CYBERARK®

CyberArk Labs

勒索軟體（Ransomware）分析及可行緩解策略

研究

簡介

「勒索軟體 (ransomware)」指企圖感染電腦、盡可能加密最多檔案、並以解密金鑰為要脅，直到受害者按照要求支付贖金的一種惡意軟體。儘管有據可查的現代勒索軟體出現時間可以追溯到 2005 年，但這種惡意軟體最近異常猖獗。僅在 2015 年，就發生近 407,000 起勒索軟體感染事件，受害者為此支付 3.25 億美元的贖金；2016 年[1]，這些數字大幅增加。

由於以下兩方面的原因，勒索軟體已成為機會主義攻擊者進行敲詐勒索的首選途徑。首先，很多公司未採取妥善的備份及復原措施。這些企業很少進行備份或備份間隔時間過長，這意味著保存在終端設備及伺服器中的資料一旦被加密，就會遭受勒索，企業只能忍痛永久性丟失重要資料，否則必須支付比特幣，以期資料能復原。其次，許多公司依賴傳統的防毒解決方案，而這些解決方案在面對勒索軟體時通常束手無策。這些解決方案通常記錄已知惡意軟體的詳細清單，然後阻止這些惡意軟體的發作。由於勒索軟體檔案的每個新版本都會有不同，而且很快就能建立新版本，因此傳統防毒解決方案有效防止感染的機率非常小。

本文介紹 CyberArk Labs 的調查結果，說明什麼是勒索軟體，以及可能最有效的可行緩解策略。一個重要發現是，管理者的權限被撤銷並開始實作應用程式控制原則之後，就可以成功防止所有勒索軟體樣本加密檔案的企圖。

從醫院到學校，再到銀行甚至 NASCAR 團隊，各種組織成為勒索軟體受害者的可能性越來越大。攻擊者要求的贖金額度也有天壤之別；一位受害者曾說，對於每台感染的電腦，攻擊者要求一個比特幣。當時，這相當於每台電腦大約 450 美元[2]；考慮到不同派系的勒索軟體會很快蔓延到整個環境中，因此支付的勒索金額可能會遠遠高於 450 美元。

1 http://cyberthreatalliance.org/cryptowall-report.pdf
2 http://www.securityweek.com/lechiffre-ransomware-hits-indian-banks-pharma-company3

