克已建立全球最完善的網路威脅資料來源之一，由超過 6380 萬個攻擊偵測器所組成，並每秒記錄數千個事件。透過結合賽門鐵克產品和服務（例如 Symantec DeepSight™ Intelligence、Symantec™ Managed Security Services、Norton™ 消費性產品，以及其他協力廠商資料來源），本網路會監控超過 157 個國家和區域中的威脅活動。

此外，賽門鐵克維護全球最完善的漏洞資料庫之一，目前包含超過 74,180 個已記錄漏洞（跨越 20 年以上）。這些是來自於超過 23,980 家廠商的 71,470 個以上的產品。

垃圾郵件、網路釣魚及惡意程式資料是透過各種來源擷取，包括「賽門鐵克探測網路」(Symantec Probe Network)，這是一個包含超過 500 萬個誘捕帳號、Symantec.cloud 及許多其他賽門鐵克安全技術的系統。Skeptic™，亦即 Symantec.cloud 專利啟發式技術，能夠在新型且精密的目標式威脅抵達客戶的網路前，先行偵測到它們。每個月已處理超過 90 億個電子郵件訊息，以及在 13 個資料中心的每日篩選後有超過 18 億個網路請求。透過廣大的反詐騙企業社群、安全廠商及超過 5200 萬位消費者及 17500 萬個端點，賽門鐵克也收集網路釣魚資訊。

「賽門鐵克網站安全」鞏固超過全球 100 萬部 Web 伺服器的安全，自 2004 年起達到 100% 的可用性。驗證基礎架構每天會處理超過 60 億個「線上憑證狀態通訊協定」(Online Certificate Status Protocol，簡稱 OCSP) 查詢。這是用來取得全球的 X.509 數位憑證的撤銷狀態。Norton™ Secured Seal 每天幾乎會在 170 個國家的網站上、以及在已啟用之瀏覽器的搜尋結果中顯示 10 億次。

這些資源讓賽門鐵克分析師擁有了無與倫比的資料來源，可藉此辨識、分析，並且針對攻擊、惡意程式碼活動、網路釣魚及垃圾郵件等新興趨勢，提供具參考價值的意見。請參閱年度賽門鐵克網路安全威脅研究報告中的結果。這提供了企業、小型企業及消費者至關重要的資訊，在現在和未來有效確保系統的安全。

內容摘要

簡介

賽門鐵克在 2015 年發現超過 4 億 3,000 萬個全新獨特的惡意程式，與前一年相較增加 36%。但也許其中最值得探討之處，是在於這些數字已不再讓我們感到驚訝。隨著現實生活與虛擬世界之間的界線日漸模糊，網路犯罪也成為我們日常生活的一部分。針對企業和國家發動的攻擊，屢屢成為新聞頭條，光是看到網路威脅的數量和成長速度，我們已經沒有太多感覺。

大多數的威脅報告都只接觸到威脅態勢的表面，而賽門鐵克涵蓋的資料廣度則能讓網路安全威脅研究報告 (ISTR) 深入檢視多個面向，包括目標式攻擊、智慧型手機威脅、社交媒體詐騙與物聯網 (IoT) 漏洞，以及攻擊者的策略、動機與行為。雖然威脅態勢的全貌中有許多值得探究之處，不過在 2015 年當中，以下六點重要發現是特別值得注意的趨勢。

在 2015 年當中，平均每週都有新的零時差漏洞被發現

進階攻擊團體仍然透過瀏覽器及網站外掛程式中未曾發現過的漏洞，持續獲得不法利益

在 2015 年，發現的零時差攻擊漏洞增加了兩倍多，來到 54 個，比前一年成長了 125%。換言之，在 2015 年平均每週都會發現一個新的零時差攻擊漏洞。2013 年，零時差漏洞的數量 (23) 比前一年度增加兩倍。到了 2014 年，漏洞的數量保持相對穩定的 24 個，因此我們做出了到達停滯期的結論。這個理論不久就被推翻。零時差漏洞在 2015 年的激增，再次確立它們在有利可圖的目標式攻擊中扮演關鍵角色。

想想這些漏洞背後所代表的價值，也就不難想見為爭奪此需求大餅的市場便隨之而生。事實上，以零時差漏洞的發現速率看來，它們有可能成為商品化的產品。目標式攻擊團體在漏洞曝光前會利用它們大肆犯案，之後便棄置不顧，轉而投向新發現的漏洞。當 Hacking Team 在 2015 年曝光時，他們的產品組合中至少有六種零時差攻擊，而這也確立了我們在追緝零時差攻擊時歸納出的職業化特徵。

幾乎所有類型的軟體都可能會有漏洞，不過對目標式攻擊來說，最具有吸引力的是普及率高的軟體。大多數的漏洞一再地在 Internet Explorer 與 Adobe Flash 之類的軟體中現身，原因就是因為這些軟體是廣大消費者與專業人員每天都會使用的軟體。2015 年使用頻率最高的五個零時差漏洞中有四個是 Adobe Flash。發現零時差漏洞後，網路罪犯會迅速地將它們加入工具組並伺機發動攻擊。在現階段，倘若沒有修補程式或如果使用者沒有及早套用修補程式，將會有數百萬使用者遭到攻擊，而受感染的人數也會高達數十萬名。

在 2015 年當中，有超過 5 億筆個人資料失竊或遺失

未完整報告自身資料外洩情況的企業數目也再創新高

2015 年底發生了公開報導以來最大規模的資料外洩事件。遭到洩露的記錄達到驚人的 1 億 9,100 萬筆。這種情況或許已經成為可觀的超大型資料外洩案例，但絕非個案。據報導，在 2015 年，總共有九起創記錄的超大型資料外洩事件發生。(超大型資料外洩事件的定義為一次外洩超過 1000 萬筆記錄的事件。)

根據報告，遭洩露的身分資料總數激增了 23%，攀升至 4 億 2,900 萬筆資料。但在這個數字背後，隱藏著更多內情。在 2015 年，有越來越多的企業選擇隱匿資料外洩的程度。選擇不回報資料外洩記錄數量的企業增加了 85%。賽門鐵克保守估計，加上未回報的資料洩漏事件，遺失的記錄數量應超過五億筆。

企業傾向選擇隱瞞外洩事件的重要詳細資料，確實是個令人感到不安的趨勢。透明公開是安全的不二法門。當前的安全產業有許多資料共用計劃正如火如荼地進行中，雖然這些計劃能協助我們改善安全產品與安全態釋，不過有些資料卻日漸難以收集。

四分之三的熱門網站中潛藏著重大的安全漏洞，足以讓所有人都暴露在風險當中

網頁系統管理員還在苦苦追趕修補程式的腳步

2015 年，每天都有超過一百萬次對使用者發起的網路攻擊。許多使用者相信，造訪知名的合法網站能讓他們遠離線上犯罪。事實不然。由於網頁系統管理員無法持續確保網站安全，利用合法網站的漏洞來感染使用者仍是網路罪犯的一貫伎倆。在所有合法網站中，有超過 75% 的網站存在未修正的漏洞。有 15% 的合法網站存在認定為「重大」的漏洞，這表示網路罪犯不費吹灰之力就能存取網站，並利用網站遂行其犯罪目的。網頁系統管理員應該要重振旗鼓，採取更積極的措施來因應風險。

在 2015 年，專門針對員工的魚叉式網路釣魚活動增加了 55%

網路攻擊者正針對大型企業發動持久戰

在 2015 年，曾遭受一次攻擊的政府組織或金融企業，預估在這一年中，很可能至少還有三次機會會被再當成攻擊目標。整體來說，曾遭受網路攻擊的大型企業中平均每家企業會被成功攻擊 3.6 次。

在過去五年內，我們觀察到鎖定員工人數少於 250 名之企業的攻擊數量呈現穩定增加，而在 2015 年，鎖定小型企業的攻擊數量總共佔了 43%，這證明各種規模的公司均暴露在風險中。

由此可知，無論是財星前 500 大企業或國家，都得承受智慧財產遭竊的風險，甚至連地方的洗衣店都有可能成為目標。舉例來說，有個聘僱 35 名員工的企業曾是競爭對手網路攻擊的受害者。競爭對手潛藏在他們的網路中兩年，藉由竊取客戶和價格資訊來獲取鉅額利益。這就是所有企業都可能淪為目標式攻擊的受害者之明確警告。事實上，專門針對員工的魚叉式網路釣魚活動增加了 55%。沒有任何企業能置身事外。對於單純以利益為出發點的攻擊者，他們的精密技術與嚴密組織足以媲美任何以民族國家做為後盾的攻擊者。藉由竊取資訊來操作股市的 Butterfly 團體就是一例。

勒索軟體在 2015 年成長了 35%

網路罪犯正使用加密工具做為武器，將公司與個人的重要資料當做人質

勒索軟體仍不斷地演進。去年，我們發現加密型勒索軟體 (加密檔案) 迫使較不具傷害力的鎖定型勒索軟體 (鎖定電腦畫面) 退出江湖。加密型勒索軟體在 2015 年成長了 35%。勒索軟體是一種可賺取暴利的攻擊類型，未來勢必會繼續引誘更多個人電腦使用者，並擴展至任何上網裝置，以此作為把柄換取利潤。在 2015 年，勒索軟體發現新目標，它們將重心從個人電腦移至智慧型手機、Mac 及 Linux 系統。同樣在 2015 年，賽門鐵克甚至示範了針對智慧型手錶和電視的概念證明攻擊。

賽門鐵克攔截了 1 億起冒用技術支援進行詐騙的案件

網路詐騙罪犯會設法讓您打電話給他們，並且乖乖地交出現金

儘管勒索軟體的威脅聲勢不斷壯大，但畢竟它們不是我們唯一面對的威脅。隨著人們從事線上活動的時間越來越長，攻擊者也在藉機尋找誘騙受害者的新方法。賽門鐵克率先在 2010 年舉報的假冒技術支援詐騙案件，已經從隨機打電話給容易輕信的受害者，進展到誘騙受害者自己直接打電話上門。

攻擊者透過警告使用者發生嚴重錯誤或問題的彈出式視窗來誘騙使用者，操控被害人撥打免付費電話號碼，再假藉「技術支援代表」的身分企圖賣給被害人無用的服務。在 2015 年，賽門鐵克就封鎖了一億起這種類型的攻擊事件。

攻擊者不斷尋找新方法，試圖利用可從線上竊取的資料獲利。去年 Netflix 進軍多個國家/地區，此舉吸引了攻擊者的注意。賽門鐵克研究人員發現，有人在黑市販售合法 Netflix 帳戶的登入資訊與密碼。這些帳戶存取資訊是透過網路釣魚或惡意程式竊取而來的。當然，在黑市轉售帳戶存取資訊已不是新鮮事。賽門鐵克不斷地在黑市看到販售竊取得來的飯店獎勵、航空公司飛行哩程點數及遊戲帳戶的廣告。

大數據

外洩

洩漏事件總數

2013	2014	2015
253	312	318
–	+23%	+2%

身分資料外洩超過 1 千萬筆的漏洞

2013	2014	2015
8	4	9
–	-50%	+125%

已外洩身分資料總數

2013	2014	2015
552M	348M	429M
–	-37%	+23%

每個外洩的身分資料平均數

2013	2014	2015
2.2M	1.1M	1.3M
–	-49%	+21%

每個外洩的身分資料中間值

2013	2014	2015
6,777	7,000	4,885
–	+3%	-30%

電子郵件威脅、惡意程式及傀儡網路

整體垃圾郵件比率

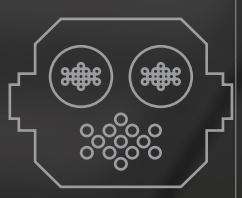
2013	2014	2015
66%	60%	53%
–	減少 6 個百分點	減少 7 個百分點

電子郵件網路釣魚比率 (非魚叉式網路釣魚)

2013	2014	2015
每 392 個就有 1 個	每 965 個就有 1 個	每 1,846 個就有 1 個

電子郵件惡意程式比率 (整體)

2013	2014	2015
每 196 個就有 1 個	每 244 個就有 1 個	每 220 個就有 1 個



傀儡網路數量

2013	2014	2015
2.3M	1.9M	1.1M
–	-18%	-42%

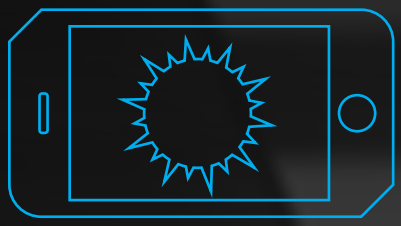
全新惡意程式變種 (每年新增)

2014	2015
317M	431M
–	+36%

加密型勒索軟體總數

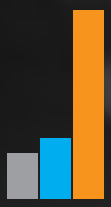
2014	2015
269K	362K
–	+35%
每天平均數 737	每天平均數 992

行動裝置



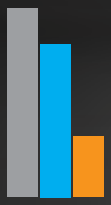
全新的行動漏洞

2013	2014	2015
127	168	528
–	+32%	+214%



全新的 Android 行動惡意程式系列

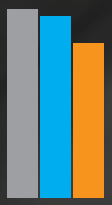
2013	2014	2015
57	46	18
–	-19%	-61%



全新的 Android 行動惡意程式變種

2013	2014	2015
3,262	2,227	3,944
–	-32%	+77%

漏洞



全新漏洞

2013	2014	2015
6,787	6,549	5,585
–	-4%	-15%

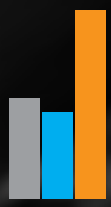
零時差漏洞

2013	2014	2015
23	24	54
–	+4%	+125%

網頁

每日攔截到的網頁攻擊數量

2013	2014	2015
569K	493K	1.1M
–	-13%	+117%



經掃描發現漏洞的網站...

2013	2014	2015
77%	76%	78%
–	減少 1 個百分點	增加 2 個百分點

...其中至關重要的百分比

2013	2014	2015
16%	20%	15%
–	增加 4 個百分點	減少 5 個百分點

發現含惡意程式的網站

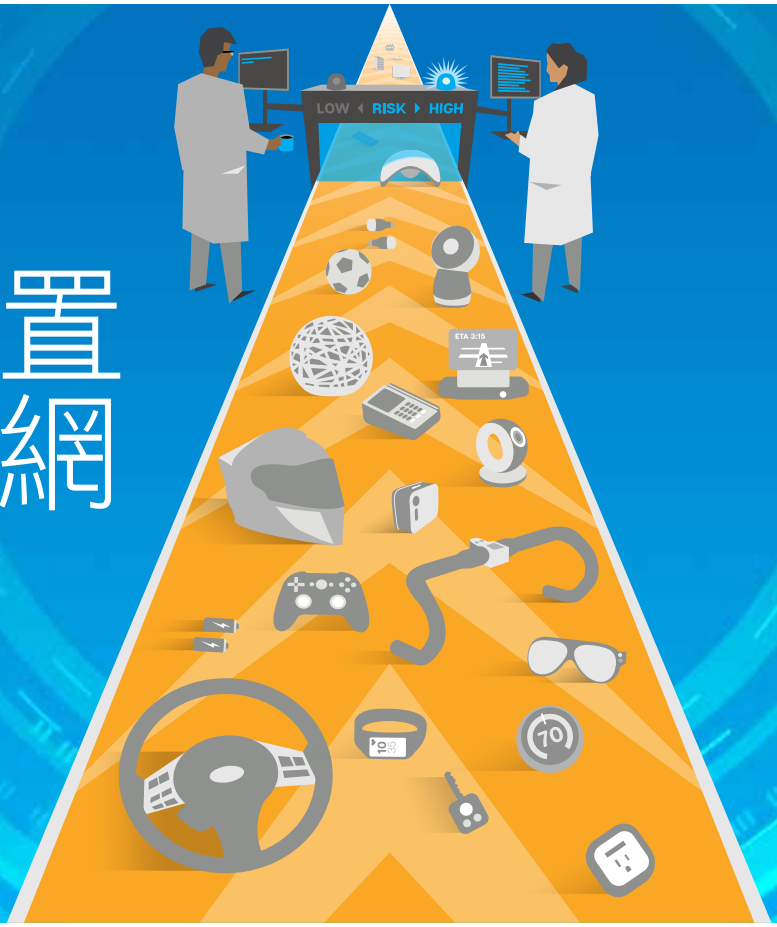
2013	2014	2015
每 566 個就有 1 個	每 1,126 個就有 1 個	每 3,172 個就有 1 個

魚叉式網路釣魚 (電子郵件目標式攻擊)

每日的魚叉式網路釣魚電子郵件

2013	2014	2015
83	73	46
–	-12%	-37%

行動裝置和物聯網



智慧型手機和行動裝置

對線上罪犯而言，智慧型手機日漸成為一個具有吸引力的目標。因此，他們正在投注更精密的攻擊，有效竊取寶貴的個人資料或向受害者勒索金錢。雖然 Android 使用者依然是主要的目標，但 2015 年也發現 Apple 裝置曾發生有效攻擊，而未越獄的 iOS 裝置也受到波及。

人手一機的時代

根據 IDC 的全球每季行動電話追蹤器 (2016 年 1 月 27 日)，在 2015 年全世界售出超過 14 億支智慧型手機，與前一年的 13 億支相比，增加了 10%。每 6 支新手機就有 5 支是執行 Android，而每 7 支手機有 1 支是執行 Apple 的 iOS 作業系統 (智慧型手機作業系統市佔率，2015 年第 2 季)。Ericsson 這家行動製造商預測，直到 2020 年底，可能會有多達 64 億支智慧型手機的訂購，幾乎每個人都擁有一支手機。

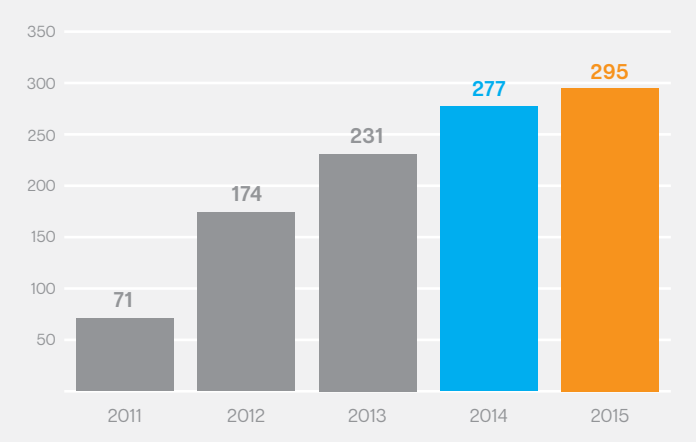
同時，高階手機和平板電腦具備強大的處理器及 4G 網路，具有高頻寬的連線能力。這些裝置也包含寶貴的個人資料。在 2015 年，Apple Pay 在世界各地的更多國家推出。隨著 Samsung Pay 和 Android Pay 也競爭想要管理您錢包中的卡片，其他行動付款系統也可能會跟進。這一切都讓智慧型手機變得非常容易吸引罪犯。

跨界威脅

透過許多應用程式商店，使用者能夠瀏覽、購買及從其桌面遠端安裝應用程式，為跨界威脅提供了絕佳的機會。在 Google Play 的一個範例中，客戶可以從其電腦使用一般 Web 瀏覽器來瀏覽 Play 商店，將應用程式直接安裝到手機中。最近某些 Windows 惡意程式的範例是，已利用這機會從受感染的桌上型電腦竊取 Google Play 階段作業的瀏覽器 Cookie，並用這些竊取的 Cookie (實際上是使用者的憑證)，在使用者不知情或不同意的情況下，冒充使用者遠端安裝應用程式到受害者的手機和平板電腦。

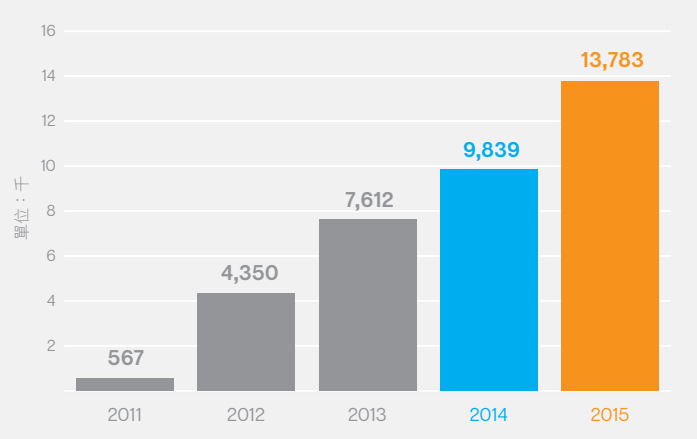
累計的 Android 行動惡意程式系列

- Android 惡意程式類型在 2015 年新增的數量成長了 6% (與 2014 年的 20% 成長率相比)。



累計的 Android 行動惡意程式變種

- Android 變種數量在 2015 年增長了 40% (與前一年的 29% 成長率相比)。



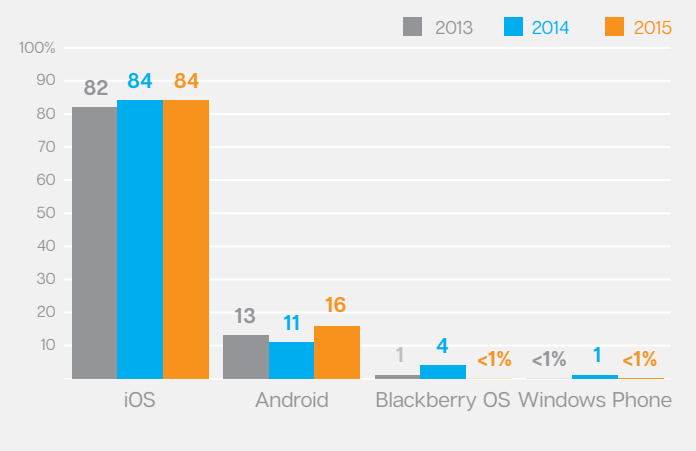
在過去的 3 年間，行動漏洞的數量每年都有增加。不像 Android 裝置，一直以來 iOS 漏洞是取得 iOS 裝置存取權的重大環節，特別就越獄而言。越獄可允許使用者安裝未經 Apple Store 授權的應用程式，並越過 iOS 整體必需的安全性。要危害非越獄的裝置就困難多了，因為它一般會要求從 Apple Store 下載應用程式才能進行安裝。Apple 的嚴格篩選程序相當著名。這就是惡意 iOS 應用程式的數量比 Android 少非常多的原因。

在 2012 年，IOS.Finfish 是第一個在 Apple Store 發現的惡意 iOS 應用程式範例。Finfish 能夠從受到入侵的裝置竊取資訊。在 2014 年發生的 OSX.Wirelurker，其使用包含 USB 連線至 Mac 或 PC 的攻擊，可潛在讓應用程式安裝在非越獄的 iOS 裝置上。

不過，在 2015 年，使用 XcodeGhost 和 YiSpecter 的攻擊顯示不需要漏洞或越獄，就能危害 iOS 裝置。稍後在本節中，我們將更仔細探討這些及更多行動威脅。

依作業系統區分的行動漏洞

- 近年來，iOS 平台上的漏洞已佔行動漏洞的最大量。通常有興趣調查越獄裝置，或取得未經授權的權限來安裝惡意程式。



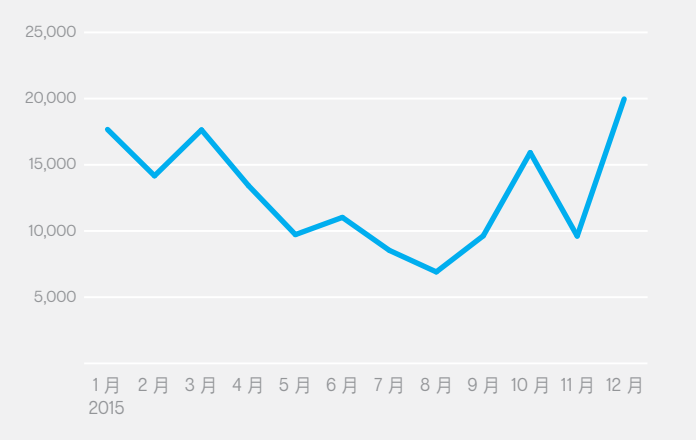
Android 攻擊越來越隱匿

Android 惡意程式變得越來越隱匿，無聲無息。例如，惡意程式作者已開始模糊程式碼，以越過特徵式安全軟體。此外，在他們開始攻擊之前，某些惡意程式現已可檢查程式是在真實的手機，還是在安全研究員使用的模擬器或沙箱上執行。

Android 惡意程式攻擊的數量在 2015 年期間起伏不定。在第 1 季，賽門鐵克每天攔截大約 550 次攻擊，是當年次數最高的期間。到第 3 季結束前，大約下降到每天 272 次，但到第 4 季結束前，又再度升高到每天 495 次。

Android 惡意程式數量

- 在 2015 年歸類為含有惡意程式的 Android 應用程式數量是 2014 年的 3 倍以上，增加了 230%。



前 10 大 Android 惡意程式

- 賽門鐵克在 2015 年攔截的 37% Android 惡意程式與 Android.Lotoor 的變種有關，一般偵測到的是可利用 Android 漏洞的駭客工具，以取得受危害 Android 裝置的根存取權限。

排行	惡意程式	百分比
1	Android.Lotoor	36.8%
2	Android.RevMob	10.0%
3	Android.Malapp	6.1%
4	Android.Fakebank.B	5.4%
5	Android.Generisk	5.2%
6	Android.AdMob	3.3%
7	Android.Iconosis	3.1%
8	Android.Opfake	2.7%
9	Android.Premiumtext	2.0%
10	Android.Basebridge	1.7%

惡意視訊留言如何導致 Stagefright 和 Stagefright 2.0

無論 Google 以多快的速度修正 Android 作業系統中的重大漏洞，一般使用者收到更新的速度取決於其裝置製造商，有時候需要等候較久時間。在 2015 年 7 月曾突顯這樣的情況。有 7 個漏洞已經過修正，其中只要透過傳送惡意多媒體訊息 (MMS)，就能讓攻擊者危害受影響的裝置；使用者只要看了惡意訊息，就會觸發此利用點而受害。

涉及的這 7 個漏洞統稱為「Google Stagefright 媒體播放引擎多重遠端程式碼執行漏洞」(CVE-2015-1538、CVE-2015-1539、CVE-2015-3824、CVE-2015-3826、CVE-2015-3827、CVE-2015-3828 及 CVE-2015-3829)，而所有都是與處理媒體播放的 libStageFright (一個 Android 元件) 有關。來自 Zimperium zLabs 的 Joshua Drake 在 2015 年 4 月和 5 月向 Google 報告這些漏洞，但更令人擔憂的是，雖然 Google 已將修補程式提供給其合作夥伴，許多製造商卻花了更久的時間才提供修補程式保護其客戶。即使 Google 已提供修補程式，但除非等到電信業者和製造商推出其自身的修補程式，否則使用者仍處於風險之中。這樣的情況使得這些漏洞的嚴重性更加複雜。這通常需要數週或數月，而且許多舊裝置可能完全再也無法收到修補程式。

不過，Google 熱切指出，具有 Android 4.0 及更高版本的裝置 (約佔 95% 的使用中 Android 裝置)，透過名為「位置空間配置隨機化 (Address Space Layout Randomization，ASLR)」的技術，擁有內建防護可抵禦緩衝區溢位攻擊。此外，Android 使用者能夠透過內建的「訊息」應用程式以及透過 Google Hangouts，關閉多媒體訊息的自動擷取。

儘管這方法能提供部分緩解，但如果已下載及開啟異常或惡意多媒體訊息，就無法阻止漏洞受到利用。

在 2015 年 10 月，公開了另外兩個 Android 漏洞 (CVE-2015-6602 和 CVE-2015-3876)，與原來的 Stagefright 錯誤相似。同樣地，這些漏洞如果受到利用，就會允許攻擊者取得受到危害之裝置的控制權。這次的情況是，如果使用者檢視 .mp3 或 .mp4 檔案的預覽就會受害。透過建立惡意音訊或視訊檔案，攻擊者誘騙使用者在未經修正的 Android 裝置預覽歌曲或影片。

Google 先前已修正 libStageFright 程式庫，所以它不會再自動處理此類訊息。不過，攻擊者仍有可能透過行動瀏覽器利用 libStageFright。名為 Stagefright 2.0 的這些新漏洞，也可能會透過攔截式攻擊和仍使用 Stagefright 的協力廠商應用程式，而遭受利用。針對在 8 月發現及報告的這些新漏洞，已在 Google 的「10 月每月安全更新」中隨附提供其修補程式。

網路釣魚和勒索軟體使 Android 使用者處於水深火熱之中

除了熟悉的誘騙手法，像是將惡意程式碼隱藏於表面上合法的應用程式內，或偽裝成其他更有用的形式，攻擊者正使用更精密的技術來獲取受害者的金錢。例如，賽門鐵克研究員已發現一個新的 Android 網路釣魚木馬程式，可藉由在合法的銀行應用程式之上，彈現出假造的登入網頁，誘騙使用者輸入其銀行憑證。同樣地，最近的Android 勒索軟體在使用者的鎖定畫面顯示假造的 FBI 警告，透過複製 Google 的設計風格，讓它看起來更合法及令人生畏。我們也已發現手機勒索軟體開始將檔案加密，例如圖片，而不只是變更手機的存取 PIN 碼。

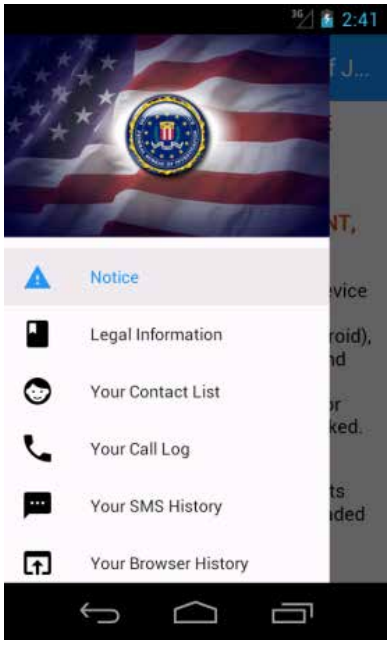
Apple iOS 使用者現正面臨前所未有的風險

歸功於 Apple 對其應用程式商店及作業系統的嚴密管控，一直以來 iPhones 和 iPads 的威脅都較為少見且規模有限。但這在 2015 年已發生轉變。

- 在 2015 年，我們發現 9 個系列的新 iOS 威脅 (相較之下，以往全部總計是 4 個)。
- 稱為 XcodeGhost 的這個非法販售的開發人員軟體已感染多達 4,000 個應用程式。
- YiSpecter 惡意程式已藉由使用企業應用程式預先佈建架構，完全越過應用程式商店。
- 調查員發現 Youmi 已內嵌於 256 個 iOS 應用程式。此軟體在應用程式中是用來顯示廣告，但也會在未經使用者同意的情況下，將個人資料傳送到遠端位置。
- Apple 之 AirDrop 無線檔案傳輸系統中的漏洞，會允許攻擊者在 Apple 裝置安裝惡意程式。

勒索軟體行動化

- 請想像，當使用者下載新潮的應用程式至其手機，但試著登入時卻發現裝置的主畫面顯示 FBI 警告且已遭到鎖定，會感到多麼挫折。
- 使用者有兩個選擇：一是繳交「罰金」 並盼望攻擊者將他們的手機解除鎖定，二是放棄取回手機中的珍貴照片、聯絡人及回憶。



深受 XcodeGhost 困擾的 iOS 應用程式開發人員

隨著 Apple iPad 和 iPhone 銷售量與日俱增，我們相信罪犯會逐漸鎖定它們，及受到其擁有者的較高可支配收入 (一般而言) 的吸引。不過，擁有者和 Apple 使用者不應再假定 Apple 裝置就能免於遭受攻擊。在 2015 年 9 月，已在中國的許多 iOS 應用程式中發現惡意程式，而且是在許多合法的 Apple Store 應用程式中發現，包括 WeChat (一個熱門的 IM 應用程式)。此問題在於，這些應用程式並非專門設計為惡意程式，但它們的開發人員已遭受惡意程式危害，將其內嵌至開發中的應用程式。

在某些非官方版本之 Apple 的整合式開發環境 (Xcode) 中，已發現稱為 XcodeGhost (以 OSX.Codgost 的名稱被偵測到) 的惡意程式碼。使用這些 Xcode 受感染版本的 iOS 應用程式開發人員，在不知不覺間允許惡意程式碼插入到他們自己的官方 iOS 應用程式，而使他們的使用者處於風險之中。

如果使用者下載並安裝受感染的應用程式，XcodeGhost 就會將該裝置的相關資訊上傳至其指令與控制 (C&C) 伺服器。攻擊者就能透過 C&C 伺服器發出指令，以執行下列動作：

- 建立假造的網路釣魚警示，以竊取受害者的使用者名稱和密碼
- 在裝置的剪貼簿上讀取及寫入資料，這可能會被用來揭露從密碼管理工具所複製的密碼
- 綁架瀏覽器以開啟特定網址 (URL)，這可能會導致其他進一步的利用

估計 Apple App Store 上有數百個 iOS 應用程式受到感染，可能影響數十萬個使用者，尤其是在 WeChat 應用程式特別熱門的中國。

正如先前的其他 iOS 威脅，此威脅不需要越獄的 iOS 裝置，這使其在行動威脅版圖中，成為一種新的且相當令人擔憂的發展。賽門鐵克在 2015 年的 9 月到 12 月之間，已攔截 33 次攻擊。此外，在 2015 年並不是只有 Apple 的 iOS 受到攻擊。Mac OS X，該公司的熱門桌面作業系統，在同一年期間也發現漏洞、利用及威脅量的上升。

YiSpecter 顯示攻擊者現今對 iOS 投以高度關注

在 2015 年，我們發現鎖定 iOS 平台的威脅擴大中，包括也是在 2015 年 10 月發現的 YiSpecter (以 IOS.Specter 的名稱被偵測到)。YiSpecter 專門設計為鎖定使用中文的人士，而且主要影響東亞的使用者，包括中國和台灣。

