# 加密勒索軟體 CryptoLocker 分析報告

李美雯
臺灣大學計算機及資訊網路中心程式設計師
作者：轉載自臺灣大學計資中心北區學術資訊安全維運中心

## 前言

近年來加密勒索軟體大舉入台，不僅一般民眾，連政府機關如鄉公所甚至中研院都蒙受其害。很多人以為加密勒索軟體與自己無關，但其實只要你有收發電子郵件開啟附件，甚至僅瀏覽網頁都有可能感染，而且加密勒索軟體針對的不僅是你的文件檔，更新的勒索軟體甚至已經盯上了遊戲紀錄檔。


圖 1 中研院電腦感染 CryptoLocker 相關新聞報導

另外，針對伺服器 Linux 版本的加密勒索軟體也已開始利用各種主流的 CMS(內容管理平台)平台漏洞進行滲透及加密目錄進行勒索。

## 何謂勒索軟體（Ransomware）

很多人可能都知道電腦會中毒，也知道木馬程式會盜取使用者的帳號密碼之類的資安威脅。但很少人知道什麼是勒索軟體（Ransomware）。其實勒索軟體

（Ransomware）的歷史已超過十年，一開始的勒索軟體（Ransomware）僅限於瀏覽器綁架、系統核心功能鎖定或是螢幕鎖定。隨後強制導引用戶到付款介面，並威脅若不付款則毀壞系統。


圖 2 傳統的勒索軟體畫面 來源: groundlabs.com

這類型的威脅通常可以用防毒軟體或特定的解毒程式來解決，如果無法解鎖的話，也至少能藉由備份硬碟內的檔案並重灌系統來解決此一問題。

然而近年來網路上出現了新形態的加密勒索軟體，其方式並非鎖定系統或瀏覽器，而是將檔案加密後，威脅使用者付款以取得解除加密的金鑰，否則使用者將永遠無法開啟檔案或會被公開檔案。

由於此類加密勒索軟體通常會使用 RSA-2048 加密。已近乎無法破解。且通訊方式和繳付的貨幣都是使用難以追蹤的 Tor（匿名網路）及比特幣（網路貨幣），造成了追查上的難度。

以下我們將介紹此類勒索軟體中較為出名的 CryptoLocker 的運作原理與預防措施。

## 加密勒索軟體 CryptoLocker 介紹

CryptoLocker 通常會偽裝成電子郵件附件，並假冒網站或公家機關的電子郵件以欺騙使用者開啟所附上的檔案，通常是偽裝成 PDF 檔案。也有利用瀏覽器或是瀏覽器外掛漏洞（如 Flash Player 或 Java）假冒網頁廣告誘騙使用者瀏覽或點擊，或是經由殭屍網路發送的案例。部份情況下也會以宙斯木馬為前導，成功入侵後再下載並安裝 CryptoLocker。

