資安攻防新層次

趨勢科技 2017 年資安預測

2017 年的資安情勢將給人一種既熟悉又陌生的感覺。儘管我們過去對 2016 年資安預測皆已一一實現，但那些威脅只不過是開啟了駭客探索更多未知攻擊領域的大門。回顧 2016 年，網路勒索異軍突起，智慧型裝置故障造成實質傷害，企業資料防護長 (DPO) 的編制更加迫切需要，因為企業資料外洩事件已成了家常便飯。

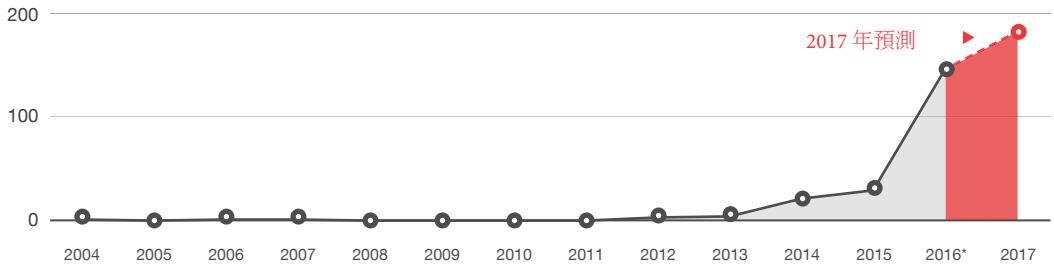
2017 年，新的挑戰將會出現，勒索病毒會開始朝不同方向發展：(1) 更多元 — 衍生出更多變種，(2) 更深化 — 成為縝密規劃的針對性攻擊工具，(3) 更廣泛 — 攻擊目標拓展至非桌上型電腦 (如行動裝置和智慧型裝置)。此外，簡單卻非常有效的變臉詐騙 (亦稱「商務電子郵件入侵」Business Email Compromise，簡稱 BEC) 將成為網路犯罪集團下一個新歡。同時，我們也將看到一些「商業流程入侵」(Business Process Compromise，簡稱 BPC) 攻擊帶來嚴重災情，例如：孟加拉銀行遭網路犯罪集團洗劫了 8,100 萬美元。未來，歹徒將發現更多 Adobe 和 Apple 的軟體漏洞並加以利用。就連原本看似不具威脅的智慧型裝置，也將成為歹徒發動大型分散式阻斷服務 (DDoS) 攻擊的工具。此外，工業物聯網 (Industrial Internet of Things，簡稱 IIoT) 裝置也將成為駭客的目標。隨著歐盟『通用資料保護法規』(General Data Protection Regulation，簡稱 GDPR) 即將上路，企業接下來勢必忙著修改內部流程以因應法規要求，連帶使得管理成本因而飆高。除此之外，企業更要對抗來自世界各個角落、動機複雜多樣、試圖入侵企業網路的網路駭客。這將是數位威脅的下一道防線，也將需要新的解決方案來因應。

趨勢科技在資安產業已累積二十五年以上的經驗，我們的威脅情勢即時監控網路和前瞻威脅研究團隊 (FTR) 讓我們隨時都能掌握威脅情勢的變化和風向，以下是我們對 2017 年及未來資安情勢的預測。

1

2017 年勒索病毒成長力道將開始平緩，但攻擊手法將朝多元化發展。

去年底，我們準確地預測到 2016 年將是「網路勒索之年」。勒索病毒的攻擊手法結合了多種不同的散布管道以及無法破解的資料加密，並且透過恐嚇伎倆來製造被害人心理壓力，使得這項昔日駭客最愛的工具成了今日網路犯罪集團的搖錢樹。此外，更發展出所謂的「勒索病毒服務」(Ransomware-as-a-Service，簡稱 RaaS)，這類由駭客經營的勒索病毒基礎架構，讓任何人都能踏入網路犯罪的領域，就算沒有技術背景也無妨。2016 年，某些勒索病毒的原始程式碼甚至在網路上流傳，駭客輕而易舉就能修改出屬於自己的變種。這也讓勒索病毒家族數量從 1 月至 9 月暴增了 400%。



* 資料日期截至 2016 年 9 月 30 日為止。

圖 1：勒索病毒家族逐年數量 (含 2017 年預測)。

2017 年，我們預測新的勒索病毒家族數量成長率將在 25% 左右，平均每個月約出現 15 個新的家族。由於勒索病毒的高峰期在 2016 年已過，因此在進入穩定期之後，歹徒將朝著多元化發展，讓病毒蔓延至更多潛在受害者、平台與更大的攻擊目標。