YiSpecter 是一個能夠利用越獄和非越獄的 iOS 裝置的木馬程式，實際上是在受危害的裝置上提供一個後門並安裝廣告軟體。此木馬程式允許攻擊者達成各種任務，包括解除安裝應用程式、下載新詐騙應用程式，以及強迫其他應用程式顯示廣告。

鎖定非越獄 iOS 裝置和憑證濫用

YiSpecter 是第一個利用 Apple 企業應用程式預先佈建架構，來危害非越獄裝置的 iOS 威脅。許多企業使用此架構向其員工合法地部署私人應用程式，而不須將應用程式公開發佈在官方 App Store。這些應用程式是使用企業憑證建立及簽署，而且不需交由 Apple 檢查，就能在 App Store 之外進行發佈。這也讓企業能夠有更大的範疇，來開發一些含有會被 Apple 拒絕的功能，但卻仍可透過此架構合法地簽署及部署應用程式。

不過，如 YiSpecter 所證明，iOS 企業憑證也可用來封裝及簽署其惡意程式。並不清楚攻擊者取得憑證存取權的方式，但有可能是他們已用企業身分向 Apple 註冊，支付必要的費用及遵循檢查程序。或者，他們可能已能從已註冊的開發人員或與其成為合作夥伴，而竊取合法憑證。

一旦攻擊者擁有有效企業憑證的存取權，就能夠建立、簽署及發佈其惡意應用程式。無需 Apple 的任何進一步介入，就有可能發佈至任何 iOS 裝置。無疑地，當 Apple 獲悉任何企業憑證的濫用，就會立即撤銷該憑證，致使任何由其簽署的應用程式變為無效。一般而言，使用者須接受信任應用程式或開發人員的請求，才能安裝企業簽署的應用程式。根據我們的經驗，詢問使用者是否信任應用程式或開發人員，幾乎是一種不太有效的安全措施，但這是惡意程式需要跨越後才能進行安裝的最後一道防線。

利用 Apple 的私人 API

YiSpecter 包含更多先進功能的其中一個原因是，它也使用 Apple 自家的私人 API，可執行標準 iOS 應用程式無法執行的活動。這些「私人 API」是保留給 Apple 自家應用程式，使其能夠執行各種系統層級的動作。其他 iOS 開發人員不應該在其應用程式中使用這些 API，而任何這樣做的協力廠商應用程式會被 Apple App Store 拒絕。無疑地，YiSpecter 能夠設法規避官方 App Store，而不依賴非官方的發佈管道來散播惡意程式。因此，此威脅能夠根據自己的目的來利用私人 API。

跨平台 Youmi 移動廣告軟體在 iOS 和 Android 偷竊個人資料

在 2015 年 10 月，Apple 從 App Store 抓出顯然違反該公司之隱私權準則的應用程式，數量多達 256 個。這些應用程式已使用來自於一家稱為 Youmi (以 Android.Youmi 的名稱被偵測到) 公司的協力廠商廣告技術，偷偷用來存取私人資訊，包括 Apple ID 電子郵件地址及行動通訊國際識別碼 (IMEI)。

不久之後，在許多 Android 應用程式中，已發現相同的廣告程式庫。它在此是用來執行能危害使用者隱私權的各種動作，包括獲取其 GPS 位置和電話號碼， 以及下載更多、可能不受歡迎的應用程式。

區分移動廣告軟體

廣告軟體及其行動變體，也就是所謂的行動廣告軟體 (或移動廣告軟體) 多年來已遍布各地，而且是一種為免費應用程式提供資金的熱門方式。其中，應用程式開發人員向其使用者呈現的每則廣告，都會獲得費用。許多人樂意釋放螢幕的一小塊區域供廣告使用，以換取免費應用程式。不過，這有時可能會在未經同意的情況下發生，或特別具有侵略性。根據賽門鐵克的記錄，含有不受歡迎之移動廣告軟體的應用程式增加了 77%。

作為避免這問題的一種方式，阻擋廣告的工具變得大受歡迎。而且藉由阻擋行動廣告，也有助於降低因移動廣告軟體流量所導致的行動數據費用，並且將螢幕上的廣告數量減至最低。此外，這類軟體也能有助於改善裝置的安全狀態，能夠阻擋可能不受歡迎的移動廣告軟體在未經使用者允許或不知情的情況下進行安裝。

運用賽門鐵克 Norton Mobile Insight 進行的應用程式分析

- 賽門鐵克已分析在 2015 年多了 71% 的應用程式，而且超過 3 倍 (230%) 是歸類為惡意應用程式。灰色軟體增加了 30%，大部分是由於含有不受歡迎之移動廣告軟體的應用程式增加了 77%。

	2013	2014	2015
已分析的應用程式總數	6.1 百萬	6.3 百萬	10.8 百萬
已歸類為惡意程式的應用程式總數	0.7 百萬	1.1 百萬	3.3 百萬
已歸類為灰色軟體的應用程式總數	2.2 百萬	2.3 百萬	3.0 百萬
進一步歸類為移動廣告軟體的灰色軟體總數	1.2 百萬	1.3 百萬	2.3 百萬
惡意程式定義	用來造成傷害的程式與檔案。惡意軟體包括電腦病毒、病蟲以及木馬程式。		
灰色軟體定義	未含有病毒且非明顯惡意的程式，但對使用者而言具有干擾性或甚至傷害性 (例如：駭客工具、非法存取軟體、間諜程式、廣告軟體、撥號木馬程式及惡作劇程式)。		
移動廣告軟體定義	使用激進的技巧，將廣告置放在行動裝置的相簿和行事曆項目，並將訊息推送到通知列。移動廣告軟體甚至還能將鈴聲置換為廣告。		

保護行動裝置

我們建議大眾與員工將行動裝置視為小型而強大的電腦，進而採取以下保護措施，包括：

- 存取控制，包括生物辨識 (如果可以)。
- 資料遺失防護，例如在裝置上加密。
- 自動裝置備份。
- 遠端尋找與清除工具 (萬一遺失裝置時)。
- 定期更新。例如，最新版的 Android，代碼名為 Marshmallow (6.0 版本) 已在 10 月推出，並且包含許多專門針對遏止攻擊者而設計的功能。根據 Statista，在 2015 年 10 月，KitKat (4.4 版本) 仍是最廣泛使用的 Android 版本 (佔 38.9%)，而 Lollipop (5.0 版本) 則佔 15.6%。
- 請避免從不熟悉的網站下載應用程式，並且只安裝來自於信任來源的應用程式。
- 請勿將裝置越獄。越獄裝置通常更容易受到安全方面的問題侵擾。
- 請特別留意應用程式要求的權限。
- 請盡可能經常更新應用程式，或者如果發現可疑的應用程式，請將其刪除並等候新版上市。
- 如果您懷疑帳戶已受到入侵，請變更您的 Apple ID 密碼，或您的 Google Play 密碼。此建議可擴展為保護任何協力廠商應用程式商店上的帳戶憑證。
- 請注意任何可疑的電子郵件，或在您的裝置要求憑證、或任何其他個人識別資訊的推送通知。
- 直到您套用修補程式後，在使用您的手機瀏覽器預覽不請自來的音訊和視訊檔案時，請謹慎地進行。
- 一旦電信業者或裝置製造商發佈任何安全更新，建議 Android 使用者立即套用更新。
- 額外的行動安全解決方案也有助於保護惡意程式侵擾，而企業應考慮能有助於在企業之內保護及管控行動裝置的行動管理工具。

未來展望

我們預測行動威脅在 2016 年將繼續激增。我們很快可能會看到針對黑市交易之手機的類似 PC 攻擊套件。

同時，Apple 和 Google 正致力於保護其作業系統及更廣闊的生態系統。尤其，針對用於驗證和簽署應用程式以及應用程式供應的技術，我們預期會有所改善。手機使用者將會習慣經常預設開啟的應用程式和頻繁的作業系統更新，以及需要在行動裝置上安裝安全軟體。

這也許是個進步的指標，而不是造成失望的理由。這表示透過找出和修正問題，事實上安全研究人員、作業系統、開發人員及應用程式作者都越來越注意行動安全。儘管我們預期明年行動裝置將遭受更多攻擊，但仍希望透過妥善的預防措施和持續投資安全性，讓使用者享有更高的攻擊防護層級。

物聯網

透過網路連線的物品正迅速倍增。在 2015 年，我們發現許多概念證明和真實的攻擊事件，找出了車輛、醫療裝置及更多產品的嚴重漏洞。製造商必須針對安全問題排定優先順序，以降低嚴重之個人、經濟及社會後果的風險。

數之不盡的物品

物聯網時代已經來臨。只要注意我們自己的環境周圍，就能發現這對我們日常生活造成的影響。現今一般智慧型手機具備比太空梭更高的運算能力；現今智慧手錶可從網路下載更新；咖啡店的銷售點終端機全部都可連線到公司的中央財務系統；現今許多車輛具備衛星導航和藍牙連線；透過網路連線的自動調溫器可以控制我們家中的溫度。

例如，在美國每 100 個居民就有 25 個線上裝置，而這還只是開始而已。Gartner 預測在 2016 年有 64 億個連線物品將會在全球使用，而且到 2020 會達到 208 億 (Gartner, Inc.，新聞稿，2015 年 11 月 10 日)。

如果物聯網傳遞預期的 2 兆美元經濟效益，設計者和製造商就必須因應重大的安全挑戰。然而，前景並不理想。

物品的危險因子

賽門鐵克在去年已發現概念證明攻擊的增加，而且越來越多的物聯網 (IoT) 攻擊正在肆虐。從無數的案件看來，漏洞相當明顯而且全都太容易利用。IoT 裝置通常缺乏嚴格的安全措施，而且有些攻擊能夠利用在一些 IoT 裝置和路由器中發現之底層 Linux 型作業系統的漏洞。許多問題源於廠商針對驗證和加密，所建置的機制的安全程度 (或根本完全未建置)。以下有一些範例：

- **車輛。**在研究人員呈現一件嘗試從遠端操控汽車的概念證明攻擊後，Fiat Chrysler 即已召回 140 萬台汽車。在英國，小偷已入侵免鑰匙車門開啟系統來偷竊車輛。
- **智慧型家用裝置。**數百萬個家庭易遭受網路攻擊。賽門鐵克調查發現在 50 個市面販售的裝置中有多個漏洞，包括可從線上遠端開啟的「智慧」門鎖 (不須輸入密碼)。
- **醫療裝置。**研究人員已在許多裝置中發現潛在致命漏洞，例如：胰島素幫浦、X 光系統、CT 掃描儀、醫用冰箱及植入式除顫器。
- **智慧型電視。**根據賽門鐵克調查，數億台透過網路連線的電視可能容易遭受以下攻擊：點按詐欺、殭屍網路、資料竊取、甚至勒索軟體。
- **內嵌式裝置。**數千個每日裝置，包括路由器、網路攝影機及網路電話，共用相同的硬編碼 SSH 和 HTTPS 伺服器憑證，讓超過 400 萬個裝置容易受到攔截和未經授權存取的攻擊。

我們預測在來年會看到更多與此類似的事件。如果裝置能被駭客入侵，情況就有可能如此。此外，有概念證明攻擊之處，真實攻擊總是會隨之而來。我們甚至可能預見 IoT 裝置變成攻擊企業的偏好途徑，而且可能是資安事端應變人員最難以辨識和移除的攻擊。

就目前已連線裝置的不良安全狀態來看，在罪犯眼裡它們會日漸成為具有吸引力的目標。罪犯會尋找容易下手的目標，正如小偷比較喜歡沒有警報器或家犬的家庭。

洞燭先機：物品的風險

連線至網際網路的物品

20 數量達數十億

19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1

物品的危險因子

醫療裝置。研究人員在胰島素泵和植入式除顫器等數十個裝置上發現潛在的致命漏洞。

智慧電視。根據賽門鐵克研究指出，數億台連線至網際網路的電視可能都暴露在點選詐騙、傀儡網路、資料竊取甚至勒索軟體的風險之中。

汽車。在研究人員示範一起嘗試從遠端操控汽車的概念證明攻擊後，Fiat Chrysler 召回了 140 萬台汽車。在英國，小偷入侵車輛的免鑰匙車門開啟系統竊取車輛。

現今**每 100** 位美國居民就有**25 個連線裝置**[1]

208 億[1]
（預估）

64 億

49 億

39 億

2014 2015 2016 2020

1 資料來源：gartner.com/newsroom/id/3165317

家庭自動化到 2020 年到達臨界點

物聯網即使已獲得漸增的注意力及迅速發展，但當談到家庭自動化時，物聯網仍尚未受到空前絕後的關注。也許阻礙 IoT 優勢的其中一個最終障礙，是與標準化通訊協定相關。目前，我們已發現使用妥善建立的通訊協定 (例如 Wi-Fi 和 Bluetooth®) 之互連 IoT 裝置的大幅成長。使用 802.11b/g/n/ac 無線通訊協定的裝置，包括智慧型電視、智慧自動調溫器、IP 攝影機，及其他裝置，正在四處出現。使用藍牙 4.0 的裝置 (例如：健身追蹤器、智慧手錶及其他穿戴式裝置)，也幫助了 IoT 獲得市場青睞。

不過，這些通訊協定在許多家庭自動化案例中未達到預期效果。最新 Wi-Fi 技術相當適合快速和有效的無線連線，但有會讓小型裝置疲憊的電力要求。在本案例中藍牙的運作確實比較好，但它的短距限制對於與數英尺之外的通訊而言，就不太理想了。但這並不表示無法達成。只是不可能用價格低廉到足以使此技術普及化的方式進行。

許多廠商已著手因應這些通訊挑戰，雖然還沒有人能成為主流。這已導致零星分化的市場，競爭無線通訊規格受到特定廠商或廠商群組束縛限制。最終可能為小型、低功率 IoT 裝置開啟門戶的是 Wi-Fi HaLow™ (IEEE 802.11ah)，這是針對 IoT 和穿戴式裝置的新通訊協定，預定在 2016 至 2018 年期間完成及驗證。一旦推出，路由器製造商可以快速將通訊協定導入至其產品中，就和其他通訊協定一樣 (例如 802.11ac)。這樣做會開啟門戶，讓消費者更輕鬆且便宜地將家庭自動化。

無疑地，在推出任何新技術時，攻擊層面會隨而擴大，就安全觀點來看，呈現了各種新問題。已發現專屬 IoT 網路含有多個安全漏洞。有些極其微小，有些相當嚴重。關於 IoT 和家庭自動化的根本問題並不是「我們應該如何進行？」，而是「我們應該如何安全地進行？」。

隨著共同標準的採用，有可能較舊的專屬通訊協定將會中途退出，為市場潛在更大的整合鋪路。儘管較大型的知名品牌名稱會繼續發行自己的產品，小型創新的 IoT 公司對於尋求將產品組合迅速擴展到相關領域的企業而言，將會成為具有吸引力的目標。然而，網路安全必定是採用這種新 IoT 技術成功的核心所在。當有更多的家庭可以連線，消費者將難以忽略這個新科技承諾的益處。

遠端控制的便利性、自動化、輕鬆使用及它們所帶來的益處，相對於會導致駭客開啟 IoT 鎖定、停用 IoT 小偷警報或一般 IoT 裝置受到的嚴重破壞之潛在風險，這兩面的衡量得失至關重要。

如何保護已連線裝置

保護物聯網須有和 IT 安全性的其他領域一樣的全面性方法。很可惜，兩個工業 IoT 生態系統，像是工業網路聯盟 (IIC) 和消費者 IoT 生態系統，例如 AllSeen 聯盟，仍然很早就定義了此不斷快速演進領域的標準。為了符合這點，賽門鐵克已發行其安全參考架構，並隨著線上信任聯盟 (OTA) IoT 信任架構、以及生活重大內嵌式系統的美國國土安全部 (DHS) 安全性原則，為 IIC 和 AllSeen 貢獻心力。

須在裝置內建多層安全性及用以管理它們的基礎建設，才能達成有效安全性，包括驗證、程式碼簽署、以及裝置內建安全性 (例如「內嵌式重大系統保護」技術)。分析、稽核及提醒也是瞭解這領域浮現之威脅本質的重要關鍵。最後，強大的 SSL/TLS 加密技術在驗證和資料防護中扮演了重要角色。

邁向安全連線的未來

和其他網路安全層面一樣， 某些威脅比其他來得更加危險， 而雖然駭客入侵適合監控可能造成不便，數百萬台車輛中的漏洞可能是更為嚴重的危險。同樣地，醫療裝置中的後門可能會讓竊賊得以存取醫療記錄 (雖然在相當小的規模)，或可能導致嚴重傷害或甚至死亡的可能性。

雖然已充分瞭解補救措施，但製造商必須排定安全性的優先順序，並在創新、容易使用及上市時間限制之間找到恰當的平衡。從根本上而言，企業和消費者必須確保供應商有在其購買的 IoT 裝置中建置安全性。■

網頁威脅

網路攻擊、工具組，以及利用線上漏洞

如果 Web 伺服器容易遭受攻擊，則這些伺服器主控的網站及造訪這些網站的人們也很難防守。攻擊者正在利用任何可入侵網站的漏洞，並佔領主機伺服器。網路攻擊工具組的易用性和廣泛可用性讓網路攻擊數量逐漸提升，進而在 2015 年增加一倍。

網站擁有者仍未如預期經常修正及更新其網站與伺服器。這就像打開窗戶讓網路罪犯爬進來，並充分利用他們所發現的一切。

在過去三年中，超過四分之三的網站，經掃描之後發現包含未修正的漏洞，其中有七分之一 (15%) 是在 2015 年被視為嚴重漏洞。

經掃描發現漏洞的網站

▶ 如果利用其中一個關鍵的漏洞，可能會讓惡意程式碼無需使用者的互動即自動執行，可能造成資料外洩，並進一步危害受影響網站的訪客。

2013	2014	2015
		
77%	76%	78%
	減少 1 個百分點	增加 2 個百分點

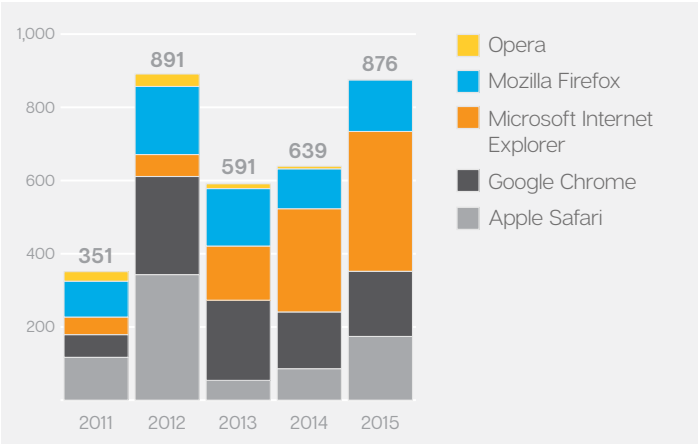
嚴重漏洞的百分比

2013	2014	2015
		
16%	20%	15%
	增加 4 個百分點	減少 5 個百分點

有問題的外掛程式

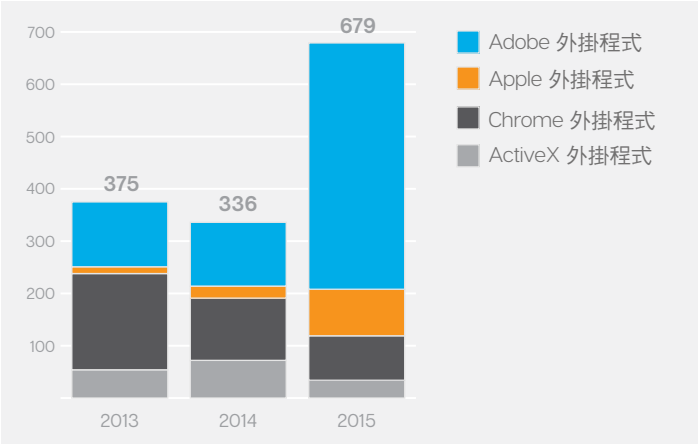
不只是作業系統使得 Web 伺服器容易遭受攻擊。儘管許多主要的內容管理系統供應商在近年來已提高安全性，並實施自動更新，這些系統的外掛程式安全性仍是一個很大的問題。

瀏覽器漏洞



年度外掛程式漏洞

▶ Adobe 外掛程式的漏洞數量在 2015 年不斷增加，這表示攻擊者正尋求不僅是在跨平台利用外掛程式，而是無處不在的外掛程式。大多數 Adobe 漏洞與 Adobe Flash Player (也稱為 Shockwave Flash) 相關。



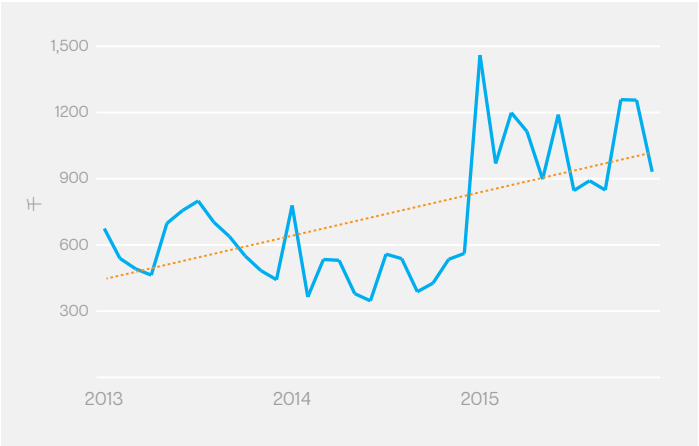
Flash 末日將至

Adobe Flash Player 多年來不斷遭受惡意攻擊，並且在 2015 年佔了 10 個歸類為零時差的漏洞 (17%)，相比之下，2014 年是 12 個 (50%)，2013 年是 5 個 (22%)。有了這些豐富的採集資料，很明顯可以瞭解攻擊者為何偏好攻擊 Flash。Apple、Google 和 Mozilla 皆對 Flash 外掛程式表示擔憂，而且 Google 最近宣佈 Flash 不再受到 Chrome 原生支援。Mozilla 則採用不同的一般外掛程式策略，繼續在 Firefox 中支援 Flash。

從安全性的角度來看，我們預計 Adobe Flash 在明年會逐漸退出常用工具之列。

每月攔截到的網路攻擊數量

▶ 圖表顯示自從 2013 年以來每天平均攔截的網路攻擊數。2015 年每天攔截的網路攻擊數平均是 100 萬個，與 2014 年相比之下，增加了 117% (兩倍以上)。



採用 Web 伺服器的外掛程式

不僅是 Web 瀏覽器的外掛程式不易防守且容易遭受攻擊。以勢力占全球網站四分之一的 WordPress 為例。任何人可寫入 WordPress 外掛程式 — 而且他們經常這麼做。外掛程式範圍從有用的到完全荒謬的皆涵蓋在內，例如「登出輪盤」(Logout Roulette)：「在每一個管理頁面載入，您會有十分之一的機會登出。」

問題是，有些外掛程式極度不安全。Windows 因為其龐大的使用者群而吸引了許多攻擊，這一點同樣適用於 WordPress 外掛程式。可以並將利用 WordPress 網站上發現的脆弱外掛程式。

無論是適用於瀏覽器或伺服器的外掛程式，都需要定期更新，因為它們很容易受到安全漏洞的攻擊，而且應盡量避免使用舊版本。

將外掛程式的風險降至最低

- 定期更新外掛程式。
- 觀看媒體和安全清單中的警告事項。
- 嚴選用來降低攻擊層面的外掛程式。

插入感染

在 2015 年，賽門鐵克也看到了 Team GhostShell 的回歸，其宣稱已入侵眾多網站。今年初，賽門鐵克安全機制應變中心團隊報告：

「從首次出現開始，最近發布的駭客入侵網站名稱似乎是隨機的，而且沒有任何跡象表明已鎖定任何特定國家或產業。該集團很可能根據網站本身的漏洞來入侵網站。

依循其先前的作案手法，該集團很可能透過 SQL 插入攻擊方式，以及不當設定 PHP 程序檔來危害資料庫。」

同樣地，這些很可能都是較佳網站和伺服器管理所防止的駭客。SQL 插入是一種歷史悠久的攻擊方法，其能不斷運作是因為管理員為了搜尋查詢而建立之參數中的不必要弱點。

網路攻擊工具組

抵禦新的和未知的漏洞是很困難的，尤其是可能沒有修補程式的零時差漏洞，攻擊者正努力嘗試在廠商推出修補程式之前，先利用這些漏洞。

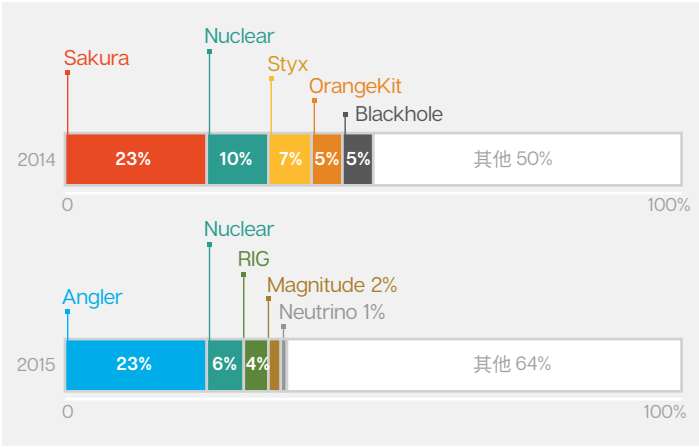
在 2015 年，義大利公司 Hacking Team 遭受入侵之後，先前未知的零時差攻擊已遭攻擊者公開。零時差漏洞的攻擊已公諸於世，並在數小時之內，整合至攻擊工具組。

釣魚式惡意廣告

Angler 刺探套件在 2013 年首次出現，可說是當今最複雜的刺探套件，並已開創許多其他刺探套件經常跟隨的技術進步，包括使用反網路安全對策。例如，Angler 可從記憶體中下載並執行惡意程式，無需將任何檔案寫入磁碟，試圖透過傳統的安全技術來規避偵測。此外，Angler 在 2015 年以驚人速度成長的一項重要因素是，它非常快速地將越來越多的新零時差攻擊整合至武器庫。

前 5 大網路攻擊工具組

- Angler 刺探套件是 2015 年最常用的刺探套件，並佔所有刺探套件網路攻擊的 23%。它在去年已大幅成長，而且它在 2014 年未列在前五大排行中。



Angler 是 2015 年最活躍的刺探套件，而且賽門鐵克每天攔截由此套件引發的成千上萬個攻擊。總體而言，攔截的 Angler 攻擊數已超過 1950 萬。Angler 最愛的傳送機制是惡意廣告，偏好易受攻擊的 Adobe Flash 漏洞。Windows 是 Angler 在 2015 年偏好的鎖定目標。Windows 7 特別佔了 Angler 攻擊的 64%，而 Windows 8.1 佔了 24%。此外，Mac OS X 在 2015 年並未出現在使用 Angler 工具組的攻擊行列上，但是這一點預計會隨著網路罪犯試圖攻擊 Apple 生態系統而產生改變。

技術支援詐欺執行 Nuclear，擴散勒索軟體

在 2015 年，賽門鐵克記錄了技術支援詐騙的增長，相較於去年提高了 200%。

技術支援詐騙不是新的戰術，而且每天有成千上萬的人在世界各地被鎖定目標。最早的技術支援詐騙類型是客戶中心員工陌生電訪使用者，嘗試向他們銷售支援套件，以解決其目標受害者電腦中不存在的問題。

這些詐騙已隨著時間演變，最近的例子可能會顯示看似無止盡的假警告訊息、鼓勵目標受害者撥打免費電話以尋求協助。撥打號碼後，聽起來似乎很專業的客服中心人員試圖說服目標受害者安

裝惡意程式及電腦中其他不必要的應用程式，同時聲稱將會解決他們的問題。

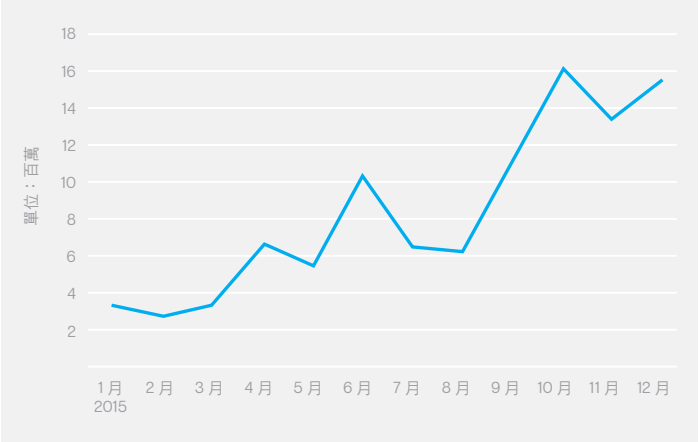
在最新的變種中，發現技術支援詐騙者使用 Nuclear 刺探套件，將勒索軟體放置到目標受害者的電腦中。當勒索軟體加密電腦中的檔案時，詐騙者會轉移使用者的注意力，可能增加機會以賺取受害者的金錢。

儘管這不是第一次發現技術支援詐騙者安裝勒索軟體，但最新範例是在其網站上加入惡意 HTML iframe，將訪客重新導向主控 Nuclear 刺探套件的伺服器。已發現刺探套件在其他漏洞之間採用最近的 Adobe Flash Player Unspecified Remote Code Execution Vulnerability (CVE-2015-7645)。如果成功，則會放置 Trojan.Cryptowall (勒索軟體) 或 Trojan.Miuref.B (資訊竊取木馬程式)。

這是賽門鐵克初次看見技術支援詐騙與 Nuclear 刺探套件並行使用以傳送勒索套件，如果這證實是有效的組合，此趨勢將持續下去。雖然技術支援詐騙者與刺探套件攻擊者聯手合作可能很合理，但技術支援詐騙者的 Web 伺服器可能已受到使用 Nuclear 刺探套件的個別集團入侵。

攔截的技術支援詐騙

- 總體而言，賽門鐵克在 2015 年已攔截超過一億個惡意程式或與技術支援詐騙相關的刺探套件攻擊。
- 技術支援詐騙最常鎖定的目標國家為美國、英國、法國、澳洲和德國。



惡意廣告

2015 年中期充斥著惡意廣告的帳戶，幾乎影響支援廣告之 Internet 的每一個區段。一個可能的解釋是，比起濫發垃圾郵件連結以感染網站，惡意廣告只是感染網站訪客的一種更簡單的方法。這對攻擊者而言，更容易嘗試並入侵受歡迎的網站，或試圖在熱門的高流量網站上主控惡意程式，因為這意味著他們不需要考慮複雜的社交工程差別，在這幫壞蛋的「管道」中進一步消除。

廣告公司往往不會從人們提交的廣告中要求許多資訊，因此很容易讓犯罪份子偽裝成合法企業並上傳可在任何網站上出現的惡意廣告。

多虧使用 Cookie，惡意程式作者也可以根據地理位置、時間、公司、興趣或最近的 Internet 活動，調整自己的惡意程式碼，或重新導向以鎖定使用者幾乎所有的子集合。

最常刺探利用的網站分類

- 技術和企業相關網站是 2015 年主控惡意內容與惡意廣告最受歡迎的網站。

2015 年前 10 名最常遭受攻擊網站的分類		2015 年受感染總數量的百分比網站	2014 前 10 名	2014 %
1	科技	23.2%	科技	21.5%
2	商務	8.1%	託管	7.3%
3	搜尋	7.5%	部落格	7.1%
4	部落格	7.0%	商務	6.0%
5	動態	6.4%	匿名	5.0%
6	教育	4.0%	娛樂	2.6%
7	網域停泊	3.2%	購物	2.5%
8	娛樂	2.6%	非法	2.4%
9	購物	2.4%	網域停泊	2.2%
10	非法	2.1%	虛擬社群	1.8%

不幸的是，惡意廣告是眾所皆知的難以追蹤，而且犯罪份子越來越狡猾，在一兩個小時之後，就會將惡意程式碼從廣告中移除，使其幾乎難以察覺。因為它是強大的、有效的，而且難以分析，我們預計惡意網告的使用會持續增加。因此，廣告攔截程式的需求增加可能反而有助於減少惡意廣告的負面影響。

網站擁有者的網路安全挑戰

無論是商店、工作或支付稅單的方式，線上服務的信任與信心已對我們的生活方式變得至關重要。值得慶幸的是，變化所帶來的是使用及保護 Internet 的方式，以加強線上隱私、安全和交易的信任。

網站安全涵蓋的不僅僅是伺服器與訪客之間傳輸至網站時的資訊。如果企業想重拾人們的信任與信心，他們需要針對需要不斷關注及留意的整個生態系統，審視自己的網站。

無法加強網站安全性的後果很可能會超出個別公司的成本費用：這將有損消費者的信心，而且其廣泛的經濟影響可能相當巨大。

別說廢話開始行動吧

根據美國國家零售業聯盟 (National Retail Foundation)，隨著消費者線上購物的數量已超過商店購物的數量，在美國 2015 年的感恩節週末假期期間，天平終於傾斜。

電子商務是大企業，而且根據歐洲電商組織 (Ecommerce Europe)報導，全球企業對消費者的電子商務營業額已成長 24%，在 2014 年達到 1.9 億美元。然而，相較於 Frost & Sullivan 預估在 2020 年企業對企業電子商務市場價值的 6.7 兆美元，可能顯得很小。Frost & Sullivan 預測包括所有形式的電子商務，包含使用 Internet 和電子資料交換系統。

甚至政府變得越來越依賴數據服務，以保持其帳冊平衡。例如，英國政府最近透露在 2014 年，透過數據和技術的轉變，已節省 17 億英鎊。

儘管 SSL/TLS 憑證、信任標記，以及良好的網站安全皆有助於維護線上經濟，如果人們對於線上經濟的安全基礎失去信任和信心，一切經濟活動皆可能處於風險之中。

網站仍容易遭受惡意程式與資料外洩的攻擊

網站是主要攻擊的關鍵因素：它們是進入網路的一種方式，它們是進入敏感性資料的一種方式，而且它們是接觸客戶和合作夥伴的一種方式。

例如，針對 Linux Web 伺服器之惡意程式的增加 (包括網站主機)，證實犯罪份子已意識到網站背後的基礎架構，相較於由 SSL/TLS 憑證加密的資訊，是有同等價值的，甚正更有價值。

