行政院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	NCCST-ANA-2016-0096	發布時間	Fri Oct 07 14:53:35 CST 2016
事件類型	攻擊活動預警	發現時間	Thu Oct 06 00:00:00 CST 2016
警訊名稱	Dropbox 帳戶密碼外洩，建議使用者儘速更新帳號密碼		
內容說明	Dropbox 公司 8 月 25 日於官方部落格說明有 6,800 萬筆帳戶密碼遭盜取，導致個人帳號資料外洩，當中包含電子郵件與經雜湊處理的密碼，目前遭盜取的相關帳號密碼已被公布於網路供人下載。 為避免資安疑慮，建議曾註冊 Dropbox 服務之使用者，應立即變更密碼亦可啟用雙重認證機制(註 1)。此外，若使用相同的電子郵件帳號和密碼登入其他網站或機關/單位相關服務，請一併更改，並各別設定不同的密碼。另可檢視用以註冊 Dropbox 服務的機關電子郵件帳號是否有異常登入行為，以確保資訊設備安全性。 為避免駭客偽冒 Dropbox 公司發送密碼更改要求信件，請詳細檢視寄件來源與相關連結，避免點擊電子郵件中的超連結去更改密碼。 註 1：如何啟用 Dropbox 帳號的兩步驟驗證 [https://www.dropbox.com/account/security]		
影響平台	無		
影響等級	低		
建議措施	1.相關應用程式服務與系統使用之帳號，需設定強健的密碼並定期更換，非必要使用之帳號或應用程式服務，應予以停用、刪除、移除或關閉。 2.清查郵件伺服器中的異常登入紀錄，如追查是否有國外 IP 連線登入，或使用非員工本身之內網 IP 登入員工帳號的情況。 3.針對有發現異常登入情況之使用者帳號，重建帳號及密碼並需符合複雜性需求。議一般使用者登入密碼設定至少 8 個字元。密碼中至少包含 1 個大寫英文字母、1 個小寫英文字母、1 個阿拉伯數字及 1 個特殊字元。 4.加強使用者對社交工程電子郵件的安全性認知，勿開啟不明來源郵件之附檔。 5.避免以機關公務電子郵件信箱帳號註冊外部服務，或透過外部雲端服務傳送公務資料，以降低資料外洩風險疑慮。		
參考資料	https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-to-keep-your-files-safe/		