此外我們也預測，勒索病毒將成為資料外洩事件中的常客。網路犯罪集團會先竊取機密資料並拿到地下市集上兜售，然後再安裝勒索病毒來挾持資料勒索贖金，左右逢源賺取雙重利潤。

行動勒索病毒預料將追隨桌上型電腦勒索病毒的發展腳步，因為行動用戶這一塊目前仍是歹徒尚未完全開發的處女地。此外，非桌上型電腦終端機 (如 PoS 銷售櫃台系統和 ATM 提款機) 也同樣可能遭到勒索病毒攻擊。

目前，挾持智慧型裝置的價值對歹徒來說似乎還太小，因為其花費的精力遠超過獲利。比方說，假使智慧型燈泡遭駭，消費者直接換掉燈泡或許還比支付贖金來得便宜。不過，歹徒若能駭入車輛的電腦系統並要脅讓煞車失靈，也許可以撈到一筆贖金，但話說回來，開發這類攻擊所需的精力，或許會讓這類勒索手法顯得不太值得。

企業現在已明白，勒索病毒攻擊是件有可能發生且代價高昂的事。萬一工業環境感染勒索病毒，或者工業物聯網遭到攻擊，其損失可能更大。例如，歹徒若以生產線的運作或設備的溫度為要脅，便有機會勒索到大筆的金額。

儘管勒索病毒攻擊並無百分之百有效的預防措施，然而，最好的方法還是藉由網站與電子郵件閘道防護，從來源攔截這類威脅。此外，機器學習也是一項強化多層式防護不錯的技術，甚至能偵測出獨特、新出現的勒索病毒。

2

物聯網裝置將在分散式阻斷服務 (DDoS) 攻擊當中扮演更大的角色，而工業物聯網系統也將成為針對性攻擊的目標。

人們從未想過身邊成千上萬的網路攝影機也有安全疑慮，那些現已成了 Mirai DDoS 攻擊的大本營，該項攻擊行動已癱瘓了多家大型網站。許多連網的裝置就像蟄伏的間諜一樣，直到被網路犯罪集團觸發之前都不具威脅。根據我們預測，針對物聯網及相關基礎架構中的重要環節，2017 年將有更多的網路攻擊，不論駭客是利用開放的路由器進行大型 DDoS 攻擊，或是針對某台連網汽車進行單一針對性攻擊。

我們預測，網路犯罪集團將使用類似 Mirai 殭屍網路的惡意程式來發動 DDoS 攻擊。從 2017 年起，一些服務導向、新聞、企業和政治相關的網站，將遭到有系統的大規模 HTTP 流量攻擊，而歹徒攻擊的動機則包括金錢、洩憤，或其他特定要求。

不幸地，我們也預測廠商將無法及時阻止這類攻擊發生。沒錯，Mirai 攻擊事件的確導致網路攝影機廠商因而召回其產品，但這並未促使廠商針對一些尚未遭到攻擊、但同樣有危險性的產品進行程式碼重新檢測。因此，駭客永遠不缺可攻擊的漏洞。

