勒索病毒當道的時代

TrendLabs℠ 2016 上半年資訊安全總評

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

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

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

內容

4

勒索病毒稱霸威脅版圖

7

變臉詐騙蔓延全球

9

漏洞攻擊套件收錄新漏洞並散布勒索病毒

12

Adobe Flash Player 與物聯網 (IoT) 平台發現的漏洞數量持續增加

15

資料外洩災情肆虐各種產業

17

新版 PoS 惡意程式帶來新式攻擊

18

舊漏洞重獲新生

20

違反常理的銀行木馬程式

22

威脅情勢回顧

2015 年底，我們預言 2016 年將成為「網路勒索之年」[1]，其背後的因素包括資料外洩事件頻傳，歹徒進一步利用這些資料來從事網路勒索，以及類似的網路威脅數量不斷增加。

的確，2016 上半年，勒索病毒 Ransomware (勒索軟體/綁架病毒) 攻擊事件突然暴增，災情遍及各種產業。我們在 2016 上半年當中偵測及攔截了將近 8,000 萬個勒索病毒威脅。勒索病毒數量的急速成長，顯然意味著網路犯罪集團能夠輕易從勒索病毒獲得龐大的不法利潤。隨著勒索病毒數量持續增加，以及越來越多企業因被迫支付贖金而蒙受損失[2]，我們相信「勒索病毒當道的時代」將會持續下去。

就連原本專門經營漏洞攻擊套件的網路犯罪集團也開始注意到勒索病毒。在 2016 上半年當中，我們已開始發現會散布勒索病毒的漏洞攻擊套件。例如 Sundown[3] 和 Hunter 兩個漏洞攻擊套件今年開始挾帶勒索病毒，此外 Rig 也改變其套件所收錄的勒索病毒。同時，隨著 Angler 漏洞攻擊套件的使用率下滑，一些新的漏洞也被收錄到既有的漏洞攻擊套件當中。

除了勒索病毒之外，還有另一種變相的網路勒索叫做「變臉詐騙」(亦稱為「商務電子郵件入侵」Business Email Compromise，簡稱 BEC)，這類攻擊目前仍持續對受害者造成相當可觀的損失。有鑑於受害總金額已高達 30 億美元，美國聯邦調查局 (FBI) 特別針對多個產業發出緊急通告，請他們小心提防變臉詐騙。變臉詐騙要能成功，歹徒必須先入侵企業某高層主管的電子郵件帳號，然後利用長官的權威，再配上一些社交工程技巧與其他入侵手法便能得逞。

今年才過了一半，但我們已看到能夠癱瘓企業的威脅出現。在這份報告當中，我們整理出 2016 上半年發生的所有重大資安事件，讓企業針對網路犯罪集團可能利用的漏洞進行一番總體檢。同時，也再次強調企業必須謹慎尋找能夠阻止網路犯罪集團的解決方案，以免讓我們的預言成真。

註：文中所有提到「偵測」一詞的之處，皆指趨勢科技安全防護產品在使用者裝置上發現並攔截到的威脅。除非另有說明，否則本報告當中的數字皆來自趨勢科技 Smart Protection Network™ 雲端防護基礎架構所蒐集之資料。該基礎架構結合了雲端與用戶端技術來支援企業內安裝的產品以及雲端代管式服務。

勒索病毒稱霸威脅版圖

2016 上半年，勒索病毒的發展遠遠超乎我們預期。我們在前六個月就發現 79 個新的勒索病毒家族，這數字已經遠遠超越我們 2015 年一整年所偵測到的勒索病毒家族數量。同時，我們 2016 上半年所發現的勒索病毒家族數量也暴增了 172%。如需完整的勒索病毒家族清單，請參閱「威脅情勢回顧」一節當中的「表 3」。

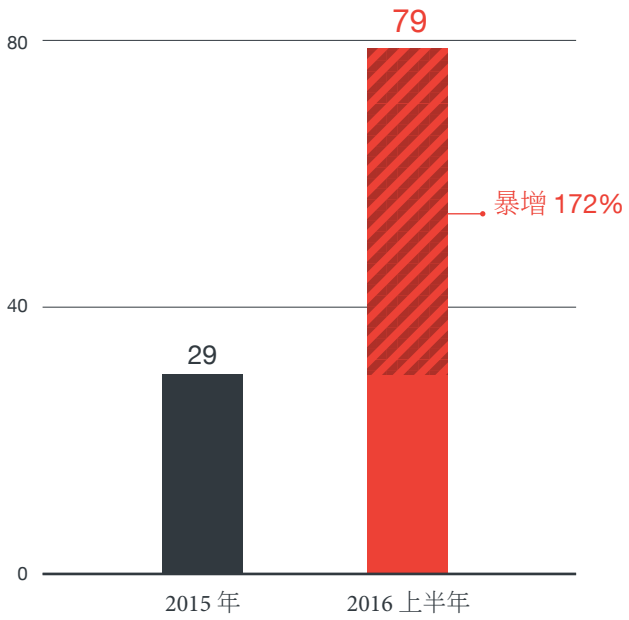

圖 1：新增加的勒索病毒家族 (2016 上半年)。

除了勒索病毒攻擊的數量令人擔憂之外，勒索病毒對企業造成的傷害之深，也讓這項威脅值得注意。根據 FBI 指出，勒索病毒在今年前三個月總計對企業造成了 2.09 億美元的財務損失。支付贖金固然不值得鼓勵，但對某些企業機構來說，這卻是救回重要檔案最快的方法，例如：好萊塢長老教會醫療中心 (Hollywood Presbyterian Medical Center) 支付了 17,000 美元[4]，加拿大卡加立大學 (University of Calgary) 支付了 16,000 美元[5]，美國南加州荷瑞郡 (Horry County) 學區支付了 10,000 美元[6]。勒索病毒除了能讓網路犯罪集團向企業勒索之外，還可能造成企業暫時停擺，使得日常營運和生產力受到莫大影響，例如，好萊塢長老教會醫療中心的網路就因此遭到癱瘓。

勒索病毒不斷成長，並頻繁出現新的變種。我們在 2016 上半年當中偵測及攔截了將近 8,000 萬個勒索病毒威脅。其中，58% 是經由垃圾郵件所挾帶的附件檔案，40% 是從專門散布勒索病毒或漏洞攻擊套件的網站下載的檔案，另有 2% 是實際的勒索病毒檔案。儘管如此，網路犯罪集團仍不斷開發新的手法和技巧來逼迫使用者支付贖金。例如，JIGSAW 勒索病毒每隔一小時不付贖金就會刪除一批檔案[7]，SURPRISE[8] 勒索病毒在過了期限之後會提高贖金。

2016 上半年也發現了多個專門攻擊企業電腦和端點裝置的勒索病毒，此外數量也有所成長。例如，CRYPSAM 會利用 Java 應用程式的漏洞來感染一些未修補的伺服器。這些伺服器一旦感染 CRYPSAM，與該伺服器連接的每一個網路都將被該勒索病毒感染[9]，此時，網路上的端點裝置只好自求多福。ZCRYPT 勒索病毒已知可經由 USB 隨身碟感染，這類隨身裝置在任何企業都很普遍[10]。除了 CRYPSAM 和 ZCRYPT 之外，還有其他勒索病毒家族也會對企業造成損害，這些家族包括：CRYPJOKER、前面提過的 SURPRISE，以及專門鎖定資料庫相關檔案、甚至報稅檔案的 POWERWARE[11]。另外，還有專門鎖定網站檔案的 CRYPRADAM 和 KIMCIL。

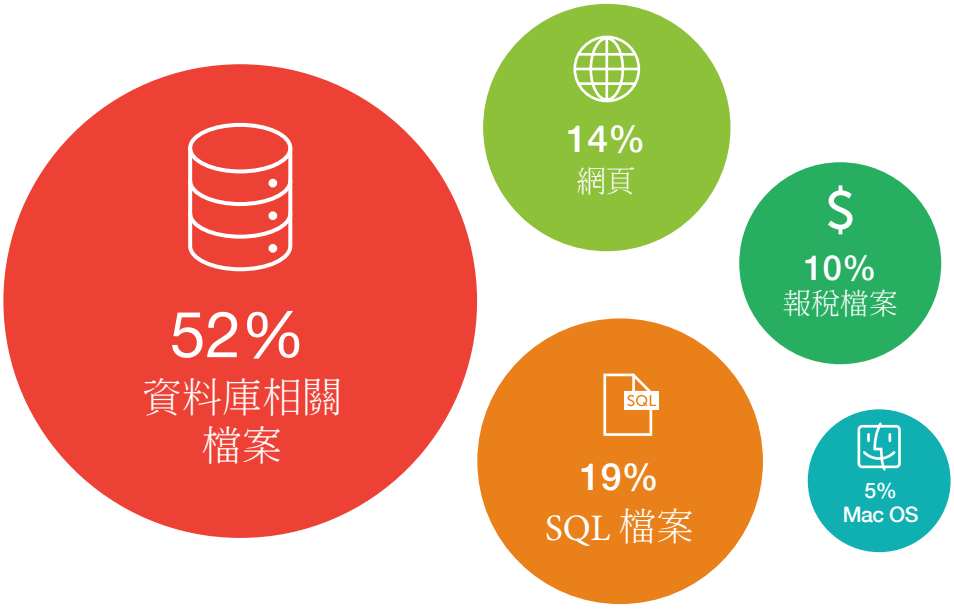

圖 2：已知勒索病毒家族會加密的企業檔案 (2016 上半年)。

從散布管道來看，勒索病毒已經開始經由電子郵件或垃圾郵件以外的途徑散布。2016 上半年，我們持續發現會散布勒索病毒的漏洞攻擊套件。還有，我們也看到經由遠端桌面遙控軟體散布的勒索病毒。既然勒索病毒的散布管道已經改變，我們相信傳統的資安防護已不再足夠，因為駭客經常會攻擊企業可能疏於防範的地方。

