報告

McAfee Labs
2017 年威脅預測

2016 年 11 月

intel Security

McAfee Labs 探討未來一年內可能會發生的主要威脅。

關於 McAfee Labs

McAfee Labs 是威脅研究、威脅情報和網路安全先進理念的全球領先來源之一。借助來自檔案、web、郵件和網路等主要威脅媒介數百萬台傳感器提供的資料，McAfee Labs 提供實時威脅情報、關鍵分析和專家意見，以增強保護並降低風險。

McAfee 現在是 Intel Security 的一部分。

www.mcafee.com/tw/mcafee-labs.aspx

關注 McAfee Labs

簡介

歡迎閱讀《McAfee Labs 2017 年威脅預測報告》。本報告分成兩個部分，第一部分將深入探討三個非常重要的主題，從長遠觀 點對每個主題做出預測。

- 在報告的開頭，我們首先概覽網路安全領域一些難以解決的問題，以及安全行業在早期為解決這些問題付出的努力。本報告匯集了 Intel Security 眾多思想領導者所看到的最緊迫的技術安全挑戰。隨後，我們對這些挑戰進行了總結和剖析。我們將指出其中的六大難題。
- 接下來，我們再討論雲端威脅。十一位 Intel Security 思想領導者共同預測了在未來兩至四年內將會出現的雲端威脅，以及預期將要採取的法律和行業回應措施。我們預期將會看到哪些威脅和安全違規？地緣政治問題、法規、監管行動將如何影響這種環境？雲端服務提供商和安全供應商將會採取哪些回應措施？

- 我們最後討論的是有關威脅和物聯網的問題。十位 Intel Security 思想領導者使用與討論雲端威脅形勢相同的方法，對威脅和安全違規、法律和邊界、供應商回應措施進行預測。

第二部分對 2017 年的威脅活動進行了具體預測。我們對未來一年的預測涵蓋了眾多威脅，包括勒索軟體、所有類型的漏洞、利用威脅情報改進防禦、以及移動設備上的攻擊。

此外，我們還：

- 預測勒索軟體將在明年中期達到高峰，但隨後開始衰退。
- 討論為什麼威脅情報共享將在 2017 年取得重大進步。
- 解釋為什麼實體安全和網路安全行業將更緊密地融合。
- 預測駭客行動主義者會將目標瞄準消費者隱私，並闡述立法者和企業將如何採取回應措施。
- 討論為什麼安全供應商和執法機構將進行空前密切的合作，共同打擊網路犯罪分子。
- 詳細討論為什麼一些最常用應用程序中的安全漏洞將在 2017 年持續減少。
- 描述“假冒”內容的規模——包括產品評論、好評、廣告、安全警告等——如何持續增加，從而削弱網際網路上的信任。
- 解釋為什麼機器學習將用於增強社交工程手段攻擊。

我們希望這些主題能夠在您制定近期計劃和遠期策略時為您提供寶貴的意見。

我們通過自己的威脅報告用戶調查不斷收到來自讀者的寶貴回饋。如果您願意分享有關本威脅報告的觀點，請點擊此處填寫一份只需五分鐘時間就能完成的簡單調查。

祝您和您的摯友親朋節日快樂。

——*Vincent Weafer. McAfee Labs 副總裁*

目錄

McAfee Labs 2017 年威脅預測

以下四項領導者協同編寫了此份報告：

Jonathan Anderson
Yuriy Bulygin
Peter Bury
Torry Campbell
David Coffey
Carric Dooley
Brian Dye
Lynda Grindstaff
Barbara Kay
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Shishir Singh
Martin Stecher
Jamie Tischart
Ramnath Venugopalan
Lori Wigle
Candace Worley

2017 年威脅預測的研究及編寫人員：

Christiaan Beek
Yuriy Bulygin
Douglas Frosst
Paula Greve
Jeannette Jarvis
Eric Peterson
Matthew Rosenquist
Fernando Ruiz
Craig Schmugar
Rick Simon
Bruce Snell
Dan Sommer
Bing Sun
Adam Wosotowsky

難以應對的安全挑戰

分享反饋意見

難以應對的安全挑戰

—McAfee Labs

數字資訊安全領域始終面臨著各種挑戰。為了應對攻擊者層出不窮的變化，我們持續不斷地推出更新和修補程式。主要軟體版本在推出了重要新功能的同時，也會帶來意料之外的漏洞。緊急通知和修復在新漏洞攻擊被發現之後才會發布。

難以解決的大問題是那些需要進行基礎研究、新的產品分類、並需要海量時間和工作量進行開發，以及需要持續關注的問題，而這些通常需要多個行業參與者通力合作。本文中，我們討論了六個此類挑戰。

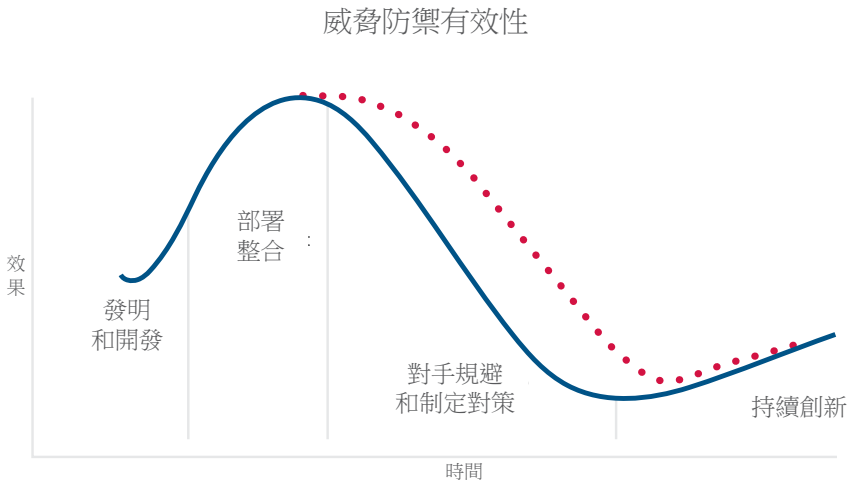
我們還會遇到一些難以解決的大問題。這些全局性問題無法通過修補程式或軟體更新得到解決。解決這些問題需要進行基礎研究、新的產品分類、並需要海量時間和工作量進行開發，以及持續不斷的關注，而這些通常需要多個行業參與者通力合作。

過去幾年內，隨著雲端服務的快速普及使用，內部網路和外部網路之間的外圍邊界逐漸消失，新設備的增長速度令人難以置信，這些因素都對保護所有數字資訊的傳統方法提出了挑戰。本文將討論安全行業面臨的六大挑戰，並提供行業採取行動應對這些挑戰的一些示例。

威脅防禦有效性

攻擊和防禦雙方都在不斷調整和演進。下圖顯示了某種類型的防禦隨著時間推移的典型演進過程。隨著新技術的開發，它的有效性迅速增加，最終可以隨時進行部署。部署之後，它將廣泛應用在現實場景下，開發團隊可以收到反饋，另外還包括應用於其他防禦中，從而進一步提高有效性。這種防禦技術將不斷增強，直至到達一定的有效性級別，促使對手採取回應措施。在這個階段，攻擊者會進行實驗，發現規避這種防禦的方法，制定出對策，從而降低了這種防禦技術的價值。

隨著新技術的開發，它的有效性迅速增加。這種防禦技術將不斷增強，直至到達一定的有效性級別，促使對手採取回應措施。攻擊者會進行實驗，發現規避這種防禦的方法，制定出對策，從而降低了這種防禦技術的價值。我們需要通過將曲線向右上移動，提高威脅防禦有效性。



安全行業的挑戰是向上向右移動這條曲線，到達紅色虛線的位置，從而延長威脅防禦有效性的生命週期。全面影響這種生命週期的行動包括：

- 降低我們和對手之間的資訊不對稱。
- 提高發動攻擊的成本，降低從中獲得的收益。
- 提高安全操作的可見性。
- 發現攻擊者對合法工具和憑據的利用。
- 保護分散資料。
- 在沒有代理的情況下進行檢測和保護。

降低資訊不對稱性

對手掌握的有關我們防禦的資訊，多於我們掌握的有關他們攻擊的資訊，這種不對稱性嚴重影響了威脅防禦有效性曲線。對手可以針對安全防禦，測試他們的攻擊方法，而不會遭受損失，無論是在實驗室中，還是在實際情景中，都可發起針對已部署系統的攻擊。他們可以針對我們進行測試，但我們卻察覺不到大部分測試，因而無法從攻擊者一方汲取經驗。為了讓曲線朝有利於我們的方向移動，我們是否可以製定相應方法來防止攻擊者針對我們進行測試，檢測到他們的實驗並從中吸取經驗，在可能的情況下誤導他們？

對手對我們的防禦的了解程度比我們對對手的攻擊了解更深。攻擊者可以對安全防禦進行不會遭受懲罰的攻擊測試。我們卻察覺不到大部分測試，因而無法從攻擊者一方汲取經驗。我們必須制定相應的方法防止攻擊者針對我們進行測試，檢測到他們的實驗並從中吸取經驗，然後儘量誤導他們。

防止攻擊者針對我們進行測試是非常困難的，甚至可能是無法解決的問題。但是，更加廣泛地共享有關攻擊的資訊，是我們可以採取的第一個關鍵步驟，有助於消除這種不對稱性。當我們共享和匯總有關攻擊的資訊時，我們可以更好地了解這些攻擊方法，以便找到我們算法中的漏洞。這讓我們能夠更加快速地調整和改進防禦。

流經各個網絡單元——例如雲端環境、虛擬機、物聯網設備——的遙測系統中的大量詳細資料有助於我們更好地了解攻擊方法。我們正在學習如何將資料科學應用到這些資訊中，以便更好地識別攻擊模式，並且更加快速地創建攻擊指標。我們還有潛力改變防禦的可預測性，讓對手更難發現特定弱點。這需要不同防禦層實時協同工作，讓通過某一個層的攻擊或探測被另一個層終止。

提高發動攻擊的成本，降低攻擊獲得的收益

金錢是大多數網路攻擊者的主要動機。我們是否可以提高發動攻擊的成本並降低攻擊獲得的收益？如果我們能夠減少攻擊獲得的經濟收益，降低攻擊成功率，提高捕獲的可能性，我們就能降低攻擊目標的吸引力。分析一下執法資料，我們將會發現，網路犯罪的調查和起訴與犯罪嚴重程度呈反比關係。對於物理犯罪，我們通常針對最嚴重的罪行進行起訴。但對於網路犯罪，針對高級別攻擊進行調查和起訴更加困難，因為它們通常跨越多個司法管轄區，犯罪者通常掌握了更多技能和資源，可以幫助他們規避檢測和起訴。針對這種情況，可以採取的一種回應措施是迷惑攻擊者，增加他們花費在特定攻擊上的時間，從而更加簡單地跟踪、識別、捕獲和起訴這些網路犯罪。

網路犯罪的調查和起訴與犯罪嚴重程度呈反比關係。我們必須減少攻擊所獲得的經濟收益，降低攻擊成功率，提高捕獲的可能性，從而降低攻擊目標的吸引力。

安全供應商顯著加強了他們與執法機構的合作。我們顯然能夠收集有助於執法和起訴的資訊。專注於防禦欺騙行為的安全公司已經進入市場，他們利用誘餌迷惑對手，將他們的注意力從更有價值的目標引開。與執法機構以往使用標記票據、汽車跟踪以及其他可跟踪性和恢復工具相似，網路安全也在增加對數字誘餌、報警文件及其他無法消除的標記的使用，旨在幫助找到攻擊者。

提高可見性

我們對資訊資產的控制比較有限，由於資訊資產的數量和分佈位置急劇增加，控制級別還在降低。我們需要幫助組織改進安全狀況的可見性。

通常只有在出現安全違規事件之後，組織才了解到他們的資訊資產受保護的情況如何。在影子 IT、各種類型的雲、“自帶設備”趨勢等因素的影響下，我們更難清楚了解安全操作的有效性。幾十年以來，企業一直在尋找識別和控制所有企業資產的製勝法寶。事實上，我們對資訊資產的控制比較有限，由於資訊資產的數量和分佈位置急劇增加，控制級別還在降低。幾乎沒有任何公司能夠宣稱他們牢固掌握了資訊資產的位置和控制權。因此，我們需要幫助組織改進安全狀況的可見性。

公司和安全供應商的安全操作正將重點從 IT 資產轉移到資料資產，從“偽絕對-絕對”防禦覆蓋轉移到資訊靈通的風險管理。我們擁有的工具能夠識別和分類資料，監控資料使用情況，並應用適當的策略，必要時還能阻止資料移動。利用這些工具，組織能夠更加有效地量化他們的風險狀況，發現嚴重的安全缺陷，並且適當地集中資源。安全意識比較好的組織會將基本統計資料與前一個月的資料進行比較，與會計賬目非常相似。而安全意識更好的組織則會確立地區、國家、行業的基準，用於進行比較，就像投資者那樣。但是，很多常見安全指標並不具有很強的可操作性。我們認為，要能夠對在受保護環境中的威脅行為採取接近實時的操作，我們還有很多工作要做。

識別披著合法外衣的攻擊

許多攻擊通過使用盜取的憑據開始實施。合法工具究竟被用於合法目的還是可疑活動？判斷兩者之間的差異是非常困難的。我們需要開發可針對每個活動進行合法性測試的模型。

很多攻擊首先使用盜竊的憑據，然後使用合法的管理工具來攻擊目標系統和洩露資料。傳統方法基於文件簽名或其他標準來查找惡意或可疑對象，從而檢測非法行為，但在此類情況下，傳統方法無法奏效。使用的對像已知是合法的，但被用於惡意目的。因此我們必須確定操作的意圖。它是正常業務登錄還是攻擊？加密是用於保護資料還是洩漏資料？這次 PowerShell 會話是管理員發起的還是惡意探測？

合法工具究竟被用於合法目的還是可疑活動？判斷兩者之間的差異是非常困難的。我們目前可以使用的唯一方法是行為分析，但它在網路安全領域還處於發展初期。它是一個良好的開端，但還需要構建一個模型，針對每次活動開展合法性測試，而不僅是針對文件和憑據。我們需要分析操作和資料移動，試圖確定其意圖，無論它們是來自外部操作人員還是未經授權的內部人員。此步驟要求了解有關活動上下文的大量資訊。

一種具有爭議的可能性是展開用戶信譽和預測分析。它的概念是評估特定帳戶遭受入侵和盜竊或被用於未經授權的內部活動的概率。通過收集上下文中的用戶行為，從在不同系統上重用密碼的趨勢到作業描述和典型工作時間，我們可將不同操作與一系列預期的合法活動進行比較，並標記超出特定風險級別的活動。這是一個敏感區域。在這種技術成為主流之前，我們還需要解決所涉及的隱私、道德和法律等重大問題。

保護分散資料

資料在企業周邊之外移動，因而容易出現無意洩露和遭受針對性攻擊。資料將移動到雲和個人設備，還會移動到合作夥伴、供應商和客戶。資料移動和到達目的地時，更需要保護。

資料在企業周邊之外移動，因而容易出現無意洩露和遭受針對性攻擊。資料要移動到雲端和個人設備，還要移動到合作夥伴、供應商和客戶。我們如何在移動過程中保護資料，確保它安全到達目的地。雖然組織僅有不足 20% 的資料始終在這種擴展生態系統中移動，但是 70% 的資料遺失都與這種移動相關。目前，有些機構試圖對資料進行加密，並在單獨的郵件中發送密鑰，將保護資料的責任移交至鏈條中的下一個人，從而保護此種類型的資料移動，這將導致信任範圍很小。我們必須找到如何擴展信任範圍，同時又維持更好的控制。

在早期階段，我們要使用資料分類和丟失防護系統來管理和擴展分散資料的信任範圍。資料在移動過程中始終具有安全性，從而實現持久的策略執行，這是下一個步驟。我們必須能夠在下一次使用過程中保護資料，這一點類似於數字權限管理機制。

在沒有代理的情況下進行檢測和保護

在將來的許多實例中，將不能把代理安裝到設備上來保護設備。我們必須找到其他保護途徑。

過去，很多安全功能要通過在我們保護的設備上運行代理來實現。但在今後的很多情況下，這種方法將不再可行。物聯網設備的存儲空間和計算能力非常有限，操作系統變得更加封閉以提高安全性，各種操作系統和設備類型數量繁多，超出了任何供應商的研發能力，汽車和關鍵基礎設施等行業的元器件生命週期很長，無法隨時更新。要確保未來的網路安全，解決大部分難以解決的重大問題，必須在無代理的環境實現安全。

無代理安全技術已經開始演進，早期的解決方案試圖從多個方向解決問題。芯片設計人員正在增強硬體級別安全性、存儲器保護、受信任執行環境。行為分析安全產品從外部進行監控，能夠隨時隔離和調查存在可疑或異常行為的設備。處理和分析仍然必須利用某種計算資源來進行，但我們將更多地利用靈活的計算資源，而不是使用專門的代理。分佈式實施點已經出現，它將擴展到由設備組成的整個網路，多個點之間相互實時通信和協作，以便執行檢測和保護操作。