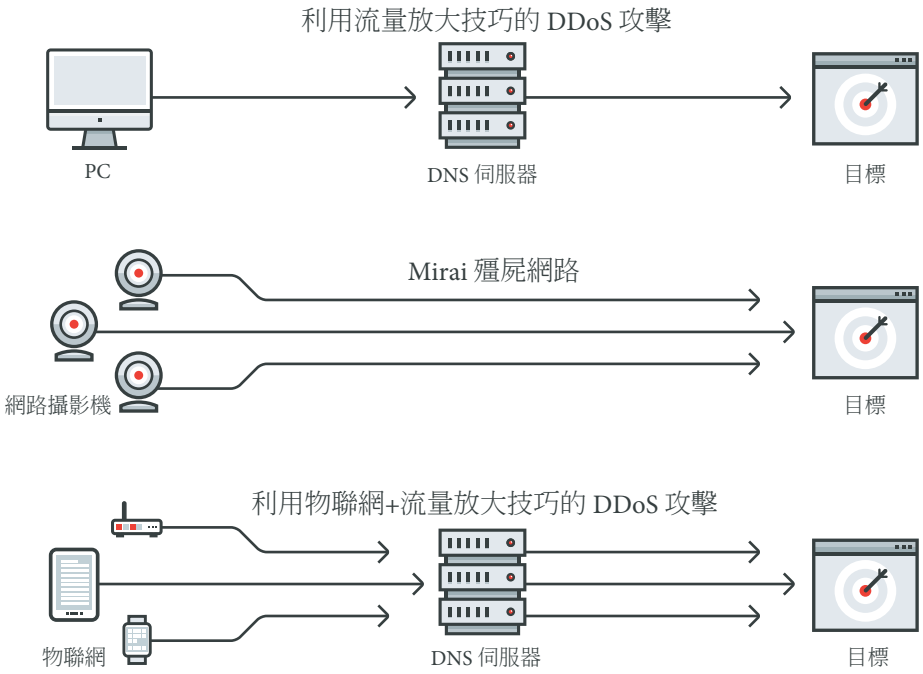


圖 2：Mirai 殭屍網路不需使用 DNS 伺服器來癱瘓目標，但仍足以讓許多使用者無法連上目標網站。理論上，物聯網殭屍網路也能發動流量放大技巧來發動 DDoS 攻擊，並且造成更大傷害。

雖然，物聯網能讓工業環境 (如製造和發電)更有效率，但駭客也將以 BlackEnergy 惡意程式為基礎，開發出更具威力的攻擊。再者，由於監控與資料擷取 (SCADA) 系統被發現的漏洞數量大幅增加 (在 2016 年當中有 30% 都是由 TippingPoint 所揭露)，因此 2017 年，工業物聯網的發展趨勢將為企業帶來前所未有的資安危機和風險，並且連帶影響消費者。

其實，製造這些智慧型裝置及設備的廠商，大可在產品開發過程當中將安全列為重點，來主動降低這類危險。除此之外，IoT 和 IIoT 的使用者也必須預先設想歹徒可能的攻擊情境，藉此找出並防範可能出問題的環節。例如，一家工廠必須在網路防禦當中設置網路入侵防護系統 (IPS) 來偵測並攔截惡意的網路封包。

3

變臉詐騙太容易得逞將使得 2017 年的針對性詐騙數量增加。

專門以全球企業財務部門為攻擊目標的「變臉詐騙」，其手法是先駭入某個電子郵件帳號，然後再透過該帳戶指使員工將一筆款項匯到歹徒的銀行帳戶。這類攻擊除了必須預先針對目標做足功課以了解如何撰寫一封具有說服力的電子郵件之外，其實並無特殊之處，但就連這項工作也只需要具備良好的網路搜尋技巧即可。

我們預料，由於變臉詐騙太過容易得逞，尤其是假冒執行長的詐騙，因此將成為網路犯罪集團最愛的詐騙手法之一。這類詐騙不僅容易得逞、經濟效益極高，而且不需太多基礎架構。平均每次變臉詐騙的 不法獲利高達 14 萬美元，幾乎可以買一間小坪數的房子。據估計，近兩年來變臉詐騙的不法獲利總金額高達 30 億美元。相較之下，勒索病毒攻擊的平均不法獲利僅有區區 722 美元 (約等於 1 比特幣)，但若目標對象是企業的話，金額倒是可以達到 3 萬美元左右。

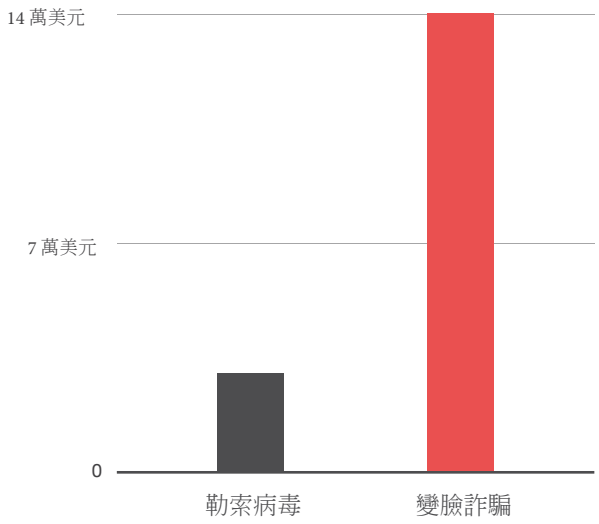


圖 3：勒索病毒攻擊與變臉詐騙企業平均損失金額比較。

不法獲利的速度也將推升我們所預測的成長趨勢。根據我們對 Predator Pain 變臉詐騙的案例研究，駭客在短短的六個月內就累積高達 7,500 萬美元的不法淨獲利。除此之外，司法機關偵辦跨境犯罪的牛步速度，也讓這項威脅更容易得逞。例如，警方花了兩年多的時間才將某位從 2014 年起即陸續詐騙多家企業的奈及利亞不法之徒逮捕歸案。