調查方法

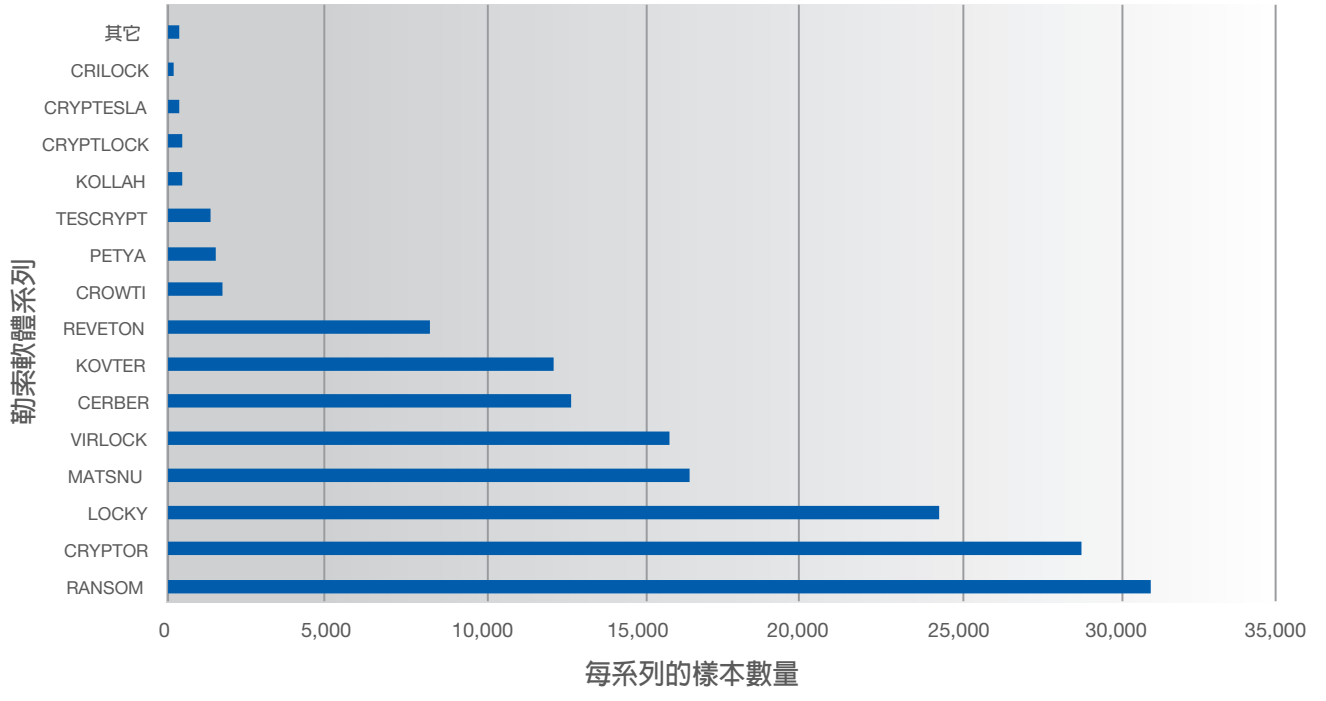
為進行本次調查，CyberArk 使用真實的勒索軟體樣本及可測試勒索軟體的活體實驗室環境。CyberArk Labs 團隊建立專用實驗室，並安裝真正的實體設備及真實檔案，使勒索軟體可以執行並傳播，如同在受害公司內的情況一樣。迄今為止，該團隊已測試超過 157,000 個惡意軟體樣本，而且現在該團隊每天要測試大約 2,000 個新樣本。這些樣本代表來自 30 多個不同惡意軟體系列的勒索軟體，其中最多的樣本來自 Cryptolocker、Locky 及 Matsnu——這些是全世界最常見而且惡名昭彰的勒索軟體系列之一部分。

鑑於勒索軟體系列種類繁多，這 157,000 份測試樣本只是所有勒索軟體中的一小部分。然而，由於勒索軟體的多樣性，這些樣本對所有勒索軟體來說是相當具有代表性的。儘管每個新出現的勒索軟體會與早先的版本略有不同，但所有版本的感染及執行方法大同小異。勒索軟體只是利用不同的檔案雜湊來避開偵測。

