Cisco Ransomware Defense：封鎖勒索軟體

您知道您可以防範勒索軟體，儘管它總是想方設法入侵嗎？只有 Cisco 能夠提供擁有此功能的資安產品和架構。

概述

檔案和資訊是企業的命脈。維護這些資訊及企業生產力完整無缺且安全無虞，是沒有任何妥協的餘地。

但是，勒索軟體會將檔案加密進行勒索，只有支付比特幣的贖金，才能換回檔案。如果沒有妥善的防護對策，勒索軟體就會造成重大的損失，導致組織無法營運。

勒索軟體通常透過入侵程式套件、惡意廣告 (網站上遭感染而能夠擴散惡意軟體的廣告)、網路釣魚 (假冒可信任的寄件者所寄出的詐騙電子郵件) 或垃圾郵件活動進行擴散。實際的感染是因為有人按一下網路釣魚電子郵件中的連結或附件，或按一下遭感染的廣告或遭破壞的網頁中的連結，這些電子郵件、廣告或網頁會導致任何接觸的人遭感染。

運用 Cisco® Ransomware Defense。這可透過從 DNS 層到端點、網路、電子郵件和全球資訊網的分層做法，降低勒索軟體感染的風險。我們透過架構方法提供整合的防護措施，充分掌握並防範勒索軟體。

優勢

- **降低勒索軟體的風險**，讓您專注於企業營運
- 運用對於嘗試取得最高權限的威脅前加以阻絕的資安措施，達到**立即防護**的效果
- 運用涵蓋從 DNS 層到網路和端點的架構方法，達到**充分掌握和防範**的效果
- 運用強大的網路區隔**避免惡意軟體大規模擴散**
- **獲得對於勒索軟體領先業界的 Talos 威脅研究**和情報

擴散迅速且強大的威脅

今年的勒索軟體相當猖獗，而且獲利相當豐厚。勒索軟體很快就成為獲利最豐厚的惡意軟體類型。

FBI 表示市場年產值預估達到 10 億美元。Cisco Talos 研究顯示，一次勒索軟體活動每年可產生高達 6000 萬美元的價值。勒索軟體愈來愈受到重視，甚至有電視節目做專題報導。

攻擊者有資金和慾望持續發動更致命的勒索軟體攻擊。我們相信勒索軟體將會更有能力自行擴散，企圖攻佔公司網路的更多部份。這足以摧毀自從 1970 年代以來奠定的公司 IT 功能。

目前對於勒索軟體採取的回應大多採用單點產品。我們必須考慮採取更有架構的做法來因應企圖造成感染的各種載體。

這個解決方案概述說明發動攻擊的各種載體和方法。防護人員必須防護電子郵件和網路、阻絕對於網際網路上的惡意基礎設施進行的存取、阻止任何勒索軟體檔案接觸端點、阻止使用命令和控制回呼，並避免勒索軟體輕易造成大規模感染。

您需要的產品

Cisco Ransomware Defense brings 整合思科資安架構的所有必要元件來因應勒索軟體挑戰。您應該選擇所有元件或其中一個元件來滿足立即的資安需求。

Ransomware Defense 包括：

- Cisco Umbrella，這可透過 DNS 層阻止威脅入侵網路
- Cisco Advanced Malware Protection (AMP) for Endpoints，這可阻止惡意的勒索軟體檔案在端點執行

- 雲端和內部部署的 Cisco Email Security，這可阻止網路釣魚和垃圾郵件訊息擴散勒索軟體
- 對於經由思科電子郵件安全閘道傳遞的不明附件進行的靜態和動態分析 (沙箱)，透過輕鬆的授權即可將 Advanced Malware Protection 加入電子郵件資安產品中。
- Cisco Firepower™ 新一代防火牆 (NGFW)，這可阻絕命令和控制流量，以及網路傳輸的任何惡意檔案
- Cisco ISE 透過思科網路對於網路進行動態區隔，因此勒索軟體無法大規模擴散

藉由 Ransomware Defense，組織能夠使用網路加強因應勒索軟體的擴散。即使在最不理想的感染狀況下，也無法在網路上輕易擴散。

感染爆發後，Cisco Security Services 可在事件回應時進行立即分類。這些也能夠簡化 AMP、NGFW 和其他解決方案產品的部署。

關鍵功能

- 阻絕勒索軟體入侵網路或下載到筆記型電腦上
- 因應勒索軟體入侵網路的最不理想狀況

資安服務有助於對抗勒索軟體

勒索軟體感染爆發時，思科資安服務事件回應團隊可進行立即分類。這個團隊會引導您進行識別、隔離和補救。過程中會運用分析和資料採礦、鑑識影像分析、遭感染系統動態檢測、惡意軟體反向工程，以及攻擊手法分析和重新實施。

此外，Cisco Security Integration Services 可因應解決方案層級的架構挑戰。這能夠簡化 AMP for Endpoints 和 Cisco Firepower NGFW 之類的解決方案技術進行部署的過程。我們的團隊在整合式資安解決方案的交付方面擁有深厚的專業知識，能夠加速採行所需的資安技術，確保防護不中斷。

「我們減少了 90% 以上的勒索軟體....從此再未遇到勒索軟體事件。」

— 世界級醫療產品製造商

思科優勢

勒索軟體將不擇手段設法入侵貴公司。網路釣魚電子郵件、遭侵害的網頁橫幅、垃圾郵件 — 許多載體需要保護。只有思科能夠提供面對勒索軟體挑戰所需的資安架構。單點產品並不足夠。我們的解決方案有我們領先業界的 Talos 研究小組支援，對於勒索軟體進行廣泛的威脅研究，提供有效的分層防護效果。我們將阻絕勒索軟體，並防治趁隙而入的網路侵害 — 這是最不堪想像的事實。

獲得免費的評估

讓貴公司專注於最有效的企業營運。運用我們的免費評估，瞭解貴公司目前暴露於勒索軟體風險的程度。詳情請聯絡思科銷售代表。

C22-737492-00　2016 年 6 月