變臉詐騙郵件特別不容易偵測，因為這類郵件並未挾帶惡意程式或執行檔，不過企業仍可利用網站閘道或電子郵件閘道端的防護產品來攔截這類威脅。儘管這類資安技術可偵測異常的流量和惡意檔案的行為或元件，但若受害者依然毫無戒心，將錢乖乖送給歹徒，那麼要防範變臉詐騙就難上加難。企業必須實施更為嚴密的政策來控管正常和異常的交易，包括層層把關的驗證，此外，超過一定門檻的大筆交易需經過更多的驗證關卡才能執行。

4

商業流程入侵將逐漸獲得網路犯罪集團青睞，目標將鎖定財務相關部門。

孟加拉銀行 (Bangladesh Bank) 因為遭到網路搶劫而造成高達 8,100 萬美元的損失。有別於變臉詐騙利用的是人為疏失，網路搶劫則需要對大型機構處理金融交易的流程有更深入的認識。我們將這類攻擊稱為「商業流程入侵」(Business Process Compromise，簡稱 BPC)。

我們預料，儘管歹徒的最終目標仍是將資金匯出，但 BPC 的攻擊對象並不只侷限於財務部門。其可能的攻擊手法包括：駭入採購系統，進而暗中攔截原本應該匯給廠商的款項。此外，駭入付款流程系統也能收到類似效果。犯罪集團還有一種手法是駭入出貨中心的電腦系統，將高價值的商品轉寄至歹徒指定的地點。2013 年就曾出現過這樣的案例，比利時安特衛普港口 (Antwerp Seaport) 的貨櫃系統就曾遭駭客入侵以方便他們走私毒品。

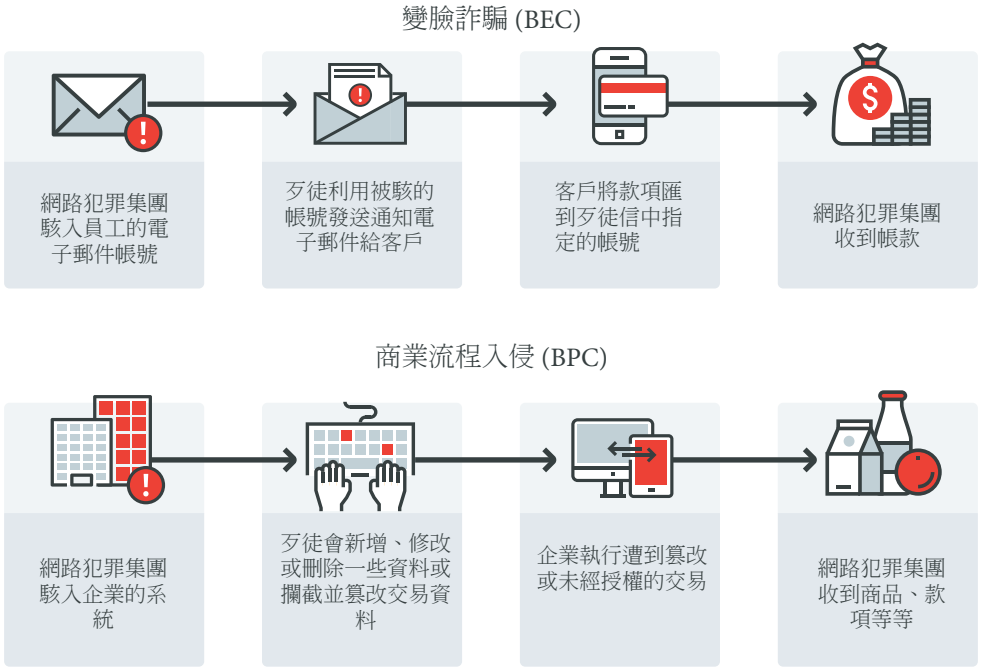


圖 4：BEC 和 BPC 攻擊過程比較。

目前，網路犯罪集團發動 BPC 攻擊的目標還是為了錢，而非為了政治動機或蒐集情報，然而這些攻擊和鎖定目標攻擊所採用的方法和策略非常類似。若我們比較企業網路遭到勒索病毒攻擊、BEC 和 BPC 攻擊的平均不法潛在獲利 (分別為 20 萬、14 萬及 8,100 萬美元)，就不難理解為何網路犯罪集團，甚至一些國庫短缺的不肖政府會更偏愛 BPC 這種攻擊方式。

