公文電子交換系統之安全防護建議

A Best-Practices of Security on the EOD Exchange System

■ 林佳明 Lin, Char-Mi
國家資通安全會報技術服務中心組長
Manager, Information & Communication Security Technology Center

壹、前言

政府機關必須不斷針對演化中的資安威脅環境進行應變。目前政府資安防護最大的一項挑戰就是進階持續性滲透攻擊（Advanced Persistent Threats，簡稱 APT），該攻擊會針對特定組織與個人製作出難以辨識且多方位的攻擊。然而從攻擊者的角度，如何快速大規模進行惡意程式擴散或隱匿在被信任的資料交換通道進行攻擊，一直是 APT 攻擊者發展攻擊手法的首要目標。公文電子交換系統正好就符合 APT 攻擊者喜愛的要件，所以如何避免因為公文電子交換系統導致使用者系統遭駭，進而造成機敏資料外洩成為公文系統操作人員與資安防護人員的重點工作之一。以下將以發生過之公文電子交換系統資安事故案例為主，提供公文電子交換系統之安全防護建議。

貳、基本的安全防護

首先針對公文電子交換系統（Electronic Official Document Exchange System）的環境與使用方式談及安全防護建議之前，應該先對被保護的系統採取基本的安全防護作為。依據微軟提供的建議，一般使用者面對非零時差（0-day）惡意程式的攻擊，應優先採取的三個安全建議措施為：

一、盡可能快速、即時的，安裝包含作業系統與所有應用程式的，所有的更新程式（Patches）。

二、所有的軟體（包含作業系統）盡可能快速、即時的，使用最新的版本，因為通常新的版本會提供新增的安全功能。

三、盡可能的採用或加快轉移到 64 位元的架構，因為現在的惡意程式或攻擊大部分都是針對 32 位元的架構研發的。

長程來說，一般使用者應規劃採取的安全建議措施為：

一、採用雙因子（Two-factor Authentication）認證。

二、採用可信任的平台模組（Trusted Platform Module），例如資料傳輸應規劃採用加密通道避免被竊聽，建立可信任的資料傳遞方式。

三、網路存取保護，針對網路存取方式與來源

進行管制，限縮攻擊的路徑。

四、系統直接存取的限制與管理，避免資訊設備被以實體的方式入侵。

五、採用 IPv6，IPv6 相較於 IPv4 增加了部分的安全功能。

參、內部公文簽核系統的安全防護

過去曾發生某機關發送之電子公文附件夾中帶惡意巨集程式，導致受文機關被駭的資安事故。事後追查發現駭客利用本機管理者權限，進行內網擴散，並監控內部公文伺服器之待發送公文，進而篡改內容。

因為公文電子交換 eClient 系統，並未提供內部簽核流程，僅負責將發文人員所製作之公文傳遞給收文機關，因此許多政府機關會另外開發內部使用之公文簽核系統，將之與公文電子交換 Xml-box 系統界接。駭客透過監控內部公文伺服器，利用公文撰寫人員提交公文給上層簽核，或簽核後內部公文伺服器將公文傳遞給公文電子交換 Xml-box 系統的時間差，將電子公文附件篡改成帶有惡意程式的文件，讓公文電子交換 Xml-box 系統進行傳遞，入侵意示圖如圖 1。

針對此一類型的攻擊，公文製作方，建議應對公文的 " 完整性 " 進行加強管理。導致資安風險的主因，是公文附件被非授權的篡改，在開發內部公文簽核系統時，應將公文加密或簽章功能列入需求中。也就是說，公文撰寫人員在產出公文上傳至簽核系統時，簽核系統必須針對上傳的文件進行簽章檢查，在每一個公文簽核的傳遞過程中，都必須再三的檢查簽章是否合宜，確保就算簽核系統遭駭，因駭客沒有單一個人的數位憑證，因此無法篡改公文。公文接收方，建議應在公文電子交換 eClient 系統上安裝防毒軟體，或者主機型入侵偵測系統（Host-based Intrusion Prevention System，簡稱 HIPS），在接收公文時與開啟公文附件時確認是否有公文是否有被暗藏惡意程式。

