勒索病毒之友善提醒:

近日旅行同業大量傳出勒索病毒災情,受害電腦內的重要檔案都在瞬間一一被加密成.crypl 檔。

根據趨勢科技統計資料顯示,台灣地區勒索病毒攻擊人次在 5 月份達到新高,共計 50 萬人次遭內含勒索病毒的網頁攻擊,較 4 月份成長 3 倍,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,使用戶難以用任何方式方式解開加密,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(如下圖),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。

故提醒旅遊同業謹記**預防勒索軟體綁架電腦之三不及三要如下:**

不上鉤:標題特別吸引人的郵件務必停看聽。

不打開:不隨便打開 email 附件檔。

不點擊:不隨意點擊 email 夾帶的網址。

要備份:重要資料要備份。

要確認:開啟電子郵件前，要確認寄件者身分。

要更新:病毒碼一定要隨時更新。

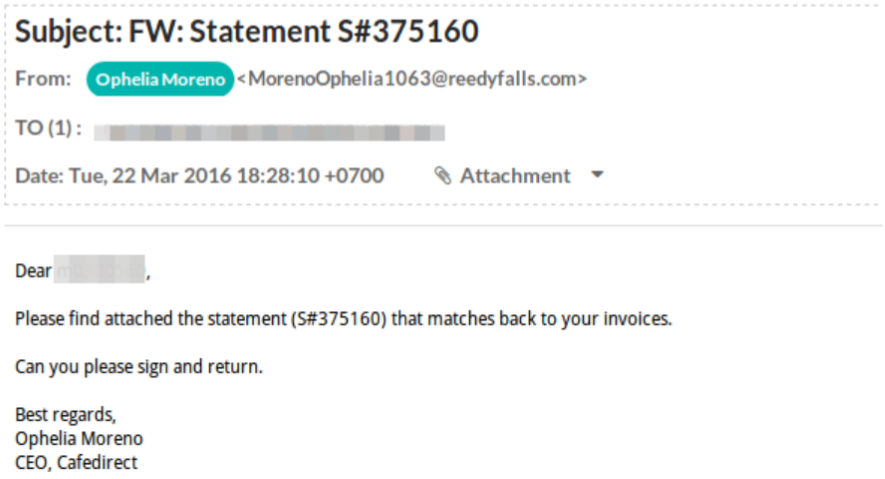
勒索病毒範例郵件如下:

病毒郵件

js附件發票 - 勒索病毒郵件案例

發佈於 3月 23rd, 2016
類型： 病毒郵件

案例的發票郵件附檔zip內含有病毒的js (javascript)檔案，開啟後會啟動Locky勒索軟體，受害電腦會被加密並被勒索贖金。



郵件大意：
『親愛的XXX，隨函附上發票（S＃375160）。希望您能回覆。最好的祝福，...』

點擊附件會下載一個zip壓縮檔，解壓縮後可以看到數個.js的檔案(如下圖)。