作業報導

# ●加密勒索軟體攻擊手法及資安防護研析

內政部警政署資訊室 李權龍

## 壹、前言

勒索病毒最早於2005年在東歐俄羅斯境內出現第一個受害案例，隨著加密技術快速發展，至2013年在金融科技及匿名網路等技術助長下發展更臻成熟，逐漸開始在全球肆虐。臺灣在近2年亦陸續遭受肆虐，根據資安廠商統計2016年受害數量相較去年已有數倍成長，受害企業已經高達252家，達到歷年高峰。

勒索軟體危害越來越猖獗，是2016年最主要的資安攻擊手法之一，必需正視其所帶來的負面效應，強化各式資安防護作為以為因應。

## 貳、問題研析

一、 自2013年起，被稱為史上最狠毒的勒索病毒Cryptolocker現蹤，如不慎感染此類病毒，磁碟內的檔案將遭無預警加密，唯有依據指示支付贖金後，才能得到解密金鑰。此類病毒大部分在使用者不慎觸發後，即會將磁碟中所有的文件、圖片、影音檔等進行RSA-2048至4096強度不等之加密，部分變種還會連帶加密網路共用資料夾，擴大受害範圍。

二、 目前得知加密勒索軟體主要散布管道，以電子郵件社交工程、瀏覽網站、社群媒體及檔案分享為主，多數使用者在電腦未安裝防毒軟體、系統和軟體未持續更新及缺乏警覺性之資安意識情況下，自然成為受害目標。

三、 內政部警政署近期攔截及蒐獲之樣本主要為經壓縮檔包裝過之腳本檔，並以JS、WSF及DOCM檔等為主。研析其攻擊採腳本檔之策略，主因為可避開防毒軟體對二進位檔之檢測，經過程式碼混淆化編碼，可有效降低被偵測到之機率，此也考驗使用者資安意識對社交工程防護之能力。