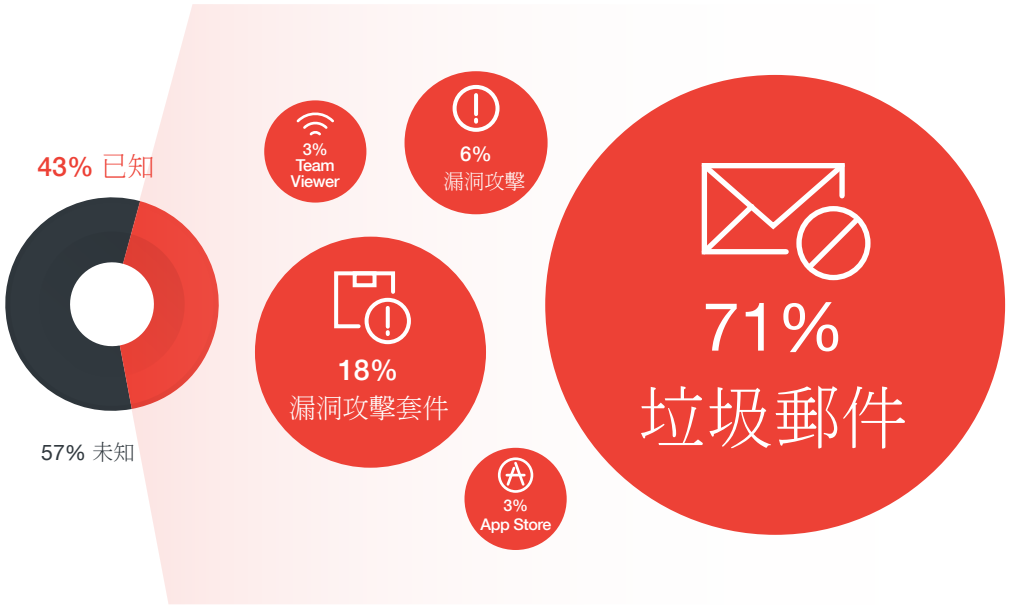

圖 3：已知的勒索病毒感染管道 (2016 上半年)。

網路犯罪集團的目標是企業最珍貴的資產，儘管勒索病毒的威脅如此猖獗，企業還是有一些方法可以避免感染勒索病毒。教育員工小心勒索病毒的危險固然重要，但一套多層式的資安防護策略更能有效防止勒索病毒滲透企業網路和端點，避免營運所需的關鍵檔案和資料遭到損毀。

既然已經有勒索病毒能夠攻擊伺服器未修補的漏洞，那麼定期修補或更新軟體有其必要。不過，軟體修補絕大部分取決於廠商正式釋出修補程式的頻率，以及網路系統管理員將修補程式套用至所有端點裝置的速度。因此，企業應認真考慮虛擬修補解決方案，該技術能在缺乏修補程式的空窗期當中有效保護關鍵的系統。

在網路防禦方面，企業應採用能夠監控網路連接埠並且具備信譽評等分析與攔截、腳本模擬、零時差漏洞偵測等技術的解決方案。此外，企業也應尋找具備客製化沙盒模擬分析的解決方案，如此，IT 系統管理員就能在一個安全的環境當中觀察疑似勒索病毒檔案的行為。

另一個企業可採取的策略是，透過行為監控和應用程式控管來保護一般使用者。行為監控可偵測系統內是否出現短時間之內加密大量檔案的行為，進而阻止這類加密動作以防止端點裝置遭到勒索病毒侵襲，避免損害擴大。至於應用程式控管解決方案，則可以只允許白名單內的正常應用程式執行。

變臉詐騙蔓延全球

所謂的「變臉詐騙」(亦稱為「商業電子郵件入侵」Business Email Compromise，簡稱 BEC)，是一種專門入侵企業高層主管電子郵件帳號，然後利用該帳號指示財務部門匯款至歹徒銀行帳戶的詐騙伎倆，可說是目前對企業最危險的一種網路威脅。根據 FBI 的統計，從 2015 年 1 月至 2016 年 6 月，全球變臉詐騙的受害企業超過 22,000 家，總損失金額超過 30 億美元[12]。從變臉詐騙的分布來看，不論大型企業或中小企業都無法倖免。根據我們的初步研究發現，變臉詐騙最猖獗的地區是美國、英國、香港、日本和巴西。此外，其他地區也曾經出現過一些變臉詐騙，如下圖所示。從這些資料，我們可以歸納出一個結論：變臉詐騙的確成為一個巨大的威脅。

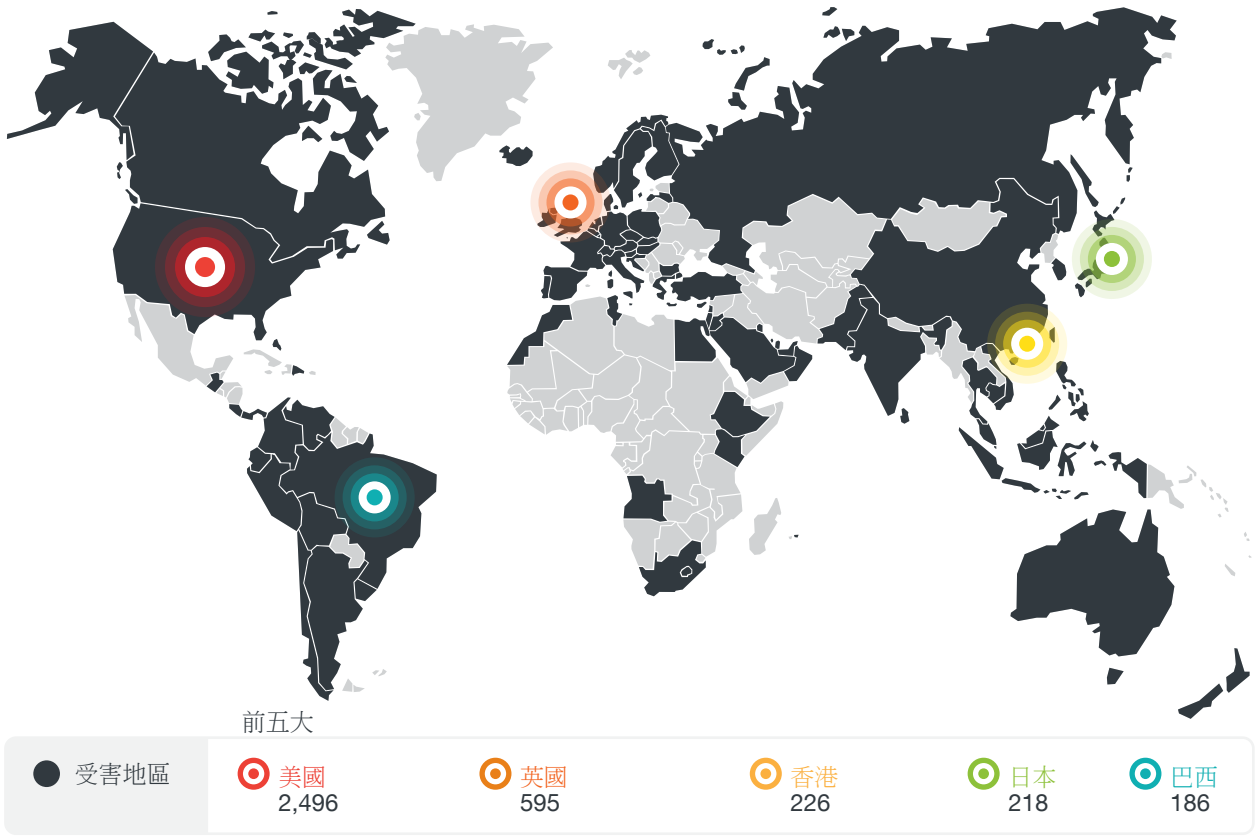

圖 4：變臉詐騙最猖獗的地區 (2016 上半年)。

變臉詐騙是否能夠成功，端看其是否能夠針對選定的對象使用適當的技巧。歹徒會運用他們對社交工程手法的理解，再配合他們研究目標對象之後的心得。在多數情況下，變臉詐騙都是假冒公司內能夠掌握財務的人員，可能對象包括公司的執行長、總經理、財務長，甚至是財務總監。根據我們 2016 年 1 月的監控資料，我們發現變臉詐騙鎖定財務長的機率比公司內任何其他職務都來得高。歹徒一旦選定某個擁有充分權限的目標，下一步就是誘騙受害對象核准一筆轉帳來支付某張發票的金額或某筆和解金[13]。

