警政署強化資訊安全作為心得分享

壹、緣起

資訊安全一直是各級政府機關所重視之議題，亦投入大量人力與物力從事防禦工作，建置防毒系統、防火牆、入侵偵測系統等各式各樣的安全防護機制，但有用嗎？還是沒用呢!這些機制確實有 80%防護效果，但仍有 20%的威脅因子造成資料外洩情事。經警政署長期觀察與發現，這 20%的威脅因子主要來自於個人電腦的使用者已習於使用電腦瀏覽網頁、收發 E-MAIL 信件與存取隨身碟資料，而電腦病毒或惡意程式也正利用此特性進行感染與持續擴散，不僅機關內部公務個人電腦，連家中私有電腦亦遭受同樣攻擊，然而基於資訊專業技術的相對弱勢使用者卻也渾然不覺電腦已遭受入侵，危及機關機密公務資料或民眾個人隱私的安全。爰此，警政署爲解決這 20%的威脅，於 98 年規劃建置「先進資安威脅監控與分析系統」(以下簡稱本系統)，並於同年 10 月完成驗收上線使用。

貳、系統功能介紹

本系統研發基於：一、如何讓內部員工於第一時間內掌握威脅來源與態樣，弭平不對等的資訊認知，強化資安威脅感受度與自我防護能力。二、使資訊安全防護人員快速掌握機關所遭受的威脅，並在最短時間內擬訂防護措施，以保護機關的資訊安全。其功能說明如下（如圖１）:

一、 彙整資安防護機制資訊：彙整 Shadow Server 資料(相關網站：http://www.shadowserver.org/)、攔截惡意電子郵件系統(警政署自行研發非市售產品)、郵件防毒牆、掃毒資料庫、資產管理資料庫、代理伺服器系統等相關紀錄與資料。

二、 部署惡意程式捕獲工具：主要作爲捕捉掃毒軟體無法掃除或是網路防火牆無法辨識之惡意程式，以補強防毒機制與防火牆之不足，通常這種惡意程式經加密(或稱加殼)保護或是新式的攻擊手法。此工具分爲個人電腦端軟體與機動式 USB 捕獲工具二種，前項目前部署在警政署內部個人電腦，監測有無異常執行程式，後項則提供各警察機關或同仁居家電腦使用，協助檢測有無惡意程式。

三、 自動化惡意程式分析工具：當前項捕獲惡意程式時，將惡意程式交由此工具進行分析，爲能快速分析惡意程式植入位置或有無內藏中繼站網址、網域等資訊，全程採用自動化方式分析，啓動 VM 環境，並執行此惡意程式，在從記憶體分析程式碼，並產出相關報表。

四、 惡意網站分析工具：主要功能在於檢查網址(URL)是否內藏惡意程式，用於檢測警察機關網站是否遭受網頁掛馬攻擊或植入可疑連結，以解決日趨嚴重的惡意網頁問題。除此之外亦將警政署內部使用者連結之排名前 10 大網站進行分析，俾利掌握使用者最常連結網站是否有遭受網頁掛馬攻擊或植入可疑連結等潛在威脅，以事先防禦方式，避免使用者電腦不當連結而遭到入侵。

