政府機關整體資安策略探討

李相臣　高大宇

壹、前言

網際網路的日益盛行與無遠弗屆，網路服務的時間便利、區域無限、應用多元更讓大家沈浸在資訊科技應用的便利網路環境之中。然而，電腦使用者在拜訪某些特定網站時，有時必須執行某些動態廣告網頁、下載特定程式或打開不明電子郵件，只要執行開啓執行功能都可能讓木馬程式植入你的電腦中，進而竊取個人重要的資料，從事犯罪行爲。電腦系統與應用程式的出現漏洞，往往給予思想偏激的程式設計者發揮的機會。在此資訊進步迅速、網路科技精進的今日，網路資訊安全的衝擊持續成爲人們討論的熱門話題，網路駭客組織不斷的發表與創新攻擊軟體，使得專業入侵軟體程式不停地在網路上流通，社會大衆如何預防、及早發現電腦系統被入侵，避免不必要的干擾與損害，已成一非常重要的議題。

貳、現況

電腦已成爲所有資料與機密資料之儲存單元，網路亦已漸成交換訊息之主要橋樑，透過實體或虛擬方式連結資料與資料之節點，以資訊網路入侵方式深入敵境不著痕跡流竄網路世界的技術，也將是未來制敵機先的獲勝關鍵。網路無國界，環遊世界輕而易舉，這也造成資訊入侵犯罪具有跨國特性，因此，必須藉助國際合作方式方可能奏效，尤其當犯罪證據置於世界各地，追緝問題將更爲困難，其困難度與複雜度遠高於一般案件。然而，一但涉及敵對國家的特定目標蒐集情報行爲，便顯得十分複雜，爲了能深入敵境取得有效資料回傳而不被發現，目前較常用的手法爲利用已知通訊埠，透過特定稀有及罕見之非標準傳輸封包格式回傳，爲目前較爲常見的竊密方法，如何因應處理也在在考驗資安人員的應變能力。目前我國的資訊社會在政府機關不斷推廣便民E化與M化的同時，資訊社會中一股竊密入侵風潮亦正日益興盛，不論是透過電子郵件或惡意網站，將木馬和後門程式植入受害者的電腦，再將有價值資料透過電子郵件或檔案傳送到指定網址，幾乎成爲入侵者取得資料的固定行爲模式。

例如，民國九十三年四月國內數家銀行因其網路銀行電腦遭駭客植入惡意程式竊取帳號、密碼及機密資訊導致網路銀行客戶遭駭客盜領，該惡意程式會在受害者電腦裡僞裝成正常的應用程式檔名，透過電子郵件竊取機密資訊傳送給駭客並盜領存款得逞。財政部金融局與銀行公會爲防堵網路銀行帳戶遭盜領事件擴大，希望各銀行暫時先關閉網路銀行非約定帳戶功能，而且，客戶如果在網路上進行非約定帳戶交易，必須先打電話給銀行確認交易帳戶。若網路金融交易制度的建立仍僅建置在帳號密碼、憑證或鍵值（Key）的信任基礎之上，一旦電子信任機制保護不當，整個交易制度便限於危險之境。又如，民國九十三年五月國內金融機構、科技公司及政府單位等機構，遭到駭客大規模以木馬惡意程式入侵內網竊取機密文件，造成盜領金錢轉帳損失，而被害者遭流失、竊取的機密資料則無法估計。凡此種種資訊入侵事例實已成爲網路社會中無法避免的犯

罪淵藪。

參、面臨問題

近幾年不斷出現政府機關電腦機密資料遭竊、帳號密碼遭盜用、銀行存款遭提領、網路證券遭冒名下單、電腦病毒發作、金融機構電腦當機及網頁遭置換，這些點點滴滴都讓大家眞實地見到電腦系統帶來的便利與危害。爲使電腦系統造成損害降至最低，資訊單位應專人觀察電腦對外通訊方式及封包內容以察覺異狀。而電腦使用者應具備基本惡意程式自我檢測能力，針對所屬電腦（含伺服器及個人電腦）進行全面性的檢查，並加強資訊部門之資安觀念，提高資通安全之重視程度及因應能力。以下，本文謹從「惡意程式作者不斷湧現」、「資訊法律觀念未能深入人心」、「原始程式分享交換刺激技術成長」、「機構電腦的資安被駭事件頻傳」、「內網電腦遭入侵後主動對外報到」及「兩岸入侵技術設計交流密切」等問題進行探討。

問題一：惡意程式作者不斷湧現

就日前殺手病毒及 peep 木馬作者的落網新聞觀察，年輕的程式設計者在日常生活工作之餘，往往會找個本身感興趣的工作深入研讀，希望能有「出人頭地的一天」！爲了一戰成名，往往會希望在網路虛擬世界中獲得尊重，開發一種獨一無二、廣爲流傳的「躲避防毒（或防火牆）程式」也就成爲地下駭客組織或電腦病毒組織成員寄望的目標。對於一個廣受尊重的惡意程式（或破壞入侵程式）作者而言，最在乎的是別人對他的正面評價、改善建議與言詞讚美。爲了獲得其他高手的支持與支援，往往也不吝嗇於「分享原始程式碼」，分享原始程式碼的動機在於獲得其他同儕之認可，若能以物易物（彼此交換珍藏或互通測試心得）或獲得實質利益（贊助金錢）則更能滿足其成就感。