總結

提高整個安全行業的威脅防禦有效性是遏制對手的關鍵。多家行業參與者必須協同工作，共同解決單個修補程式或軟體更新無法解決的全局性問題，這一點至關重要。我們需要更加廣泛地在業界領先公司之間分享資訊，這樣不僅能為我們提供更多的詳細遙測資料，而且有助於增強反欺騙技術。通過增加預測性分析的使用，提高組織資產和分散資料的安全可見性，減少專門代理的使用，我們能夠提高威脅防禦生命週期的有效性。

雲端威脅、法規和供應商回應措施

分享反馈意见

雲端威脅、法規和供應商回應措施

您能夠外包工作，但不能外包風險

Intel 的 11 位思想領導者共同對接下來兩到四年的雲端威脅和回應進行了展望。

我们的专家阵容：

Yuriy Bulygin
Peter Bury
David Coffey
Carric Dooley
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Shishir Singh
Jamie Tischart
Candace Worley

本文解答了下面的問題：

- 我們預計將會看到哪些雲威脅和安全違規？
- 地緣政治問題、法律、法規行動將如何影響雲端環境？
- 我們預測雲端服務提供商和安全供應商將會採取哪些回應措施？

雲端服務提供商正在建立信任和贏得客戶。越來越多的敏感資料和業務關鍵流程正在轉移至公有雲和私有雲。攻擊者將適應這種轉變，繼續尋找最簡單的方式來獲得經濟收益，或者實現他們的目標。在未來兩至四年內，我們的重點是雲安全的演進。我們預期將會看到哪些威脅和安全違規？地緣政治問題、法規、監管行動將如何影響這種環境？我們預測雲端服務提供商和安全供應商將會採取哪些回應措施？

威脅和安全違規

雲端服務不斷地快速成熟與發展，即為組織和國家帶來了機會，也為犯罪分子提供了可乘之機。我們通過討論做出了以下 11 條預測，在未來兩至四年內，這些預測很可能變成顯而易見的現實。

人們對雲端的信任度會提高，雲中的敏感資料和處理將會增多，導致針對雲端攻擊的可能性增大。

第一條預測非常簡單，但它為其他雲威脅預測奠定了基礎。過去幾年內，向雲端應用程序、雲端服務、雲端存儲遷移的速度加快，我們預測這種趨勢還將持續。雲端服務提供商已經顯著改進了安全控制和客戶保證，而且還將繼續進行改進。如果沒有發生影響到多個企業、國家、經濟行業的重大安全違規或中斷事件，用戶對雲端服務的信任將會繼續增加。所有類型和規模的組織會將更多處理和資料遷移到雲，很多企業將完全依賴雲。攻擊將會進行調整，新威脅隨之興起，並發生安全事件。

企業仍將關鍵功能保留在受信任資料中心和網路。

雖然資料在向雲遷移，但大多數企業不會完全外包他們的專有處理和存儲功能，他們將保留對企業非常關鍵的核心資料和知識產權。具有諷刺意義的是，公共雲毫無疑問比私有雲更加安全，因為它們通常擁有更加專業的安全團隊，掌握了從芯片到應用程序等領域的專業知識。構建私有雲的公司必須確信能夠保護所有層的安全，從應用程序到操作系統，從硬體到管理程序。當前，公司發現保護關鍵資料變得日益困難，因為周邊的定義不太明確。隨著雲端服務使用的增加，這一問題將變得更加突出，公司及其雲端服務提供商必須明確定義允許哪些資料通過，受到哪種類型的保護。

雲端服務的速度、效率、成本仍將與控制、可見性、安全性產生衝突。提供商及其客戶將選擇不同的平衡點。

雲端服務的速度、效率、成本仍將與控制、可見性、安全性產生衝突。
對於尚未積極利用雲端服務的組織而言，妨礙其得到更廣泛採用的第一位障礙是安全性。（但是，這些組織已經在使用雲，因為很多員工的文件都存儲在 Google、Dropbox、iCloud、OneDrive 或其他雲端服務上。）對於已經遷移至雲的組織而言，安全性下跌至第二位或第三位的障礙，位於運營一致性和財務監督之後。服務提供商必須改進雲端服務的速度、效率、成本，但另一方面又要兼顧控制、可見性、安全性，這種矛盾將會反映在雲端服務中。提供商將選擇不同的平衡點，它們最終會在價格和服務協議中反映出來，為公司提供最合適他們期望的安全狀況的選項。雖然雲端服務當前大多是存儲、服務器、應用程序的虛擬化，但在未來四年內，我們預期服務將會變得更加精細。雲將更多成為事件驅動的容器，而不是基於服務器的代碼。容器的平均生命期要比虛擬機短得多，基於代碼和資料運行，隨後消失。這種向更高的速度和效率的轉變將會顯著增加安全壓力，並與安全發生更多衝突。

我們熟悉的身份驗證方案及其控制系統仍將是雲保護中的最薄弱技術環節。我們預計針對管理員帳戶的定向憑據盜竊和暴力攻擊將增多。

我們熟悉的身份驗證方案及其控制系統仍將是雲保護中的最薄弱技術環節；很多攻擊首先將憑據竊取做為重點。

在可以預見的將來，密碼以及創建和使用密碼的用戶仍將是大多數技術中的最大薄弱環節。雲身份驗證也不例外，它為憑據竊取帶來很大收益。有些攻擊者非常耐心和老練，他們將會挖掘社交網路、以前失竊的密碼以及其他個人身份資料，以圖盜竊憑據，尤其側重於雲管理憑據。目標釣魚攻擊、虛假招聘活動和其他一些手段已在使用中，而且將繼續使用。內部身份驗證系統，例如 Active Directory，與雲端服務提供商使用的身份驗證系統進行交互的能力有限。雲應用程序的使用日益廣泛，而且人們喜歡在所有雲端服務中都使用相同或相似的密碼，導致這個問題進一步加劇。針對管理員帳戶的目標憑據盜竊和強力攻擊將會增加，攻擊者還會密切關注管理員帳戶活動。

攻擊將來自所有方向，同時利用“東-西”和“南-北”攻擊媒介。
正如我們在 Black Hat 大會和其他安全會議上聽到的討論內容那樣，犯罪分子將繼續探索新的攻擊媒介，並且成功實施攻擊。在傳統的系統和網路中，大多數攻擊遵循“南-北”模式，企圖在堆棧中上下移動，以增加權限、攻擊漏洞、獲取對資料或應用程序的訪問。雲攻擊者將繼續使用這種模式，另外還會尋求利用“東-西”攻擊的機會。“東-西”攻擊是在虛擬機、容器或其他雲項目之間移動，在服務甚至組織之間跳轉。攻擊者將利用雲的規模和攻擊面的增大，廣泛掃描尋找漏洞，然後試圖攻擊使用同一家雲端服務提供商的多個組織，或者衍生惡意流程，為後續的監視和洩露提供立足點。

各服務層之間脫節、不一致的設置及控制是第二個薄弱環節。攻擊者將成功利用這些脫節和不一致性。

各服務層之間脫節、不一致的設置及控制是第二個薄弱環節。攻擊者將成功利用這些脫節和不一致性。

從基礎設施到應用程序，組織分別使用了多家不同類型的雲端服務提供商。組織並不能始終清晰地劃分雲端服務提供商和自己之間的責任界限，因而在安全方面留下了可以利用的漏洞。這並非技術的失敗，而是流程的失敗。組織擁有工具，知道應該採取哪些措施，但有時他們假定某項工作是由另外一方負責的。此外，如果組織使用了多家雲端服務提供商，由於不同或不一致的控製或術語，多家供應商分別負責的安全狀況可能有所不同。出現這種情況的一部分原因是他們使用了大量不同安全標準，影響到一致性，進而影響到比較能力。這些流程失敗和安全控制不一致將為網路攻擊留下可乘之機。要杜絕這種現象，他們必須更好地理解流程，讓雲安全控制標準變得更加成熟。

在將計算和資料遷移到雲端時，可見性和控制仍將是企業面臨的關鍵問題。

雲端運算能夠根據需要移動流程和資料，這會為我們提供極大優勢，但也可能導致嚴重的安全或隱私問題。我們見過一些案例，有人賄賂員工，以求分享他們的密碼。對於所有類型的組織而言，不知道或無法控制資料存儲在何處或執行哪些流程，都會導致一系列棘手問題。無論這些組織是希望將資料存儲在國界範圍內，以遵守國家的隱私法規，還是出於安全原因，限制流程僅在特定的雲端環境中運行，防止第三資料或知識產權離開公司本地，或者了解雲的使用模式，他們查看和限制資料在雲中和雲間的移動的能力都遠遠落後於需求。如果攻擊者利用合法媒介（應用程序、憑據等）來實現可能非法的目的，我們必須採用基於上下文的行為分析。在可以預見的未來，這些可見性和控制問題仍將存在。

攻擊者，包括僱傭的職業攻擊者，將利用雲實現規模化、快速以及匿名等目的。

令人遺憾的是，我們沒有簡單的方法來防止雲資源被攻擊者利用。一旦發現濫用行為，它們將被立即終止，但整個過程可能花費長達幾個月時間。另外，攻擊者還會利用雲資源進行大規模強力攻擊，通過多種媒介發起復雜攻擊，在多個站點和國家之間迂迴進行攻擊以逃避起訴。由於使用雲資料存儲服務，它也可能構成竊取資料的倉庫，攻擊者可以挖掘這個倉庫以尋找寶貴的連接和關聯。雲具有很多特徵，包括持續變化的帳戶、IP 地址、服務位置以及短暫存在的容器，這些特徵有助於居心叵測的攻擊者更長時間地隱藏身份，讓他們更加難以跟踪。在未來兩至四年內，這種狀況將無法改變。

“勒索拒絕服務”將成為針對雲端服務提供商和依賴雲開展運營的組織的常見攻擊。

由於一個雲可能包含很多租戶，因此針對雲端服務提供商發起拒絕服務攻擊具有更大的誘惑力。大多數服務提供商能夠很好地防禦傳統的拒絕服務攻擊。但是，攻擊者將繼續努力尋找他們可以利用的漏洞。一旦找到，他們會立即發起攻擊。如果組織完全依賴於雲，企業和雲之間可能有多個點遭受攻擊，讓業務陷入停頓。其中包括網際網路連接、DNS 服務和其他基礎設施組件。要攻擊依賴雲開展運營的企業，攻擊者並不需要攻擊雲端服務提供商。相反，攻擊者可以乾擾企業對雲的訪問，然後劫持公司資料，以此進行勒索。

除了基於憑據弱點的資料洩漏之外，成功的公共雲資料洩漏事件仍然比較少，但影響卻不斷增加。

雲端服務提供商掌握的雲安全專業知識通常遠強於他們所服務的公司，因此，除了由於憑據失竊導致的資料洩漏之外，成功的雲資料洩漏事件預期仍會較少。但是，當資料洩漏能夠提供對多家客戶的大型資料庫的訪問時，雲端服務資料洩漏產生的潛在後果是非常嚴重的。雲端服務提供商或受影響組織是否會受到資料洩漏的嚴重影響，很大程度上取決於相應人員是否在其責任範圍內付出了合理的努力。

物聯網設備的數量和多樣性不斷增長，將會破壞一些雲安全模式，導致攻擊者成功通過這些設備發起進攻。

大多數身份驗證都需要用戶和設備之間的交互，或兩部設備之間的交互。隨著更多物聯網設備和服務的推出，這些設備將與多部其他物聯網設備進行通信，並以機器速度做出信任決定。企業嚴重缺乏安全架構、受信任證書頒發機構以及對這種通信的控制，因而導致資料洩漏，產生可能被利用的漏洞。雲端服務提供商努力將當前模式推行到這種新環境中，但這樣會產生很高的延遲和復雜度，而它們都是引發安全故障的因素。我們已經看到過攻擊者通過無安全保護的物聯網成功入侵企業網路的情況，他們的下一個攻擊目標是雲。

法律和邊界

雲威脅和資料洩漏事件將會導致來自政治和法規的雙重回應。技術進步的高速度妨礙了有效的立法，而立法的滯後又妨礙了技術進步。各個國家/地區製定了不同甚至相互矛盾的法規，讓消費者、企業、雲端服務提供商很難找到法律依據。

法律將無法跟上技術進步的速度。雲端服務提供商、其客戶和新興網路保險行業要經過多年的訴訟，才能明確建立正確的行為。

法律將無法跟上技術進步的速度。法規將使用諸如“盡職調查”和“合理努力”之類的字眼，讓雲端服務提供商及其客戶面臨遭受起訴的風險。

法律無法跟上技術革新的步伐，這並非新聞。有關雲中資料保護和消費者隱私的法律也不例外。在提及雲資料安全時，司法機構將會使用諸如“盡職調查”和“合理努力”之類的字眼，以確保立法保持有效性，而不會立即過時。遺憾的是，他們需要一定的時間和很多的訴訟，才能通過法律程序來足夠詳細地定義這些術語。對於系統和資料的網路安全，通常無法應用簡單的“是或否”測試，特別是在雲安全領域，多個實體必須協同提供保護。同時，雲端服務提供商及其客戶，還有新興的網路保險行業，將會作為原告和被告，經歷多年的訴訟，辯論他們是否付出了“合理努力”。因為遭受雲威脅的公司將努力證明他們採取了能夠做到的一切來保護客戶，公眾認知將在其中扮演重要角色。

資料出入司法轄區的移動將成為長期挑戰。保護消費者的法規將限制雲利用。

為了保護消費者的隱私，政府機構將通過法規，要求組織將其收集的個人資料存儲在公民所屬國家/地區的邊界範圍內。這會向企業挑出挑戰，要求他們必須識別和分類資料。而對於雲端服務提供商而言，則必須為資料和流程移動提供更加精細的控制。如果位於某個國家的大型資料中心受到攻擊影響，而最近的備份位於邊界之外，服務協議如何對此做出規定？跨國公司如何將客戶資料、銷售資料、產品資料分離開，以便根據新法律實施控制？此類挑戰將會限制雲利用，因為組織可能被迫在某些國家/地區建立自己的資料中心，或者確定在這些國家/地區開展業務是否成本過高。

有些司法轄區將對雲端服務提供商及其關聯企業提出最低運營要求，並且進行認證和/或審計。

如果雲端服務提供商破產，資料如何處理？如何保護企業和消費者，以防止犯罪分子或某些國家創建以資料收集為主要目標的惡意雲端服務？雲端服務提供商與其分包商或關聯企業之間的責任劃分應遵守什麼法律要求？對於這些問題，政府機構可能採取的另一個應對措施是對在他們國家/地區運營的雲端服務提供商提出最低運營要求，進行獨立認證，或者提出審計條件。定義這些條款和關係層是一個嚴峻的挑戰，將在業界形成對立的觀點，並且引發激烈討論。無論法律如何規定，資料洩漏的風險和最嚴重後果將由服務提供商承擔，而不由分包商或關聯企業承擔。

供應商的回應措施

威脅、資料洩漏和相關立法將促使雲端服務和安全供應商在技術和服務方面採取回應措施。他們將會增強身份驗證系統，開展企業級別的控制，實現安全功能的自動化，從而減少差距和不一致，另外威脅情報共享將會改進檢測。以下是我們預期供應商將在未來兩至四年內針對雲威脅採取的十大回應措施。

密碼必須被更安全的身份驗證系統取代，但這些系統不能過度妨礙登錄過程。生物識別、多級別身份驗證、行為分析將幫助保護服務提供商及其客戶的資料。

生物識別、多級別身份驗證、行為分析將幫助保護服務提供商及其客戶的資料。

密碼必須被更安全的身份驗證系統取代，但這些系統不能過度妨礙登錄過程。短期內，我們預計將會看到多要素身份驗證的增加，通常使用手機或“質詢-回應”系統。這種技術首先將應用於管理員，因為管理員憑據失竊帶來的後果是最嚴重的。我們還將看到行為分析技術被用於檢測帳戶登錄中的異常活動。長遠來看，我們預期生物識別技術的採用將會大幅增加，此類設備的外形尺寸讓用戶感覺舒適和易用。指紋將被其他唯一特徵取代或結合使用，比如面部、心跳或視網膜，這些技術的實施在商業上具有可行性。

企業級別的可見性和控制將幫助管理影子 IT 的資訊向雲的移動，並協調在雲中執行的工作的複雜度和規模。

在雲端服務提供商的幫助下，企業的業務部門能夠將工作負載移動到雲，而無需 IT 人員介入。在很多公司，安全或 IT 團隊不能知道這些業務部門何時將資料或流程移動到雲，這種情況有可能波及整個企業。他們請求供應商提供工具，以增加可見性和資料控制，從而滿足這種需求。我們預期資料丟失防禦和策略協調工具將會更加適合雲使用。下一個步驟將是支持雲的擴展，它讓企業能夠直接通過雲端服務提供商應用安全控制和策略。