許多針對網站基礎架構的攻擊可透過定期維護及修正來避免，但是數字卻顯示網站擁有者並不竭力定期更新。賽門鐵克在 2015 年掃描的網站中，有四分之三有漏洞 - 已經好幾年沒有改變了。

網路罪犯在 2015 年持續在網站安全的基礎架構中發現漏洞，包括 FREAK，使得攻擊者攔截安全連線，以強制伺服器降級到更容易破解通訊協定的加密。

分散式阻絕服務 (DDoS) 攻擊在 2015 年也持續證明對企業的破壞性。雖然大規模的攻擊 (例如 2015 年末攻擊 BBC 的事件) 經常佔領頭條，但是當主機關閉伺服器、讓多個網站離線時，各種規模的企業仍是攻擊的目標，而且較小的網站經常受到間接傷害，因為攻擊不僅只是針對其用戶端。

緩和策略與工具可以用來抵禦 DDoS 攻擊，但是如果網站管理者想讓自己的網站保持安全，則需要花時間瞭解並加以部署。

轉移至強化的驗證

不全是壞消息。2015 年，在加強及採用 SSL/TLS 憑證方面，以及憑證授權中心 (CA) 的倡議方面，已有好幾項進展，使得核發 SSL/TLS 憑證更加透明化。

重要的是，根據 Sandvine 的研究指出，美國所有下游 Internet 中將近 40% 現在是加密的狀態，而且預計在未來一年將增長到全球 Internet 流量的 70% 以上。

不幸的是，在一切都進行加密的世界裡，消費者對於安全性有一種錯覺，每當他們看到瀏覽器中的 HTTPS，他們正在使用的網站已經過確認和驗證，就以為一定是真實的。在現實中，線上詐騙在經過驗證的網域 (DV) 網站上已行之有年，它並未針對網站背後的企業進行驗證。

有了 DV 憑證，CA 將會在所討論的網域中確認聯絡人以批准憑證要求，通常是透過電子郵件或電話，而這通常是自動的。因此，DV 憑證通常比更嚴格的「延伸驗證」(EV) SSL 憑證還要便宜，因後者需要更多的審查與驗證。

雖然 DV 憑證驗證網域擁有者的同意，但他們不會嘗試確認誰才是真正的網域擁有者，使其非常適合網路釣魚和攔截式 (man-in-the-middle, MITM) 攻擊。賽門鐵克希望看到企業的對策，尤其是 PCI 法規推動的政策，以強化更強驗證的需求，並採用 EV SSL 憑證，提供更高水平的保證。

SSL/TLS 的加密也將透過從 SHA-1 轉變到 SHA-2 變得更強大。從歷史角度來看，SHA1 是非常受歡迎的單向雜湊功能，其中從來源產生的每一個雜湊皆是唯一的。不應該有「衝突」，其中兩個不同來源將產生相同的雜湊；不過，第一個弱點早在 2005 年即發現。當 Google 宣佈即將不再支援網站使用 SHA1，並且將對嘗試使用在 2017 年 1 月 1 日到期的 SHA-1 憑證存取網站的訪客顯示安全警告時，這在 2014 年到了非解決不可的地步。其他幾個瀏覽器廠商皆紛紛效仿，宣佈 SHA-1 的告終。

安全社群正取得很大的進展，並真正有機會大幅減少網路攻擊的成功次數，但只有在網站擁有者挺身而出並採取行動時才會發生。

加速推動隨時待命的加密

根據 Sandvine 的研究指出，美國所有下游 Internet 中將近 40% 現在是加密的狀態，而且預計全年將增長到全球 Internet 流量的 70% 以上。此急遽增加起因於幾個因素：

- **大公司的承諾。**Internet 上某些知名企業已採用 HTTPS，包括 Facebook、Twitter 以及最近的 Netflix。
- **搜尋引擎喜好設定。**Google 在 2014 年宣布採用「HTTPS Everywhere」，對於搜尋排名會產生正面的影響，鼓勵網站擁有者利用它來獲取搜尋引擎排名的優勢。
- **HTTP 升級。**網際網路工程任務小組 (IETF)，負責為 Internet 建立標準的組織，在 2015 年公佈新版本的超文字傳輸通訊協定。其又稱為 HTTP/2，很可能在不久的將來採用作為標準，現在仍是草案狀態，HTTP/2 可啟用「更有效地利用網路資源」，表示 HTTP/2 旨在針對立即可用的網站，提供更好、更快速的回應效能。而且每一個主流瀏覽器表示，只有在結束 SSL/TLS 時才會支援 HTTP/2。實際上，這會讓網站使用新標準來強制進行加密。

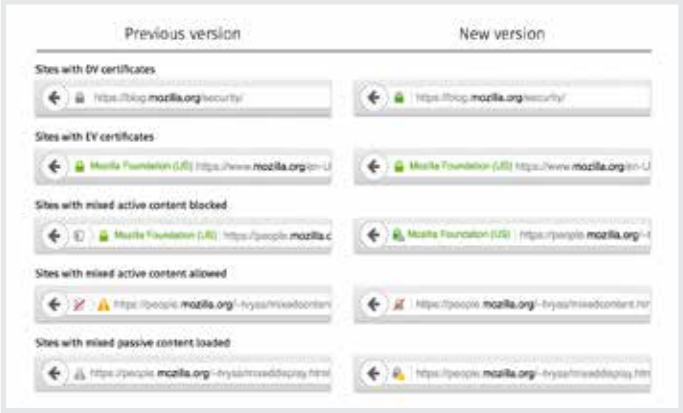
希望在未來幾年內，Internet 上的每一個頁面都有一個 SSL/TLS 憑證。賽門鐵克已與 Web 主機代管供應商合作，以協助他們提供加密，作為網站擁有者服務的一部分。

增強的安心保證

某些主流瀏覽器也正在改變他們的安全性指標 — 透過在網址列使用顏色和符號，以向訪客顯示網站的安全程度 — 當受 SSL/TLS 保護的網頁包含易受攔截式竄改攻擊的不安全內容時，會有清楚的標示。換言之，當網站無法達到隨時待命的加密，及其構成的危險時，會有更清楚的標示。

這只是我們努力推動對網站訪客和線上購物者，提供額外安心保證的範例之一，其他還包括信任標誌和購物保障，有助於減輕許多購物者在線上購物時的恐懼，例如無法親自與店家老闆見面或親手接觸要購買的商品。

▶ 摘錄自 Mozilla 的安全性部落格



必須使網站更難以遭受攻擊

企業對於 SSL/TLS 建置必須更為主動。這並非一次就能完成的任務。促使流程自動化及簡化的工具至關重要。

SSL/TLS 通訊協定程式庫的更新會定期發佈 (例如 OpenSSL)，以抵禦此類漏洞攻擊，但網站擁有者仍須進行安裝。由 SHA-1 憑證移轉至增強的 SHA-2 也正在加速成長。不過， 企業還是必須妥善地部署新憑證，才能使變更有效。

網站管理員須考慮防護、偵測及應變，而不是單純考慮防護。網站管理員須使用自動化工具持續監控其網站的漏洞或攻擊跡象、阻止這些攻擊，然後再隨之報告、更新及修正。

SSL/TLS 和企業的應變

SSL/TLS 依然是線上隱私權、驗證及加密的核心，但需要有維護和警戒的信任基礎架構將其包圍，才能維持有效。企業必須學習及適應。

加密的演進

在 1994 年 8 月 11 日，Daniel Kohn 將 CD 賣給在費城的一位朋友。他的朋友使用信用卡消費 $12.48，再加上運費。這是第一筆受到加密技術保護的交易。Daniel 當時經營的網站要求客戶下載一種特殊的瀏覽器，以進行安全交易，該瀏覽器採用其網站信賴的 PGP 加密標準。

紐約時報在隔天的報導中發表評論：

> 「因層出不窮的網路安全性漏洞之報導而感到驚恐，許多人和企業不願意在網路上傳輸敏感性資訊，包括信用卡號碼、銷售資訊或私人電子郵件訊息。」

20 年後，人們的考量依然如昔，即使他們的行為顯示願意冒險在發生問題時，仰賴銀行的協助。然而，在缺乏一致且安全的 SSL/TLS 基礎架構下，這種狀態薄弱的信任將會瓦解，而電子商務將無法運作。

眾志成城

自 1994 年以來，SSL/TLS 的力量已取得很大的進展，而在業界標準往前邁進下，今年則已從 SHA-1 切換至 SHA-2。

隨著運算能力的增強，駭客也能透過天生的蠻力來破壞雜湊的演算法。許多專家預測 SHA-1 在不久的將來會變得容易遭受攻擊。這就是為何主流瀏覽器已協議在未來兩年內要停止支援 SHA-1 憑證。如此一來，若有任何訪客嘗試存取繼續使用此憑證的網站，將會看到一則安全性警告。

「目前的規劃是在 2017 年 1 月 1 日 [停止接受 SHA-1 憑證]。然而，有鑑於 SHA-1 的近期攻擊，我們也正在考慮將截止日盡可能提早到 2016 年 7 月 1 日的可行性。」Mozilla 表示，而且，陸續都有將這些日期進一步提早以加速變更的相關討論。

賽門鐵克提供免費升級服務，但大型企業須確保擁有適當的完整移轉規劃，以更新目前可能無法辨識 SHA-2 的任何裝置和應用程式。

瀕臨崩潰邊緣？

- 在 2015 年 3 月發現了稱為 FREAK 的漏洞。攻擊者會攔截受影響伺服器與用戶端之間的安全連線設定，可能會強迫使用「出口等級」加密，這比目前一般使用的加密形式弱很多。因此在現今可用的運算資源下，會讓交易訊息容易受到破解。
- 預估支援 9.6% 之前 100 萬個熱門網站網域的伺服器起初容易受到攻擊，而 9 個月後仍有 8.5%。

從漏洞潛入

即使加密已日漸強大，今年鎖定 SSL/TLS 的許多攻擊已將焦點集中在更廣泛的 SSL/TLS 生態系統之弱點。

賽門鐵克已發現去年焦點更集中在與 SSL/TLS 建置相關的程式碼程式庫，因此我們已目睹一連串定期的漏洞更新和修正。

這是個好消息。不過，去年最常見的是 Web 伺服器未經修正的漏洞。這表示網站擁有者並未跟上這些發佈。網站管理員須維護其 SSL/TLS 建置的完整性，這相當重要。這並非一裝即合，以後都不用再管的任務。

經掃描 Web 伺服器發現未提供修補程式的前 10 大漏洞

- POODLE (Padding Oracle On Downgraded Legacy Encryption) 利用過時的加密形式 (SSL 3.0)，而不是 TLS。

	名稱
1	SSL/TLS POODLE 漏洞
2	遺失的 X-內容-類型-選項標題
3	遺失的 X-框架-選項標題
4	已使用薄弱的雜湊演算法登入 SSL 憑證
5	跨網站程序檔漏洞
6	遺失的嚴格-傳輸-安全性標題
7	偵測到 SSL v2 支援
8	加密階段作業 (SSL) Cookie 中的遺失安全屬性
9	支援 SSL 薄弱的加密套件
10	SSL 和 TLS 通訊協定重新交涉漏洞

雖然我們並未發現任何和 2014 年的 Heartbleed 具有同等潛在危險的漏洞，但 OpenSSL 在 2015 這一整年中已發佈一些更新和修補程式。OpenSSL 是最廣泛使用的 SSL 建置和 TLS 加密通訊協定之一，佔所有 Web 伺服器的三分之二使用率。

它發佈的更新是針對遍及低度風險至高嚴重性的漏洞，而這可能會讓攻擊者得以執行攔截式攻擊以竊聽安全通訊，或發動阻絕服務攻擊。

檢查和制衡

為了強化 SSL/TLS 生態系統，賽門鐵克已力圖爭取 DNS 憑證授權中心 (CAA) 的普及採用。這可讓企業或 DNS 擁有者指定，要向哪個憑證授權 (CA) 購買 SSL/TLS 憑證。如果有惡意行為者或不清楚公司政策的員工，試圖從核准清單之外的 CA 購買憑證，該 CA 可檢查 CAA 並提醒 DNS 擁有者該要求。

這會降低在不知情的情況下，以合法企業之名稱發行流氓憑證的風險，從而降低讓罪犯得以設立已認證網路釣魚網站的風險。

為了更容易辨別出流氓憑證，賽門鐵克也正在遵循 Google 的要求，將我們發行的所有 EV 憑證記載在其憑證透明化記錄中。自 2016 年 3 月起，賽門鐵克也開始記錄 OV 和 DV 憑證。如其作者們所述，隨著可以監控和稽核憑證之軟體的運用，這建立了「一個公開的架構，可讓任何人以幾乎即時的方式，觀察及驗證新發行與現存的 SSL 憑證」。

信任服務、電子化辨識 (eID) 及電子化信任服務 (eTS)

在 2015 年 9 月，歐盟執行委員會已完成針對採用新式 eIDAS 規定所要求之所有執行法的採用。此規定是法規環境中的一項重大改變，在全歐洲的企業、公民及公家機關間開啟了安全且流暢的電子互動。

此外，這也是往前邁進的重要一步。透過合格信任服務之 EU 信任標記的執行，促使對憑證授權中心 (CA) 有更大的安全性要求。新信任標記將可協助您清楚區分合格的信任服務與市面上的其他服務，在此類重要線上服務培養更高的透明度與信心。■

社交媒體、詐騙及電子郵件威脅

社交工程與攻擊個人

在 2015 年，網路罪犯所使用之某些攻擊和戰術的複雜性與殘酷性表現出個人在線上是多麼脆弱，而且在線上安全方面，不斷削弱大眾的信任。資料外洩、政府監視，以及老式的詐騙手法集結在一起，對個人隱私展開進一步的侵犯，無論是個人照片、登入憑證或病歷。個人資料毫無隱私可言。

不要輕易相信任何人

在 2015 年，賽門鐵克看到了大量傳統的詐騙事件和惡意程式攻擊，目的是在收集個人資訊。例如，某個詐騙在 Instagram 上對大批追蹤者做出免費的保證，同時誘騙使用者洩露自己的密碼。某些冒充稅務官員的攻擊，企圖誘騙人們下載惡意程式電子郵件附件。

利用最簡單的方法，許多詐騙還是要靠一般大眾不良的安全習性而得逞。但是，我們也看到了安全性不佳的網站如何暴露客戶資料。在後面的例子中，如果網站很容易將資料外洩，則無論密碼有多強都是沒用的。

更令人擔憂的是，在 2015 年，利用複雜社交工程的攻擊，可規避專門保護使用者的雙重驗證系統。

藉由完成合法的密碼重設程序，並透過 SMS 來冒充 Google，詐騙可利用有聲譽之品牌的大眾信任來存取電子郵件帳戶，而不引起受害人的懷疑。

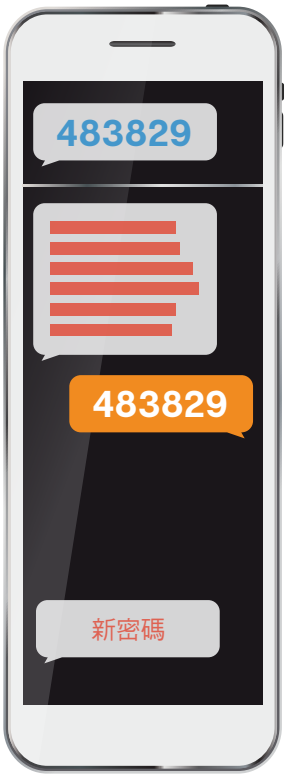
Gmail 詐騙的運作方式

攻擊者取得受害者的電子郵件地址和電話號碼（這兩項資料通常都可以公開取得）。

攻擊者偽裝成受害者，並向 Google 要求重設密碼。

3

Google 將代碼寄給受害者。



4

攻擊者利用類似以下訊息傳送簡訊給受害者：

「Google 偵測到您的帳戶出現異常活動。若要阻止未經授權的活動，請使用傳送到您行動裝置的代碼回應。」

5

受害者因此會預期收到 Google 傳送的密碼重設驗證代碼，並將代碼傳給攻擊者。

6

攻擊者接著便可重設密碼，一旦取得所需內容或設定轉寄，便可再次偽裝成 Google 通知受害者全新的暫時性密碼，將受害者蒙在鼓裡。

秘密與謊言

僅管傳統詐騙仍持續進行，2015 年也看到更多的色情詐騙和隱私權威脅。

線上「性勒索」已行之有年，最近的例子在亞洲尤為普遍，已轉向惡意的 Android 應用程式。這些詐騙者使用吸引人的頭像或個人檔案照片，鼓吹目標受害人分享明顯含有性內容的影片。然後，這些罪犯會鼓勵受害人使用 Android 應用程式「繼續聯絡」，從中收集受害人的電話號碼、帳戶詳細資料，及其所有聯絡資料。

現在，利用涉罪的影片，以及受害人親友的列表，結夥威脅受害人支付高額款項，否則要將明顯的性內容傳送給受害人所有的聯絡人清單。由於威脅性質非常敏感，受害人往往難以前往有關當局尋求協助，結果選擇支付數百甚至數千美元給攻擊者。

在 Ashley Madison 攻擊之後，隨之而來的是垃圾郵件的激增，已呈報的郵件帶有主旨行像是「如何檢查您是否遭受 Ashley Madison 駭客的攻擊」或「Ashley Madison 已駭客入侵，你的配偶是否欺騙您？」。這波入侵事件更不尋常的可能原因在於，其後果遠遠超出金融領域，影響人們的個人關係及聲譽。

使用社交媒體的社交工程

社交媒體仍是詐欺者青睞的目標，因為罪犯設法利用人們在自己的社交圈內的信任來散播詐騙活動、假連結，以及網路釣魚。為了成功，涉及的社交工程必須具有說服力，因此，我們看見更進步且更巧妙的戰術來欺騙可能的受害者。

某個詐騙特別費盡心力建立包含數十萬個 Twitter 假帳號的整個族譜資訊，每個分支持續提高可信度，以從真正的 Twitter 使用者獲得追蹤者與轉推數。在族譜資訊的頂端是冒充新聞媒體與知名人士的帳戶，甚至策劃來自真實帳戶的真實推文，使其看起來可信度更高。

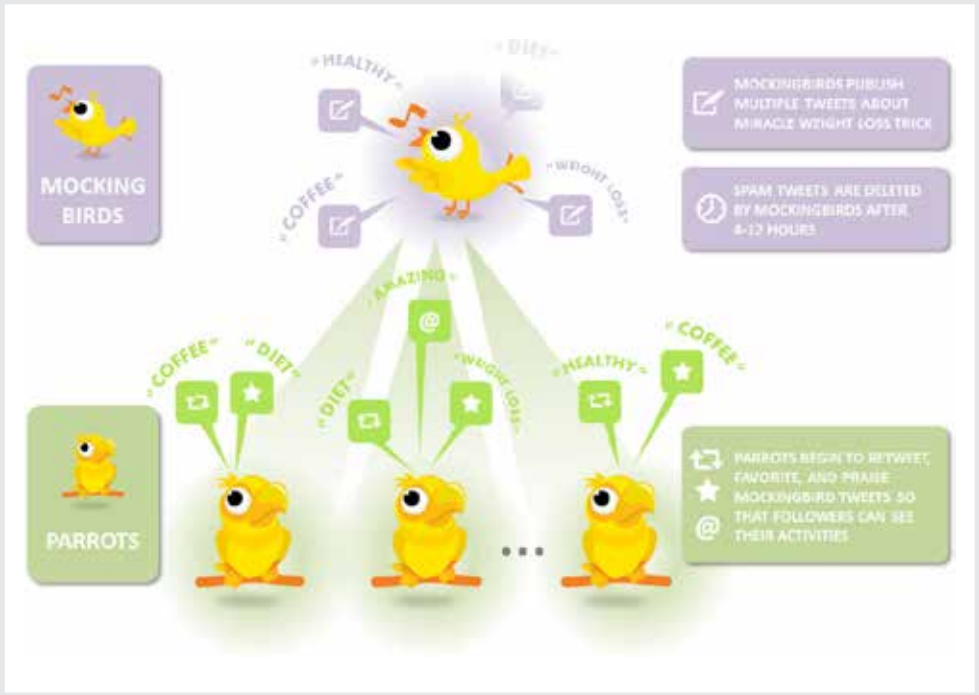
透過發現這些冒名帳戶，我們確定已使用三種帳戶：

- 「知更鳥」(Mockingbird) 帳戶：利用品牌與名人頭像假冒他人
- 「鸚鵡」(Parrot) 帳戶：使用竊取女性推文和圖片的假帳戶
- 「雞蛋」(Egg) 帳戶：使用預設的「雞蛋」頭像假扮成沒有任何推文的新使用者

來自「知更鳥」帳戶的每則推文收到將近 1,000 次轉推和 500 次收藏，但都不是真的，因為它們源自於第二帳戶，我們稱之為「鸚鵡」。因此，「鸚鵡」帳戶是一個非常有效的戰術，它會追蹤所有人，並且希望真正的 Twitter 使用者會追蹤回來。

如果這些「鸚鵡」帳戶只從「知更鳥」帳戶轉推垃圾內容，他們很快會形跡敗露，這就是為什麼他們也會張貼其他推文的原因，通常會複製來自真正 Twitter 使用者的推文並轉推即時動態資訊。

另一方面，大多數「雞蛋」帳戶從未撰寫單一推文。相反地，他們只會被用來加強數以百計的「鸚鵡」帳戶追蹤者數量。

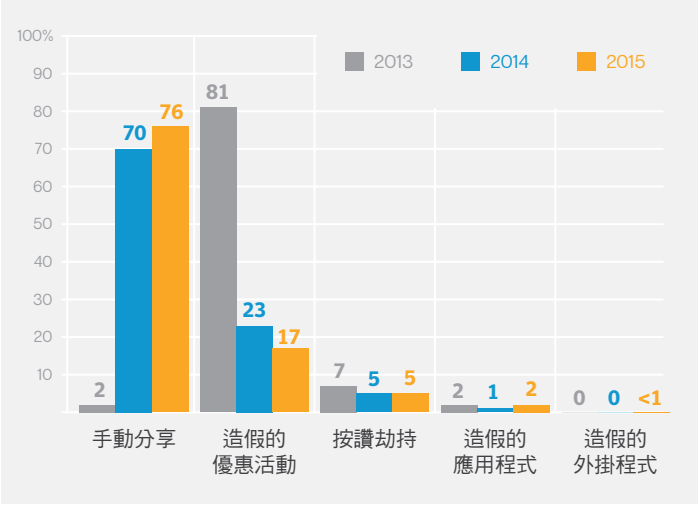


圖形顯示垃圾郵件的運作方式。擷取自白皮書。

這種複雜的作業集中在減肥的垃圾郵件。操作者費盡心力防止反垃圾郵件措施，並且能夠長時間執行。

社交網路詐騙需要某種形式的互動，而且手動分享仍是 2015 年社交媒體攻擊的主要途徑，在去年如滾雪球般的技術之下已不斷擴大。

社交媒體



- **手動分享** – 這些是靠受害者實際進行分享詐騙，透過向其展示動人的影片、造假的優惠活動或他們與朋友分享的訊息。
- **造假的優惠活動** – 這些詐騙邀請社交網路使用者加入附有獎勵的造假事件或群組，例如免費的禮品卡。加入時通常會要求使用者與攻擊者分享憑證，或傳送文字至高額收費號碼。
- **按讚劫持 (Likejacking)** – 透過造假的「讚」按鈕，攻擊者哄騙使用者按下會安裝惡意程式的網站按鈕，而且可能會在使用者的動態消息中發佈更新以散播攻擊。
- **造假的應用程式** – 邀請使用者訂閱看似與社交網路整合搭配使用的應用程式，但事實不然，而且可能會用來竊取憑證或收集其他個人資料。
- **造假的外掛程式** – 邀請使用者安裝外掛程式以觀看影片，但其為惡意外掛程式，且可能會在未經許可的情況下，重新發佈造假影片訊息至受害者的簡介頁以進行散播。範例包括：安裝造假的 YouTube 進階瀏覽器延伸功能以觀看影片、或出現需安裝 DivX 外掛程式的通知，以及確切而言各式各類造假的外掛程式。如需詳細資訊，請造訪：http://www.symantec.com/connect/blogs/fake-browser-plug-new-vehicle-scammers

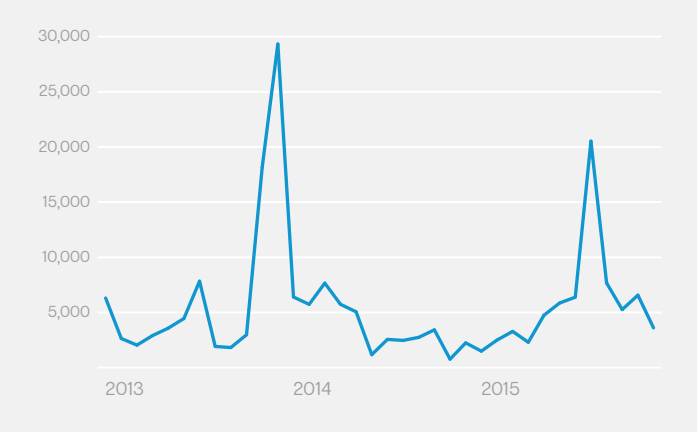
不受語言和位置阻隔

在 2015 年發現的其他形式攻擊，也證明了他們多麼樂於成為經驗老到且冷酷的犯罪份子以牟取利潤。無論您居住在哪裡，說著什麼語言，您仍可能處於網路攻擊者的威脅之下。以巴西的支付系統 Boleto 為例。Boleto 可視為非常當地的利基系統，但是在 2015 年，出現了三個專門針對它的惡意程式系列。

全球各地類似的本地化攻擊顯示，無論所在何處或何種語言，網路罪犯皆努力操控受害者。採用利用網路釣魚工具組的網路釣魚詐騙，使其非常容易對某個國家的目標進行活動、變更範本，以及快速地鎖定其他目標。通常，此類本地化攻擊使用的語言已透過範本自動轉譯，且對非母語人士而言可能具有說服力。

社交媒體上網路釣魚 URL 的數量

- 此圖表顯示社交媒體如何在過去攻擊的社交工程中扮演重要角色。近年來，這些網站已壓制此類濫用行為，並讓攻擊者更難利用它們。



抵禦社交工程攻擊

根據美銀美林全球研究 (BofA Merrill Lynch Global Research) 指出，網路罪犯每年耗費的全球經濟費用高達 5750 億美元，該報告接著表示，在可能的最壞情況下 (2020「Cybergeddon」案例)，網路罪犯可從 Internet 所建立的價值中汲取高達五分之一。

人人有責竭盡所能防止發生這種情況。

對消費者而言，是時候改變壞習慣了。很多人都知道網路安全的基本知識，但人們仍繼續共用密碼。事實上，在美國有超過三分之一的人共用密碼，且與網路銀行帳戶共用該密碼。人們需要對鞏固線上安全負起更多責任。

使用者應該對於在社交媒體上追蹤的對象更加謹慎。Bot 傀儡程式像真人一樣出現越來越多，而且有時難以察覺。當您選擇社交媒體上要信任的對象時，請考慮下列建議：

- **對於新的追蹤者保持懷疑的態度。**如果任何人追蹤您，請勿自動追蹤回去。查看他們的推文。看看他們的轉推內容看起來是否像垃圾郵件？如果是，很可能是 Bot 傀儡程式。
- **數字可能說謊。**即使這些隨機的追蹤者有成千上萬的追蹤人數，但這些數字可輕易造假。請勿根據他們的追蹤人數而決定追蹤他們。
- **查看「已認證」徽章。**Twitter 使用者在追蹤之前，應該一律先行檢查看看知名品牌或著名人士是否已經由 Twitter 認證。藍色的認證徽章表示 Twitter 已驗證帳戶的真正擁有者。

對網路安全冒險是無法接受的，我們應該屏棄隱私已不復存在的誤解。隱私權是非常珍貴的東西，而且應該悉心保護。

對於企業而言，這意味著在教育、網路安全意識訓練，以及良好的數位安全檢疫方面朝著安全努力。每一位員工應該致力於保持數位健全。CIO 與 IT 經理人員需要知道他們面臨多少風險，並開始主動監控症狀，以便在讓客戶資料與客戶信心置於風險之前，先診斷出數位問題。

電子郵件和通訊威脅

IT 系統持續受到快速演化的惡意程式攻擊。電子郵件仍是網路罪犯的選擇媒介，而且電子郵件數量持續增長，而網路釣魚和垃圾郵件衰退 – 後者佔了入埠電子郵件流量一半以上。網路釣魚攻擊的目標鎖定對象更多，而且惡意電子郵件在數量和複雜度方面不斷增長，突顯出電子郵件如何保持作為網路罪犯的有效媒介。

電子郵件濫用

無論企業和消費者使用之即時通訊技術的日益普及，電子郵件仍繼續佔領著數位通訊的主導地位。賽門鐵克估計，在 2015 年，每天大約有 1,900 億封電子郵件在流通，我們預計在 2016 年底會增加 4%。每個企業使用者平均每天會寄送 42 封電子郵件，而且越來越多人是在行動裝置上閱讀電子郵件。對於想要以電子方式與最多人數取得聯繫的網路罪犯而言，電子郵件仍是達成目的的不二首選。

難怪網路罪犯仍將電子郵件廣泛地用於垃圾郵件、網路釣魚，以及電子郵件惡意程式。在 2015 年，賽門鐵克看見電子郵件威脅的下滑。來自網路釣魚和惡意程式的電子郵件形式攻擊皆歸類於垃圾郵件，並佔了所有垃圾郵件的大約 1%。賽門鐵克進一步分析歸類為惡意程式及網路釣魚的垃圾郵件，因為這些威脅可能具有顯著的有害後果。

賽門鐵克掃描全球企業電子郵件流量的重要比例，讓我們直接瞭解此媒介及其帶來的安全性威脅。許多企業電子郵件永遠不會傳出企業外部，因為在四分之三入埠的外部企業電子郵件流量中，有一半以上是垃圾郵件。

垃圾郵件趨勢

在 2015 年，超過一半的入埠企業電子郵件流量是垃圾郵件，儘管近年來已逐漸下降。在 2015 年，垃圾郵件已達自 2003 年以來的最低水準。然而，垃圾郵件問題並不會消失。垃圾郵件作者正在尋找其他方式來接觸對象，包括使用社交網路和即時通訊，這兩種類型是行動裝置上找到的最熱門應用程式。除了利用電子郵件以外，垃圾郵件作者不斷尋求改進他們的戰術。

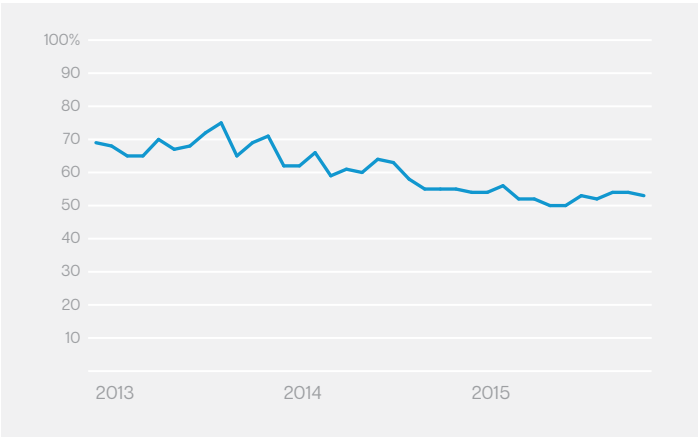
此外，賽門鐵克觀察到俗稱「雪靴垃圾郵件」的增加。比喻來說，雪靴是專為在廣大地區中分散穿戴者重量而設計，而雪靴垃圾郵件在廣大範圍的 IP 位址中配置大量的垃圾郵件。顧名思義，這種技術旨在藉由在極短時間內寄送大量的垃圾郵件，規避反垃圾郵件技術，例如擴散延遲和 IP 位址信譽。同時，藉由快速地輪替網域及重複循環 IP 位址，這可以使他們難以迅速攔截。

整體垃圾郵件比率

2013	2014	2015
		
66%	60%	53%
	減少 6 個百分點	減少 7 個百分點

每日估計的全球垃圾郵件比率

▶ 六月，垃圾郵件自 2003 年以來首次跌破 50%。



依產業區分的垃圾郵件比率

▶ 某些產業會收到比其他人多的垃圾郵件，但範圍大約只有 5% 左右。

產業詳細資料	電子郵件為垃圾郵件的百分比
採礦業	56.3%
製造業	54.2%
建築	53.7%
服務	53.0%
農、林、漁業	52.9%
零售業	52.7%
無法分類的機構	52.6%
批發業	52.5%
公共行政	52.2%
金融、保險及不動產業	52.1%
運輸及公共事業	51.8%
非標準產業分類相關的產業	
醫療保健業	54.1%
能源業	53.0%

依公司規模區分的垃圾郵件

▶ 沒有特定的公司規模會收到比其他更多的垃圾郵件，其範圍只有 1.5 %。

公司規模	電子郵件中的垃圾郵件 %
1-250	52.9%
251-500	53.3%
501-1000	53.3%
1001-1500	51.9%
1501-2500	52.6%
2501+	52.5%

網路釣魚趨勢

多年來，憑藉著不斷發展的網路罪犯市場，網路釣魚活動已變得更容易操作。攻擊者將透過一些專業的網路釣魚套件，與其他販售給想要進行網路釣魚活動的詐騙者合作。

這些套件通常是以 $2 美元到 $10 美元的價格來交換，而且其使用者不需要太多的技能即可操作這些套件或自訂其網頁，以滿足他們的需求。詐騙者可能會為了自身目的，使用從這些攻擊竊取的資料，或將其販售給地下市場以牟取利潤。

賽門鐵克報告指出，針對企業內的特定部門，嘗試進行網路釣魚的次數和複雜度不斷攀升。雖然有一些嘗試進行的網路釣魚似乎為顯而易見，例如假冒快遞追蹤的電子郵件，某些公司的法律和財務部門皆成為精心設計的網路釣魚攻擊目標。

