CYBERARK

CYBERARK LABS

# 完全公開：

## 勒索軟體解密

### 檢視加密路徑及緩解策略探討

WWW.CYBERARK.COM

# 前言

勒索軟體是當今最無孔不入且最危險的網路威脅之一。最新的勒索軟體攻擊可在整個公司內迅速散播，削弱用戶的生產力並中斷業務營運長達數小時、甚至數天。2017 年的 WannaCry 攻擊事件感染 150 多個國家地區的 300,000 部電腦，英國國民保健署（NHS）等機構組織陷入大亂，該機構被迫關閉重要醫療設施、取消手術，也不接受患者長達數天。研究公司 Cybersecurity Ventures 預測，到了 2021 年，全球企業每年因勒索軟體的損失將超過 200 億美元。[1]

由於兩個主要原因，勒索軟體已成為投機性攻擊者的首選勒索手段。首先，在備份及復原能力方面，許多組織未養成良好的安全習慣。一般組織都很少備份資料，即使備份也是偶爾為之，這意味著一旦終端及伺服器上的資料被加密及挾持以要求贖金，組織就只能交出比特幣希望能換回資料，不然就眼睜睜看著重要資料永久遺失。其次，許多組織都依賴傳統防病毒解決方案，但這些方案通常無法有效攔阻勒索軟體。這些解決方案的運作方向，都是維護一個已知惡意軟體清單並阻止該惡意軟體未來執行。由於勒索軟體檔案會隨著每個新版本略為變化，而且分分鐘都有新版本產生，傳統防病毒解決方案幾乎不可能預防感染。

本文記述 CyberArk Labs 為調查勒索軟體並了解哪種潛在緩解策略最有效所做的研究。其中一個主要發現是，如果移除本機管理員權限且應用程式控制政策設置到位時，便能阻止 100% 的勒索軟體樣本執行檔案加密。

## 內容

前言 ..... 2
建立實境勒索軟體實驗室 ..... 2
分析加密路徑 ..... 3
探討勒索軟體類型的共通點 ..... 5
評估緩解策略 ..... 6
建議 ..... 7
總結 ..... 7

勒索軟體攻擊的真正代價遠超出所付的贖金。勒索軟體攻擊可能會阻礙業務發展、傷害公司聲譽及影響利潤。2017 年 NotPetya 勒索軟體攻擊使聯邦快遞公司蒙受足足 3 億美元的收益損失。[2]

# 建立實境勒索軟體實驗室

為進行這項研究，CyberArk 需要真實的勒索軟體樣本以及一個可測試勒索軟體的真實實驗室環境。CyberArk Labs 團隊是內部團隊，為開發創新的資安解決方案以應對新出現的威脅及合規挑戰而成立，他們打造出一個配有實體機器及真實檔案的專門實驗室，能夠讓勒索軟體就像在受害組織內一樣執行及傳播。團隊迄今測試過 250 多萬個勒索軟體樣本，目前每天仍在不斷測試新樣本。樣本代表來自數十種不同惡意軟體家族的勒索軟體，其中來自 Cryptolocker、Petya 和 Locky 的樣本數量最多，它們正是目前最常見且惡名昭著的勒索軟體家族。

以勒索軟體的分支數量來看，這 250 多萬種樣本只是所有勒索軟體的一小部分。不過，基於勒索軟體的多態性，這些樣本在整體勒索軟體之中的代表性很高。儘管每個新版本勒索軟體與前一版略有不同，但所有版本都有相同的感染及執行方法。它們只有不同的檔案雜湊值，以便躲避偵測。

[1] Cybersecurity Ventures，2020 年
[2] https://www.reuters.com/article/us-fedex-results/cyber-attack-hurricane-weigh-on-fedex-quarterly-profit-idUSKCN1BU2RG

