德國品質
專業技術
SINCE 1985

G Data

CTB-Locker

惡意勒索軟體分析

惡意勒索軟體

何謂惡意勒索軟體（Ransomware）:

駭客利用木馬程式或釣魚郵件等將表面上不會對系統造成迫害的軟體殖入電腦中，等到用戶不經意觸發執行該軟體，就會與伺服器連線並啟動該軟體的功能，進而對電腦中的檔案造成一些不可預期的動作！駭客團體再經由此軟體發佈訊息，此訊息大概的意思皆為如果要讓電腦恢復原狀必須經由付費的方式來達成；此一行為與勒索無異，因而稱為**惡意勒索軟體**。

勒索軟體來源：

最早的勒索軟體出現於 2005 年，在俄羅斯境內出現！期後開始全球傳播，駭客集團將這些勒索付費稱之為「贖金」，再轉變以「罰款」的形式出現，讓使用者不得不馬上支付。更甚者還有的透過本土語音訊息傳播勒索公告！

傳播模式：

1. 假冒知名網路商發佈釣魚郵件進行傳播（Chrome、Facebook、PayPal 等）
2. 透過惡意網址進行木馬及不明軟體安裝

CTB - Locker 及其變種 CryptoLocker：

執行該軟體所造成的危害：

該惡意軟體會嘗試連接被勒索者所控制的伺服器，成功連接後伺服器就會產生一組 2048 位元的 RSA 加密金鑰配對，並且送出公開金鑰到被感染的電腦；同時也會有效將整個硬碟與其相連結的網路硬碟中的檔案，利用公開金鑰進行加密，並將檔案加密的紀錄存入一個登錄碼。這個過程中，會將特定副檔名的資料檔案進行加密。

駭客源頭追捕困難：

CryptoLocker 伺服器可能是一個本地或其他的代理伺服器，會頻繁地在不同國家間進行重新定位，造成追蹤源頭的困難度。

防範困難點：

使用者部份

1. 對於未知異常郵件（E-Mail）沒有足夠的警覺心
2. 隨意開啟未知郵件的附件檔案
3. 隨意下載具有風險的軟體
4. 隨意點擊未知的連結

作業系統部份

1. Windows XP 微軟已不支援更新，但大多數企業都還在使用此系統，安全漏洞過多！
2. 建議將作業系統提升至 Windows 7 或以上
3. 未定期將所有微軟作業系統 Windows Update【安全性更新】全都更新至最新！
4. 使用非法授權破解版微軟系統

勒索程度：

※ 被駭 PC 索價 11,900 台幣或 300 美元，或是兩比特幣。

※ 72 小時未付款，私人金鑰將會在伺服器端摧毀，並且無法打開這些被加密的檔案。

※ 超過 72 小時，付款價格將會增長到十比特幣。(約 3250 美金 2014.10)

※ 一旦被駭導致檔案經加密演算法被鎖，目前無可行的解法。

※ 一台 PC 被駭，經由內網極有可能全公司網路檔案全遭殃。

※ 因加密共享文件而會占用公司頻寬，區網會變的很緩慢。

CryptoLocker 預防勝於治療：

1. 該軟體為多語系：中文 (繁體、簡体)、英文、西班牙文、德文、日文、韓文、泰文。
2. 感染途徑：
   (1) 竄改瀏覽器使其導向惡意網站
   (2) 發佈釣魚郵件進行傳播
   (3) 點選彈跳視窗時強制安裝此木馬。
3. 下列未更新受感染的機率越大 (請協助電腦端升級軟體版本以及移除不明的軟體)
   (1) 舊版 Java　　(2) 舊版 Adobe Reader
   (3) 舊版 Adobe Flash Player　　(4) 沒有將 Windows Update 更新到最新
4. 由於微軟已不支援 Windows XP，建議用戶更新作業系統為 Windows 7 或以上
5. 少點閱一些不明的 Mail (未知寄件者、來信標題或內容亂碼怪異、夾帶檔為 *.exe 等)
6. 定期的檔案備份可以減輕檔案遺失或被加密的風險 (異地備份，外接裝置備份等)

不幸遭此勒索軟體入侵緊急處理事項

1. 馬上拔掉網路線：避免透過區域網路傳染給辦公室或家裡的其他電腦。
2. 如果檔案加密的工作還沒全部執行完成，強制關機並把硬碟拔起來再用其他電腦
   (最好是 Linux 或 Mac 作業系統) 去讀硬碟，也許還有機會把未被加密的檔案救出來！
3. 完整格式化硬碟後重灌電腦。