其中一些包括嘗試轉帳，雖然看起來出乎意料，卻因為員工誤信電匯要求及其他真正的網路釣魚攻擊，某些公司已損失數百萬美元。涉及這些網路釣魚攻擊的社交工程更加複雜且更具針對性。它們不僅傳送一般詐騙郵件給大量的人們，同時也尋求開發長期的關係、驗證存取公司資訊，並建立信任。

社交工程需要研究與偵查、審查社交媒體簡介，以及潛在目標的線上活動，以瞭解他們的工作、同事及企業架構。此資訊可輕鬆地在線上取得，網路釣魚電子郵件更加個人化，並且有說服力 — 顯示對企業的認識，並瞭解主要執行者和工作流程。

許多企業成為首要目標，而且假設技術可提供自動保護是錯誤的觀念。僅管採用先進的控制機制和技術作為防護，企業仍有賴員工的能力，來偵測進階與目標鎖定的網路釣魚活動。

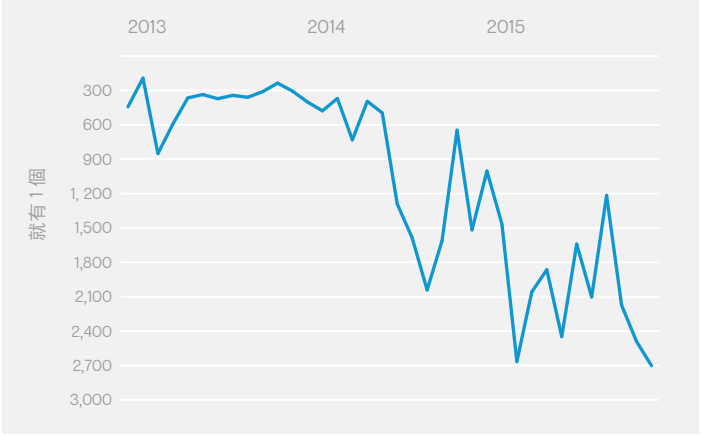
一次嘗試成功即可對公司聲譽和口碑造成嚴重損害。

電子郵件網路釣魚比率 (非魚叉式網路釣魚)

2013	2014	2015
每 392 個 就有 1 個	每 965 個 就有 1 個	每 1,846 個 就有 1 個

網路釣魚比率

▶ 網路釣魚數目在 2015 年不斷波動，但在整年之中仍維持逐步下降。



依產業區分的電子郵件網路釣魚比率

▶ 零售業是 2015 年最常受到網路釣魚攻擊的產業。

產業詳細資料	網路釣魚電子郵件比率
零售業	每 690 個就有 1 個
公共行政	每 1,198 個就有 1 個
農、林、漁業	每 1,229 個就有 1 個
無法分類的機構	每 1,708 個就有 1 個
服務	每 1,717 個就有 1 個
製造業	每 1,999 個就有 1 個
金融、保險及不動產業	每 2,200 個就有 1 個
採礦業	每 2,225 個就有 1 個
批發業	每 2,226 個就有 1 個
建築	每 2,349 個就有 1 個
運輸及公共事業	每 2,948 個就有 1 個
非標準產業分類相關的產業	
能源業	每 2,525 個就有 1 個
醫療保健業	每 2,711 個就有 1 個

電子郵件網路釣魚比率

▶ 沒有特定的公司規模會收到比其他更多的垃圾郵件，其範圍只有 1.5 %。

公司規模	電子郵件網路釣魚比率
1-250	每 1,548 個就有 1 個
251-500	每 758 個就有 1 個
501-1000	每 1,734 個就有 1 個
1001-1500	每 2,212 個就有 1 個
1501-2500	每 1,601 個就有 1 個
2501+	每 2,862 個就有 1 個

電子郵件惡意程式趨勢

就像網路釣魚詐騙一樣，分布在電子郵件中的惡意程式需要社交工程以說服其收件者開啟附件或點擊連結。附件可以偽裝成假發票、Office 文件或其他檔案，並經常利用開啟該類型檔案所使用的軟體應用程式來攻擊未修正的漏洞。惡意程式連結可能會使用網路攻擊工具組，將使用者引導至受入侵的網站，以放置某些惡意程式到他們的電腦。

像 Dridex 的威脅專門利用垃圾電子郵件活動，並在寄件者地址和電子郵件內文中包含真正的公司名稱。絕大多數的 Dridex 垃圾郵件偽裝成財務電子郵件，例如發票、收據和訂單。這些電子郵件包括惡意的 Word 或 Excel 附件，以及可放置專門鎖定網路銀行資訊之實際惡意程式的酬載。

這種特殊攻擊背後的網路犯罪集團已使用許多不同的技術來傳送垃圾郵件與惡意程式：從簡單的惡意程式附件、指向刺探套件登陸頁面之郵件內文中的超連結、惡意 PDF 附件，以及文件巨集。

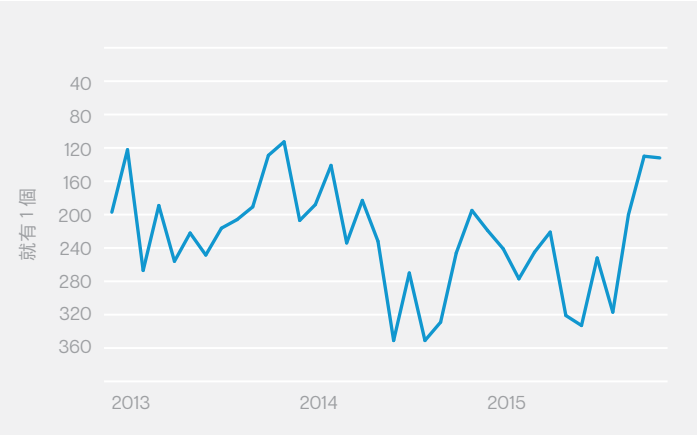
電子郵件惡意程式的衰退方式不同於一般垃圾郵件，而且相比之下，因為相對的低數量，更有可能受到波動。高峰出現在進行大型活動時。

電子郵件惡意程式比率 (整體)

2013	2014	2015
每 196 個 就有 1 個	每 244 個 就有 1 個	每 220 個 就有 1 個

電子郵件流量中偵測到病毒的比例

▶ 自 2014 年起，2015 年的整體電子郵件惡意程式比率已增加。電子郵件仍然是網路罪犯的有效媒介。



電子郵件中的惡意檔案附件

▶ 在 2015 年，Office 文件是最熱門的附件類型，帶有執行檔的附件變得越來越不受歡迎。1.3% 的附件類型為可執行檔，包括 .exe、.com、.pif 及其他類型。

排行	副檔名	在電子郵件中遭到攔截
1	.doc	55.8%
2	.xls	15.0%
3	.zip	8.7%
4	.htm	7.9%
5	.docm	2.4%
6	.js	2.2%
7	.mso	1.9%
8	.html	1.6%
9	.exe	0.9%
10	.png	0.8%

依產業區分的電子郵件病毒比率

- 在 2015 年，擁有惡意程式型惡意程式最高比率的產業為零售業，其中有超過 1% 的電子郵件歸類為惡意郵件。

產業詳細資料	電子郵件中的惡意程式比率
零售業	每 74 個就有 1 個
公共行政	每 151 個就有 1 個
農、林、漁業	每 187 個就有 1 個
服務	每 199 個就有 1 個
批發業	每 234 個就有 1 個
建築	每 240 個就有 1 個
製造業	每 243 個就有 1 個
無法分類的機構	每 277 個就有 1 個
採礦業	每 304 個就有 1 個
金融、保險及不動產業	每 310 個就有 1 個
運輸及公共事業	每 338 個就有 1 個
非標準產業分類相關的產業	
能源業	每 319 個就有 1 個
醫療保健業	每 396 個就有 1 個

依公司規模區分的電子郵件流量中惡意程式比率

- 電子郵件流量中惡意程式的最高比率是在 251-1000 位員工的公司規模分組。範圍是 0.4%。

公司規模	電子郵件中的惡意程式比率
1-250	每 184 個就有 1 個
251-500	每 82 個就有 1 個
501-1000	每 189 個就有 1 個
1001-1500	每 312 個就有 1 個
1501-2500	每 168 個就有 1 個
2501+	每 352 個就有 1 個

通訊攻擊

我們發現基本加密中成功的攻擊與漏洞都是用來保護電子郵件傳輸。例如，Logjam 攻擊利用金鑰交換機制的弱點，以啟動任何加密的交換。

- 使用賽門鐵克的 SSL 工具組，客戶可以檢查其網域是否有 Logjam 漏洞，以及其他重大漏洞。
- 使用此免費工具檢查重大問題 (例如 POODLE 或 Heartbleed)，以及您的 SSL/TLS 憑證安裝中的潛在錯誤。

電子郵件加密

電子郵件加密是有價值的，因為它保護郵件的隱私，並且有助於驗證寄件者。由於基礎技術中的漏洞 (請參閱以上內容)，同時也因為尚未廣泛使用而面臨威脅。

雖然網路郵件系統 (例如 Microsoft 的 Outlook.com 與 Google Mail) 在用戶端使用加密，而且幾乎所有電子郵件系統皆會為加密的傳輸排定優先順序，但是驚人比例的電子郵件會使用未加密的 SMTP 傳輸來傳送。Google 報告指出，在 2015 年，大約 57% 的入埠電子郵件已加密，而前年是 51%。同一時期，離埠加密電子郵件的數量已從 65% 上升到 80%。這對於某些要使用加密技術傳送的垃圾郵件是不尋常的。早在 2010 年，用於 TLS 加密的 Rustock 殭屍網路已作為掩護發送垃圾郵件的一種手段。

良好的桌面型與閘道型電子郵件加密工具確實存在，包括賽門鐵克本身的工具，但是企業需要善用其可用技術，以保護傳輸中和儲存中的電子郵件。

電子郵件安全建議

企業和個人需要明白，即使他們不認為自己是網路罪犯的明顯目標，但這並不表示他們是免疫的。

在個人層級上，這意味著保持警惕的方式如下：

- 請勿開啟來自不明寄件者的電子郵件
- 尋找鎖頭圖示，並在您輸入敏感性資料的任何網站上檢查加密憑證
- 存取敏感性資料時，切勿使用不安全的網路

企業保持警惕的方式：

- 盡可能部署電子郵件加密機制
- 確保電子郵件已針對惡意程式、垃圾郵件及網路釣魚掃描
- 使用網頁安全系統攔截對已知網路釣魚網站的存取

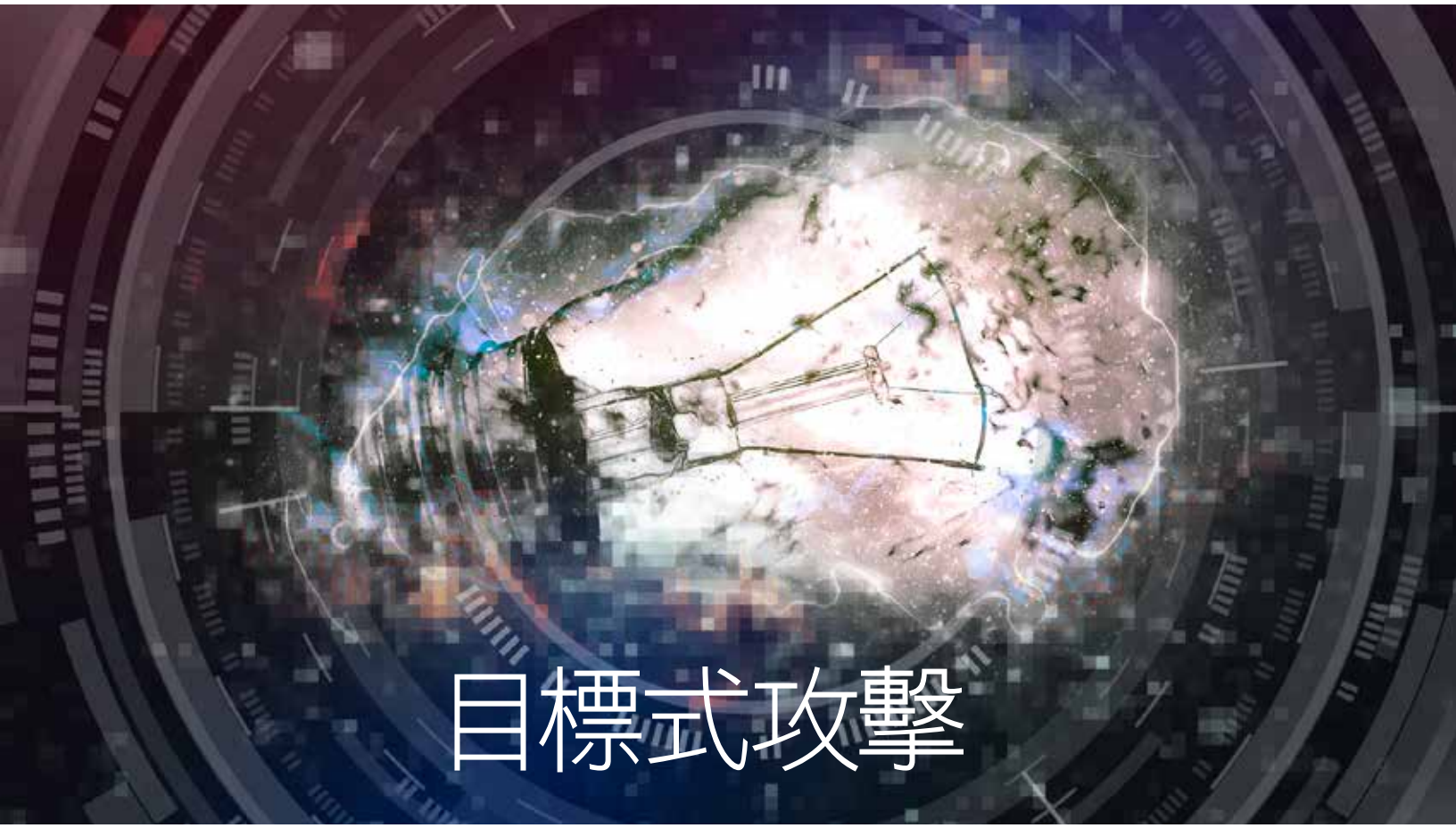
未來展望

隨著連續三年的下滑，如果不再繼續下降，我們期望網路釣魚攻擊至少維持目前水準。網路釣魚攻擊已變得更具目標性，而較少利用全面撒網的方式。許多攻擊都轉向社交媒體，加劇了電子郵件數量的下滑。全球某些地區比其他地方遭遇更多電子郵件網路釣魚攻擊 – 在許多英語系國家、北美以及西歐地區的跌幅最大。

人們將繼續在線上進行越來越多的動作，由於 Internet 存取和線上交易在開發中國家之間越來越普遍，我們甚至可以看到網路釣魚攻擊在這些地區的滋長。例如，支付水電費、預約醫生、申請大學、管理飛行常客帳戶，以及購買保險，全部皆為網路釣魚攻擊提供豐富的靈感。

隨著企業提供更多線上服務，他們需要注意到安全性的需求，必須與客戶協同合作，以進一步教育他們並建立信任。此外，他們可能需要考慮雙重驗證，以確保客戶的信心，並減少網路釣魚詐欺的成本。

正如我們所見，越來越多的網路罪犯轉向更複雜的電子郵件威脅，其中惡意程式作者、勒索軟體建立者、網路釣魚者，以及詐騙者會尋求利用他們認為連結中最脆弱的環節 - 人類。社交工程 (或「標頭駭客」) 對任何嘗試存取擁有潛在珍貴資訊的可能攻擊者而言，是一個重要的元素。■



目標式攻擊

目標式攻擊、魚叉式網路釣魚及智慧財產竊盜

針對政府機關與各種規模之企業進行的持續性且複雜的大範圍攻擊，對國家安全與經濟構成更大的風險。零時差漏洞數目逐漸成長，並揭露了其作為網路攻擊之武器的證明。魚叉式網路釣魚活動變得更加隱密，鎖定極少數所挑選企業中的少數個體。

持續性攻擊

在 2015 年 2 月，7,800 萬筆病歷記錄在 Anthem (美國第二大醫療保健提供者) 的一次重大資料外洩中曝露。賽門鐵克追蹤一個資金雄厚之攻擊組織的攻擊，名稱為 Black Vine，該組織與中國 IT 安全公司 Topsec 有關聯。Black Vine 負責使用客製開發的先進惡意程式，對多個產業進行網路間諜活動，包括能源業與航太業。

2015 年其他網路間諜活動的知名目標包括白宮、五角大廈、德國聯邦議院，以及美國政府的人事管理局，其遺失了 2,150 萬筆人事檔案，包括機密資訊，例如醫療與金融記錄、逮捕記錄，甚至指紋資料。

這些攻擊事件在世界各地之精密、資源充足，以及持久性網路間諜攻擊中不斷攀升。目標包括國家機密、智慧財產權 (例如設計、專利和計畫)，而且從最近的資料外洩、個人資訊即足以證明這一點。

賽門鐵克持續調查 Regin 木馬程式，讓我們進一步窺探到國家支援之攻擊者的技術能力。其揭露了 49 個新模組，每一個模組都

增加了新功能，例如鍵盤側錄、電子郵件與檔案存取，和廣泛的指令與控制基礎架構。賽門鐵克分析師評論表示，Regin 的成熟程度與複雜度顯示，此威脅的發展可能會讓資源充足的開發人員團隊花上好幾個月或好幾年來進行開發。

目前，利用遭受破壞的網站進行魚叉式網路釣魚和水坑式攻擊是目標式攻擊的偏好途徑。然而，隨著其他技術層引進企業，其攻擊層面更為廣泛。隨著企業轉為更偏向雲端技術和物聯網裝置的普遍性，我們預期看見在未來一兩年內，目標式攻擊會尋求利用這些系統中的漏洞。雲端服務特別容易遭受攻擊，例如 SQL 插入式攻擊，很可能會成為首要瞄準的目標。魚叉式網路釣魚活動依據使用者 (而非雲端服務供應商) 利用設定錯誤和不良的安全性，將成為攻擊者容易攻擊的對象。

為了規避偵測，魚叉式網路釣魚活動數量逐漸增加，但已成為鎖定每個活動中的少數個體。我們預計魚叉式網路釣魚活動將很快地僅包含一個單一目標，或在相同企業中少數挑選的個體。此外，更大型的魚叉式網路釣魚活動很可能透過採用高度覬覦零時差漏洞之遭受入侵的網站，全部使用網路型水坑式攻擊來進行。

零時差漏洞與水坑式攻擊

零時差漏洞對於攻擊者特別有價值。事實上，由於零時差漏洞似乎是少見的商品，攻擊者會密切防衛其攻擊，以便其可使用得更久，並且保持未被偵測的狀態。

精密的水坑式攻擊利用遭受入侵的網站，僅在造訪者進入源自特定 IP 位址的網站時才會啟用。以這種方式減少附帶損害，使其不太可能發現隱蔽的攻擊。此外，這種方式也對於可能從不同位置造訪網站的安全研究人員變得更加困難。一旦相關廠商公開揭露了攻擊，這些水坑式攻擊網站往往會針對不同的零時差漏洞，轉為使用另一個未公開的攻擊，以保持隱蔽。

2015 年的 Hacking Team 資料外洩事件引人注目的原因是，攻擊者並非為了金錢或身分；他們是為了追求網路武器，例如零時差攻擊。Hacking Team 是一間專門協助政府使用者執行秘密監控並開發間諜軟體的義大利公司。先前未知的零時差攻擊在攻擊行動中揭露，並由攻擊者公開。武器化零時差漏洞和集團使用之各種木馬程式的詳細資料會在幾天內於公開論壇中分享，並且在幾小時內，刺探套件作者已將其整合至刺探工具組。

零時差的多元性

2015 年發現 54 個前所未有的零時差漏洞，比去年發現的數量增加了一倍以上。發現未知漏洞，並指出如何利用這些漏洞，儼然已成為進階攻擊者的專門技術，而且此趨勢的變化沒有任何跡象。

零時差漏洞

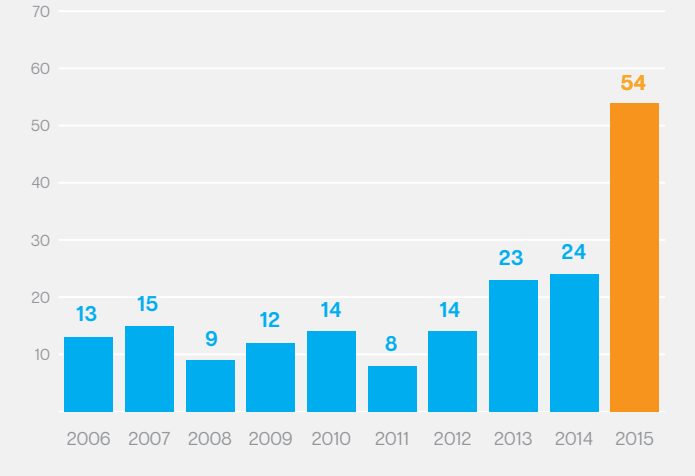
▶ 零時差漏洞在黑市中的價格昂貴。有鑑於此，並加上其本身性質，我們認為尚未發現之零時差漏洞的數量應該更多。

2013	變更	2014	變更	2015
23	+4%	24	+125%	54

在 2015 年發現的大部分零時差皆以鎖定多年之舊式、「準確可靠」的技術為目標。攻擊者在這一年內累計了10 個個別零時差漏洞來對付 Adobe Flash Player。Microsoft 從惡意的零時差開發人員獲得同等關注，雖然找到鎖定其軟體的 10 個零時差漏洞已散佈至 Microsoft Windows (6x)、Internet Explorer (2x) 以及 Microsoft Office (2x)。在 2015 年，也已透過四個零時差漏洞鎖定 Android 作業系統。

零時差漏洞，年度總數

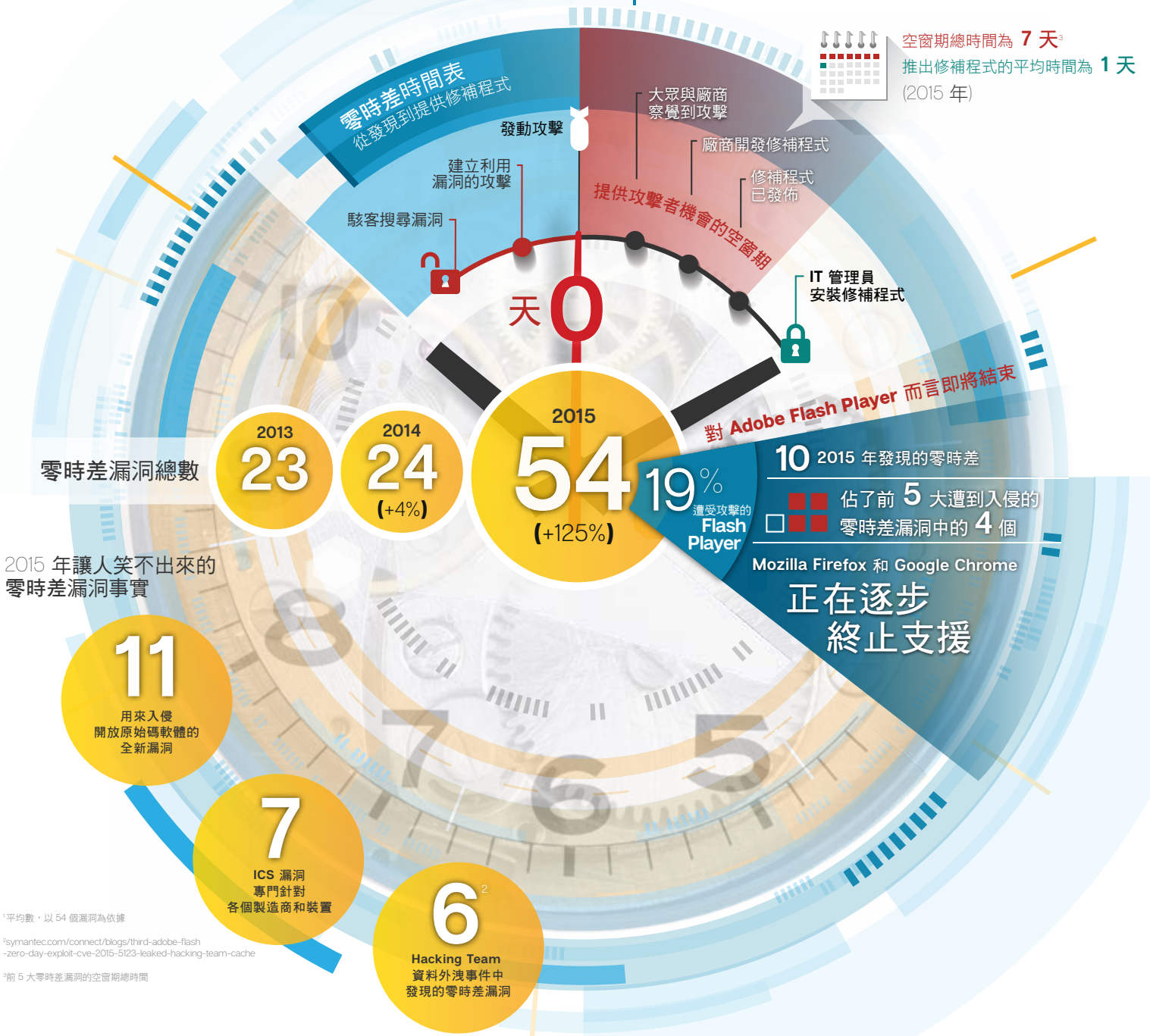
▶ 零時差漏洞的最高數量已在 2015 年揭露，證明此領域的研究市場已逐漸成熟。



2015 年每週發現的全新零時差漏洞[1]

進階攻擊團體仍然透過瀏覽器及網站外掛程式中未曾發現過的漏洞，持續獲得不法利益。

2015 年時發現了 54 個零時差漏洞。



[1]平均數，以 54 個漏洞為依據

[2]symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache

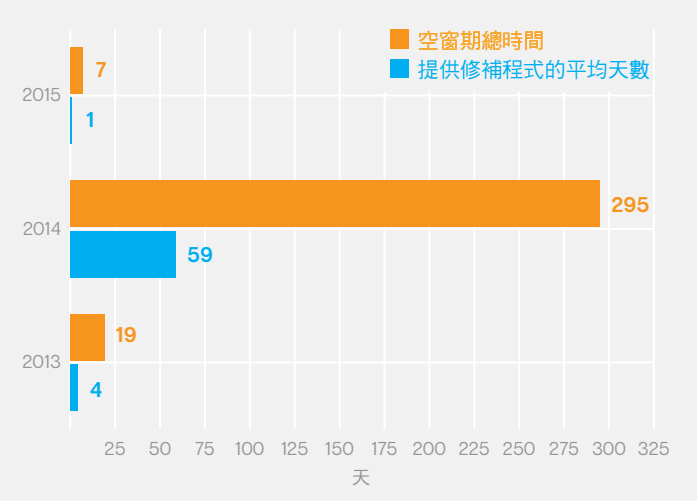
[3]前 5 大零時差漏洞的空窗期總時間

不足為奇的是，有 11 個零時差漏洞已用於攻擊開放原始碼軟體。有些攻擊已鎖定常用的程式庫與套件，而其他則以開放原始碼網路開發工具為目標，像是內容管理系統與電子商務平台。透過持續攻擊 OpenSSL 以及 Samba，網路通訊協定也被高度鎖定。

不過，值得大多數人關注的是，攻擊者似乎是在工業控制系統 (ICS) 中發現並利用零時差漏洞，ICS 是一種裝置，可用來控制從工業製造到發電廠的一切事物。在 2015 年期間，有七個已知的零時差漏洞鎖定各種不同的製造商和不同的裝置。

前 5 大零時差漏洞、修補程式及簽章時間

- 儘管 2015 年揭露了更多零時差漏洞，有一些是概念證明，但是比起 2014 年，廠商通常在 2015 年更快速地提供修正。



這種攻擊背後的動機並不明確，但是範圍可從地緣政治的紛爭到贖金相關的攻擊，一併涵蓋。無論如何，如果不仔細監控，此類攻擊在未來可能會造成更嚴重的後果，而且看起來不可能很快消失。

前 5 大最常刺探利用的零時差漏洞

- 除了 CVE-2015-0235 以外，最常鎖定的零時差攻擊與 Adobe Flash Player 中的漏洞相關。
- 此資料是以漏洞公開後發生的攻擊為準。

	2015 年攻擊	2015	2014 年攻擊	2014
1	Adobe Flash Player CVE-2015-0313	81%	Microsoft ActiveX Control CVE-2013-7331	81%
2	Adobe Flash Player CVE-2015-5119	14%	Microsoft Internet Explorer CVE-2014-0322	10%
3	Adobe Flash Player CVE-2015-5122	5%	Adobe Flash Player CVE-2014-0515	7%
4	堆積型緩衝區溢位亦稱為「Ghost」CVE-2015-0235	<1%	Adobe Flash Player CVE-2014-0497	2%
5	Adobe Flash Player CVE-2015-3113	<1%	Microsoft Windows CVE-2014-4114 OLE	<1%

在 CVE-2015-5119 的個案中，賽門鐵克已先掌握可偵測到攻擊四天的特徵，然後再公開揭露漏洞。有時候，現有的特徵可以成功阻止採用新漏洞的攻擊，而且即使事前已存在防護，仍會經常更新特徵以阻止更多攻擊。此外，此漏洞是在 Hacking Team 外洩中揭露。

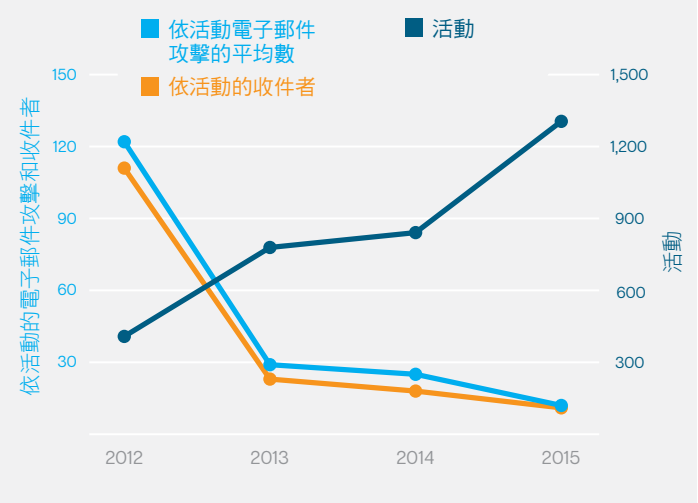
魚叉式網路釣魚

不只是可能包含隱藏攻擊的網站。先前未知的漏洞可能會利用附加在電子郵件中的受感染文件來攻擊企業。此類攻擊就是所謂的魚叉式網路釣魚，而且高度依賴良好的社交工程，以便偽裝成電子郵件以取得信任。

魚叉式網路釣魚電子郵件是以分批的方式，或是透過活動，傳送給極小群的人，通常不是一次傳送給所有人，而是單獨傳送或可能鎖定企業中一個以上的對象。久而久之，如果這些攻擊證明無效，則不同的攻擊可能會用來針對相同的人。不過，近年來，攻擊者在幾次嘗試失敗之後，快速轉換戰略，以保持不被偵測的狀態。在過去幾年中，他們越來越容易透過不同的攻擊，或鎖定企業中不同的員工，以持續進行攻擊。

魚叉式網路釣魚電子郵件活動

- 在 2015 年，活動數量不斷攀升，而每個活動中的攻擊數和收件者人數卻持續下降。隨著時間的縮短，這些類型的攻擊很顯然地變得更加隱蔽。



	2013	2014	2015
活動	779 +91%	841 +8%	1,305 +55%
依活動的收件者	23 -81%	18 -20%	11 -39%
每個活動的平均電子郵件攻擊數	29 -76%	25 -14%	12 -52%
活動的平均期間	8 天 +173%	9 天 +13%	6 天 -33%

魚叉式網路釣魚攻擊透過更小、更短且鎖定更少收件者的活動來進行，不太可能引起懷疑。幾年前，目標式攻擊活動可能已針對上百人或更多人，任何人都可能變得多疑並提高警覺。透過更少數的人，此比率已大幅降低。

在 2015 年，金融業是最大的目標，所有魚叉式網路釣魚電子郵件中，有 34.9% 是針對該產業中的企業，比去年高出 15%。一年至少發生一次以該產業中的企業為目標的可能性為 8.7% (大約 11 件就有 1 家是金融業)。有這麼多的攻擊針對該產業，某些公司會比其他公司更加積極的被鎖定。通常，這類企業可預計在一年中至少被鎖定四次。攻擊者只需要成功一次，而企業卻必須杜絕每一次的攻擊以保持安全。企業應該考慮發生此類安全缺口時 (並非假設)，該怎麼做。

成為魚叉式釣魚網站攻擊目標的產業排名

- 在 2015 年，我們將服務小組 (先前是「服務 - 專業」和「服務 - 非傳統」) 合併成一個群組。我們也發現了一些最常被鎖定的子產業，包含能源產業，其中包括一些採礦業和醫療保健，皆屬於服務類別的一部分。
- *「組織中的風險」圖是產業中的企業在一年內被攻擊至少一次的可能性衡量。例如，如果組織中有 100 名客戶，其中 10 名客戶為鎖定對象，則表示風險為 10%。

產業詳細資料	分佈	依企業的攻擊數	團體中的風險 %*
金融、保險及不動產業	35%	4.1	8.7%
服務	22%	2.1	2.5%
製造業	14%	1.8	8.0%
運輸及公共事業	13%	2.7	10.7%
批發業	9%	1.9	6.9%
零售業	3%	2.1	2.4%
公共行政	2%	4.7	3.2%
無法分類的機構	2%	1.7	3.4%
採礦業	1%	3.0	10.3%
建築	<1%	1.7	1.1%
農、林、漁業	<1%	1.4	2.0%
非標準產業分類相關的產業			
能源業	2%	2.0	8.4%
醫療保健業	<1%	2.0	1.1%

