解析網路攻擊發展趨勢與防護之道

一、前言

臺灣 So-net 網站近期遭駭客入侵，會員個人資料外洩，導致信用卡被盜刷約 1,840 張，國內幾乎所有發卡銀行都中獎。經警方調查，駭客可能來自中國大陸，係以俗稱「釣魚網站」的假網頁，藉由郵寄電子郵件、圖檔等方式夾帶木馬程式入侵。無獨有偶地，日前有超過 50 家位於美國、歐洲及澳洲的銀行，也同樣遭駭客以網址嫁接（Pharming）的方式進行攻擊，駭客利用假造的銀行網站與 pharming 技術，讓使用者登入假網站，趁機竊取個人資訊，相關損失尚無法預估。駭客主要是利用微軟系統的漏洞，當使用者登入正確的網址時，會被導向事先假造的銀行網站，而未安裝修補程式的電腦，將會被載入主要木馬程式，以及來自俄羅斯網站的其他 5 個副檔，爾後若連上已被鎖定攻擊的網站時，就會被自動導向假網站，所鍵入的資料也都會被記錄，並送回位於俄羅斯的伺服器。

二、何謂「目標式攻擊」？

以往一支病毒程式攻擊所有電腦的「亂槍打鳥」模式已不復見，取而代之的是針對特定目標族群，成群結隊地入侵。依趨勢科技針對這類「目標式攻擊」所做的研究發現，目標攻擊通常區分 3 個步驟：首先由不法分子或犯罪組織針對特定對象發出網路釣魚郵件，邀請收件人前往瀏覽某個網站，而當收件人受誘騙進入該網站之後，其電腦便會被自動植入「下載器」（downloader），控制者便可在受害電腦上監聽傳輸資料，最後下載器除會向操控者報到之外，亦可自動連結到某些特定的網站，同時將所有的木馬工具包或更多的「下載器」運送到該電腦，使其能力不斷增強，而該受害電腦也可經由網路芳鄰的連結，伺機發動攻擊，使同一網段中的電腦無一倖免。目標式攻擊可怕的地方，在其成群結隊入侵的特性，以及不斷自動更新升級的手法，除可有效地避開防毒軟體的偵測之外，就算發現了，也可能因為複合式病毒或太多木馬，清不掉也清不乾淨。

此外，因為每一台電腦的原始檔案都不一樣，感染途逕及處理方法也不盡相同，因此資訊部門人員無法以標準的作業程序，將解決方案快速部署至整個網路，而陷入左支右絀、疲於奔命的窘態。

目標式攻擊的另一個問題是中毒後的清除程序，由於清除工作不只是還原某一種惡意程式的某一種損害行為，因為一次攻擊所包含的惡意程式碼往往不只一種，而且攻擊的時程也可能持續一週甚或數月，檢測人員除須終止所有非正常的程序、刪除惡意程式所建立的檔案或修正登錄設定之外，還必須確認哪些資訊可能已遭受入侵、哪些惡意程式碼可能殘留、哪些系統是近期內的交互感染，有沒有新的病毒或木馬等，並應防止這些程式碼再度發動攻擊或進一步對系統造成損害等。

三、自我防護之道

網路有句名言：「網際網路的時代，有誰會知道坐在螢幕前的是一條狗或是病毒？」形容得十分貼切，因為吾人每日所瀏覽的網站、所收的 e-mail 到底是不是偽冒的，實難察知，因此，惟有建立資安憂患意識，隨時提高警覺，始能避免受駭。以下整理上網時特應避免的行為，籲請注意：

1. **不隨意開啟不明來源之電子郵件**。
2. **不隨意執行郵件內夾帶之檔案或連結**。
3. **避免下載免費軟體或圖檔**。
4. **不隨意點擊網頁內的連結網址**。
5. **不隨意點擊彈出式廣告或不明內容視窗**。

※6. **避免使用點對點（P2P）軟體分享檔案**

7. 不使用盜版軟體或破解程式。
8. 不使用網路駭客工具。
9. 避免點擊即時通或部落格內不明的網路連結。
10. 避免依安全警告訊息點擊或開啟視窗。

上列危險動作，僅提供自我檢查，惟當務之急，還是建議網友安裝一種以上的反間諜軟體，並定期掃描檢測，以確保安全；另以下幾項觀念，屬資安基

本認知，亦應防範：

沒有任何一種防毒軟體可以偵測所有的惡意程式，病毒檔案類型除傳統的.doc、.exe、.dll、.com、.sys 外，.ppt、.xls.、.htm 及.wmf 等類型漏洞的利用則屬新興攻擊方式。

駭客都是夜行性動物，根據各企業組織「資安監控中心」分析結果顯示「愈夜愈美麗」，因此**隨手關機或中斷網路連線，環保又安全**。

所有 p2p 的服務除易招惹病毒或木馬外，等於在防火牆或防毒軟體開了一個門等著大家來光顧。

所有的駭客手法中，以透過 e-mail 的釣魚手法最難防範，不管資安教育做得再落實，只要 e-mail 偽裝得夠好仍會淪陷（攻心）。

如果你的防毒軟體在系統內重覆發現同一個病毒且清不掉，代表已知型的病毒夾藏未知病毒，複合病毒代表你的電腦具有高風險。

所有的木馬都是用網路保密協定（SSL）加密與中繼站連結，因此網路型入侵偵測機制對木馬而言，形同虛設。

所有的駭客工具通常夾帶有木馬程式（天下沒有白吃的餐）。

軟體弱點仍以「緩衝區溢位攻擊（buffer overflow）」為榜首，因此安裝防火牆、防毒軟體及適時的漏洞修補是必要也是基本防護。

四、結論

網際空間「所見不一定即所得」，這個道理每個人都應了解。當攻擊的目標從系統轉移到網路應用程式，再轉移至個人用戶時，表示「防毒以外的保護」才是防堵這些新型資安威脅的最佳對策。因為問題的根源不僅止於個人電腦，同時還涉及網路傳輸設備。當然，安全的解決方案與機制沒有所謂的照表操課保證成功的公式，網路社群也往往會鬆懈一般使用者的心防。一味地強調多重防護機制，可以有效防範來自外部的威脅，然而事情只做了一半；另一半，甚至是更大部份的威脅是來自內部人員，因此，惟有積極地縮小組織內部人員的資安貧富差距，使所有成員都是資安偵察員，才能化被動反應為主動防禦，才能在安全防禦與攻擊者這場無止盡的攻防競賽中超前。