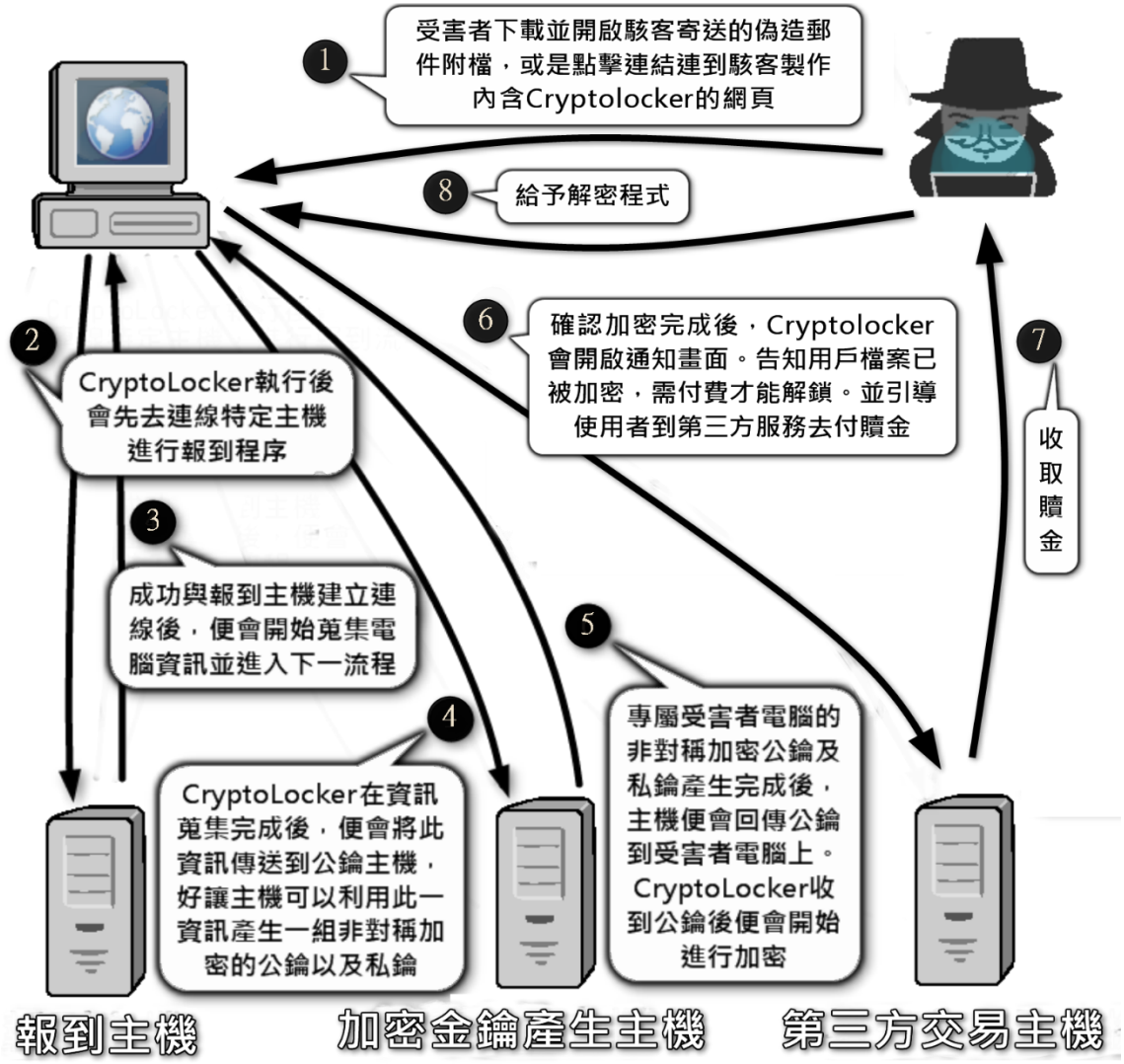


圖 3 攻擊流程圖

CryptoLocker 第一次執行時會以隨機名稱自行安裝於我的文件，並修改登錄檔以便在開機時自行啟動。後續會連接勒索者所控制的伺服器進行報到。報到成功後便會蒐集電腦資訊加密傳送到伺服器。伺服器利用此資訊產生一組非對稱加密的公鑰以及私鑰，並將公鑰加密回傳給受感染的電腦。

CryptoLocker 收到公鑰後，會把整個硬碟與相連結的網路硬碟（僅限支援的網路芳鄰及本身有在系統內存在同步資料夾的網路硬碟服務）中的檔案利用公鑰進行加密。同時也會破壞常見的備份檔案（如 Windows 內建的還原功能）。加密過程中僅會將特定附檔名的資料檔案進行加密，例如文件、試算表或是簡報檔案、圖檔或 AutoCAD 檔案。

整個加密的流程結束後，CryptoLocker 便會顯示訊息告知用戶檔案已經被加密，必須支付現金或比特幣才能解開這些檔案。並告知付款動作必須在時限內完成，否則會銷毀私鑰、增加贖金或公布持有的檔案。

