勒索軟體防護指南

財團法人台灣網路資訊中心

Notification

This document is marked TLP: GREEN, is for limited disclosure, and is restricted to the community. Sources may use TLP: GREEN documents when information is useful for the awareness of all participating organizations as well as among peers within the broader community or sector. Recipients may share TLP: GREEN information with peers and partner organizations within their sectors or communities but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

目　　錄

什麼是勒索軟體?

勒索軟體是一種惡意軟體，以加密設備上的文件來威脅受害者，要求受害者支付贖金(通常是加密貨幣)才能解密文件，還會嘗試傳播感染網路上其他設備，無差別或是針對具有高價值的目標攻擊。

勒索軟體的犯罪模式十分成功，因此不斷演變出新的變種或與其它惡意軟體結合形成更有威脅的攻擊行為，可針對各種組織或應用領域進行攻擊，不只會影響到服務或企業的正常運作，甚至可能造成受害企業的倒閉。

勒索軟體類型

勒索軟體可以進行無差別的攻擊(Indiscriminate Attack)，即駭客大規模且不加選擇地散布勒索軟體進行攻擊，亦或是針對性的目標式攻擊(Targeted Attack)，鎖定醫療組織、工業企業和運輸等行業，以取得更高的贖金，目標式攻擊使用更複雜的魚叉式網路釣魚(Spear Phishing)或利用進階持續性滲透攻擊(Advanced Persistent Threat, APT)及系統漏洞進行攻擊，以避開日益精進的垃圾郵件過濾系統及資安防護機制。

勒索軟體造成的威脅損害類型為：

1. 資料可用性：是最主要的威脅傷害型態，加密受害電腦中的檔案，要求受害者支付贖金換取解密金鑰，然而即使受害者願意支付贖金，也未必能確保資料完整的恢復。

2. 系統可用性：特徵是阻止受害者存取受感染的電腦或行動裝置，鎖住電腦螢幕與瀏覽器導致無法使用，藉以達到威脅的目標，。

3. 隱私挾持(Doxware)：主要是對資料的機密性造成傷害，駭客將受害者電腦中的資料大量加密和上傳，以洩漏該隱私或機敏資料作為要脅，迫使受害者支付贖金換取資料不外洩。

勒索軟體的攻擊途徑

要防範勒索軟體，必須先對勒索軟體的攻擊途徑有所瞭解。勒索軟體感染在完整的攻擊行為中，是屬於末尾的步驟，因此企業如果能在先期發現攻擊跡象，便有可能阻止勒索軟體攻擊，也就是盡早發現憑證盜竊和橫向移動的跡象，可防止勒索軟體悄悄入侵企業網路。

駭客入侵電腦或企業網路的主要方式為：

1. 資安漏洞遭利用：勒索軟體會利用受攻擊目標的資安漏洞直接感染，例如 2017 年的 WannaCry 勒索軟體，掃描檔案分享的 SMB (Server

Message Block) 協定漏洞，進而快速感染。若沒有直接可感染的漏洞，則透過可植入後門或提取權限的漏洞來逐步入侵，尤其是 AD (Active Directory)、防毒軟體類型的伺服器，因具有檔案分派安裝權限，遭入侵後，修改其群組原則、工作排程，即可大量派送安裝勒索軟體，達到索取贖金的目標。

2. 網路釣魚攻擊：勒索軟體可能透過釣魚電子郵件或釣魚網站，誘導受害者點擊執行惡意連結與附件，或是針對性的發起魚叉式網路釣魚攻擊，偽裝成合法的組織、企業或關係人，強化受害者點擊執行惡意檔案的誘因，一旦執行惡意附件，勒索軟體就開始對檔案加密，若是惡意連結，則會導向使用者到已掛馬的網頁上，再進行勒索軟體的下載。

3. APT 攻擊：APT 攻擊為潛伏期長且深度隱藏的攻擊手法，攻擊者入侵到內網後，取得管理者帳號密碼等資訊，在內網橫向擴散勒索軟體，再一次性加密多台重要主機資料，將威脅最大化。

4. OT 網路攻擊：在工廠產線的 OT(Operational Technology)網路環境中，勒索軟體會先攻擊 IT 網路設備，而由於 IT 設備與 OT 環境連結，故即使 IT 設備被攻擊不一定會影響到 OT 環境，也可能造成關鍵的工廠操作流程出現問題，例如近期所發生，美國燃油供應商 Colonial Pipeline 遭勒索軟體攻擊而停止服務，甚至讓美國政府宣布進入緊急狀態。

受到勒索軟體攻擊，初期特徵是因為對大量檔案做加密運算，所以會發現硬碟使用率會大幅提升，另外，受影響的檔案通常會被修改副檔名。

檔案被加密結束後，在大多數的狀況下，因勒索軟體需要向受害者要求贖金，所以會將勒索訊息顯示在設備螢幕上，亦或是留下相關文件，也會有連路方式，讓受害者可以與攻擊者溝通付款的議題。

攻擊者甚至可能威脅要在網上發布數據以迫使受害者支付贖金，例如 MAZE 勒索軟體的攻擊者，公佈了 Hammersmith Medicines Research 的醫療檔案以迫使他們支付贖金。

勒索軟體預防措施

個人事前預防措施

1. 保護系統

- 使用防毒軟體，並及時更新系統、軟體和應用程序：攻擊者通常利用未修補的漏洞來訪問未經授權的系統和網路，以執行後續惡意活動。

- 應安裝防毒/防惡意軟體並保持其病毒碼/惡意特徵碼更新。每周至少對系統和網路執行一次掃描，並掃描所有收到的文件。
- 當移動儲存設備連接時應執行防毒掃描。
- 將系統、應用軟體更新到最新版本，並下載最新的安全更新檔。