當商業流程遭到攻擊時，企業並不容易掌握相關的風險，因為，一般的資安防護都將焦點擺在確保裝置不會遭駭客入侵。所以網路犯罪集團會利用這點資訊上的落差，然而企業可利用應用程式控管 (Application Control) 這類資安技術來防止歹徒進入營運關鍵系統的終端機，此外，端點防護機制也要能夠偵測歹徒在企業內的橫向移動。企業的文化必須養成嚴謹的政策執行和作業習慣，才能有效防範利用社交工程手法的攻擊。

5

Adobe 和 Apple 平台新發現的漏洞數量將超越 Microsoft。

2016 年，Adobe 新發現的漏洞數量首度超越 Microsoft。2016年截至目前為止，Zero-Day Initiative (ZDI) 漏洞懸賞計畫所發現的 Adobe 和 Microsoft 新漏洞數量分別為 135 個和 76 個。此外，2016 年也是 Apple® 新漏洞發現數量最多的一年，截至 11 月為止共有 50 個，較前一年的 25 個大幅成長。

我們預測，除了 Microsoft 之外，未來 Adobe 和 Apple 的產品也將發現更多的軟體漏洞。除了因為 Windows PC 出貨量近年來持續衰退之外，另一項因素是有越來越多使用者平常使用智慧型手機或商用平板而非一般電腦。除此之外，廠商針對安全性所做的改進，也讓駭客更難在其作業系統中找到新的漏洞。

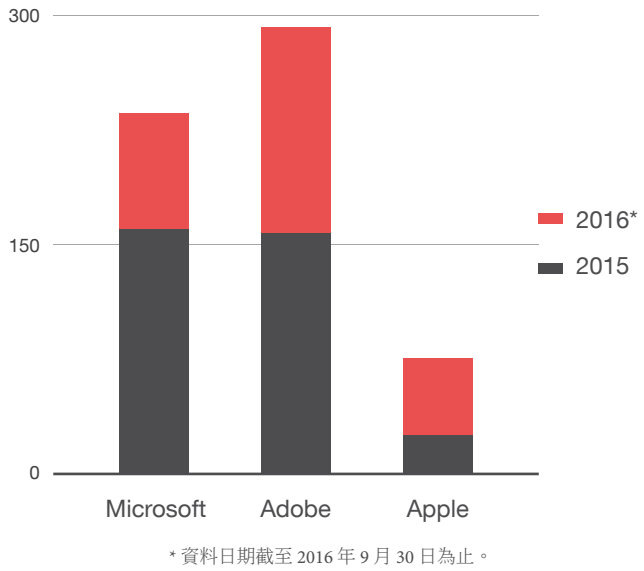


圖 5：ZDI 漏洞懸賞計畫所揭露的 Microsoft、Adobe 和 Apple 漏洞。

所有的 Adobe 漏洞最後都會被收錄到漏洞攻擊套件當中。未來，漏洞攻擊套件將是威脅情勢當中揮之不去的夢魘，網路犯罪集團除了用它來散布勒索病毒之外，或許還會發現其他全新的用途。在 Angler 漏洞攻擊套件的作者遭到逮捕之後，漏洞攻擊套件沉寂了一陣子。但如同當年 BlackHole 和 Nuclear 遭到破獲之後的情況一樣，馬上就會有新的漏洞攻擊套件取而代之。

當購買 Mac 電腦的消費者越來越多，歹徒的目光就會開始轉向 Apple 的軟體漏洞。今年，美國 Mac 出貨量成長，使得 Apple 的市占率更勝往年。再加上 Microsoft 在資安方面的改善，進一步讓網路犯罪集團的目光轉向非 Microsoft 系統。除此之外，由於 Apple 已宣布不再支援 iPhone® 4S，因此，一些在新版作業系統中已經修正的漏洞，在老舊的裝置上形同門戶洞開。

漏洞防堵技術是有效主動防範未修補漏洞和零時差漏洞的唯一方法。漏洞攻擊對許多企業來說都是無可逃避的現實，尤其是那些仍在使用老舊過時系統或軟體的企業。因此，漏洞防堵技術的角色尤其重要，特別是針對一些熱門常用軟體 (如 Apple 和 Adobe 軟體) 的漏洞。此外，Apple 和 Adobe 產品的使用者也應妥善保護自己的端點和行動裝置，以防範專門利用這類漏洞的惡意程式。

