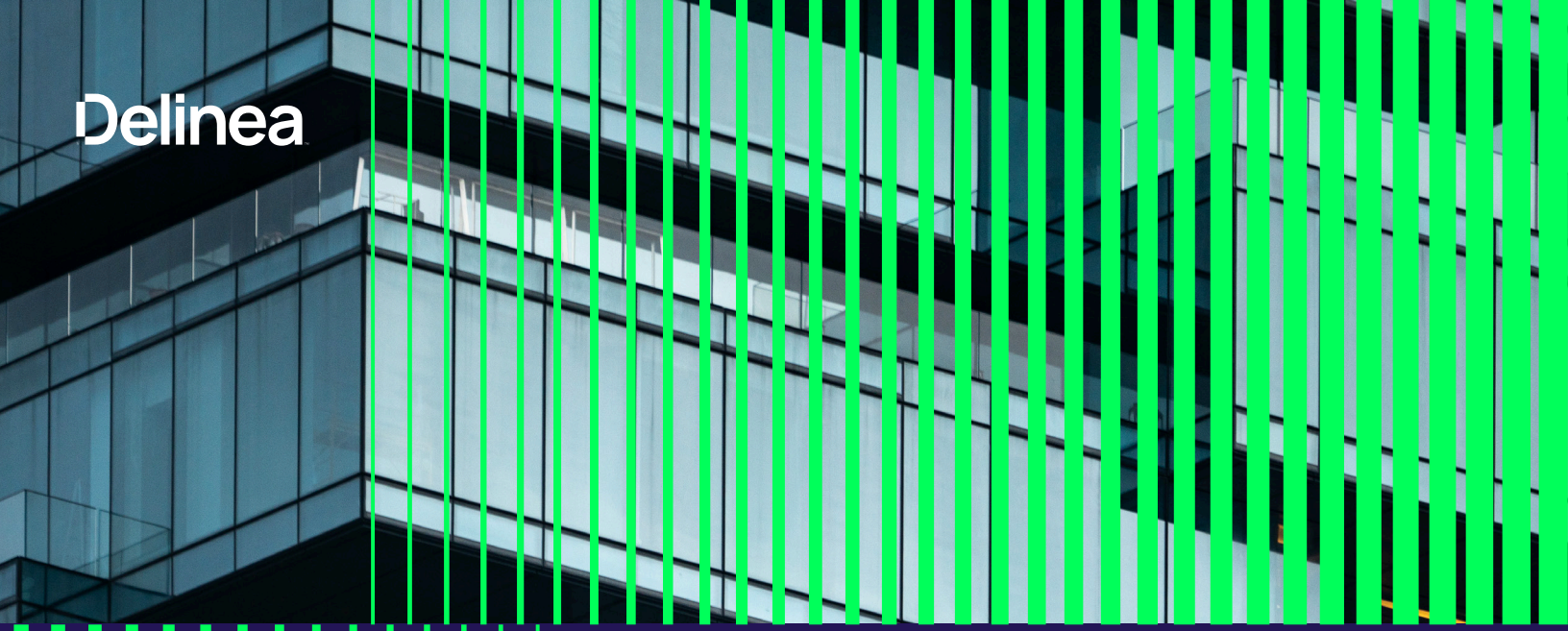
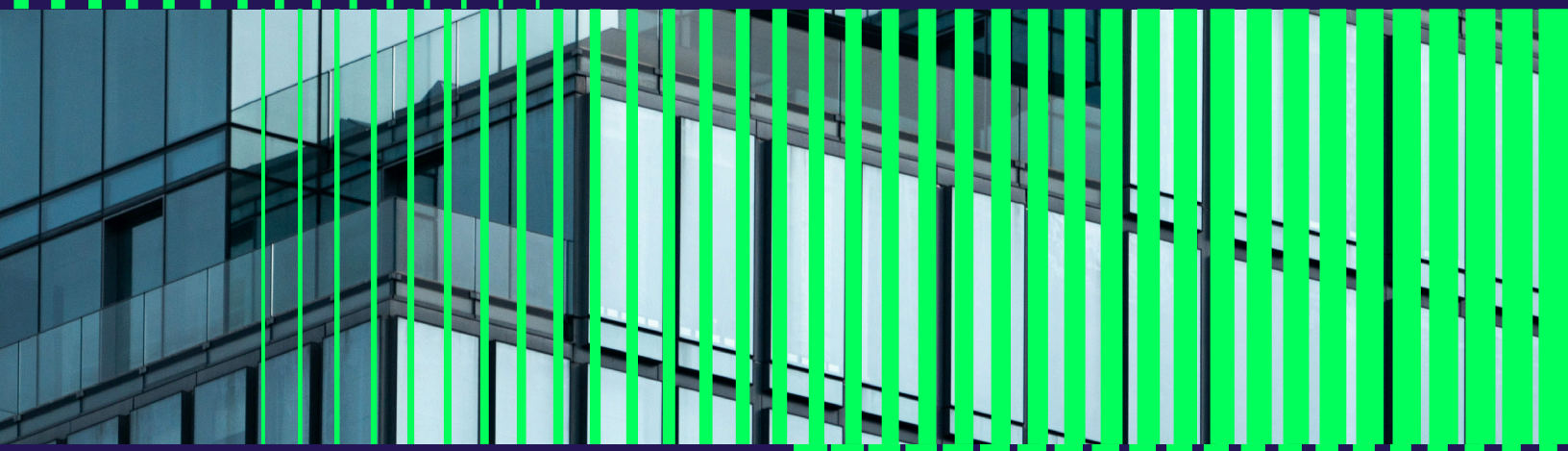