- 僅在需要時啟用 Microsoft Office 巨集：勒索軟體可能透過惡意 Microsoft Office 檔案感染，誘使受害者啟用巨集以查看檔案內容。
- 提高資安意識：這是防止勒索軟體攻擊的關鍵，應提高資安意識及良好的網路使用習慣，例如識別可疑電子郵件，不要隨意點擊連結，不打開未知或不受信任來源的電子郵件的附件。

2. 保護資料

- 維護更新的備份並保持離線：定期執行資料備份有助於在發生勒索軟體攻擊時恢復資料，而備份資料建議以儲存媒體進行離線儲存。
- 啟用 Windows 受控制資料夾存取功能：微軟已在 Windows10 中內建有資料夾的存取控制功能，但預設並未啟用，需手動調整設定。其功能是限制只有安全的應用程式才能存取特定資料夾，防止勒索軟體對資料進行加密或竊取。

企業組織事前預防措施

企業或組織除前述措施外，需要採取更為積極的方法來保護系統和資料。

1. 保護系統

- 強化具派送功能伺服器安全：防毒軟體中控、AD 伺服器、資產管理系統等因具有軟體派送功能，更需注意安全更新，並密切觀察其群組原則或工作排程不正常異動狀況。
- 最小化開放埠的設置：勒索軟體可能會利用對外曝露的服務和開放埠（例如 RDP 埠 3389 和 SMB 埠 445）在網路中傳播，除了確認其開放的必要性外，還應確認使用這些服務的對象為可信任。
- 實施網路分段區隔並監控流量
  - 在實施網路分段區隔後，如果某一區段受到威脅，至少可限制勒索軟體在網路中的傳播。
  - 監控任何可疑連接的網路流量，並阻止任何與已知惡意 IP、URL 的網路連線行為。

- 在工控環境，更應將 IT 與 OT 環境實施強烈的網路分段區隔措施，避免造成工安問題。

- 實施應用程序控制：應考慮安裝可控制應用程序、目錄白名單的軟體，僅允許執行已批准的程序，以防止惡意軟體程序被執行。
- 人員的最小使用權限：為了減少攻擊者獲得管理權限的機會，應該：
  - 控制和限制存取權限，僅限於需要完整存取權限才能執行工作的人員獲得授權。
  - 為管理者以外的使用者提供工作所需的最低權限。
  - 查看和管理所有使用戶帳戶的使用情況，並禁用非活動帳戶。
  - 實施多因子身份驗證。
- 提高資安意識：應定期對員工進行培訓，建立良好資安意識及網路使用習慣，並進行社交工程演練，提高訓練成效。
- 監控可疑活動：監控可疑掃描活動和未經授權的登錄嘗試，對防止遭到攻擊具有極大幫助。

2. 保護資料

- 加密重要或敏感資料：應對重要或敏感資料進行加密，如果資料被竊取，可以使攻擊者難以處理這些資料，另外，某些勒索軟體僅對常用文件類型（例如圖檔和文檔）起作用，則加密還可以防止它們檢測到文件。
- 維護更新的備份並保持離線：定期執行資料備份有助於在發生勒索軟體攻擊時恢復資料，而備份資料必須離線儲存且不能連接到既有企業網路中，可防止勒索軟體透過網路影響備份資料。
  - 3-2-1 備份原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。
- 定期維護關鍵系統的映像檔：虛擬機或服務器的映像檔包括預先配置的作業系統和相關的應用軟體，當發生攻擊，而需要重建系統，可以利用這些映像檔達到快速部署恢復。

3. 準備事件應變計劃

- 在事件發生之前，制定事件應變計劃並進行演練，以測試計劃是否可行是非常重要的。在受到攻擊時難以即時判斷正確作法，透過已制定好的計劃並實施，將有助於員工了解要採取的行動，並確定各項系統與環境的恢復優先等級。

- 如在工控環境，不只是 IT 環境需要制定事件應變計畫，更應依據設備機台特性分類制定各別的事件應變計畫，以完善整體安全。

被感染後的應變措施

大多數被勒索軟體加密的資料難以被破解，但可採取以下步驟降低影響：

1. 立即斷開受感染設備與所有網路的連接，無論是有線、無線還是基於行動網路。在非常嚴重的情況下，可考慮關閉 Wi-Fi、禁用任何核心網路連接（包括交換機）以及斷開 internet 連接。
2. 重置包括密碼在內的權限憑證。
3. 確認受感染設備已完全的清除並重新安裝作業系統。
4. 在利用備份進行還原之前，需確認該備份沒有任何惡意軟體，如果已非常確認備份和連接它的設備是乾淨的，則恢復工作應該只從備份進行。
5. 將設備連接到乾淨的網路，以便下載、安裝和更新作業系統和所有其他軟體。
6. 安裝、更新和執行防毒軟體。
7. 監控網路流量並執行防毒掃描以確定是否仍有感染。
8. 大多數被勒索軟體加密的資料難以被破解，但仍可嘗試透過勒索軟體名稱、副檔名等資訊，檢閱該病毒的類型，在 no more ransom project[1] 的網站上，尋找可信任資安單位提供的解密工具。
9. 可尋求外部資安專業單位協助事件處理。
10. 建議將攻擊事件資訊藉由 TWCERT/CC[2]分享，以幫助國內外其它企業組織防範相關攻擊，減少勒索軟體的影響。

[1] https://www.nomoreransom.org/zht_Hant/decryption-tools.html

[2] https://www.twcert.org.tw