儘管變臉詐騙通常不會用到惡意程式，但仍有一些案例是利用惡意程式來犯案。這些惡意程式當中有的是一些簡單但卻有效的資訊竊取程式，例如鍵盤側錄程式。我們在 2014 年的變臉詐騙報告當中即指出，這類詐騙經常使用 Predator Pain 和 Limitless 這類鍵盤側錄程式[14]。某些駭客會在變臉詐騙當中使用鍵盤側錄程式來竊取一些可讓他們暗中執行非法銀行轉帳的機密資訊。

變臉詐騙非常狡猾。儘管其概念非常簡單，但歹徒所用的技巧卻相當複雜，而且成效卓越，因為他們利用的是人們對權威的敬畏。所以，防範變臉詐騙最有效的方法就是適當的員工教育和有效的資安產品雙管齊下，在威脅進入員工的信箱之前就預先攔截。

員工是防範變臉詐騙的最後一道防線。因此，企業必須訂定一些實務原則，好讓員工在遇到催促他們緊急轉帳的電子郵件時能有規則可循。這些原則包括：仔細檢驗要求付款的電子郵件、提升員工對變臉詐騙的防範意識、向執法機關檢舉詐騙案件。

既然大多數的變臉詐騙都不需要用到惡意程式，傳統只能偵測電子郵件是否含有惡意連結或惡意附件的電子郵件防護，並不足以防止變臉詐騙。企業需要一套能夠偵測電子郵件當中是否暗藏社交工程技巧的防護產品，以有效防止變臉詐騙的電子郵件。

漏洞攻擊套件收錄新漏洞並散布勒索病毒

雖然勒索病毒在 2016 上半年獨占鰲頭，但漏洞攻擊套件也沒有閒著，只是不如以往那麼普遍、那麼強烈。從 2016 年開始，我們便看到一股轉變的趨勢，使用 Angler 套件的攻擊逐漸減少。第一季，Angler 相關的攻擊事件減少了 33%，到了第二季，數量更持續下滑。

Angler 相關的攻擊數量萎縮，從 2016 年 6 月的媒體報導中可以知道，應該跟英國和俄羅斯逮捕了 50 名網路犯罪分子有關。此外，Angler 套件的使用率下滑，很可能代表網路犯罪集團認為 Angler 已經「遭到破解」，若再使用的話，可能讓執法人員盯上他們。所以，網路犯罪集團決定另覓出路。看到 Angler 套件開始走下坡，其他漏洞攻擊套件也趁機崛起。當散布 Angler 套件的網站存取次數開始下滑，數據清楚顯示專門散布 Neutrino 套件的網站存取次數便開始增加。

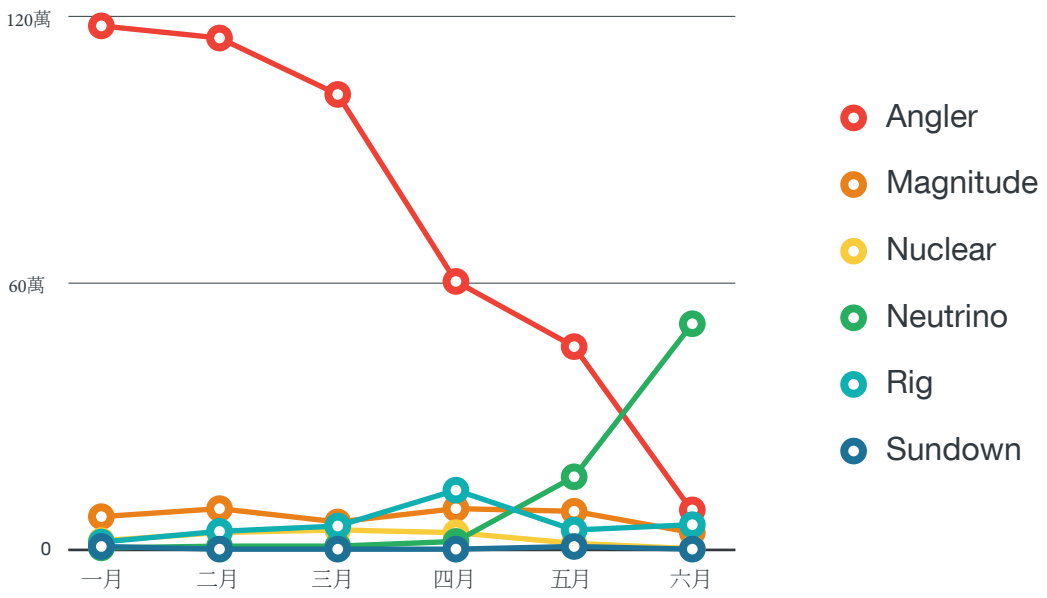

圖 5：專門散布漏洞攻擊套件的網址存取次數 (2016 上半年)。

今年六月，我們發表了一篇有關漏洞攻擊套件開始散布勒索病毒的報告[15]，包括 Rig、Hunter 和 Sundown 三個套件，它們會散布 GOOPIC 和 CRYPTOSHOCKER 勒索病毒。儘管 Rig 是一個相當新的漏洞攻擊套件，但其受害者已經遍布 40 多國，其中，日本是首要目標。當今年 Rig 和 Nuclear 開始改變其散布的勒索病毒時，還特別引起我們的注意 (從原本的 CRYPWALL、CRYPTESLA 和 CRYPCTB 換成 GOOPIC、CERBER、LOCKY 和 CRYPTESLA)。至於 Sundown 和 Hunter 則是今年才開始散布勒索病毒。

漏洞攻擊套件	散布的勒索病毒 (2015 年)	散布的勒索病毒 (2016 年)
Angler	CRYPWALL	CRYPWALL
	CRYPTESLA	CRYPTESLA
	CRILOCK	CRILOCK
		WALTRIX
Neutrino	CRYPWALL	CRYPWALL
	CRYPTESLA	CRYPTESLA
		CERBER
		WALTRIX
		LOCKY
Magnitude	CRYPWALL	CRYPWALL
		CERBER
Rig	CRYPWALL	GOOPIC
	CRYPTESLA	CERBER
Nuclear	CRYPWALL	CRYPTESLA
	CRYPTESLA	LOCKY
	CRYPCTB	
	CRYPSHED	
Sundown		CRYPTOSHOCKER
Hunter		LOCKY
Fiesta	CRYPTESLA	

表 1：各漏洞攻擊套件所散布的勒索病毒。

2016 上半年，一些新發現的漏洞也被收錄至現有的漏洞攻擊套件當中，大部分都是 Adobe® Flash® Player 的漏洞，其次是 Microsoft Internet Explorer® 和 Microsoft Silverlight® 的漏洞。有好幾個漏洞攻擊套件都收錄了這些新的漏洞。Angler 是收錄新漏洞最多的套件，Magnitude 和 Neutrino 也不遑多讓。儘管收錄了新的漏洞，但 2016 上半年漏洞攻擊套件新收錄的漏洞總數還是低於 2015 年。

即使 Angler 相關的攻擊已減少，但這不代表企業就能夠開始鬆懈。根據我們的資料顯示，漏洞攻擊套件的威脅依然非常活躍，因為新的漏洞攻擊套件填補了 Angler 所留下的空缺，而且漏洞攻擊套件開始散布勒索病毒，有些套件甚至收錄了不少新的漏洞。這只意味著一件事：歹徒一直在尋找機會利用這些舊漏洞來發動針對性攻擊。在這樣的情況下，企業不論大小、不論產業都必須更小心防範漏洞攻擊套件進入其系統。從下圖可看出歹徒試圖攻擊這些漏洞的情況越來越多。

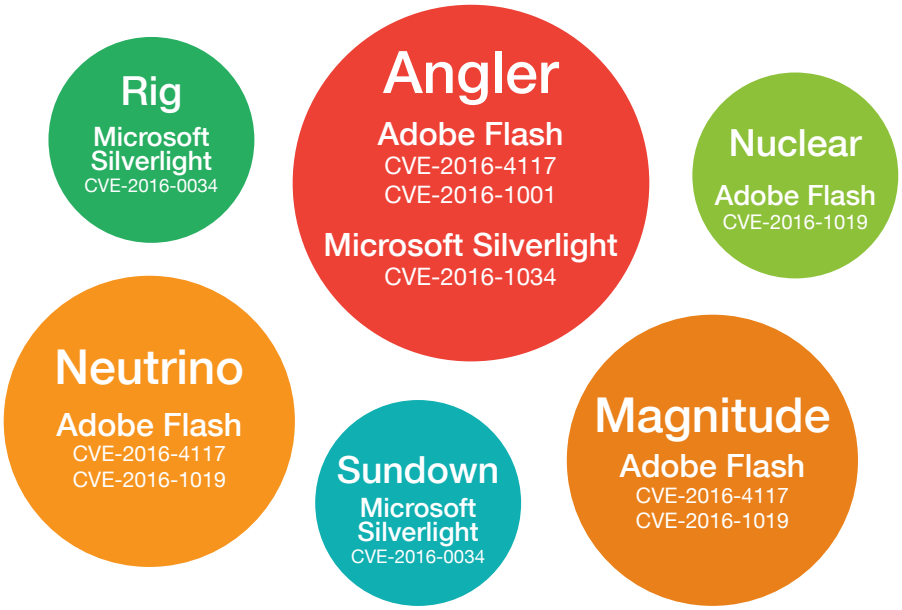

圖 6：各家漏洞攻擊套件所收錄的漏洞 (2016 上半年)。

漏洞攻擊套件入侵企業網路的途徑，就是經由未修補的軟體漏洞。然而在大多數情況下，定期套用修補程式可說是一項既耗時又耗成本的挑戰。手動修補的另一項難題是，當企業在等待廠商釋出正式修補程式時，企業等於處於空窗期。再者，若企業仍在使用一些老舊的軟體，那麼風險就更高。解決這類漏洞問題的最好辦法之一就是所謂的「虛擬修補」，這項技術可以防堵系統漏洞，防範專門利用這些漏洞的攻擊套件。