Delinea

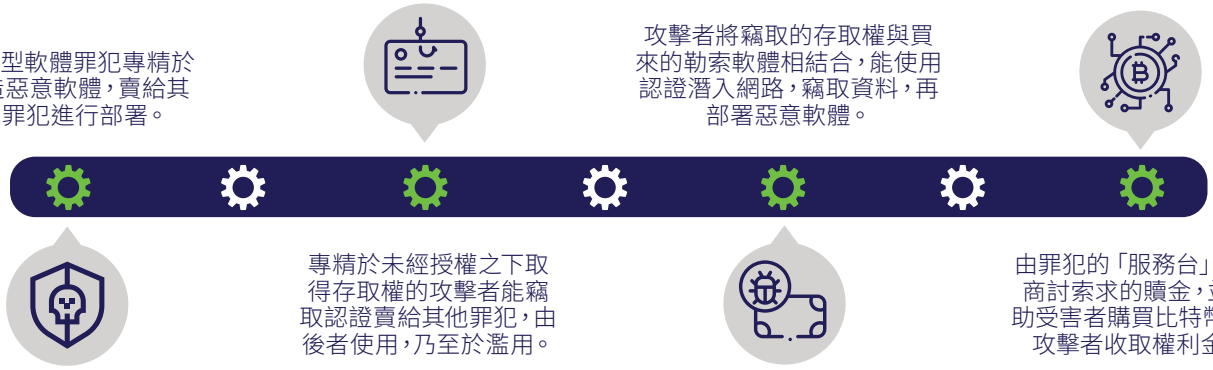
勒索軟體逐漸增加

如何降低風險並回應攻擊



白皮書

勒索軟體逐漸增加



勒索軟體即服務

案例增加的其中一個原因在於，勒索軟體製造者建立聯盟網路（或稱夥伴計畫）已成為常見的現象。依照這種新的模式，勒索軟體製造者會將成品免費提供給網路罪犯。經過罪犯部署軟體、向目標收取贖金之後，再將某個百分比的贖金分給製造者做為回報。製造者的風險最低，也有更大的成功機會。