本次研究的目的是分析所測試勒索軟體樣本的行為，確定哪些策略最有效能緩解這些攻擊所造成的危害。因此，測試團隊考量以下策略的優勢及挑戰：

- 應用程式白名單
- 應用程式黑名單
- 應用程式灰名單
- 最小權限
- 備份及復原

圖 1：**所測試及分析的每個勒索軟體系列的樣本數量**



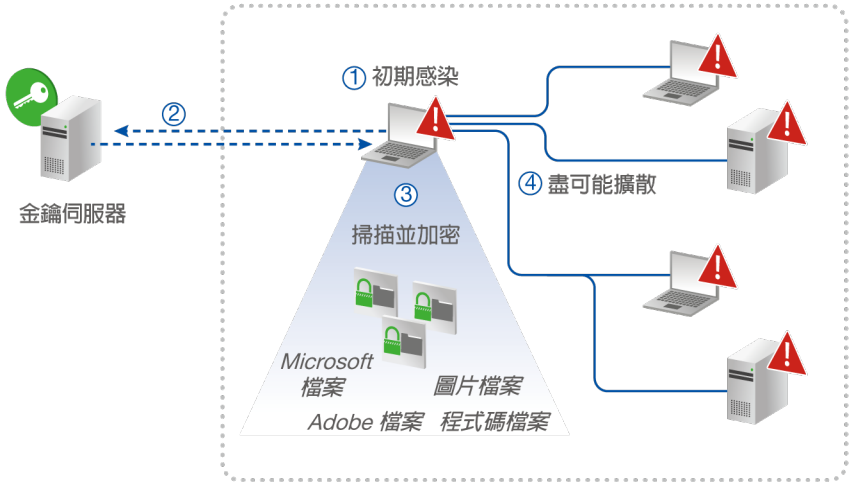
經驗與教訓：加密路徑

在評估潛在的緩解策略之前，研究團隊首先設法瞭解勒索軟體的一般運作方式。第一步驟是瞭解勒索軟體如何滲透到企業中，第二步驟是瞭解感染後出現的情況。

如同大多數惡意軟體，勒索軟體一般也透過網路釣魚或 Web 下載方法傳播，在使用者成為受害者的一刻，勒索軟體會在受害者電腦中植入惡意的可執行檔。然而，為了逃過終端設備防禦措施，某些進階勒索軟體的設計使用看似無害的可執行檔或徹底跳過檔案下載步驟。在這些情況下，一開始勒索軟體執行檔沒有加密功能，因為這會引發告警。而是，在執行完畢後，該檔案會直接下載一個編碼過的程式碼至電腦記憶體中，然後開始從記憶體中執行加密流程，進而避開傳統防毒解決方案的偵測。接著，當受害者執行看似無害的檔案時，該檔案會啟動 cmd.exe，使用 Windows Command Shell 來下載編碼過的 VB 程式程式碼，使用 cscript.exe 執行這個惡意 VB 程式碼，然後啟動檔案加密程序，同時避開許多傳統終端威脅偵測解決方案的偵測。儘管我們測試的大多數勒索軟體樣本未到達此進階程度，但這些例子說明某些勒索軟體發展者的技術水準不容小覷。

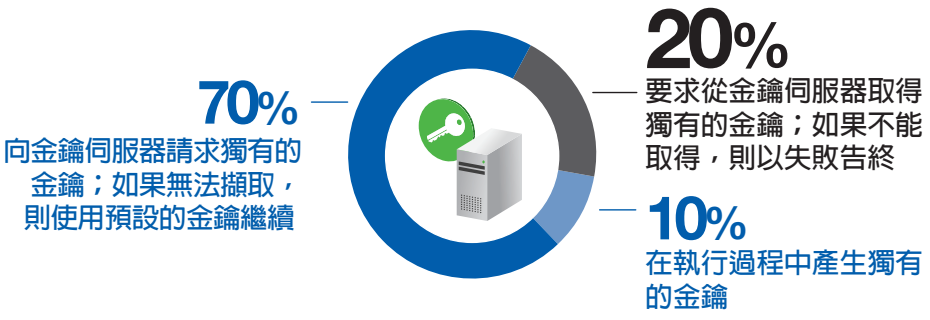
接下來，一旦使用者被感染，勒索軟體就開始執行；大多數勒索軟體版本的行為模式相同。圖 2 顯示大多數勒索軟體開始執行後的常作業流程。

圖 2：**勒索軟體作業流程**



勒索軟體被觸發並開始執行後，分析的樣本中有 90% 首先嘗試與攻擊者所管理的金鑰伺服器進行連線——這台伺服器中儲存用於對電腦中的檔案進行加密的獨有公開金鑰 在 20% 的情況下 如果不能建立連線 勒索軟體就會失敗。然而，即使不能從金鑰伺服器中取得獨有的金鑰，70% 的勒索軟體樣本能夠使用預設的公開金鑰執行。要特別說明的是，這種方法對攻擊者來說可能不太有效，因為受害者可能會使用購買的預設解密金鑰，將使用相同金鑰加密的所有檔案解密。其餘 10% 的的勒索軟體樣本檔案本身含有獨有的金鑰產生器，因此不需要外部連線。根據此發現結果，研究團隊注意到，如果公司能夠限制勒索軟體建立外部連線的能力，一般就能阻止勒索軟體執行，或迫使攻擊者使用預設金鑰，進而最大幅度減小攻擊造成的財務影響。

