張元成

寄件者: 國家資通安全會報技術服務中心 <ncert@icst.org.tw>
寄件日期: 2015年12月18日星期五 下午 5:45
收件者: ncert@icst.org.tw
主旨: [資安訊息警訊] 國家資通安全會報技術服務中心（事件編號：ICST-ANA-2015-0068)
簽名者: ncert@icst.org.tw

國家資通安全會報 技術服務中心

漏洞/資安訊息警訊

發布編號	ICST-ANA-2015-0068	發布時間	Fri Dec 18 17:14:31 CST 2015
事件類型	攻擊活動預警	發現時間	Fri Dec 18 00:00:00 CST 2015
警訊名稱	加密勒索軟體猖獗，請加強系統/應用程式更新與資料備份作業		
內容說明	近期勒索軟體攻擊事件頻傳，使用者電腦一旦遭植入該惡意程式，將導致該電腦可存取的檔案(含網路磁碟機、共用資料夾等)全數加密無法開啟讀取，藉以勒索使用者支付贖金換取檔案解密。 依相關研究報告資料顯示，勒索軟體傳染途徑以應用程式漏洞(如 Flash Player)與社交工程為主，且遭加密檔案無法自行解密還原。請各級政府機關儘速確認相關應用程式更新情況，定期備份重要檔案，加強資訊安全宣導，避免開啟來路不明郵件或連結。		
影響平台	所有平台		
影響等級	高		
建議措施	1.清查重要資料，並參考下列做法定期進行備份作業： -定期執行重要的資料備份。 -備份資料應有適當的實體及環境保護。 -應定期測試備份資料，以確保備份資料之可用性。 -資料的保存時間與檔案永久保存的需求，應由資料擁有者研提。 -重要機密的資料備份，應使用加密方式來保護。 2.檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。 3.確認作業系統、防毒軟體，及應用程式(如 Adobe Flash Player、Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。		

	4.若使用隨身碟傳輸資料，應先檢查隨身碟是否感染病毒或惡意程式。 5.若疑似遭受感染時，可參考下列做法： -應立即關閉電腦並切斷網路，避免災情擴大。 -通知機關資訊人員或廠商協助搶救還沒被加密的檔案。 -建議重新安裝作業系統與應用程式，且確認已安裝至最新修補程式後，再還原備份的資料。 -備份資料在還原至電腦之前，應以防毒軟體檢查，確保沒有殘存的惡意程式。 6.加強教育訓練，請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。 7.此則警訊僅作通知，無需進行通報作業。如機關發現遭駭情況，依內部資安事故處理程序處理，並至通報應變網站執行通報作業。
參考資料	104 年第 2 次政府資通安全防護巡迴研討會-近期資安威脅趨勢 http://www.icst.org.tw/NewInfoDetail.aspx?lang=zh&seq=1465

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)
地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@icst.org.tw