成為魚叉式釣魚網站攻擊目標的產業 (依群組區分) – 醫療保健

▶ 醫療保健屬於服務業標準產業分類群組，但我們特地在此提出來釐清。

產業詳細資料	分佈	依企業的攻擊數	團體中的風險 %*
醫療服務業	<1%	2.0	1%

成為魚叉式釣魚網站攻擊目標的產業 (依群組區分) – 能源

▶ 能源公司歸類在「採礦」類別或「運輸與公共事業」類別，視其業務性質而定。我們特地在此提出來釐清。

產業詳細資料	分佈	依企業的攻擊數	團體中的風險 %*
能源業	1.8%	2.0	8.4%
石油與天然氣開採	1.4%	3.4	12.3%
電力、天然氣和衛生服務業	<1%	1.6	5.7%
煤礦業	<1%	1.0	8.1%

成為魚叉式釣魚網站攻擊目標的產業 (依群組區分) – 金融、保險及不動產

▶ 存款機構包括零售銀行產業中的企業。

產業詳細資料	分佈	依企業的攻擊數	團體中的風險 %*
金融、保險及不動產業	34.9%	4.1	8.7%
存款機構	18.9%	5.9	31.3%
控股及其他投資辦事處	8.3%	2.9	11.0%
非存款機構	3.7%	6.7	5.3%
不動產	1.4%	2.4	2.2%
保險代理人、經紀人與服務	<1%	2.1	4.0%
保險人	<1%	1.6	10.1%
證券及商品經紀人	<1%	2.2	3.7%

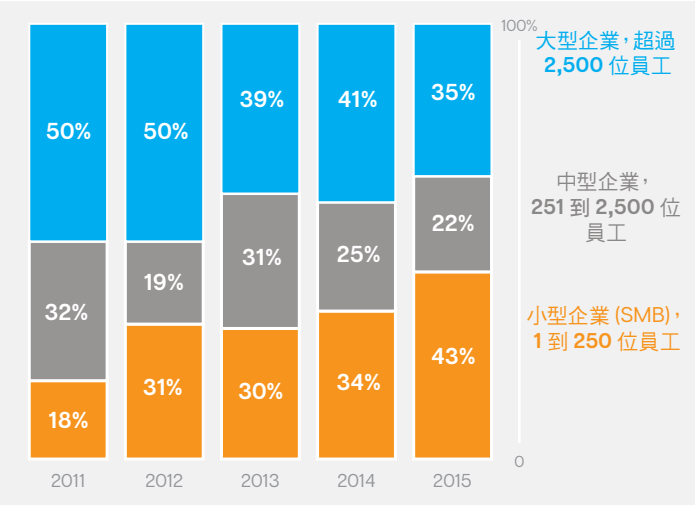
成為魚叉式釣魚網站攻擊目標的產業 (依群組區分) – 公共行政

▶ 公共行政業包括國家、中央政府機構，以及地方政府。

產業詳細資料	分佈	依企業的攻擊數	團體中的風險 %*
公共行政	2.0%	4.7	3.2%
行政、立法和一般	1.8%	5.7	3.6%
司法、公共秩序與安全	<1%	4.3	1.1%
經濟方案管理	<1%	1.1	7.3%
國家安全和國際事務	<1%	2.5	3.5%
人力資源管理	<1%	1.0	2.0%

魚叉式網路釣魚攻擊 – 依鎖定企業的規模

- 雖然許多攻擊是針對少數企業，但針對小型企業的攻擊在 2015 年持續增長 2%。



魚叉式網路釣魚攻擊的風險比率 – 依企業規模

- 鎖定小型企業的可能性是每 40 家就有一家 (3%)，表示攻擊已融合在少數企業中。大型企業的可能性是每 2.7 家就有一家 (38%)，這表示大型企業是更廣泛的攻擊焦點，具有更高的頻率。

產業詳細資料	2015 年風險比率	2015 年風險比率 (以 % 顯示)	依企業的攻擊數
大型企業 (員工人數大於 2,500 人)	每 2.7 個就有 1 個	38%	3.6
中型企業 (251 - 2,500 位員工)	每 6.8 個就有 1 個	15%	2.2
小型企業 (SMB) (1 - 250 位員工)	每 40.5 個就有 1 個	3%	2.1

目標式攻擊中使用的魚叉式網路釣魚電子郵件分析

- Word 和 Excel 之類的 Office 文件，在將惡意程式放到目標電腦之攻擊的傳送機制中，仍是相當受歡迎的媒介。令人驚訝的或許是執行檔類型仍然很受歡迎，不過，在 2015 年，魚叉式網路釣魚附件佔了至少 36%。在非鎖定式的電子郵件惡意程式中，執行檔附件佔了惡意程式附件大約 1.3%。

排行	附件類型	2015 年整體百分比	附件類型	2014 年整體百分比
1	.doc	40.4%	.doc	38.7%
2	.exe	16.9%	.exe	22.6%
3	.scr	13.7%	.scr	9.2%
4	.xls	6.2%	.au3	8.2%
5	.bin	5.4%	.jpg	4.6%
6	.js	4.2%	.class	3.4%
7	.class	2.6%	.pdf	3.1%
8	.ace	1.7%	.bin	1.9%
9	.xml	1.6%	.txt	1.4%
10	.rtf	1.4%	.dmp	1.0%

2015 年的主動攻擊團體

在 2015 年活耀的一些比較著名的目標式攻擊團體包含如下：

- Black Vine – 與 IT 安全公司 Topsec 相關聯的攻擊，主要鎖定航太業和醫療保健 (包括 Anthem)，尋找智慧財產和身分
- 進階威脅團體 9 (ATG9，亦稱為 Rocket Kitten) – 由伊朗人組成的團隊，針對記者、人權活動人士以及科學家進行國家支援的間諜攻擊
- Cadelle 和 Chafer – 由伊朗人組成的團隊，主要攻擊中東地區的航空業、能源業和電信業，有一間公司位於美國
- Duke 和 Seaduke – 主要對付歐洲政府機構、知名人士，以及國際政策和隱私研究機構的國家支援攻擊；賽門鐵克認為該組織從 2010 年就開始發動攻擊

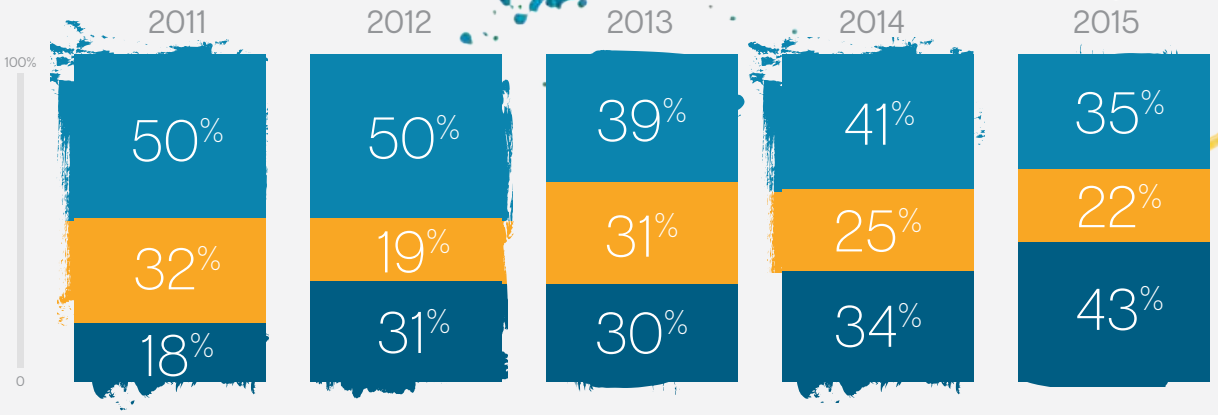
大小企業均是攻擊者的目標

如同在空白畫布上潑漆，無論規模大小，攻擊所針對的企業似乎都是隨意挑選。
如果要獲取利益，攻擊者會隨意發動攻擊。

專門針對員工人數**不到 250 名的企業**進行攻擊的情況，在近五年來有穩定增加的趨勢。

員工人數
- 大型企業，超過 **2,500** 位員工
- 中型企業，**251 到 2,500** 位員工
- 小型企業 (SMB)，**1 到 250** 位員工

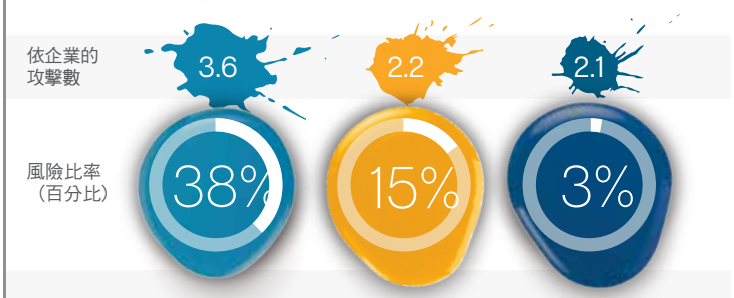
依目標企業規模區分的魚叉式網路釣魚攻擊



網路攻擊者打算長期針對大型公司，但所有企業無論規模大小，均暴露在目標式攻擊的風險之中。**事實上，專門針對員工的魚叉式網路釣魚活動數量在 2015 年成長了 55%。**

2013	2014	**2015**
779	841	**1,305**
+91%	+8%	**+55%**

2015 魚叉式網路釣魚攻擊的風險比率 — 依企業規模



- 進階威脅團體 8 (ATG9，亦稱為 Emissary Panda) – 針對金融、航空、情報、電信、能源和核子工程產業發動攻擊，以尋找智慧財產；著名的是利用 CVE-2015-5119 (Hacking Team 資料外洩事件中發現的零時差漏洞)
- Waterbug 和 Turla – 由俄羅斯人組成的團體，針對政府機構和大使館進行魚叉式網路釣魚和水坑式攻擊；賽門鐵克認為此團體是從 2005 年開始活躍
- Butterfly – 針對 IT、藥物、商品 (包括 Facebook 和 Apple 的內線交易) 等身價數十億元的企業進行攻擊

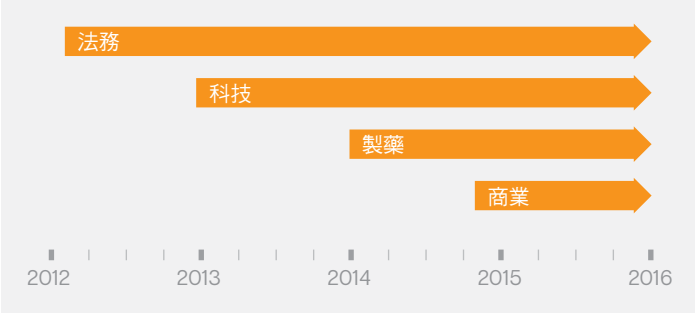
從高階企業攻擊和蝴蝶效應中獲益

Butterfly 是一群組織非常嚴密，而且能力非常高的駭客，其著眼於透過將市場機密資訊販售給出價最高的投標者，在各公司間進行間諜活動，以期在股市中獲利。攻擊者可能具有存取權的資訊類型包括電子郵件、法律文件、政策文件、訓練教材、產品說明，以及從專家安全系統收集得來的資料。此類遭竊資料也可能對於內線交易目的極具價值。

當這些攻擊在 2012 年和 2013 年危害某些知名公司 (包括 Apple、Microsoft 和 Facebook) 時，賽門鐵克是在當時初次發現這些攻擊。然而，他們也部署了精密的對策以掩蓋其追蹤，包括加密的虛擬命令與控制伺服器。

對產業發動蝴蝶攻擊 (Butterfly Attack) 的時間表

- Butterfly 團體已活躍好幾年，鎖定各種企業，包括與淬取天然資源相關的企業。
- 他們在攻擊中使用零時差漏洞，顯露出在商業動機攻擊中前所未見的精密程度。
- 圖形顯示 Butterfly 對不同產業領域攻擊時的時間表。



網路安全、網路破壞及應對黑天鵝事件

黑天鵝事件在發生時是史無前例和無法預測的；然而，在進一步分析之後，專家有時候會推斷其可能可預測。以前的人相信所有天鵝都是白色的，直到 1697 年，在澳洲發現黑天鵝，才有了「黑天鵝事件」一詞的出現。如果網路間諜活動很常見，網路破壞行動不普及可能是令人難以理解的事。造成實際損害的實際能力類似於網路間諜活動所需的能力，而且目標設定的逐漸增加得益於網路連線裝置的激增，包括工業控制系統。

英國政府 2015 年的安全與防衛評估井然地歸納出下列挑戰：

> 「威脅英國的網路行動者的規模已逐漸成長。威脅越來越不對稱，而且變得越來越全面。可靠且一致的網路防禦通常需要進階技術和大量投資。但是越來越多擁有國家級資源的州/省，正在開發可潛在部署於衝突中的先進能力，包括針對 CNI [關鍵國家基礎設施] 和政府機構。而非國家級的行動者，包括恐怖份子和網路罪犯可使用容易取得的網路工具和技術，以用於破壞用途。」

伊朗核計劃的 Stuxnet 網路攻擊是在實體架構上進行 Internet 攻擊的最著名例子。這可能是在不為人知的角落中發生的成功攻擊，或在某處感染，但尚未啟動。對於全世界重要的基礎架構皆能免疫是不太可能的事。2014 年末對德國鋼鐵廠的攻擊是個警告，預告著日後可能發生更嚴重的攻擊。

透過名為 Trojan.Laziok 的情報竊取威脅發現，有關網路破壞活動的可能揣測持續到 2015 年。這種特殊威脅似乎是專為中東地區的能源業進行偵查式攻擊所設計。Laziok 並未明確地設計用來進行攻擊重要基礎架構，而是收集有關其侵害系統的資訊。正如同在第 20 期 ISTR 中探討的，這些攻擊可以像對重要系統直接攻擊一樣強而有力，透過瞭解他們正遍歷的系統類型，提高攻擊者能力，以進一步滲透環境。簡而言之，如果攻擊者知道他們要入侵或可入侵的電腦類型，即可決定如何繼續攻擊其惡意程式的目標。

網路破壞和「混合戰」的威脅

混合威脅的概念已在網路安全方面出現很長一段時間，傳統上是指擁有許多不同攻擊媒介的惡意程式，例如將惡意的特洛依木馬程式碼放置到受感染的裝置，並感染系統上的其他程式碼，同時透過電子郵件或一些其他方式散播本身。然而，「混合戰」一詞是指一種戰爭類型，結合了傳統和非傳統的情報與網路戰爭。根據北大西洋公約組織指出：「此詞至少在 2005 年早期出現，隨後用來描述 2006 年黎巴嫩戰役中真主黨 (Hezbollah) 的策略。」

直到 2015 年底，有關網路破壞的揣測已轉變成此類攻擊的真正跡象。在 12 月 23 日，停電事件襲擊西烏克蘭的伊萬諾-弗蘭科夫斯克地區。在未來幾天和幾週多管齊下的網路攻擊之後，細節浮出水面，不僅在該地區的八個州省停電，同時也掩蓋了攻擊者的行動，使其難以評估停電的程度。

攻擊背後的惡意程式似乎是 BlackEnergy 木馬程式 (Backdoor.Lancafdo) 和 Trojan.Disakil 的強力組合。為了展開攻擊，BlackEnergy Trojan 最有可能用於貫穿整個網路，允許攻擊者收集有關他們入侵的電腦情報，直到連線至關鍵系統，讓他們可切斷與斷路器的連線，造成該區域的供電中斷。不過，它看起來不像是木馬程式自行中斷電力。相反地，它可讓攻擊者發現關鍵系統，然後得以全面控制系統，然後可在這些系統上使用原來的軟體擊垮電網。

值得注意的一點是，攻擊者似乎已計劃攻擊到這樣的程度，因此他們可將斷電時間延長到超過精確指定實際網路攻擊的時間點。他們能夠做到這一點的一種方法是，針對電力供應商的客服中心執行電話阻絕服務式 (TDoS) 攻擊，讓客戶無法撥打電話進來，並讓操作員留在黑暗中，以延長斷電的時間。

但是，這種快速決定性的攻擊似乎與在攻擊中使用 Trojan.Disakil 有關係。高度破壞性的 Trojan.Disakil 很可能用於覆寫系統檔案，並清除操作員可能會在電腦上著手重新恢復電力的主要開機記錄。因此，不僅會擊垮電力，也會攻擊用來恢復電力的系統，迫使操作員在通常可透過可用軟體恢復的情況下，手動恢復供電。

就像任何網路攻擊一樣，屬性是難以確定的。根據環境證據與目前的地緣政治紛爭，很容易得出結論；不過，在此個案中，沒有確鑿的證據。目前已知 BlackEnergy 木馬程式背後的集團已活躍多年，並已鎖定烏克蘭的多家企業，以及西歐國家、北大西洋公約組織和其他國家的企業。在這些攻擊事件發生的前後，也發現此集團攻擊烏克蘭的媒體企業。這可能不是我們聽到的最後一個攻擊事件。

烏克蘭的網路破壞攻擊活動，對於混合戰的使用與效果產生許多爭議，而且這似乎不會是此類攻擊的終點，特別是全球某些地區的國際局勢高度緊張，以及來自針對許多國家政府將網路恐怖主義提上議程的管理風險。

小型企業和隱私攻擊

小型企業當然有比較少的 IT 預算，因此，花在網路安全上的費用比起大型企業來說相對較少。不過，此趨勢已持續多年，儘管證據顯示每年魚叉式網路釣魚攻擊鎖定小型企業的傾向佔有較大的比例。

與 2014 年的 34% 相比之下，賽門鐵克在 2015 年阻絕了 43% 針對小型企業的魚叉式網路釣魚攻擊。此外，攻擊者的焦點縮小，主要針對少數企業，相較於前年的 45%，2015 年大約有 3% 的小型企業成為攻擊目標。這些企業一年平均至少有兩次成為攻擊目標。這項轉變是來自 2014 年對於分散更廣的攻擊全面撒網的方法，到了 2015 年，狙擊式的攻擊方法更減少了目標鎖定數，這也有助於這些攻擊能夠規避偵測。

最困難的挑戰是知道您的公司何時成為網路攻擊者的目標，特別是當大多數的網路安全頭條新聞著重於國家爭奪公司機密時，以及幾千萬筆信用卡詳細資料和其他個人資訊在外洩事件中洩露時。人們很容易相信目標式攻擊只會發生在其他公司。不過，沒有任何企業會因為規模太小或太不知名而不會成為鎖定目標，隱私攻擊事件就是一個很好的例子。

General Linens Service, Inc. 是一間非常小型的公司，只有一個據點和 35 名員工，也許看起來不太可能成為目標。他們為餐旅服務業提供亞麻布製品的服務，包括制服和地毯清潔。由於它似乎不可能成為國家的鎖定目標，因此它是隱蔽在網路兩年的 General Linen Services, LLC的競爭對手。也許公司名稱是刻意選擇相似的，因為他們可透過存取目標公司的發票來竊取客戶資料長達兩年之久，可讓他們查看對方的收費金額，提供顯著的優勢。問題是他們如何做到這一點；小型企業針對競爭對手展開網路攻擊似乎要使用極端的手段。然而，根據透露指出，攻擊者注意到兩家公司皆為其網頁的入口網站使用相同軟體，而且目標公司並沒有變更預設的管理密碼。這一點讓攻擊者存取他們的資料 157 次。好消息是，General Linen Services, LLC 已被逮捕並判有罪，而 General Linens Service, Inc. 發現下列安全性最佳實務準則的重要性。

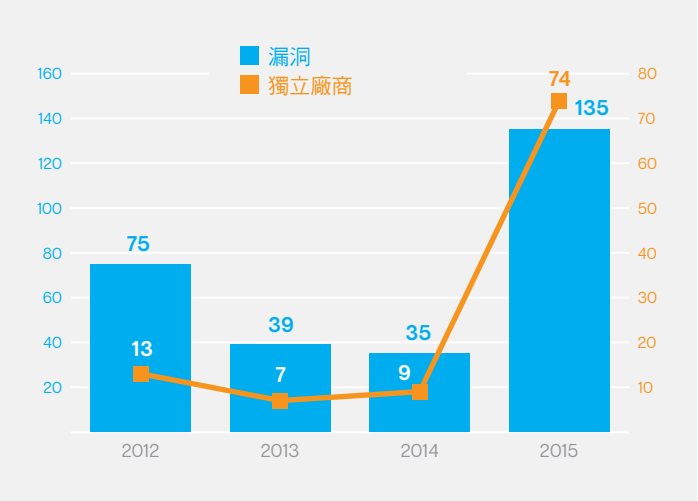
工業控制系統容易遭受攻擊

工業控制系統 (ICS) 應用在全球各地的工業生產與公用事業服務等眾多領域，並且經常連接至 Internet 以供遠端監控和控制使用。透過 2015 年這些漏洞數的逐漸增長強調，揭露這些系統中的漏洞是研究的主要領域。

影響 ICS 的實際漏洞數目估計要高出許多，因為許多企業藉由使用商用現貨軟體 (COTS) 產品來標準化其平台，例如 Windows 或 Linux 也會受到漏洞的影響，但這些都不會計入在內。此外，與企業網路連接的 ICS 管理系統會提高暴露於通常與這些作業系統相關聯之威脅中的可能性。

工業控制系統中揭露的漏洞

▶ 在 2015 年，至少有七個漏洞與各種不同的 ICS 製造商和裝置有直接關聯。



隱匿絕非防禦

抵禦網路間諜活動最有價值的保護方法是只要知道它是可能發生的。所有企業皆可能遭受利用水坑式攻擊和魚叉式網路釣魚等技術的目標式攻擊。小型企業與無名企業皆無保護。

事實上，在 2015 年，魚叉式網路釣魚攻擊的小型企業佔了較大比例 (43%)，但是成為鎖定目標的可能性已逐漸減少。當更多的攻擊已指定集團時，這些攻擊著重於更小型、更不顯眼的企業數 (3%)。

相對於大型企業，其佔了魚叉式網路釣魚攻擊 35%，每 2.7 家就有一家 (38%) 被鎖定目標至少一次。這意味著透過其方式，更加全面性的散佈活動，規模更廣泛。

確認風險之後，企業可採取步驟，透過下列方式來保護自己：審查其安全性和資安事端應變計劃、視需要尋求建議及協助、更新技術防禦、落實執行人事政策與培訓，並隨時更新保持最新資訊。■

資料外洩與隱私權

大小規模的資料外洩

無論是內部攻擊或是著重網站和銷售點裝置的網路詐騙，2015 年依然盛行的資料外洩讓受害者付出的代價更勝以往。自 2013 年來，超大型資料外洩的數量已攀升到最高點。資料外洩數量持續攀升，但其中並未公布外洩的完整範圍；除非法律要求，否則鮮少有公司會拒絕公布這些數字。

局勢現況研究報告

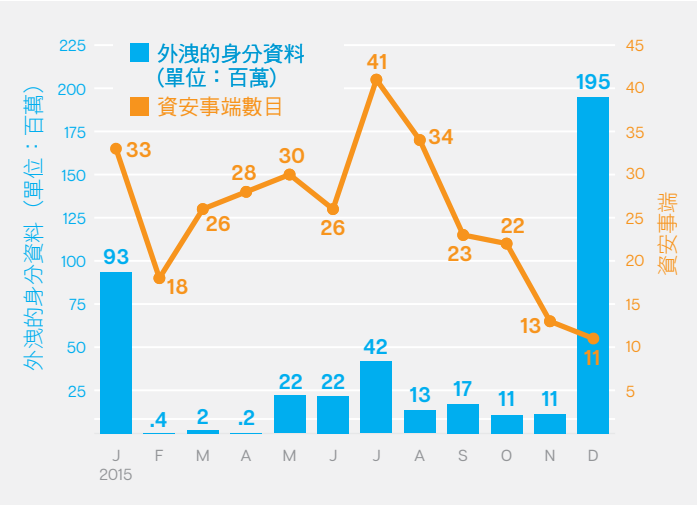
賽門鐵克數據顯示，資料外洩總數在 2015 年略升 2%。該年度也可觀察到共有 9 起超大型資料外洩事件，超越 2013 年 8 起資料外洩的記錄，其中每起事件包含 1 千萬筆以上的身分資料。另一項新記錄則是將近年底時所創下，共有 1 億 9,100 萬筆身分資料曝光，超越最大型單起資料外洩的過往記錄。

肇因於此大型資料外洩，曝光的身分資料總筆數躍升 23%，達到 4 億 2,900 萬筆。但是更令人關注的是，越來越多企業對於資料外洩的真正程度密而不宣，因此此數字可能會更高。2015 年時，回報的資料外洩數字 (不包含曝光的身分資料數據) 增加了 85%，從 61 攀升到 113。賽門鐵克估計曝光的身分資料總數 (若完整回報資料外洩) 可能至少有 5 億筆。

這個數字相當驚人，但由於資料並不完整，因此這也可能只是炒作出來的數據。每起漏洞事件曝光的身分資料平均數已減少了約 1/3，每起資料外洩事件達 4,885 筆。然而這並無法減少關注的原因，反而顯示出各起資料外洩事件中遭竊的資料更加珍貴，對企業造成的影響也比往年更大。

資料外洩時間表

▶ 2015 年 12 月的一起大規模資料外洩導致創下年度曝光身分資料的新記錄。7 月共有 41 起事件，也是資料外洩事件數字有史以來最高的月份。



因此，網路資安保險理賠也變得越來越普及。今年度的 NetDiligence Cyber Claims 研究發現，理賠金額高達 1500 萬美元，而一般理賠則在 3 萬美元至 26 萬 3,000 美元之間。但數位資產投保的價格則是不斷攀升，進一步促成資料外洩整體價格的高漲。

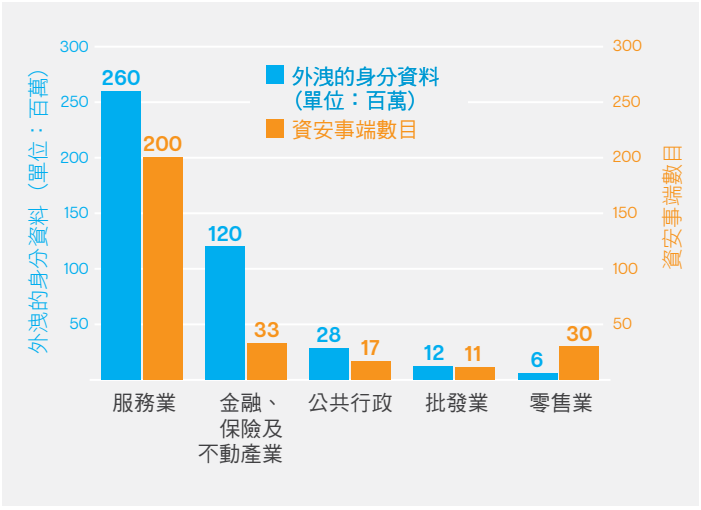
零售商的平均保險費在 2015 年上半年飆升 32%，而醫療保健業則有部分保險費成長 3 倍。根據路透社指出，現在普遍採用較高的自付額 (deductible)，即便是規模最大的保險公司，也不會針對風險客戶簽下超過 1 億美元的保險單。

綜觀各個類別的產業，無論在資安事端數量或曝光的身分資料方面，服務業遭受資料外洩攻擊的次數遠比其他產業要高。但是觀察這些上層分類之中的子產業，會發現每個案例的發生原因均不相同。

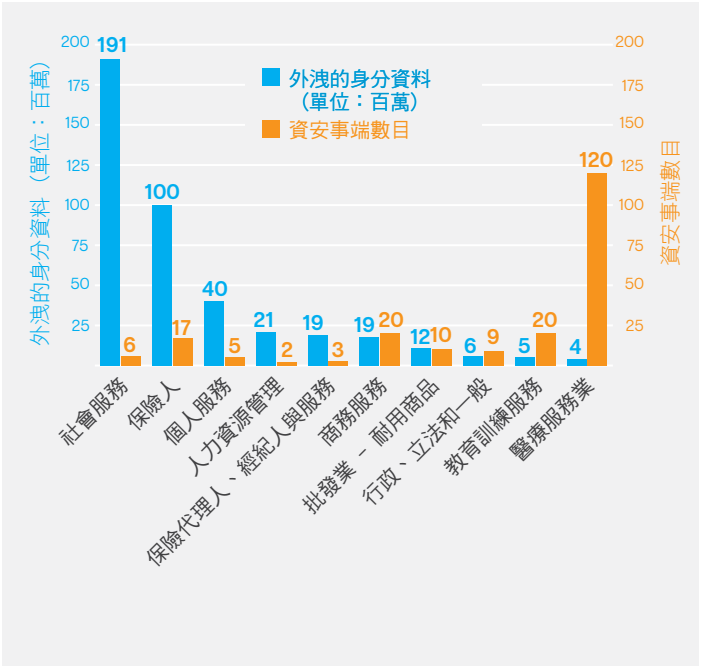
醫療服務子產業中出現的資料外洩事件數量最多，實際佔了該年度所有資料外洩的 39%。如果回報資料外洩的醫療保健業採用最嚴格的規則，這樣便完全不會感到意外。不過此產業曝光的身分資料數量相對來說比較少。資料外洩事件數字高，但曝光的身分資料相對低，由此可見資料本身相當珍貴，因此產生多起小型資料外洩事件。

造成絕大多數身分資料曝光的子產業，則非社會服務業莫屬。不過這大部分是因為這起打破記錄的資料外洩事件，共有 1 億 9,100 萬筆身分資料曝光。若忽略此項資料外洩事件，社會服務業則居於本清單的底部。(巧合的是，這也是此產業因為資料外洩事件數字而納入產業清單的原因。)

前 5 大遭外洩資料的上層產業 (根據曝光的身分資料數量及資安事端區分)



遭外洩資料的子產業排名 (根據曝光的身分資料數量及資安事端區分)



關於 Anthem 受到攻擊的實情

攻擊時間 2015 年 1 月 26 日

共有 7,800 萬筆病患記錄外洩。

一般認為此漏洞是一個網路間諜組織的傑作，該組織資源充沛，賽門鐵克稱其為「黑色藤蔓」**(Black Vine)**。該組織似乎可運用各種資源讓它持續一段時間執行多項同步攻擊。他們運用了：

- **攻擊者專屬的基礎架構**
- **零時差攻擊**
- **自訂開發的惡意程式**

三種變種的名稱分別是：

1) **Hurix**、2) **Sakurel** 及 3) **Mivast**

以 Trojan.Sakurel 的名稱被偵測到　Backdoor.Mivast

所有變種都具備下列能力：

- 開啟後門程式
- 執行檔案和指令
- 刪除、修改及建立登錄機碼
- 收集和傳輸遭入侵電腦的相關資訊

前 10 大遭入侵的子產業 (依資安事端數目區分)

醫療保健業	120	批發業	10
商業	20	餐飲業	9
教育單位	20	行政、立法和一般	9
保險業	17	存款機構	8
飯店業	14	社會服務	6

前 10 大遭外洩資料的產業 (依資安事端數量區分)

- 醫療服務是服務業中的子產業，服務業發生的 200 起資料外洩事件中有 120 起事件歸因於醫療保健。

	產業	資安事端數目	資安事端 %
1	服務	200	65.6%
2	金融、保險及不動產業	33	10.8%
3	零售業	30	9.8%
4	公共行政	17	5.6%
5	批發業	11	3.6%
6	製造業	7	2.3%
7	運輸 及公共事業	6	2.0%
8	建築	1	<1%

前 10 大遭外洩資料的子產業 (依資安事端數量區分)

	產業	資安事端數目	資安事端 %
1	醫療服務業	120	39.3%
2	商務服務	20	6.6%
3	教育訓練服務	20	6.6%
4	保險人	17	5.6%
5	旅館與其他住宿	14	4.6%
6	批發業 - 耐用商品	10	3.3%
7	餐飲業	9	3.0%
8	行政、立法和一般	9	3.0%
9	存款機構	8	2.6%
10	社會服務	6	2.0%

前 10 大遭外洩資料的產業 (依曝光的身分資料數量區分)

- 就曝光的身分資料而言，服務業佔了 60%，而社會服務子產業則佔了其中絕大多數。

	產業	資安事端數目	資安事端 %
1	服務	259,893,565	60.6%
2	金融、保險及不動產業	120,124,214	28.0%
3	公共行政	27,857,169	6.5%
4	批發業	11,787,795	2.7%
5	零售業	5,823,654	1.4%
6	製造業	3,169,627	<1%
7	運輸及公共事業	156,959	<1%
8	建築	3,700	<1%

前 10 大遭外洩資料的子產業 (依曝光的身分資料數量區分)

	產業	資安事端數目	資安事端 %
1	社會服務	191,035,533	44.5%
2	保險人	100,436,696	23.4%
3	個人服務	40,500,000	9.4%
4	人力資源管理	21,501,622	5.0%
5	保險代理人、經紀人與服務	19,600,000	4.6%
6	商務服務	18,519,941	4.3%
7	批發業 - 耐用商品	11,787,795	2.7%
8	行政、立法和一般	6,017,518	1.4%
9	教育訓練服務	5,012,300	1.2%
10	醫療服務業	4,154,226	1.0%

這不禁讓人疑惑，風險是如何成為資料外洩的因素。企業可能遭受大量的資料外洩事件或暴露大量身分資料，但這就表示資料本身的用途就是不良善的嗎？

舉例來說，48% 的資料外洩是因為資料意外曝光所造成。在這些案例中個人資料的確已經曝光，無論是公司共用資料的對象有誤，抑或網站設定有誤，導致不慎公開了私密記錄。但是這些資料被意圖不軌的人士掌握了嗎？在大部分情況下很可能不是。一名退休的奶奶意外收到含有他人醫療保健記錄的電子郵件，但不太可能運用此資訊並竊取其身分。這樣的情況並不是完全不會發生，只是這類型的資料外洩事件大多數風險較低。

如果駭客或內部竊取才是造成資料外洩的主因，這樣的風險就相對較高。在這些案例中，其動機非常有可能是竊取資料。有鑑於此，以下列舉幾項高風險產業。

針對資安事端篩選並肇因於駭客和內部竊取的產業排名

	產業	資安事端數目
1	醫療服務業	53
2	旅館與其他住宿	14
3	商務服務	14
4	批發業 - 耐用商品	9
5	教育訓練服務	9

醫療服務子產業依然穩坐事件數量的第一名，但現在第二名則是飯店及其他住宿子產業。有趣的是，在這項特殊的子產業中所有的外洩資料都涵蓋信用卡資訊，但確實回報遭竊的身分資料數量只佔了 7%。若是以高風險原因而論，商務服務業則從第二名下降至第三名。此產業中遭到入侵的公司主要是由線上企業或軟體製造商主導。

