From: 國家資通安全會報技術服務中心
Sent: Thursday, January 21, 2016 3:21 PM
To: ncert@icst.org.tw
Subject:［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-2016-0010）

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-2016-0010	發布時間	Thu Jan 21 14:44:52 CST 2016
事件類型	攻擊活動預警	發現時間	Thu Jan 21 00:00:00 CST 2016
警訊名稱	駭客利用 Pass-the-Ticket 手法進行內部擴散攻擊，請加強網域伺服器安全防護		
內容說明	近期發現駭客在入侵機關網域伺服器(DC，Domain Controller)，取得系統內處理使用者身分認證之預設帳號 krbtgt 所對應的密碼雜湊值後，即可任意登入網域內的所有主機，在機關內部進行擴散攻擊。 依實際案例與相關研究資料顯示，駭客首要條件需成功入侵 DC，取得主機管理者權限後才能從中擷取預設帳號 krbtgt 的密碼雜湊值，進而施行後續 Pass-the-Ticket 手法，達到內部擴散的目的。請各級政府機關加強 DC 防護並留意 DC 內具管理者權限帳號之登入使用狀況，避免密碼遭竊取後所帶來的攻擊。		
影響平台	Windows 作業系統		
影響等級	高		
建議措施	1.確認 DC 主機之安全性 a.確認 DC 主機內具管理者權限帳號的登入來源與使用狀況是否存在異常 b.檢測 DC 狀況，確認是否存在惡意程式或其他入侵跡象 2.若 DC 遭入侵，則建議應採取以下應變措施 a.參考微軟提供之 DC 建置安全作業要點進行 DC 重建作業，網址如下:htt		

	ps://technet.microsoft.com/en-us/library/dn487446.aspx b.重新設定 DC 內預設帳號 krbtgt 密碼兩次，重設後應重開機以確保設定啟用；依微軟建議，兩次設定間隔應在 10 至 12 小時，可參考以下兩種密碼更改方式 (1).手動更改 krbtgt 密碼,步驟可參考 104 年第 2 次政府資通安全防護巡迴研討會議題二-近期駭客攻擊案例分享簡報 p.43~p.44,網址如下:http://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1251 (2).可利用微軟提供之 powershell 工具重新設定 krbtgt 密碼,網址如下:https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51#content 3.重新檢視 DC 管理維運方式 a.以本機登入操作為主，避免遠端登入進行管理 b.限縮 DC 內具管理者權限帳號之使用 c.定期檢視系統內管理者權限帳號之登入與使用狀況 4.此則警訊僅作通知，無需進行通報作業。如機關發現遭駭情事，請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議題二-近期駭客攻擊案例(Pass-the-Ticket)分享 http://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1251 微軟技術文件 https://technet.microsoft.com/en-us/library/dn487446.aspx

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