這項研究的目的在於分析所測試的勒索軟體樣本的行為，以決定哪種策略或許最能有效減輕這些攻擊造成的損害。因此，團隊考量的是以下策略的優點與挑戰：

- 應用程式允許
- 應用程式封鎖
- 應用程式限制
- 最小特權
- 備份及復原

## 分析加密路徑

在評估潛在的緩解策略之前，研究團隊首先試圖了解勒索軟體的典型行為。圖 1 所示為大多數勒索軟體樣本在開始執行之後遵循的典型工作流程。一個有趣的發現是，儘管各種勒索軟體家族採取相似的工作流程，但不同的家族具有不同的「觸發器」，即促使勒索軟體執行的動作。有些家族立即開始執行，有些家族則等待網際網路連線，有些家族等待滑鼠游標移動，另一些家族等待某個 Microsoft Office 應用程式執行。

### 解密：4 種勒索軟體家族

**迷宮式勒索軟體** – 勒索軟體的新趨勢之一，這些樣本會洩漏用戶的檔案，而不只是加密。攻擊者將威脅若未支付贖金便會發佈資料。

**冠狀病毒勒索軟體** – 一種趁著 covid19 疫情興風作浪的勒索軟體。它與憑證竊取程序（KPOT）一起傳遞。

**蛇式勒索軟體** – 一種鎖定目標企業的勒索軟體，採用 Golang 編寫並將程式碼混淆。感染一部機器之後，蛇將開始例常的勒索軟體行為，例如從系統刪除影子副本及備份、將用戶檔案加密等。值得注意的是，它會消除系統上與工業控制系統和 SCADA 相關的所有程序，以便對其檔案進行加密。

**Snatch 勒索軟體** – 一種獨特的勒索軟體，透過執行在安全模式下運作的惡意活動來停用許多安全產品。

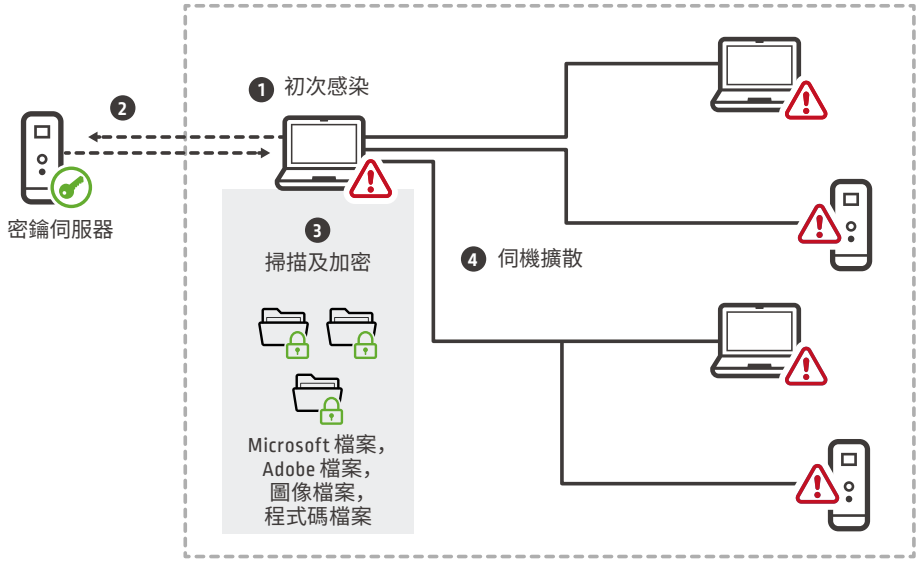


*圖 1：勒索軟體流程*

勒索軟體被觸發執行之後，分析的樣本中有 90% 會先試圖與攻擊者管理的密鑰伺服器進行通信，該伺服器保存著用來加密機器上檔案的唯一公共密鑰。在 20% 的案例中，若未能建立連線，勒索軟體便會失敗。但還有整整 70% 的勒索軟體樣本即使無法從密鑰伺服器擷取唯一密鑰，也能使用預設公共密鑰執行。顯然此做法對攻擊者的作用不大，因為受害者可能使用一個為解密購買的單一預設解密密鑰，解除使用同一密鑰加密的所有檔案。剩下的 10% 勒索軟體樣本已在本身檔案內建一個唯一公共密鑰，因此無需建立外部連線也能執行。根據此觀察結果，研究團隊指出若組織能限制勒索軟體建立外部連線的能力，則通常可以阻止勒索軟體執行或強迫攻擊者使用預設密鑰，進而將攻擊的金錢損失降至最小。