問題二：資訊法律觀念未能深入人心

法律刑罰之立法目的乃爲「大多數的人類謀幸福」，期望藉由實務運作解決社會運作過程中所產生的種種偏差或不法行爲。相關法律條文的適用尚須努力瞭解、觀察與體會各種出現問題方能對問題有更清晰的判斷，得到更多整體性預防被害良策。資訊入侵犯罪問題本身是一種多元性、技術性、國際性與法律性的社會現象，必須從不同層面與角度思考，不必小題大作，瞭解眞實事件方可尋求解決之道。

問題三：原始程式分享交換刺激技術成長

繼先前傳出微軟原始程式碼遭駭客侵入竊取之後，這些年來微軟系統的系統漏洞與應用程式弱點相繼出現偌大瑕疵，雖然微軟公司已不斷地努力強化提升安全功能，相關的修補程序也日漸頻繁。然而對於習慣吹毛求疵的程式設計者一旦取得這些原始碼，經過深入解析，破解漏洞問題，取得他人系統存取權力，往往也成了網路留名者的追求目標。

問題四：機構電腦的資安被駭事件頻傳

國內許多民間企業只想利用電腦輔助本身工作之進行，卻不管伴隨電腦系統出現的漏洞破壞，未能關心異常連線狀態，即使是高科技公司的逾百台電腦主機，也僅僅只有少數一、二人負責，更別談那些電腦設備較少的中小型企業。面對資訊蛻變的高科技時代，不斷充實、日日更新、深入解析原委，才能走在時代的尖端。所有機構的資訊安全人員應該針對電腦出現異常、CPU 使用量激增、電腦反應遲緩及帳號密碼無端遭竊等問題，經常性地偵測網路連線狀態實際瞭解相關狀況，查察電腦是否存在主動對外報到連線，甚至有無外洩鍵盤輸入帳號密碼、電腦檔案內容或整個資料庫，避免受害及事態持續擴大。

問題五：內網電腦遭入侵後主動對外報到

有別於傳統的網路遠端遙控工具僅可藉由收送雙方的 IP Address 位址相互溝通，現今的入侵技術著重在惡意程式的附加綑綁其他正常

檔案、反端口遙控技術、原始碼等資訊技術相互交流分享與如何使資訊防護工具（如防毒、防火牆）無法偵測，尤其是反端口遙控技術可利用受害內網電腦對外報到特性，直接邀請網路外部主機可以完全掌控遭植入的受害內網主機，外來入侵者甚至具備檔案總管(檔案下載、執行、刪除等全部功能) 、遠端桌面監控、遠端執行程序管理、遠端登錄編輯器等主要功能，功能強大者甚至具備搜尋最近存取檔案內容。由於入侵者使用惡意程式僞冒在已被允許存取的應用系統對外通訊服務上，故可使用一般的系統服務對外報到，一般防毒、防火牆及入侵偵測系統無法察覺，需要由專業能力足夠的資訊安全人員細心一點方能發現。

問題六：兩岸入侵技術設計交流密切

當設計攻擊程式技術到達一定水準，期望的是：「能夠找到志同道合的同伴」，由於入侵技術在中國大陸的討論情形尚較國內熱絡，基於同文同種情誼，兩岸惡意程式作者或入侵者在相互交流上早已密切熱絡聯繫，絲毫不受兩岸緊繃的複雜政治關係影響。許多國內的高科技業者也紛紛在中國大陸及世界各國成立分公司，由於中國大陸人工較爲便宜，部分國內資訊業者會將程式研發重心轉至中國大陸方面，然而，這樣的長期作法卻可能讓國內政府、經濟、民生或交通等相關應用系統基礎技術掌控在敵對國家手中，對於私有機密檔案文件的保護功效便日益困難。

肆、建議事項

攻擊者僞冒於正常服務之中，難以察覺、偵測與解析。然可針對電腦出現異常、CPU 使用量激增、電腦反應遲緩及帳號密碼無端遭竊等問題，偵測網路連線狀態實際瞭解相關狀況，查察電腦是否存在主動對外報到連線，有無外洩鍵盤輸入帳號密碼、電腦檔案內容、甚至整個資料庫，以避免受害事態持續擴大。由於各受害單位電腦使用者如不知電腦資料遭入侵且不知電腦資料可被竊取，依然將重要公務內容登打於各受害主機之中，入侵者將可在需要時，取得重要機密資料，侵害程度實難估算。由於最近發現的惡意程式部分會僞冒系統檔案，以相同（或類似）檔名命名，並藏身在系統目錄中，由於採開機自動執行且對外部主機主動報到方式，一般的資訊人員很難注意，以下，謹建議一些基本資訊安全觀念，提供自我安全保護的基本自我檢測防護。

