能仁家商電腦中心資安快報：　　2017/04/14

何為綁架病毒：

現在的加密綁架軟體很可惡！會向受害者勒索金錢，並限時 3 天內付贖金，甚至要求以虛擬貨幣比特幣付款，才能得到可解開加密檔案的私鑰，否則，銷毀私鑰讓受害者再也沒有機會救回檔案

現階段，大多數的加密勒索軟體都是透過釣魚郵件入侵，若使用者風險意識不夠，就很可能受害，導致檔案無法存取。

從大多數的加密勒索病毒的執行過程來看，一般都是會向遠端遙控 C&C 主機取得加密金鑰，再暗中加密受害電腦中的檔案，像是先使用 AES 加密檔案，再用非對稱金鑰 RSA 加密來將 AES 金鑰加密，且金鑰長度是 2048 位元，使用戶難以用暴力方式解開加密，因為即便用超級電腦，都要運算個好幾年才能達到目的。

當用戶電腦中的重要檔案，像是 Word、Excel、PowerPoint、PDF、JPG 檔，等近百種常見檔案格式，都被惡意加密後。加密勒索病毒就會跳出要求付贖金的勒索訊息，並限期在很短時間內（像是 3 天）就要給付，否則銷毀金鑰，讓用戶再也無法解開檔案。同時，勒索給付方式上，為了更隱匿蹤跡，會要求以比特幣等金流機制來給付，才能取得解密金鑰。

當使用者看到勒索訊息時，同時也會發現，無法開啟被加密的檔案，文字檔即便開啟，也會是亂碼顯示。而且，新的變種加密勒索軟體，甚至連檔案名稱也能加密，這將使用戶無法分辨哪些檔案無法使用，可能更影響使用者心理狀態，讓用戶焦慮而順從付款。

感染勒索病毒的四個主要症狀

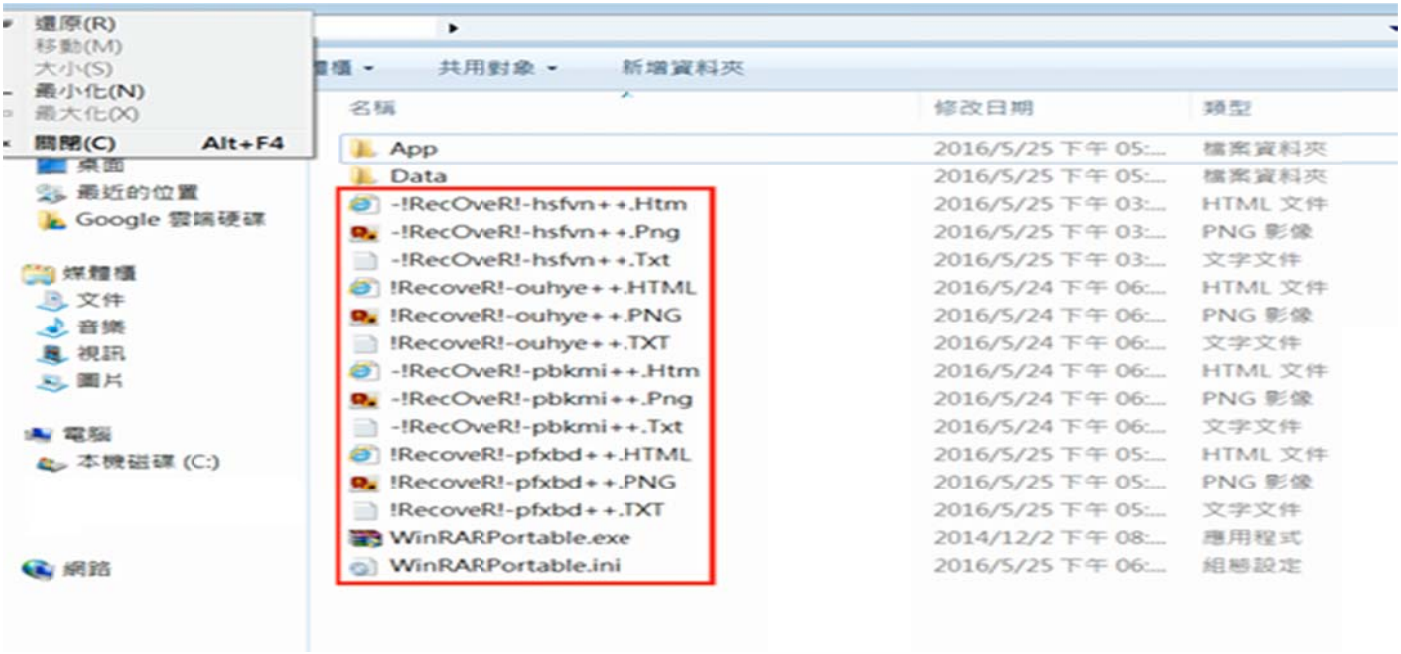
文/羅正漢 | 2015-12-19 發表

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：

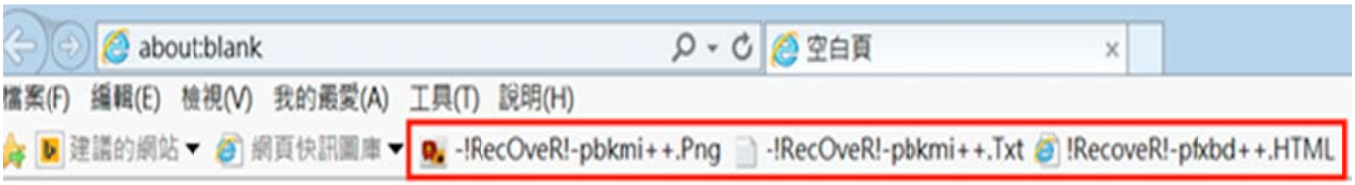
1. 出現不明對外連線
2. 發現各目錄下開始出現奇怪副檔名的檔案，例

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：



Q&A

遭受加密勒索軟體入侵後，真的沒有辦法破解嗎？

大部分的加密勒索軟體，若都是經由 2,048 位元 RSA 和 AES 加密，幾乎已經不可能自行暴力破解救回檔案。

被勒索當下即時處置

1.斷網：斷開網路連線

2.斷電：馬上關機（5 分鐘內還有資料可以救回.. 看電腦速度)

3.保留電腦 通報資訊人員

4.不要付錢

資料來源：https://blog.trendmicro.com.tw/?p=18070