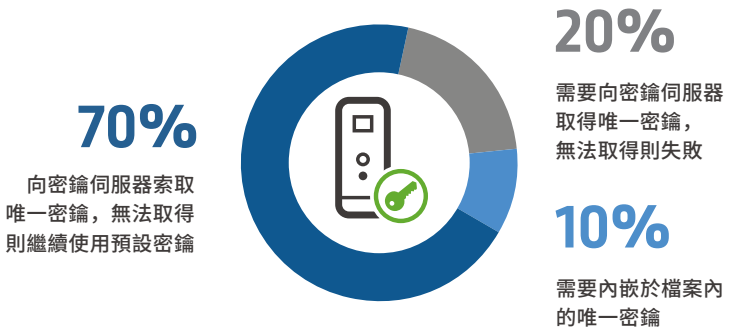


*圖 2：依賴唯一加密密鑰的勒索軟體百分比*

接著，勒索軟體開始掃描受感染的機器，尋找特定類型的檔案。勒索軟體樣本搜尋過數種檔案類型及副檔名，包括：

- Microsoft Office 檔案：.doc, .docx, .xls, .xlsx, .ppt, .pptx
- Adobe 檔案：.pdf, .ai, .psd, .indd, .ps, .eps
- 圖像檔案：.jpeg, .png, .gif, .bmp, .tiff, .pcx, .emf, .rle, .dib
- 程式碼檔案：.c, .h, .cpp, .py, .vb

找到檔案之後，勒索軟體開始加密程序。有些勒索軟體家族會系統化逐個目錄掃描搜尋檔案，並在發現之後立即對其進行加密。在此情況下，整個加密至通知過程僅需數秒至數分鐘時間。其他勒索軟體家族行事則更隱密以躲避偵測。這些家族的樣本首先會產生一份所有欲加密檔案的清單，然後隨機開始加密程序，以躲過終端威脅偵測解決方案的監控。

勒索軟體在忙著加密檔案的同時也會儘可能侵入更多的機器。為此，勒索軟體會在受感染的機器內搜尋已連線的磁碟機、終端和伺服器並儘可能擴散，以最大程度增加挾持勒索贖金的系統數量。這通常以兩種方式進行。第一種方式：大多數勒索軟體樣本都能找到可從受感染終端存取的共用磁碟機及網路磁碟機。如果用戶帳戶可存取這些磁碟機，則勒索軟體也能存取。第二種方式：勒索軟體樣本經常掃描尋找連線的機器，並嘗試重新使用用戶憑證來存取這些機器。如果登入成功，勒索軟體便能夠擴散，以增加受感染機器的總數量並提高受害者的復原成本。

一旦完成加密程序且勒索軟體開始嘗試透過網路傳播之後，用戶便會收到一則類似圖 4 的勒索通知。為了取得解密受影響檔案所需的密鑰，用戶必須向攻擊者支付款項（贖金）。付款通常要求以比特幣支付，對於比特幣新手，有些攻擊者甚至會設立「服務台」來協助受害者購買比特幣並完成資金轉移。


*圖 3：向遭受 CTB-Locker 感染的用戶發出的勒索軟體通知。*

# 探討勒索軟體家族的共通點

儘管不同勒索軟體家族的樣本特徵略有不同，但它們都有三個共通點：

- 它們可輕易感染機器
- 一旦發生感染，絕大多數檔案都會加密
- 勒索軟體檔案本身很容易刪除

## 感染

必須知道的是，傳統的防病毒軟體通常無法有效阻止勒索軟體。這是因為傳統的防病毒軟體依賴已知的黑名單，這意味著必須已得知特定的惡意軟體（即必須已感染至少一部機器）才能將它加入黑名單。由於大多數勒索軟體家族具備多態性，因此沒有任何兩個樣本完全相同。相反的，攻擊者會為每個新的目標受害者快速建立一種全新、略為變種的惡意軟體，永遠比黑名單技術搶先一步並避開偵測。