圖 3：**依賴獨有加密金鑰的勒索軟體百分比**



接下來，勒索軟體開始掃描受感染的電腦，以查找特定類型檔案。勒索軟體樣本搜尋幾種檔案類型及副檔名，包括：

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

找到檔案後，勒索軟體開始進行加密。某些勒索軟體系列的成員會逐步掃描每個目錄中的檔案，然後在發現檔案後立即進行加密。在這些情況下，從加密到通知的整個流程只需要幾秒鐘到幾分鐘時間。而另外一些勒索軟體則更隱秘地進行操作以躲避偵測。這些勒索軟體系列的樣本首先產生要加密的檔案的清單，然後以隨機方式開始加密，以確保不會被終端威脅偵測工具發現。

在忙於加密軟體的同時，勒索軟體同時還嘗試最大幅度增加被感染電腦的數量。為此，勒索軟體搜尋受感染的電腦，查找相連的磁碟機、終端設備及伺服器，並盡可能廣泛地擴散，以最大幅度增加可勒索的系統數量。此步驟通常透過以下兩種方式完成。首先，大多數勒索軟體樣本都能夠查找到共用磁碟機以及可以透過受感染的電腦存取的網路磁碟機。如果使用者帳戶可以存取這些磁碟機，則勒索軟體就可以存取這些磁碟機。其次，勒索軟體樣本通常掃描連線的設備，並嘗試利用該使用者帳號來存取這些機器。如果登入成功，勒索軟體就能夠擴散，進而增加受感染機器的總數，增加受害者的復原成本。

加密操作完成而且勒索軟體開始嘗試透過網路擴散時，使用者就會收到一份勒索通知，如圖 4 所示。若想得到解密被加密檔案所需的解密金鑰，使用者必須支付贖金給攻擊者。一般要求透過比特幣進行贖金支付。對於不熟悉比特幣的新手，某些攻擊者還「體貼地」設立「服務台」，讓受害者知道如何購買比特幣並完成轉帳操作。

圖 4：**被 CTB-Locker 感染後使用者收到的勒索軟體通知**

不同勒索軟體系列的共通性

儘管來自不同勒索軟體系列的樣本的具體特徵互不相同，但勒索軟體有 3 個相同點：

- 可以輕鬆感染電腦
- 一旦感染後，絕大多數檔案會被成功加密
- 勒索軟體檔案可以容易的自行刪除

感染

一個重要發現是，傳統的防毒軟體通常不能有效阻止勒索軟體。這是因為傳統的防毒軟體依賴已知的黑名單，這意味著特定惡意軟體必須已經為我們所知（也就是說，必須已經感染至少一台電腦），然後才能新增到黑名單中。由於大多數勒索軟體系列的多樣性，沒有完全一樣的樣本。通常，針對每個新的目標受害者，攻擊者會迅速開發改頭換面的惡意軟體新變種，使黑名單技術失效並成功避開偵測。此外，某些派系的勒索軟體還可以避開更先進的基於行為分析的終端威脅偵測工具，尤其是從記憶體中或從 Windows Command Shell 中執行的勒索軟體。

感染如此簡單，據此研究團隊得出的結論是：儘管使用防病毒及終端威脅偵測解決方案是有效的安全保護措施，但這些解決方案面對複雜多變的惡意軟體並不總是有效。為了防止勒索軟體感染電腦，企業必須採取更積極主動的方法來保護終端設備及伺服器安全性，如應用程式白名單及 / 或應用程式灰名單。

加密

另一重要發現是，儘管許多現代惡意軟體系列需要本機管理者權限才能正常執行，但很多勒索軟體系列不需要這些管理者權限。儘管有 70% 的勒索軟體嘗試取得本機管理者權限，但如果不能取得這些權限，只有 10% 的勒索軟體最終會以失敗告終。

因此，研究團隊的結論是，企業應該撤銷本機管理員權限，同時亦應該積極主動控制應用程式以防止檔案加密。特別需要強調的是，CyberArk Labs 團隊證明，在所有情況中，禁止未知應用程式執行讀取、寫入及修改檔案的操作並撤銷本機管理員權限，就可以防止勒索軟體導致的檔案加密。