安全評估、身份驗證、風險減輕、雲審計是自動化可以彌補人類專家存在不足之處，並幫助解決人手不足的部分領域。

安全自動化有助於解決人才短缺問題。

安全技能缺乏將是對雲端服務提供商的一大威脅，但也為他們提供了機遇。要將這種威脅轉化為機遇，必須將安全經驗融入自動化工具中，以簡化雲安全控制，讓更多用戶能夠有效地設置和監控他們的保護。在安全評估、身份驗證、風險減輕、雲審計這些方面，自動化能夠更充分地利用專家經驗，增加環境感知，將功能擴展到業務管理人員。

雲訪問安全代理不斷成熟，提供更出色的安全性、更高的可見性、更多的控制。

制定策略並將其應用於雲端服務身份驗證，對於保護組織仍將非常重要。雲訪問安全代理 (CASB) 是製定和實施策略的一種很好方式，但無法解決身份驗證的核心問題。資料是最有價值的資產，也將更多成為保護重點，CASB 將日臻成熟，並與其他安全系統協調或集成，以確定雲中的哪些資料需要安全保護，以及如何實施保護。

增加對資料在靜態或流通狀態下的保護，將成為一些雲端服務提供商的競爭優勢。

一些基礎雲端服務，例如存儲或處理器租賃，將會逐漸商品化。為了在競爭中佔據優勢，有些雲端服務提供商將為在他們的系統中存儲、處理和傳輸的資料提供額外保護。這些高級服務不僅提供加密，還包括完整性檢查、實時監控和增強型資料丟失防護技術，為他們提供長期競爭優勢。

對雲端服務提供商操作的審計和可見性將成為常態。

在四年內，實時審計和可見性將成為大多數雲端服務提供商的標準服務，這可能是客戶要求、競爭壓力、行業法規導致的結果。無論是領先還是標準的雲端服務組件，都將能夠回答客戶提出的問題“我們資料在什麼地方？”。靜態審計和歷史記錄視圖不足以確保高價值資料和工作流程達到足夠的保護級別。

安全解決方案將變得更有預測性和規定性，幫助檢測新興威脅，在它們危及系統之前終止攻擊。

安全解決方案供應商將開始使用機器學習來預測和中止攻擊，預先防止危害。

保護雲基礎設施本身的安全解決方案將變得極其關鍵，因為如果基礎設施遭到威脅，攻擊者將能直接訪問多個客戶的應用程序和資料。此類事件將會大量發生，因此供應商也將持續開發先進的自動化工具，用於快速診斷和解決事件。安全解決方案基於使用機器學習和 Big Data 分析的技術構建，將變得更有預測性和規定性，幫助檢測新興威脅，在它們危及系統之前終止攻擊。

我們將看到企業與雲提供商之間威脅情報共享大幅增多，從而改進攻擊的識別並縮短應對時間。

多家雲端服務提供商將合作建立威脅情報共享組織，它們將改進身份標識，縮短對攻擊的反應時間。

目前，很多組織和雲端服務提供商尚未認識到威脅情報共享的益處。今後幾年內，在法規或威脅攻擊的驅使下，企業和雲端服務提供商之間將進行更多的威脅情報共享，其益處也將變得愈加明顯。雖然這種共享可能有時令人為難，但組織將認識到，實時共享有關成功和失敗攻擊的情報的益處遠大於弊端。

雲安全的技術和保證標準將繼續加強。

Cloud Security Alliance 等組織已經制定了有關雲端服務管理的各種標準、準則、認證和最佳實踐。迄今為止，他們的重點還是開發為客戶提供更高透明度的標準和指南。雲安全標準當前只是次要的工作，但對於安全雲設計和操作的重大意義，人們達成了更多共識。我們預測，在未來兩至四年內，他們將製定明確的保證標準，不僅更加全面，而且還會得到領先雲端服務提供商的積極採用。

網路安全保險市場將會增長，但由於法律條款的解釋不清晰，無法確定是否發生可保險的安全事件，它仍然面臨挑戰。

我們預期保險公司將會提供針對網路空間的保險，還提供安全評級，幫助降低保險成本。有些國家/地區將出台一些法規，同時隨著雲端服務的日臻成熟，有助於增加用戶對雲端服務的信任。但是，雲安全保護仍然是帶有主觀性的業務，有很多免責條款。在目前這個階段，我們尚不具備做出有關成本、索賠、可保事件的客觀決策所必需的基礎設施和經驗。

總結

隨著雲端服務的使用持續增加，這些服務作為攻擊目標具有更高的價值。雖然很多公司仍會將最敏感資訊存儲在私有資料中心，但速度、效率和成本的壓力將迫使他們將資料存儲在受信任網路之外和遷移到雲中，這樣可以實現很多優勢。企業開始學習如何在運營中應用雲端服務，但控制、可見性、安全等方面的脫節將會導致出現資料洩漏。

攻擊來自所有方向 —包括在組織堆棧中的上下移動、在使用同一雲端服務企業之間的移動。憑據和身份驗證系統仍將是最易受攻擊的攻擊點，因此網路犯罪分子將全力竊取憑據，尤其是管理員憑據，因為它們能夠提供最大範圍的訪問。

針對安全和隱私問題，政府機構採取的最常見回應措施是對服務提供商進行認證，提出最低運營要求，並採取其他監管控制行動。各個司法轄區的做法存在很大差異，有時這些管制措施會限制雲使用。跨國組織在跨越國境邊界使用雲端服務時將會非常謹慎。法律無法跟上雲技術和雲端服務的發展步伐。訴訟將成為重要手段，大部分在違規事件發生之後，原告和被告試圖爭辯哪些行動才算是“合理努力”。

雲端服務提供商和安全供應商將努力增強身份驗證系統，逐漸採用生物識別技術，作為最佳解決方案。服務提供商及其客戶將努力提高服務可見性，實時審計將成為一項標準服務。新興技術將在靜態和傳輸狀態下更好地保護資料。為了應對大量的快速威脅，企業將利用行為分析、安全自動化、共享威脅情報服務來改進檢測和糾正功能。機器學習將成為預測和終止攻擊的一種方式，防止它們造成危害。

物聯網威脅、法規和供應商回應措施

分享反饋意見

物聯網威脅、法規和供應商回應措施

歡迎開發充滿希望的物聯網領域

Intel 的 10 位思想領導者共同對接下來兩到四年的物聯網威脅和回應進行了展望。

我們的人員陣容：

Jonathan Anderson
Yuriy Bulygin
Carric Dooley
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Ramnath Venugopalan
Lori Wigle
Candace Worley

本文解答了下面的問題：

- 我們預計將會看到哪些物聯網威脅和安全違規？
- 地緣政治問題、法律、法規行動將如何影響物聯網環境？
- 我們預測物聯網設備開發商和安全供應商將會採取哪些回應措施？

物聯網攻擊威脅真實存在，但犯罪分子獲得經濟收益的機會仍然具有不確定性。網路犯罪分子將找到有利可圖的模型，動機驅動的攻擊最終將擴散開來。

物聯網覆蓋了各個行業的數百甚至數千種設備。事實上，物聯網指的並不是很多種設備，而應該是由設備構成的網路，它可以實現和提供各種服務，其中很多服務是基於雲的。因此，物聯網威脅和回應措施與雲威脅和回應措施存在著密切關聯。

在很多行業，這些支持雲的設備網路可以視為利益社區。例如，工廠車間就是製造商的利益社區，該網路包含製造產品所需的各種設備。在醫院環境中，滿足醫療人員需求的醫療設備和相關網路構成了一個利益社區。

攻擊者將有很多盜竊資料、拒絕操作、造成危害的機會。在本文中，我們的重點是物聯網安全功能在未來兩至四年內的演進。我們預期將會看到哪些威脅和安全違規？地緣政治問題、法規、監管行動將如何影響這種環境？我們預測物聯網設備開發商和安全供應商將會採取哪些回應措施？

威脅和安全違規

對於網路犯罪分子或某些國家而言，物聯網設備是非常具有吸引力的攻擊渠道，有以下一種或兩種原因：它們可能是資料或元資料的潛在來源，或者是造成危害的潛在攻擊媒介。我們通過討論做出了以下 10條預測，在未來兩至四年內，這些預測很可能變成顯而易見的現實。

物聯網攻擊威脅真實存在，但犯罪分子獲得經濟收益的機會仍然具有不確定性。

目前，攻擊物聯網設備的漏洞和機會確實存在，但犯罪分子從攻擊中獲取非法經濟收益的機會卻受限於多種因素，例如位於網路中的高價值位置的特定物聯網設備數量不足、缺少通過攻擊賺取收益的清晰模式。如果通過物聯網設備成功發起了攻擊，那麼犯罪分子的目的是什麼？是將盜竊的資料在駭客網站上銷售？還是對網路進行破壞（比如讓企業網路中斷）？未來四年內，犯罪分子將會解開這個謎題，經濟動機的攻擊將變得非常廣泛。有趣的是，確實存在一些可進行破壞的機會，但截止目前我們看到的這種案例很少，可能是因為潛在的犯罪者害怕報復。

勒索軟體將遷移到物聯網，因為事實證明它是犯罪分子牟取經濟收益的相對簡單的方式。

勒索軟體將成為主要威脅。

對威脅進行預測時，最大的挑戰之一是將潛在動機與實際機會關聯起來。有些廣為人知的物聯網設備駭客或漏洞攻擊很難大規模實施。我們確信，勒索軟體隨時可能移植到物聯網領域，事實證明它是犯罪分子牟取經濟收益的相對簡單的方式。攻擊一部或多部物聯網設備及其控制平面或雲聚合點，然後劫持它們以進行勒索，與入侵大量設備並獲取其資料相比，這是牟取經濟收益的更簡單、更快速方式。在配電和醫療保健垂直市場，我們已經看到了物聯網設備被劫持以進行勒索的情況。

駭客行動主義將成為最大的恐懼。

對於使用物聯網設備和連接的很多組織而言，雖然勒索軟體將成為現實的威脅，但駭客行動主義卻是他們最大的恐懼。根據我們的推斷，大多數犯罪分子都希望牟取經濟收益，他們對破壞或嚴重干擾企業運營並不感興趣。但是，激進分子通常表現出一些不合常理的行為，以展示自己的威力。這些行為可能是控制和更改投票機記錄，打開水壩的閥門，或者破壞化工廠的安全系統，它們都可能帶來災難性的危害。在未來兩至四年內，駭客行動主義者將會蠢蠢欲動，但只有極少數人取得成功。

某些國家對關鍵基礎設施的攻擊始終都將是令人擔憂的問題，但由於害怕遭受物理或網路報復，這些攻擊只會零星發生。

某些國家發起的攻擊是除駭客主義行動之外的最大威脅。破壞或損害另一個國家/地區的軍事或經濟能力的機會是真實存在的，在過去一年內，我們已經看到過幾次攻擊。這些攻擊主要在 SCADA 系統上，它們是物聯網設備的一種。但是，由於害怕受害方在軍事、經濟或網路上進行報復，對關鍵基礎設施發起此類攻擊的頻率受到限制。

物聯網設備將快速推動當前隱私法律的邊界，政府機構對這種變化的反應仍將非常緩慢。

物聯網將嚴重剝奪消費者隱私權。

以前就有人宣告了隱私權的死亡，也許過於誇張，但現在物聯網讓我們距離這個目標更近一步。大量的物聯網設備在進行監視、監聽、錄像或資料收集，或者在密切關註消費者的行動。很多情況下，消費者向公司付費購買服務，允許對自己進行跟踪。當然，詳細條款列在用戶許可協議中，但大多數消費者不會閱讀這些條款，而且也別無選擇。物聯網設備將快速推動當前隱私法律的邊界，政府機構對這種變化的反應仍將非常緩慢。用戶對隱私權的預期將會影響到設備供應商和服務運營商，因為有些國家的政府要求提供明確協議和選擇權，甚至為使用或分享他人的資料進行補償。

我們將看到物聯網設備會被作為竊取資料和知識產權、破壞關鍵基礎設施並進行其它類型威脅攻擊的突破口。

物聯網設備將成為入侵控制、監控、資訊系統的有用攻擊媒介。

在未來兩至四年內，我們將看到物聯網設備會被作為竊取資料和知識產權、破壞關鍵基礎設施並進行其它類型威脅攻擊的突破口。很多剛進入市場的新型物聯網設備存在弱點，沒有安全保護。已經投入使用的物聯網設備通常也存在類似弱點或已知漏洞，無法進行修補或升級。還有一些情況，我們將安全的設備連接到網路，但沒有適當的隔離或分段，無意間讓攻擊者獲得對受信任環境的訪問。最後，還有來自運營部門的壓力：“系統工作正常。不要動它！”這些因素累加在一起，使得物聯網設備成為入侵很多類型的系統和組織的開放通道。

在讓產品支持網際網路協議時，設備製造商還會犯下低級錯誤。

公司讓他們的設備支持網際網路協議，有兩個主要原因：為了提高效率；為了收集有關設備使用的資料。其中有些公司以往在網際網路連接設備方面經驗很少。因此，有些公司會犯下低級錯誤，汲取教訓，或者重歷網際網路安全的威脅和風險。不幸的是，他們面臨的安全環境比以前更加險惡。必須對安全違規、法規、學習進行一定的組合，讓安全成為所有組織的常規工作的一部分。這個學習期將持續四年以上。

物聯網設備的控制台將成為主要目標。

當人們談及物聯網攻擊時，通常指的是直接針對物聯網設備的攻擊。雖然設備級別的攻擊很常見，但它們通常很難實現大規模攻擊。攻擊一輛自動駕駛汽車、一個互聯閥門、一把智能門鎖無法獲得可觀的收益回報。因此，攻擊者通常願意將物聯網設備的控制台作為攻擊目標。控制台具有一定級別的訪問權限，用於監控進程和更改設備上的設置。安全工作的重點一直放在物聯網設備上，而對於控制這些設備的系統，卻沒有給予同樣的重視。大多數重要物聯網設備部署的規模都比較大，這意味著它們的控制台將非常複雜，可被攻擊的入口比較多。通過影響控制流中的資訊完整性，或者突破薄弱的認證系統或憑藉竊取的登錄憑證來直接破壞控制器本身，攻擊者能夠從中獲得更大的非法經濟收益。

收集來自設備的資料的聚合點將成為主要目標。憑據和身份驗證系統是弱點。

收集來自設備的資料的聚合點也將成為主要目標。

物聯網系統中的另一個潛在弱點是聚合點，它是收集來自多部物聯網設備的資料的位置。與控制台相同，攻擊聚合點也會為攻擊者牟取非法經濟收益創造機會。既然這樣能夠把握資料傳送的大動脈，為什麼還要分別攻擊多部設備，一步一步收集資料呢？攻擊者不會每次劫持一輛汽車的資料來進行勒索，而是通過維護系統接管汽車經銷商的所有汽車資料。憑據和身份驗證系統仍然是弱點。當然，大多數物聯網設備聚合點都將在雲中，因此雲本身的漏洞和麵臨的威脅也會影響到聚合點的安全。

勒索軟體將攻擊支持網際網路的醫療設備。

我們目前還不知道攻擊者為什麼要攻擊收集患者資訊的醫療設備，但這種事情正在發生，醫療資料正在洩漏。未來兩至四年內，這種情況很可能仍將持續，我們將知道他們為什麼盜竊醫療資料。更糟糕的是，監視和控制人體系統（包括心臟起搏器、胰島素泵和神經刺激器等）的醫療設備也都會連接到網際網路。惡意攻擊者將這些醫療設備視為除醫療勒索軟體攻擊之外的下一條攻擊途徑。攻擊者成功地將醫院作為勒索軟體攻擊目標，因為醫院需要即時訪問資訊。心臟起搏器也是醫院需要即時訪問資料的一個例子，因此在這些設備支持網際網路之後，攻擊者將試圖尋找這些設備中的漏洞，如果取得成功，他們能夠敲詐很多不義之財。

法律和邊界

隨著物聯網威脅和安全違規事件的發生，促使我們在政治和法規上採取應對措施。技術進步的高速度妨礙了有效的立法，而立法的滯後又妨礙了技術進步。各個國家/地區製定了不同甚至相互矛盾的法規，讓消費者、設備製造商、服務提供商更難找到法律依據。

盜亦有道？

在加州一家醫院最近遭到勒索軟體攻擊之後，駭客團體的一些成員對攻擊者嗤之以鼻，認為他們是“有史以來最愚蠢的駭客，就像他們沒法再黑掉別的東西”，還有“如果有人因此死亡或受傷，這就完全錯了。”駭客通常也有一定程度的同情心，這聽起來似乎有些不可思議。物聯網攻擊在經濟上能夠產生誘人的收益，但也可能導致患者死亡或受傷，一些駭客會謹慎從事，限制攻擊的次數和嚴重性。

法律將滯後於物聯網設備技術及其採用，從而引發訴訟。

法律無法跟上技術革新的步伐，這是眾所周知的事實。物聯網設備和系統具有諸多優勢，包括改進醫療效果、提高製造效率和家居生活質量，並且提供眾多可能性，雖然存在安全和隱私問題，但它的採用還將增長。因此，我們將會看到一些引發訴訟、抗議和消費者憤怒的事件。由於文化規範和訴訟速度不同，各個國家/地區的訴訟存在很大差異。對於立法機構而言，制定法律將是一大嚴峻挑戰，因為存在相互競爭和衝突的各種利益。有些司法轄區，例如歐盟，很可能在這個領域領先一步，其他司法轄區則會持觀望和等待態度。

