電子書

無法防止勒索軟體的 5 大理由

NetApp

目錄

有鑑於多年來出現不少勒索軟體高調的攻擊行動，以及感染後的嚴重後果，您或許會認為勒索軟體的預防方法應該已經相當成熟，已經能夠快速且完全地消滅勒索軟體了。

想起過去相當猖獗的刺探利用套件威脅，像是惡名昭彰的 Angler，雖然當時對任何資安團隊而言都是非常令人頭痛的問題，但由於研究人員努力不懈加以箝制，現在這類刺探利用套件已經消失在大家的記憶之中。

可是，勒索軟體仍然四處橫行，而且實際上是不可能完全滴水不漏地全面防範勒索軟體。以下就來細數其中原因。

5

回報豐厚

由於成功攻擊能夠帶來豐厚回報，讓攻擊者的攻擊動機更甚以往。美國、加拿大及歐洲等地組織的平均支付贖金金額，從 2019 年的 115,123 美元激增至 2020 年的 312,493 美元，相當於年成長率高達 171%，而 2021 年第一個會計季度的平均贖金甚至達到 850,000 美元之多。自 2019 年以來，與勒索軟體相關的資安事件增加了 65%，攻擊頻率還在持續成長，預估到 2031 年之前，將從每 11 秒一起攻擊事件增加到每 2 秒就有一樁，這意味著，此類攻擊將會越來越普遍。就以上數據來看，不難瞭解為何勒索軟體持續成為大受歡迎的犯罪手段。

即使執法單位建議採取反抗措施，但有許多組織仍舊選擇支付贖金。公司無疑希望保護本身資料，不過由於業務中斷的成本通常遠高於贖金，所以支付贖金變成最符合成本效益的選項。

4

成本便宜

另一方面，從事勒索軟體活動的實際開支成本相當低廉。現今攻擊者只要花非常便宜的金額，就能購買到預製的勒索軟體套件，套件中包含了部署攻擊和從中營利所需的一切，包括加密服務、Payload　植入程式和混淆工具。一般的勒索軟體即服務 (RaaS) 訂閱價格，大約從每月略高於 100 美元起跳；如果是更複雜強大的變體版本，價格可能高到上千美元，不過獲得回報的可能性也隨之增加。其中也包含支援計畫，確保攻擊者能夠從服務中獲取最高價值。

3

證實有效

勒索軟體是一門很賺錢的事業，如果您還認為這是由穿著帽 T 的罪犯，在黑暗房間中偷偷摸摸的犯罪行動，請拋棄這樣的刻板印象；勒索軟體已經有精密的網絡結構，就像任何企業的合作夥伴計畫一樣。DarkSide 是 RaaS 的最新範例之一，最早出現在 2020 年 8 月，在 11 月變成 RaaS 散佈模式。從回報的資安事件來看，一般要求金鑰解鎖資料的贖金介於 20 萬至 200 萬美元之間。DarkSide 勒索軟體的營運者不僅獲得豐厚報酬，也將自己定位為「俠盜羅賓漢」，從獲利豐厚的大型企業身上取得金錢，再將收入投入慈善捐款。從針對資料外洩網站的調查報告來看，目前為止至少有 90 家受害企業受到 DarkSide 影響。總體而言，DarkSide 網站上目前有 2TB 以上的竊取資料，可說是進一步迫使受害者支付贖金的另一項動機。

2

快速回收投資報酬

勒索軟體如此具有吸引力的另一項原因，就是透過電子郵件附件、惡意URL、不安全的遠端桌面傳輸協定或惡意廣告等等進入組織內部之後，它們可以快速移動散佈，勒索軟體會隨即掃描網路找出檔案，然後加密內容並要求贖金，遺憾的是，一旦開始加密，此過程就幾乎無法復原。另一項新興趨勢也值得大家警惕，那就是攻擊者會先竊取資料然後再予以加密。Colonial Pipeline 負責供應美國東岸 45% 的燃料，在 2021 年 5 月遭受勒索軟體攻擊。這項攻擊行動由 DarkSide 或附隨組織執行，DarkSide 除了鎖定 Colonial Pipeline 的電腦系統，也竊取 100GB 以上的企業資料。DarkSide　竊取資料的行為，對受害者而言就像是一頭牛被剝了兩層皮，他們不僅要求受害者支付贖金以解鎖受感染的電腦，也要求支付贖金才能取回遭竊的資料，並同時威脅受害者，如果不支付贖金就要公開竊取的資料。

1

人員不可靠

目前我們已經介紹了勒索軟體為何如此猖獗，但並未說明如何才能阻止它們。雖然確實可以利用更理想的修補檢疫做法來預防大量的攻擊行為，但導致不可能全面防範的最主要原因是「人」。