Adobe Flash Player 與物聯網 (IoT) 平台發現的漏洞數量持續增加

談到新漏洞的發現，關鍵在於時機。對於資安研究人員來說，最好的時機莫過於在駭客開始利用漏洞來發動攻擊之前。然而對駭客來說，最好的時機是資安研究人員發現之前，或者在軟體廠商釋出修補程式之前。因為企業被困在這場抓漏洞的競賽當中，企業必須搶先一步防堵網路上的漏洞，以免遭到攻擊、蒙受損失。

對企業來說，想要搶先一步就必須隨時掌握最新發現的漏洞，並且確實對所有需要的系統進行修補。光是 2016 上半年，趨勢科技 (加上 TippingPoint) 和 ZDI 漏洞懸賞計劃在市面上各家軟體當中就發現了 473 個漏洞，其中漏洞最多的是 Adobe Flash 和研華科技 (Advantech) 的 WebAccess 遠端監控軟體。以下是漏洞發現數量最多的十大軟體：

由趨勢科技所發現 (與 TippingPoint 合作)		經由 ZDI 漏洞懸賞計劃發現	
產品	#CVE	產品	#CVE
Adobe Flash	28	Web Access	108
Android	11	Adobe Reader DC	26
OS X	11	Storage Resource Monitor Profiler Module	24
iOS	8	Foxit Reader	23
Microsoft Office	5	Internet Explorer	22
Internet Explorer	3	Adobe Acrobat Pro DC	19
Qualcomm	1	OS X	17
Apache Active MQ	1	Application Testing Suite	15
ffmpeg	1	LeviStudio	14
Edge	1	Edge	13

表 2：漏洞發現最多的十大應用程式 (2016 上半年)。

Adobe Flash Player 被發現的漏洞數量，跟歹徒嘗試利用該平台發動零時差攻擊與勒索病毒攻擊的數量有關。今年稍早，我們發現一些來自 Magnitude 漏洞攻擊套件的零時差攻擊，其目標是 Adobe Flash Player 某些版本中的 CVE-2016-1019 漏洞。已收錄該漏洞的套件讓許多系統都不幸感染了勒索病毒[16]。

駭客利用 Adobe Flash Player 漏洞來發動零時差攻擊的作法已行之有年，未來勢必仍會持續下去。去年即出現了多起利用 Adobe Flash Player 漏洞的零時差攻擊。其中一個使用 Angler 套件來散布惡意廣告[17]，另一個則是駭客掌控了受害的電腦[18]。此外，還有一個 Adobe Flash 零時差漏洞出現在 Pawn Storm 攻擊行動當中，這是一項遍及全球多個重要目標的攻擊行動[19]。

漏洞數量排名第二的是研華科技的 WebAccess 軟體，這是一個網站式人機介面 (HMI) 以及監控與資料擷取 (SCADA) 軟體，可從遠端將工業流程自動化。今天，許多全球的公家機關和民間機構都在使用 SCADA 軟體。光是研華科技的據點就遍布全球 23 個國家，其大部分客戶都集中在大中華區和美國[20]。在我們發現的 108 個 WebAccess 軟體漏洞當中，有 28 個是零時差漏洞。

就發現漏洞這件事來說，像 ZDI 這樣的懸賞計畫是個不錯的辦法，尤其對像研華科技的 WebAccess 這類應用在物聯網 (IoT) 和 SCADA 系統的軟體程式來說特別有效。這類平台很多在開發時都是以功能 (而非安全) 為主要考量，這一點，讓使用者暴露在許多風險當中。隨著 IoT 日漸普及，再加上專門針對 SCADA 基礎架構的威脅正虎視眈眈，SCADA 和 IoT 平台的安全性顯得非常重要。

除了趨勢科技和 TippingPoint 合作發現的這些漏洞之外，今年上半年還有許多其他重大的漏洞被發現。除了 Adobe Flash Player 的零時差漏洞之外，Pwn2Own 2016 世界駭客大賽期間也發現了 21 個新的漏洞，這是一個一年一度的漏洞研究競賽，參加的都是來自全球的資安研究專家。該活動期間還揭露了六個瀏覽器漏洞和六個系統核心漏洞[21]。以下是被發現漏洞的產品及漏洞數量：

- Microsoft Windows: 6
- Apple OS X: 5
- Adobe Flash: 4
- Apple Safari: 3
- Microsoft Edge: 2
- Google Chrome: 1

就在 Pwn2Own 大賽結束後一個月，TippingPoint 的 ZDI 計劃在 Apple® 的 QuickTime® for Windows 發現了兩個重大漏洞。這兩個漏洞出現的時機，剛好在 Apple 宣布不再為 Windows 版 QuickTime 提供安全更新之後[22]。

就在資安人員和駭客陷入漏洞的修補和攻擊競賽之際，企業和產業應該嘗試以最有系統的方式來解決漏洞的問題。例如，ZDI 就提供獎勵來鼓勵資安研究人員以負責任的方式揭露系統漏洞，並且擔任中間人的角色來協助解決軟體廠商產品當中所發現的漏洞。這對漏洞研究人員和軟體廠商來說是個雙贏的局面，因為它提供了一個良好的資訊溝通管道。光是 2016 上半年，ZDI 收到的 Adobe 漏洞就超過了 Microsoft 漏洞。

雖然趨勢科技和 TippingPoint 的通力合作或許無法全面阻止網路犯罪集團利用軟體漏洞，但雙方的合作卻能協助企業搶先歹徒一步，並且為其網路建立堅強的防護，甚至防範尚未被發現的漏洞。當軟體廠商尚未釋出正式修補程式或者已經終止產品支援時，企業必須利用虛擬修補技術來提供有效且高效率的防堵，避免漏洞遭到攻擊。藉由這類資安過濾機制，企業就能主動掌控自己的系統安全，不必擔心成為駭客攻擊的受害者。除此之外，隨時保持軟體更新，勤於修補已經公開的重大漏洞，也能為企業提供一層額外的保障。

資料外洩災情肆虐各種產業

資料外洩現在已經成了常態。不論每一年的威脅主角是什麼，資料外洩永遠都是一項普遍且損失慘重的威脅，尤其對企業更是如此。2016 年最近的一個案例是社群網站 Myspace 外洩了 3.6 億筆使用者名稱和密碼[23]。儘管 Myspace 目前已不像過去那樣流行，但駭客還是可能利用這些偷來的帳號密碼來試圖登入受害者在其他網站的帳號。今年三月，Verizon (威信通訊) 也發生了嚴重的資料外洩，駭客偷走 150 萬筆 Verizon Enterprise Solutions 客戶的聯絡資訊並拿到地下網路上公開兜售[24]。值得注意的是，「財星 500 大」(Fortune 500) 企業當中有 97% 都是 Verizon 的客戶。

2016 上半年，不論政府機關、醫療產業，甚至娛樂產業都傳出資料外洩的災情。在第一季季末，美國癌症治療機構 21st Century Oncology 表示遭駭客竊取了 220 萬筆病患個人資訊[25]。一個月前，駭客盯上美國國稅局 (IRS) 並竊取了 464,000 筆非重複的社會安全號碼，並利用這些資料偽冒納稅人申請退稅[26]。

每當有企業或機構發生資料外洩，歹徒就會得到今日最寶貴的商品，也就是資訊。不論是個人身分識別資訊 (PII)、醫療記錄、支付卡資料，甚至是帳號登入資訊，歹徒都能找到利用這些資訊的方法，包括：金融詐騙、身分冒用、散發黑函、間諜行動，甚至勒索。儘管身分識別資料外洩不一定會直接造成財務損失，但企業卻可能蒙受遠大於財物損失的信用和商譽損失。一旦發生這樣的情況，企業將前途堪憂。

既然資料外洩是企業揮之不去的真實風險，IT 系統管理員必須預先做好準備，採用能夠有效防範資料外洩事件的解決方案。在資料外洩原因方面，裝置遺失依然是排行第一。我們的研究發現，裝置遺失占了所有資料外洩的 41% [27]。在今日的世界中，資料越來越行動化，人們經常利用筆記型電腦、行動裝置、隨身碟、甚至

雲端來存取資料。正因如此，企業很重要的一點是採用能夠在各個環節上追蹤、保護及加密機密資料的解決方案，如此一來，就算裝置遺失或失竊也不怕。此外，企業應再搭配嚴格的政策來規範儲存在行動裝置上的機密資訊。