研究顯示，透過結合使用應用程式灰名單及撤銷本機管理者權限的方法，就可以**100% 有效防止勒索軟體對檔案進行加密。**

刪除

與有些很難查找並刪除的複雜惡意軟體不同處在於 受分析的勒索軟體樣本一旦被偵測到就可以很容易找到並刪除。這意味著受害企業如果平時積極主動備份檔案，就可以大幅減小勒索軟體的影響，而且不需要在支付高額贖金及永久性丟失資料之間做出選擇。反而是，檔案被加密後，受害企業可以找到受感染電腦中的勒索軟體檔案，從系統中刪除勒索軟體檔案，然後從備份復原受感染的檔案即可。

因此，積極主動備份終端設備及伺服器中的檔案，有助於緩解勒索軟體造成的危害。定期備份重要的檔案，有助於更輕鬆地從勒索軟體攻擊中復原，減小這種惡意軟體造成的危害及影響。

評估緩解策略

在選擇一種或多種方法來緩解勒索軟體造成的風險之前，企業應全面考慮每種選項的優勢及挑戰。本段落描述 CyberArk Labs 團隊進行評估及測試的緩解策略，以及各自的優劣勢。

應用程式白名單

本質上，應用程式白名單對於阻止勒索軟體 100% 有效，因為應用程式白名單可以阻止不完全可信的應用程式滲透到環境中。儘管這種緩解策略在防止勒索軟體攻擊方面非常有效，但在實務中很難做到此點。若想有效實施應用程式白名單策略，IT 團隊必須精確地知道企業內的每個使用者及每個系統需要哪些應用程式以及哪些應用程式版本，然後明確地將每個應用程式版本列入到白名單中。對於一般具有靜態特點的伺服器，應用程式白名單可能是最理想的方法；但對於通常要求執行多種企業應用程式的使用者來說，這種方法可能會中斷使用者工作。

應用程式黑名單

利用應用程式黑名單，企業可以防止已知惡意軟體（即，已經感染至少一台電腦的惡意軟體）在公司環境中執行。儘管應用程式黑名單有助於偵測及阻止舊版機會主義惡意軟體，但在防止勒索軟體方面卻不是非常有效。每天，成千上萬種新的勒索軟體樣本如雨後春筍般出現，讓傳統黑名單方法束手無策[3]。因此，研究團隊認為，儘管應用程式黑名單總體來說是一種最佳實踐，但在偵測或防止勒索軟體方面卻效果不彰。

應用程式灰名單

利用應用程式灰名單，企業可以防止已列入黑名單的已知惡意軟體在其環境中執行，並限制未完全可信賴的應用程式之權限。應用程式灰名單比白名單更靈活，而且可用於防止未知應用程式執行存取網際網路及讀取、寫入或修改檔案等操作。如果不能存取網際網路，勒索軟體就不能存取其金鑰伺服器。這樣就使 20% 的勒索軟體立即失效，使另外 70% 的勒索軟體必須使用預設金鑰嘗試進行加密。更重要的是，透過限制讀取、寫入及修改檔案的權限，勒索軟體就不能取得存取及加密檔案所需的權限。CyberArk Labs 團隊利用勒索軟體樣本測試應用程式灰名單時發現，如果受感染的使用者擁有本機管理者權限，則在 99.993% 的情況下可以有效防止檔案被加密；如果該使用者沒有本機管理者權限，則可以 100% 有效防止檔案加密。

最小權限

最小權限不僅是良好習慣，而且還列入 Microsoft 的「10 大不變的安全法則（Ten Immutable Laws of Security）」。有趣的是，儘管單靠撤銷本機管理者權限通常就能有效防止大多數現代惡意軟體造成的危害，但 CyberArk Labs 團隊注意到，在分析的所有勒索軟體樣本中，最小權限只能有效防止其中 10% 造成危害。根據此發現，CyberArk Labs 團隊重申撤銷本機管理者權限及控制應用程式雙管齊下的重要性。尤其需要強調的是，在全面撤銷使用者的本機管理者權限之前，企業應該全面評估自己的環境，瞭解此做法造成的工作效率挑戰。某些合法的企業應用程式及工作需求管理者權限才能正常執行，如果全面性立即撤銷這些管理者權限，可能會導致業務運營中斷。