五、 資訊威脅監控平台：將本系統各項功能所產生之資料，彙整後再經過交叉比對統計分析，產生各種視覺化、圖型化威脅趨勢分析報表，並以網頁方式呈現內部單位所

遭受資安威脅情形，俾利資安人員進行各種防禦措施，並發佈予內部人員隨時掌握攻擊的態樣，以達完全防護機制。

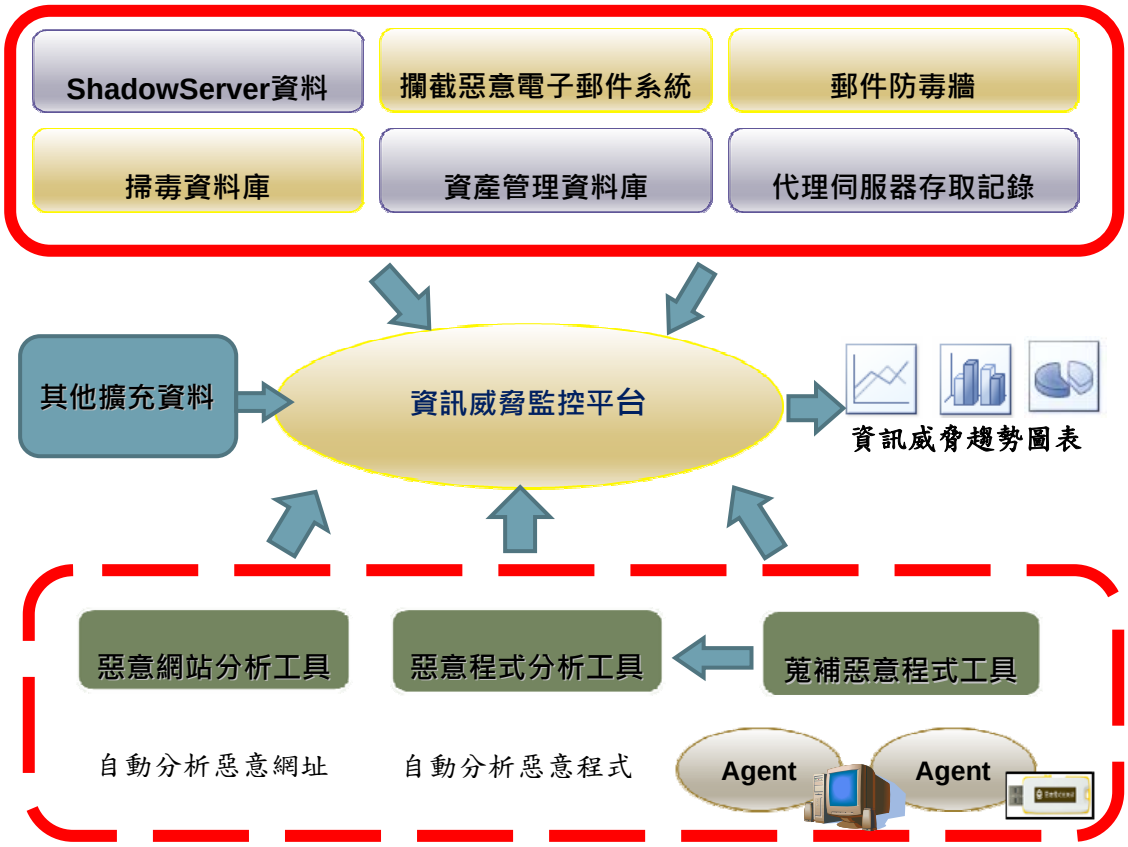

圖 1　先進資安威脅監控與分析系統功能示意圖

參、效益

由近來觀察駭客攻擊警政署的手法與態樣分析，主要利用「0-Day」與「目標式網路釣魚」結合方式攻擊特定使用者，並誘使使用者開啓電子郵件點擊藏有惡意程式之 Word、PDF 等檔案或者連結惡意網站，以入侵使用者電腦，伺機竊取機敏資料。本系統除了用於防範此類型攻擊方式外，亦藉由整合各個監控子系統，產出資訊威脅趨勢報表，以獲得即時的資訊，其效益如下：

一、　對使用者：本系統資訊威脅監控平台採用網頁方式呈現(如圖 2)，讓使用者隨時掌握外來資安威脅情況，這平台展現了排名前 10 大惡意程式(如圖 3)、10 大惡意郵件(如圖 4)、10 大受攻擊部門(包含惡意程式與惡意郵件威脅如圖 5、6)以及電子郵件攻擊的態樣(如圖 7)，強化使用者資安威脅認知與感受度，以免遭受入侵。對資訊安全管理者：本系統分析惡意程式或郵件均採用自動化方式處理，減少管理者人工分析作業；另亦藉由資訊威脅監控平台掌握內部單位威脅程度，如 A 部門遭受惡意程式攻擊排名第 1 名時，可以進一步分析該部門使用者可能因使用 USB 隨身碟而引起等因，

並針對該部門同仁強化資安宣導，如此才能逐步並澈底解決資安問題，減少資安事件發生。由於本系統強調即時性，只要一發現中繼站網址或網域立即封鎖，避免使用者不當連結，並快速回應駭客攻擊，如曾於 98 年 12 月 10 日發現駭客利用 PDF 漏洞植入惡意程式攻擊警政署，經本系統分析並立即封鎖連結，而此漏洞至 99 年 1 月 13 日才發佈更新，期間若未加以阻擋恐已造成大量資料外洩了。

