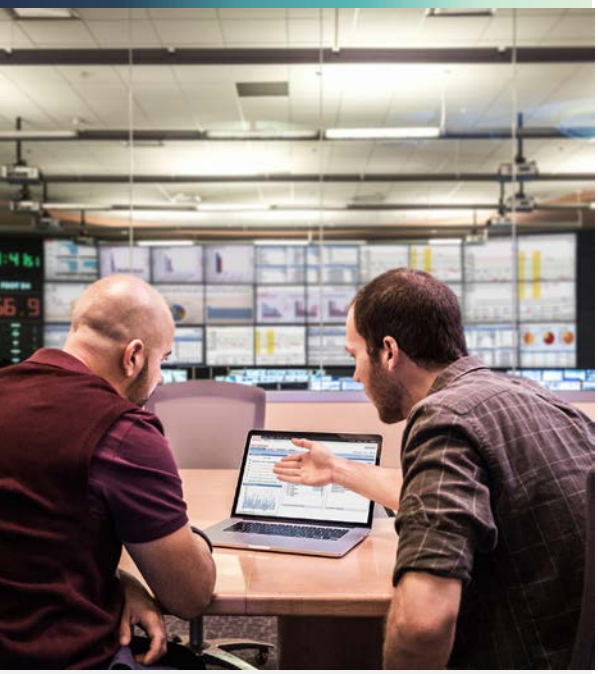

優勢

- 運用可在威脅嘗試發起攻擊之前加以封鎖的資安措施，**降低**感染勒索軟體的**風險**
- **即時防範**勒索軟體有助於您專注於業務營運。
- **整合式分層防護措施**為您提供涵蓋 DNS 層到網路和端點的卓越可視性和回應能力。
- **動態區隔**可以將勒索軟體侷限在網路的特定部份。
- 思科 Talos 資安情報和研究團隊提供**領先業界的情報**。

思科勒索軟體防護解決方案

勒索軟體的崛起

勒索軟體是一種惡意軟體，會將使用者的檔案（文件、相片和音樂）加密並藉此進行「勒索」。攻擊者要求使用者必須付款（通常使用比特幣）才能解密並取回檔案。

勒索軟體已迅速成為獲利最豐厚的惡意軟體類型，市場年產值預估達到 10 億美元。

勒索軟體通常透過網頁或電子郵件入侵電腦或網路。在網站上，勒索軟體可透過傳送惡意軟體的受感染廣告（稱為「惡意廣告」）進行侵入。使用者在瀏覽含有惡意廣告的網站時，會自動下載惡意軟體或重新導向到入侵程式套件。在電子郵件中，勒索軟體使用網路釣魚或垃圾郵件訊息做為攻擊切入點。使用者只要按一下網路釣魚或垃圾郵件中的連結，勒索軟體就會下載並呼叫命令和控制伺服器。

勒索軟體也可利用入侵程式套件來控制系統。入侵程式套件是軟體套件，目的是識別終端系統上的軟體漏洞。發現漏洞後，這些套件接著會在有漏洞的系統上上傳和執行惡意程式碼，例如勒索軟體。

未來，勒索軟體不僅會鎖定個別使用者，也會鎖定整個網路。透過半自動程度更高的擴散方法，勒索軟體作者可以藉機入侵網路並進行橫向移動，以控制很大一部份網路，進而最大化影響並最大程度提高收到付款的機率。

運用更有效的資安措施降低勒索軟體風險

由於勒索軟體可透過許多方式入侵組織，因此降低感染勒索軟體的風險需要採取基於產品組合的解決方案，而非單獨依靠一種產品。組織必須盡可能防範勒索軟體，偵測它是否入侵系統，並進行防治以減少損害。

思科勒索軟體防護解決方案採用涵蓋從網路到 DNS 層、電子郵件和端點的防護措施，藉助思科資安架構有效保護企業。它以領先業界的 Talos 威脅研究為後盾，可達到充分防範勒索軟體的最高回應能力。

「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

此解決方案包含下列元件：

- **思科 Umbrella**，保護公司網路內外的裝置。它會在裝置連線到存在勒索軟體的惡意網站之前阻絕 DNS 要求。
- **思科端點進階惡意軟體防護 (AMP)**，可阻止勒索軟體檔案在端點開啟。
- **具備進階惡意軟體防護 (AMP) 功能**的思科電子郵件安全解決方案，可阻絕垃圾郵件、網路釣魚電子郵件以及惡意電子郵件附件和 URL。此項技術與端點運用的技術相同，只是部署於電子郵件閘道。
- 採用進階惡意軟體防護 (AMP) 和思科 Threat Grid 沙箱技術的**思科 Firepower 新一代防火墻 (NGFW)**，可控制已知及未知的惡意軟體，並阻絕對於勒索軟體主機進行的命令和控制回呼，達到阻止威脅的效果。
- **Cisco TrustSec via the Cisco network**，可對網路進行動態區隔，因此能確保服務和應用程式的存取極為安全，並且勒索軟體無法橫向擴散。
- **思科安全服務**，可在出現事件回應時進行即時分類。同時也能簡化 AMP、NGFW 和其他解決方案產品的部署。

後續步驟

與思科銷售代表聯絡，瞭解思科勒索軟體防護解決方案的詳情，讓貴公司專注於最有效的企業營運。

C45-737465-00 06/16