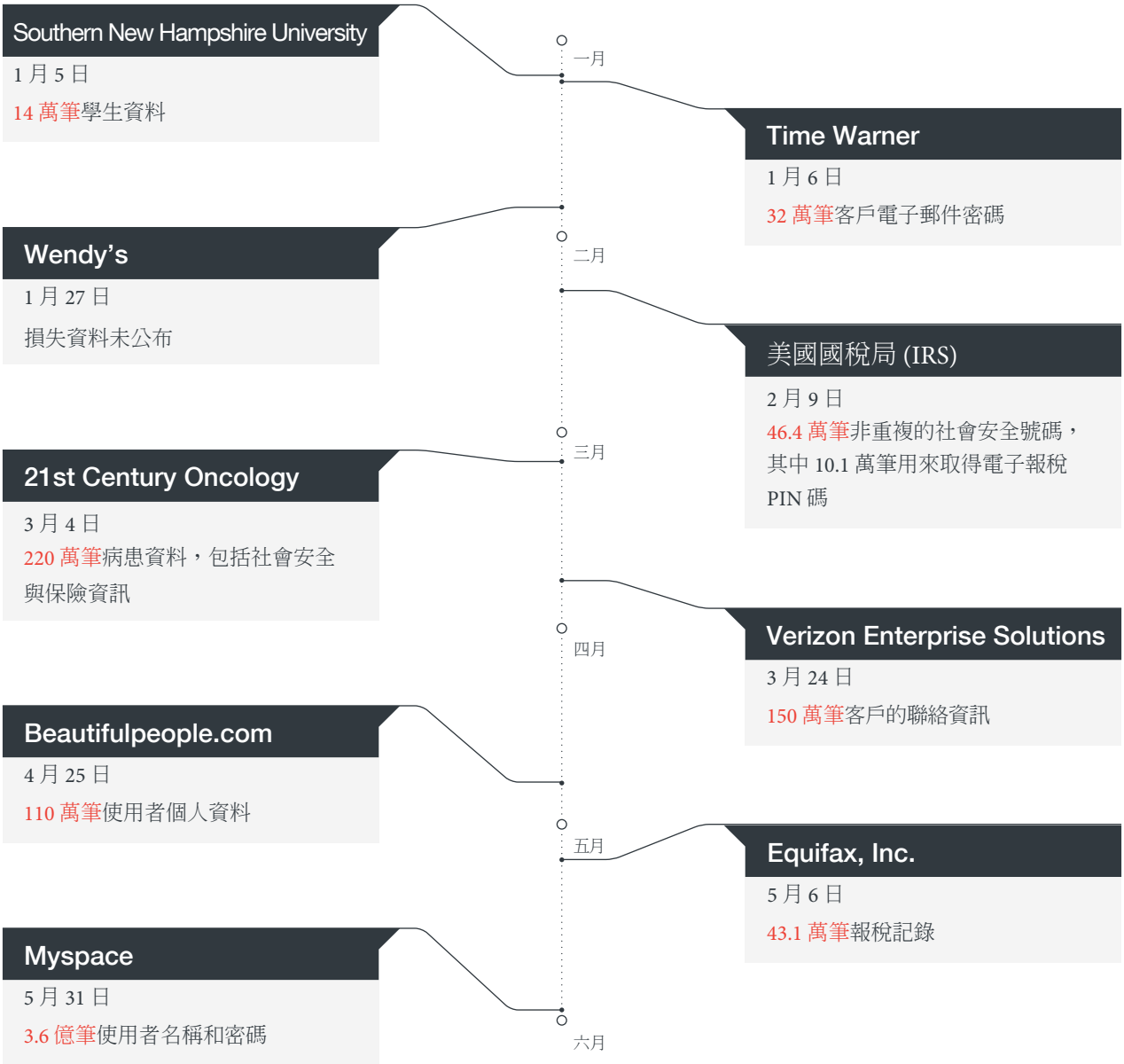

圖 7：資料外洩時間表 (2016 上半年)。

僅次於裝置遺失的資料外洩原因是：駭客入侵 (不論使用暴力破解或社交工程技巧) 和惡意程式，這也是駭客最常用的兩種竊取資料的方法。要防範這兩項，企業必須採用能夠偵測、分析、回應進階惡意程式與其他駭客竊取技巧的解決方案。

新版 PoS 惡意程式帶來新式攻擊

今年 6 月，我們發現了一個新的銷售櫃台系統 (PoS) 惡意程式，擁有超高效率的偷竊能力。我們將它命名為 FASTPoS，因為該惡意程式在被感染的終端機刷卡之後就立刻將竊取到的資料傳送給駭客，而非等到排定的時間再傳送資料。由於 FastPoS 回傳資料給駭客的時機如此迅速，我們認為這個 PoS 惡意程式應該是專為網路環境不大的中小企業所設計。儘管如此，FastPoS 惡意程式的受害者已遍及台灣、日本、香港、巴西、法國、伊朗、美國等地[28]。

除了 FastPoS 惡意程式之外，還有具備類似「蠕蟲」功能的新版 FighterPoS 惡意程式，它可從某個 PoS 終端機擴散至同一網路下的另一台終端機[29]。FighterPoS 的作者之所以增加這項功能，似乎是為了擴充版圖。原本一開始，感染 FighterPoS 的受害者只侷限於巴西，但在最近的幾次更新，我們注意到 FighterPoS 已開始攻擊美國的受害者。雖然 PoS 惡意程式已經不再是什麼新聞，但這類惡意程式仍持續不斷進化，而且對企業的殺傷力更強。除了營業損失的風險之外，企業還必須面對洩漏客戶資料的後果。

為了防止端點裝置感染 PoS 惡意程式，企業可採用一些具備應用程式控管或白名單列表的解決方案。這類功能可讓 IT 系統管理員防止裝置安裝任何不在白名單內的應用程式和/或更新。

舊漏洞重獲新生

每一次的攻擊，網路犯罪集團都會試著尋找最容易的入侵途徑，其中一個最容易的途徑就是含有漏洞的系統，不論新舊。在 2016 上半年期間，我們發現許多試圖經由 Microsoft IIS 漏洞 (CVE-2015-1635) 和兩個 Shellshock Bash 漏洞 (CVE-2014-6271/CVE-2014-6278) 的攻擊。

對企業來說，Shellshock (或稱 Bash Bug) 是很重要的一個漏洞，因為該漏洞的影響範圍涵蓋全球數十億台伺服器和裝置。Shellshock 漏洞絕大部分出現在 Unix、Linux 和 Mac OSX 系統，可讓駭客從遠端執行指令來取得系統控制權，甚至不需經過身分認證。經由此漏洞，駭客還能存取伺服器上儲存的機密資訊，或者在伺服器上留下後門，方便他們將來進出[30]。

今年上半年，利用 Shellshock 漏洞的攻擊有越來越多的趨勢，這很可能意味著歹徒正試圖利用舊漏洞來發動新的攻擊。下圖顯示試圖利用前述各項漏洞的攻擊數量：

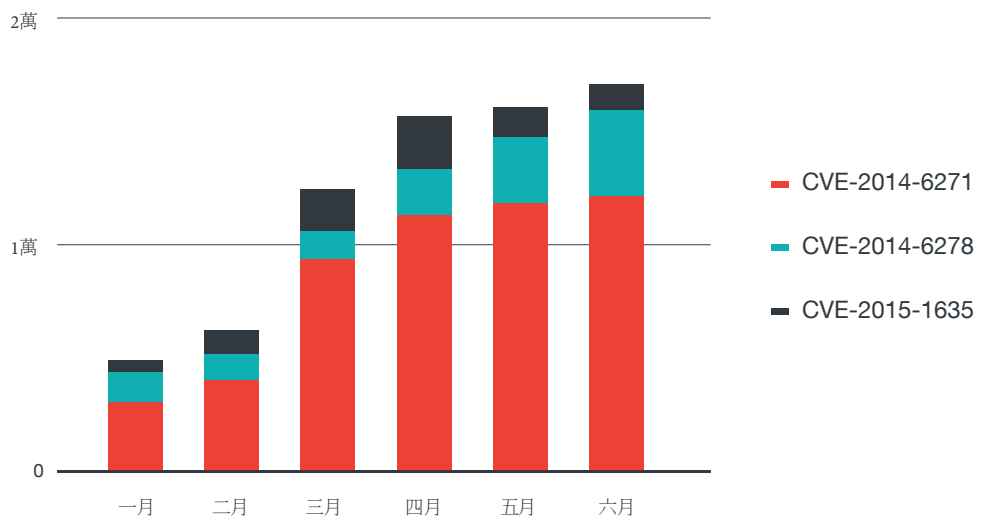

圖 8：各個漏洞運用在攻擊中的次數 (2016 上半年)。

要防範伺服器遭到漏洞攻擊，企業必須定期修補伺服器。不過，要頻繁地手動修補和更新軟體可說是一項挑戰，因為，每個月都會有數百個軟體漏洞被發現。除了手動修補軟體的流程缺乏效率之外，企業在等候軟體廠商正式釋出修補程式的空窗期，也會讓駭客有機可乘。要解決這項問題，企業必須採用具備虛擬修補技術的解決方案，這類技術能夠在正式的修補程式出現之前防堵漏洞。此外，虛擬修補技術還能為已經終止支援的老舊系統或軟體提供立即的漏洞防護。

違反常理的銀行木馬程式

一般來說，當犯罪集團遭到逮捕之後，犯罪率應該會下降才對，但今年的銀行木馬程式卻反其道而行。就在 2015 年結束之前，DYRE/DYREZA 銀行木馬程式幕後的網路犯罪集團遭到了逮捕。但銀行木馬程式並未因此而中斷，原因是 QAKBOT 東山再起。我們相信 QAKBOT 的偵測數量增加是因為有其他網路犯罪集團趁機崛起，填補了 DYRE/DYREZA 的作者遭到逮捕之後所留下的空缺[31]。