圖 2　資訊威脅監控平台示意圖

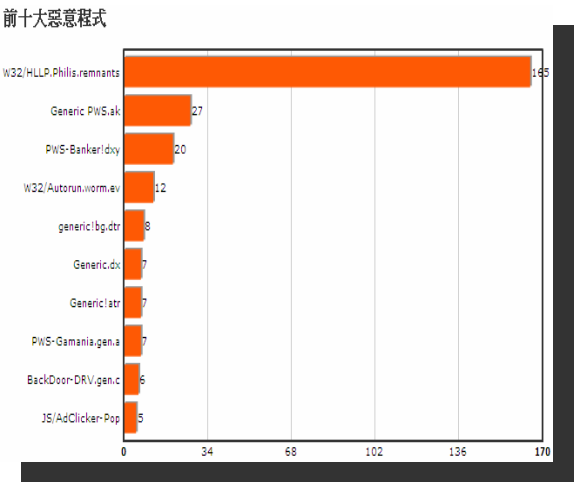

圖 3　前 10 大惡意程式示意圖

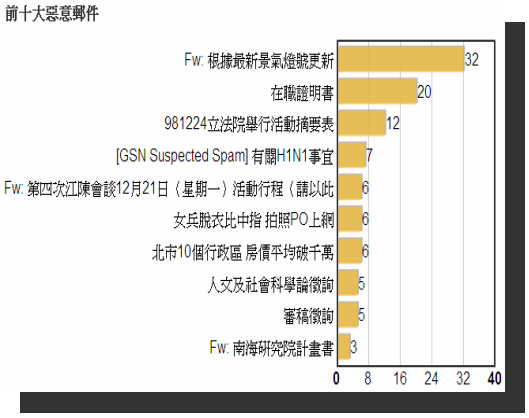

圖 4　前 10 大惡意電子郵件示意圖

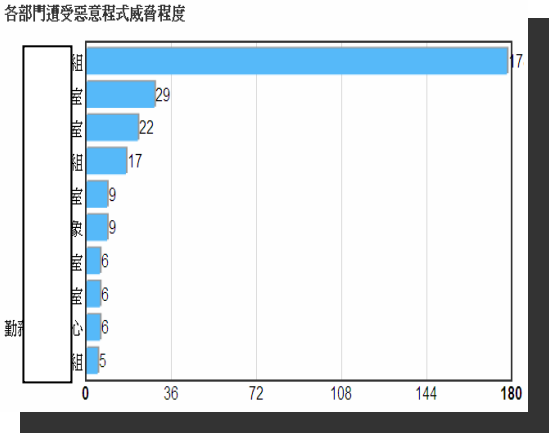

圖 5　各部門惡意程式威脅示意圖

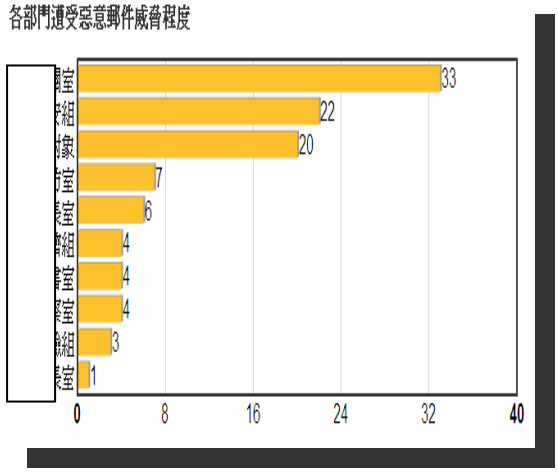

圖 6　各部門惡意電子郵件威脅示意

圖 7　惡意電子郵件態樣示意圖

二、 對機關：資安事件往往爲新聞媒體所大肆報導的新聞議題，不僅影響機關聲譽與形象，亦引起民眾對機關的不信任感，本系統甫上線使用經統計 98 年 12 月份業已分析駭客所使用之中繼站網址 13 個與網域名稱 22 個，有效掌握駭客攻擊來源，並立即啓動防護措施，降低資料外洩情事發生，維護機關聲譽與形象。

肆、結論

警政署資訊室主任李相臣常言：「資訊安全防護工作關鍵在於速度」，若未能即時掌握敵暗我明攻擊手法，恐將造成大量資料外洩，本系統強調的是防護的速度，期在最短時間內完成防護部署，亦讓使用者有正確的使用網站、電子郵件、隨身存取設備觀念一同參與保護資訊的安全，防止目前駭客最常使用之「0-Day」與「目標式網路釣魚」結合型的攻擊手法，以達機關資訊安全。

（本文由警政署資訊室技正蘇清偉 提供）