勒索軟體的目標

任何公司或個人不分大小，都能淪為勒索軟體的目標。這些類型的攻擊目前已如此常見，以致於所有組織都必須做好應付的準備。

城市由於一旦受害即必須公開揭露，因此似乎也包括在勒索軟體攻擊的最常見目標之中。不過，僅佔估算案例中的大約 10%。[i] 根據 Verizon 資料外洩調查報告 (DBIR)，公用事業、醫療組織、出版公司及金融機構也經常成為攻擊目標。[ii]

勒索軟體的代價

要求的贖金可達數千萬美元。除了財務風險之外，也能造成聲譽損失。勒索軟體攻擊即使未獲成功，也容易引發主管機關要求調查，和招致客戶提出法律訴訟。

勒索軟體攻擊已達新高。勒索軟體不僅在頻率上增加，也變得更加老練、更易得手，而且更有破壞力。勒索軟體是危險的數位武器，因為它有許多變體並且會對商務持續性造成劇烈的影響。瞭解可以如何提升復原能力，以免成為下一個勒索軟體受害者。

> 勒索軟體目前已成大事業，成為組織型網路犯罪的部分生產線。

勒索軟體的攻擊如何進展

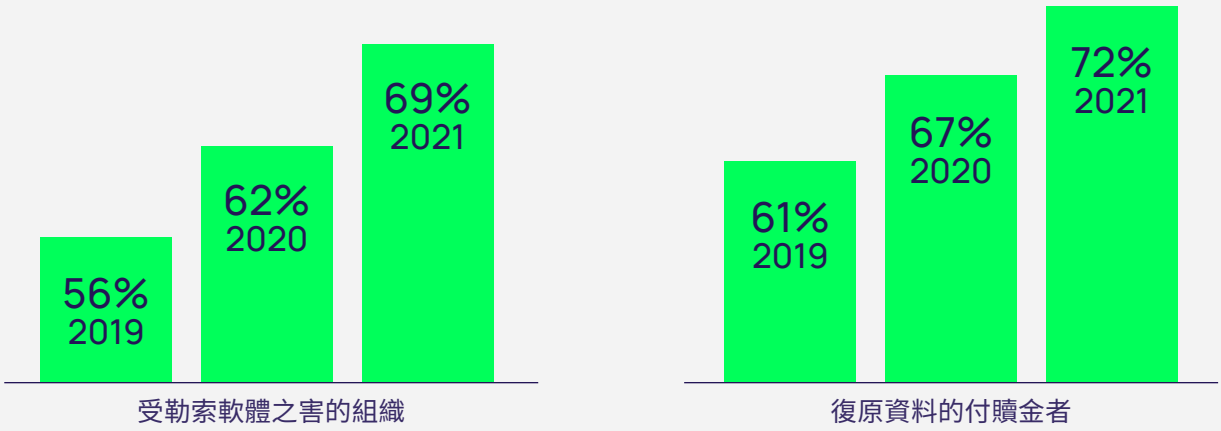
在進階威脅中，攻擊者會花時間研究出一份潛在目標名單，收集關於其系統和使用者的資訊，找出弱點。攻擊者可能會搜遍社交媒體帳號、求才公告、討論板，或其他通訊。

找到弱點之後，下一步就是突破網路安全周邊，這對大多數攻擊者而言輕而易舉。

勒索軟體攻擊經常利用網路釣魚策略，誘使不察的受害者點按看似正當的電子郵件。一經點按，即可釋出惡意軟體，入侵受害者的工作站。

助長勒索軟體行業

因為資料復原的可能性提高，導致去年有 57% 受害者願意支付贖金，但並非只要支付就都能復原資料。[iii]



一旦攻擊者能夠存取工作站，其目標便設在升高存取權，以便自由行動。他們會映射網路，以便找到利用價值更高的資產。歹徒從端點利用本機特權帳號，將觸角伸到組織的其餘部分。甚至能夠安裝工具，以便隨心所欲地重返。

> 這類活動發生時，您必須有所察覺，以縮短資料外洩的「停留時間」。這是指攻擊被察覺之前的時期；這段時間當中，攻擊者可能已經順利存取、避開偵測，竊取資料，並且離開而不留痕跡。