您相信員工絕對不會刻意傷害組織，可是勒索軟體感染事件仍然不斷發生，那是因為員工並未隨時保持高度警戒，提防惡意連結、電子郵件或網路釣魚等花招百出的種種危險。

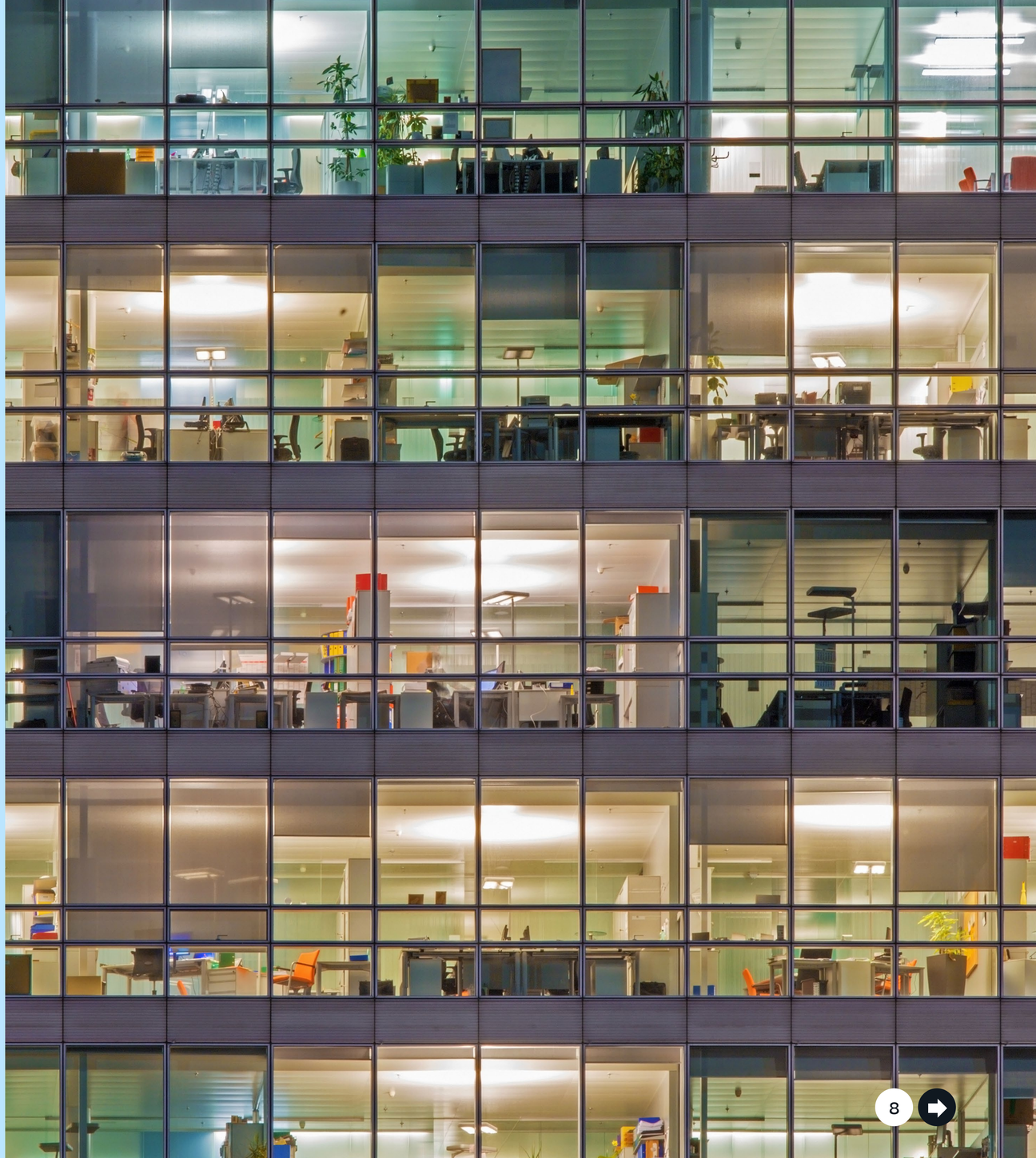
許多讀者可能都相當熟悉必須強制參加的例行資安認知電腦訓練，訓練當然沒有壞處，不過即使是最瞭解資安的員工，在點擊連結或開啟電子郵件時，還是可能出現暫時判斷失誤的情況。如果人員在實際工作過程中，沒有高度限制的資安政策介入其中把關，光是判斷失誤就足以造成傷害。我們需要在幾秒鐘內完成偵測，而不是幾分鐘、幾小時甚至更長的時間。