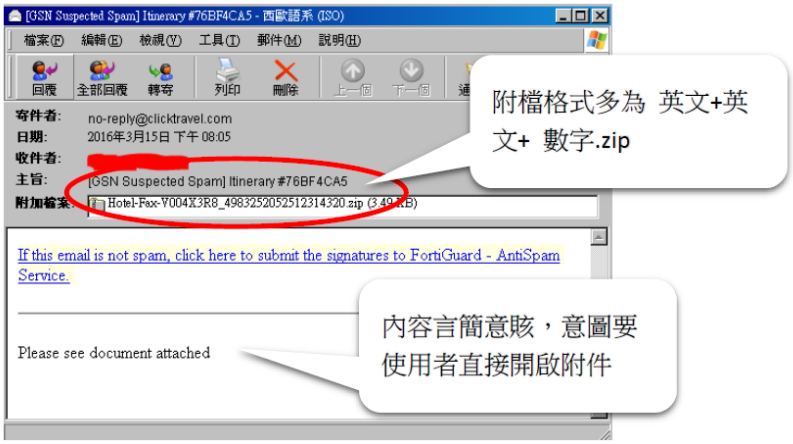

圖 1：勒索軟體郵件樣本

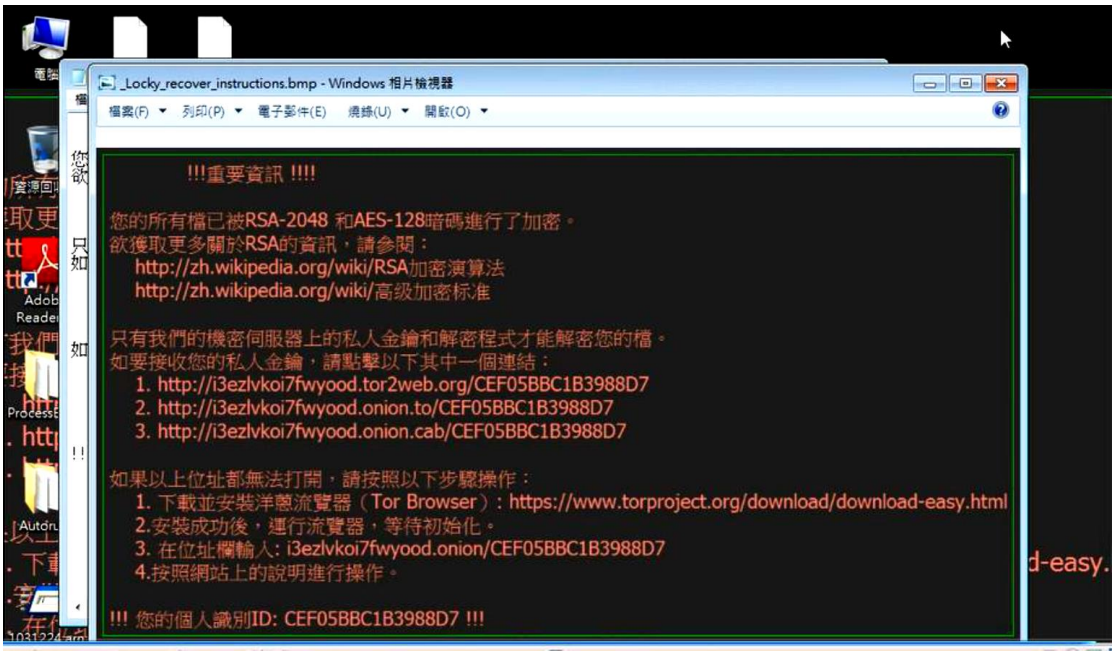


圖 2：使用者中勒索軟體病毒遭加密後之螢幕畫面

四、 據 2015 年趨勢科技統計資料顯示，臺灣地區勒索病毒攻擊人次在 5 月份達到新高，共計 50 萬人次遭勒索病毒的網頁攻擊，較 4 月份增加 3 倍。另在災情部分，國內外已有不少災情傳出，除一般民眾外，不乏企業及政府機構。單是 2016 年第 1 季，就有 326 起，較 2015 年第 4 季發生的 178 起，足足增長 83%，不僅有逐季攀升的態勢，數量更是有接近倍增的情況。

五、 加密勒索軟體至今仍持續不斷變化其攻擊手法，無論是透過電子郵件、植入網站廣告、P2P 分享及論壇分享等途徑擴大其感染範圍，再加上其利用比特幣（Bitcoin）透過匿名網路 Tor（The Onion Router，洋蔥路由器），造成執法單位追查犯罪金流上之困難度。

## 參、防護建議

一、建議一般民眾可採行之防護方式如下：

（一）平日養成重要檔案備份習慣，分散資料毀損之風險。

（二）對於來路不明之郵件提高警覺。

（三）網路危機四伏，瀏覽應特別注意安全，並持續更新瀏覽器至最新版。

（四）選購具信譽之商業防護軟體，增強電腦上網防護能力。

（五）定期維護電腦安全狀況，時常更新。

（六）瞭解新聞時事脈動，降低資安風險。

二、建議企業組織及政府機關可採行之防護方式如下：

（一）定期辦理資安意識教育訓練及電子郵件社交工程演練。

（二）建置郵件過濾系統，將可疑攻擊攔截並列入監控。

（三）建置瀏覽網頁代理伺服器，過濾資安威脅內容。

（四）宣導重要檔案文件，應養成備份習慣。

（五）重要或核心業務主機管理人員，應落實管理紀律，避免災損擴大。

（六）建立集中式之作業系統及軟體更新修補派送機制。

（七）妥善處理災後應變，降低損害。

（八）規劃雲端備份，降低資料遺失風險。

## 肆、結語

加密勒索軟體拜金融科技創新產物比特幣及匿名網路活動難以追蹤所賜，於近幾年迅速竄起。截止目前為止，全球尚無一套有效之偵測及防護方式可完全因應此種威脅。民眾及企業組織除須正視此威脅的嚴重性外，參酌本文建議做好事前預防工作，可降低此種病毒帶來之災損。

## 參考資料


一、勒索軟體：恐嚇取財手法十年進化史，趨勢防毒公司。http://blog.trendmicro.com.tw/?p=12957

二、網路勒索案件創新高 臺灣地區 5 月遭勒索病毒攻擊人次高達 50 萬 威脅急增 3 倍，趨勢防毒公司。http://www.trendmicro.tw/tw/about-us/newsroom/releases/articles/20160615093010.html

三、趨勢科技：勒贖軟體 Q2 季增 3 倍，中時電子報。http://www.chinatimes.com/newspapers/20160826000155-260204

四、企業面對 CryptoLocker 的因應與自保之道，ithome。http://www.ithome.com.tw/node/83541

五、肆虐升溫，勒索軟體災情擴大的 7 項原因，ithome。http://www.ithome.com.tw/news/107150