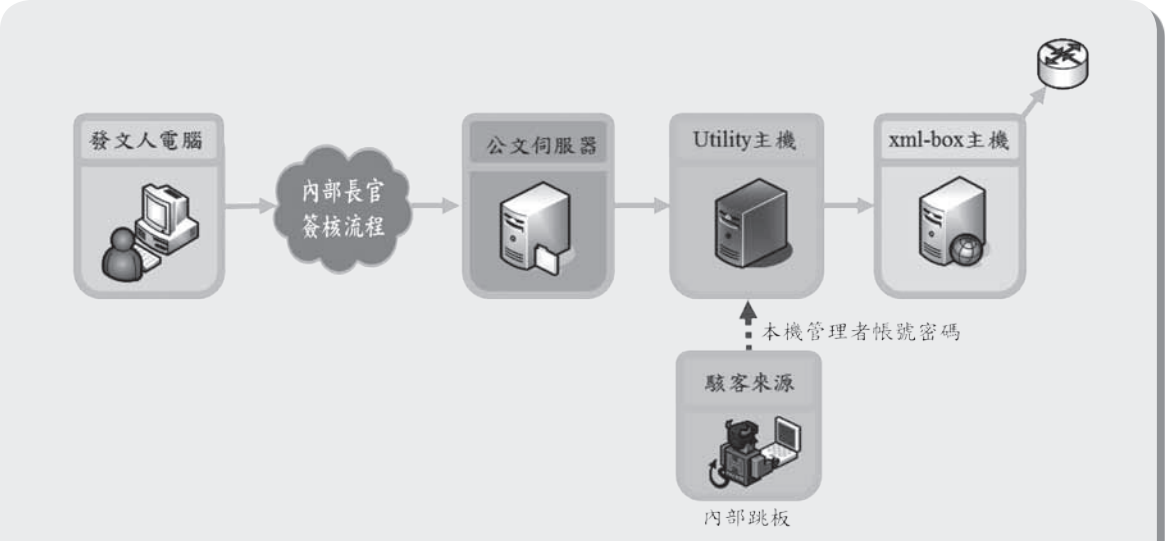

圖 1：內部簽核系統入侵意示圖

資料來源：國家資通安全會報技術服務中心整理

肆、文件傳遞時的安全防護

第二個案例，係某機關接獲 G2B2C 統合交換中心通知，表示該機關發送之電子公文附件存有惡意行為。經事後鑑識發現，其中公文承辦人電腦存有源自別公務機關發送之惡意公文附件，承辦人表示，本案公文附件是先以該惡意公文附件編修繕打，再依正常管道進行公文發送。

由於公文承辦人電腦已安裝更新程式，並採用最新的 OFFICE 版本，因此在編修繕打惡意公文附件時，並未觸發惡意程式的執行，無法觀察到異常行為。而此一案例的問題點，在於公文承辦人使用並非原創的文件當作公文附件，在沒有確認檔案可信度的狀況下，自然原始檔案中的所有惡意模組都被保留下來，進而影響可能沒有安裝更新程式的收文單位。

針對此一類型的攻擊，建議公文製作方應在採用他人製作或透過第二者取得之檔案時，重新開一個新的檔案，僅複製資料內容至新的檔案，再行傳遞公文承辦人自行重新再製的無害檔案。

伍、公文電子交換 eClient 系統之安全防護

第三個案例，係公文電子交換系統使用者端程式（eClient）更新機制異常，駭客透過更新機制散佈惡意程式。經事後鑑識分析發現，公文電子交換網路系統中的公文電子交換用戶端（eClient）版本更新伺服器遭受攻擊，駭客利用修改版本更新伺服器內進行版本更新用的網頁程式原始碼，竄改 eClient 軟體更新路徑，使得機關內裝有 eClient 的主機進行更新時，會連線至異常的路徑下載並執行已遭置換成含惡意程式的更版程式，最後連線中繼站進行報到。

針對此一類型的攻擊，建議公文電子交換用戶端（eClient）的使用者，應將 eClient 視為不能完全信任的系統進行管制。通常針對這類型的系統（正確性無法由機關自行確認的軟體），應放置在內部非軍事區（Demilitarized Zone，簡稱 DMZ）區域，與使用者環境或內部網路環境進行隔離，當發生危害的時候，可以將損害降低自最小。若不確定自動更新機制是否安全的狀況下，使用者可以採取自行下載更新檔，進行人工更新作業。在安裝與套用更新時，應該針對系統的網路狀況進行監控與檢視，確認安裝任意軟體或更新後，系統未發出異常之網路行為，確認系統的安全狀況。

陸、結語

公文電子交換系統是我國用以傳遞公文資料的重要系統，也是駭客覬覦的首要目標之一，應嚴格限制 eClient 的外部連線，若非必要，可禁止遠端連線管理或只開放特定有需要的來源端連入，關閉不使用的連接埠，以降低外部入侵的可能性並易於事後追查。考慮備份並定期檢視 eClient 主機之系統日誌檔與應用程式紀錄檔，利於盡速掌握異常情形的發生，降低影響程度與範圍。加強針對主機內程式的保護機制，定期確認原始碼的完整性，避免非授權下的修改或遭置換。可要求資通安全監控中心（Security Operation Center，簡稱 SOC）監控對於 eClient 系統的系統登入與網路連線狀況加強監控與分析，以便早期發現入侵的情事進行相關應變作為。