勒索軟體易於感染，研究團隊因此得出結論，雖然使用防病毒軟體可確保良好的安全，但對多態性惡意軟體仍然無效。為了防止勒索軟體感染機器，組織必須採取更主動預防性的做法來保護終端和伺服器安全，例如限制或封鎖某些應用程式。

## 加密

必須知道的第二點是，儘管許多現代惡意軟體需要本機管理員權限才能正確執行，但許多勒索軟體卻不需要這些權限。

研究團隊因此得出一個結論，儘管組織應刪除本機管理員權限，但他們也必須主動控制應用程式以防止檔案被加密。具體而言，CyberArk Lab 團隊已證明，當未知應用程式拒絕讀取、寫入及修改檔案特權，同時將本機管理員權限刪除，可百分百防止由勒索軟體發起的檔案加密。

## 清除

不同於某些不易定位及刪除的複雜惡意軟體，所分析的勒索軟體樣本一旦被偵測到，便很容易定位及刪除。這意味著，主動備份檔案的受害組織可以大大減低勒索軟體的危害，而無需煩惱該不該支付昂貴贖金以免永久失去資料了。相反的，一旦檔案被加密，受害組織便可在受感染機器上找到勒索軟體檔案，將它們從系統中刪除，然後從備份中復原受影響的檔案。

因此，主動備份終端及伺服器上的檔案有助減輕勒索軟體造成的損害。經常備份高價值檔案可讓組織更容易從勒索軟體攻擊中復原，並可減低這類惡意軟體所造成的損害影響。

# 評估緩解策略

在選擇一種或多種技術來緩解勒索軟體相關風險之前，組織應考量每種選擇的效益與挑戰。本節介紹經過 CyberArk Lab 團隊評估及測試的緩解策略，以及每種策略的優缺點。

**研究表明，限制應用程式與刪除本機管理員權限雙管齊下，可百分百有效防止勒索軟體對檔案進行加密。**

## 允許應用程式

從本質上，應用程式允許在阻止勒索軟體方面百分百有效，因為它可阻止所有未被明確信任的應用程式滲入環境。雖然這種緩解策略在預防勒索軟體攻擊方面非常有效， 但實務上要做好這件事極其困難。為了有效允許應用程式，IT 團隊必須確切了解組織內每個用戶和系統需要哪些應用程式及應用程式的版本，並且 IT 團隊必須將應用程式的每一個別版本明確列入白名單。對伺服器（一般為靜態伺服器）來說，應用程式允許可能是個理想的做法，但動態的用戶終端通常需要各式各樣的業務應用程式，此做法可能會使用戶的生產力停擺。

## 封鎖應用程式

使用此做法，組織可阻止已知惡意軟體（即已經感染至少一部機器的惡意軟體）在其環境內執行。雖然這有助於偵測及封鎖較舊版本的投機型惡意軟體，但在防禦勒索軟體方面的效用極低。每天都有成千上萬的新勒索軟體樣本釋放，傳統的應用程式封鎖方式根本無法跟上。[3] 因此，研究團隊確定即使封鎖應用程式是一般的最佳做法，但它對偵測或阻止勒索軟體無效。

## 限制應用程式

使用此做法，組織可阻止已知、被封鎖的惡意軟體在其環境內執行，同時限制所有未明確信任之應用程式的可用權限。相較於允許應用程式，此做法更靈活，並可阻止未知的應用程式執行存取網路及讀取、寫入或修改檔案之類的動作。不僅如此，限制讀取、寫入及修改檔案權限可讓勒索軟體無法取得存取及加密檔案所需的權限。當 CyberArk Lab 團隊利用勒索軟體樣本測試此做法時，在受感染用戶持有本機管理員權限的情況下，該做法在防止檔案加密方面的有效率為 99.97%；對於用戶未持有本機管理員權限的情況，在防止檔案加密方面的有效率為 100%。