備份及復原

資料備份應該成為企業災難復原策略的一部分，而自動備份可以確保備份檔案的完整性及最新狀態。檔案備份不能防止勒索軟體攻擊的發生，但可大幅減小這些攻擊造成的危害。企業只需要從最近的備份中復原受影響的檔案，而不需要支付贖金來復原被加密的資料。企業應權衡資料丟失及復原的成本與備份及儲存成本，並根據公司的具體風險容忍能力及預算來訂定檔案或資產的優先順序。

3 http://www.businessinsider.com/fighting-ransomware-with-antivirus-2016-19

建議

根據在 CyberArk Lab 進行的研究，團隊建議企業利用以下緩解方法來降低勒索軟體相關的風險，同時避免影響企業工作效率。

- 在使用者終端設備上設置應用程式灰名單，防止新的勒索軟體等未知應用程式存取網際網路並取得加密檔案所需的讀取、寫入及修改檔案權限。
- 在伺服器上使用應用程式白名單來最大幅度提高這些資產的安全性。
- 撤銷普通使用者帳戶的本機管理者權限以減小攻擊面。
- 自動提升特定授權使用者的帳戶權限，讓使用者可以高效率工作，同時避免授予不必要的權限。
- 使用防毒工具來防止常見的已知惡意軟體。
- 以自動方式定期備份終端設備及伺服器中的資料，實現有效的災難復原。

總結

在分析及測試 157,000 多個勒索軟體樣本後，CyberArk Labs 證明，另外一種主動安全保護方法可有效防禦勒索軟體，進而最大幅度減小此類攻擊造成的影響。

除了撤銷普通使用者帳戶的管理者權限並定期備份資料（這兩種方法都被看作是標準 IT 最佳實踐）外，企業還應該考慮採用灰名單方法來在終端設備上進行應用程式控制。利用這種方法，企業就可以防止既不完全可信也沒有列入黑名單的未知應用程式存取網際網路並取得對特定檔案類型的讀取、寫入及修改權限。這樣，企業就可以完整保護對惡意軟體的攻擊目標，而不是單純依賴偵測多種惡意軟體（這在實際應用程式中難度大得令人難以置信）的能力。在 CyberArk Lab 進行的測試表明，如果應用程式灰名單及撤銷本機管理者權限兩種方法雙管齊下，就可以 100% 有效防止勒索軟體取得必要的權限，使勒索軟體無法存取受保護的檔案類型並完成加密流程。

關於 CYBERARK LABS

CyberArk Labs 是一支由網路安全專家組成的團隊，主要致力於研究針對企業網路發起的針對性攻擊，包括攻擊者所使用的方法、工具及技術，以及可用來偵測並緩解此類攻擊的方法及技術。

關於 CYBERARK

CyberArk（NASDAQ：CYBR）是專注化解利用內部權限攻擊企業核心網路的最狡猾攻擊威脅的唯一資安公司。CyberArk 專門致力於阻止網路攻擊，防止網路攻擊造成業務中斷。公司積極主動地防禦網路安全威脅，防止攻擊升級所造成不可彌補的損失。公司深受全世界最領先的公司信賴，包括 40% 的財富 100 大公司及全球 20 大銀行中的 17 家。這些公司利用 CyberArk 的解決方案來保護最寶貴的資訊資產、基礎架構及應用程式。CyberArk 是一家全球性公司，總部設在以色列 Petach Tikvah，美國總部位於麻塞諸塞州 Newton。公司亦在歐洲、中東及非洲（EMEA）及亞太區設有多個辦事處。有關 CyberArk 的更多資訊請存取：www.cyberark.com。

美國總部

CyberArk

60 Wells Avenue

Newton, MA 02459

1-888-808-9005

或（617）965-1544