2016 年全球威脅報告

無懼前行

製作呈獻

FORCEPOINT Security Labs™

FORCEPOINT
POWERED BY Raytheon

目錄

精華摘要

去年網路攻擊發生重大變化，威脅的面貌因而改觀。雖然受到密切監看，竊取資料的惡意軟體依舊常見，對您組織的資料而言，最大的威脅可能在於自主性強的現代員工。新近出現大批勒索軟體的攻擊者能躲過隱密的安全措施，宣稱已將您的資料加密並據以向您勒贖，此法已蔚為能快速取得獲利的途徑。攻擊者面臨新的反惡意軟體工具，將往昔的攻擊方法重新搬出，回頭利用登上桌面、負荷著巨集的 Microsoft® Office 檔案。趨勢上日漸改採取使用不一致控制的雲端運算技術，對安全性構成嚴重挑戰。同時在背景中有新的殭屍網路，考驗著安全業界究竟有多大能耐，可偵測及攔截對手的短期戰術及大方向的目標。

因此，優先重點放在告知決策者有關存在於廣大外界、全球及其網路內之這些攻擊的主要來龍去脈，以便能將大多數的時間與資源應用在最嚴重的威脅之上。為了忠實體現「無懼前行」此一格言，Forcepoint 的 Security Labs、特別調查 (SI) 團隊及 Office of the CSO (OoCSO) 團隊持續不斷釐清全球攻擊活動所形成的紛繁複雜的亂象，識別出影響最大的威脅和突破，並就每一步提出專業的指引。

Forcepoint **2016 年全球威脅報告**就目前影響最大的許多網路安全威脅作一明確細表，這些威脅對遭受波及組織的技術、營運與經營成本構成深遠影響。本報告的每一章節末，皆會以指引作結束，由 Forcepoint Security Labs 團隊提出對付所述威脅的最佳方法。

1. 內部威脅：惡意與意外

Forcepoint 與協力單位的研究（見第 5 頁）顯示，就內部活動而制訂政策和對特權憑證進行管理，是組織十分缺乏準備下的安全議題。足足有 30% 的安全努力依然聚焦在於邊界的防線[1]，所調查的組織中為內部威脅專案特地編列預算的不到 40%[2]。然而，許多員工具有權限可進行遠端連線，不時進出網路存取伺服器內的資料（也就是您最敏感的資料所在之處）已成工作中的常態。

2. 進階威脅與特別調查團隊的個案研究：揭露「JAKU」與破解勒索軟體

對於進階威脅，Forcepoint 的特別調查團隊能提供數一數二的清楚視野，這是由專精於揭發威脅的獨特工具、戰術及程序（TTP）的威脅研究專家與事故因應專家所組成的菁英團隊。SI 團隊去年取得的主要工作成績包括發現名為 JAKU 的新殭屍網路活動，及破解名為 Locky 的頑固勒索軟體品種。

3. WEB 與電子郵件：雙管齊下的威脅

員工哪怕處於限制再多、安全防範再森嚴的工作環境，若無 Web 和電子郵件一般並無法發揮生產力，使得這類媒介成為傳送惡意承載內容（充滿惡意軟體的網站連結和惡意電子郵件附件）的理想途徑。目前不受歡迎的（例如，垃圾、惡意）電子郵件將近 92% 含有 URL，電子郵件中有惡意巨集存在者升高 44.7%（見第 20 頁）。

4. 移轉至雲端之舉仍籠罩在安全疑慮中

雲端技術的成本、擴充性及可使用性，讓許多企業暫且忘卻其安全疑慮，但在許多考慮轉為雲端技術者的眼中，雲端供應商與其本身環境之間的安全控制如此地不一致，造成資料保護上令人亂了陣腳，安全成為一大難題。有些諷刺的是，資訊長 (CIO) 與資訊安全長 (CISO) 即使延宕採行雲端技術，卻仍由於員工為了個人生產力與便利，自行決定使用偏好的雲端應用程式，不由自主地身陷安全泥沼中。接受調查的決策者中超過 80% 感受到「影子」IT 將帶來嚴重後果[3]。

5. FORCEPOINT 的 OFFICE OF THE CSO 所具備的思維

2015 年，Forcepoint 的 Office of the CSO 團隊將合併與收購 (M&A) 活動視為橫跨產業區塊的一大網路安全風險觸發因素。實際案例中，OoCSO 拿出自己在於網路安全與資料保護身為領導者的專業，點出創造 Forcepoint 本身的 M&A 活動，亦即前 Websense® 與 Raytheon Cyber Products (RCP) 公司以及 Stonesoft® 新一代防火牆 (NGFW) 事業體的整合時，於過程中管理全面安全控制的方式。

FORCEPOINT 的成立

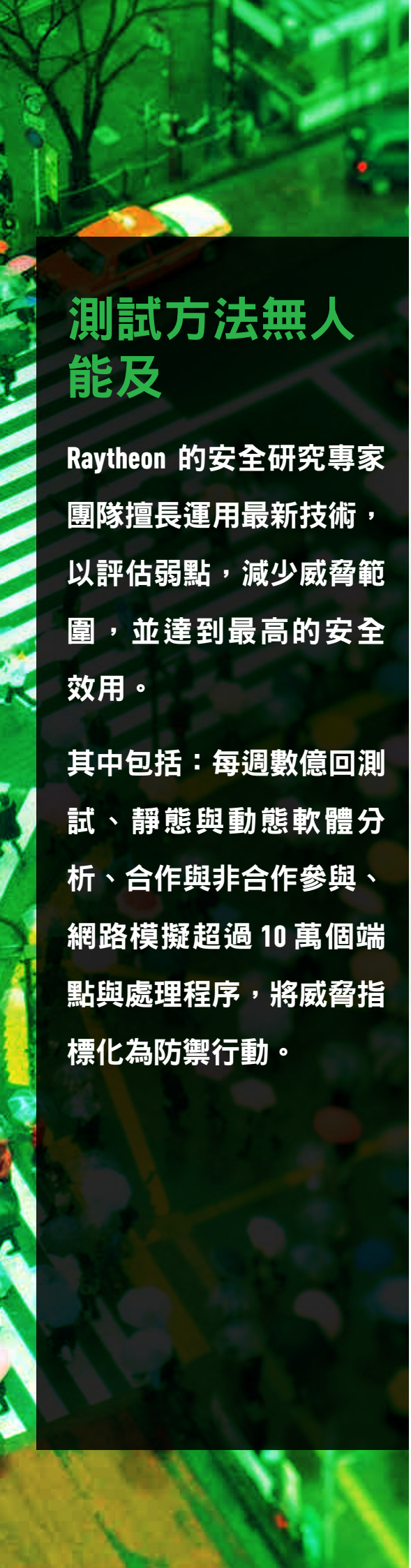
Forcepoint 這家為網路安全帶來新作法的新公司，於 2016 年 1 月 14 日開張。為 Raytheon Company 與 Vista Equity Partners 所成立合資企業的 Forcepoint 結合三家成功的企業：Websense、Raytheon Cyber Products 及 Stonesoft，各有其豐富的創新歷史。屬於合資企業的 Forcepoint 握有強大資產能輔助客戶維持安全，接續取用 Raytheon 廣大的資源、智慧財產與網路專業，以解決網路的最大難題。於本報告中，我們會不時舉出「由 Raytheon 提供」的方法，這些方法能夠給 Forcepoint 與客戶在應對現今充滿挑戰的資訊環境時提供重要且無人能及的優勢。