針對已曝光身分資料進行篩選，並肇因於駭客和內部竊取的產業排名

	產業	身分洩漏
1	保險人	100,301,173
2	個人服務	40,500,000
3	人力資源管理	21,500,000
4	保險代理人、經紀人與服務	19,600,000
5	商務服務	18,405,914

就具有資料外洩高風險的身分資料而言，保險人和保險代理人、經紀人及服務子產業都在前五名。這兩個子產業幾乎就佔了 2015 年將近一半的超大型資料外洩事件。這又呈現出另一個有趣現象：在和保險相關的資料外洩事件中，幾乎有 40% 都包含醫療保健記錄。假如醫療保健費用與涵蓋這類費用的保險公司有所重疊，那麼這樣的情況便可以想見。令人在意的是，攻擊者可能已經知道這類高價值資料可以透過保險相關產業取得，比起小型醫院或私人診所，這類產業可以獲得的數量更多。

依據任何其他名稱

可以掌握的個人詳細資料越多，就越容易進行身分詐騙。罪犯將鎖定保險、政府及醫療保健組織，竊取更完整的個人檔案資料。

竊賊需要的資訊類型在 2015 年依然相同，排名也只有些微更動。真實姓名仍是最常見的曝光資訊類型，佔所有資料外洩數字的 78% 以上。如同 2014 年，住家地址、出生日期、政府 ID (例如 SSN)、醫療記錄以及財務資訊均在 40% 至 30% 的範圍，不過出現的順序有些微改變。至於前 10 名，電子郵件地址、電話號碼、保險資訊以及使用者名稱/密碼則同樣以 10% 至 20% 的範圍出現。

這並不表示信用卡資料就不是常見目標。每張信用卡在黑市的價值不會特別高，原因是信用卡公司可以迅速發現異常的消費模式 (信用卡持卡人也可以)，而且遭竊的卡片資料和其他財務資訊的保存時間有限。然而竊取的信用卡資料仍有一定的市場。

前 10 大曝光的資訊類型

▶ 財務資訊包括遭竊的信用卡詳細資料和其他金融憑證。

	2015 年類型	2015 %	2014 年類型	2014 %
1	真實姓名	78%	真實姓名	69%
2	住家地址	44%	身分證字號 (例如 SSN)	45%
3	出生日期	41%	住家地址	43%
4	身分證字號 (例如 SSN)	38%	財務資訊	36%
5	醫療記錄	36%	出生日期	35%
6	財務資訊	33%	醫療記錄	34%
7	電子郵件地址	21%	電話號碼	21%
8	電話號碼	19%	電子郵件地址	20%
9	保險	13%	使用者名稱與密碼	13%
10	使用者名稱與密碼	11%	保險	11%

儘管美國引進 EMV 標準 (亦即「密碼刷卡」技術) 意謂著罪犯將來透過銷售點 (POS) 裝置取得的資訊價值將會降低，但對於罪犯而言，零售業仍是一個利潤豐厚的產業。EMV 是一項針對使用微晶片的卡片所設立的全球化標準，自 1990 年代到 2000 年代早期某些國家便已採用此項技術。EMV 可用來驗證密碼刷卡交易，而隨著近幾年眾多的大型資料外洩事件以及信用卡詐騙比例攀升，美國的信用卡發卡公司試圖轉而使用此技術，以減少這類詐騙帶來的影響。

以往罪犯可以取得「磁軌 2」(Track 2) 資料，也就是針對儲存在信用卡磁條上的部分資料進行速記。此方式更容易複製信用卡，而且如果取得 PIN 碼，也可在商店甚至 ATM 上使用。磁軌 1 (Track 1) 儲存的資料比磁軌 2 更多，而且包含持卡人姓名、帳戶號碼以及其他任意資料。如果在航空公司使用信用卡預約時，此時航空公司會使用磁軌 1。這類資料的價值也反映在線上的黑市售價；每張卡片的磁軌 2 資料價值高達 100 美元。

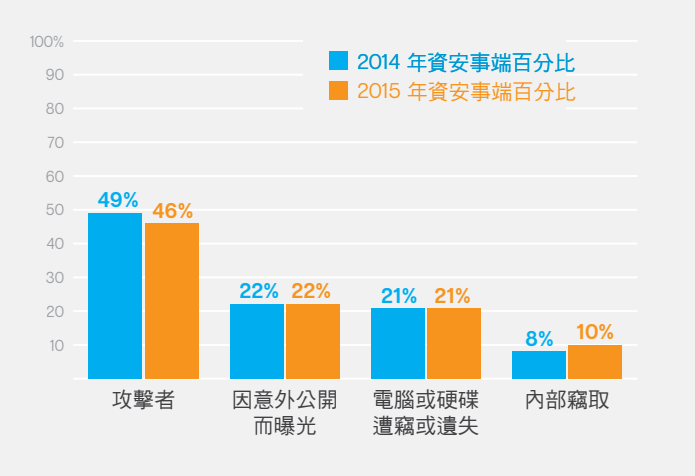
截至 2015 年 10 月為止，有 40% 的美國消費者持有 EMV 卡片，而估計有 25% 的商家將支援 EMV 技術。信用卡如果轉而採用 EMV 標準，複製起來便更加困難，因為若要使用卡片，必須搭配 PIN 碼使用。雖然這樣的轉換再搭配 POS 安全機制的其他改善措施可能需要好幾年才能完全實現，但若要大規模竊取 POS 將變得更加困難，而且罪犯所獲得的利潤勢必也會減少。

內部人員威脅

雖然內部竊賊只佔了 2015 年資料外洩的 10% 左右，但 NetDiligence Cyber Claims 研究報告指出，2015 年提出的理賠中，內部人員涉案就佔了 32%。Ashley Madison 總裁表示，一名心生不滿的內部人員被指控必須為該年度其中一起最為公開的資料外洩事件負責。雖然該事件尚未定案，但如果屬實，則突顯出意圖不軌的內部人員可能造成的潛在傷害。

資料外洩主因 (依資安事端區分)

▶ 涉及內部竊取的資安事端比例從 2014 年不到 1%，在 2015 年攀升到 10%。



2015 年有超過 5 億筆的個人資訊記錄遭竊或遺失

比起以往，有更多公司不願完整回報資料外洩的程度

36% 資料外洩事件

醫療服務子產業中出現的資料外洩事件數量最多，實際佔了該年度所有資料外洩的 39%。如果提報資料漏洞的醫療保健業採用最嚴格的規則，這樣便完全不會感到意外。

39%

120 包含醫療記錄的

4 百萬 外洩的身分資料

2015 年的統計數據

已外洩的身分資料**提報總數**

數量（單位：百萬）

2015	429	+23%
2014	348	-37%
2013	552	

由於許多公司拒絕完整透露資料外洩的程度，因此這些數字可能會更高。

大多數的冰山隱匿在水中，水底下還有巨大的冰體隱而未現。關於資料外洩所提報的外洩身分資料數量，猶如冰山一角。還有哪些隱匿未現？

提報的外洩身分資料

Anthem 共有
7,800 萬筆
的病患記錄外洩

美國人事管理局共有
2,200 萬筆
個人記錄外洩

未提報的外洩身分資料

雖然許多公司不願回報實際已外洩的記錄數量，但可能已經有超過數億人遭到入侵。

2014 **61**

2015 **113** +85%

2015 年未提報的外洩身分資料事件

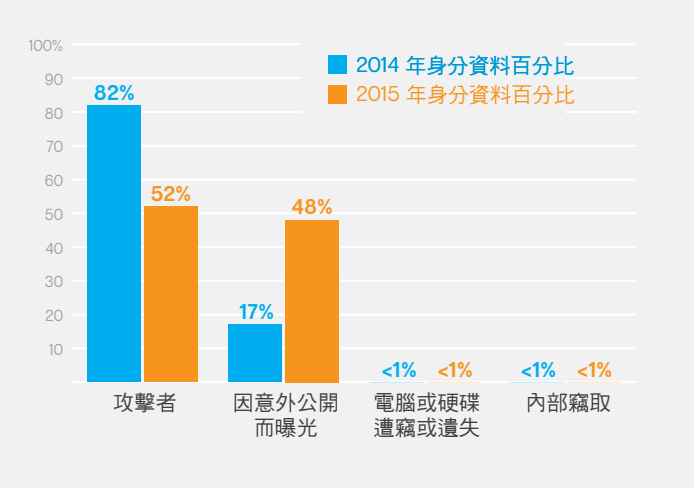
有鑑於這樣的事實，可能有

500 百萬* 筆身分資料已遭到外洩

*預估

資料外洩主因 (依曝光的身分資料區分)

- 因意外公開而曝光的身分資料比例從 2014 年的 22% 攀升到 48%。



因意外公開而曝光的身分資料比例從 2014 年的 22% 攀升到 48%。

內部人員威脅已成為網路安全的一項熱門主題，但在 2015 年時，政府機構不僅開始留意，更進一步採取行動。

- 根據 MeriTalk 聯邦內部威脅報告指出，超過 3/4 的美國政府機構表示比起去年，他們的機構花費更多心力專注於對抗內部人員威脅。
- 英國國防企業中心在 2015 年贊助了多項專案，旨在監控員工的數位行為，以便預測並即時找出內部人員威脅，同時透過學習模擬工具協助人員找出風險。

隱私法規和個人資料價值

網路罪犯不僅對於「擁有入侵能力的人」感興趣，「洩漏資料的人」也會引起他們的注意。無論資料遭竊的原因是資料外洩事件、意外洩漏或甚至過去合法張貼在網路上，個人資料在地下經濟中仍有其價值。直到最近，許多人均未發現個人識別資訊的潛在價值，而且對於這類資訊的防護態度又顯得無關緊要。近十年來社交媒體的出現，讓更多人分享更多的個人資料，比例之高前所未有，但隱私控管卻不是許多社群網路應用程式的首要之務。

無論是執行身分詐騙、強化網路釣魚詐騙的社交工程，甚至作為目標式攻擊開端的事前偵察，都可以/也將會使用個人資料犯案。當不肖人士發現這類資料的潛在價值後，促使社群網路服務開始加強並嚴密執行隱私控管，也有越來越多人更重視自己的個人資料。舉例來說，歐盟法院在 2014 年 5 月裁定的「被遺忘權」(right to be forgotten) 在資料收集社群中掀起一陣浪潮，而在 2015 年年底也讓 Google 一共收到 348,085 則刪除特定搜尋結果的要求。

根據 Google 的常見問題集指出，許多人認為此舉只對想要隱瞞醜聞或避免罪證的人有利而已，不過要求移除的常見案例中有一部分則是包含個人聯絡或地址資訊的網站，網站中甚至包含「僅涉及個人健康、性取向、種族、民族、宗教、政治派別及工會地位相關資訊的內容」。

隨著歐盟法院裁定 2000 年的「安全港協議」無效後，今年再次引起大眾對於隱私的重視。根據歐洲消費者聯盟總監 Monique Goyens 解釋，這項裁定確認「允許美國公司僅透過宣稱遵守歐盟資料保護規範的方式，而無任何主管機關進行審查的協議，明顯沒有存在的必要。」英國衛報 (The Guardian) 當時評論這可能「有助於阻止美國政府透過歐盟取得使用者的資料」，同時「可能從使用者和資料監管機構方面展開深入調查、投訴及訴訟。」

然而，在 2016 年 2 月，歐盟委員會和美國同意跨大西洋資料流動的新架構：歐美隱私屏障 (EU-US Privacy Shield)。新架構專門處理裁定舊式「安全港架構」無效之後，歐洲法院所載明的需求。新聞稿指出，「此項新安排將會針對美國公司提供更嚴格的義務，以保護歐洲人的個人資料，並由美國商務部和聯邦貿易委員會 (FTC) 提供更強大的監控與執行，包括透過與歐盟資料保護機關的加強合作。」

調查遍及歐洲的七千人，賽門鐵克「2015 隱私現況報告」(2015 State of Privacy Report) 指出，在英國，只有 49% 的消費者擔心他們的資料不安全。而在整個歐盟地區，最不信任比率為：科技公司 (22%)、零售商 (20%)，以及社交媒體公司 (10%)。賽門鐵克察覺由於對這些公司缺乏信任所造成的聲譽問題，可能是從最近備受關注的資料外洩資安事端所產生。

我們預計不願意分享個人資訊的人將不斷增加，並且開始改變消費者的線上行為。資料隱密性變成此類關注的其中一個主要原因是，現今的消費者清楚地瞭解他們的資料保存價值。當涉及資料隱密性時，技術服務供應商應該特別留意，因為消費者只能信任技術部門做出正確行動來保護資料，未來幾年需要做更多工作來建立並維持所需的信任等級。

由於不斷發生資料外洩事件，而且人們的生活逐漸轉向線上，因此，我們希望在 2016 年之後，可看見在保護個人隱私權方面，能受到更多管制並享有更多司法權益。在如何保護資料安全方面，企業與客戶之間需要更加透明化。安全性需要嵌入公司的價值鏈中，但是它也應該在內部視為贏得客戶關係的需求，而不僅僅是成本。

賽門鐵克政府事務資深總監表示：「確實有實際一致的觀點，顯露隱私權是企業的競爭優勢，而且隱私權問題也決定了消費者的行為。關鍵是要確保消費者有權瞭解其資料的用途，以及如何保護其資料。」

降低風險

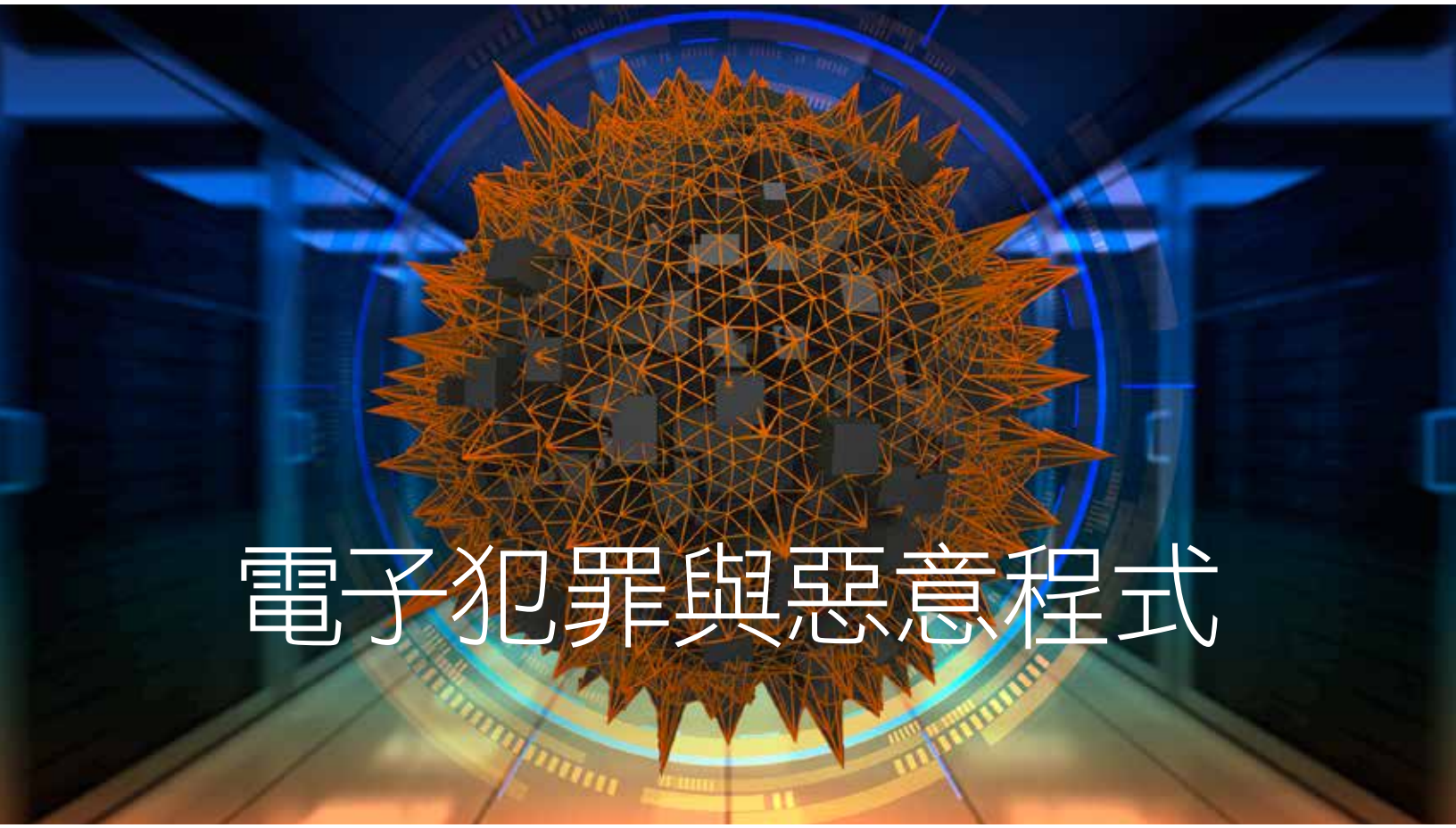
儘管這些都是重要的步驟，但是透過基本常識也可避免大量的資料外洩，包括：

- 修正漏洞
- 保持良好的軟體檢查功能
- 部署有效的電子郵件過濾
- 使用入侵預防與偵測軟體
- 限制第三方存取公司資料
- 適時部署加密機制以保護機密資料
- 實作 Data Loss Prevention (DLP) 技術

當然，這些都與防止外部人員攻擊有關。當涉及到減緩惡意程式的風險或意外的內部人員威脅時，企業需要著重在員工教育與防止資料外洩。

就像教育大眾在醫院裡咳嗽要捂住嘴巴或消毒雙手一樣，我們應該使用相同的方式來訓練員工基本的安全檢查功能。企業也應該使用防止資料外洩技術來尋找、監控及保護其資料 – 無論是否在企業中 – 以便他們能即時知道誰正在做什麼、使用何種資料。DLP 可防止某些類型的資料從企業外流，例如信用卡號碼和其他機密文件。

安全性應該是營運和員工行為最基本的一環，而非附加項目或應付稽核人員的要素。資料外洩不太可能隨時停止，但是如果企業意識到安全性遠超出 CIO 或 IT 經理人員的限制，則其規模和影響肯定會減少。安全性掌握在每個員工的手中。■



電子犯罪與惡意程式

地下經濟與執法機構

地下經濟正在迅速發展，網路犯罪同樣快速成長，但正如我們所見，2015 年重大逮捕與截獲事件的數量正在提升，無論網路罪犯身在何處，執法機關現在也能迅速跟上罪犯的腳步。勒索軟體攻擊日益多元化，其攻擊對象包含 Linux Web 伺服器，而且加密型勒索軟體也不斷成長。

網路影子下的企業

無論是追求的目標或要求的贖金方面，網路罪犯變得越來越專業，作風也相對大膽。這些犯罪企業認為自己是全方位企業，涵蓋各個領域，每個領域都有自己的專長。如同合法企業擁有合作夥伴、合夥人、經銷商及廠商等，這些企業同樣也隱匿在影子下經營。

近幾年黑市的電子郵件地址價格偏低，信用卡則維持相對低廉但穩定的價格。然而如果是「奢華」資料，亦即有效的賣家帳戶驗證或尚未遭到凍結的信用卡驗證，則價格相對水漲船高。

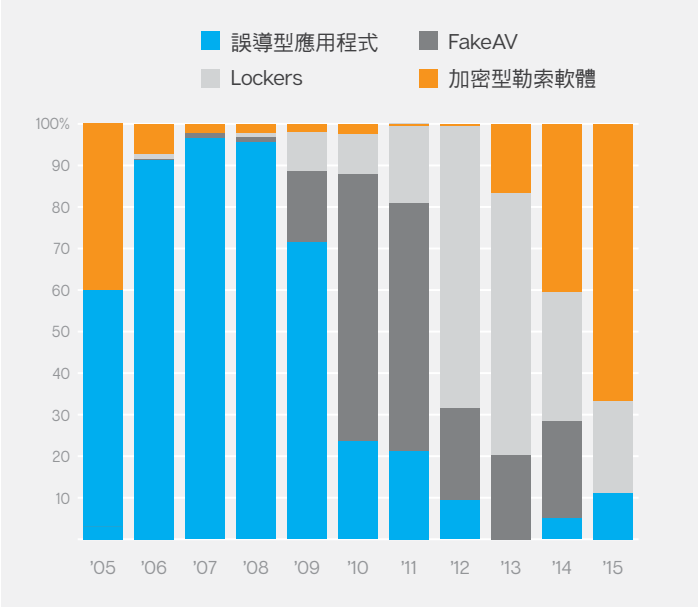
在市場另一端，偷渡式下載 Web 工具組 (含更新及 24 小時全天候支援) 每週的租用費為 100 美元至 700 美元不等，分散式阻絕服務 (DDoS) 攻擊每天的訂購金額則在 10 美元至 1,000 美元之間。而市場頂端的零時差漏洞售價則高達數十萬美元。而這些數據自 2014 年來就少有變動。

挺身而出

勒索軟體在近幾年漸漸成為主流，而在 2014 年有許多人預見這個趨勢將會持續下去。然而我們觀察到勒索軟體攻擊越來越多元，但數量上卻無明顯增長。攻擊目標已轉往行動裝置、加密檔案，以及使用者必須付費才能復原的任何內容。

加密型勒索軟體日益成為主流

▶ 2005 年至 2015 年之間辨識出的全新系列誤導型應用程式、假冒的安全軟體 (假冒的防毒軟體)、鎖定勒索軟體 (locker ransomware) 及加密型勒索軟體的比例。



2015 年時一名賽門鐵克研究員展示了智慧電視可能容易受到勒索軟體的攻擊，儘管目前尚未觀察到這個趨勢。

現在有些勒索軟體也會威脅在網路公布受害者的檔案，除非受害者支付贖金；如果維持有效備份的傳統建議在此情況下毫無助益，這樣有趣又險惡的手法比例很可能就會提高。

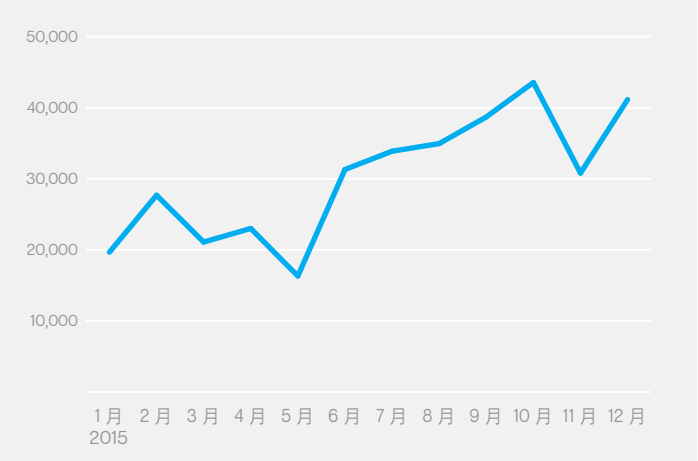
在人類歷史上，世界各地的人們從未經歷過規模如此龐大的勒索事件。但為何罪犯對勒索軟體情有獨鍾，尤其是加密型勒索軟體？隨著黑市充斥著遭竊資訊，以及在美國推出更安全的 EMV 標準 (密碼刷卡 (chip-and-PIN)) 金融卡作為卡片付款方式後，罪犯利用遭竊的信用卡詳細資料所能獲得的潛在利潤已然減少。

信用卡詐騙必須多人才能執行，而消費者立法可確保將受害者的財務損失降到最低。相較之下，攻擊者可以透過地下來源取得勒索軟體工具組，並鎖定想針對的受害者，而受害者除了支付全額贖金，可能別無選擇。罪犯無須透過中間人即可直接付費購買，而受害者的損失也無從減少，因此可獲得最大利潤。

為了對受害者施壓要求支付全額贖金，加密型勒索軟體的一項伎倆就是威脅在一段時間後破壞私密金鑰的唯一複本，而加密的資料可能就會永遠遺失。

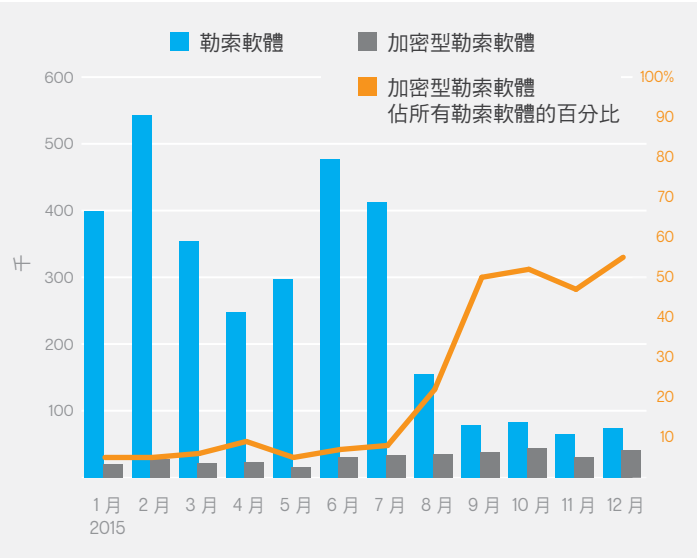
各時期的加密型勒索軟體

▶ 隨著越來越多的傳統鎖定式勒索軟體迅速退燒，加密型勒索軟體卻持續成長。加密型勒索軟體採用相當強大、明顯牢不可破的金鑰加密手法挾持受害者的個人檔案進行勒索，並使用只有罪犯才能存取的金鑰將檔案加密。

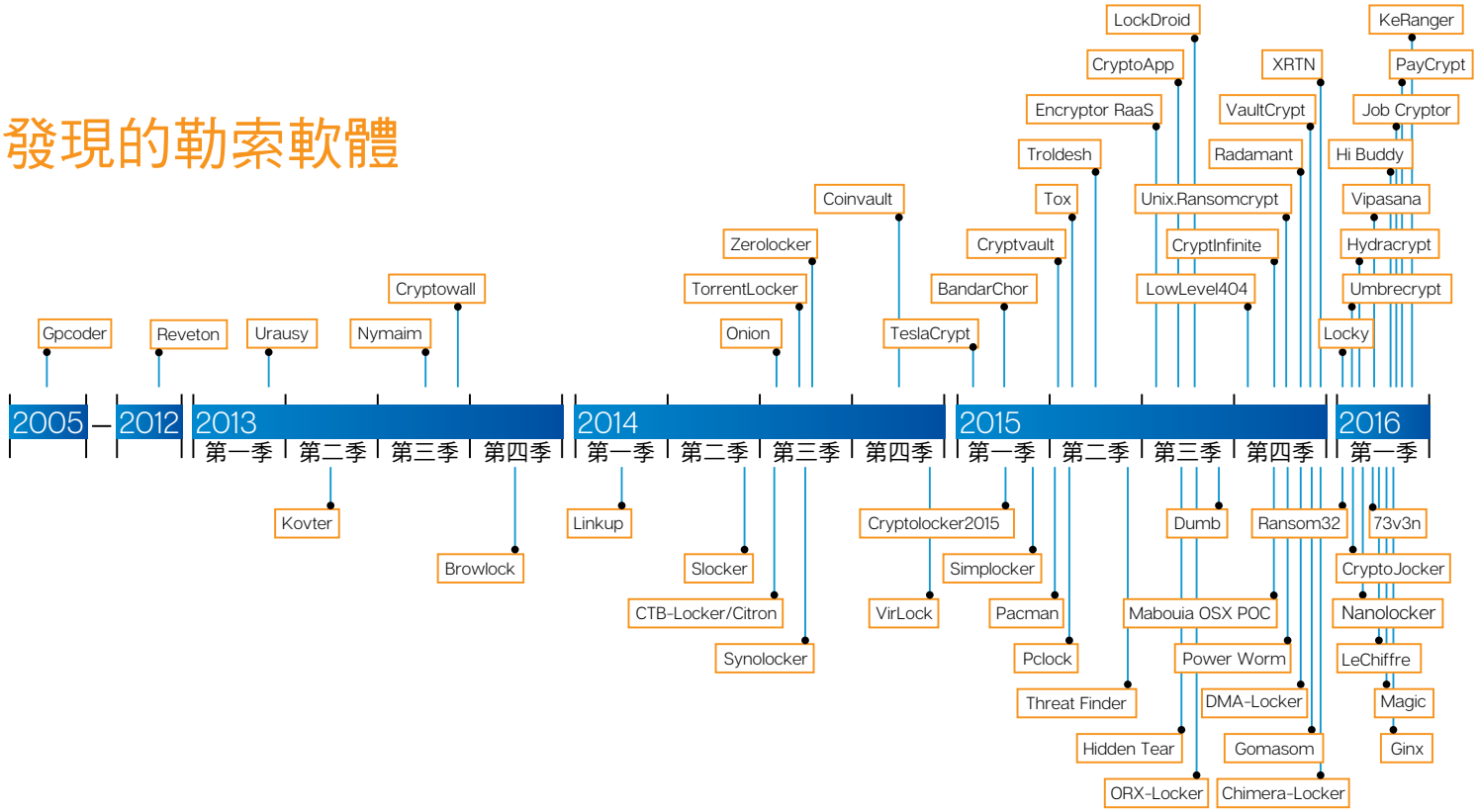


加密型勒索軟體佔所有勒索軟體的百分比

▶ 雖然本圖表顯示 2015 年傳統勒索軟體有穩定下降的趨勢，但加密型勒索軟體目前仍佔據所有勒索軟體的絕大部分。



發現的勒索軟體



2015 年時勒索軟體也會鎖定 Linux Web 伺服器，將與 Web 應用程式、封存檔及備份等有關的檔案加密。Linux 勒索軟體的進化也反映出 Windows 勒索軟體的幾個特點：初始版本相當基本、加密手法拙劣、要復原加密的檔案相對簡單。然而就像使用 Windows 勒索軟體，我們可以預見隱匿在這項新趨勢背後的罪犯將迅速從錯誤中學習，未來將發動更精密複雜的攻擊。

全球問題，本地攻擊

隨著美國總統選舉逼近，引導受害者接觸惡意程式的垃圾郵件不斷使用美國總統初選作為釣餌。垃圾郵件作者善於玩弄深入內心、扣人心弦的主題，例如全球事件、中東難民危機、移民、以及外交政策議題、經濟，甚至恐怖主義等。

2015 年 1 月時，美軍指揮部的 Twitter 和 YouTube 帳戶遭到自稱聖戰恐怖組織 ISIS (又稱為 IS、ISIL 或達伊沙 (Daesh)) 的支持者入侵。美軍中央司令部表示這是「網路破壞行為」，而非嚴重的資料洩漏。

但是 2015 年 4 月時，法國電視網路 TV5 Monde 回報他們遭到宣稱隸屬恐怖組織 ISIS 的團體入侵。根據相關報告指出，在這次攻擊中不僅電視台停擺，其網站和社交媒體網頁同樣中斷無法使用。駭客張貼聲稱是身分證的文件，以及在伊拉克和敘利亞參與反 ISIS 作戰的法國士兵親戚簡歷。

這兩個案例突顯了一個情況：恐怖份子運用網路威脅作為大肆散佈訊息的工具。Internet 不僅成為線上激進份子專用的工具、恐怖組織之間溝通的媒介，更是籌措營運資金的利器。因此，要求執法機關破解加密通訊協定整體上對於 Internet 通訊技術完整性來說，很可能造成廣泛且深遠的影響。

提到恐怖主義，近期有個電子郵件活動模仿中東及加拿大當地的執法機關官員，冒充成能夠讓目標受害者避免於所在位置遭受恐怖攻擊的安全秘訣，欺騙民眾下載惡意程式。該封電子郵件偽裝執法機關的位址，並列入活動期間仍在職的官員姓名。電子郵件的主旨列通常會反映出任職於目標公司的員工姓名。

為了讓這類型的攻擊更有說服力，需進行相當程度的研究，而我們觀察到該組織確實研究後才寄出這些網路釣魚電子郵件。再者，在沒有任何員工資訊的情況下，他們會將電子郵件寄給公司裡的其他人作為開端，例如客服人員或 IT 人員。

這樣的研究與在地化程度顯示出專業水準不斷提升，而這樣的情況在傀儡網路詐騙中越來越普及。地下經濟不僅僅是銷售遭竊的

商品而已，更是具備如同合法企業部門可以預見的專業人才與組織之完整企業。

傀儡網路與僵屍電腦的崛起

如同其他眾多產業，新興經濟 (特別是中國) 已成為 2015 年網路犯罪的青睞目標。其中一項重大因素便是去年採用的寬頻明顯成長。中國政府在 2013 年公布拓展寬頻覆蓋範圍的計畫，到了 2020 年範圍將涵蓋鄉村與城市。這項全面策略的其中一個里程碑就是在 2015 年時要讓 4 億戶中國家庭享有固定寬頻連線。此外，隨著寬頻速度增加，價格依然相當低廉。對於想要入侵全新高速網路連線電腦來源的網路罪犯而言，上述各點都足以讓中國成為目標。

依來源分類的惡意活動：Bot 傀儡程式

▶ 中國是 2015 年眾多 Bot 傀儡程式活動的來源，該國的 Bot 傀儡程式相關活動迅速增加了 84%。相較之下，美國的 Bot 傀儡程式活動則下跌了 67%。一般來說，對抗網路罪犯所採取的執法活動成功率，以及提高網路安全意識，都是 Bot 傀儡程式沒落的重要因素。