在與面向消費者的物聯網設備、服務及其資料收集相關的訴訟中，隱私權將成為主要焦點。回應將受到文化標準的影響，而如何適應這些差異將成為公司的挑戰。

各個司法轄區在隱私權方面存在很大的法律和文化差異。

在與面向消費者的物聯網設備、服務及其資料收集相關的訴訟中，隱私權將成為主要焦點。這種現像在很大程度上是由於消費者方面的壓力驅動的，在發生幾次嚴重資料盜竊之後，隱私權還將得到進一步重視。各個國家和行業針對這種情況的回應措施將會受到文化規範的影響，存在很大差異。對於企業而言，克服這些差異將是一大嚴峻挑戰，並將導致他們延緩甚至避免進入某些市場。

物聯網設備安全性將成為企業的一條重要購買標準。隱私性將成為消費者的一條更重要購買標準。

這是兩個獨立而又有些關聯的內容，將在物聯網設備和安全行業產生一些衝突。企業將考慮物聯網設備和系統的安全性，並將其作為首要購買標準。這將推動安全功能的發展，例如設備認證、資料加密、受信任的更新、基於硬體的安全、受信任的執行環境。消費者在購買物聯網設備時將更多考慮隱私性，但仍會影響到便利性。這種狀況鼓勵改進的設備加密，可能推動設備匿名等功能的發展，或者要求企業給予一定的直接或間接補償，才允許他們收集和使用個人資料。

供應商的回應措施

威脅、安全違規和相關立法將促使物聯網設備製造商、服務提供商、安全供應商在技術和服務方面採取回應措施。他們將會增強設備安全性和隱私性，開髮用戶身份保護功能，擴展基於硬體的防禦，另外保險服務也將演進，將物聯網系統實施也納入保險範圍。以下是我們預期在未來兩至四年內將會採取的針對物聯網威脅的七大回應措施。

如果使用免費的產品，您要以提供自己的資料為代價。

消費者逐漸意識到，他們保存在智能手機等物聯網設備上的資料具有重要價值，應該為分享這些資料得到補償。免費的產品和服務通過資料收集或定向廣告創造收入，在未來兩至四年內，這種現象將變得更加明顯。有些產品提供付費選項，不會收集資料，而有些產品則根據收集的資料量，向消費者支付數額不等的費用。所有這些都要求物聯網設備和系統開發商提供安全和隱私保護。

經過改進的新加密選項。

從上文的預測推論，能夠在傳輸全程始終保護物聯網設備生成的資料安全，對於防止中間人攻擊極為重要。無論是遠程攝影機、支付卡讀卡器和位置跟踪設備，還是製造監控系統，在中游捕獲物聯網生成的資料現在非常容易。為解決這個問題，供應商將提供更多加密選項和更強的密鑰，從而提升安全性，還將以硬體作為輔助，以最大程度減少性能影響。在未來四年內，我們將看到這些選項。

基於硬體的隱私和安全功能將內置到一些物聯網設備硬體中。

與傳統的 IT 設備相比，在軟體中保護物聯網設備的難度更大，原因可能是它們的外形尺寸太小、數量過多或缺少人機互動。因此，基於硬體的安全將變得更加重要。例如，受信任的執行環境已經在一些處理器中存在，僅允許指定進程運行和訪問資料；物聯網設備開發商將開始使用這些技術。在兩至四年內，物聯網設備製造商將推廣這種產品功能，我們甚至還將看到分區或受信任的應用程序開始通過應用程序市場出售，以供設備使用。更多安全功能內置到物聯網設備硬體中，為實現出色的安全性和隱私性奠定牢固基礎。

安全供應商將引入和支持行業標準以保護物聯網設備身份。

增強隱私性的一種方法是確保服務提供商永遠不知道設備身份。設備身份驗證可以抽象化，並由第三方提供，第三方隨即向服務提供商確認物聯網設備是受信任組的成員。他們也可以使用塊環鏈技術，塊環鏈與比特幣使用的技術相似，可以提供交易匿名，因而交易無法關聯到特定的物聯網設備或帳戶。服務提供商仍然可以收集和出售資料，但是作為一個聚合集，無法識別設備身份。在未來四年內，我們預期這種方法將從專有技術變成行業標準。

將開發控制系統以集中自動管理和保護物聯網設備。

物聯網設備控制系統將用於集成和保護在 2020 年之前推出的眾多物聯網設備。

物聯網設備不僅數量龐大，而且功能有限，因而很難通過我們保護傳統 IT 系統的方式來進行管理和保護。因此，人們將開發控制系統，用於自動集中管理和保護物聯網設備。關鍵功能將包括自動設備身份驗證、物聯網設備軟體和更新管理、隱私和安全策略管理。由於我們很難在現場快速更新所有設備，因此就需要額外的安全防禦，以抵禦零日攻擊。

物聯網設備的行為監控將成為新興技術。

行為監控將是未來兩至四年內的一種新興保護技術，當物聯網設備執行了異常或未經授權的操作時，它可以檢測出這些操作，並且採取相應行動。作為針對零日攻擊或憑據偷竊的一種防禦手段，行為監控具有尤其重要的意義，能夠規避傳統的安全陷阱。在物聯網設備或其控制器上檢測到異常活動時，無論這些異常活動是基於時間（為什麼在凌晨 2 點請求此活動？）、基於其他物聯網設備的上下文（為什麼此閥門在相關進程沒有運行時打開？）、基於黑名單（汽車的製動系統應該始終無法遠程禁用），行為監控功能都可以停止命令，並採取即時行動來減輕威脅，或者提示用戶按說明操作。

物聯網系統實施的網路安全保險和風險管理將會發展。

物聯網設備和系統中的漏洞將會加大風險。由於物聯網設備具有諸多優勢，公司和消費者仍將採用這些設備，但公司要努力管理它們帶來的風險。保險服務也將應運而生。企業和保險公司必須定義和監控最低工作要求，適應不斷演變的法律和管制環境。由於成功的物聯網攻擊可能帶來的損害，保險服務將成為物聯網系統計劃的一個不可或缺的部分。

總結

過去幾年內，共有數十億部物聯網設備投入運行，也帶來了切實存在的網路攻擊威脅。但是，要謀劃如何從攻擊中牟取非法經濟收益，犯罪分子還需要一定的時間，因此針對這些設備的成功攻擊數量很難大幅增加。

物聯網的採用極大地增加了攻擊面。由於物聯網設備的安全性較差，加上製造商犯下的低級錯誤，這一問題將會變得更加複雜。其中有些漏洞將被作為初始攻擊媒介利用，讓攻擊者能夠進入控制、監控和資訊系統。勒索軟體最可能成為近期的重大威脅。收集來自物聯網設備的資料的聚合點也將成為近期的主要攻擊目標。

消費者隱私洩漏，立法機構對公民關注問題的回應措施，都將成為媒體報導的熱點。但是，物聯網設備實現的便利和效率遠大於弊端，因此採用率仍會居高不下。各個司法轄區的法規存在很大差異，滯後於市場發展，訴訟將在指引物聯網市場發展方向上扮演重要角色。

供應商將採取很多回應措施，以鼓勵和支持市場採用。新加密選項、芯片嵌入的安全和隱私功能、用於管理和保護物聯網設備的設備控制系統、物聯網設備的行為監控都將快速推出和演進。

消費者將會更深刻地認識到個人資料的內在價值，這也是一大重要變化。消費者期望供應商提供共享物聯網設備收集的個人資料的更多選項，包括補償。

2017 年預測

分享反饋意見

2017 年預測

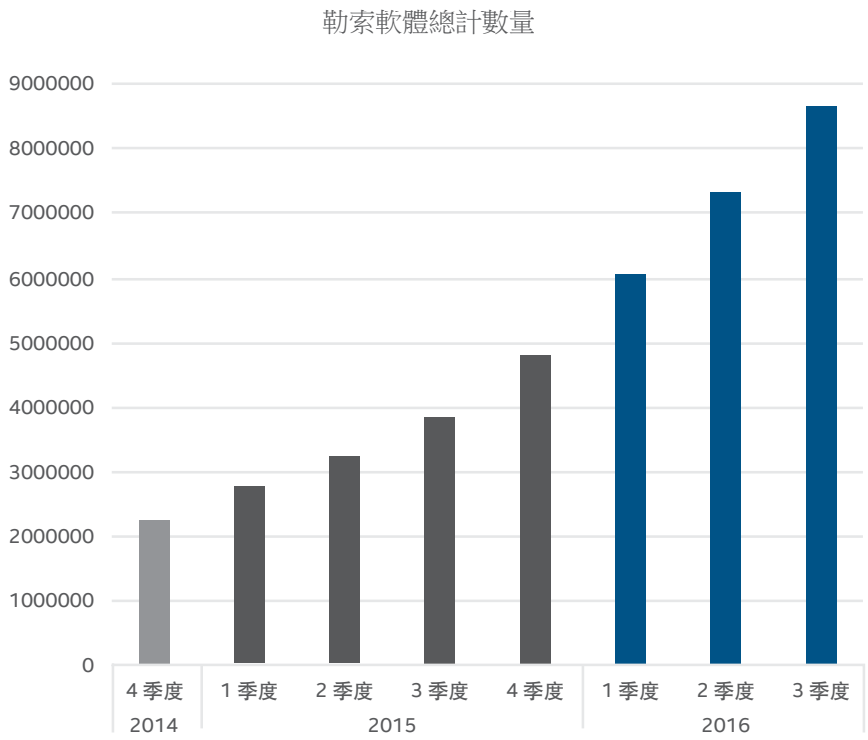
勒索軟體將在 2017 年下半年衰退

—Christiaan Beek

我們預測，2017 年下半年，勒索軟體攻擊的規模和效果將下降。

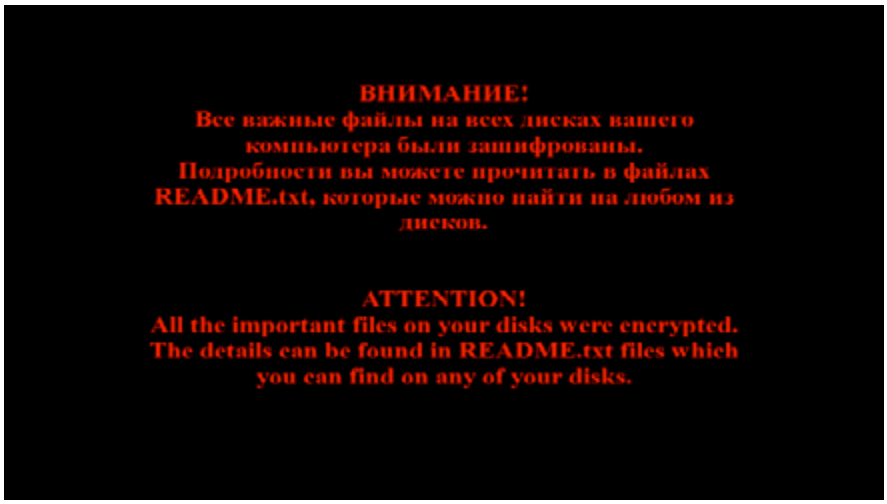
在 2017 年下半年之前，勒索軟體仍將是一大嚴重威脅。2017 年上半年，“勒索軟體即服務”模式、在黑市上出售的定制勒索軟體、來自開源勒索軟體代碼的創意衍生攻擊方式仍將肆虐橫行。勒索軟體在所有行業和地區都產生了影響，迫使安全行業採取斷然行動。我們預測，截止 2017 年底，由於“No More Ransom!（停止勒索）”協同作業等計劃開展，反勒索軟體技術的發展、持續執法行動等因素，勒索軟體的規模和效用將會降低。

勒索軟體的概念最先出現在上世紀 90 年代。比特幣推出之後，2013 年首次被 CryptoLocker 勒索軟體系列用於勒索贖金，這也為匿名勒索支付打開了方便之門，讓攻擊者能夠逍遙法外。CryptoLocker 和 CryptoWall 等勒索軟體“先驅”的創建者來自銀行木馬領域，在如何實施成功的網路犯罪方面，他們具有豐富的經驗。他們很快汲取了重要經驗，當攻擊減緩時，能夠迅速調整和改變他們的基礎架構和代碼。有一些團伙將繼續從事勒索軟體攻擊，尋找牟取非法經濟收益的新方式。當前，我們的對手是很多規模較小、不太複雜的團伙，他們被有組織團伙創造的可觀收入吸引。正如 Cyber Threat Alliance 的 *CryptoWall 3.0 威脅報告*所述，來自單個勒索軟體系列的收入可能超過 3.25 億美元。正如我們多次討論的那樣，由於有了這些成功實例，導致勒索軟體系列和攻擊大幅增加。犯罪分子希望發掘這條生財之道，他們或者結成聯盟，或者使用公共代碼。 2017 年，隨著安全行業和國際執行機構聯手主動檢測和回應這些案件，這些小規模攻擊行動將會有所減少。



資料來源：McAfee Labs 2016 年。

此外，安全行業還開始開發工具和功能，以協助公司抵禦勒索軟體。在 2016 美國 Black Hat 大會上，Intel Security 的進階威脅研究團隊展示了針對物聯網設備的勒索軟體概念驗證，包括以汽車的車載資訊娛樂系統為目標的勒索軟體，它能夠控制汽車的製動系統，直至車主支付贖金。該進階威脅研究團隊的研究重點是威脅的未來趨勢，並且參與行業協作，旨在讓人們了解勒索軟體，並在早期階段減小這些勒索軟體威脅。



比特幣混幣：中斷比特幣的發送地址與目標地址之間的連接。

為勒索軟體氾濫打開了方便之門的虛擬貨幣的前景如何？比特幣能否生存下來？勒索軟體攻擊者是否放棄比特幣並尋找新的支付方法？即便使用比特幣混幣，也不足以阻止交易鏈接分析。另外，其他一些比特幣服務在 Bitcoinference 會議上遭到與會者批評，他們抱怨有些服務沒有混幣，超節點使用不安全，可能暴露身份。因此，我們預測勒索支付方法將會轉向 Monero 和 Zerocoin/Zerocash 等虛擬貨幣。

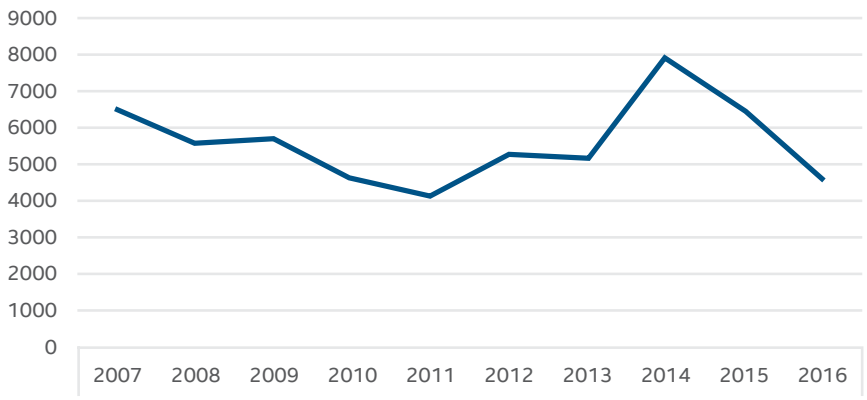
針對 Windows 的漏洞利用降溫，而針對其他平台的漏洞利用愈演愈烈

—Bing Sun、Haifei Li、Stanley Zhu 和 Debasish Mandal

近年來，利用客戶端軟體漏洞的難度顯著加大，從而提高了通用可靠的漏洞利用的開發成本。為了成功地滲透最新操作系統（例如，在 64 位 Windows 10 操作系統上運行的經過全面修補的 Microsoft Edge 瀏覽器），攻擊者必須利用進階攻擊技術，將多個高質量漏洞組合在一起。雖然在一些駭客大賽上（例如 Pwn2Own 2016）已經展示了成功的攻擊，但我們尚未見到先進的漏洞利用方法，例如那些自動散佈型的漏洞利用。我們懷疑這些漏洞利用手段僅適用於少數人，僅出現在非常重要的進階攻擊中。

發現的新漏洞數量

美國國家漏洞資料庫



截至 2016 年 9 月 20 日的数据。

我們相信，對 Windows 和 Flash 中的漏洞的利用將繼續下降，但是以基礎設施軟體和虛擬化軟體為目標的利用將增多。

回顧 *McAfee Labs 2016 威脅預測報告*，我們的很多漏洞利用預測已經成為事實。基於我們今年的觀察，我們期望對 2017 年的漏洞利用趨勢的預測達到相同的成功率：