## 最小特權

這一步不僅只是良好的安全習慣，也列入 Microsoft 的「十大不變安全法則」之一。有意思的是，雖然只要移除本機管理員權限通常便可有效防止大多數現代惡意軟體造成的損害，但 CyberArk Lab 團隊指出，僅執行此措施只能有效防止所分析的 10% 勒索軟體樣本造成的損害。根據此觀察結果，CyberArk Lab 團隊重申刪除本機管理員權限及控制應用程式雙管齊下的重要性。值得注意的是，在完全移除用戶的本機管理員特權之前，組織應評估其環境，以了解此舉對生產力可能造成的潛在問題。某些合法的業務應用程式及任務需要管理員權限才能正常運作，立即刪除這些權限而未設定所需任務的例外政策可能會導致業務中斷。

[3] http://www.businessinsider.com/fighting-ransomware-with-antivirus-2016-1

## 備份及復原

各個組織的災難復原策略都應考慮到資料備份，自動備份也有助於確保備份完整且最新的檔案。檔案備份無法阻止勒索軟體攻擊，但可大大降低這些攻擊造成的損害。組織無需支付贖金來取回被加密的資料，而只需要從最近的備份中復原受影響的檔案。企業應在備份及儲存的成本與失去、修復及復原資料的成本之間權衡考量，並根據企業各自的風險承受能力及預算決定備份檔案或資產的優先順序。

# 建議

根據 CyberArk Lab 進行的研究結果，團隊建議組織採用以下緩解技術，在不損害業務生產力的情況下減輕勒索軟體的風險。

- 限制用戶終端上的應用程式，以防止未知應用程式（例如新的勒索軟體實例）存取網路並取得加密檔案所需的讀取、寫入及修改權限。
- 允許伺服器上的某些應用程式，以極力提升這些資產的安全性。
- 從標準用戶帳戶刪除本地管理員權限，以減少攻擊面。
- 自動為特定的獲授權任務升級帳戶特權，以保持用戶的生產力，而無需提供不必要的特權。
- 使用防病毒工具防禦常見及已知的惡意軟體。
- 自動而頻密地從終端和伺服器備份資料，以確保有效的災難復原。

為達到最佳效果，CyberArk Lab 建議組織評估其環境，以找出所有包含敏感檔案或高價值檔案的終端及伺服器。在允許靜態伺服器上的應用程式之後，組織應確定終端上哪些檔案類型包含的資訊最為重要（例如：.xlsx、.pptx、.pdf 等）。如此評估可協助組織了解哪些檔案類型最有價值，進而協助組織建立有效的灰名單政策，保護這些檔案類型免受未知應用程式的攻擊。

## 總結

在分析及測試 250多萬個勒索軟體樣本之後，CyberArk Lab 證明有一種主動預防性的替代安全做法可以有效防禦勒索軟體，進而將此類攻擊的影響減至最小。

除了從標準用戶帳戶刪除管理員權限及定期備份資料（這兩種方法均被視為標準 IT 最佳實踐做法）之外，組織還應考慮採用一種限制做法來控制終端上的應用程式。藉此做法，組織可防止既未被明確信任、也未被封鎖的未知應用程式存取網路並取得對預先定義之檔案類型的讀取、寫入及修改權限。如此一來，組織便可專注於保護對惡意應用程式目標（檔案）的存取，而不僅僅依賴在實務上難度極高的多態性惡意軟體偵測能力。在 CyberArk Lab 內進行測試時，應用程式限制及刪除本機管理員權限雙管齊下經證實可百分百有效防止勒索軟體取得存取受保護檔案類型及完成加密程序所需權限。