國家資通安全會報 國家資通安全科技中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2016-0031	發布時間	Fri Apr 08 17:15:22 CST 2016
事件類型	攻擊活動預警	發現時間	Fri Apr 08 00:00:00 CST 2016
警訊名稱	近期勒索軟體 Locky 活動頻繁，請提高警覺		
內容說明	近期加密勒索軟體活動異常活躍。其中名稱為 Locky 的勒索軟體自 2016 年 2 月開始肆虐，因把受害者的電腦資料和網絡共享資源加密且將副檔名改為 .Locky 而得名。Locky 使用 RSA-2048 與 AES-128 加密機制來加密檔案資料，所以遭到加密的檔案資料幾乎無法自行復原。Locky 會根據被害者電腦的語言來顯示勒索信件內容，勒索受害者 0.5 至 1 個比特幣（一個比特幣大約等於 13600 元新台幣）以換取解密金鑰。 Locky 的常見傳播方法是透過夾帶附件的垃圾郵件，附件多為帶有惡意巨集的 WORD 或 EXCEL 檔案或內有惡意的.js 檔案的壓縮檔。受害者會被要求開啟巨集功能，一旦開啟，Locky 便會被安裝到受害者的電腦內。另外就是透過放置惡意程式在已被入侵的網站。該網站的訪客會被重新導向到另一個攻擊網站，該網站會利用訪客的系統或已安裝程式的漏洞，來安裝 Locky 到受害者電腦內。目前新加坡、馬來西亞、香港和日本都有許多受害案例傳出，建議所有電腦使用者應提高警覺，小心防範。		
影響平台	N/A		
影響等級	中		
建議措施	1. 刪除收到的可疑電子郵件，特別是內含連結或附件的郵件。 2. 針對要求啟動巨集以觀看其內容的微軟 Office 檔案，必須提高警覺，必要時請與寄件者確認其檔案是否含有巨集。 3. 定期備份電腦上的檔案及演練資料還原程序。 4. 確實持續更新電腦的作業系統、應用程式及防毒軟體等至最新版本。 5. 如不幸受到感染，請立即將受害電腦的網路連線及外接儲存裝置拔除。建議在清除惡意軟體前不要開啟任何檔案。 6. 我們不建議支付贖金，支付贖金只會助長勒索軟體更加猖獗。		
參考資料	1.https://www.hkcert.org/my_url/zh/blog/16031802		

	2.https://www.hkcert.org/my_url/zh/alert/16031701 3.http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims 4.https://blog.avast.com/a-closer-look-at-the-locky-ransomware 5.http://blog.checkpoint.com/2016/03/02/locky-ransomware 6.https://metrics.torproject.org/hidserv-dir-onions-seen.html