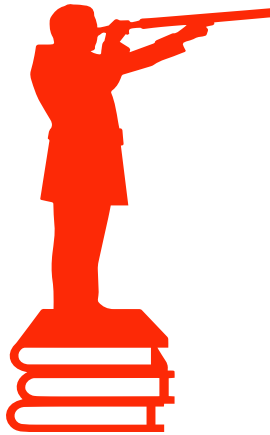

苗栗縣政府
政風處 11月宣導
病毒綁架電腦

資訊安全宣導：病毒綁架電腦

一、中毒途徑與癥兆主要途徑除了透過「社交工程」或其他方式誘騙使用者執行看起來像一般帳單、有 .exe 副檔名的Word或PDF文件、色情的照片或影片的綁架軟體之外，還會透過各種方式以病毒或木馬等方式散布這些惡意程式，甚至還會透過區網傳染給辦公室裡的電腦。

等電腦中毒之後，會發現電腦的檔案、照片、文件、Word、Excel…通通都被鎖起來、全部被改名，無法開啟，如果要使用原本的檔案的話，則會跳出一個說明視窗需要中毒者付錢，方可解鎖。



二、病毒名稱

檔案加密勒索病毒TorrentLocker及2015年4月出現的CryptOLOcker，另外2015年9月還有更新的進化版出現~ 以上勒索病毒至今日仍無復原被加密檔案的方法出現。

加密勒索病毒是如何運作的呢?

加密技術為勒索軟體的重點之一，目前已從過去的對稱式金鑰加密(symmetric key cryptography)改良成非對稱式金鑰加密(asymmetric key cryptography)。
在2017年，林敬黃與王周玉的論文「勒索病毒感染途徑個案鑑識分析中提到，當使用者機器被勒索病毒感染時將透過多個Proxy Server(通常是合法但已被駭客入侵的proxy server)連上C&C(Command&Control)Server請求Public Encryption Key。
在C&C Server中，會為每個感染的機器產生成一對Public/Private Encryption Key，並將Public Encryption Key傳回到受感染的主機（Private Encryption Key不會離開C&C Server）。
然後，Public Encryption Key將用來加密對用戶來說是最重要的文件，勒索成功後，在要求贖金過程，為求隱匿網路位址，要求受害者使用高匿名性的比特幣（Bitcoin）進行贖金支付。

三、檢查是否有感染

這病毒有潛伏期，不會馬上就讓使用者發現檔案被綁架了，可以先用搜尋軟體，檢查電腦有没有以下檔案：(中獎者電腦可能會含有的檔案)

- HELP_TO_SAVE_FILES.txt
- HELP_RESTORE_FILES.txt
- DECRYPT_INSTRUCTIONS
- RECOVERY_FILE.txt
- .encrypted（在原本檔案後加入.encrypted 的副檔名）
- .ezz .ecc .ccc（最新）

四、預防方法：

1.這種加密病毒來源多半是藏在網頁廣告、假網站、非法郵件、隨身碟等，所以建議在使用網路上請特別小心。

2.盡量不要瀏覽未知網站或連結，特別是大陸網站(xxx.xxx.cn)。
不要開啟不熟悉的網頁或是不明電子郵件附件或連結，瀏覽網頁時顯現的彈出式視窗不要點選安裝，也不要安裝非公務使用或是網路流傳之破解軟體，避免感染病毒。

3.開啟電子郵件附件時小心是不是偽裝檔名的 exe 執行檔。

4.請勿使用「空間下載器」或迅雷 P2P 之類的下載工具程式。

5.請勿使用來源不明的隨身碟。

6.最重要的，就是請記得定期備份你的重要資料和郵件，因為被加密後要救也都救不回來，只有全部刪除了！

五、已經中毒的話，該怎麼辦？

1. 發現電腦有異常、開始出現檔案被加密無法開啟等狀況時，馬上拔掉網路線，避免病毒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，馬上關機、把硬碟拔起來再用其他電腦(最好是Linux或Mac)去讀硬碟，看看能不能把未被加密的檔案救出來，也許還有一點點機會。
3. 完整格式化硬碟、清乾淨後，重灌電腦。
4. 記住這次教訓，要常備份、要裝防毒軟體並更新 Windows Update、少開奇怪檔案。

六、一定要用外接硬碟備份！

重要檔案一定要定期備份（重點在定期、常常備份），而且必須使用公務用之外接硬碟、USB 隨身碟、記憶卡或燒成光碟等方式做備份（雲端備份也可以）。

因為當電腦病毒肆虐、開始加密你電腦中的所有文件、照片或影片檔時，萬一妳的外接硬碟或USB隨身碟、記憶卡還連接著電腦，那一定會被牽連、跟著被加密了！

所以為了避免被波及，一定要定期針對重要資料另外備份，不要只是放在同一台電腦或區網裡的其他電腦，而是一定要備份到外接儲存設備，備份完後把線拔掉、另外收起來放！

看起來很麻煩？對，是很麻煩，但是跟所有檔案都被綁架、加密比起來，你會慶幸還好有備份！


THANK YOU
廉政專線:
037-356639
苗栗縣政府
政風處關心您❤