攻擊者一般會使用管理員認證盡可能感染大量系統，包括數位備份在內。他們會竊取敏感資料，關閉關鍵系統，讓企業完全停擺。部分事件中，勒索軟體造成的干擾之大，能使人員有生命危險，例如限制存取醫療記錄或緊急通訊系統。

一旦組織任由其宰割，攻擊者通常會威脅除非交付贖金，否則就要釋出機密資訊或者破壞資料。

所有使用者現在都是特權使用者

勒索軟體的受害者面臨艱難的選擇

您應該拔掉插頭，關閉系統嗎？

您需要知道：

- 能夠回頭手動作業嗎？
- 哪些系統還能運作？
- 攻擊者還能存取系統嗎？

若您成為受害者，一般有三種選擇：


還原備份


支付贖金


不做行動，希望能夠重建

某位商業使用者可能正在閱讀電子郵件、開啟附件、瀏覽網際網路，點按連結，或是插入 USB 裝置。如果這位使用者在工作站上有未受管的本機管理員權限，則無論從何取得安裝的可執行檔，皆能安裝並執行任何應用程式。一旦讓攻擊者接管使用者的工作站，就也有相同的能力。攻擊者能夠迅速地安裝具傳染性或惡意的工具，取得對您組織其餘部分的存取權。

不幸的是，隨著勒索軟體攻擊增加，選擇支付贖金的組織百分比也在增加。這是因為在支付贖金後，網路罪犯按照承諾歸還系統和資料存取權限的情況越來越普遍。

根據 2021 年網路威脅防禦報告顯示：「組織越有信心會在支付贖金後復原資料，就越可能實際支付贖金。」「越來越多組織支付贖金的趨勢，鼓勵了網路罪犯增加勒索軟體攻擊量，這表示又會湧現另一波的勒索軟體受害者。這是一種惡性循環，但遺憾的是，這種循環看起來不可能在近期內得以打破。」[iv]

如何降低風險並回應勒索軟體攻擊

傳統的網路安全性解決方案無法防止勒索軟體感染組織並造成大規模中斷情況。傳統的簽章式防毒程式無法預防並偵測這些攻擊類型，因為勒索軟體的變體獨特而且快速成長。加密資料也不一定能阻撓勒索軟體攻擊。攻擊者可能仍會威脅要公開揭露資料，預期其他人會因為有機會破解加密而願意支付。

為了打擊勒索軟體，您需要超越傳統的網路式網路安全性解決方案，採用新的工具組和思維。如同您為了預防勒索軟體應該做的努力，您也應假設自己將會在某個時間點成為目標。因此，您需要安全性策略來協助您準備和回應。

來自 CISA 和 MS-ISAC 的基準預防建議

美國聯邦機構網路安全和基礎結構安全局 (CISA, the Cybersecurity and Infrastructure Security Agency) 負責保護國家的網路安全性和通訊基礎結構，而跨州資訊共享和分析中心 (MS-ISAC, the Multi-State Information Sharing and Analysis Center) 則合力編製了勒索軟體指南。[v]該指南對惡意軟體預防和回應概述了幾項建議，包括偵測和分析、圍阻和根除，以及復原和事件後活動。

至少，所有組織應採用 CISA 和 MS-ISAC 為了打擊勒索軟體而建議的最佳做法和安全性方法。

備份所有關鍵資訊

在復原程序中，備份至關重要。您應定期執行並測試備份，以限制資料或系統喪失時造成的影響，同時加快復原程序。理想上，您應將關鍵資料保存在分開的裝置，並將備份離線儲存，或與生產網路隔離，並且僅提供有限存取權。

保持系統和軟體為最新

攻擊者會以未套用安全性更新的舊版作業系統做為目標。請確定隨時跟上技術供應商的建議，安裝所有修補程式。管理修補程式能舒緩超過 80% 的網路威脅，僅剩棘手的零時差攻擊需要應付。[vi]