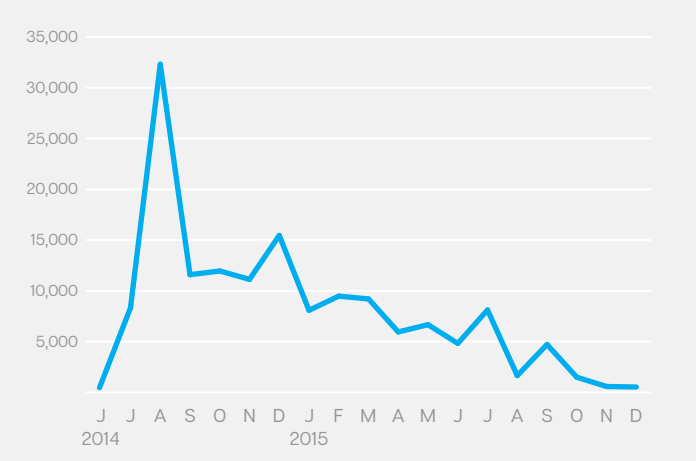
	2015 年國家/地區	2015 年全球 Bot 傀儡程式百分比	各個國家/地區 Bot 傀儡程式百分比的變化	2014 年國家/地區	2014 年全球 Bot 傀儡程式百分比
1	中國	46.1%	+84.0%	中國	16.5%
2	美國	8.0%	-67.4%	美國	16.1%
3	台灣	5.8%	-54.8%	台灣	8.5%
4	土耳其	4.5%	+29.2%	義大利	5.5%
5	義大利	2.4%	-71.2%	匈牙利	4.9%
6	匈牙利	2.2%	-69.7%	巴西	4.3%
7	德國	2.0%	-58.0%	日本	3.4%
8	巴西	2.0%	-70.1%	德國	3.1%
9	法國	1.7%	-57.9%	加拿大	3.0%
10	西班牙	1.7%	-44.5%	波蘭	2.8%

Dyre 後果與執法機關

就在警方於 2014 年關閉數個主要金融傀儡網路後，Dyre 進而取代了金融傀儡網路的位置。Dyre 不僅入侵一般 Web 瀏覽器並攔截 Internet 銀行交易階段作業來竊取資訊，更在受害者電腦上額外下載惡意程式，將電腦連結至犯罪者傀儡網路電腦的網路中。

與時俱進的 Dyre 偵測

▶ 本圖表顯示在 2015 年傀儡網路中斷前 Dyre 惡意程式活動的衰退情形。這也許暗示著經營模式已有漏洞。



Dyre 最初興起於一次最危險的金融詐騙行動，詐騙的客戶遍及全球 1,000 多家銀行和其他公司。

然而，這個操控 Dyre 金融詐騙木馬程式的網路犯罪集團，卻在 11 月一次俄羅斯執法行動下遭受重大打擊。如安全機制應變中心部落格中所述，賽門鐵克遙測資訊已確認該集團的活動確實中斷。Dyre (賽門鐵克偵測到的是 Infostealer.Dyre) 透過電子郵件活動四處散播，但自 2015 年 11 月 18 日起便再也觀察不到任何與 Dyre 有關的電子郵件活動。不久之後，Dyre 木馬程式及相關惡意程式的偵測數量便急速下降。先前在 2015 年年初，每個月感染數量估計超過 9,000 筆。11 月時下降到每個月不到 600 筆。

執法機關在捕捉這類網路罪犯方面的效率越來越高，而遏止這些行為的重大成功彰顯出國際之間協調合作所產生的效益。攻擊組織很少侷限在一個國家，而面對橫跨多個司法管轄區的重大組織，與執法機關跨國合作可說是確保這些成功作為足以繼續打擊網路罪犯的一項重要因素。我們期待明年將有更多成功對抗網路罪犯的執法行動。

當網路罪犯的風險提高，潛在的獎賞就會減少，進而增加想要成為網路罪犯的阻礙。2015 年其他顯著的成功案例包括：

- **Dridex 停擺。**Dridex 傀儡網路專門竊取銀行憑證。10 月時，一項國際執法行動努力過濾數千部遭入侵的電腦、切斷傀儡網路對這些電腦的控制，最後控告一名人士。然而這只能算是成功了一部分，因為 Dridex 仍繼續散播，表示這項操作仍有許多關鍵要素正在運作。因此，我們可以預見該組織將在 2016 年繼續構成重大威脅。
- **Simda 停擺。**執法機關在 4 月時捕獲到 Simda 傀儡網路控制者所擁用的基礎架構，包括眾多指令與控制伺服器。根據國際刑警組織表示，「網路罪犯運用 Simda 取得電腦的遠端存取權，藉此竊取銀行密碼等個人詳細資料，並安裝和散播其他惡意程式。」
- **扣押 Ramnit。**2 月時在一場由歐洲刑警組織主導、賽門鐵克和 Microsoft 等提供協助的執法行動中，扣押了由隱匿在 Ramnit 傀儡網路背後的網路犯罪組織所擁有的伺服器和其他基礎架構。
- **跨國銀行與金融服務詐騙相關起訴書。**聯邦當局至少起訴了 4 名與入侵事件有關的人員，這些入侵事件共竊取了 1 億筆以上的客戶記錄。這些人被控入侵多家金融機構，並涉嫌哄抬股價。2014 年發生的一起攻擊事件網羅了 8 千多萬筆客戶記錄，美國司法部將這起漏洞稱為「美國金融機構史上最大的客戶資料竊盜案」。

網路犯罪和避免受害的方法

企業和個人都必須瞭解到，即便認為自己不會成為網路罪犯的明顯目標，但並不表示不會成為受害者。

關鍵在於保持警覺，就個人而言：

- 不要開啟不明寄件者寄送的電子郵件。
- 在任何需要輸入機密資料的網站上尋找鎖頭圖示，並確認 SSL 憑證。
- 避免透過不安全的網路存取機密資料。

就企業方面而言，保持警覺的作法包括：

- 部署入侵防護與偵測軟體。
- 瞭解持有的寶貴資料，並應用防止資料外洩技術。
- 監控資料位置以及存取資料的人員。
- 確保在偵測到攻擊時，擁有完善的資安事端應變計畫。如果發生攻擊，不是該採取什麼樣的行動，而是何時該採取行動。

雲端與基礎架構

電腦、雲端運算及 IT 基礎架構

IT 系統持續受到快速演化的惡意程式攻擊。沒有一種作業系統能夠自動免疫，而針對 Linux 和 Mac OS X 的惡意程式威脅也不斷增加。甚至雲端代管與虛擬化系統同樣容易遭受攻擊。惡意程式能夠尋找虛擬化環境並加以感染。

保護系統

只要不使用 Windows 作業系統就能避免攻擊的日子對我們來說還很遙遠。針對 Mac OS X 和 Linux 的攻擊在 2015 年大幅增加，因此若要避免承受攻擊的後果，不只 Windows，對於所有作業系統而言網路安全都不可或缺。

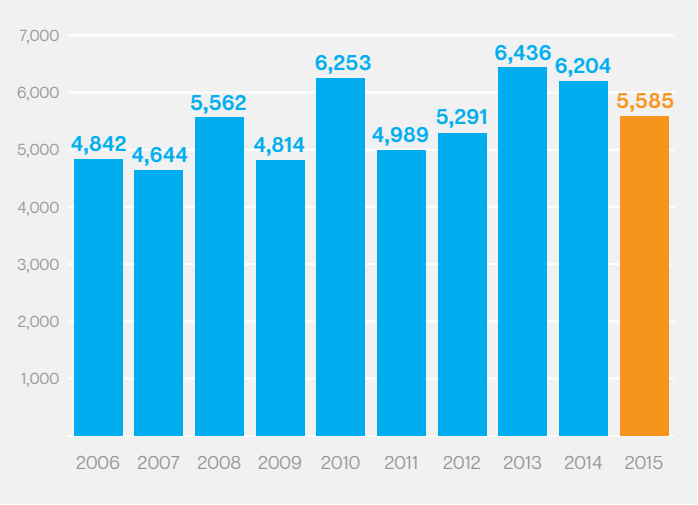
網路安全影響著我們每個人。企業需要保護電腦和 IT 基礎架構，才能阻止資料遭竊、詐騙及惡意程式攻擊。同樣地，企業和消費者都應該留意挾持資料的勒索軟體、身分竊取以及使用電腦作為跳板攻擊他人的攻擊者。

就基礎面來說，網路安全是保護 IT 各個層面的重要結構，包括電腦、伺服器及網路。但問題是惡意程式無所不在。我們在 2015 年觀察到越來越多的系統受到攻擊，包括 Linux、Mac、虛擬化電腦及雲端系統。每年雲端需處理許多我們的資料，無論是客戶關係管理、開立發票服務、社交網路、行動電子郵件以及各式各樣的其他應用程式等。

攻擊的其中一個途徑就是刺探利用漏洞，而大部分的系統都有漏洞。這些漏洞存在於使用的作業系統和應用程式中，也是網路安全的一個重要環節。如果漏洞未加以修正，就會讓準攻擊者有機可趁，供其刺探利用並使用這些漏洞執行惡意企圖。研究人員每年都會發現全新漏洞，其中最炙手可熱的便是零時差，這是目前為止尚無修補程式的一項特殊漏洞。

漏洞總數量

▶ 本表顯示，自 2013 年起感染情況有下降的趨勢，但 2015 年時明顯加劇。



有潔癖的人或許不喜歡，但細菌和病毒無所不在。它們存活在我們的皮膚或空氣中，趕也趕不走。同樣地，漏洞也是運算環境的一部分。它們不可能消失，而無論因為粗心、設定錯誤或人為錯誤，這些拙劣的修正方式才是惡意程式感染的主因。管理完備且妥善修正的系統不太容易受到感染。

沒有任何東西會自動免疫

去年賽門鐵克觀察到幾乎各種電腦、作業系統及其他基礎 IT 服務都會受到威脅，

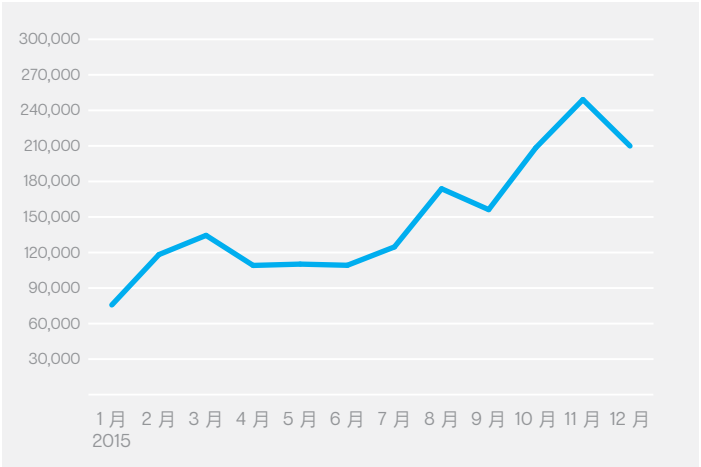
- **Mac OS X** 也不例外。除了在 2015 年發現更多漏洞，還搜尋到概念證明勒索軟體和多種木馬程式的適用手段，針對受影響的電腦進行未經授權存取。
- **MySQL**。賽門鐵克研究人員搜尋到攻擊熱門資料庫系統 MySQL 的惡意程式，而攻擊者會用來在其他系統上發動阻絕服務攻擊。
- **Linux**。Linux 惡意程式在 2015 年成長迅速，包括可供駭客感染未修正之 Linux Web 伺服器的攻擊套件。
- **虛擬化系統**。即便是虛擬化系統也無法免疫。有 16% 的惡意程式能夠常態地辨識並刺探利用虛擬機器環境，而 VENOM 等漏洞可讓攻擊者避開受感染的虛擬機器，並攻擊同一系統內的其他虛擬機器，甚至攻擊主機虛擬機器管理員軟體 (Hypervisor)。

Mac OS X

2015 年有大量攻擊鎖定 Apple 的 Mac OS X 作業系統，包括稱為 Mabouia (以 OSX.Ransomcrypt 的名稱被偵測到) 的概念證明勒索軟體威脅，也是第一個對 OS X 產生效用的檔案式勒索軟體威脅。以往也發現過針對 Macs 的瀏覽器式威脅，包括透過惡意網站鎖定 Safari 的勒索軟體。

再者，自 2015 年以來，OS X 惡意程式的數量已增加了兩倍 (成長率 100%)。第 1 季時，賽門鐵克每天大約阻擋了 3,650 個攻擊，到了第 4 季季末則提升至 7,255 個。

Mac OS X 惡意程式數量



OS X 端點中遭攔截的前 10 大 Mac OS X 惡意程式

▶ 使用未建立特定定義的一般偵測方式可額外阻擋許多 OS X 惡意程式變種。一般偵測可防範許多共用相似特徵的木馬程式。

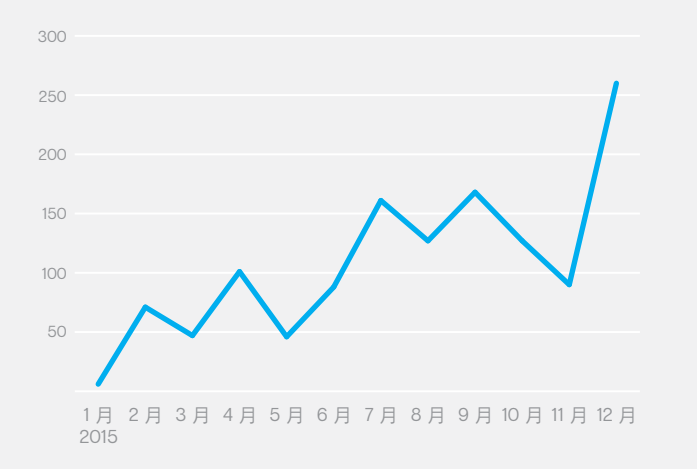
排行	惡意程式名稱	2015 年 Mac 威脅百分比	惡意程式名稱	2014 年 Mac 威脅百分比
1	OSX.Sudoprint	42.0%	OSX.RSPlug.A	21.2%
2	OSX.RSPlug.A	16.8%	OSX.Okaz	12.1%
3	OSX.Klog.A	6.6%	OSX.Flashback.K	8.6%
4	OSX.Keylogger	5.6%	OSX.Keylogger	7.7%
5	OSX.Wirelurker	5.0%	OSX.Stealbit.B	6.0%
6	OSX.Luaddit	3.2%	OSX.Klog.A	4.4%
7	OSX.Flashback.K	3.1%	OSX.Crisis	4.3%
8	OSX.Crisis	2.1%	OSX.Sabpab	3.2%
9	OSX.Okaz	1.7%	OSX.Netweird	3.1%
10	OSX.Stealbit.B	1.6%	OSX.Flashback	3.0%

火線上的 Linux

相較之下儘管整體數量減少，但是自該年度開始，攻擊 Linux 的惡意程式數量幾乎成長了四倍 (增加 286%)。第 1 季時，賽門鐵克每天大約阻擋了 1.3 個攻擊，到了第 4 季季末則提升至 5.2 個。

Linux 惡意程式數量

▶ 2015 年賽門鐵克觀察到針對 Linux 的惡意程式有激增的趨勢；在其他基礎網路服務中，Linux 是網站伺服器裡最常見的作業系統。



Linux 端點中遭攔截的前 10 大 Linux 惡意程式

▶ 2015 年有 55% 的 Linux 惡意程式與 Linux.Xorddos 變種有關；這類木馬程式可在受影響電腦上開啟後門，並且包含能夠隱藏網路流量和其他檔案的 Rootkit 裝置。此木馬程式也可下載其他潛在的惡意檔案。

排行	惡意程式名稱	2015 年 Linux 威脅百分比
1	Linux.Xorddos	54.9%
2	Linux.Dofloo	13.9%
3	Linux.Wifatch	12.7%
4	Linux.Shelock	4.2%
5	Linux.Spalooki	3.9%
6	Linux.Kaiten.B	3.8%
7	Linux.Mumblehard	2.4%
8	Linux.Moose	1.6%
9	Linux.Raubdo	1.0%
10	Linux.Xnote	0.5%

Linux 相當普及，只要一部伺服器便可容納任一代管供應商資料中心裡的數千個網站。Linux 已成為吸引駭客的目標，因為攻擊者只要存取一部伺服器，便可潛在感染該伺服器代管的所有網站，以及所有訪客和客戶。

攻擊者經常會使用連結至入侵工具組的程式碼感染受影響的 Web 伺服器，或是傳送垃圾電子郵件並竊取使用者名稱和密碼。此外，受影響的 Web 伺服器通常會成為攻擊者執行其他更廣泛攻擊的跳板，包括十分強大的 DDoS 攻擊，其中代管供應商的頻寬通常會比使用寬頻連線的家庭使用者大上許多。

專用的自動化攻擊工具組越來越多，網路罪犯可輕易針對 Linux 系統進行攻擊。這些工具組可協助攻擊者找出潛在易受攻擊的伺服器、掃描不安全的內容管理系統和其他外洩的網頁應用程式。

2015 年時也發現了針對 Linux 的勒索軟體，如果特定檔案的附檔名與網頁應用程式有關，便成了鎖定目標。此程式也會加密含有「backup」(備份) 字眼的封存檔和目錄，在沒有執行離站備份的情況下，任何人幾乎都束手無策。

雲端和虛擬化系統

「雲端運算」一詞涵蓋各式各樣的技術解決方案和環境，包括軟體即服務 (SaaS)、平台即服務 (PaaS) 或是基礎架構即服務 (IaaS) 模式。IaaS 在各企業之間日益普及，而隨著越來越多的資料和服務移往雲端，也引起安全研究人員和網路罪犯的注意。和各種系統一樣，每次服務堆疊引入新的層級，攻擊層面就會增加。當雲端環境受到 SQL 插入漏洞的危害時，也可能受到其他問題影響。舉例來說，賽門鐵克在 2015 年發現設定錯誤和管理不善 (使用者所造成，而非雲端服務提供者) 讓雲端代管系統暴露在未經授權存取的風險之中。此外，也發掘到 11,000 個可公開存取的檔案，有些還包含敏感性個人資訊。遭竊的雲端式系統憑證會定期在黑市交易，金額通常不到 10 美元。

雲端漏洞

雲端系統在本質上不一定比傳統 IT 服務還要不安全。不過管理員需要確保使用的雲端服務設定妥善，並妥善保護所有資料。管理員應審慎控管雲端系統的存取權，最好能採用雙重驗證。

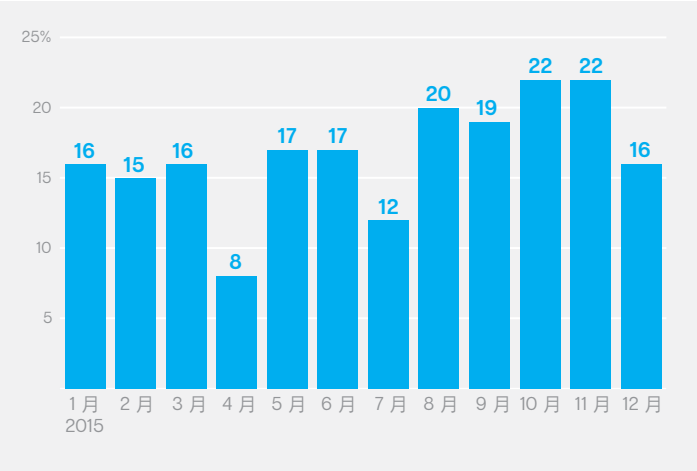
VENOM 等漏洞可讓攻擊者避開訪客虛擬機器 (VM)，並存取原生主機作業系統以及在同一平台上執行的其他 VM。刺探利用 VENOM 錯誤的攻擊者可能竊取受影響系統中任何虛擬機器的敏感性資料，並取得主機區域網路及其系統的較高存取權。VENOM 錯誤 (CVE-2015-3456) 自 2004 年便已存在於開放原始碼的 Hypervisor QEMU 中，在預設情況下通常會安裝在使用 Xen、QEMU 及 KVM 的各種虛擬化基礎架構中。但是有一點必須注意，VENOM 不會影響 VMware、Microsoft Hyper-V 及 Bochs Hypervisor。

直至今日，VENOM 錯誤還沒有已知的實際刺探利用情形，而 QEMU 的開發人員和其他受影響的廠商也針對 VENOM 製作並發佈相關修補程式。

每 6 個惡意程式變種就有 1 個 (16%) 能夠偵測虛擬化環境的存在 (2014 年時每 5 個惡意程式變種就有 1 個 (20%))。此能力可協助惡意程式有效躲避偵測，尤其是使用虛擬化的安全沙箱系統。更令人在意的是，攻擊會偵測何時能夠刺探利用並感染同一系統中的其他虛擬機器。

虛擬機器感知的惡意程式樣本比例

▶ 約有 16% 的惡意程式能夠常態地偵測並辨識虛擬機器環境的存在，第 4 季時達到顛峰 (約 22%)。



比起以往，現在擁有健全的虛擬系統安全設定檔顯得更加重要。維護虛擬機器和雲端服務安全的方式，和其他服務及裝置相同。政策應涵蓋虛擬和實體基礎架構，而針對整個平台採用整合式安全工具則有助於在日後減少這類問題發生。

保護 IT 基礎架構

在面對這些威脅以及其他類似情況時，以往的建議對於任何基礎架構服務依然有效，包括檔案伺服器、Web 伺服器以及其他連線至網路的裝置：

- 隨時掌握新興威脅相關資訊。
- 使用修補程式和更新將系統維持在最新狀態。
- 使用整合式安全軟體，包括防惡意程式技術。
- 使用僅允許已知流量的強大防火牆，並定期檢視存取記錄檔以偵測潛在的可疑活動。
- 採用多層式防護，萬一某層遭到入侵，還有其他層可以保護系統其他區域。
- 套用完善政策並妥善訓練人員。
- 以最低權限為基礎控制存取權。
- 部署網路入侵防禦和偵測措施，並監控在伺服器上執行的電子郵件服務。
- 隨時執行離線備份。

留意雲端系統。其他額外考量如下：

- 維護所有用來存取雲端式管理功能的憑證安全，並且務必以「有需要知道」為基礎控管存取權。
- 務必瞭解雲端資源設定，並據此進行設定。
- 啟用事件記錄，以追蹤存取雲端資料的對象。
- 閱讀雲端供應商的服務層級協議，瞭解維護雲端資料安全的方式。
- 將雲端 IP 位址納入漏洞管理程序，並針對透過雲端提供的任何服務進行稽核。

隨處保護資訊

當公司將 IT 系統移往虛擬和雲端代管環境時，均需面臨全新的安全挑戰。此外，如同以往一般，人性本身就是一種威脅，無法妥善管理安全性將導致影子 IT (Shadow IT) 系統。影子 IT (Shadow IT) 係指在組織未明確許可的情況下於組織內部使用的解決方案，以及在非 IT 部門使用的解決方案。對於部分員工來說，有時為了滿足立即需求而使用外部產品相當容易。IT 決策者應瞭解影響員工使用這些解決方案的原因，以及 IT 部門何時應介入協助擬定這些決定。

掌握組織動向以及某些團隊是否正在尋找未提供的服務或應用程式，然後決定如何解決其需求並以安全方式提供服務，這些對資訊長來說都至關重要。採用正確程序是保護資訊和資料的關鍵，即使這些資料不是在企業內部。

DDOS 攻擊和傀儡網路

分散式阻絕服務 (DDoS) 攻擊的數量及密度都有不斷攀升的趨勢，但大部分的攻擊時間都在 30 分鐘以內。租用型傀儡網路 (botnets-for-hire) 的供應進一步推動了這股攀升趨勢，我們可能會發現物聯網助長這些傀儡網路大軍的威勢。

氾濫的 DDoS

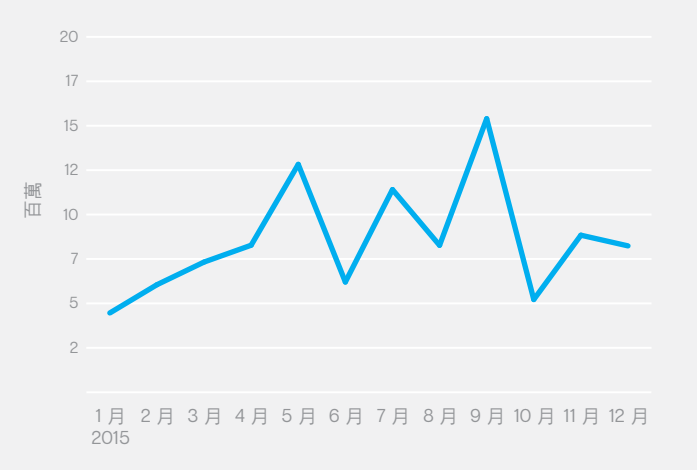
有些 DDoS 攻擊仍會透過中斷組織網站的方式進行敲詐和勒索，為罪犯提供許多獲得贖金的機會。追蹤資金流向使得這樣的方式變得不易執行，而 DDoS 防護技術則意謂攻擊者需要越來越大的頻寬才能造成影響。但是最近某些大型攻擊卻是駭客行動主義者組織和國家行為者 (state actor) 共同策劃而成。

最好的例子便是近期 BBC 遭到攻擊的事件，跨年夜時 BBC 的網站和 iPlayer 等 (BBC 在英國的網際網路隨選電視 (catch-up TV) 和電台服務) 相關服務停擺長達數個小時。根據宣稱發動此次攻擊的反 IS 國家組織新世界駭客 (New World Hacking) 表示，這是史上規模最大的 DDoS 攻擊事件。攻擊者宣稱 BBC 的規模正好可以測試他們的能力，而且攻擊流量高達 602 Gbps。

發動 DDoS 攻擊可以獲得獎勵，最明顯的方式就是勒索。攻擊者會威脅受害者支付贖金，否則將持續攻擊受害者網站。DDoS 在 2015 年也作為「干擾用」工具，並結合部分重大的目標式攻擊進行；攻擊者會大量湧入目標組織網站，讓 IT 團隊以為這是要求贖金的開端。實際上，隱匿攻擊正同時悄悄進行。

賽門鐵克全球智慧型網路發現的 DDoS 攻擊量

▶ 本圖表顯示每個月 DDoS 攻擊的數量，此數量於 2015 年下半年呈現增長趨勢，並在年底前逐漸減少。當攻擊時間縮短且變得隱蔽時，出現了幾個明顯的活動高峰。



賽門鐵克全球智慧型網路發現的前五大 DDoS 攻擊流量

▶ 大多數的 DDoS 攻擊都屬於 ICMP 流量攻擊，係指大量的 (通常是)「Ping」要求最後會使目標過載，直到目標再也無法處理合法流量為止。

	2015 年攻擊	2015 年攻擊率	2014 年攻擊	2014 年攻擊率
1	一般 ICMP 流量攻擊	85.7%	DNS 放大攻擊	29.4%
2	一般 TCP SYN 流量阻絕服務攻擊	6.4%	一般 ICMP 流量攻擊	17.2%
3	一般 Ping 廣播 (Smurf) 阻絕服務攻擊	2.1%	一般 Ping 廣播 (Smurf) 阻絕服務攻擊	16.8%
4	一般 Teardrop/Land 阻絕服務攻擊	2.0%	一般 Teardrop/Land 阻絕服務攻擊	7.2%
5	RFProwl 阻絕服務攻擊	0.6%	一般 ICMP 無法存取的阻絕服務攻擊	5.7%

不同的攻擊團體會有各自偏好的 DDoS 活動，而 ICMP 流量攻擊就是 Darkness/Optima 傀儡網路使用的主要方法之一。隨著時間過去，有些方法 (尤其是放大攻擊) 的效果已然退化。例如，當媒體廣泛涵蓋重大攻擊時，將有更多人會修正伺服器。此外，先前用來執行攻擊的傀儡網路可能已遭撤下，或已升級成能夠提供新功能的較新版本。

簡單有效

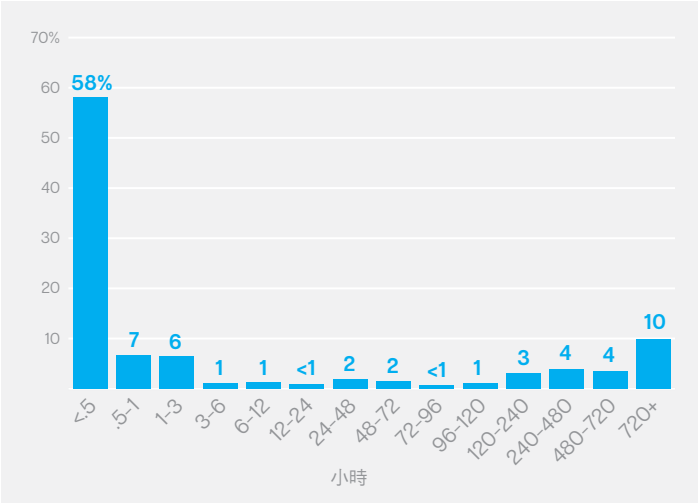
為何 DDoS 會如此熱門？這個答案和我們在 2002 年 12 月首次寫到 DDoS 時一樣：DDoS 容易設定、難以阻止，而且成效卓越。隨著租用型傀儡網路的興起，這點更無庸置疑。

根據賽門鐵克合作夥伴 Incapsula 指出，在 2015 年下半年所有 DDoS 網路層攻擊中約有 40% 都和租用型傀儡網路有關。當罪犯得努力感染多部易受攻擊的裝置並建立專屬傀儡網路才能執行 DDoS 攻擊，租用預製的傀儡網路反而更加輕鬆，也能節省更多時間。

2015 年黑市的價格仍相當穩定，DDoS 攻擊每天的訂購價從 10 美元至 1,000 美元不等。但企業得付出的代價顯然高出許多，甚至高達上千倍以上，需取決於業務性質和公司網站的重要性。2015 年 Incapsula 的報告指出，DDoS 攻擊讓組織每小時需付出高達 40,000 美元的代價。於是攻擊者以此方式成功挾持公司要求贖金所獲得的可能獎賞，將足以彌補他們訂購攻擊所支付的金額。舉例來說，一間澳洲電子郵件供應商遭受攻擊，攻擊者要求支付價值 6,600 美元的 20 枚比特幣。另一家公司支付要求的贖金後不久又遭到另一波攻擊。

依持續時間區分的網路層 DDoS 攻擊分佈圖 (第 3 季)

▶ 本圖表顯示截至 2015 年第 2 季結束，仍有比例相當高的 DDoS 攻擊持續數小時、數天、數週或甚至數個月。本圖表由 Incapsula 提供。

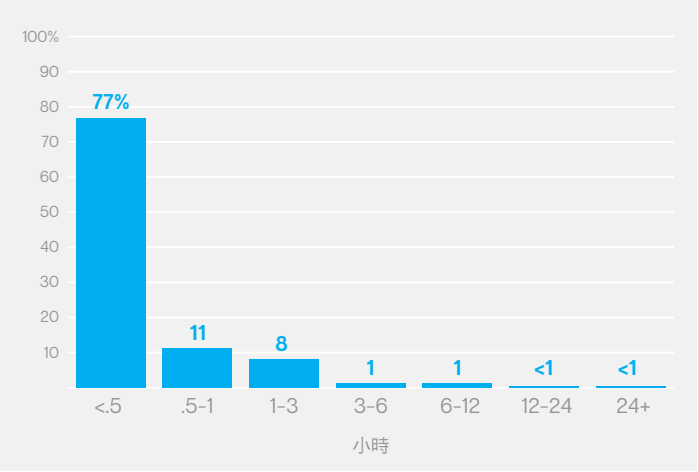


這些短暫的游擊式攻擊顯示出廣泛使用以服務方式提供 DDoS 攻擊的趨勢，而整體傀儡網路資源必須和其他訂購者共用，因此訂購者可運用的資源有限。不過要讓訂購者執行時間較短的中型攻擊，這樣的資源通常就已足夠。此方式也可協助攻擊者判斷目標基礎架構減緩這類攻擊的效率，以及是否需要提高攻擊量。Incapsula 的報告也指出，100 Gbps 以上的攻擊已相當普遍，而且隔天即可減緩這類攻擊。

相較於 2015 年第 2 季，「DDoS 即服務」普及率的提升正好可解釋第 3 季網路層攻擊持續時間大幅下降的原因。這些租用型 DDoS 服務當中，有一部分可視為「壓力程式」(stresser)，因為發動 DDoS 攻擊並不合法，會隱藏於幕後，因此推測可用來作為「壓力測試」伺服器應變能力。

依持續時間區分的網路層 DDoS 攻擊分佈圖 (第 2 季)

▶ 本圖表顯示第 3 季結束時，持續超過一天的 DDoS 攻擊數量幾乎已完全消失，佔所有 DDoS 攻擊的比例不到 0.5%。
本圖表由 Incapsula 提供。



傀儡網路的內容為何？

對於執行攻擊的罪犯而言，無論採取租用或建立方式，傀儡網路都是 DDoS 攻擊的關鍵。傀儡網路規模越大，可以傳送的同步要求就越多，攻擊的破壞力也越大。

但不只是受感染的電腦會成為罪犯利用的機器大軍。十月時我們發現惡意程式鎖定 MySQL 伺服器，比起傳統的消費性電腦，這類伺服器通常為攻擊提供了更大的頻寬。這並不是全新手法，但顯示出罪犯仍持續打造規模更大、效率更高的傀儡網路。

我們也發現 2015 年罪犯頻繁使用物聯網 (IoT) 提升傀儡網路等級。而 CCTV 監視器證實是最受歡迎的目標，可能原因是該監視器是最普及的一項 IoT 裝置，2014 年全球運作中的專業安裝視訊監控攝影機共有 2 億 4,500 萬部。

就長遠來看，很可能是罪犯將頻繁使用易受攻擊的 IoT 裝置來執行大規模 DDoS 攻擊。在採用各項解決方案減緩 DDoS 攻擊之際，企業也將面臨全新挑戰，針對非傳統裝置執行妥善的安全措施，確保這些裝置不會成為問題來源。也許更令人關注的是，在未設置適當安全性的情況下，將更難以掌握印表機、冰箱、恆溫器甚至烤麵包機何時會真正成為有害全域傀儡網路的一部分。■

結論

網路安全為何如此重要？

這是賽門鐵克網路安全威脅研究報告的第 21 版，自初版以來已有大幅度的改變。每年我們都會重新審視報告的架構和內容。除了著重威脅並報告研究中的發現，賽門鐵克也會追蹤產業趨勢，並在報告中試圖突顯重要發展並展望未來趨勢。我們不只是查看電腦系統、智慧型手機和其他產品，研究的範圍還擴及國家安全、經濟、資料防護及隱私等廣泛概念。