6

網路宣傳將成為一種常態。

2016 年，全球將近半數的人口 (46.1%) 都已能夠連上網際網路，不論是透過智慧型手機、傳統電腦或網際網路資訊站。這表示有越來越多人能夠輕易取得各種資訊，不論資訊的來源和可信度如何。

網際網路滲透率的提升，為有意透過網路這個免費工具來影響民意風向的人，開啟了全新的契機。最近世界各國的選舉結果，反映出社群媒體和各種網路消息來源對選民在政治判斷上的影響力。

前不久，我們才看到網路爆料平台 (如 維基解密WikiLeaks) 成了宣傳的工具。就在美國大選前一週，許多高度機密的文件在該網站上曝光。此外，我們也從網路犯罪地下市集的長期監控中發現一些初階駭客在網路上宣稱他們經由散布選舉相關的假新聞來賺錢。根據他們表示，只要將使用者導向一些抹黑候選人的新聞網站，每個月就能輕鬆賺到 20 美元。除此之外，還有一些專職的網路駭客團體受人資助在 Facebook 和 LinkedIn 這類社群媒體上張貼一些宣傳內容。他們甚至會利用這些平台的電子內容篩選機制來提高其曝光率。

由於網路資訊缺乏審查機制，因而難以辨別真偽，再加上一些想要操弄民意的有心人士或是單純只是支持特定候選人的用戶拼命轉貼的結果，經常導致這些不實內容和消息一夕爆紅。這對不熟悉網路生態的使用者來說，實在很難判斷資訊的真假。

雖然 Facebook 和 Google 會主動將不實的新聞廣告下架，而 Twitter 也增加靜音功能讓使用者過濾掉惱人的留言或對話，但就目前來看，還是無法發揮立竿見影的效果。

法國和德國即將到來的選舉，以及英國脫歐之後的後續發展，都將受到網路資訊和電子媒體的影響。我們將很可能看到更多經由 PawnStorm 之類的網路間諜行動所挖掘的機密資訊出現在網路宣傳當中。

任何人只要能夠策略性運用這類手法來左右大眾輿論，就可能創造出對自己有利的結果。2017 年，社群媒體的使用、濫用及誤用的情況勢必更加普遍。

7

「通用資料保護法規」的上路，將使得企業機構的管理成本增加。

歐盟即將上路的「通用資料保護法規」(GDPR)　不僅適用歐盟會員國，凡是需要蒐集、處理和儲存歐盟人民個人資料的全球企業機構都將適用。2018 年，當該法規正式上路時，違反的企業最高將可能受到該公司全球營收 4% 的罰鍰。

我們預料，GDPR 將掀起一波企業政策和流程的變革，並且大幅提高企業管理成本。根據 GDPR 的要求：

- 所有企業皆須設置一名資料防護長　(DPO)。我們曾經預測至　2016　年底，全球僅有半數的企業會有 DPO 的編制。這項預測正逐步實現，這也意味著，企業將花費一筆支出來雇用、訓練和維持這個新的高階經理人編制。
- 使用者必須被告知其被賦予的最新權益，企業也必須確保使用者能夠行使這些權益。隨著這項變革上路，歐盟人民現在將真正擁有自己的個人資料，提供給廠商的資料只是「暫借」性質，因此，企業的整個資料處理相關流程都將受到影響。
- 企業必須只蒐集絕對必要的資訊，並且改變現有的資料蒐集作法來配合法規。

這些改變將迫使企業徹頭徹尾重新檢討整個資料處理流程以確實符合規範，並且將歐盟規範下的資料和其他地區的資料分開。這對跨國企業來說特別艱難，因此，這些企業將必須考慮是否專門為歐盟規範下的資料建置另外一套儲存系統。此外，也必須仔細檢視其雲端儲存廠商的資料保護條款。企業必須投資一套完整的資料防護解決方案，再配合完整的員工訓練，以便能夠落實 GDPR。

8

歹徒將開發出能夠躲避今日偵測技術的最新針對性攻擊手法。

有關針對性攻擊的最早記錄大約是在十年之前，然而時至今日，歹徒的技術能力早已更加純熟，反觀我們的網路基礎架構卻沒有太大改變。根據我們的觀察，歹徒能夠適時調整其攻擊的工具、手法和程序來配合不同國情和不同企業目標，因此我們預料，未來的針對性攻擊勢必會出現一些意料之外的全新技巧。