若被害者妥協付款，則會在確認付款後，讓用戶下載預載用戶私人金鑰的解密程式，以供用戶使用解密檔案，有些變種為了取信用戶，還會分次加密，以在

客戶聯繫時，提供解除部分檔案加密的金鑰以取信顧客，好得到解除剩餘檔案加密的贖金。

## CryptoLocker 預防措施

並非所有的安全軟體都能偵測到 CryptoLocker，有些防毒軟體只能在加密進行或完成後才能偵測到 CryptoLocker。想要預防 CryptoLocker，最好的方式是培養良好的資安觀念。

基本原則是不開啟可疑來源的連結（譬如以短網址或轉址廣告連結呈現的網址）或是附加檔案（譬如沒有給予電子信箱資訊的單位來信並給予附件檔案要求開啟操作）從來源方面來阻擋受感染的可能性。

有鑑於加密勒索軟體也常使用已知的常用軟體或瀏覽器外掛漏洞進行攻擊，平時勤於更新瀏覽器、Flash Player 或 JAVA 等瀏覽器外掛程式以及作業系統也是預防的方法之一。

加密勒索軟體除了偽裝機關來信引誘開啟附檔、以短連結附上錯誤說明欺騙使用者造訪惡意網站或頁面外，也會透過第三方廣告投放系統散播，在日本先前就有出現知名影音網站的內嵌廣告和討論區開啟外部連結會出現的轉址廣告夾帶 CryptoLocker 的狀況。也因此如果有出現重大的安全漏洞發布但卻還沒得到廠商更新時，可以考慮先以阻擋廣告的方式來避免。

即使安全軟體有時無法偵測到最新或變種的加密勒索軟體，以至於使用者感染加密勒索軟體，使用者若能在加密勒索軟體進行加密一開始時，藉由觀察檔案名稱附檔名出現異常變化或是發覺系統運作效能異常低落等跡象，進而發現中毒並及時進行斷網關機，惡意軟體有時只會加密到一小部分的檔案。斷網關機後使用 PE 等系統救援工具立即清除該惡意軟體並進行資料備份，也可以降低資料的傷害數量。

使用者平時也應養成定期的異地檔案備份習慣（譬如使用外接硬碟儲存重要檔案），這樣即使遭受加密勒索軟體威脅，也可以不用支付贖金，而直接進行磁區或系統還原，或重新安裝作業系統。

## 參考資料

1. 維基百科 CryptoLocker 條目 https://zh.wikipedia.org/wiki/CryptoLocker。
2. 維基百科 Ransomware 條目 https://en.wikipedia.org/wiki/Ransomware
3. 網管注意！勒贖軟體已盯上 Linux 網站 http://www.ithome.com.tw/news/99865
4. 傳統勒索軟體圖片來源

http://blog./ransomware-attacks-on-the-rise-what-are-you-doing-to-protect-your-business

5. 趨勢科技加密勒索軟體 TAG http://blog.trendmicro.com.tw/?tag=加密勒索軟體
6. 緊急處理加密勒索軟體威脅 7 原則 http://www.ithome.com.tw/tech/101366
7. 加密勒索軟體威脅透過廣告傳播
   http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/
8. 加密勒索軟體利用 Joomla Zero-Day 進行滲透及加密目錄，以勒索使用者
   http://news.softpedia.com/news/joomla-zero-day-accounted-for-the-majority-of-web-attacks-in-q4-2015-499742.shtml
9. 加密勒索軟體利用 Flash Player Zero-Day 進行滲透
   http://news.softpedia.com/news/recently-fixed-flash-player-zero-day-used-to-deliver-ransomware-485522.shtml
10. http://blog.groundlabs.com/ransomware-attacks-on-the-rise-what-are-you-doing-to-protect-your-business
11. 網頁廣告成勒索軟體散播溫床，紐約時報、BBC、MSN 皆中招
    http://technews.tw/2016/03/18/web-advertising-ransomware-json/