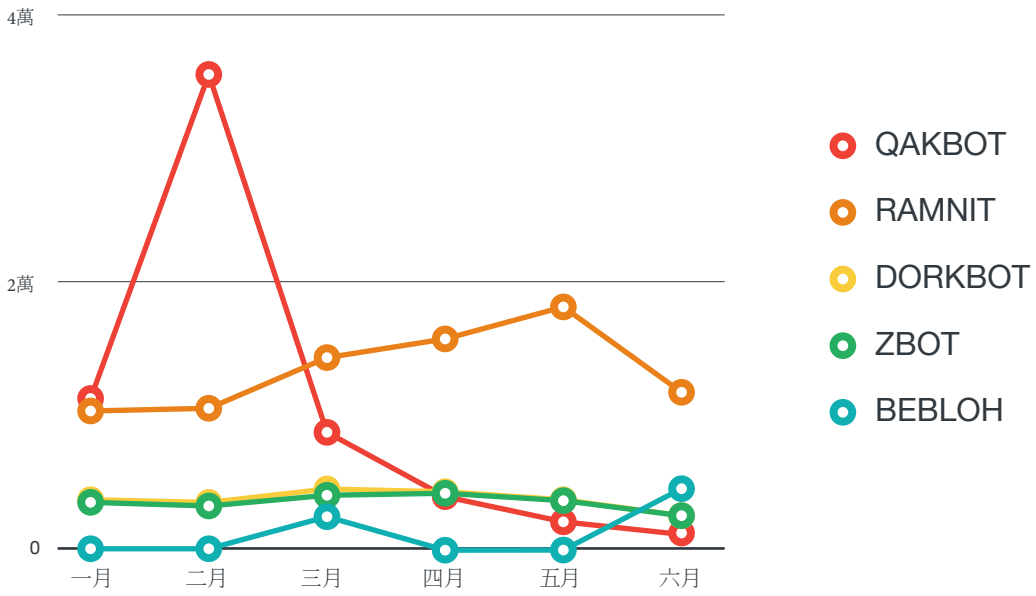

圖 9：惡意程式家族排行榜 (2016 上半年)。

QAKBOT 是一個包含多個元件的威脅，對企業的影響深遠。自從 2007 年出現以來，QAKBOT 總是有辦法入侵使用者的裝置並竊取資訊，受害者遍及美國、加拿大和巴西。QAKBOT 所覬覦的重要資訊包括銀行帳號密碼、上網瀏覽習慣，以及使用者的敏感資訊。QAKBOT 之所以難以應付，是因為它一直持續不斷演進 (今年稍早即出現兩個變種：WORM_QAKBOT.SMUV 和 WORM_QAKBOT.SMUX) 以及它匿蹤的行為。

面對像 QAKBOT 這樣的銀行木馬程式，銀行和客戶都應負起安全責任，因為，許多企業員工都會經由企業內部網路來使用網路銀行，不論是透過桌上型電腦或是行動裝置。因此，對使用者而言，銀行帳號資訊一旦被偷，財務損失將在所難免，因為網路犯罪集團可以利用這些資訊來暗中執行轉帳交易，或者將這些資訊出售變現。對銀行業來說，感染銀行木馬程式很可能為企業帶來出乎意料的成本，因為銀行可能要賠償客戶的存款損失，並且還要花費成本從損害中復原。

QAKBOT 可經由各種感染途徑進入使用者的系統，例如：當使用者瀏覽到一個惡意的網站，或者當使用者經由一封電子郵件下載到一個惡意的 PDF 檔案。在這樣的情況下，最理想的解決方案是能夠同時防範網站、檔案、電子郵件等多重入侵點的防護產品。這樣的解決方案必須能夠提供一種環環相扣的威脅防禦，根據網站、檔案及電子郵件等管道的威脅資訊來攔截惡意活動。

除了保護端點裝置、讓裝置免於這項威脅之外，銀行網站也應採用雙重驗證機制。同時，銀行網站也應鼓勵客戶不論在開啟電子郵件、瀏覽網站或下載檔案時，都應隨時保持警戒及安全意識。