這意味著，歹徒將採取更多能夠躲避現代化資安技術的方法。例如，過去駭客大多使用執行檔，後來改用文件檔案，而現在則是較常使用腳本和批次檔。他們將開始運用一些更複雜的沙盒偵測技巧，並且觀察目標網路是否會將未知檔案傳送至沙盒模擬環境當中分析，甚至會攻擊沙盒環境，讓沙盒模擬分析失去作用。此外我們也預料，虛擬機器規避 (VM Escape) 的技巧將成為進階漏洞攻擊程序當中備受重視的元素。虛擬機器跳脫技巧除了能夠躲避沙盒模擬分析之外，在雲端當中也有各種不同的攻擊應用。

諸如此類的駭客技術提升，將對 IT 和資安系統管理員造成更大的負擔。他們必須尋找能夠讓他們全面掌握整個網路與資料流向的資安技術，不僅要能偵測入侵跡象 (IoC)，而且要在一開始就能掌握一些攻擊跡象。

所謂的未知威脅，有可能是已知、既有威脅的全新變種，或者是從未發掘過的全新威脅。採用機器學習技術的資安解決方案可以有效防範前者，而沙盒模擬分析技術則可以掌握後者。有別於單一技術，那些經由不斷監控、回應攻擊並開發主動式防範方法而累積出來的跨世代多層式防禦技術，將是對抗針對性攻擊的關鍵。

我們如何正面迎戰駭客攻擊？

機器學習並非什麼新發明的資安技術，不過，卻是對抗已知及未知勒索病毒和漏洞攻擊套件等威脅的關鍵要素。機器學習須融入多層式防禦系統當中，先藉由手動或自動方式將資料輸入到數學演算法當中來加以訓練。接著，再將網路流量餵入這套模型當中，讓機器快速判斷網路內容 (檔案和行為) 是否為惡意。

此外，企業還必須採用通過考驗的防護來對抗駭客在 2017 年可能推出的偵測干擾技巧。面對這項挑戰，企業需要結合各種不同防護技術 (而非採用單一解決方案)，並且涵蓋整個網路，形成環環相扣的威脅防禦。例如下列技術：

- 進階的惡意程式防護 (不單只有黑名單)
- 在網站及郵件閘道上的垃圾郵件與網路釣魚防護
- 網站信譽評等
- 入侵偵測系統
- 應用程式控管 (白名單)
- 內容過濾
- 漏洞防堵
- 行動應用程式信譽評等
- 主機與網路入侵防護
- 主機防火牆防護