內部威脅

內部威脅是指自組織內部來源發起或得到合作（無論刻意與否）的攻擊。攻擊者相中以組織內部人士作為目標，或者經由商業合作夥伴和協力供應商，操弄員工，誘使其揭露自己的憑證，於是得以在網路中進行存取。罪犯持竊得的憑證可在網路之間移動，存取甚至移除敏感資料，往往到有人注意時為時已晚。內部威脅造成的入侵案例持續攀升，以內部人士意外之下發生的情形為最大的問題起源。Forrester 所調查於 2015 年經歷過入侵事件的企業中，內部事故為最大成因，其中超過 50% 是由於不慎誤用或使用者出錯[4]，稱為「意外內部人員」。

意外內部人員的範例：

- 員工點按電子郵件中可疑的連結，不知情之下將惡意代碼下載至所用的機器。
- 員工使用「撿到的」USB 隨身碟（Idaho National Laboratory 一項研究揭露，撿到 USB 隨身碟的員工有 20% 會將其插入工作用的電腦[5]）。
- 員工遺失內有專屬資訊的筆記型電腦、平板電腦或儲存裝置。
- 員工忽視安全政策，將工作帶回家於下班時間使用。



測試方法無人能及

Raytheon 的安全研究專家團隊擅長運用最新技術，以評估弱點，減少威脅範圍，並達到最高的安全效用。

其中包括：每週數億回測試、靜態與動態軟體分析、合作與非合作參與、網路模擬超過 10 萬個端點與處理程序，將威脅指標化為防禦行動。

根據 Forcepoint 贊助 Ponemon Institute 所作的研究[6]，員工之所以成為公司安全的最大威脅，主因在於內部濫用難以發現。例如，用來取得合法使用者平常所能夠存取之敏感資料的，往往是從有效使用者帳號盜取的憑證，特別能夠規避引發警訊。一項 2016 年 3 月的調查[7] 亦作此呼應；其中發現，察覺惡意內部活動或具權限的使用者憑證遭駭客劫持，是銀行最無防備的主要領域。以個人裝置（稱為自備裝置，簡稱 BYOD）執行業務的風氣日益盛行，這使得內部威脅更加複雜，給駭客更多管道取得立足點而不在安全團隊的雷達中現跡。於是，組織不斷地在存取資料與資料遭竊或誤用的風險之間求取平衡。

往往導致不慎損失重要資料的脆弱環節在於使用者對於資料處理不當，因為不知該如何運用有效的安全措施或不小心。

2015 年資料侵害事故中，員工錯誤／疏忽將近佔 15%[8]

... 既然只有略過半數的員工知道公司的安全政策，原因不難推測[9]。

儘管損失越來越大（驗證憑證、智慧財產、企業財務資料，及個人識別資訊（PII）最常因而失守），組織仍繼續以效果不彰的方式教育員工，員工也依舊不知如何在工作上施行良好的安全措施[10]。既然內部威脅是清楚又存在的危險，為何邊界防禦仍比內部威脅專案更為優先？

Ponemon 近期的一項研究[11] 提出了一些洞見。雖然是已公認的問題，但受訪組織之中不到 40% 對內部威脅專案設立專用預算。此表示企業組織欠缺脈絡資訊，加上有大量的誤判且能見度不足，大多數是倚賴並不適合解決此問題的現有工具。更精湛的技術，結合資料外洩防護 (DLP) 與使用者行為分析工具，與其他 IT 和商業系統活動（例如 RFID 存取記錄和 IP 記錄）建立交互關聯，現正演進為可判定威脅出自真正內部人士或是偽裝者以竊得的憑證所為。

然而，內部威脅並不只是「IT」問題，必定也涉及人事。
高效的內部威脅專案應能結合技術控管、風險管理計劃與員工最佳實務訓練。成功的內部威脅專案所應具備的重要條件包括：

- **政策**：佈達政策，指出組織內應用技術的方式該如何，從說明適當的裝置為何，到資料的經手以及網際網路的使用皆包括在內。
- **流程**：將適當的職務隔離，與其他檢查點套用至流程中。
- **技術控管**：依照最低權限原則，根據各人個別被指派的角色而限制存取權限。
- **風險管理**：識別並發展風險管理計劃，對風險最高的面向執行最高優先管控措施。
- **稽核與監看**：確認各關鍵部分皆有效果，並且符合組織需要。

內部威脅個案研究：資料與縮編

依照 Forrester 安全調查[13] 指出，過去 12 個月的入侵案中有 39% 肇因於內部事故。其中 26% 是由於刻意濫用或惡意，56% 起因於不慎誤用資料（18% 為兩者結合）。

以下 Forcepoint 個案研究於此首度分享，舉例說明典型的內部威脅情境。經過合併與收購 (M&A) 活動之後，客戶展開軟體工程人員縮編流程。其中告知員工即將遭到遣散，部分即刻生效，其餘則待目前的專案完成。慷慨的全套遣散待遇，包括全年薪資，依照公司內部留有的智慧財產與資產條件來發放。讓人驚訝的是，仍有大量的工程師返回桌面，開始試圖竊取機密資料。組織對此情境有所準備，運用 Forcepoint 的「SureView® 內部威脅」技術觀察高風險員工的行為（依照 30 天典型日常行為所測得）。結果不尋常的作業，企圖將檔案複製並儲存到 USB 儲存裝置或電子郵件檔案，及透過 Web 通道將原始程式碼往外送到雲端儲存空間，於 Forcepoint 技術之下立即現形。「SureView 內部威脅」除能阻止入侵之外，更重要的是，公司能夠識別違反資遣協議企圖竊取資料的員工，保護最珍貴的智慧財產。雖然這個特定案例示範的是惡意的內部人員，但意外的內部人員（其憑證遭竊或電腦被劫持）也同樣能因為不尋常的網路移動、下班時存取或傳輸資料，而輕易觸發相同的警示。

FORCEPOINT 的指引

1. 瞭解您組織的具體風險何在，並知道原因。莫遲疑，建立起標準使用者行為的基本界線。瞭解使用者的歷史行為，是發現可能為內部威脅異常的必要步驟。
2. 透過認知安全風險訓練及教育方式，賦與使用者權力，以主動解除風險。
3. 制訂內部資安事故的因應計劃，建立一套內部資安事件的辨別、溝通管道及往上呈報的正式處理流程。
4. 考慮投資採用提供精密的行為分析和長期追蹤的解決方案，以迅速識別可導致或意味入侵破壞的使用者行為。藉由及早辨識有風險的使用者，可於威脅入侵前事先或開始後不久，即加以遏止。