- Adobe Flash：它仍然是基於漏洞的自動散佈型攻擊的主要目標。在安全公司 2016 年發現的所有零時差漏洞中，Flash 零時差漏洞（例如 CVE-2016-4117 和 CVE-2016-1019）佔據了大約 50% 的比例。由於降低風險的關鍵功能（向量長度 Cookie 檢查）在 2015 年 7 月推出，能夠阻止很多 Flash 漏洞利用，我們在 2015 年就預測 Flash 漏洞利用熱潮將在 2016 年降溫。因此，自動散佈型 Flash 漏洞利用在 2016 年顯著降低（截止撰寫本文時僅有 4 種，而在 2015 年有 11 種）。在加入降低風險功能之後，一種新型的 Flash 漏洞利用（使用 ByteArray 和 BitmapData）很快出現（CVE-2015-7645）。Adobe 還在繼續為 Flash 添加降低風險的功能，例如 ByteArray 長度 Cookie 檢查、獨立堆、系統堆、內存保護器。雖然這些新功能都並不完美（有些還會引發新問題），但總體而言，它們會增加漏洞利用的難度。因此，我們認為，將 Flash 作為一種攻擊媒介的現象將在 2017 年繼續減少。尋找 Flash 中的漏洞變得日益困難，而利用漏洞更是難上加難。
- Microsoft Internet Explorer 和 Edge：正如 2016 年威脅預測報告所述，針對 IE 和 Edge 的攻擊仍將保持很低水平。今年截止目前，尚未發現自動散佈的真正 IE 零日利用。雖然 CVE-2016-0189 和 CVE-2016-0034 漏洞利用是從瀏覽器傳播和執行的，但它們實際上分別是腳本引擎和 .Net 框架的漏洞。隨著攻擊面減小（沒有文檔模式、沒有 Visual Basic 腳本、沒有瀏覽器幫助程序對象和 ActiveX、沒有 Silverlight 等）和風險減輕功能增強，Edge 成為更加安全的瀏覽器。自從 Edge 發布以來，我們還沒發現任何自動散佈的針對 Edge 的零日利用。總體而言，Microsoft 瀏覽器的風險減輕功能似乎非常有效。有些風險減輕功能幫助我們消除了特定類別漏洞（例如，自推出獨立堆和記憶體保護功能以來，“釋放後使用”缺陷顯著減小），而其他一些功能讓漏洞利用變得更加困難。Control Flow Guard 是最關鍵的風險減輕功能之一，它可以防止漏洞利用劫持程序的執行流。我們預測，IE 和 Edge 漏洞利用在 2017 年將變得更加困難，特別是在 64 位平台上，創建和控制特定記憶體佈局將具有極大挑戰性。
- Java、PDF 和 Microsoft Office：2016 年，針對 Java、PDF 和 Office 應用程序的攻擊沒有什麼變化。考慮到龐大攻擊面和代碼複雜性，我們曾經認為 Office 漏洞利用將會顯著增長。但是，這種情況並未發生。原因可能是 Office 缺乏腳本語言支持，使得攻擊者很難開發漏洞利用。另一方面，我們預期不會看到基於 Office 的其他類型功擊（例如基於宏的勒索軟體）在 2017 年氾濫。

- Windows 內核：雖然一些風險減輕功能（主管模式執行保護、Win32k 系統調用篩選、內核地址空間佈局隨機化改進、字體解析遷移到用戶模式）已經推出，但內核模式漏洞利用仍然非常猖獗。此外，這些漏洞通常是對抗應用程序沙盒（例如 AppContainer）和實現權限提升的最有力武器。它們已經在零日攻擊 (CVE-2016-0165/0167) 和駭客大賽 (CVE-2016-0176) 中得到很好的展示。考慮到攻擊面龐大，內核空間提供的保護和風險減輕功能相比於用戶空間比較薄弱，我們預測內核模式漏洞利用在 2017 年仍會氾濫。
- 基礎架構軟體：2017 年，對基礎架構漏洞的攻擊將非常活躍。看一下 OpenSSL 公告列表，我們會發現每個版本都對很多漏洞進行了修補。除了 OpenSSL 之外，我們還可在其他開源軟體中找到關鍵漏洞，例如 CVE-2015-7547（glibc DNS 客戶端中的基於堆棧的緩衝區溢出）和 CVE-2016-5696（一種 Linux 缺陷，可利用來劫持網際網路流量）。
- 傳統組件與新功能：雖然大多數惡意軟體編寫者的重點攻擊目標是新功能，例如適用於 Linux 的 Windows 子系統，它有 216 種新系統調用和 700KB 代碼，但也有一些編寫者將目標瞄準了傳統組件。自從在 glibc 中存在 15 年以上的關鍵漏洞 GHOST (CVE-2015-0234) 被發現以來，安全研究人員已經開始重新檢查傳統代碼。例如，2016 年，我們在 Web Proxy Autodiscovery Protocol 中發現了嚴重錯誤 (BadTunnel)。該錯誤已經在代碼中存在了 20 年。由於重要傳統組件的安全性多年以來一直被忽視，安全研究人員已在著手消除長期漏洞。我們預期將在 2017 年發現和修復更多問題。
- 虛擬化軟體：隨著雲技術的持續快速採用，虛擬化安全成為一個熱門話題，吸引了安全研究人員和攻擊者的關注。很多深入研究結果已經公開。 7 月，我們對 Xen 管理程序中的一個關鍵漏洞進行了修補，該漏洞允許 “Guest to Host Escape” （ “Po Tian” 漏洞，CVE-2015-7835）。 9 月，Intel Security 的進階威脅研究團隊發現了 Xen 漏洞 XSA 188，該漏洞會導致 Linode 雲託管服務重新啟動基於 Xen 的服務器。我們還記錄了 VMware 中的關鍵錯誤，例如 CVE-2016-5332、CVE-2016-2077 和 CVE-2016-2079。Microsoft Hyper-V 並不能免於風險：我們發現了與 Hyper-V 相關的多個 CVE（MS16-045 和 MS16-046）。此外，Microsoft 的 Windows 10 中的基於虛擬化的安全/虛擬安全模式也成為新的功能目標；我們已經找到和公佈了它的一些安全問題。另一方面，雖然人們已經在虛擬化軟體中發現了很多漏洞，但與成熟的瀏覽器漏洞利用相比，虛擬機 (VM) 攻擊仍然缺乏系統和通用的漏洞利用技術及方法，無法全面覆蓋特定類型的虛擬機安全問題。大多數虛擬機逃逸案例高度依賴於漏洞本身，例如 CVE-2015-7835、CVE-2016-3710 和 CVE-2015-7504。由於虛擬機已經成為攻擊者的目標，我們相信針對虛擬化軟體的系統化漏洞利用和先進攻擊手段的出現只是一個時間問題。可能就在 2017 年發生。

- 安全產品：2016 年，我們已發現了安全產品中的大量嚴重漏洞。年初，Google 研究人員在 FireEye 裝置中發現了一個嚴重的遠程代碼執行漏洞。之後，Google 研究人員在大多數主要防惡意軟體供應商的產品中發現了一些漏洞。而在夏天，洩露的 Equation Group 資料暴露了大量針對各種防火牆產品的漏洞（包括若干未修復的零日漏洞）。毫無疑問，此趨勢也會在 2017 年延續。

富有經驗的攻擊者們越來越多地將威脅目標鎖定在硬體和韌體

— Yuriy Bulygin

軟體，包括操作系統和應用程序，毫無疑問必須依賴硬體才能正常運行。硬體漏洞可以侵蝕整個軟體堆棧的運行和安全。利用硬體漏洞可能威脅整個系統，所以無需攻擊軟體堆棧。此外，硬體被攻擊成功的系統如果不更換有漏洞的硬體，可能很難修復。最後，系統的基於軟體的安全機制和保護方法全部不值得依賴，因為這些安全機制和保護方法都以硬體未受損為前提。

不過，也有緩解因素。相比軟體堆棧，硬體不容易受到攻擊，而攻擊硬體幾乎始終涉及攻擊某種類型的硬體邏輯漏洞，而不是攻擊軟體堆棧中經常會發現的大量軟體漏洞。硬體攻擊面少導致攻擊複雜。因此，我們很少在硬體中發現漏洞，也很少發現攻擊者以硬體為目標或攻擊硬體成功。同樣，一般的惡意軟體幾乎從來不針對硬體。

過去幾年中，安全研究人員發現了一些硬體漏洞——包括微處理器和 DRAM 技術 [1、2、3、4] 中的漏洞，以及可用於實施與操作系統無關的邊信道攻擊的漏洞 [1、2、3]，這可能通過暴露位於相同位置的虛擬機來影響雲端環境 [1、2、3、4]。

計算機系統中往往有用於在該系統中初始化、引導和執行低級維護任務的特製軟體和硬體。此類特製軟體和硬體有自己的微控制器和軟體堆棧，通常稱為韌體。BIOS、統一可擴展韌體接口 (UEFI)、EFI 和 Coreboot 就是這樣的特製韌體。此外，USB、硬碟、固態碟、擴展卡甚至充電器之類外部設備通常有自己的韌體。

韌體的屬性使其成為了重大攻擊目標。韌體通常永久存儲在非易失性存儲（如閃存設備）中，可以完全訪問管理的硬體，並且隱藏得很好，難以被操作系統和安全軟體發現。系統韌體在操作系統接管控制前運行。此外，韌體不過是軟體，所以往往具有類似漏洞，但是內置保護措施和漏洞緩解措施卻更少。

威脅研究人員已證實可以通過系統韌體中的漏洞 [1、2、3] 對預啟動身份驗證實施攻擊，包括使用基於 Trusted Platform Module（如 Microsoft Windows BitLocker [1、2]）或 Windows Secure Boot [1、2、3、4] 的全盤加密攻擊系統。可通過預啟動攻擊安裝隱匿和持久性 Rootkit、後門程序或蠕蟲 [1、2、3、4、5]，以及破壞基於安全內核和隔離用戶模式以及 Microsoft Windows 10 中的 Credential Guard 和 Device Guard 之類虛擬化技術的可信執行環境 [1、2]。

除了系統韌體，安全研究人員還在 USB 設備 [1、2、3]、網卡 [1、2]、嵌入式鍵盤控制器 [1]、主板管理控制器 [1、2、3]、LTE/3G/GSM 基帶調製解調器 [1、2]、CPU [1、2]、電池 [1]、家用路由器 [1、2、3、4]、辦公打印機 [1、2]、IP 電話 [1]、ARM TrustZone 的韌體和安全軟體 [1、2、3、4、5] 以及其他許多設備中發現了韌體漏洞。

民族國家發起的駭客組織、行業間諜團體和有組織犯罪團體之類對手都對攻擊系統韌體非常感興趣。兩年前，Equation Group 對硬碟驅動器上的韌體發起了攻擊 [1]。2015 年，我們發現了這個 Hacking Team 的第一個商用 UEFI 韌體 Rootkit [1]。最近，Shadow Brokers 的一項聲明表明有理由相信該組織牽涉通過永久性植入攻擊 Equation Group 的網路防火牆韌體 [1、2]。

硬體和韌體是相當複雜的目標，但是成功攻擊它們則可以讓對手不為人察覺地永久訪問大量硬體資源，以及在系統的軟體堆棧中植入後門程序。我們預測到 2017 年，民族國家攻擊者之類高級對手將繼續在硬體和韌體中尋找他們可以攻擊的漏洞。我們相信高級對手有能力攻擊其韌體基於傳統 BIOS、(U)EFI，或固態碟、網卡和 Wi-Fi 設備之類其他設備類型上的韌體的系統。

我們預測到 2017 年，高級對手將繼續在硬體和韌體中尋找他們可以攻擊的漏洞。我們相信他們有能力攻擊其韌體基於傳統 BIOS、(U)EFI，或固態碟、網卡和 Wi-Fi 設備之類其他設備類型上的韌體的系統。這些高級漏洞中有一些可能出現在常見惡意軟體攻擊中。

這些高級漏洞中有一些可能出現在常見惡意軟體攻擊中。在 2017 年，我們將看到用於攻擊基於 UEFI 的操作系統啟動加載程序，甚至安裝韌體 Rootkit 組件的惡意軟體的 Bootkit 組件；用於攻擊基於虛擬化的可信執行環境（如 Windows 10 中的 VBS）的韌體攻擊；以及感染操作系統的早期啟動階段（包括啟動加載程序和韌體）的勒索軟體。

在防禦一方，我們可能會看到更多商用安全技術可以深入了解韌體和其他低級系統組件，而不只是傳統軟體堆棧提供的系統組件。

“無人機劫持”將威脅投放到了天空中

—Bruce Snell

無人機的主流化趨勢仍在延續。無人機最初不過是孩子的玩具，現在則作為發燒友有點奢侈的愛好真正“起飛”。無人機發展順利，正在成為承運商、執法機構、攝影師、農場主、新聞媒體等的重要工具。很難否認無人機現在對各種企業和政府機構的價值更大了。最近我們發現一架無人機被安裝了一套完整的駭客套件，可以在住宅、企業或者重要基礎設施的房頂著陸，還可以嘗試侵入局域網中。

在 2015 年，在 DefCon 展示了一次概念驗證攻擊，這次攻擊表明輕輕鬆鬆就可以接管玩具無人機。儘管接管孩子的無人機看起來很有趣，無傷大雅，但是一旦我們看到無人機的使用增加，潛在問題也會開始增多。

- 送件：Amazon 和 UPS 均已宣布計劃通過無人機送包裹。這為想賺快錢的犯罪分子創造了切實的目標。送貨無人機很有可能從專門位置起飛，所以很容易確定其交通模式。希望“劫持無人機”快件的人可以定位無人機的常規路線，然後等待目標出現。送件無人機一飛到空中，就可能被送到地面上，這樣犯罪分子就可以盜竊包裹。說句公道話，此類盜竊是否成功還兩說，因為不太容易知道包裹裡面有什麼，但是總歸有利可圖。
- 攝影隊：無人機的出現讓空中攝影現在變得簡單多了。快速搜索“攝影無人機”就可以返回多頁結果，這些結果指向業餘攝影師和專業攝影師都可以使用的高質量、昂貴的設備。這種高質量設備對犯罪分子的吸引力非常大，是他們實施無人機劫持的目標。犯罪分子把無人機弄下來就可以轉賣，真的是天降橫財。

- 私人禁飛區：已經發生了幾場事故，在這些事故中，有人被房屋上空的無人機惹惱，採取了主動措施（槍擊、扔石子等）來對付無人機。可利用無人機中的軟體漏洞在房屋周圍設立電子圍欄，幹掉飛得太近的無人機或使其改向。儘管這好像是哪些喜歡鄰里之間“老死不相往來”的人的福音，無人機在許多地方法律法規中還屬於灰色地帶。這個灰色地帶可能引發爭議，還可能為設立私人禁飛區的人招致法律訴訟。

- 執法：越來越多的執法機構借助無人機輔助監控和控制人群。在抗議或無特定目標槍手這樣氣氛高度緊張的場景中，警用無人機很容易成為躲避執法的人的攻擊目標。這種場景在動作電影中出現了無數次。壞人（或英雄）採取精心製訂的措施幹掉目標的安全資料源。現在，我們不在牆上安裝安防攝影機，而是把攝像機安裝到無人機上。隨著抗議者與駭客活動分子之間越來越混雜，擁有監控無人機擊落技術的抗議者的比例顯著增多。

這些攻擊如何進行？許多研究人員發現大量消費類無人機配備了開放端口和弱身份驗證方法，所以擁有合適設備的人可以向受害者的無人機發送指令。到目前為止，這還是人為參與程度極深的行為，但是就如同我們過去看到的那樣，通常遲早會出現可輕鬆繁殖的新利用手段。

商用無人機上發現的大多數漏洞都可以通過軟體更新輕鬆修復。當然，這需要製造商發布修補程式。雖然高端無人機的修補速度可能極快，廉價無人機卻可能飛很久後才會推出修補程式。正如我們在使用其他物聯網技術時的發現，設備一旦聯網，很快就會有人開始想辦法侵入。由於物聯網設備（包括無人機）往往沒有採取多少或者根本就沒有採取安全措施就匆匆趕著上市，所以很容易成功侵入。由於無人機通常設計成可以輕鬆、快速安裝，並且使用不加密的通信和大量開放端口，所以可能更容易侵入。

在 2017 年，我們將看到無人機被配有方向天線的筆記本電腦上運行的軟體從空中擊落。我們還將看到執法機構使用更多無人機監控人群，而抗議者將發起無人機攻擊侵入以通過方程快速除掉監控無人機。

根據我們的預測，2017 年無人機漏洞工具包將找到方法進入網際網路的黑暗角落。一旦這些工具包開始擴散，晚間新聞中遲早會出現無人機被侵入的新聞。即使沒有現成的無人機劫持工具包，我們也會開始看到與無人機有關的事故增多。

在 2017 年，我們將看到本地新聞報導有人厭煩了鄰居家的孩子操控無人機飛過他家後院。無人機被配有方向天線的筆記本電腦上運行的軟體從空中擊落，而不是被上了膛的鳥槍擊落。鑑於網際網路的病毒特性，這很快將在全球 Facebook 留言板上出現，並引發支持和反對此類行為的爭論，導致衝突升級和產生負面影響。

