資安通報

(截錄自 2016 年 12 月 08 日 BY TREND LABS 趨勢科技全球技術支援與研發中心)

近日傳出勒索病毒駭人新手法,先盜用 Facebook 帳號,再以私訊假冒好友分享偽造的圖片,誘拐被害者下載惡意瀏覽器外掛,再暗中植入惡名昭彰的勒索病毒 Locky。

提到 Locky ,不得不提到年初的這個案例:Locky 勒索軟體迫使醫院緊急將所有電腦關機,改用紙本作業,四月在台灣有傳出大量散播案例,它利用一封看似發票的信件主旨,加上使用者對 Microsoft Word 檔比較沒有防備的心態,造成不少台灣民眾檔案被綁架。詳情請看:從勒索軟體 Locky 加速散播,看巨集惡意軟體新伎倆

它的變種藉著改良版的漏洞攻擊套件散播,專門攻擊本地端安裝的 Revive 和 OpenX 開放原始碼廣告伺服器,而且台灣是遭攻擊排行榜第一名 !

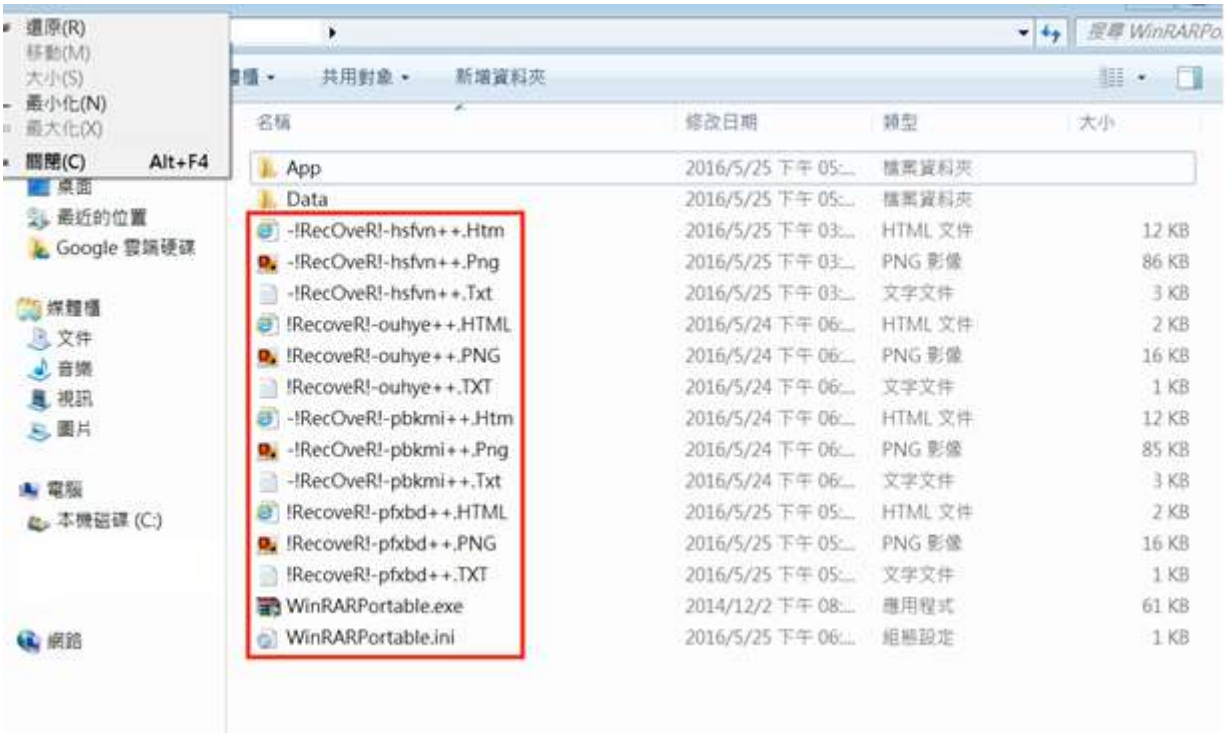
到底感染勒索病毒時會出現什麼症狀?在第一時間該如何緊急處理?我們來重點複習一下:

感染勒索病毒的四個主要症狀

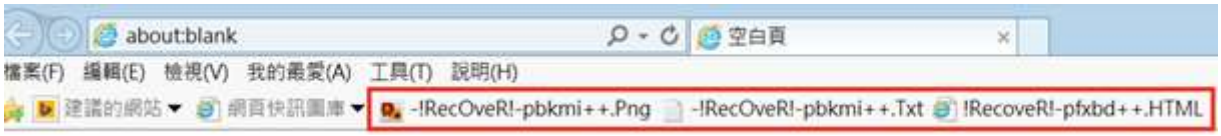
感染勒索病毒時,勒索病毒會連線到 C&C 伺服器下載加密金鑰並且開始加密電腦中的檔案,然後在電腦上放置 Ransom Note 檔案(支付贖金的說明檔案)。因此,當下列症狀出現時,就有可能就是遭到勒索病毒感染:

1. 出現不明對外連線

2. 各目錄下開始出現奇怪副檔名的檔案，例
   如：.crypt、.ECC、.AAA、.XXX、.ZZZ 等等
3. 突然出現很多 Ransom Note 檔案（支付贖金的說明檔案）或捷徑，通常是.txt 檔或是.html 檔，如下圖：



4. 在瀏覽器工具列發現奇怪的捷徑，如下圖：



中了勒索病毒有何緊急措施？

在發現異狀的當下請記得四招：

1. 立即切斷網路，避免將網路磁碟機或共享目錄上的檔案加密。
2. 立即關閉電腦電源：關閉電腦電源的目的是不讓勒索病毒繼續加密電腦中的檔案，關機時間愈快被加密的檔案愈少，建議強制關閉電腦電源
3. 保留電腦，通報專業資安人員
4. 不要付錢

資訊人員的緊急處理措施：

1. 暫時停用帳號，暫時停止該帳號的網路存取權限

2. 檢查該帳號權限可寫入的共享資料夾是否遭受感染
3. 取出硬碟，透過另一台電腦備份尚未加密的檔案

面對勒索病毒的防範之道 :三不三要

面對如此恐怖的勒索病毒，趨勢科技建議採取三不三要：

三不:

- 不上鉤：收到標題吸引人的郵件，務必停看聽
- 不打開：不隨便打開 Email 附件檔案
- 不點擊：不隨意點擊 Email 中的網址

三要

- 要備份：依據 3-2-1 原則妥善備份重要資料—在兩種不同媒介上建立三個備份，其中一個備份要放在不同地方
- 要確認：打開 Email 前要確認寄件者身份
- 要更新：作業程式、軟體、病毒碼要隨時保持更新狀態，當軟體廠商(例如 Flash/SilverLight/IE)公布修補程式請盡快更新。