進階威脅

特別調查團隊的個案研究

IT 規模與複雜度巨幅增加，使得何謂「進階威脅」的傳統觀點迅速過時。隨著傳統邊界瓦解，資料散佈於端點、網路、行動與雲端中，組織目前面臨影響擴大的「彙整威脅」。面對這類新的複雜問題，需要有創新的作法，而能夠分享威脅情資及縮短威脅潛伏時間的整合解決方案，已日益章顯出其重要性[14]。

威脅潛伏時間自攻擊者進入網路起計，持續至離開或強制退出為止。將潛伏時間縮到最短可降低攻擊者達成內部橫向擴散及移除重要資料的機會。

這類新的進階攻擊是 Forcepoint 特別調查團隊重視的焦點，該團隊在安全漏洞出現攻擊工具、戰術與流程 (TTP) 超出正常範圍時，就會投入工作。SI 團隊的整合技能與知識，涵蓋反向工程、進階攻擊分析及藉由與執法機關合作，有效抵消對躲避偵測惡意程式的中和作業。

SI 團隊也從已知的攻擊資料取得參考點，深入探究許多層次，以瞭解新的 TTP 和建立緩解技術。此方式即被運用來分析該首度描述的 JAKU — 一種新近被辨認出的全球殭屍網路活動。

JAKU 簡介

JAKU 是一種持續的全球殭屍網路活動。其展現出基礎架構及 TTP 的再利用，並且表現出分裂的個性。JAKU 群聚大批受害者，透過執行作業活動，對特定受害者進行具高度針對性的攻擊。結果形成機器資訊的資料外洩、建立使用者檔案，及併入更大的攻擊資料庫裡。

經 Forcepoint Security Labs 進行六個月的調查，已能全球性地精確描繪出指揮控制伺服器與受害者的位置。透過靜態行為分析，Security Labs 團隊已能瞭解此殭屍網路所用的攻擊元件以及追蹤機制。他們於研究中的調查全程皆與各執法機構協調進行，現已來到能公開分享洞見的階段。Forcepoint 的客戶早在此調查於 2015 年 10 月展開之前即已受到保護，免除 JAKU 構成的威脅。

「可謂顯著的變化是一場活動之內同時執行若干作業，以幾乎相同的 TTP 群聚數千個受害者，同時執行目標鎖定的作業。」

– Forcepoint 首席科學家 Richard Ford 博士談 JAKU

平均潛伏時間：93 天

最長潛伏時間：348 天

前五大 JAKU 受害國家／地區統計

JAKU
事實與數據

調查至今所花的時間：

6 個月

受害者位置：

全球

（明顯聚集於日本、南韓與中國）

承載內容的遞送是透過：

暴露於受害的 BITTORRENT 網站、使用未經授權的軟體及下載盜版軟體

所用的躲避偵測技術：

密碼編譯、圖像隱碼術、假檔案類型、隱身導入、反病毒引擎偵測（及其他）

指揮控制伺服器的位置：

馬來西亞、泰國及新加坡

受害者數目：
19k

惡意程式類型：
多階段追蹤及資料滲出惡意軟體

有 JAKU 受害者的國家數目
134

JAKU 相關常見問答

JAKU 的完整技術分析何時能公諸於世？

分享所有已知入侵指標 (IOC) 的完整技術撰述，將於 2016 年 5 月 4 日在 Security Labs 部落格發佈。

此研究有安全業界的哪些其他成員參與？

Forcepoint 特此褒揚 Kaspersky 於 Dark Hotel 活動的分析中下了十足的功夫，同時英國國家犯罪調查局 (NCA)、CERT-UK、Europol 及 Interpol 也於此調查惠予合作協助。對於資訊收集、比較及分析，唯有採取協同方式，網際網路方能成為更安全的場地，供人們執行業務，過著現代生活。

FORCEPOINT 的指引

1. 在組織內建立程序，以縮短可能的潛伏時間[15]。
2. 限制、甚或避免接觸 Torrent 網站及非法軟體。
3. 監看不尋常的活動，例如送往指揮控制伺服器、已知的威脅情資系統的流量。

不容忽視的力量

「DEEPRED」是 RAYTHEON 工程師與 FORCEPOINT 電腦專家組成的團隊，目前正參加美國國防高等研究計劃署的「網路大挑戰」，建立能夠尋找軟體安全瑕疵並立即加以修正的電腦程式。DEEPRED 將於 2016 年 8 月在拉斯維加斯的駭客大會 DEF CON 爭奪 2 百萬美元獎項。

對勒索軟體作出反擊：
LOCKY 概覽

將您的檔案加密，接著向您出售加密金鑰，以供擷取檔案的惡意程式，便得到勒索軟體這個名號。若資料主無法擷取檔案，勒索軟體便等同於是摧毀資料的元兇。

去年當中，勒索軟體變得十分常見。Forcepoint Security Labs 已開始追蹤勒索軟體技術的發展，此軟體經常透過惡意電子郵件的附加檔案或惡意廣告傳送，已行之有年。

經過新聞披露一間醫院[16] 就造成服務停擺的攻擊支付贖金，SI 團隊便展開調查，研究如何防範檔案遭到加密，並與更廣大的社群分享這套知識。

FORCEPOINT 能將 LOCKY 解鎖：
將網域產生演算法實施反向工程

Forcepoint 能為客戶提供保護，防範用以散播 Locky 承載內容的誘餌（附帶內含惡意巨集之 Microsoft Office 文件檔案的惡意電子郵件），Forcepoint Security Labs 亦已能將檔案加密程序停用。

Locky 採取 128 位元 AES 加密，能將 SQL 資料庫、原始程式碼、比特幣錢包及其他檔案等進行加密。我們「威脅防護雲端安全」（行為檔案沙箱）中承載內容分析模組，能識別出對已知指揮控制伺服器的明顯呼叫。

可惜的是，Locky 運用「網域產生演算法」，能基於時間戳記和種子數值產生一組不同的網址。因此，有可能未進一步調查之下，不盡然能得知所有網址。Security Labs 的第一次分析顯示，Locky 每日與多達六個網址通訊。

Forcepoint Security Labs 將 Locky 勒索軟體的網域產生演算法 (DGA) 實施反向工程，並公開揭露，給防禦者機會作出反擊，並封鎖勒索軟體所接觸的網域存取[17]。藉由阻止勒索軟體存取已知的網址，並取得在某一特定日子所用的必備加密金鑰，讓檔案不受侵害。

五天之後，惡意程式作者更改所用的 DGA，並更新種子數值。勒索軟體這時就能在某一特定日子與 14 個網域通訊。Forcepoint 再一次揭露該演算法，提供接下來連續30 天中所通訊的網域清單[18]。在繼續監看之下，Forcepoint 發現惡意程式作者於 23 天後再度改變戰術[19]。