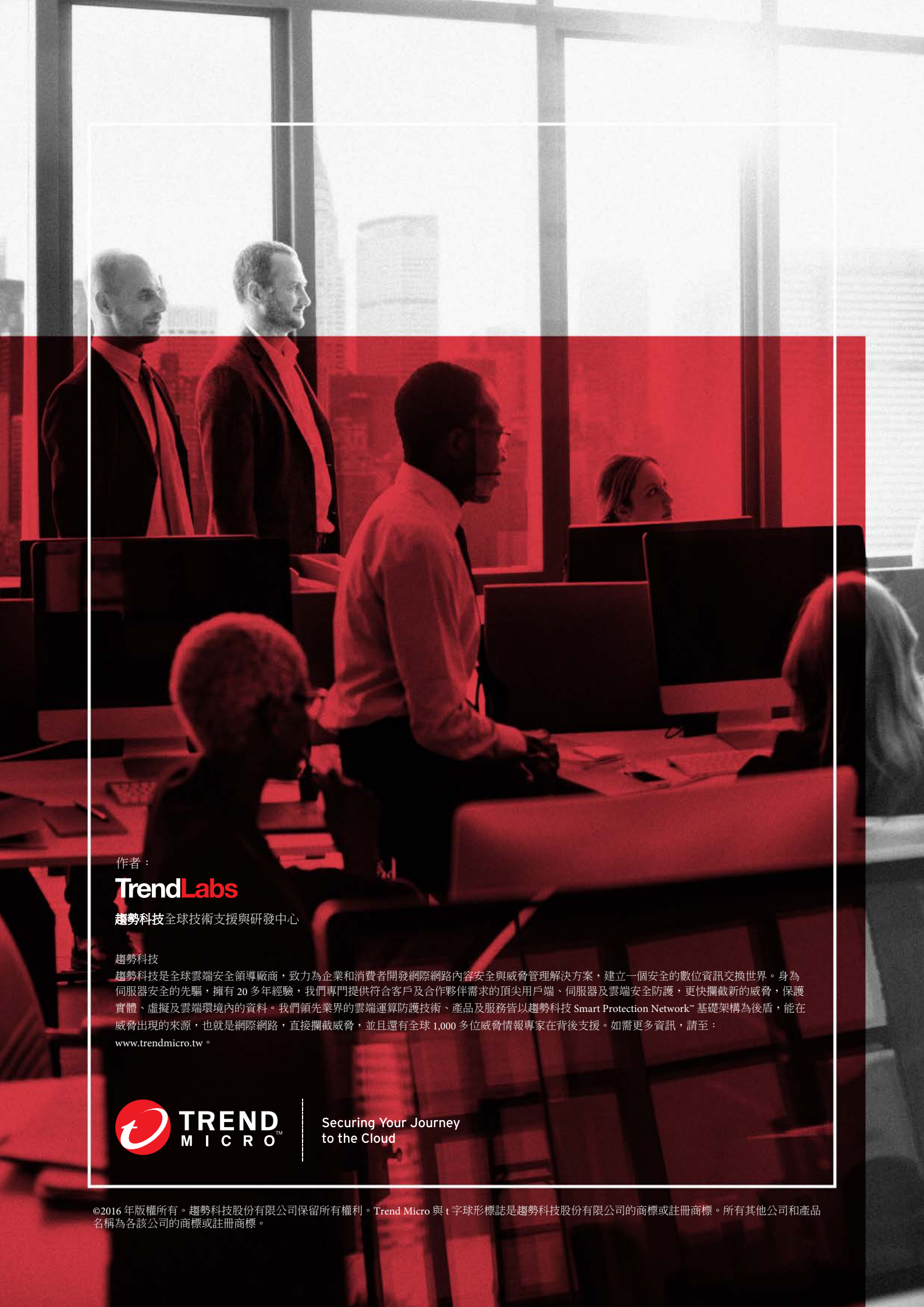
只要以上各項技術密切配合就能有效偵測今日絕大多數的威脅，但若要偵測「零時差」和「未知」威脅，企業就必須採用行為與異動監控，並且搭配沙盒模擬分析技術。

IoT 帶來了方便，也帶來了風險。智慧型裝置使用者必須先學會如何保護自己的路由器，然後才將智慧型裝置連上路由器以及網際網路。同時，在購買新的智慧型裝置之前，也應將安全納入考量：裝置是否具備安全驗證功能？是否可以變更密碼？是否可以更新？是否將網路通訊加密？是否有對外開放的連接埠？廠商是否提供韌體更新？

凡是需要蒐集歐盟人民個人資料的企業，未來管理成本都將大幅增加，因為企業必須大幅變更業務流程，並且聘用資料防護長以符合 GDPR 的要求。此外，徹底重新檢討公司的資料防護策略，也有助於通過這項稽核。

因應新的挑戰需要新的端點防護，例如通過市場考驗、可偵測已知及未知威脅的跨世代防護技術，再加上一些進階的防護技巧，如：應用程式控管、漏洞攻擊防範與行為分析、沙盒模擬分析偵測、高準度機器學習等等。

此外，教導員工如何防範社交工程攻擊，並且認識變臉詐騙等最新威脅，亦有助於培養良好的資安文化，強化企業的防禦以面對2017 年及未來的資安情勢。



作者：

TrendLabs

趨勢科技全球技術支援與研發中心

趨勢科技

趨勢科技是全球雲端安全領導廠商，致力為企業和消費者開發網際網路內容安全與威脅管理解決方案，建立一個安全的數位資訊交換世界。身為伺服器安全的先驅，擁有 20 多年經驗，我們專門提供符合客戶及合作夥伴需求的頂尖用戶端、伺服器及雲端安全防護，更快攔截新的威脅，保護實體、虛擬及雲端環境內的資料。我們領先業界的雲端運算防護技術、產品及服務皆以趨勢科技 Smart Protection Network™ 基礎架構為後盾，能在威脅出現的來源，也就是網際網路，直接攔截威脅，並且還有全球 1,000 多位威脅情報專家在背後支援。如需更多資訊，請至：www.trendmicro.tw。

TREND MICRO™

Securing Your Journey to the Cloud

©2016 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro 與 t 字球形標誌是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。