避免從電子郵件附件啟用巨集

如果使用者開啟電子郵件的附件，啟用了巨集，內嵌程式碼即可在機器上執行惡意軟體。請提高警覺，封鎖可疑來源所發，帶有附件的電子郵件訊息。

強制實施密碼最佳實務

攻擊者只要能夠誘騙使用者交出密碼，勒索軟體攻擊經常就能得逞。請確保密碼夠複雜，讓攻擊者難以猜出。務使人員和系統定期變更密碼，不共用，儲存方式不可讓攻擊者能夠輕易取得。

實作應用程式控制

藉由將信任的應用程式加入至允許清單，您可做到僅限於經過核准的軟體能夠下載、經過核准的程式能夠執行。

採行最低權限態勢

藉由將最低權限的原則套用到所有系統、裝置和服務，限制大多數使用者安裝及執行應用程式和程式的許可權。

限制面向網際網路的 RDP 存取

由於遠距工作的情形增加，RDP 成為勒索軟體的常見攻擊媒介。確保 RDP 設定正確，並啟用安全功能。停用或限制 RDP 存取高風險服務，以強化系統防禦。

制訂網路安全意識計畫

教育員工網路釣魚攻擊的跡象。採行密碼最佳實務，例如建立複雜的密碼、定期變更，並且避免共用，讓員工拉起對抗網路犯罪的強力防線。

超越基準的強化勒索軟體防護

隨著攻擊者變得更加精到，您的惡意軟體預防計畫也必須持續演進。除了 CISA 和 MS-ISAC 提出的基準建議之外，您還可採取下列步驟，營造更強的安全態勢。

不僅設置最低權限，還採行特權存取管理

在最低權限環境中，您僅向使用者提供其執行任務所需的存取權和許可權。但您仍然必須監測並管理權限，以確保最低權限控制如所預期地運作。

PAM 能強化安全控制，使攻擊者更難以竊取密碼和濫用權限。密碼隨機化、輪換，並且持續管理，能限制攻擊者的行動途徑。使用 PAM 解決方案能迫使攻擊者冒更高的風險，讓您更有能力在入侵者尚未造成更多損害之前及早察覺。

在最低權限策略中包含限制管理存取權。去除使用者工作站的本機管理權限，攻擊者即無法利用這樣的權限擴大對目標的攻擊。

請確保持續稽核並探索特權帳號和要求特權存取的應用程式、於無必要之處將管理員權限去除，採行多重要素驗證，以舒緩使用者帳號的易受入侵。

不僅施行密碼最佳實務，還利用 PAM 使其逐漸消弭

人員若有眾多密碼和認證必須記住，會陷入網路疲勞，可能會忽略實行密碼最佳實務。您可讓密碼從人員日常工作中逐漸消弭，協助避免發生這種疲勞現象。

利用現代 PAM 解決方案，大多數使用者甚至從未見到自己的密碼。在 PAM 解決方案，則是能夠自動產生密碼，並且儲存、輪換、追蹤。使用企業 PAM，不必擔負選擇技術解決方案並且維持最新的重任，使用者只需享用即可。

不僅設置允許清單，還採行完整應用程式控制

除了將某些應用程式加入至允許清單之外，您亦可建立拒絕清單，封鎖已知的惡意應用程式。未知的應用程式可隔離到沙箱內或限制清單中，進一步審查後再行核准。

藉由充分地控制應用程式，您能以及時又恰好足夠為原則，將存取權升高。如此一來，使用者和系統能執行完成任務所需的功能，您卻不必擔心無限制的常設管理員存取權會為勒索軟體開啟一扇窗。

不僅施行寬廣的意識計畫，同時還設置內嵌大使

為使您的意識計畫成效更高，請於各部門內任命一位網路安全大使，以協助落實安全原則、察覺威脅，並且遇事件發生時予以因應。此法能協助提振一切 IT 安全團隊的效率，同時確保責任擔負，以實作並維持網路安全措施。