部分企業訴諸付出費用，往往高達數千美元[20]，然支付贖款未必能確保檔案可恢復到能夠存取的狀態。

部分勒索軟體的變種，例如 CTB-Locker 無須與指揮控制伺服器 (C&C Server) 聯繫即可存取將檔案加密所需的金鑰，導致防禦者少一個機會能干擾此摧毀資料的事故。因此 Forcepoint 全力在惡意軟體的威脅生命週期早期階段加以攔截，尤其在「引誘」階段（指網路罪犯建立看似無害的電子郵件或其他誘餌，愚弄使用者去按下通往受害網站的連結[22]）。

勒索軟體目前也在順應目標當地語言進行自我調整[23]，或是反其道而行，刻意避免感染特定區域的使用者[24]。惡意程式作者可能會藉由此法去避開他們攻擊地執法單位的注意，或是針對較可能支付高額贖金的國家和經濟體進行攻擊。

勒索軟體常見問答

檔案受感染後，勒索軟體將之加密的速度有多快？

*立即；*一旦能連線到它的指揮控制處時。

勒索軟體只要列舉所有磁碟，搜尋其目標檔案類型（依照副檔名），便會開始加密。

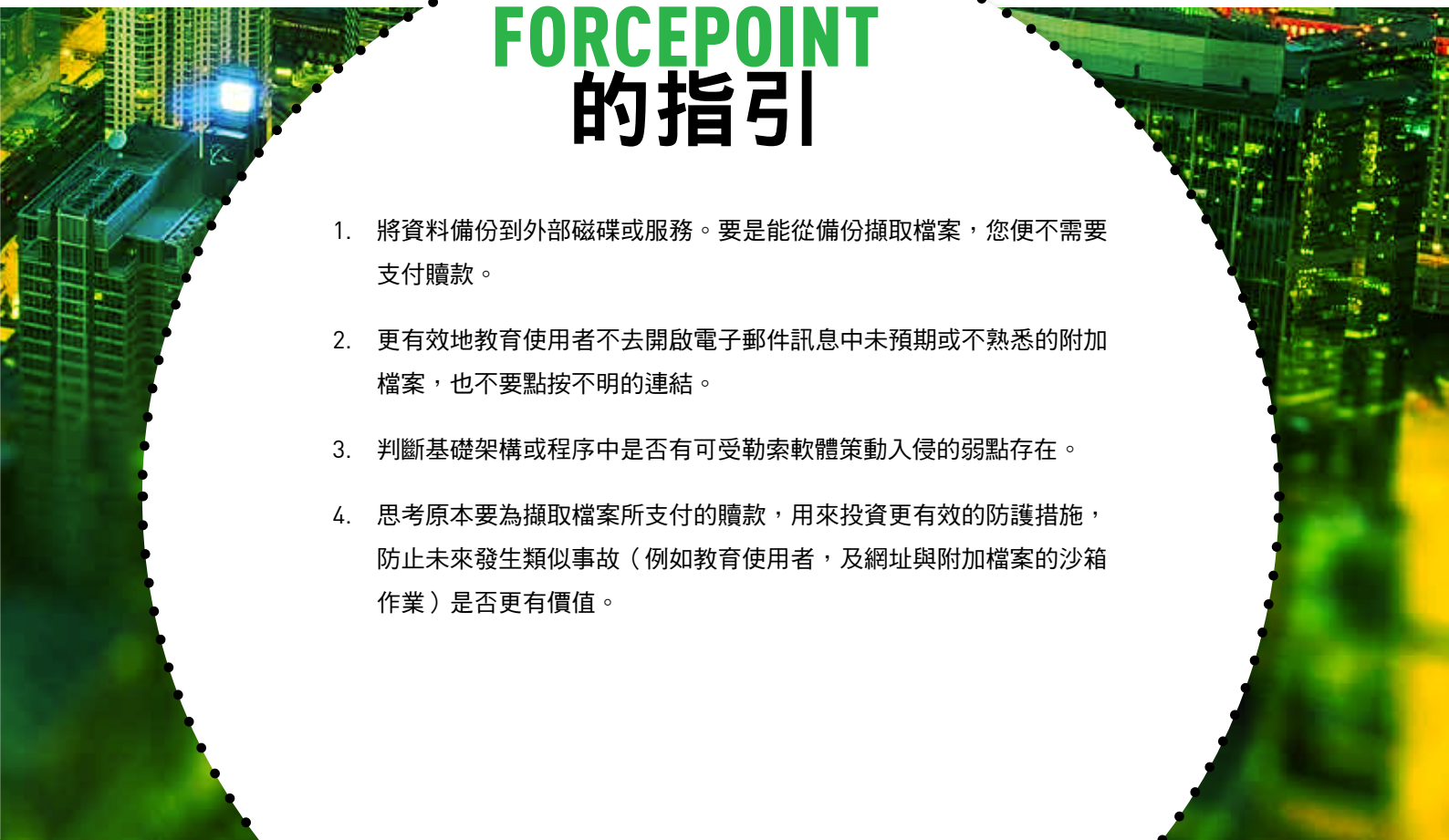
值得注意的是，部分勒索軟體不需連線到指揮控制處即可開始加密，那是因為能夠自行產生金鑰，而只要加密程序完成，金鑰資訊就會傳回指揮控制處。CTB-Locker 便是不需連線到指揮控制處的例子。

付款給勒索軟體之後，有多大機會能取回檔案？

惡意程式作者有釋出檔案的動機，以便鼓勵未來的受害者付款。然而，若儲存金鑰資訊的指揮控制伺服器被去除，則即使付過贖款，仍無法將檔案解密。

勒索軟體採用哪些加密演算法？

部分勒索軟體變種採取對稱演算法，例如 AES-256 (Teslacrypt)，有些使用公開金鑰 RSA-2048（CryptoLocker、CryptoWall）。偶爾會見到勒索軟體使用自訂密碼編譯演算法。



FORCEPOINT 的指引

1. 將資料備份到外部磁碟或服務。要是能從備份擷取檔案，您便不需要支付贖款。
2. 更有效地教育使用者不去開啟電子郵件訊息中未預期或不熟悉的附加檔案，也不要點按不明的連結。
3. 判斷基礎架構或程序中是否有可受勒索軟體策動入侵的弱點存在。
4. 思考原本要為擷取檔案所支付的贖款，用來投資更有效的防護措施，防止未來發生類似事故（例如教育使用者，及網址與附加檔案的沙箱作業）是否更有價值。

曝光躲避偵測技術

新一代防火牆 (NGFW) 是用來控制使用者與應用程式，同時具備非常有效的攻擊辨識與減輕威脅的功能。與傳統防火牆相比有許多不同之處，其中就包括應用程式認知能力，能細膩地追蹤網路流量狀態。NGFW 也是提供網路能見度的絕佳工具。