在 2017 年，我們還將看到執法機構使用更多無人機監視人群。一開始，抗議者的反應是朝警用無人機扔東西，但是後來抗議者會發起無人機攻擊侵入，通過方程快速除掉監控無人機。

政策制定者將如何應對這些事故？美國聯邦航空管理局已在匆忙制訂規則約束商用無人機的飛行條件和飛行區域，但是我們還是有許多用戶需要面對，並且必定有一些我們還沒有考慮到。雖然商用飛行的增長速度緩慢，商用無人機的使用卻在，疾飛猛進，讓政策調整者艱難應對。

移動威脅將包括勒索軟體、RAT、被破壞的應用市場

—Fernando Ruiz

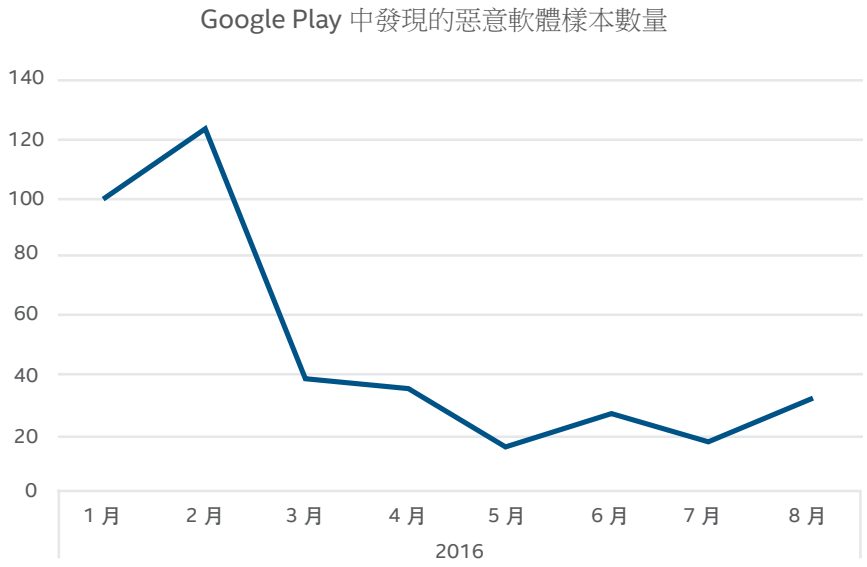
McAfee Labs 發現移動惡意軟體在 2017 年將保持增長勢頭，主要威脅包括勒索軟體、銀行業務特洛伊木馬程序和遠程訪問工具。

根據我們的預測，在 2017 年，移動勒索軟體將繼續發展，但是移動惡意軟體作者的關注重心將改變。攻擊者將把移動設備鎖定與其他類型的攻擊（如憑據盜竊）結合，以便訪問銀行帳戶和信用卡等對象。

McAfee Labs 的移動惡意軟體研究團隊已收錄了大量針對移動設備的勒索軟體，特別是在 2016 年第 2 和第 3 季度。範圍涵蓋用於鎖定屏幕的小概念驗證到旨在威脅外部記憶體的大型 crypto 惡意軟體。第 2 和第 3 季度的一個引人矚目的移動勒索軟體系列是 Android/Jisut。這款勒索軟體用於更改移動設備的鎖定 PIN，並要求通過比特幣或預付費卡付款。

根據我們的預測，在 2017 年，移動勒索軟體將繼續發展，但是移動惡意軟體作者的關注重心將改變。由於移動設備通常會將資料備份到雲，所以直接勒索收費才解鎖設備通常很難成功。因此，移動惡意軟體作者結合了移動設備鎖與其他攻擊形式，如盜竊憑據。例如，我們今年發現安全行業確定為移動勒索軟體的 Android / Svpeng 之類系列現在正在變異為針對銀行業務憑據，想方設法從受害者帳戶盜竊資金。我們相信在 2017 年，銀行業務特洛伊木馬程序將出現，出自勒索軟體作者之手。這類惡意軟體結合移動設備鎖和其他勒索軟體功能與傳統的中間人攻擊，旨在盜竊主要和次要身份驗證要素，讓攻擊者可以訪問銀行帳戶和信用卡。

我們在 2016 年看到了針對 Android 的遠程訪問工具 (RAT) 的擴散。它們偽裝成合法的支持實用程序，並在第三方市場提供。這些 RAT 用於窺探 Pokémon Go 發燒友、恐怖分子支持者和安全人員，並將社交網路用作傳播渠道。鑑於商用間諜軟體和 RAT 的發展及其複雜性，我們預計 2017 年將有更多受害者成為這種惡意軟體的無差別攻擊目標。有漏洞的智能手機是完美的間諜平台，任何知道攻擊方法的人都可以控制。



儘管我們和其他方建議僅從可信應用程序市場下載應用程序，此步驟還是被證明不足以保證所有用戶的安全。2016 年，Google Play 中有幾次出現了惡意應用程序，即使很快就被刪除。我們強烈建議用戶在 2017 年即使從可信市場安裝應用程序，也要關注應用程序的評論。這樣的關注加上有效的防惡意軟體應用程序，對防止智能手機被感染至關重要。

從未知且不可信的市場下載應用程序的危險性始終更高，這一點在 2017 也不會改變。此類危險包括鏈接到其 URL 在 Instagram、YouTube 視頻或 Tweets 上顯示的應用程序。這些全部都可以傳播惡意軟體或間諜軟體。使用流行的社交媒體可能導致被感染，因為熟悉的環境可能引誘用戶忽略安全風險。

物聯網惡意軟體打開家的後門

—Bruce Snell

消費電子產品繼續迅速增長。特別是物聯網消費產品，這個領域到 2019 年預計將達到大約 18 億台設備。這個市場俗稱“智能家居”或“互聯家居”，包含各種成功品牌和產品，以及大量想擠進來的小公司。

我們在商業上有“最簡可行產品”這一概念，簡稱 MVP。儘管 MVP 這個縮寫常見的含義是“最有價值球員”，這裡卻指的是擁有足以讓先行者願意購買產品的最少產品功能。家居物聯網市場“粘性”極高，顧客一旦購買智能自動調溫器或照明系統，可能就不會更換它們。因此，搶市場既快又激烈，家居物聯網設備製造商通常會採用 MVP 方法。例如，他們中的許多會依賴第三方代碼庫縮短開發流程和降低成本。

這樣的魯莽行為和對第三方軟體的依賴可能會引發安全威脅。良好的編程實踐要求開發人員徹底檢查產品中的所有第三方代碼庫。不幸的是，匆忙開發 MVP 並上市以打敗競爭對手時，代碼通常在經過最少的測試後拋出，依靠發布後修補程式來更正出現的缺陷。當開發人員面臨時間壓力時，往往會忽視安全。即使考慮到了安全，也會這樣做。我們發現一些消費類物聯網產品帶有嚴重的安全漏洞，並且多年都未曾修復。

我們把這種場景再升級一下。如果網路犯罪分子想要找到方法進入安全性極低的家居網路中的各種產品，在消費物聯網設備中植入後門程序就是一個很好的方法。幾年前就出現了一個這樣的好例子，當時天星 N9500 山寨了三星智能手機並在各大在線市場中銷售，而這款手機的韌體中就安裝有惡意軟體。

我們將發現廣泛使用的庫或消費物聯網空間中直接嵌入的庫內隱藏惡意代碼。此類代碼將隱藏在 HTML 渲染庫、網路庫和攝影機庫之類對像中。

該惡意軟體不針對具體製造商，也不嘗試攻擊製造商的代碼庫，而是更輕鬆地創建一個廣泛使用的代碼庫的“免費”版本，該版本中包含後門程序，並提供給眾多物聯網設備製造商。我們已在 Android 端廣泛使用的代碼庫中發現了惡意代碼，所以不難想像物聯網設備也會出現這種現象。

在接下來的一到一年半中，我們將發現廣泛使用的庫或消費類物聯網空間中直接嵌入的庫中隱藏惡意代碼。我們也會發現消費類物聯網設備應用與智能手機應用之間進行某種形式的合謀。

2017 年我們將在哪些地方發現惡意代碼？從攻擊者的角度來看，代碼庫的迷人之處有一部分在於可以直接訪問操作系統或設備硬體的關鍵組件。因此，我們預計將發現以下地方隱藏著惡意代碼：

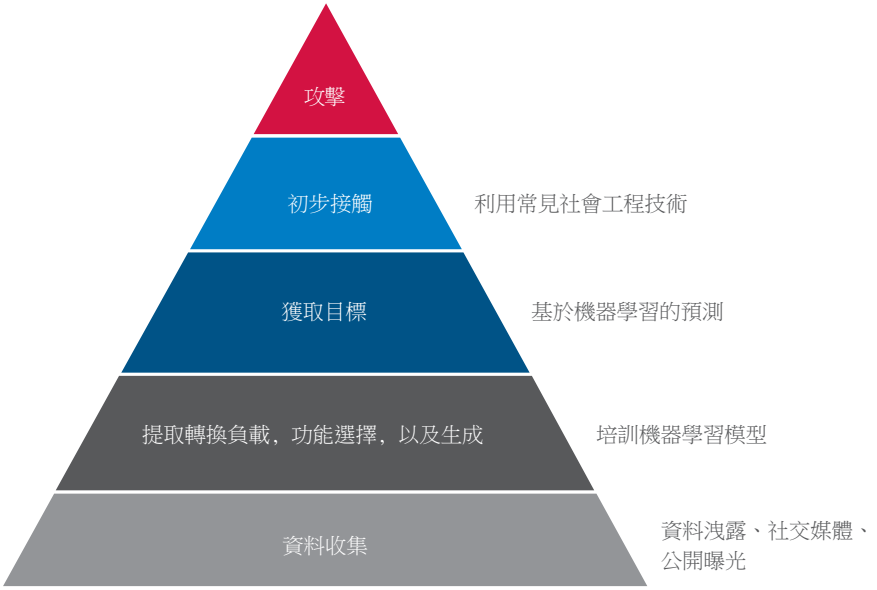
- HTML 渲染庫：某些物聯網設備擁有的管理界面不過是用於執行配置的網頁。自然就會在可在這些網頁渲染時直接訪問它們的代碼中隱藏惡意代碼。這樣就可以讓惡意軟體收集用戶名和密碼，並在管理界面本身中執行惡意軟體。管理家裡的智能燈時，沒有誰會懷疑可能被感染！
- 網路庫：我們往往以為家庭網路是安全的。當惡意軟體在家庭網路中取得立足點之後，通常就可以探查該網路的所有流量，因為家庭網路通常非常簡單，並且還開放。惡意軟體探查用戶名和密碼之類資訊，並將其發送到其他地方的控制服務器。由於惡意軟體可以直接訪問該網路，所以通常很難注意到此行為。
- 攝影機庫：除了攻擊托兒所或住宅安全系統的攝影機之外，難道還有更好的方法可以跟踪人而不引起疑心？惡意軟體藏在安全攝影機後面，所以可以捕獲和發送毫無戒心照常生活的對象的照片和視頻。

我們預計，2017 年上市的部分家居物聯網設備中將安裝有後門程序。鑑於這些設備的特徵，窺探和盜竊個人資訊這樣的行為可能多年都不會被發現。

機器學習加快了社交工程攻擊

—Eric Peterson

隨著機器學習在教育、商業和研究領域越來越普及，最近幾年機器學習工具包、文檔和教程的出現呈爆發趨勢。短短一個小時內，一個人就可以通過培訓學習到分佈式架構中的大型資料集上的複雜模型。在 2016年，我們已經看到發燒友和專業資料科學家教會了機器如何寫莎士比亞式十四行詩、作曲、像畢加索一樣畫畫，以及打敗職業圍棋棋手李世石。學習週期變得越來越短，並且所有人，包括網路犯罪分子都可以輕易接觸。安全是一場軍備競賽，而網路犯罪分子則在機器學習的幫助下調整他們的手段。

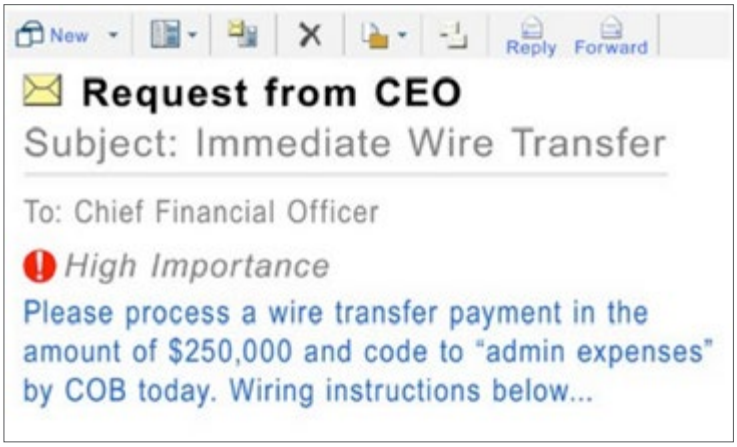


我們相信網路犯罪分子正在利用機器學習挑選受害人。現在已經有了用於執行目標選擇背後復雜分析的工具，還有超多公共資料源可用於創建和訓練惡意機器學習算法。我們預計在 2017 年，機器學習的普及將加速，並促進社交工程攻擊的進步。

我們今天跟踪的幾個持續性威脅中的一個是 FBI 標記的商務電子郵件攻擊 (BEC) 詐騙，該威脅从 2015 年年初開始一直在升級。通過 BEC 詐騙，詐騙分子以企業內的財務負責人為目標，通過嫻熟的社交工程誘騙其將資金轉入詐騙者的銀行帳戶中。在某些情況下，攻擊甚至會配合公司高層的出差日程，以提高詐騙的成功機率。據 FBI 稱，盜竊的金額超過 30 億美元，受害者遍及美國的所有 50 個州和其他 100 個國家或地區。儘管還不清楚如何選擇受害人，但是發起攻擊前顯然進行了相當多的研究。我們相信網路犯罪分子正在利用機器學習挑選 BEC 和類似詐騙的受害人。

在熟練應用的情況下，機器學習擁有解決重要、複雜、真實業務問題的潛能。回歸算法可用於預測價值，聚類算法可揭示資料集中的結構，而異常檢測算法則可用於找到異常資料點。而在底層，這些算法背後的數學原理非常高級，許多人都接觸不到。正如我們在 Trillium、Zeus 和 Angler 之類現代惡意軟體工具包中的發現，惡意軟體作者在工具包的幫助下，造成的危害遠遠超過他們個人擁有的技能可以造成的危害。我們發現，在資料科學領域，Google TensorFlow、Numpy、Scikit¬learn、Pandas 等機器學習工具和庫起到了同樣的加速作用。機器學習工具可以讓安全負責人如虎添翼。如果想當然地以為犯罪分子不會採用這些強大的工具，那就是我們的失職。

非法與合法商業模型之間的一個共性就是底線。不管從哪方面的角度出發，企業都在不斷磨礪技藝，致力於在降低輸入的同時提高輸出。以 BEC 攻擊模型為榜樣，並可獲取用於執行複雜的資料分析的機器學習工具的前提下，我們可以開始了解機器學習和犯罪活動的融合。這張攻擊三腳架的第三隻腳是資料。



僅僅在 2016 年，就有3萬位美國司法部僱員、21st Century Oncology 的 220 萬份患者記錄、150 萬份 Verizon Enterprise Solutions 客戶記錄和 Yahoo、Hotmail 和 Gmail 等各大主要電子郵件提供商的大約 1500 萬個帳戶遭到洩露。這些洩露中許多的資料已被商品化並在開放市場中出售，leakedsource.com 就是這樣的市場，它聲稱自己的資料庫中有 20 多億條記錄。從另一個角度來說，美國證券交易委員會的 EDGAR 服務則提供對超過 2100 萬份文件的免費訪問。攻擊者遊走在社交媒體資訊、盜竊的資料倉儲和公開披露的商業資訊之間，訪問超過預測模型培訓所需的資料量，以確定高價值目標。

我們來把 BEC 詐騙的生命週期視為一場可受益於使用機器學習的攻擊。網路犯罪分子知道如果向財務負責人發送精心撰寫的電子郵件，聲稱自己是組織的領導者，並且指出情況緊急，就有一定的機率欺詐成功。一些誘發攻擊的環境因素可以增加成功的可能性。從攻擊者的角度來說，回答公共域中的基本問題就可以讓他們收穫寶貴的資訊：組織內是否存在破綻的跡象？最近是否在為收購或剝離準備 SEC 文件？社交媒體帖子之間是否存在隱含多位員工跳槽線索的關聯？是否有戰略討論發給個人或私人地址或從個人或私人地址收到戰略討論？這些類型問題的每一個回答都可能充當機器學習算法的特徵向量。花時間努力工作，就可以開發可用於成功實施詐騙的模型，並用於預測未來的攻擊是否成功。

威脅實施者已經開發了可用於成功實施 BEC 詐騙的攻擊模型。現在已經有了用於執行目標選擇背後復雜分析的工具，還有超多公共資料源可用於創建和訓練惡意機器學習算法。展望 2017 年及以後，我們可能甚至會看到提供基於機器學習算法創建的“目標獲取即服務”的資料盜竊承辦商。我們預計在 2017 年，機器學習的普及將加速，並促進社會工程攻擊的進步。