威脅情勢回顧

2016 上半年，我們總共攔截了 290 億個威脅，這數字已經超越 2015 年總數的一半。威脅數量的增加，有可能是因為勒索病毒攻擊數量不斷成長所造成。

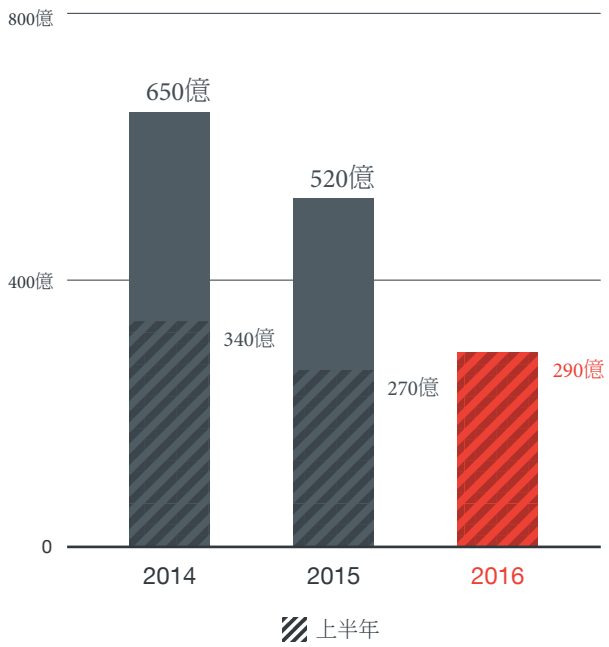

圖 10：趨勢科技 Smart Protection Network™ 已攔截的威脅總數 (2016 上半年)。

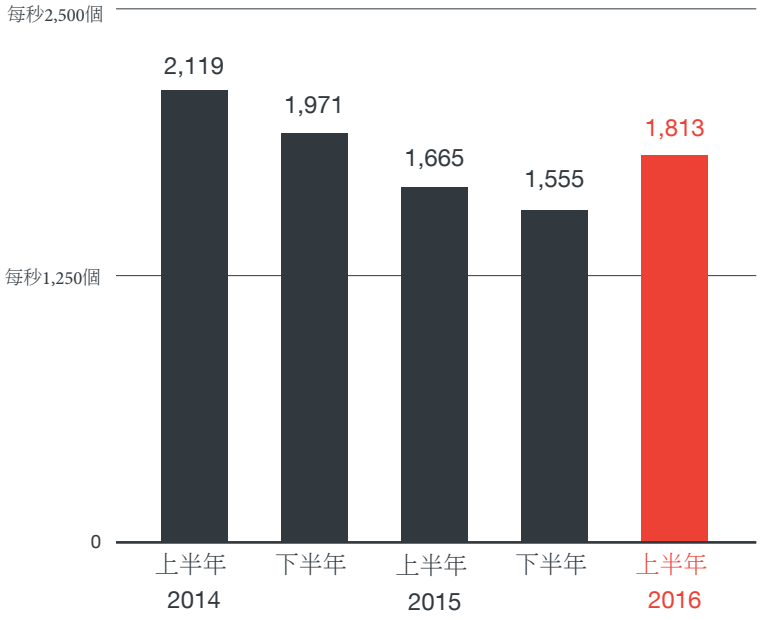

圖 11：每秒攔截的威脅數量 (2016 上半年)。

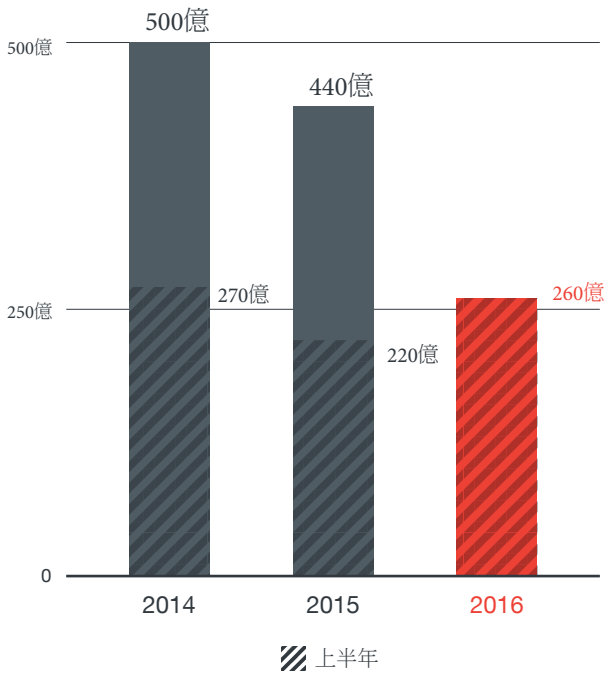

圖 12：已攔截的電子郵件威脅數量 (2016 上半年)。

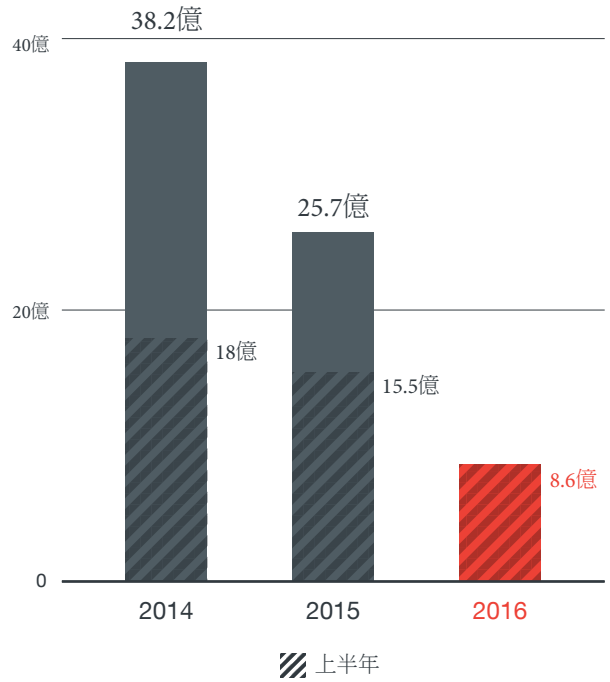

圖 13：已攔截的惡意網址數量 (2016 上半年)。

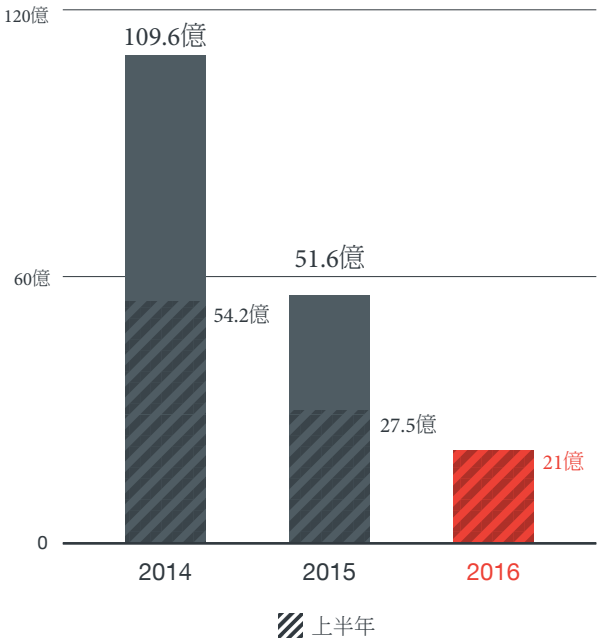

圖 14：已攔截的惡意檔案數量。

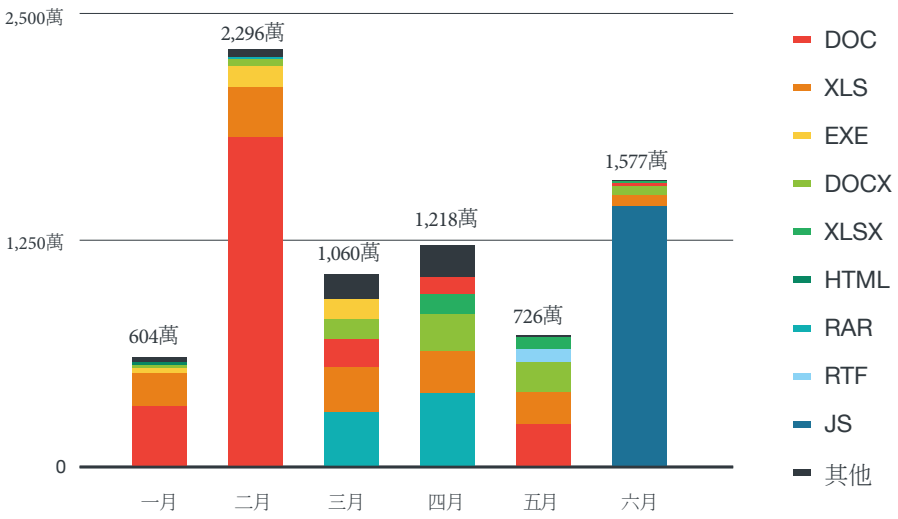

圖 15：勒索病毒相關垃圾郵件最常見的附件檔案類型 (2016 上半年)。

今年六月，垃圾郵件挾帶的 JavaScript 附件檔案數量明顯增加。主要是勒索病毒相關的垃圾郵件所散布。

圖 16：已曝光的勒索病毒事件 (2016 上半年)。

					總數
一月	LECTOOL	CRYPRADAM	CRYPNISCA	CRYPRITU	7
	EMPER	MEMEKAP	CRYPJOKER		
二月	CRYPGPCODE	CRYPDAP	MADLOCKER		6
	CRYPHYDRA	CRYPZUQUIT	LOCKY		
三月	CERBER	MAKTUB	CRYPTOSO	KIMCIL	14
	CRYPAURA	SURPRISE	COVERTON	CRYPTEAR	
	KERANGER	PETYA	CRYPSAM		
	CRYPTESLA	POWERWARE	CRYPTOHASU		
四月	CRYPSALAM	JIGSAW	EMPER 2.0	CRYPLIKI	11
	CRYPTOHOST	WALTRIX	CRYPVAULT	CRYPALPHA	
	XORBAT	ZIPPY	CRYPCORE		
五月	ROKKU	MISCHA	TAKALOCKER	DEMOCRY	19
	BRLOCK	WALTRIX 2.0	BADBLOCK	BUCBI	
	CRYPMAME	ENIGMA	ZCRYPT	CRYPDAP	
	SHUJIN	SNSLOCK	ELFACRYPT	CRIPTODC	
	AUTOLOCKY	BLOCCATO	LOCKSCAM		
六月	JIGSAW 2.0	GOOPIC	CRYPSHOCKER	BART	24
	WALTRIX 3.0	APOCALYPSE	WHITELOCK	CRYPMIC	
	CRYPHERBST	JSRAA	LOCKRVTN	SATANA	
	CRYPEDA	CRYPCUTE	JOKOZY	ZIRBAM	
	CRYPAGA	CYPHERKEY	MIRCOP		
	WALTRIX 4.0	CRYPKEYIV	XORIST		

表 3：已現身的新勒索病毒家族 (2016 上半年)。

參考資料

1. 趨勢科技。(2015 年 10 月 27 日)。*趨勢科技資訊安全情報*。「趨勢科技 2016 年資安預測：細微的界線」(2016 Trend Micro Security Predictions: The Fine Line)。上次存取時間 2016 年 8 月 5 日： http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2016

2. 趨勢科技。(2016 年 2 月 15 日)。*趨勢科技資訊安全新聞*。「勒索病毒挾持好萊塢醫院的資料」(Ransomware Attack Holds Hollywood Hospital Records Hostage)。上次存取時間 2016 年 8 月 5 日：http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ransomware-attack-holds-hollywood-hospital-records-hostage-for-3-6m

3. Joseph C. Chen。(2016 年 6 月 22 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Angler 之後的漏洞攻擊套件發展趨勢與最新加密勒索病毒活動」(After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

4. Allan Stefanek。(2016 年 2 月 17 日)。*Hollywood Presbyterian*。「好萊塢長老教會醫療中心執行長的信」(Hollywood Presbyterian Medical Center Memo from the CEO)。上次存取時間 2016 年 8 月 9 日：http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf

5. University of Calgary。(2016 年 6 月 8 日)。*UToday*。「卡加立大學大刀闊斧解決系統問題」(University of Calgary makes significant progress to address system issues)。上次存取時間 2016 年 8 月 5 日：http://www.ucalgary.ca/utoday/issue/2016-06-08/university-calgary-makes-significant-progress-address-systems-issues

6. Ryan Webb。(2016 年 3 月 7 日)。*WBTW News13*。「荷瑞郡支付將近 1 萬美元給勒索病毒駭客」(Horry County pays nearly $10k to 'ransomware' hackers)。上次存取時間 2016 年 8 月 5 日：http://wbtw.com/2016/03/07/horry-county-pays-nearly-10k-to-ransomware-hackers/

7. Jasen Sumalapao。(2016 年 4 月 19 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「新的 JIGSAW 加密勒索病毒更令人棘手」(New Crypto-Ransomware JIGSAW Plays Nasty Games)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/

8. 趨勢科技。(2016 年 8 月 5 日)。*趨勢科技威脅百科 (Threat Encyclopedia)*。「RANSOM_SURPRISE.A」。上次存取時間 2016 年 8 月 5 日： http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_surprise.a

9. 趨勢科技。(2016 年 4 月 22 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「關於系統修補的一堂課：SAMSAM 加密勒索病毒的崛起」(A Lesson on Patching: The Rise of SAMSAM Crypto- Ransomware)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/lesson-patching-rise-samsam-crypto-ransomware/

10. Jasen Sumalapao。(2016 年 5 月 31 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「加密勒索病毒只能攻擊 Windows 7 及新版作業系統，捨棄向下相容性」(Crypto-ransomware Attacks Windows 7 and Later, Scraps Backward Compatibility)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/crypto-ransomware-attacks-windows-7-later-scraps-backward-compatibility/

11. 趨勢科技。(2016 年 5 月 31 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「報稅勒索：PowerWare 加密勒索病毒攻擊報稅檔案」(Tax Day Extortion: PowerWare Crypto-ransomware Targets Tax Files)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/tax-day-extortion-powerware-crypto-ransomware-targets-tax-files/