採用的躲避偵測技術能略過解決方案的安全控制（攻擊者可能會併用數種技術，建立更難偵測的入侵方式）。這些是惡意程式作者直接因應當今最佳安全解決方案所能賦予安全管理員的能見度（包括 NGFW）而採取的戰術。

Forcepoint Security Labs 將躲避偵測技術應用的情境分為三類：進入通道（攻擊應用躲避偵測技術來通過網路防禦）；連出通道（攻擊承載內容應用躲避偵測技術來回傳）；或以躲避偵測技術來存取遭拒的資源（例如，藉由使用 TOR）。這些進階躲避偵測技術對任何組織的資料安全來說皆構成一大威脅。

現有的躲避偵測技術

進階躲避偵測技術結合多種現有躲避偵測方式，創造出新的未知躲避偵測方法，也是更成功的躲避偵測方式。已見惡意程式與漏洞攻擊作者搬出所有躲避偵測方法，操縱協定層次的串流，越過偵測。

- **IP 分割**

  IP 分段這種程序能將單一網際網路協定 (IP) 資料包分割成為多個較小的封包，為 RFC 791[25] 指定規格。

  IP 分割漏洞攻擊利用 IP 內的分割協定，將承載內容散佈至多個訊框，成為一種攻擊載體。

- **TCP 分割與亂序**

  傳輸控制協定 (TCP) 依 RFC 793[26] 所定義。其中以序列號碼能將可亂序接收的分段正確地排序。

  TCP 分割與亂序攻擊利用 TCP 的此功能來粉飾攻擊。

- **TCP URG 指標**

  也依 RFC 793 指定的還有 TCP 緊急指標欄位 (URG)。這個指標能夠指出緊急或頻帶外的資料存在，若在承載內容分析過程將之納入，能使惡意或漏洞攻擊程式碼避過偵測。

前五大 2016 年躲避偵測技術用法預測

1. 略過存取控制
以存取原應無權限的網路

2. 攻擊水坑
以無法追蹤的方式與水坑通訊不會引發尋常的警示，避免網路安全團隊預期應作的因應

3. 殭屍網路指揮控制 (C&C)
偽裝指揮控制處的來回流量能增強靈活性，維持殭屍網路的執行時間

4. 漏洞攻擊（遞送與執行）
推送原應輕易偵測得到的漏洞攻擊，以達到程式碼執行的目的

5. 滲出資料
防火牆無法偵測的流量可用來隱藏資料被竊的傳輸動作

FORCEPOINT 的指引

1. 務必配置適當技術，能識別並減緩躲避偵測技術的使用。
2. 確認全盤瞭解在威脅殺傷鍊階段中的躲避偵測技術。若在威脅生命週期的任何階段的能見度降低或不足時，則啟用最弱環節準則。

WEB 與電子郵件
雙管齊下的威脅

Web 與電子郵件是目前的主要通訊管道，也依然是網路罪犯的主要攻擊載體。廣為人知是對組織進行針對性攻擊的初步進入點，電子郵件攻擊的載體於 2015 年遞送惡意承載內容進入組織，並以 Office 文件和壓縮檔為主軸。Forcepoint Security Labs 發現，電子郵件中的惡意內容與 2014 年相較增加了 250%。Dridex[27]（一種銀行惡意程式病株）及各種勒索軟體[28] 等活動，是此數據攀升的罪魁禍首。電子郵件內的惡意程式或惡意 Web 連結，能利用弱點侵害機器，最終經由網際網路入侵至企業的全網路。電子郵件與 Web 攻擊載體於 2015 年有顯著聚集在一起的現象，不受歡迎的電子郵件裡十個中有九個內含網址。依照 Identity Theft Resource Center 的「2015 年資料外洩」報告[29]，意外電子郵件／網際網路暴露是 2015 年第三常見的資料受害成因，可見瞭解攻擊者是如何橫跨這兩種載體來進行的威脅分析，十分重要。

- **91.7%** 的不受歡迎電子郵件含有網址。
- **2.34%** 的不受歡迎電子郵件含有附加檔案。
- 電子郵件附加檔案中的惡意巨集攀升 **44.7%**，不肖份子以巨集傳送裝載於 Web 的進一步承載內容。
- **68.4%** 的電子郵件是垃圾郵件（自 2014 年的 88.5% 下降）。

Forcepoint 的資料指出嵌入 Microsoft Office 檔案類型的惡意巨集，是 2015 年的重大攻擊傳送時的機制。去年的威脅報告[30] 揭露，於 2014 年底的三十天期間觀察到三百萬個惡意巨集。於 2015 年底期間實施類似的取樣作法，Forcepoint 發現超過四百萬個巨集，較 2014 年攀升 44.7%。

前五大電子郵件附加檔案的惡意檔案類型

1. ZIP 封存
2. SDOS/WINDOWS 程式
3. 文字檔型式
4. MICROSOFT WORD 97
5. MHT 格式

裝載惡意內容的前十大國家

1. 美國
2. 義大利
3. 德國
4. 俄羅斯
5. 土耳其
6. 愛爾蘭
7. 英國
8. 法國
9. 荷蘭
10. 印尼

裝載著網路釣魚網站的前八大國家

1. 美國*
2. 貝里斯
3. 香港
4. 比利時
5. 英國
6. 智利
7. 德國
8. 瑞典

*於美國裝載的網路釣魚網站比其餘前 8 國更多

FORCEPOINT 的指引

1. 探索可以兼顧分析 Web 與電子郵件攻擊兩者載體的安全解決方案，可使各產品的效用發揮至更大。
2. 實施使用者教育／訓練專案，定期提醒使用者有哪些典型的方式可識別惡意電子郵件，其中有附加檔案或網址，可能會觸發 Web 連線，帶入更多承載內容。
3. 考慮啟動網址沙箱作業與附加檔案沙箱作業技術，以防使用者作出錯誤決定，或未能認出惡意電子郵件。

移轉為雲端技術

有更多公司因為成本節省和協同合作而採行雲端技術。雲端運算技術雖然仍為成長中的市場，但因其具備可以減少硬體與支援需求，為員工賦予靈活性和速度以利他們完成重要商業任務等優點，移轉作業已逐步且穩定地在進行。Harvard Business Review Analytic Services 的一項全球分析中[31]，答覆者有 85% 表示其組織將於接下來的三年期間，將會中度至廣泛地使用雲端應用的工具。

雖然對於企業使命帶來多方面的優勢，部分組織卻放緩採用雲端 IT技術，因疑慮雲端應用的項目可能在安全保護的效果不彰，或可能與法規要求有所衝突而裹足不前。超過 60% 的組織指出「安全疑慮」為延緩採行雲端技術的最重要理由[32]。依照 Ponemon 的研究[33]，對於雲端應用程式與產品難以強制實施高效的安全方法，以及雲端的資料安全未確立究竟應由使用者還是雲端供應商負責，是引發疑慮的因素。