建議一：檢查利用已知系統對外通訊服務：

已知受害主機主動利用已知（常用）系統程式或通訊服務對外聯絡，由於這些多被視爲正常使用致無法輕易察覺入侵異狀。資訊人員應協助使用者注意電腦未執行該通訊服務時，如發現異常對外之主動式連線通訊，便需檢查啓動該電腦通訊服務的應用程式、所在目錄與實質通訊內容。千萬不要因爲不知如何檢查或沒有發現異常狀況便掉以輕心，我們必須警覺到當所屬電腦一旦連上網際網路，危險便開始存在，如何免除災害、加強防護力則是每一個資訊安全人員與使用者的未來注意重點。

建議二：檢查匿身系統目錄的惡意程式與暫存檔案

由於入侵者習慣將惡意程式及竊得檔案藏在系統檔案目錄，減少擁有電腦者的察覺可能，故電腦使用者當發現電腦系統出現異狀時，不妨檢查此區查看有無異常檔案，期能儘早察覺異狀。

建議三：檢查電腦開機自動啓動設定與常用應用程式

大多數的惡意程式會在電腦重新開機時設定爲自動啓動，保持電腦處於被入侵狀態。此部分可藉由檢查登錄編輯器（Registry）中開機組態設定觀察異常程式得知異狀。此外，有的入侵者會用綑綁技術將電腦使用者的必用電腦檔案（如 Word、IE 等），做一置換動作，這將

使得觀察異常工作更加困難。

建議四：注意防堵變種惡意程式

由於大多數的惡意程式原始碼會以「以物易物方式」公開，取得的程式設計者可隨意變化感染、植入、啓動的作法，致使變種程式不易防堵。雖然惡意程式個別行爲態樣多變，難以偵測發覺，惟仍具一定的行爲模式。只要負責的資安人員夠用心研究、細心探究異同變化，還是有機會找出可疑程式。

建議五：建置 Proxy 機制阻擋非標準協定對外傳輸資料

攻擊者爲達成竊取檔案的目的，通常會費心地使用非標準的通訊封包協定，使用在建置龐大的不明連線網路，對外傳輸資料。由於傳輸過程無法正常解譯，需透過特定程式還原成原始文件格式，受害機構內網資料被竊已成爲必然。但如受害機構內部可透過建置 Proxy 機制讓內網電腦即使不小心遭植入問題惡意程式，也因直接向 Proxy 主機報到後被視爲異常通訊封包協定而遭丟棄處理，當可減少內網持續遭破壞竊密的現象。此外，爲降低內網一旦遭入侵後可能衍生的迫切危害，亦可採內網區分不同 VPN 方式相互隔離，避免入侵事件的迅速擴大。

建議六：資訊安全專責人員的設置

由於目前政府機關推行資訊委外政策，約聘僱人員遇缺不補，在資訊人力不足的狀況下，網管人員通常僅委由一人兼任（尚須負責其他雜務公文或程式設計等工作），一人負責四、五十台伺服電腦的狀況也屢見不鮮。在此現象之下，實需專責人員集中具體可行的資訊安全工具、技術與方法，有效輔導各政府機關做好基礎防護工作，而非「頭痛醫頭」，捨本逐末。機構內部的資安管理應該持續投入專有人力維護，雖然對機構而言，實際功效不易彰顯，然疏未注意卻可能衍生資料外洩的危機。

建議七：保防與政風人員的資安訓練

由於資訊科技的普遍應用，資安問題已非資訊單位所能完全掌控，電腦使用者本身的使用習慣與機靈程度更是攸關資訊檔案是否容易遭竊的關鍵重點，政府機關之保防與政風等重要人員更需接受適當之資訊安全訓練，密切注意電腦是否存在異常入侵行爲。作法上可從基礎資訊安全教育著手，讓所有員工知道如何做好基本安全檢查工作，再結合豐富資安專業能力的人才，妥適改善企業資安政策、稽核系統安全。

建議八：重要資料應儲存攜帶式紀錄體

當重要資料儲存在連通網際網路電腦中的時間越久，被入侵竊密的機會便越高，若能將重要檔案另行儲存在其他輔助儲存設備，在需要時再予連結使用，當可減少暴露於網路上的機會，進而降低資料被竊的機率。

伍、結論

不應把資安問題視爲是資訊部門的工作，使用者本身的使用習慣與機構主管的資安認知與重視程度是資安成敗關鍵的要素，根據慣例，兼職資安人力往往無法落實資安維護工作，因爲實在有太多的雜務讓兼職資安人員無法心無旁騖的專心維護資訊系統的安全運作，管理階層要先有資安觀念，再推動系統管理者的最新安全威脅防制技術與員工的資安認知，較能引起上行下效功用。定期資安檢查防護工作經常被忽視，其實從例行檢查過程中，可以防範許多不當入侵行動，並避免資訊資產的外洩損失。任何機構的資訊單位應該採定期資安評估方式，持續性執行並藉由內部評估方式，促使內部網路使用安全能持續地被注意，以防範可能衍生的意外事件發生。♥

（本文作者李相臣現職為刑事警察局偵查第九隊隊長、高大宇現職為刑事警察局偵查正）