網路安全的重要

本報告深入檢視網路安全和網路威脅，並著重顯著的變化和發展。然而我們必須記住，網路犯罪一定有受害者。舉例來說，勒索軟體從電腦鎖定對象，以珍貴的家庭照片勒索贖金、綁架未完成的小說手稿，以及阻止存取退稅、銀行記錄和其他有價值文件。再者，誰也無法保證支付贖金後就能夠贖回這些資料。企業和家庭使用者都是受害者，儘管網路安全應該才是首要之務，但通常也會仰賴備份作為最後一道防線。

目標式攻擊會竊取企業寶貴的智慧財產，而資料外洩則會破壞企業的聲譽，甚至威脅到企業的存續。網路保險理賠的數量與金額也不斷增加，保險費甚至也越來越高。就廣泛意義而言，網路安全問題威脅著國家安全和經濟成長，最終則會影響到我們每一個人。

網頁安全和產業責任

定期推出抵禦這類漏洞的更新程式，包括 SSL/TLS 通訊協定程式庫 (例如 OpenSSL)，但是網站負則人仍必須自行安裝這些更新程式。從這次報告中可以發現，過去數年來推出更新程式的速度還不夠快。每年易受攻擊的網站數量依舊持續增加，鮮少有明顯改善。從 SHA-1 憑證轉向使用更強大之 SHA-2 憑證的趨勢逐漸明朗，企業必須妥善部署全新憑證才能讓這樣的改變有所成效。

2015 年罪犯持續在網站安全的底層基礎架構中尋找漏洞，並入侵底層加密系統的弱點，讓攻擊者能夠攔截並控制安全連線。對於安全性、隱私權以及強大加密能力的廣泛爭論，最終會影響到我們每一個人。

沒有任何東西會自動免疫

沒有任何系統會自動對網路威脅免疫，從本次報告中可以清楚看到因自滿、疏忽及無能而忽略風險的結果。在 2015 年，史無前例的漏洞數量被確定當成作為武器之用的零時差攻擊行為，而網路攻擊行為套件則不斷適應與演化，速度之快更勝以往。隨著連線的裝置增加，就有更多漏洞遭到刺探利用。若要確保工業控制系統 (ICS) 和社群醫療裝置安全無虞，維護網路連線裝置安全將變得至關重要。

隨著軟體漏洞的數量不斷增加，以及針對不同系統的攻擊行列，再加上 Windows 系統的威脅將延伸到其他作業系統、行動裝置以及其他 IoT 裝置，未來影響的範圍將更加廣泛。

數位衛生學和更乾淨的未來

對於網路安全，我們經常探討到感染和病毒。但是我們在今年觀察到無所不在的攻擊、大型資料外洩以及進階威脅等態勢，都顯示出威脅與醫學的類比。撇開感染不談，我們認為疾病分為慢性和急性、惡性以及良性。

我們排除未受感染和入侵等情況，而應轉向思考影響、穩定性、健康、感染漏洞以及復原能力等健康模式。身為 IT 安全專家，我們應著重在預防、偵測、移轉以及完整的解決方案。藉助流行病學的概念，資安事端應變規劃以及安全模擬等工具也變得越來越重要且實用。

對於個人和公司來說，網路安全將更傾向於「健康」和「衛生」，而非「醫療」，並且著重在日常預防工作，而不是尋求萬靈藥或治療方法。我們都需要維持數位層面的健康和清潔，而且需要一而再地重新學習安全習慣。

同樣地，IT 部門也需要主動降低持續入侵和惡意程式帶來的風險，並迅速找出漏洞。遺憾的是，迅速搜尋攻擊需要持續、主動地保持警覺。資訊安全無法等候支援票證開啟，或是使用偏好的安全工具就能確切地找出問題。您必須要能在不必應變漏洞時主動深入探索資料，才能維護安全。

身為企業的我們也需要開始調整心態，轉而執行更多調查和臨床研究，我們也會持續研究造成「數位疾病」的習慣或跡象。如同酒後駕車一般，置網路安全於不顧同樣不可取。

網路安全不光只是採用正確技術，員工也必須保持良好的數位衛生習慣，無論在家或辦公室都一樣。教育和深刻認識網路安全問題，都可協助每個人保持更良好的數位健康。只要留意可能面對的風險數量，就可以有效降低風險，同時學習如何辨識徵兆及診斷「數位疾病」，就能避免自己和客戶的資料暴露在風險之中。我們應該摒除再也沒有隱私權這樣的誤解。隱私權十分寶貴，而且應該受到妥善保護。■

如需最新的更新數據，請造訪：賽門鐵克每月威脅研究報告

企業適用的最佳實務準則指南

採用深度防禦策略

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。

監控網路入侵嘗試、漏洞及品牌濫用

接收廠商平台的全新漏洞和威脅相關警示，以利主動矯正。透過網域警示和虛構網站報告，追蹤品牌濫用情形。

光靠端點防毒是不夠的

在端點上安裝最新版防毒軟體十分重要。部署並使用具備額外防護層的全方位端點安全性產品，包括：

- 端點入侵防護，可防範未提供修補程式的漏洞遭到刺探利用、防範社交工程攻擊，以及阻止惡意程式侵入端點。
- 瀏覽器防護，避免隱晦不明的網頁式攻擊。
- 檔案和網頁式信譽解決方案，提供各種應用程式和網站的風險與信譽評等，防範變異迅速的變種惡意程式。
- 觀察應用程式行為並防範惡意程式的行為防範能力。
- 應用程式控制設定，可避免應用程式和瀏覽器外掛程式下載未經授權的惡意內容。
- 裝置控制設定，避免和限制使用各類 USB 裝置。

維護網站安全，避免遭受攻擊和惡意程式感染

定期評估網站是否有漏洞和惡意程式，避免破壞您與客戶之間的信任關係。另外也請考慮下列方式：

- 選用含延伸驗證的 SSL 憑證，為網站使用者顯示綠色的瀏覽器位址列。
- 在網站顯眼處顯示認可的信任標誌，向客戶展現您對安全性的承諾。

保護私密金鑰

取得數位憑證的來源必須是公認且值得信任的憑證授權中心，而且能夠展示卓越的安全性實務。根據賽門鐵克的建議，這些組織應：

- 使用獨立的測試簽章和版本簽章基礎架構。
- 在安全、防竄改及密碼編譯的硬體裝置上維護金鑰安全。
- 執行實體環境安全，防範資產遭竊。

使用加密和 DLP 保護敏感性資料

實施並強制執行安全政策，將任何敏感性資料加密。請務必連同客戶資料一起加密。這樣不僅可以避免資料外洩，也可以降低組織內部潛在資料外洩的傷害。

限制存取敏感性資訊。這應包括可協助預防資料外洩並將影響降到最低的資料遺失保護 (DLP) 解決方案。

- 執行可搜尋敏感性資料位置、監控資料用途以及防止資料遺失的 DLP 解決方案。
- 當資訊透過網路離開組織時監控其流向，並監控外部裝置或網站的流量。
- 應該將 DLP 設定為能夠辨識並阻擋可疑複製行為或下載敏感性資料。
- DLP 也可用來辨識網路檔案系統和電腦中的機密或敏感性資料資產。

企業適用的最佳實務準則指南

確保允許在公司網路中使用的所有裝置都具備妥善的安全性防護

如果實施自攜裝置 (BYOD) 政策，允許存取網路的任何裝置請務必至少建立安全性設定檔。

實施抽取式媒體政策

如果可行的話請限制未經授權的裝置，例如可攜式外部硬碟和其他抽取式媒體。無論是否有意，這類裝置都可能引入惡意程式並促使智慧財產外洩。如果允許使用外部媒體裝置，請在裝置連線到網路時自動掃描有無病毒，並使用 DLP 解決方案監控及限制將機密資料複製到未加密的外部儲存裝置。

積極更新和修正

更新、修正以及移轉過時且不安全的瀏覽器、應用程式及瀏覽器外掛程式。此方式也可應用在作業系統上，除了電腦外，行動裝置、ICS 及 IoT 裝置同樣適用。透過廠商發佈的自動更新，使用最新版本的病毒和入侵預防定義。

大部分的軟體廠商都會致力修正遭刺探利用的的軟體漏洞；然而這類修補程式必須確實採用才能發揮效果。盡可能將修補程式部署自動化，以持續防範整個組織的漏洞。

強制執行有效的密碼政策

確保密碼擁有足夠的強度。密碼長度至少 8 到 10 個字元，並混用字母和數字。鼓勵使用者避免在多個網站上重複使用相同密碼，也不得向他人透露密碼。應定期變更密碼，至少每 90 天變更一次。

務必定期備份

建立並維護重要系統和端點的定期備份。萬一發生安全性或資料緊急事件，應可使用備份輕鬆將服務停機時間和員工生產力的影響降到最低。

限制電子郵件附件

請將電子郵件伺服器設定為攔截或移除所有內含 .VBS、.BAT、.EXE、.PIF 及 .SCR 等副檔名之檔案附件的郵件，因為這些附件常用來散播病毒。企業應該調查允許附加成為電子郵件附件的 .PDF 相關政策。務必使用安全軟體妥善保護郵件伺服器，並完整掃描電子郵件。

務必妥善配置感染和資安事端應變程序

- 備妥安全廠商聯絡資訊，以備不時之需；瞭解您要致電的對象，以及如果有一或多個受感染的系統時要採取的步驟。
- 務必妥善配置備份及復原解決方案，萬一攻擊成功或發生災難性資料遺失時，便可還原遺失或受損的資料。
- 善用網路閘道提供的感染後偵測能力、端點安全解決方案及防火牆辨識受感染的系統。
- 隔離受感染的電腦，避免組織內部發生進一步感染的風險，並使用信任的備份媒體進行還原。
- 如果惡意程式碼或其他威脅入侵網路服務，在執行修補程式之前請先停用或攔截存取這些服務。

教育員工

今年和以往一樣，基本常識和良好的安全習慣可以長時間維護網站和伺服器的安全。

- 除非預期來自已知的信任來源，否則切勿開啟附加檔案；另外，如果不是來自信任來源，或者下載時已針對惡意程式進行掃描，否則也切勿執行自網路下載的軟體 (如果允許下載)。
- 即便電子郵件或社交媒體程式上的 URL 來自信任來源或友人，點選時仍務必留意。
- 部署 Web 瀏覽器 URL 信譽外掛程式解決方案，在搜尋時這類解決方案會顯示網站信譽。
- 盡可能限制使用企業認可的應用程式軟體，並避免下載檔案共用網站提供的軟體。請務必直接從信任廠商網站下載套件。

企業適用的最佳實務準則指南

- 教育使用者安全的社交媒體行為。乍看之下相當吸引人的產品以及熱門主題，通常都是詐騙的第一步。並非所有連結都會導向實際的登入頁面。
- 鼓勵使用者在任何網站或應用程式中採用雙步驟驗證 (如有提供)。
- 請務必在每個電子郵件帳戶、應用程式及登入中使用不同的密碼，特別是工作相關網站或服務。
- 提醒您請運用常識判斷。使用防毒和安全軟體不表示就可以恣意造訪惡意或有問題的網站。
- 鼓勵使用者發現任何可疑跡象時發出警訊。舉例來說，如果 Windows 使用者看到一則警告說明點選 URL 或使用搜尋引擎 (表示假冒的防毒感染) 後會受到「感染」，請教導使用者運用 Alt-F4、CTRL+W 或工作管理員關閉或結束瀏覽器，並通知服務台。

保護行動裝置

建議使用者和雇主將行動裝置視為功能強大的小型電腦，並根據下列方式加以保護：

- 存取控制，包括生物辨識 (如果可以)。
- 資料遺失防護，例如在裝置上加密。
- 自動裝置備份。
- 遠端尋找及清除。
- 定期更新。例如代碼為「Honeycomb」的最新版 Android，具備各式各樣專門杜絕攻擊者的功能。
- 常識。請勿破解裝置，並且務必使用信任的應用程式市集。
- 訓練，尤其著重在應用程式要求的權限。
- 安全性解決方案，例如 Symantec Mobility 或 Norton Mobile Security

我們觀察到過去三年來，每年的行動漏洞數量都在增加，儘管這可能是一項發展指標，而不是造成失望的原因。這表示安全研究人員、作業系統開發人員及應用程式撰寫人員實際上更加留意行動安全，而且找出更多問題並加以修正。

儘管我們預期明年行動裝置將遭受更多攻擊，但仍希望透過妥善的預防措施和持續投資安全性，讓使用者享有更高的攻擊防護層級。

打造裝置安全性

ICS 和 IoT 平台多元化的本質讓主機式入侵偵測系統 (IDS) 和入侵防禦系統 (IPS) 能夠搭配平台和應用程式專用的可自訂規則集和政策，成為適合的解決方案。

但是，ICS 和 IoT 裝置製造商必須全力確保裝置內建安全性後才可出貨。

針對在 ICS 和 IoT 裝置上執行的軟體和應用程式直接內建安全性，應可避免遭到許多打算閃避高層級防禦的攻擊。製造商應在軟體開發過程中採用及整合這類原則。

企業使用者和消費者必須確保供應商在購買的 IoT 裝置中內建基礎安全性，而不是將其視為固定的選擇項目。

團隊努力

消費者的信心是在無數不同組織擁有的各個網站之間進行多重互動所建立而成。但只要發生一次資料遭竊或偷渡式下載等不愉快的體驗，信譽便會受損，消費者心中也會留下負面印象。

如同報告一開始所述，明年確實有機會可以降低網路攻擊的成功數量，並限制網站可能對消費者構成的風險，但網站擁有人必須承諾並採取行動方能實現這個願景。

在 2016 年採用完整的網站安全性，同時和賽門鐵克攜手合作，讓這一年成為網路安全年，同時也是不利網路罪犯犯罪的一年。■

網站擁有者的最佳實務準則

為了達到有效的網站安全性，須小心謹慎建置，且須持續監控和維護。

雖然有工具可以協助您保持網站生態系統的安全，所有一切仍應以教育作為開端。您已瞭解風險，現在請找出可行的處理方式。

符合業界標準

- **建置隨時待命的 SSL。**在網站的每個網頁上建置 SSL/TLS，以使訪客與您網站的每次互動都受到加密。透過 OV 或 EV SSL/TLS 憑證切換至「HTTPS Everywhere」(別稱)，以證明您的可信度，也能改善您的搜尋排名並為升級至 HTTP/2 作準備，提供更好的效能。
- **移轉至 SHA-2。**如報告中所討論的，自 2016 年 1 月 1 日起，憑證授權中心應已停止發行 SHA-1 憑證。但您必須確保也已升級任何舊版憑證，而且也已升級目前可能無法辨識 SHA-2 的任何裝置和應用程式。
- **請考慮採用 ECC。**賽門鐵克也提供使用 ECC 加密演算法。所有主流瀏覽器，甚至行動瀏覽器，可在所有的最新平台支援 ECC 憑證，而與業界標準 2048 位元 RSA 金鑰相較之下，256 位元 ECC 金鑰的破解難度是它的 64,000 倍。

正確使用 SSL/TLS

SSL/TLS 是否良好視其建置和維護而定。因此，請務必：

- **通訊協定程式庫應保持為最新狀態。**SSL/TLS 導入是一種持續進行的任務，而且重要的是，若使用的軟體有任何修補程式或更新，須盡速導入。
- **請勿讓您的憑證過期。**持續追蹤您擁有那些憑證、由哪些憑證授權中心發行，以及憑證何時到期。賽門鐵克提供各種自動化工具以協助您達成此目標，讓您有更多時間執行主動安全任務。
- **顯示已辨識的信任標記。**在網站中相當明顯的位置顯示信任標記 (例如 Norton Secured Seal)，以向客戶展現您為其安全所付出的努力。

妥善管理 SSL/TLS 金鑰。限制存取金鑰的人數；讓個別的管理員各自管理保有金鑰之伺服器的密碼，及管理實際存放金鑰的系統；以及使用自動化憑證和金鑰管理系統以減少人力需求。

如有任何影響 SSL 金鑰的漏洞，您應迅速通知 CA，以撤銷對應之憑證。

採用全方位的網站安全

- **定期執行掃描。**密切注意您的 Web 伺服器，並當心漏洞或惡意程式。自動化工具會有所助益。
- **使用防毒軟體。**防毒軟體並不是只供電腦和智慧型手機使用。它也能供伺服器使用，而且有助於防止您的整個網站基礎架構受到嚴重惡意程式攻擊。
- **嚴格慎選外掛程式。**您用來管理網站的軟體也會含有漏洞。您使用的協力廠商軟體越多，您面臨的攻擊層面就越大；因此請僅部署絕對必要的軟體。
- **考慮整體生態系統。**您已部署 Web 應用程式防火牆以防禦插入攻擊嗎？您的 Web 應用程式程式碼簽章是否安全？您是否有自動化工具可偵測及防禦 DDoS 攻擊的日漸普遍問題？

賽門鐵克提供各種工具，讓維護完整網站安全變成一種直接且有效率的任務。

透過以下方法，避免影響您與客戶之間的信任關係：

- 定期評估網站是否有任何漏洞。
- 每天掃描網站是否含有惡意程式。
- 為所有的階段作業 Cookie 設定安全旗標。
- 保護您的網站安全以防範攔截式 (MITM) 攻擊和惡意程式感染。
- 選用含延伸驗證的 SSL 憑證，為網站使用者顯示綠色的瀏覽器位址列。
- 在網站顯眼處顯示認可的信任標誌，向客戶展現您對安全性的承諾。

團隊不分你我

消費者的信心是在無數不同企業擁有的各個網站之間進行多重互動所建立而成。只要有一次不佳的經驗，就足以傷害客戶心中每一次的信譽。

如報告中所述，在來年確實有機會可降低成功網路攻擊的數量，並限制您的網站可能會對消費者造成的風險，但這需要靠網站擁有者的承諾與行動才能將其落實。

在 2016 年，採用全方位網站安全，與賽門鐵克攜手打造網路安全的光明年和網路罪犯的黑暗年。

20 項重大安全管控

概述

網路安全 20 項重大安全管控的委員會，是一個依優先順序排定的清單，其設計理念在於為改善對抗實際威脅的風險狀況提供最大效益。20 個管控領域的清單是由一群美國和國際機構及專家之國際性組織所產生，分享實際的資安事端，並協助更新清單以對抗不斷演進的全球網路安全威脅。在網路安全中心 (CIS) 的領導下，CIS 重大安全管控 (簡稱「管控」) 已由個人和機構所組成的國際性社群發展成熟，並已在 2015 年更新至第 6 版。如需詳細資訊，請參閱 http://www.cisecurity.org/critical-controls 中找到的文件。

經由策略性地選擇安全管控架構，以作為啟動、建置及測量其安全態勢及管理風險的參考，許多企業面臨網路安全之挑戰和與日俱增的威脅。多年來，在提供已整合知識和已證實指引以保護重大資產、基礎架構及資訊的共同目標下，已發展出許多安全管控架構 (例如 NIST)。根據我們現今擁有關於攻擊和威脅的資訊，企業應立即採取哪些最重要的步驟來鞏固系統和資料之安全？

「重大安全管控」的設計理念在於，提供企業必要的資訊，以一致且持續的方式提高其安全態勢。「管控」 是一組相對較小的安全行動 (依優先順序排列、妥善檢查且受到支援)，企業可將其用來評估及改善其目前的安全狀態。

若要建置「管控」，您必須瞭解對企業、資料、系統、網路及基礎架構而言重要的是什麼，而且您必須考量攻擊者的行動，其可能會影響您在業務或操作中獲得成功的能力。

前 5 大優先順序

每個企業應著重採用前 5 項管控措施。這有助於建立安全基礎，並對於防止攻擊有最立即的影響。企業可以由此基礎運用其他符合企業之業務需求的管控措施。

以下頁面會以表格的形式呈現有關 ISTR 中已辨識之領域的概述，並將其與「重大安全管控」結合：

01

清查已授權和未授權裝置

主動管理 (清查、追蹤及修正) 網路上的所有硬體裝置，只讓已授權裝置獲得存取權限，並且尋找未授權和未管理裝置以及防止它們獲得存取權限。

02

清查已授權和未授權軟體

主動管理 (清查、追蹤及修正) 網路上的所有軟體，只允許已授權軟體進行安裝和執行，並且尋找未授權和未管理軟體以及防止它們安裝或執行。

03

行動裝置、筆記型電腦、工作站及伺服器的硬體和軟體安全設定

透過嚴密的設定管理來建立、執行及主動管理 (追蹤、報告、修正) 筆記型電腦、伺服器及工作站的安全設定，並且變更管控程序，以防止攻擊者利用容易遭受攻擊的服務和設定。

04

持續漏洞評估和矯正

持續獲得、評估及對新資訊採取相關行動以辨識漏洞，來矯正及將攻擊者的機會管道減至最少。

05

管控管理權限之使用

用來追蹤/管控/防止/修正電腦、網路及應用程式管理權限的使用、指派及設定的程序及工具。

重大控管

06

維護、監控及分析稽核日誌

收集、管理及分析可協助偵測攻擊、瞭解攻擊或從攻擊復原之事件的稽核日誌。

07

電子郵件和 Web 瀏覽器防護

將攻擊層面減至最少，並且將攻擊者透過其與 Web 瀏覽器和電子郵件系統的互動來將操縱人類行為的機會降至最低。

08

惡意程式防禦

使自動化的使用最佳化，以啟用防禦快速更新、資料收集及修正性動作，並同時在企業中的多個端點管控惡意程式碼的安裝、散播及執行。

09

限制和管控網路通訊埠、通訊協定及服務

管理 (追蹤/管控/修正) 網路裝置上持續進行之通訊埠、通訊協定及服務的操作使用，以將攻擊者可利用的漏洞管道減至最少。

10

資料復原能力

運用通過實證的方法，用來妥善備份重要資訊的程序和工具，以進行及時復原。

11

網路裝置的安全設定 (例如防火牆、路由器及交換器)

透過嚴密的設定管理來建立、執行及主動管理 (追蹤、報告、修正) 網路基礎架構裝置的安全設定，並且變更管控流程以防止攻擊者利用容易遭受攻擊的服務和設定。

12

邊界防禦

偵測/防止/修正不同信任等級之傳輸網路中的資訊流通，並將重點放在危害安全的資料。

13

資料防護

用來防止資料洩漏的程序和工具，降低已洩漏資料的影響，及確保敏感性資訊的隱私權和完整性。

14

根據瞭解的需求管控存取

用來追蹤/管控/防止/修正重大資產 (例如資訊、資源及系統) 之安全存取的程序和工具，這是根據已核准的類別依照哪些人員、電腦及應用程式有存取這些重要資產之需求和權限的正式判定。

15

無線存取管控

用來追蹤/管控/防止/修正無線區域網路 (LAN)、存取點及無線用戶端系統之安全使用的程序和工具。

16

帳戶監控和管控

防止攻擊者冒充 I 主動管理系統和應用程式帳戶的生命週期 (建立、使用、休眠及刪除)，以將攻擊者可利用它們的機會降至最低。

17

透過安全技巧評估和適當訓練彌補差距

對於企業中的所有功能角色 (排定任務的優先順序 – 對企業及其安全相當重要)，識別支援企業防護所需之特定知識、技巧及能力；透過政策、企業規劃、訓練及認知方案，發展及執行整合式方案以評估、辨識差距及矯正。

18

應用程式軟體安全

管理所有內部開發及收購之軟體的安全生命週期，以防止、偵測及修正安全弱點。

19

資安事端回應與管理

透過發展和建置資安事端回應基礎架構 (例如規劃、定義的角色、訓練、通訊、管理監督) 來保護企業資訊及其信譽，以迅速發現攻擊，且進而有效抑制損害、根除攻擊者的存在，及還原網路和系統的完整性。

20

滲透測試和紅軍演練

藉由模擬攻擊者的目標和行動，測試企業防禦的整體實力 (技術、程序及人員)。

重大管控防護優先順序

	強化防禦	加強偵測	降低影響
行動裝置	03 04 07 11 18	01 02 06 08 15	05 10 13 17
物聯網	03 04 11 14 18	01 02 06 08 15	05 09 12 17
網頁式威脅	03 04 07 18	01 02 06 08 16	05 09 10 12 17
社交媒體和電子郵件威脅	03 04 07	01 02 08 20	05 10 12 17
目標式攻擊和魚叉式網路釣魚	03 04 07 11 14 18	01 02 06 08 16 20	05 09 10 12 13 17 19
資料外洩	03 04 07 11 14 18	01 02 06 15 16 20	05 09 10 12 13 17 19
電子犯罪與惡意程式	03 04 07 11 14 18	01 02 06 08 16 20	05 09 10 12 13 17 19
雲端與基礎架構	03 04 11 14 18	01 02 06 08 15 16 20	05 09 10 12 13 17 19
Web 伺服器	03 04 11 14 18	01 02 06 08 16 20	05 09 10 12 13 17 19
DDOS 和傀儡網路	03 04 11 18	01 02 06 08 20	05 09 12 17 19

消費者的最佳實務準則

自我防護

使用包含以下功能的現代化網路安全解決方案，以達到抵禦惡意程式碼及其他威脅的最大防護效果。

- 防毒軟體 (檔案式和啟發式) 和行為惡意程式防護，可防止執行未知的惡意威脅。
- 雙向防火牆將會攔截惡意程式，以防它有可能利用在您電腦中執行之容易遭受攻擊的應用程式和服務。
- 瀏覽器防護將會防止隱晦不明的 網頁式攻擊。
- 使用信譽評等式工具，可在下載前先檢查檔案和網站的信譽和信任度，並可檢查 URL 信譽，並針對透過搜尋引擎找到的網站提供安全評比。
- 請考慮建置跨平台家長防護網，例如 Norton Online Family。

定期更新

將您的系統、程式及病毒定義檔保持為最新狀態；請一律接受廠商要求的更新。

執行已過期的版本會使您暴露在受到 網頁式攻擊利用的風險中。請僅直接從廠商網站下載更新。盡可能選取自動更新。

謹慎提防恐嚇軟體伎倆

號稱免費、破解版或盜版的軟體版本，會讓您暴露於惡意程式或社交工程攻擊之中，試圖以誘騙手法讓您認為電腦已受到感染，並要求您付款以將其移除。

使用有效密碼政策

請確定密碼混合了字母和數字，也請經常變更密碼。密碼不應含有字典中的字詞。請勿將同一個密碼用於多個應用程式和網站中。

使用複雜的密碼 (大寫/小寫和標點符號)。複雜密碼和密碼管理應用程式也會有所助益。

按下滑鼠前請三思

除非是您預期的電子郵件或信任的寄件者，否則切勿檢視、開啟或將電子郵件附件複製到您的桌面，或執行任何電子郵件附件。即使收到的電子郵件附件是來自於信任的使用者，也請保持存疑的態度。

- 即使是來自於信任的來源和朋友，在按下電子郵件中的 URL 或社交媒體通訊時，仍請格外留意。請勿在未使用預覽工具或外掛程式將網址展開前，盲目地按下短 URL，而。
- 造訪網站前，請使用 Web 瀏覽器外掛程式或 URL 信譽網站，顯示網站的信譽和安全評比。
- 對搜尋引擎結果請保持存疑的態度；執行搜尋時，請僅按下信任的來源，尤其是媒體中的熱門話題。
- 對要求您安裝媒體播放器、文件檢視器及安全更新的彈出式警告，請保持存疑的態度。請僅直接從廠商的網站下載軟體。
- 請注意您在公用網站上分享的可用檔案，包括遊戲、BitTorrent 及任何其他點對點 (P2P) 交換。請將 Dropbox、Evernote 及其他使用保持在只取得相關資訊的最小程度，並只在經過核准可用於企業時才進行使用。

保護您的個人資料

限制您在網路上公開可取得的個人資料量 (尤其是透過社交網路)。這包括個人和財務資料，例如銀行登入或生日。此外：

- 經常定期檢查您的銀行、信用卡及信用資訊，確認是否有不合法的活動。
- 避免從公用電腦 (例如圖書館、網路咖啡店及類似機構) 或未加密電腦，進行銀行交易或線上購物。

Wi-Fi 連線

使用公用無線熱點時，請將以下事項納入考量：

- 透過 Wi-Fi 網路連線至電子郵件、社交媒體及共用網站時，請使用 HTTPS。檢查您正在使用的應用程式和網站的設定和喜好設定。
- 當您造訪登入的網站或分享任何個人資訊時，請尋求綠色瀏覽器網址列、HTTPS 及可辨識的信任標記。
- 將您的家用 Wi-Fi 網路設定為增強式驗證，並且一律需要輸入唯一的密碼才能進行存取。
- 當您造訪登入的網站或分享任何個人資訊時，請尋求綠色瀏覽器網址列、HTTPS 及可辨識的信任標記。
- 將您的家用 Wi-Fi 網路設定為增強式驗證，並且一律需要輸入唯一的密碼才能進行存取。

參與人員

總編輯 Paul Wood
編輯主任 Ben Nahorney
資料分析員 Kavitha Chandrasekar
美術指導 Scott Wallace
技術顧問 Kevin Haley

執筆人

文字編輯 Marianne Davis
資訊圖表 Steven Rankin

支援人員

Axel Wirth
Bartlomiej Uscilowski
Brian Witten
Candid Wueest
Dermot Harnett
Dick O' Brien
Dipesh Shah
Dylan Morss
Efrain Ortiz
Gaurang Bhatt
Gavin O' Gorman
Himanshu Mehta
Kent McMullen
Laura O' Brien
Mario Ballano Barcena
Michael Klieman
Nicholas Johnston
Peter Coogan
Pierre-Antoine Vervier
Preeti Agarwal
Rauf Ridzuan
Roberto Sponchioni
Roger Park
Sara Groves
Satnam Narang
Shankar Somasundaram
Stephen Doherty
Vaughn Eisler
William Wright

特別感謝

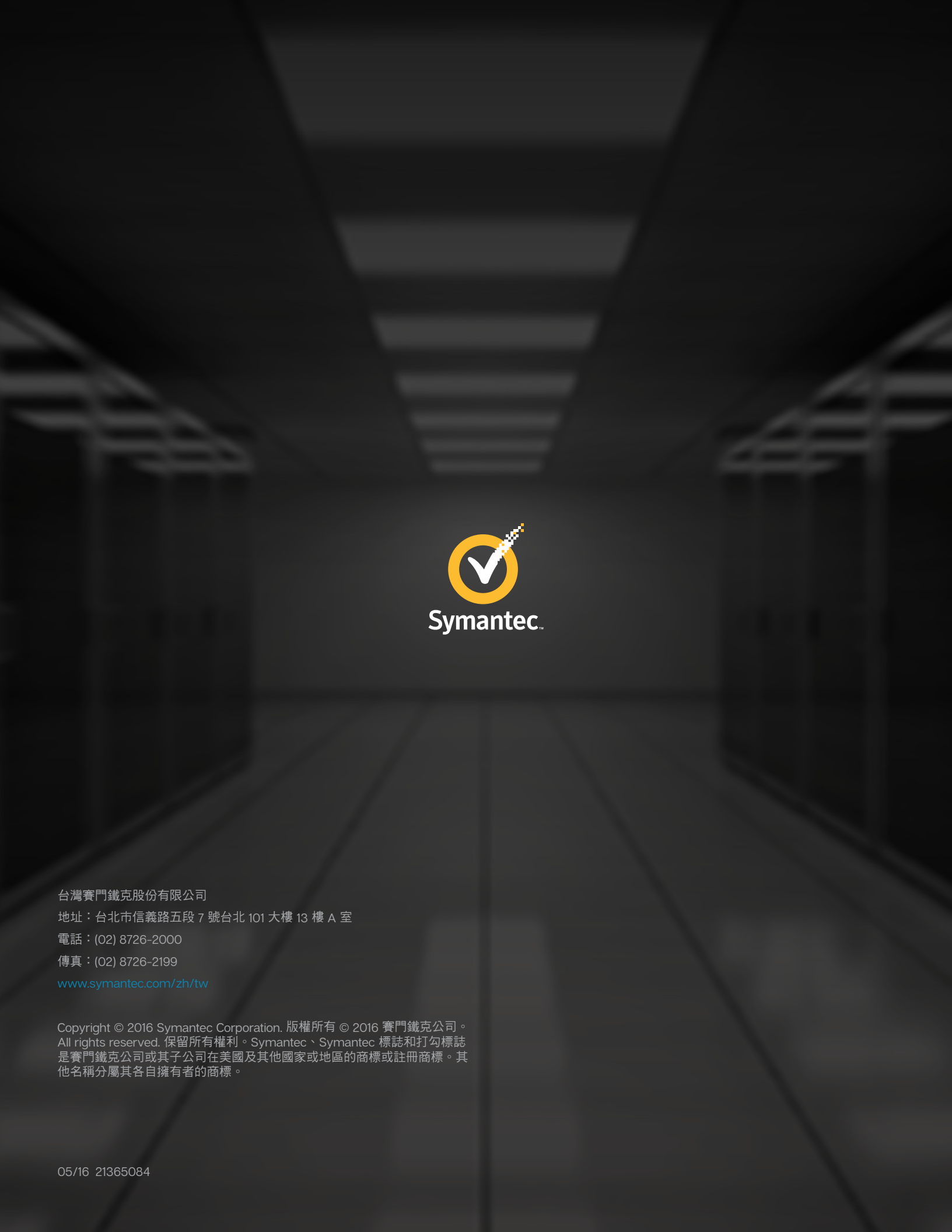
Alejandro Borgia
Anna Sampson
Cheryl Elliman
Jennifer Duffourg
Linda Smith Munyan
Mara Mort

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 是網路安全領域的全球領導廠商。我們運行全球規模最大的網路情報網之一，因而得以發現更多線上威脅，並保護更多客戶免於遭受新一代網路攻擊。無論最重要的資料存放於何處，我們都能協助公司、政府機構和個人妥善保存。

更多資訊

- Symantec APJ: http://www.symantec.com/en/aa
- ISTR 和賽門鐵克智慧型資源：http://symc.ly/APJ_2016ISTR_TW
- 賽門鐵克安全機制應變中心：http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/



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

www.symantec.com/zh/tw

05/16 21365084