然而，抗拒採行雲端技術恐怕無法延緩其受人使用。員工、團體甚至所有的分部單位，經常不顧公司尚未採用而逕自移轉到雲端，當遇到外部解決方案更能達到生產力的要求時，便會略過核准或正式的整合作業。如此一來，便有可能容許未批准的技術擾亂組織的安全和法規遵循的規範，讓企業暴露在不想要且計劃外的風險之中。

影子 IT

非您想要的雲端技術

- **只有 8%** 的公司知道影子 IT 在組織內的範圍
- **71%** 對於影子 IT 有些許至極深的疑慮*

*「雲端技術採行實務與優先順序調查報告」，2015 年 1 月，雲端安全聯盟

超過 80% 的 IT 決策者覺得影子 IT 對 IT 安全蒙上風險，其中三分之一視為極顯著的風險，16% 認為這是最顯著的風險[34]。然而，使用影子 IT 者只有 34% 相信這對安全構成風險，其中超過半數指出此方式能提高業務部門的生產力[35]。可惜的是，若 IT 見不到資料，也無法充分加以保護，於是形成資料外洩或遭竊的完美環境。

IDG Enterprise 一項調查[36] 發現，CIO 們相信 2016 年會是 IT 服務採行雲端技術上線比常駐於本機更多的第一年。涵蓋所有運算平台與系統，以資料為中心的安全與隱私解決方案，是符合安全與隱私規範的關鍵。除了有資料認知能力的防禦功能之外，第三方獨立評鑑，例如 CSA STAR Certification[37]，有助於判定雲端服務供應商的安全性。

FORCEPOINT 的指引

1. 資料外洩防護 (DLP) 解決方案與新一代防火牆 (NGFW) 能協助組織體認其影子 IT 的範圍。
2. 一旦得知使用者正連線到哪些服務與 IT 實體，組織即可以落實資料保護與使用的指導原則，訓練使用者，或可根據安全政策停用此 IT實體。
3. 員工往往利用影子 IT 跳脫思考與工作的框架。而管制過多可能會導致使用者受到挫折，嘗試略過限制。因此建議可考慮與員工一同工作，協助提高其生產力，而非全盤扼殺他們創新的企圖。

需要網路人才

眼見資料持續移動，逐漸遠離邊界的防禦，培育網路安全人力陣容，是保護資訊免受網路威脅的重要任務。Raytheon 的年度研究「保障我們的未來：弭平網路人才斷層」[38] 與美國國家網路安全聯盟合作之下，在長期共同打造強健的人才培育搖籃之餘，也努力找出網路人才之所以出現斷層的根本原因。

THE OFFICE OF THE CSO 的思維

新事業體的收購與合併活動趨勢上升，但整合公司的過程，會使保護組織敏感資料的複雜度提高。鑑於標準普爾 (S&P) 500 大企業中，目前已有 84% 的企業是由智慧財產 (IP) 與其他無形資產所構成[39]，讓資料可供適當人士存取，而在資料被存取時，保護資料免於外洩、遭竊和誤用實屬必要之事。保護敏感資料，維持競爭優勢所需的技術與商業流程，是合併、收購和其他企業所主張的既定項目。IP 或其他資料外洩對聲譽有立即影響，能導致法律與監管行動，不利於競爭地位、股價和股東價值。原獨立組織要能成功整合，建立藍圖以保護重要資料的合併與管理，已為不可或缺的工作。

FORCEPOINT 的成立：網路安全組織如何安然整合

2016 年 1 月 14 日，Websense、Raytheon Cyber Products 與 Stonesoft NGFW 事業體整合，宣告成立新的合資企業。這家新公司名為 Forcepoint，是經過將近一年的商業系統整合而得到的碩果。

評估

在Websense、RCP 與 Stonesoft 開始整合任何資料、系統或程序之前，必須先評估每家公司內外的安全情勢。由第三方來執行穿透測試，挖掘出網路暗處以尋找出安全弱點的相關通訊私語，或公司不曾知情的持續入侵行動。此外也要求負責資安的員工詳細列表其安全專案，包括使用者教育、弱點管理、資料分類與流量，以及存取控制的管理等。這番安全盡職的查核，證實資安政策確實有在施行，也凸顯可能的相異之處，例如這家組織的資安要求較嚴，其餘組織必須跟進。

評量

我們本身的安全評估完成之後，也就開始評估即將合併各實體的網路有哪些威脅。此實例中配置了自訂工具，以偵測及報告可疑的活動，也評鑑網路健全度，以便發展安全的指引。此指引往往簡單到修補伺服器或更新憑證。

「瞭解哪些資料集對合併後的公司而言是重要的，並找出資料的所在位置，以及了解有哪些加以保護的控制在實施，讓我們能更清楚地看出所需處理的風險何在。」

-DAVE BARTON
FORCEPOINT CISO

同時，RCP 與 Websense 的「明星資產」（IP、財務資料等）經過認定，亦發展妥善溝通以對抗公司整併時常見的目標針對性威脅與惡意活動（例如垃圾郵件和網路釣魚攻擊）。Forcepoint 收到看似（但並非）Raytheon 所發的合法電子郵件，其中索取敏感資料和財務資訊，所幸積極的安全措施已經到位，並未淪為這些惡意入侵的受害者。

行動

宣佈日未到之前，新合併實體的所有原始程式碼接受靜態與動態程式碼測試。此舉是為了判定未曾知曉或揭露的程式碼弱點。

宣佈日

網路可能尚未相互連接或可直接通訊，但仍有一些步驟要採行，以確保接下來數個月的整合工作能夠順利進行。首先是與全體員工溝通資料存取政策事宜，尤其關於過渡時期如何處理關鍵或敏感資料。員工也需要瞭解專屬計價模式和其他競爭資訊，於收購未正式完成之前不可向人透露。如此主動積極的先與使用者溝通，是於合併與收購 (M&A) 過程中保護資產與資訊的關鍵。