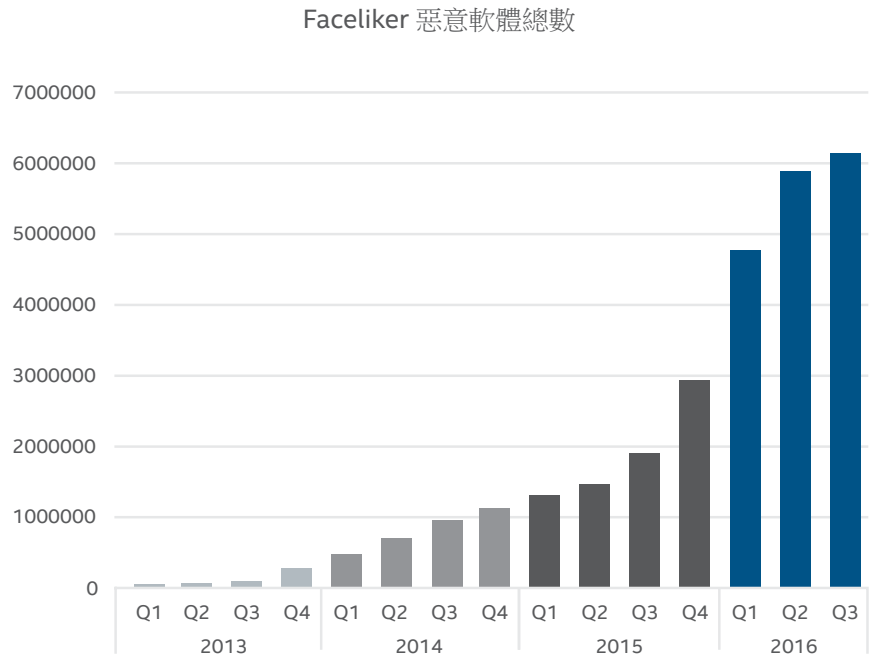
虛假廣告和買”讚”呈爆炸式增長，危及信任

—Craig Schmugar

虛假的”讚”、廣告、產品和服務評論以及網路安全警告、警報等將導致網際網路的可信度降低。

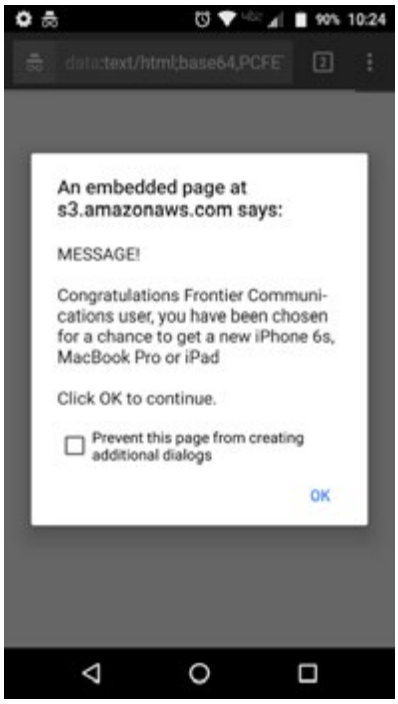
每位網際網路用戶在決策時都遭受資訊轟擊：點哪個，看什麼，在哪里花錢。這些選擇催生了一門上十億美元的網路經濟，由於這樣大的一筆資金處於危險之中，所以不法實施者在不斷找辦法佔他人的便宜。信譽是許多決策者對所做決策有信心的關鍵，所以有些人會想方設法利用信任。

最流行的一種信任建立方法是利用用戶反饋歷史記錄。據估計，一條 Facebook “讚”價值高達 200 美元或更高。因此，出現了收費點”讚”的服務。儘管 Facebook 在打擊此類實體，這仍然是一場貓鼠遊戲，最近的交手錶明惡意軟體作者在花錢讓這只“老鼠”活得更久。與付費讓低工資工作者點擊鏈接的“點擊承包”不同，點贊惡意軟體以用戶會話為依托，所以點擊行為更有可能貌似合法。

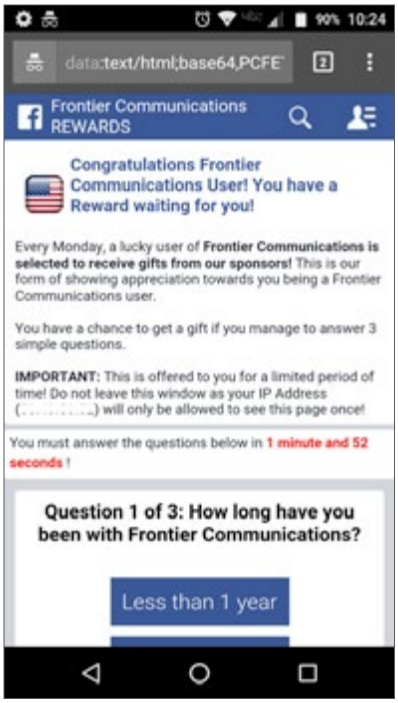


Faceliker 特洛伊木馬程序變體增多。

虛假廣告已經紮根，越來越多的廣告網路劫持用戶的瀏覽會話，無論其目的是發送惡意軟體、實施詐騙還是沒完沒了的調查。可能這些內容干擾您的網際網路體驗時您只覺得麻煩，但當通過一級網站進行交付時，其影響則令人震驚。



借助 Amanzon AWS，在澳大利亞某一主流網站實施的廣告劫持，可讓手機振動。



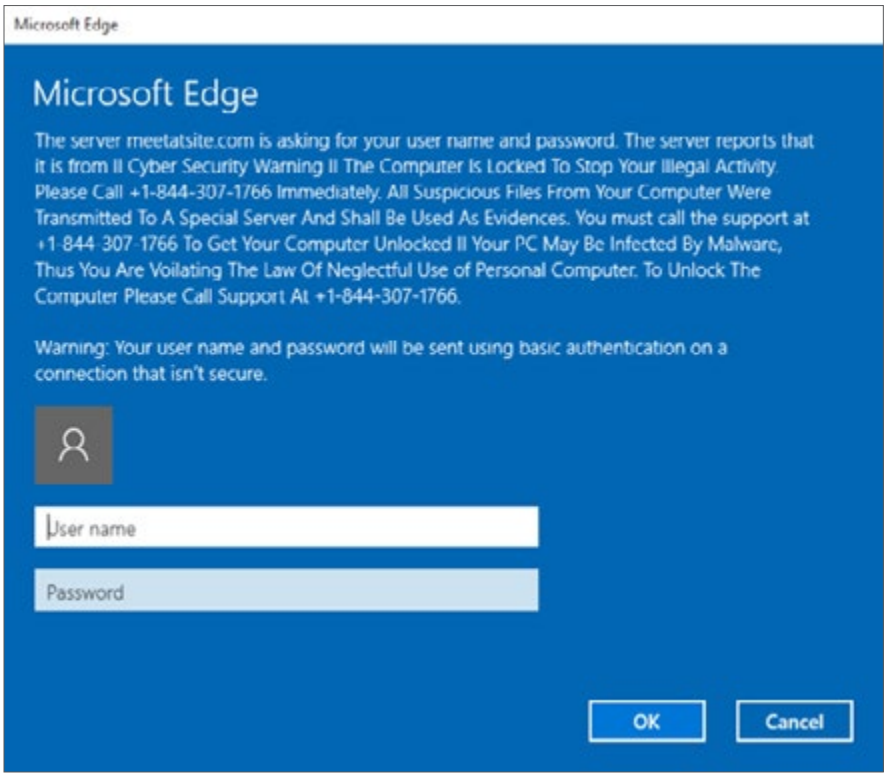
一個有害的頁面，可讓用戶不能訪問所需網站。

我們經常在一級電子商務網站上發布的產品評價中尋找其他偽造內容。由於當今世界發展迅猛，許多消費者依賴方便、一目了然的產品和服務背書。難怪賣家抵抗不了人為拔高評分的誘惑。文本、音頻和視頻評價都可以從願意創建內容的人那裡購買或從腳本讀取。

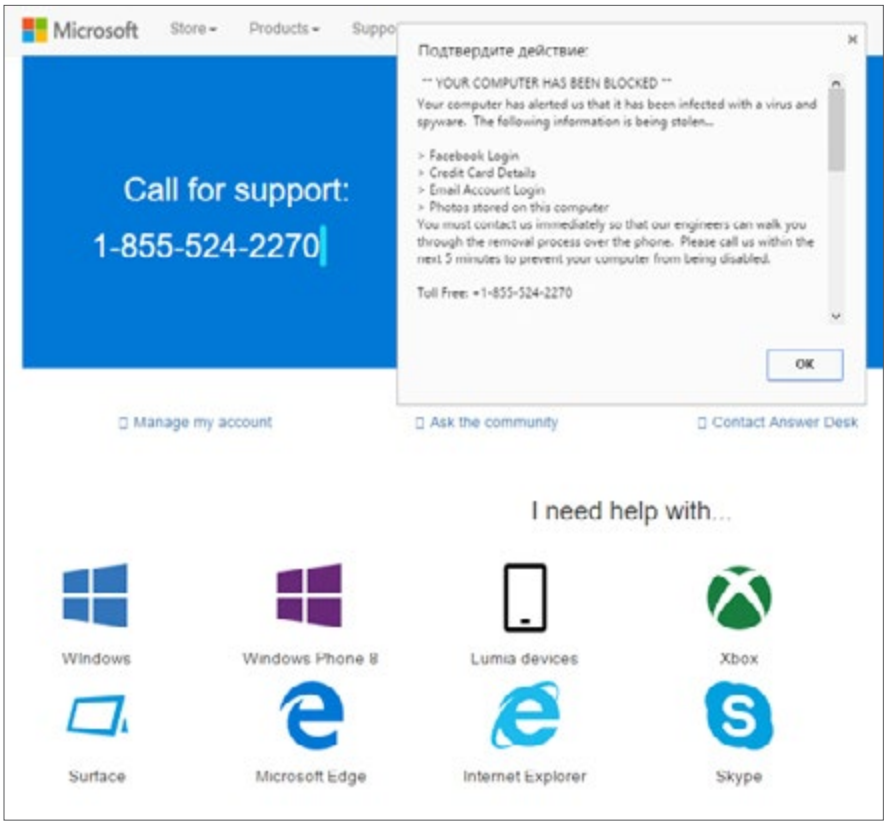
借助來自最新的基於機器學習的防禦技術，安全業界領導者正在打擊此類行為，不僅針對評價者，還針對因此類行為受益的賣家。在過去幾年奠定的基礎上建立了新的第三方網站，如 FakeSpot 和 ReviewMeta；我們可以預計這種消費者權益保護將在來年全年繼續加強。

2016 年出現了一些防禦進步，如增強統計與動態惡意軟體檢測功能和改進殭屍程序識別。可以預料騙子在 2017 年將會通過為當前目標雙倍下注或轉向抵抗力最弱的目標來反擊。對於惡意軟體作者，這可以通過創建“假面獵手”應用程序（惡意例程添加到合法軟體副本中）或複合程序（既可以充當合法程序又可以充當惡意軟體的單個應用程序）實施。這些工作將讓用戶和防禦掃描程序更分不清楚真假之間的界限。

今年早些時候，美國聯邦通訊委員會宣布將與業界合作終結錄音電話。此行動在 2017 年可能產生的影響有待觀察，但是我們再次預計那些生財之道受到影響的人將繼續另闢蹊徑。預計其中一項結果是虛假網路安全警告和備選虛假警報（如假 Windows 安裝警報）惡意軟體將增多，這些警報要求用戶發起呼叫。這些警告通常會誘騙毫無戒心的上網用戶，讓天真的受害者以為無法訪問自己的系統。



來自以為是 Microsoft 頁面的虛假警告，該警告通過要求用戶致電支持人員，索取訪問代碼以取消阻止內容



這個詐騙頁面覆蓋整個屏幕，以便將自己顯示為合法的 Microsoft 網站。還播放音頻警報，要求用戶致電某個號碼以獲取支持。

事實證明，得益於 Pokémon Go 取得的巨大成功，2016 年是增強現實進入主流的一年。用戶接受“虛假”成為逼真體驗的一部分，在這款遊戲中迷失自我。毫無疑問，除了這個成功故事，還會有更多即將到來。在完全融合了真實與虛假的世界中，我們是不是發現越來越難區分惡意虛假和渴望的想像？

廣告戰升級加劇惡意軟體傳播

—Adam Wosotowsky

廣告商與廣告攔截程序之間的這場貓鼠遊戲還將延續。惡意軟體分銷商將使用用於繞過活動內容攔截程序的廣告商技術實現惡意軟體的“隨看隨下”下載。

安全研究人員在危險的網際網路地盤上花了大量時間，這裡充斥著被攻破的網站和“隨看隨下”惡意軟體下載。為了以相對安全的方式瀏覽這塊地盤，我們使用瀏覽器的安全附加項禁用活動內容，閱讀原始網站內容代碼，訪存使用不同服務器的位片段，以及使用通過重載避免感染本地計算機的虛擬機。這些預防措施可以將“上網”轉化為難得多的過程。

大多數用戶無需做這麼多。普通用戶主要關心瀏覽器是否可用，要訪問的網站是否可以訪問。但是彈出廣告突然就冒出來了。網站開始隱藏在大量新瀏覽器窗口背後，這些窗口閃爍著毫無價值的廣告，導致要訪問的網站顯得不能使用。為了應對這種情況，瀏覽器增加了彈出窗口攔截功能，這樣廣告大戰就開始了。

現在的許多網站重複了 20 世紀 90 年代中期網站低下的可用性，儘管不是因為彈出窗口導致的。相反，它們提供不斷閃爍，非常容易讓人分心的廣告，直接覆蓋在內容上方的廣告，以及帶聲音的視頻廣告，用戶訪問頁面時，視頻廣告自動播放（結果在帶著罪惡感地瞟到附近有人時迅速關閉瀏覽器）。如果因為有人要看 50 句的文本，廣告商就向手機推送 10MB 的廣告，該公司就過分了。

用於停止執行瀏覽器中的活動內容的安全工具也會停止這些類型的廣告。就像散佈惡意軟體的人，廣告商也使用相同的掛接強制計算機執行網站提供的任意代碼，結果廣告就在無用戶權限的情況下運行。

如果廣告商僅考慮顯示其廣告，那麼用戶要訪問的網站可以直接從主域處理廣告，這樣用戶什麼都不用做就可以攔截。不幸的是，顯示廣告的價值不如在不取得用戶許可的情況下跨多個域跟踪用戶以生成用戶資料，用於銷售廣告以吸引更多客戶的價值大。這些傢伙使用同樣的技術惡意軟體分銷商收集推送的惡意感染的遙測和安裝資料。有趣的是，用於在我們進行瀏覽時停止廣告的廣告攔截程序採用了安全研究人員用於預防感染的相同方法。

用戶（及其廣告攔截程序）與努力投放廣告並收集有關用戶行為的遙測資訊的廣告商之間的廣告大戰愈演愈烈。廣告商找到了新方法繞過廣告攔截程序，但是這些方法將被更新後的廣告攔截軟體再次攔截。許多廣告攔截程序的工作方式是分析跨站點腳本和其他網頁組件，以便選擇性地攔截內容，因為很少有瀏覽器真正（向開發人員）允許用戶選擇完全禁用活動內容。您可以看到這樣做的結果：通過足量的模糊處理，壞人就可以繞開保護性的附加項。注重撈錢勝過安全隱患的廣告商正在做惡意軟體分銷商的工作。在 2017 年，惡意軟體分銷商將使用用於繞過活動內容攔截程序的廣告商技術實現惡意軟體的“隨看隨下”下載。

駭客行動主義者暴露隱私問題

—Paula Greve

駭客行動主義者將努力對消費者進行數字足蹟的教育，方法是攻擊並成功洩露包含客戶資料的一些企業雲。駭客行動主義者將披露這些個人資料以激起消費者的義憤，並強迫採取行動。這些行動將延續到不再具有新聞性或公共義憤力量對隱私法律和企業政策產生改變為止。

這些年來，收集的有關用戶的資料量呈指數增長。聚集的這些資料幫助我們改善健康，在搜索時以更快的速度達成目標，找到失散多年的好友，擁有性能更優越的家居電子系統，甚至在我們上網時保護我們。甚至在歐盟的 Guide to the EU-US Privacy Shield（歐盟-美國隱私護盾指南）中也提到了這些資料的用處：“傳輸個人資料是跨大西洋關係必不可少的重要組成部分，尤其是在今天的全球數字經濟中”（第 7 頁）。今年，從校園開展的教育孩子如何控制自己資料的活動，到有關企業如何使用個人資訊改善廣告的投放效果的文章等途徑，繼續提升對從設備收集的資料和數字足跡規模的關注。事實上，一項 TED 研究收穫了超過一打與“資料陰暗面”有關的談話。這是一個有爭議的熱門話題，在來年將繼續佔據頭條。