12. 美國聯邦調查局 (FBI)。(2016 年 6 月 14 日)。*網際網路犯罪申訴中心 (Internet Crime Complaint Center)*。「變臉詐騙/商務電子郵件入侵 (BEC)：31 億美元的詐騙」(Business E-mail Compromise: The 3.1 BillionDollar Scam)。上次存取時間 2016 年 8 月 5 日：https://www.ic3.gov/media/2016/160614.aspx

13. 趨勢科技。(2016 年 6 月 9 日)。*趨勢科技資訊安全新聞*。「數十億美元的詐騙：變臉詐騙/商務電子郵件入侵 (BEC) 背後的數字」(Billion-Dollar Scams: The Numbers Behind Business Email Compromise)。上次存取時間 2016 年 8 月 5 日：http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise

14. Ryan Flores。(2014 年 11 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Predator Pain 和 Limitless：詐騙的幕後推手」(Predator Pain and Limitless: Behind the Fraud)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/

15. Jon Oliver 和 Joseph C. Chen。(2016 年 6 月 27 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「勒索病毒為何有效：入侵途徑」(Why Ransomware Works: Arrival Tactics)。上次存取時間 2016 年 8 月 11 日：http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-arrival-methods/

16. Peter Pi、Brooks Li 和 Joseph Chen。(2016 年 4 月 7 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「零時差漏洞攻擊現身：Magnitude 漏洞攻擊套件收錄舊版 Adobe Flash Player 零時差漏洞 CVE-2016-1019」(Zero-Day Attack Discovered in Magnitude Exploit Kit Targeting CVE-2016-1019 in Older Versions of Adobe Flash Player)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2016-1019-zero-day-integrated-in-exploit-kit/

17. Peter Pi。(2015 年 2 月 2 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「趨勢科技發現惡意廣告使用新的 Adobe Flash 零時差漏洞攻擊」(Trend Micro Discovers New Adobe Flash Zero-Day Exploit Used in Malvertisements)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/

18. Peter Pi。(2016 年 7 月 11 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Hacking Team 資料外洩事件又一個新的 Adobe Flash 零時差漏洞 (CVE-2015-5123) 曝光」(New Zero-Day Vulnerability [CVE-2015-5123] in Adobe Flash Emerges from Hacking Team Leak)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/new-zero-day-vulnerability-cve-2015-5123-in-adobe-flash-emerges-from-hacking-team-leak/

19. 趨勢科技。(2015 年 10 月 13 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Pawn Storm 使用新的 Adobe Flash 零時差漏洞來攻擊各國外交部」(New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

20. 研華科技 (Advantech)。(2016 年)。*Advantech*。「公司簡介」(Fast Facts)。上次存取時間 2016 年 8 月 5 日：http://www.advantech.com/about/fastfacts

21. Steve Povolny。(2016 年 3 月 21 日)。*趨勢科技就是要安全部落格 (Simply Security Blog)*。「Pwn2Own 2016 — 趨勢科技 Trend Micro TippingPoint DVLabs 獨家零時差漏洞報導！」(Pwn2Own 2016 – Trend Micro TippingPoint DVLabs Exclusive Zero Day Coverage!)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/pwn2own-2016-trend-micro-tippingpoint-dvlabs-exclusive-zero-day-coverage/

22. US-CERT。(2016 年 4 月 14 日)。*United States Computer Emergency Readiness Team*。「Apple 終止 QuickTime for Windows 支援，新漏洞立刻現身」(Apple Ends Support for QuickTime for Windows; New Vulnerabilities Announced)。上次存取時間 2016 年 8 月 5 日：https://www.us-cert.gov/ncas/alerts/TA16-105A

23. Elizabeth Weise。(2016 年 5 月 31 日)。*USA Today*。「3.6億個 Myspace 帳號遭到外洩」(360 million Myspace accounts breached)。上次存取時間 2016 年 8 月 5 日： http://www.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/

24. Jon Brodkin。(2016 年 3 月 25 日)。*arsTechnica*。「Verizon 資料外洩之後，150 筆客戶資料被上網兜售」(After Verizon breach, 1.5 million customer records put up for sale)。上次存取時間 2016 年 8 月 5 日：http://arstechnica.com/security/2016/03/after-verizon-breach-1-5-million-customer-records-put-up-for-sale/

25. Frank Gluck。(2016 年 3 月 10 日)。*News-Press*。「資料外洩影響 220 萬名 21st Century Oncology 癌症治療中心病患」(Data Breach Affects 2.2M 21st Century Oncology Patients)。上次存取時間 2016 年 8 月 9 日：http://www.news-press.com/story/news/2016/03/09/data-breach-affects-22m-21st-century-onoclogy-patients/81525656/

26. IRS。(2016 年 2 月 9 日)。*Internal Revenue Service*。「IRS 針對電子報稅 PIN 碼的聲明」(IRS Statement on E-filing PIN)。上次存取時間 2016 年 8 月 5 日： https://www.irs.gov/uac/Newsroom/IRS-Statement-on-Efiling-PIN

27. 趨勢科技。(2015 年 9 月 22 日)。*趨勢科技資訊安全新聞*。「跟著資料循線追查：解構資料外洩事件及破除迷思」(Follow the Data: Dissecting Data Breaches and Debunking Myths)。上次存取時間 2016 年 8 月 5 日：http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data

28. 趨勢科技。(2016 年 6 月 2 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「FastPOS 信用卡竊盜又快又輕鬆」(FastPOS: Quick and Easy Credit Card Theft)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-quick-and-easy-credit-card-theft/

29. Erika Mendoza 和 Jay Yaneza。(2016 年 2 月 25 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「FighterPOS PoS 惡意程式出現蠕蟲行為」(FighterPOS PoS Malware Gets Worm Routine)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-gets-worm-routine/

30. 趨勢科技。(2014 年 9 月 29 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Shellshock 相關的故事與材料摘要」(Summary of Shellshock-Related Stories and Materials)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-shellshock-related-stories-and-materials/

31. Cklaudioney Mesa。(2016 年 2 月 18 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「QAKBOT 東山在起：網路銀行威脅儘管遭到掃蕩，仍然屹立不搖」(QAKBOT Resurges: Despite Takedowns, Online Banking Threats Persist)。上次存取時間 2016 年 8 月 5 日：http://blog.trendmicro.com/trendlabs-security-intelligence/despite-arrests-and-takedowns-online-banking-threats-persist/

32. Deutsche Welle。(2016 年 2 月 10 日)。*DW.com*。「駭客挾持德國醫院的資料」(Hackers hold German hospital data hostage)。上次存取時間 2016 年 8 月 5 日： http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf

33. Alex Hern。(2016 年 3 月 16 日)。*The Guardian*。「New York Times 和 BBC 等大型網站出現勒索病毒惡意廣告」(Major sites including New York Times and BBC hit by 'ransomware' malvertising)。上次存取時間 2016 年 8 月 5 日：https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising

34. 趨勢科技。(2016 年 3 月 24 日)。*趨勢科技資訊安全新聞*。「Locky 勒索軟體變種使得美國肯德基州醫院進入『內部緊急狀態』」(Locky Ransomware Strain Led Kentucky Hospital to an "Internal State of Emergency")。上次存取時間 2016 年 8 月 5 日：http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/locky-ransomware-strain-led-kentucky-hospital-to-an-internal-state-of-emergency

35. Sean Gallagher。(2016 年 4 月 1 日)。*Ars Technica*。「馬里蘭州醫療集團遭人從內部散布勒索病毒」(Maryland hospital group hit by ransomware launched from within)。上次存取時間 2016 年 8 月 5 日：http://arstechnica.com/security/2016/03/maryland-hospital-group-hit-by-ransomware/

36. David Fitzpatrick 和 Drew Griffin。(2016 年 4 月 4 日)。*CNN Money*。「勒索病毒犯罪浪潮興起」('Ransomware' crime wave growing)。上次存取時間 2016 年 8 月 5 日：http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/

37. Kevin Townsend。(2016 年 5 月 3 日)。*SecurityWeek*。「密西根水電公司遭到勒索病毒攻擊」(Michigan Power and Water Utility Hit by Ransomware Attack)。上次存取時間 2016 年 8 月 5 日：http://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack

38. Darlene Townsend。(2016 年 5 月 11 日)。*Computerworld*。「勒索病毒攻擊眾議院，使得 Yahoo Mail 遭到封鎖」(Ransomware attacks on House of Representatives gets Yahoo Mail blocked)。上次存取時間 2016 年 8 月 5 日：http://www.computerworld.com/article/3068623/security/ransomware-attacks-on-house-of-representatives-gets-yahoo-mail-blocked.html

39. Ericka Chickowski。(2016 年 6 月 24 日)。*DarkReading*。「NASCAR 車隊嘗到勒索病毒的痛苦教訓」(NASCAR Race Team Learns Ransomware Lesson The Hard Way)。上次存取時間 2016 年 8 月 5 日：http://www.darkreading.com/attacks-breaches/nascar-race-team-learns-ransomware-lesson-the-hard-way/d/d-id/1326047

40. Phil Muncaster。(2016 年 6 月 27 日)。*Infosecurity*。「Nascar 車隊遭勒索病毒攻擊而癱瘓」(Nascar Team Crippled by Ransomware Attack)。上次存取時間 2016 年 8 月 5 日： http://www.infosecurity-magazine.com/news/nascar-team-crippled-by-ransomware/

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流世界。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。