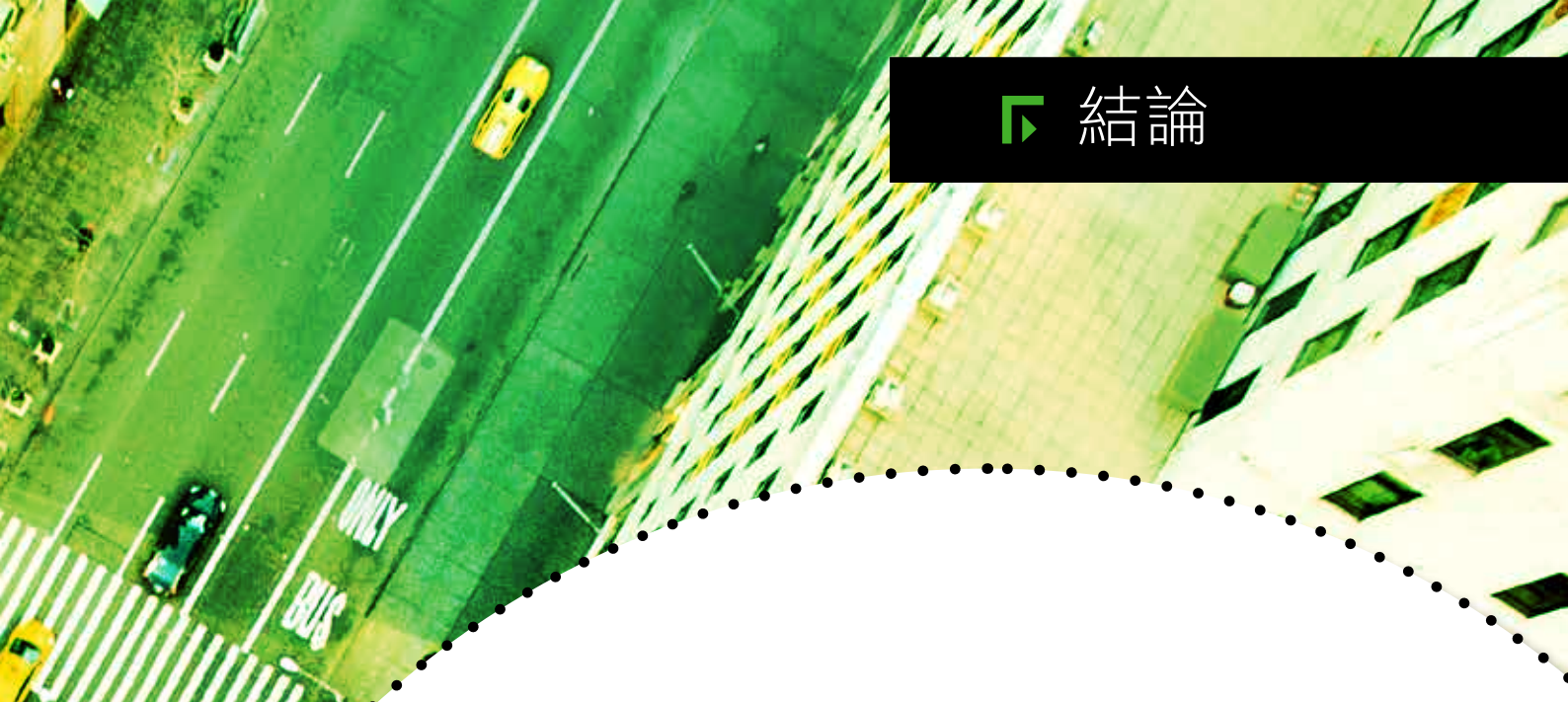
新一層次的壓力測試

Raytheon 的 Development and Evaluation (CODE) Center 開發與評量中心下的 Cyber Operations 是頂級的網路場地，用以測試現行與未來的關鍵任務系統抵禦網路攻擊的能力。CODE Center 為 Raytheon 的網際創新與全球展示中心網路之部分，該網路是協助客戶迅速確定能克服其最困難及最複雜之網路挑戰的解決方案。

第二是著手增加公司網路的監視，採用的資料防竊工具聚焦於管理員帳號的使用以及嘗試透過電子郵件或網際網路傳送敏感資料的舉動。威脅警示出現時，IT、安全及開發團隊便開始矯正所識別的威脅和弱點。如此一來，若還有任何問題，或安全政策有所差距，可在網路連接之前先行修正。

絕非全然簡單的流程中，Forcepoint 的整合比大多數情況更加複雜。Websense 與 RCP 合資企業即將完成的同時，我們收購了 Stonesoft，為了確保整合順暢安全而重新審核採取過的許多相同步驟。此外，轉為新品牌識別時，需要 IT 將員工、其工作站和資料移至新網域，即 Forcepoint.com。這些作為全是為了防止正式宣佈新公司之前，新品牌與名稱洩漏風聲。達成的方式是佈署我們自有的工具，設下限制，使得含有新名稱與其他品牌資訊的資料無法被分享到內部網路以外的地方。即使可能有這些絆腳石，但事先的規劃與工作卻能使整合飛快繼續，合併完成之前小挑戰已經被矯正且減輕。

凡是 M&A 活動，免不了涉及安全。合併過程可能出現的風險太多，若沒有安全專家的重要參與將無以發現這些風險。



結論

Forcepoint 2016 年全球威脅報告證實，過去這一年當中，攻擊的性質發生明顯轉變。網路安全經常是技術辯論、警示與「IT」問題的領域，如今終究成為最高且主流的風險，也是各地企業主管、表決選出的官員、政府機關和領導人所要面對的重要議題。

投機取巧的勒索軟體之徒、不小心的員工或構思完善的進階攻擊行為，能迅速帶來險惡的衝擊，部分案例更威脅組織財務的穩定、達成使命的能力與無價的品牌。不過，並非所有攻擊都存在威脅，於此年代，只要是與網際網路連線的辦公室或物件，都可能隨時遭受攻擊的砲轟。

我們相信需要有新的全面方針，好讓企業擁有 360 度視野與即時分析能力，獲得有意義的警示，能夠預見與溝通威脅版圖及箇中的影響，使客戶得以迅速採取行動，哪怕對手再頑強也能夠將之擊敗。Forcepoint 的 Security Labs、特別調查及 Office of the CSO 團隊等人，將繼續投入他們的專業能力，來辨識出全球的威脅和攻擊活動。一路上有指引伴隨，我們可以攜手***無懼前行***。

引用參考

1. Ponemon Institute LLC. " 2015 Cost of Cyber Crime Study: Global." October 2015. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

2. Ponemon Institute LLC. "Privileged User Abuse & The Insider Threat." May 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

3. Anderson, Ed; Nag, Sid, and Gartner, Inc. "Forecast Overview: Public Cloud Services, Worldwide, 2016 Update." February 17, 2016. https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srcId=1-3478922254

4. Shey, Heidi. "Understand The State Of Data Security And Privacy: 2015 To 2016." Forrester Research, Inc., 8 Jan. 2016. https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2015+To+2016/-/E-RES117447

5. Mearian, Lucas. "Government Tests Show Security's People Problem." Computerworld. July 6, 2011. http://www.computerworld.com/article/2510014/security0/government-tests-show-security-s-people-problem.html

6. Ponemon Institute LLC. "Ponemon Study: The Unintentional Insider Risk in United States and German Organizations." July 30, 2015. http://www.raytheoncyber.com/spotlight/ponemon/index.html

7. Bank Director. "Bank Director's 2016 Risk Practices Survey." March 21, 2016. http://www.bankdirector.com/download_file/view_inline/4996

8. Identity Theft Resource Center. "2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog." January 25, 2016. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

9. Forrester Research, Inc. "Global Business Technographics® Security Survey, 2015." July 2015. https://www.forrester.com/Global Business Technographics Security Survey 2015/-/E-sus2957

