解構 5 個勒索軟體的常見迷思

總論

從 Colonial Pipeline、Brenntag、JBS Foods 甚至美國國家籃球協會，網路勒贖攻擊事件下，成為最近的頭條新聞，並成為首要的網絡安全問題。 但是，所有的新聞報導中，對於近期的網路威脅軟體事件存有許多的誤解。

毫無疑問，軟體勒贖的問題十分嚴重，根據怡安的 2021 年網路安全風險報告，今年與勒索軟體相關的業務成本預計將達到 200 億美元，而網絡保險公司報告稱，從 2019 年到 2020 年，索賠數量增長了四倍，暴增了 336%。

贖金成本只是與軟體勒贖攻擊相關的成本和損失的一小部分，組織還也可能面臨嚴重的業務中斷損失。在某些情況下，如果不滿足攻擊者的要求，攻擊者會威脅要發布敏感資訊，這可能會損害企業的商譽。根據網絡安全風險報告，十分之七的軟體勒贖攻擊涉及揭露數據和資訊的威脅——攻擊者甚至威脅要將其賣給出價最高的人。

隨著網路威脅的發展，組織了解其攻擊性質以及應對措施是至關重要的。 “最近廣為報導的勒贖攻擊事件強調了一個事實，即網絡風險不僅僅與數據洩露有關，認知和管理網絡風險是經營公司的重要關鍵。

深度探討

與其他類型的網絡攻擊一樣，犯罪分子在執行軟體勒贖的攻擊和對潛在目標的選擇，都變得更加老練。

最近的事件促使政府對勒贖軟體所構成的威脅做出反應。 例如，美國司法部成立了一個勒贖軟體工作組小來解決這個問題，並與其他國家的執法機構合作解決這個問題。但是，雖然勒索軟體的嚴重程度變得越來越清晰，但圍繞這種類型的網絡風險仍然存在一些迷思。

迷思一: 我的公司在規模和產業等各方面，不是勒贖軟體的目標。

“當我們分析軟體勒贖攻擊模式時，它們是不分青紅皂白的，” Aon Cyber Solutions 的 EMEA 首席業務長 Richard Hanlon 說。 “這些攻擊者追逐最薄弱的環節，儘管企業投資和關注在勒贖軟體防禦和惡意軟體的偵測上，但在任何一天，都有數百個已知漏洞在企業中經常未修補或偵測到的，無論規模或產業如何，攻擊者都會利用那些最薄弱的漏洞。”

怡安專業服務商業風險解決方案高級副總裁兼執行董事 Tom Ricketts 特別表示，專業服務公司——尤其是律師事務所——已成為軟體勒贖和駭客的首要目標之一。

“駭客希望透過他們竊取的數據或侵入他們破壞的系統獲利，” Ricketts 說。 “他們需要的是：金錢和敏感數據。 專業服務公司被認為兩者兼備。 許多律師事務所過去認為，沒有人可能想要他們持有的“無趣”數據。 但駭客對內容不感興趣，真正感興趣的是該數據對公司和公司客戶的價值，可能是達數百萬美元。”

迷思二: 將數據及資訊備份就足以防止勒索軟體攻擊

老練的網絡犯罪分子可能對獲取組織所收集的個人訊息更感興趣，而不是簡單地控制其網絡或破壞數據或資訊。

支付贖金可能會導致犯罪分子提供解密密鑰，使受害者能夠重新運行系統。 但是，如果他們在攻擊過程中收集了個人身份訊息，這些犯罪分子也可能會尋求

進行二次攻擊，他們可能會威脅要賣掉資訊或是將資訊在線上公開，更進一步的威脅到公司的運作和商譽。

迷思三: 勒索軟體損失僅限於支付贖金

“支付贖金只是冰山一角，” 專家說。 “無論是什麼產業，最好在營運中斷的情況下了解勒贖軟體造成的可能損失，因為這才是勒贖軟體攻擊的最大威脅。有些公司因為無法從勒贖軟體攻擊中恢復而倒閉。”

事實上，勒贖軟體攻擊造成的損失可能遠遠超出贖金的金額和補救費用。

怡安的網路專家根據全球的經驗指出，勒贖軟體的受害者可能會失去業務，面臨第三方索賠的風險並遭受商譽損失。對於某些企業而言，攻擊造成的服務中斷可能導致客戶償還遠遠超過贖金成本。

迷思 4：威脅者在獲得網絡使用權限後會立即採取攻擊

人們談論勒贖軟體攻擊就好像它是‘零日攻擊’一樣，犯罪分子在勒贖軟體需求發出的那天就出現了，但實際上，在犯罪份子發動實際攻擊之前，通常分為數個階段。”

攻擊者通常從偵察階段開始，尋求辨識易受攻擊的目標以及如何利用它的最佳方法。

在下一階段，武器化犯罪份子應用他們學到的知識，並塑造他們的攻擊方向，可能是透過製作看起來可信的網絡釣魚電子郵件。

到執行攻擊階段時，犯罪份子可能已經在網絡中存在數月之久。 他們本可以收集並測試密碼、感染網絡、禁用防火牆並獲得對網絡的可信權限，從而使他們能夠逃避安全軟體的檢測。

“有時攻擊者會嘗試進行一次小幅攻擊，看看會有什麼反應，” 怡安的網路風險專家表示。 “然後他們根據他們從小型破壞中，學習計劃更大的攻擊。”

迷思 5：安全/防毒軟體可提供充分的勒贖軟體攻擊保護

安全軟體固然很重要，但就企業網路安全防護還是不足的。 全天候掃描和持續安全漏洞管理以及端點檢測和監控是必不可少的第一道防線。

但是我們也不能忘記人為因素，人為錯誤是組織網絡遭到破壞的第一大原因。

“這聽起來很基礎，但除了需要安裝複雜的安全軟體外，您也不能低估基本網絡健康的重要性。 您必須不斷向所信任又擁有網路權限的同仁們重申，他們如何需要具有網絡意識並始終保持警覺，確保員工接受定期培訓和教育意識，主導模擬網絡釣魚活動以衡量員工的網路安全意識，怡安的全球網路風險專家 Hanlon 說。

不相信任何人

” 當今勒贖軟體環境中的最佳方法實際上是“零信任”方法。 “即使是你認為在網絡上的人，你也必須讓他們使用多重元素身份驗證進行身份驗證，” Hanlon 說。 “而且你必須以安全系統中的高級加密的方式來做到這一點。”

期待勒索軟體攻擊

為了對抗勒贖軟體威脅，企業必須認識到自己可能成為目標。 Hanlon 表示，他們應該採取“預設被攻擊”的心態。

領導者應該挑戰他們的資訊技術專業人員，讓他們認為組織已經遭到破壞，並相應地集中其勒贖軟體防禦，永遠為預期的風險做最好的準備。