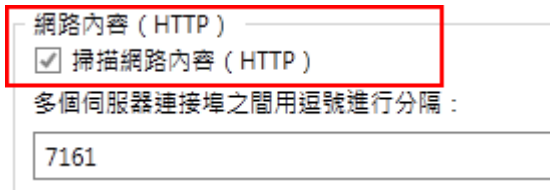
G Data 建議事項（企業版主控台：建議開啟雙引擎做防護）

CryptoLocker 主要由 Mail 及網頁為傳播途徑，下列步驟將使您的 G Data 防護更加嚴謹

1. 事先一定要安裝 G Data 防毒軟體並把病毒特徵碼更新至最新
2. 用戶端設置 > 電子郵件 > 爆發護盾；請勾選 已啟用

3. 用戶端設置 > 電子郵件 > Outlook 防護；請勾選 透過整合外掛模組防護 Microsoft Outlook

4. 用戶端設置 > 網頁 / 即時通訊 > 掃描網路內容；請勾選 掃描網路內容（HTTP）



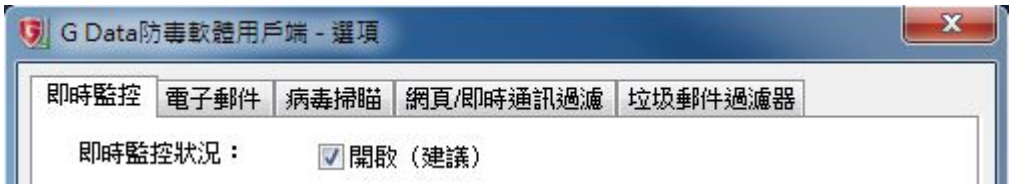
5. 用戶端設置 > 即時監控 > 行為監控；請勾選 已啟用

6. 用戶端設置 > 即時監控 > 監控狀態；請勾選 開啟（建議）

G Data 建議事項（企業版 Client 端：建議開啟雙引擎做防護）

CryptoLocker 主要由 Mail 及網頁為傳播途徑，下列步驟將使您的 G Data 防護更加嚴謹

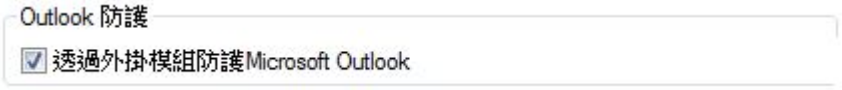
1. 即時監控 > 即時監控狀況；請勾選 開啟（建議）



2. 電子郵件 > 電子郵件防護；請勾選 已啟用（建議）

3. 電子郵件 > 掃描選項；請勾選 爆發護盾

4. 電子郵件 > Outlook 防護；請勾選 透過整合外掛模組防護 Microsoft Outlook



5. 網頁 / 即時通訊過濾 > 掃描網路內容（HTTP）；請勾選 掃描網際網路內容（HTTP）

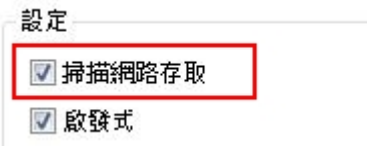
G Data 建議事項（個人版：建議開啟雙引擎做防護）

CryptoLocker 主要由 Mail 及網頁為傳播途徑，下列步驟將使您的 G Data 防護更加嚴謹

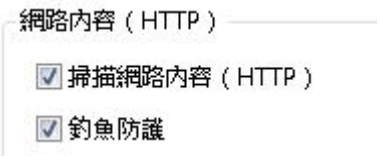
1. 事先一定要安裝 G Data 防毒軟體並把病毒特徵碼更新至最新

2. G Data 主介面 > 即時監控、網頁防護、郵件防護；綠色勾選為啟用狀態

3. 主介面 > 設定 > 病毒防護 > 即時監控 > 進階；請勾選 掃描網路存取



4. 主介面 > 設定 > 病毒防護 > 網頁防護 > 網路內容（HTTP）；請勾選下圖兩功能



5. 主介面 > 設定 > 病毒防護 > 郵件防護 > 掃描選項；請勾選 爆發護盾

CTB - Locker 加密檔案格式彙整：

Microsoft Office：*.xls , *.xlsx , *.xlsb , *.xlsm , *.xlk ,*.ppt , *.pptx , *.pptm , *.doc , *.docx

*.docm , *.pst , *.accdb

Open Office：*.odt , *.ods , *.odp , *.odm , *.odc , *.odb

Adobe：*.pdf , *.psd , *.ai , *.indd

Corel Draw：*.cdr

圖像檔案：*.jpg , *.bay , *.crw , *.sr2 , *.cr2 , *.dng , *.mrw , *.arw , *.jpe , *.ptx , *.srw , *.x3f

*.nef , *.nrw , *.orf , *.raf , *.raw , *.3fr , *.rw2 , *.mef , *.srf , *.eps ,

映像檔案：*.img

文字檔案：*.rtf , *.wpd , *.wps

Web Files：*.der , *.crt , *.cer , *.pem , *.p12 , *.p7b , *.p7c

CAD 檔案：*.dxf , *.dwg

資料庫檔案：*.mdb , *.dbf

影音檔案：*.dcr , *.r3d

資料檔案：*.pdd , *.wb2 , *.kdc

遊戲檔案：*.erf

系統檔：*.pfx

其他檔案：*.pef , *.mdf , *.dxg , *.rwl

CTB - Locker 各語系加密勒索訊息：