10. Forrester Research, Inc. " Global Business Technographics® Devices And Security Workforce Survey, 2015." August 2015. https://www.forrester.com/Global+Business+Technographics+Devices+And+Security+Workforce+Survey+2015/-/E-sus2971

11. Ponemon Institute LLC. "Privileged User Abuse & The Insider Threat." May 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

12. Litan, Avivah, and Gartner, Inc. "Best Practices and Success Stories for User Behavior Analytics." March 4, 2015. https://www.gartner.com/doc/2998124/best-practices-success-stories-user

13. Forrester Research, Inc. "Global Business Technographics® Security Survey, 2015." July 2015. https://www.forrester.com/Global Business Technographics Security Survey 2015/-/E-sus2957

14. Forcepoint LLC. "Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT." https://www.forcepoint.com/resources/white-papers/cyber-dwell-time-and-lateral-movement

15. Forcepoint LLC. "Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT." https://www.forcepoint.com/resources/white-papers/cyber-dwell-time-and-lateral-movement

16. Vanian, Jonathan. "Hollywood Hospital Pays Off Hackers To Restore Computer System." February 18, 2016. http://fortune.com/2016/02/18/hollywood-hospital-hackers-computer-system/

17. Forcepoint Security Labs and Forcepoint LLC. "Locky Ransomware - Encrypts Documents, Databases, Code, BitCoin Wallets and More..." February 19, 2016. https://blogs.forcepoint.com/security-labs/locky-ransomware-encrypts-documents-databases-code-bitcoin-wallets-and-more

18. Forcepoint Security Labs and Forcepoint LLC. "Locky's New DGA - Seeding the New Domains [RUSSIA UPDATE: 26/FEB/16]." February 25, 2016. https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains

19. @Forcepointsec Twitter handle. March 22, 2016. Tweet, https://twitter.com/Forcepointsec/status/712316915687948289

20. Winton, Richard. "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating." Los Angeles Times. February 18, 2016. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

引用参考

21. Vijayan, Jai. "With $325 Million In Extorted Payments CryptoWall 3 Highlights Ransomware Threat." Dark Reading. October 29, 2015. http://www.darkreading.com/endpoint/with-$325-million-in-extorted-payments-cryptowall-3-highlights-ransomware-threat/d/d-id/1322899

22. Forcepoint LLC (formerly Websense). "The Seven Stages of Advanced Threats." https://www.websense.com/assets/pdf/understanding-the-cyber-attack-infographic.pdf

23. Forcepoint Security Labs and Forcepoint LLC. "TorrentLocker is Back and Targets Sweden & Italy." March 15, 2016. https://blogs.forcepoint.com/security-labs/torrentlocker-back-and-targets-sweden-italy

24. Forcepoint Security Labs and Forcepoint LLC. "Locky's New DGA - Seeding the New Domains [RUSSIA UPDATE: 26/FEB/16]." February 25, 2016. https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains

25. Information Sciences Institute; University of Southern California. "DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION." INTERNET PROTOCOL, September 1981. https://tools.ietf.org/html/rfc791

26. Information Sciences Institute; University of Southern California. "DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION." TRANSMISSION CONTROL PROTOCOL, September 1981. https://tools.ietf.org/html/rfc793

27. Forcepoint Security Labs and Forcepoint LLC. "Dridex Down Under." November 5, 2015. https://blogs.forcepoint.com/security-labs/dridex-down-under

28. Forcepoint Security Labs and Forcepoint LLC. "Accounts Payable in the Czech Republic Targeted by Dridex." August 4, 2015. https://blogs.forcepoint.com/security-labs/accounts-payable-czech-republic-targeted-dridex

29. Identity Theft Resource Center. "2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog." January 25, 2016. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

30. Forcepoint LLC. "Websense 2015 Threat Report." April 8, 2015. https://www.websense.com/content/websense-2015-threat-report.aspx

31. Harvard Business Review. "How the Cloud Looks from the Top: Achieving Competitive Advantage In the Age of Cloud Computing." 2011. https://hbr.org/resources/pdfs/tools/16700_HBR_Microsoft%20Report_LONG_webview.pdf

32. Anderson, Ed; Nag, Sid, and Gartner, Inc. "Forecast Overview: Public Cloud Services, Worldwide, 2016 Update." February 17, 2016. https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srcId=1-3478922254

33. Ponemon Institute LLC. "The Challenges of Cloud Information Governance: A Global Data Security Study." October 2014. http://www2.gemalto.com/cloud-security-research/SafeNet-Cloud-Governance.pdf

34. VansonBourne. "Shadow IT ITDMs Data Summary." p. 34. July 11, 2014. http://www.vansonbourne.com/files/1914/1225/3447/VB-Shadow_IT-ITDMs-Data-Summary.pdf

35. VansonBourne. "Shadow IT BDM Data Summary." p. 24. July 22, 2014. http://www.vansonbourne.com/files/7614/1225/3401/VB-Shadow_IT-BDM-Data-Summary.pdf

36. IDG Enterprise. "2015 IDG enterprise cloud computing survey." November 17, 2015. http://www.idgenterprise.com/resource/research/2015-cloud-computing-study/

37. CAS Cloud Security Alliance. https://cloudsecurityalliance.org/star/certification/

38. Raytheon Company, "Securing Our Future: Closing the Cyber Talent Gap." October 19, 2015. http://raytheon.mediaroom.com/2015-10-26-Many-more-men-than-women-are-drawn-to-cybersecurity-careers-and-the-gap-is-widening-dramatically-new-survey-says

39. Ocean Tomo LLC. "Intangible Asset Market Value Study." March 4, 2015. http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/

FORCEPOINT 是什麼公司？

Forcepoint 的問世旨在協助組織向前發展。我們的目標是在雲端服務、混合架構及行動工作者為常態的世界中，讓有需要的客戶能夠安全地採用轉型商業技術。以往的邊界安全模型已過時，組織需要能在資料附近佈設安全功能的解決方案，無論資料是在何處，包括遍及多重環境與裝置，從網路到端點，以及從行動裝置到雲端技術。不分區域、企業是否屬於垂直型或規模大小，客戶所面臨的威脅皆越來越大，資源受限的安全團隊很難趕上。Forcepoint 平台讓組織能將安全工作的例行作業自動化，省去單點產品的修補工作，並且能揭開真正的洞見，例如這份年度威脅報告內容所述。

THREATSEEKER® INTELLIGENCE CLOUD 全球智能網路威脅情資

Threatseeker Intelligence Cloud 全球智能網路威脅情資是為使 Forcepoint 對於最新威脅具有能見度所開發。每日處理從 155 國多重輸入所收集的多達五十億個資料節點，Threatseeker 全年無休於幕後工作，協助我們保護客戶，讓客戶能夠安全地執行業務。Forcepoint 專家每日與 Threatseeker 互動，收集精準的即時威脅情資與洞見，於我們的年度威脅報告、產業深度探討及預測報告中提出深具價值的參考指引。

FORCEPOINT
POWERED BY Raytheon