不僅有以合規為重的評定，也制訂持續性的策略

與其為遵循規範而僅偶爾演練，應為安全訂定持續且不斷演進的計畫。定期評估安全控制的運作情形、測試因應事件的能力，並維持所有階層人員的安全意識。

更可以制訂措施，以持續查核特權帳號的濫用。持續稽核並探索特權帳號和要求特權存取的應用程式。這些措施可協助您避免漏接勒索軟體攻擊的警訊，達到縮短停留時間的效果。

不僅注重安全活動的持續性，同時讓其變得無法預料

大多數組織會藉由自動化協助防禦，但許多情況下，自動化傾向容易遭人料中：掃描在每週同一時間執行、修補程式每月套用一次，評定則每季或每年實施。

在人預料之中的公司即有弱點。攻擊者能猜測出空窗，利用時機。因此請改變心態，以臨機為原則更新和評定系統。將安全活動隨機化，例如探索、穿透測試，及密碼輪換。

Delinea

事件因應

在戰鬥之中，預防只是其中一部份。無論您為了封鎖惡意軟體制訂多少預防性的控制措施，精到的罪犯仍有機會趁隙闖入您的組織。

因此，您需要有一套事件因應策略。

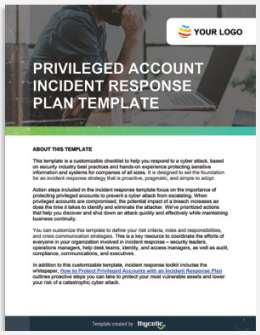
有了事件因應策略，您可防止網路攻擊釀成網路災難。IT 作業、安全和事件因應團隊可形成聯合陣線，對抗勒索軟體的攻擊、協調行動，並維持商務持續性。

應以通過測試的事件因應計畫做好準備。

取得事件因應範本

請親自見證企業權限管理解決方案如何能支援您的事件因應計畫

開始規劃



事件因應檢核表

- ☐ 責任擔負
- ☐ 通訊
- ☐ 聯絡人名單
- ☐ 明確定義威脅
  - 1) 機密性 - 資料喪失
  - 2) 完整性 - 資料毒害
  - 3) 可用性 - DDOS
- ☐ 內部能力和第 3 方責任
- ☐ 遏制（證據）
- ☐ 新聞聲明
- ☐ 法律評定
- ☐ 根除
- ☐ 復原
- ☐ 習得經驗

PAM 是事件因應的關鍵。例如在某個部門或系統內察覺出有資料外洩的情形時，請迅速變更權限和密碼，以鎖定其他系統。

行動的時機到來

勒索軟體威脅預計將大幅增加。部分安全專家已經預料，資料盜竊的案件數將會倍增。[vii]

隨著網路罪犯日益精到，您也必須提高能力。為降低業務遭受打擊的風險，您需要立即設置充足的安全控制。

請採行本文舉出的安全實務和解決方案以保護您的組織，以利於確保不致成為勒索軟體的下一個受害者。

如欲進一步了解您能如何運用特權存取管理解決方案以對抗勒索軟體，請瀏覽 delinea.com。

參考資料

i) https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html

ii) https://enterprise.verizon.com/resources/reports/dbir/

iii) https://delinea.com/resources/cyberedge-2021-cyberthreat-defense-report/

iv) https://delinea.com/resources/cyberedge-2021-cyberthreat-defense-report/

v) https://www.cisa.gov/ransomware

vi) https://ceriumnetworks.com/patch-and-vulnerability-management/

vii) https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/ransomware-on-the-rise-how-to-keep-your-company-safe/

Delinea

Defining the boundaries of access

Delinea 提供以零信任、最低權限和及時權限升高等原則為基礎的縝密安全功能。若您正在考慮遷移至雲端，或是擔憂現有的雲端資源並未受到妥善的保護，請找雲端專家討論雲端適用的 PAM。

如欲進一步了解 Delinea 的解決方案，請至 **delinea.com**。