零信任的勒索軟體防護措施

如果勒索軟體防不勝防，您可以採取什麼保護措施呢？

員工需要存取資料才能執行工作，勒索軟體也一樣，因此您的員工可能成為攻擊媒介。運用政策和角色來限制資料存取有助於防範，不過如果限制太多，就可能對生產力造成阻礙。

早期偵測、使用者行為分析、發生可疑模式時自動採取行動，都是可以採取的防護措施，而且要在幾秒鐘內發揮作用。



NetApp® Cloud Insights 以名為 Cloud Secure 的功能提供這類偵測技術，Cloud Secure 可讓您隨時監控活動、偵測異常行為，並自動做出回應。

- **監控使用者活動**
  正確識別入侵事件，擷取並分析每位使用者在內部環境和混合雲環境中的活動。於客戶環境的 VM 之中安裝輕量化且無狀態的資料收集代理程式，用它來收集必要資料。此項資料也包括 Active Directory 及 LDAP 伺服器的使用者資料，以及 NetApp ONTAP® 儲存設備的使用者檔案活動，範圍涵蓋您本身的資料中心或雲端。

  Cloud Secure 會為每位使用者建立各自的行為模型，藉此偵測使用者的異常行為。利用這個行為模型，可以偵測使用者活動中的異常變化，並分析這些行為模式，以確定是否有來自勒索軟體或惡意使用者的威脅。此行為模型可減少發生誤報。

- **偵測異常並識別潛在的攻擊**
  當今的勒索軟體和惡意軟體極其精密，使用隨機副檔名和檔案名稱，使得特徵導向（封鎖清單）的解決方案常常偵測無效。Cloud Secure 使用先進的機器學習演算法，可找出不尋常的資料活動，並偵測潛在的攻擊。此方法具備動態且準確的偵測能力，並可減少發生誤判。

- **自動回應政策**
  Cloud Secure 可向您警示可能的勒索軟體攻擊，並提供多項自動回應政策，協助保護資料免受攻擊威脅。

  偵測到異常行為時會建立 NetApp Snapshot™ 快照複本，您的資料可獲得保護，使您能夠快速復原，同時限制任何因誤報而造成作業中斷的可能性。

封鎖使用者存取資料的能力：
- 當偵測到異常的（讀取 / 寫入）使用者行為時。
- 當偵測到異常的檔案刪除行為時。

Cloud Secure 提供詳細的存取稽核記錄，可協助系統管理員迅速識別遭受入侵的資料及攻擊來源，以便快速補救及復原。

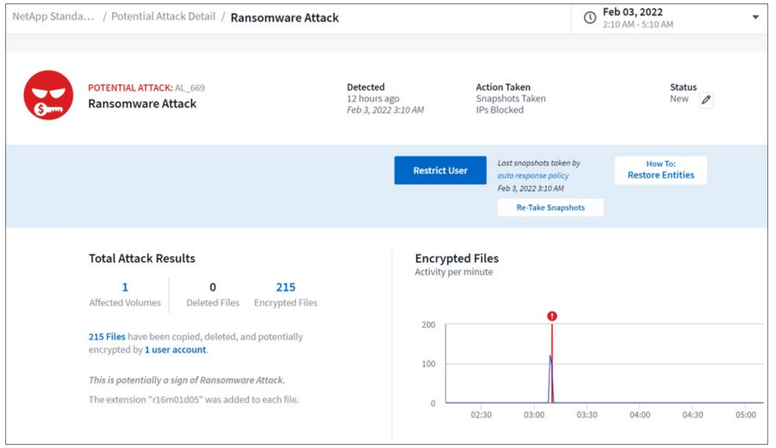


圖 1）Cloud Secure 儀表板顯示勒索軟體攻擊。

如果您有興趣深入瞭解 Cloud Secure，歡迎註冊我們的 30 天免費試用方案。
深入瞭解並開始免費試用

關於 NetApp

在這個通才遍布的世界裡，NetApp 是實力領先的專家。我們只專注於協助企業充分發揮資料價值。NetApp 將您倚賴的企業級資料服務引領至雲端，並將雲端的簡易靈活度融入資料中心。我們領先業界的解決方案適用於所有類型的客戶環境和各大公有雲。

身為引領雲端技術、以資料為中心的軟體公司，唯有 NetApp 可以協助您打造專屬的 Data Fabric，簡化作業並連結雲端，隨時隨地將正確的資料、服務和應用程式，安全地交付給正確的對象。

NetApp 台灣

台北市 110 信義區松仁路 97 號 8 樓之 2 電話：886 2 8729 5000 傳真：886 2 8729 5050

NetApp