公務機關公務電子郵件遭社交工程攻擊事件案例

一、案例大要：

某機關員工收到以承攬該機關系統建置及維護廠商工程師名義所寄送之電子郵件,該郵件開啟後除會顯示出正常簡報檔案外，另分離出經註冊為自動執行惡意程式檔案，且簡報檔經開啟後電腦會自動造訪位於泰國之未知網址。復經該機關向該名工程師查證後，該工程師表示並未寄出該封郵件，疑似駭客以該系統建置及維護廠商為身分掩護,針對該機關所為之社交工程攻擊行為。經分析該郵件內容，具有檔案加密規避防毒偵測、檔案字元反轉引誘開啟、自動植入後門及逆向連線回報功能，確認屬於惡意郵件。

二、手法分析：

(一)駭客偽裝寄送之電子郵件，內容附帶一壓縮檔「○○案進度報告.7z」，以 WinRAR 軟體展開前開壓縮檔，檔案類型顯示為螢幕保護程式，但如直接解壓縮，因控制位元被設為反向顯示，副檔名會正常顯示為 pptx。

(二)開啟「○○案進度報告.pptx」後，電腦會自動連結到泰國的的某一特定網址，且分離出「~trsad1.pptx」及「serverupdate.exe」2 個檔案，其中「serverupdate.exe」之惡意程式，駭客將其設定為自動執行，即使重開機亦會自動啟動。另為避免使用者懷疑，注入惡意程式同時會開啟「~trsad1.pptx」檔案,內容為機關內部承辦案件進度簡報，足見該維護廠商相關資訊已被駭客掌握。

(四)駭客偽裝之維護廠商與被駭機關確有系統建置及維護契約關係，寄送人與該單位間亦有業務往來，且附件簡報確與業務相關，駭客以合約與維護內容為掩護，係為針對特定單位的社交工程攻擊。

(六)本案附件以加密方式規避防毒軟體偵測，另以反轉字元方式掩護惡意行為，期降低使用者戒心，引誘使用者開啟，於開啟檔案後嘗試植入惡意程式，透過標準網頁通訊協定回報，規避資安防禦系統偵測，恐執行秘密之資料竊取或入侵行為。

三、機關防處作為：

(一)坊間多數掃毒軟體對於本案相關檔案已可有效偵測，應定期執行病毒碼更新與資安監控，以維護資安防護有效性。

(二)持續強化機關同仁資安教育訓練，避免因開啟來路不明郵件或連結，致遭社交工程攻擊。

(三)與廠商郵件往來，應先行確認後再開啟，並避免將郵件帳號提供給無關人員。

(四)機關應管控公務電子郵件帳號使用情況，發現異常情形應即時通報處理。

(五)提醒承商重視及強化自身網安作為，並嚴禁私設遠端維護機制，落實現地維護要求，避免成為駭客入侵管道。

四、結語：

駭客攻擊管道已轉向政府工程承商或維護合約廠商，並非直接以政府機關為攻擊對象，請各政風機構協調機關相關單位加強掌握委辦廠商之資安狀況，並持續檢視機關資安作為之執行情形，以有效防範駭客以公務電子郵件進行社交工程攻擊等情事。