這張照片最初由 Vincent Diamante 通過 Wikimedia Commons 在 Flickr 中以“Anonymous at Scientology in Los Angeles”為標題發布 [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)]

考慮到這些趨勢，我們預計在 2017 年，駭客行動主義者將利用這個機會“教育用戶”他們放棄的資料量有多大。我們預料這樣的行為將通過下面的攻擊實施：滲透部分用於收集資料（搜索、鏈接、連接、觀看頁面、使用產品、檢測信號等）的雲端服務，然後將內容以“公共宣傳服務”的形式公佈。根據過去的行為來判斷，一旦有駭客行動主義者團體以某個領域為目標並取得成功，也會實施類似攻擊來證明該觀點—每次攻擊都在試圖提升關注度。在這項動機下，我們預料這些資料洩露愈演愈烈，讓大家注意到更多受尊敬的網站和企業。

儘管我們預計這些攻擊將造成全球性的影響，但是可能美國企業承受的壓力最大。在美國，企業希望保持對客戶資料的控制。例如，Microsoft 已經多次上法庭“保護”用戶資料不被美國政府獲得。新的 EU-US Privacy Shield（歐盟-美國隱私護盾）為公民提供了了解哪些企業在收集哪些資料的能力。諷刺的是，希望教育歐洲公民和全世界美國企業收集了多少有關他們的資料的堅定駭客行動主義者也可以使用這個清單。

這些攻擊將引發一些擔心：從遭受攻擊的公司如何應對攻擊造成的安全後果和對客戶的信任影響，以及如何準備應對預料之中的客戶投訴衝擊，到哪些公司有45天的時間做出回應，以及客戶對回應不滿意時可做出的選擇產生的副作用。這些投訴將迫使公司採取更多措施，包括證明資料保留多久，真正需要所收集資料，以及同意發送遙測資訊的“選擇加入”、“選擇退出”與“總是發生”特性對客戶是否公平。

回顧過去指望從所竊取資料撈好處的網路犯罪分子團體造成的資料洩露的後果，被影響的人不但擔心多少資料被收集，還擔心某些資料的存在時間。個人資料被盜已經夠不幸了，但是部分資料不再精確時，進一步侵害了信任。接下來的幾年，消費者將更關注收集的資料並要求採取措施，包括進一步控制其個人資訊和持久保留政策。

我們可能看到消費者推動企業製訂“被遺忘權”政策，並允許消費者完全了解所收集資料。

總之，我們預計 2017年，駭客行動主義者將努力對消費者進行數字足蹟的教育，方法是攻擊並成功洩露包含客戶資料的一些企業雲。駭客行動主義者將披露這些個人資料以激起消費者的義憤，並強迫採取行動。這些行動將延續到不再具有新聞性或公共義憤力量對隱私法律和企業政策產生改變為止。

執法機構的打擊行動震懾網路犯罪

—Christiaan Beek

隨著私營企業與執法機構之間合作的加深，針對全球分佈式拒絕服務攻擊和殭屍網路作者的打擊行動數量也將增多。更多國家和地區將看到網路犯罪對其經濟的影響，並加大對網路回應能力的投資。

我們已經看到了最近一些值得注意的執法，其支持者打擊了一些惡意網站或實施者。Intel Security 參與了其中的部分行動。什麼是打擊行動？這是執法機構與其他各方（通常是安全提供商）聯合打擊網路犯罪行為的一系列合作行動。在最好的情況下，打擊行動可能會逮捕犯罪分子，但是在通常情況下，打擊行動只能破壞或查封網路犯罪分子使用的基礎設施。打擊行動可能需要幾個月才能產生結果，在某些情況下，可能需要數年。

例如，俄羅斯執法機構的一場大型打擊行動是在六月逮捕了 50 個人，他們多年來從俄羅斯銀行盜劫了 2500 萬美元。在 YouTube 上可以找到逮捕錄像。

在 2016 年，Intel Security 參加或幫助了四次勒索軟體打擊行動，並為另外幾次尚未公開的行動提供了支持或協助。勒索軟體打擊行動是“No More Ransom!”計劃的一部分，該計劃是執法機構和 IT 安全公司聯合打擊使用勒索軟體實施攻擊的網路犯罪分子。Intel Security 是此計劃的其中一位創始會員。

通過打擊活動，找到了許多勒索軟體的解密工具。

我們發現這會鼓勵其他安全公司加入這場針對網路犯罪的戰鬥。不幸的是，今年過早的公告危害了多月的研究和一些打擊行動。與相關執法機構核實可以防止此類危害。因為許多安全公司和全球執法機構希望加入“No More Ransom!”計劃，所以我們很有信心可以扭轉勒索軟體的猖狂勢頭。

2017 年，Intel Security 將繼續為全球執法機構的打擊行動提供協助。我們還將積極參與 No More Ransom! 計劃和類似組織，分享我們的知識和專業技能為全球社區服務。

隨著私營企業與執法機構之間合作程度加深，針對全球分佈式拒絕服務攻擊和殭屍網路作者的打擊行動數量也將增多。更多國家和地區將看到網路犯罪對其經濟的影響，並加大對網路回應能力的投資。我們採取行動的速度越快，回應和乾預能力就越高。參與與執法機構之間的聯合行動的私營企業應該預見法律後果並做好準備。下一年可能是網路犯罪分子首次開始挑戰私營供應商和執法機構之間的關係。

威脅情報共享取得巨大進步

—Jeannette Jarvis

分享威脅情報可以扭轉局面，將優勢從對手轉換到我們防禦者這一方。它破壞攻擊的生命週期，事實證明可以提高壞人的實施成本，因為他們需要將自己的資源和技術轉移到新戰術上。這場轉移已在 2016 年展開，當時 Cyber Threat Alliance (CTA) 的創始會員合作研究 CryptoWall V3 活動。這份研究報告發布後不久，惡意軟體作者放棄了對 CryptoWall V3 的關注，將努力轉到了 V4 這一新活動。CTA 將在 2017 年通過加強協作和開展更　深入的研究，繼續改善集體防禦。此項研究將披露新攻擊以及威脅的細節跡象，並共享和添加到成員的控制系統，以阻止更多攻擊。

如果共享威脅情報如此寶貴，為什麼不存在更多合作？歷史上，共享威脅情報有三大障礙：

1. 無意中共享私人客戶資訊。
2. 失去競爭優勢。
3. 公眾會知曉哪些組織受到了攻擊。

幸運的是，安全行業正在改變，這些擔心正在消散。例如，Cybersecurity Information Sharing Act 為美國政府與私營企業之間和責任保護延伸到共享實體的私營企業之間的威脅情報共享提供法律基礎。隨著此責任保護為其保駕護航，美國企業正在評估自己的共享政策。我們在 2017 年應該可以看到越來越多的威脅情報共享。

我們將看到成立值得信賴的 ISAO 社區。我們還將看到出現新的 ISAO 平台，此類平台允許企業將威脅情報自動添加到自己的安全系統中。

需要自動化工具和流程才能幾乎實時阻止攻擊。根據美國總統執行令13691，美國國土安全部長受命成立 Information Sharing and Analysis Organization (ISAO) Standards Organization。ISAO Standards Organization 已製訂了基礎指南和最佳實踐已製訂了基礎指南和最佳實踐以實現高效資訊共享與分析。在 2017 年，我們將看到根據細分市場、區域和其他相關域，圍繞利益密切相關性建立大量值得信賴的 ISAO 社區。我們還將看到出現新的 ISAO 平台，此類平台允許企業將威脅情報自動添加到自己的安全系統中。

根據我們的預測，隨著 ISAO 和其他威脅共享計劃的發展，管理和義務將得以改善。International Association of Certified ISAO (IACI) 的使命是推動 ISAO 的指導和認證，並將在 2017 年完全成立。IACI 將為全球開發和提升網路威脅共享計劃管理的組織提供協助。

為了改善我們的網路防禦，整個行業必須通力合作。眾包威脅情報與協作分析可幫助連接各方，並更好地了解攻擊全局的現狀。2017 將是威脅情報共享取得巨大進步的一年。

行業和執法機構聯手打擊網路間諜

—Christiaan Beek

由於國際法和國家 / 地區之間的協定的改變，我們預料以前國家發起的網路間諜團體將進入資訊掮客角色，並提供撈錢的“渠道”。他們的慣用伎倆依然不變。

2016 年的前九個月，Intel Security 登記了 78 個我們歸類為網路間諜或戰爭的公共案例。在大多數活動中，民族國家想方設法了解目標實體的政治觀點或背景。這些目標實體屬於政府部門，在某些情況下，為政黨的個人或成員。

這些案例的慣用伎倆都很類似，但是我們預計到 2017 年變化會非常大。每次的開始都是實施者建立主機域基礎設施，充當控制服務器或提供負載。接下來是魚叉式網路釣魚攻擊，目標在此攻擊中收到武器化的電子郵件。攻擊者有時會在嵌入式 HTML 中加入隱藏代碼，用於跟踪攻擊者計劃控制的計算機，以了解登錄了網路中的哪個位置。攻擊者在這裡使用大量工具，如各種憑據編輯器、哈希傳遞攻擊或定制腳本。在大多數情況下，後門程序遠程訪問特洛伊木馬程序在網路中保留立足點。技巧不足的實施者團體使用現成的商業 RAT（如 PlugX）並修改基本設置來為自己的活動服務。

今年的兩個網路間諜案例引起了我們的特別興趣。第一個是 Irongate。研究人員發現一段複雜的惡意軟體攻擊工業控制系統。這些代碼段與著名的 Stuxnet 網路武器蠕蟲有關。這是將惡意軟體用作網路武器的一項風險：如果該代碼洩露，必定會在其他地方出現。在某個時間點，有人會改變和改進這些惡意軟體應用程序。這導致第二個案例：Strider/Sauron，這是一段非常高級的惡意軟體，它使用模塊化方法和技術。Strider/Sauron 是真正配得上高級持續性威脅這一綽號的惡意軟體令人印象深刻的一個示例。這樣的代碼公開後，應該引起我們的擔心；我們可以預料民族國家發起的團體將學習並改變其中一些技術。

2017 年的網路間諜將會怎樣？網路間諜將永遠存在，形式為民族國家的情報行動的一部分，或由尋找產權情報並出售的有組織團體運營。由於國際法和國家/地區之間的協定改變，我們預料以前國家發起的團體將進入資訊掮客角色，並提供撈錢“渠道”。每個人都有值點什麼的資訊，但是需要有創意思維才能變現。

另一項預測與網路安全有關。據稱是 Equation Group 擁有的工具的洩漏清楚表明進階攻擊正在調查如何攻擊防火牆。如果攻擊核心路由器或 VPN 集中器成功，就可以訪問網路，並避開安全雷達自由飛翔。2017 年，我們將看到更多與這些攻擊有關的研究和探測。

實體安全和網路安全行業通力合作

—Matthew Rosenquist

安全行業即將發生戰略轉移。網路和實體安全領域將開始交匯，並將安全延伸到現實世界與數字世界之間。由於不斷採用用於改善個人生活和企業效率的技術，將迫使安全行業跨越網路安全和實體安全之間的鴻溝。此融合是這兩個領域保護人與資產這一共同目標的自然結果。

齊心合力

全球網路和實體安全行業的產值分別為大約 800 億美元和 1000 億美元。實體安全行業成熟得多，也穩定得多，而網路安全市場的特徵則是更混亂，並且正在快速成長。

多年來，它們很大程度上彼此獨立存在。實體安全注重視頻監控、門鎖和門卡讀卡器之類出入控制系統、柵欄、安全系統和用於保護寶貴資產的工具。網路安全注重保護計算機、智能設備、電信、資料、雲端和一切與網際網路相連的物品。這些資產和服務提供巨大價值，但是必須受到保護，可以抵禦不同類型的威脅。

世界在變

隨著數字工具和技術的發展和擴散越來越滲入我們的日常生活，對網路安全的需求隨之加大。趨勢是，從任何位置連接、監視和控制設備。正在為計算機系統設計更多傳感器和功能。日常設備現在正在互聯並變得“智能”。物聯網的融合正在推動這一趨勢，預計到 2020 年將有 2000 億台設備連接到網際網路。這些設備中許多為家用和商用，這兩者是實體安全行業極為核心的市場。如果您前門的新智能門鎖被竊賊打開，或者您的臥室嬰兒監視器在網際網路上現場直播，您就會感到毫無安全可言。

Gartner 估計，到 2020 年，超過 25% 的企業攻擊將涉及物聯網設備。這將導致已經不堪重負的物聯網安全開支從 2015 年的 2.82 億美元到 2018 年翻倍到超過 5.47 億美元。

警報、出入控制和視頻監控安全產品本身正在成為網路攻擊的目標。將安全設備連接到網路可以節約客戶的成本，為其提供增強功能，但是也會將他們暴露給駭客。軟體、韌體和資料都可能受到攻擊。

物理和網路安全行業將通力合作，開始基於數字威脅強化安全產品。他們將彼此共享資源增強下一代產品和服務的安全。

這兩個市場彼此需要

現在迫切需要與實體安全有關的技術以改善網路保護。IP 網路中的所有設備，尤其是直接連接到網際網路的設備，都需要網路安全保護。據估計，大約 70% 的視頻監控攝影機現在已連接到計算機網路。這形成了一個巨大的有漏洞設備池。

大量視頻監控攝影機正在被侵入。簡單的 Google 搜索就可以找到在洩露視頻資料的系統。使該問題得到關注的是公開搜索引擎 Shodan，它使用戶可以瀏覽有漏洞的網路攝影機。可以輕鬆觀看全球攝影機的直播。任何人都可以觀看臥室、銀行、客廳、嬰兒監視器室、游泳池、大學等的資料源。這些就是配置低或缺乏極為基本的安全控制導致向公眾開放的內容。專業的駭客分散性更高，有更好的工具來訪問多得多的系統。

這只是開始。隨著其他實體安全和安全系統連接到網際網路，將發生更多攻擊和侵入。最近，超過一百萬部攝影機和 DVR 受到駭客攻擊並被重新配置，成為了殭屍網路的一部分。然後，此殭屍網路攻擊網際網路上的其他系統。由於不存在檢測控制，所以所有這些發生時，設備所有者都沒有意識到他們充當了犯罪行為的幫兇。實體安全行業迫切需要基於網路的控制來強化產品和服務，以便抵禦網路攻擊者。

隨著全球湧現更多數字設備、網路服務和更廣泛的連接，對安全的需要也將上升。消費者和企業在受益於高級遠程功能的同時，也需要隱私和安全。物理與網路域之間的差異不再相對，並開始融合。如果臥室攝影機資料源受到網上陌生人的控制，消費者不會開心。他們不會關心是軟體問題還是網路問題。他們將歸咎於產品製造商、安全服務提供商或安裝程序。這同樣對商用醫護設備、汽車和工業控製成立。這些在物理和數字兩方面都必須安全。

消費者和企業高層希望實現他們的夙願：一個實體同時負責處理和修復問題。最近的調查顯示了消費者對風險的認知程度，並且他們在發生洩露時隨時準備拋棄喜愛的零售商。電信行業已經感受到了這樣的痛楚。歐洲最近的 TalkTalk 資料洩露促使超過 10 萬消費者離開，轉投另一家供應商。這些易變的期望在技術融合的助力下，將驅使網路和實體安全行業積極通力合作。

預測

在 2017 年，我們將看到物理和網路安全行業合作創建更複雜、更具粘性的安全解決方案：

1. 物理和網路安全行業將通力合作，開始基於數字威脅強化安全產品。為客戶著想，這兩個市場已統一。現在他們將彼此共享資源來增強下一代產品和服務的安全。
2. 消費者將擔心針對物理設備，旨在破壞其安全和隱私的網路攻擊。他們將需要統一的安全體驗，或關注其他供應商和提供商。
3. 網路安全解決方案提供商將開始通過為集成提供新軟體、平台和架構，開始服務和支持實體安全提供商。預計大小型網路安全公司都會發佈公告。
4. 實體安全會議將擴展到包含網路安全主題、專家和供應商。這是供應商開始在商業活動中交叉營銷時可靠的協作徵兆。

回饋。為幫助指導我們以後的工作，我們殷切希望得到您的反饋意見。如果您願意分享您的觀點，請點擊此處以填寫一份五分鐘就能完成的快速威脅報告調查。

關注 McAfee Labs

關於 Intel Security

McAfee 現在是 Intel Security 的一部分。Intel Security 憑藉其 Security Connected 戰略（創新型硬體增強安全解決方案和獨特的 Global Threat Intelligence）致力於開發具有前瞻性且經實踐驗證的安全解決方案和服務，保護用作商業或個人目的的全球系統、網路和移動設備。Intel Security 將 McAfee 的安全經驗和專業知識與英特爾的創新和可靠性能相結合，使安全性成為每種體系結構以及每個計算平台的基本要素。Intel Security 的使命是讓每位用戶放心地在數字世界中安全可靠地工作生活。

www.intelsecurity.com

McAfee. Part of Intel Security.
台北市忠孝東路七段 369 號 20F
Tel: +886 2 6622 0000
Fax: +886 2 6622 0107
www.intelsecurity.com