機密維護常識彙編（97 年 4 月份）

＊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，So-net 員工甚至高層幹部都不知自己的電腦已中毒。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。

以上只是近年電腦網路犯罪的個案，就 2006 年而言，資安研究人員大多已觀察到並提出一種現象，那就是「目標式攻擊」(Targeted Attack)或「地區型攻擊」已逐漸成為主力，相較於以往如 Code Red、Blaster、Sasser 等病毒發作時期的無差別式蠕蟲攻擊行動，攻擊者已經鎖定特定目標族群或地區，攻擊的行動複雜但精準，並廣泛採用社交工程（Social Engineering）技術，其背後所牽引的動力，已不再是單純的駭客展現功力，而是以金錢獲利為主要的動機。

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。這樣的狀況已不斷重複地上演，而各單位資安人員卻可能束手無策。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、惡意程式也搞創新

以往的駭客以「零時差漏洞」（Zero Day Exploit）為標準配備，攻城掠地、搶奪地盤的入侵行動只為證明自己的功力，但隨著軟體及網路的複雜化，加上獲利的趨使，給予入侵者更強烈的動機，因此工具的發展不僅精緻化且模組化，可隨心所欲升級，而數個工具的組合可發起一次成功攻擊，但分開使用時沒人會發覺它們不軌的行徑。此外更令人憂心的是，安全防護是被動式的，本屈居劣勢，當攻擊的時間或地點分散，除加深資安或網管人員採樣解析的難度外，變種病毒不斷繁衍與自我更新，有愈來愈多的時候我們看到中毒時，防毒軟體卻默默無言，即使發現也大多無法清除或隔離，因此國外許多專家紛紛喊出「防毒軟體無用論」。

放眼今日，惡意程式已和網路應用緊密結合，從攻擊面可嗅出駭客思維的轉變，包括鎖定特定目標較易獲利、利用網路社群遂行社交工程較易得手及獲利等面向。另從實務上來看，木馬或間諜程式發威，不論銀行或公家機關無一倖免、網路釣魚技巧使詐騙行為隱匿於無形、專為行動裝置發展的惡意程式從概念驗證到威脅成真、病毒程式可讓主機報癈，以及商業軟體所提供的工具箱（Rootkit）淪為玩家作弊利器等案例，顯示惡意程式手法不僅日新又新，且創意十足。因為在這些攻擊者的眼中，當獲得的報酬愈來愈吸引人時，惟有持續研改攻擊的方式與技巧，整合駭客、間諜及惡意軟體，甚或發展成分工細密的組織，才能滿足發動攻擊的實需。而這些整合性的精準攻擊手法，在 2007 年及未來將持續為攻擊者所用，甚或不斷發揚與創新，

網路世界將無法擺脫這些惡意攻擊者的糾纏。

四、資安廠商對網路攻擊之分析與預測

回顧 2005 年，網路攻擊主要來自即時通（IM）蠕蟲、木馬、病毒及混合式攻擊等威脅。以混合式攻擊的病毒來說，特洛依木馬程式的隱匿入侵、蠕蟲的迅速散播及間諜程式高超的偽裝技巧，三個惡意元件聯手出擊的「網路釣魚」，已使網路安全防線瀕臨崩潰。隨後，原專攻大型企業用戶網路的「勒索程式」，逐漸威脅家用電腦或小型企業用戶，因為網路勒索的歹徒不但覬覦企業大魚的豐厚回報，也狡詐地嗅出鎖定家庭用戶或小型企業可降低被捕的風險。而更甚者，利用僵屍網路（Bot Net），展開分散式服務阻斷攻擊，以驚人的流量癱瘓那些不願付款的網站。

到了 2006 年，這些模式除轉變得更精緻外，更有整合之勢。依資安公司 Tipping Point 近期公布 2006 年以 20 大網站為對象所遭受攻擊的分析報告指出，2006 年由於網路詐騙而招致的損失，較 2005 年上升 4 至 5 倍。該公司並提出 6 大主要攻擊趨勢，這項公告將有助資安人員更有效率地調整組織的防護機制，以對抗不斷出現的新漏洞，從而避免電腦遭非法操控及竊密，攻擊趨勢如次：

零時差攻擊（Zero day attack）已不再只襲擊 IE 瀏覽器，更有蔓延至 Microsoft 其他應用軟體的趨勢。

現存 Microsoft Office 產品如 PowerPoint 及 Excel 的漏洞，其攻擊有加遽之勢。

針對性或目標性之攻擊持續上升。

證據顯示較多針對軍方及政府機構外包合約商網站而發動的魚叉式網路釣魚攻擊（註 1），已擴散至其他類型機構。

網路語音（VoIP）攻擊已透過轉售通話謀利，並有可能加進錯誤引導訊息，屆時將影響傳統電話網路。

網路應用軟體持續出現大量的漏洞。

此外，趨勢科技也發表 2006 年資安威脅分析與 2007 年的資安預測報告。其中 2006 年組織型犯罪仍以「身分竊取」、「商業間諜」及「商業勒索」為主，而殭屍網路已成為尋找攻擊目標的駭客們所普遍運用的工具。預判 2007 年網路攻擊事件將愈演愈烈，並以社交網站為主要的攻擊目標。究其原因，係多數國家頻寬已大幅提升，使得不管是影音檔案、新興的應用程式或其他資料類型檔案的下載運用，變得非常普遍。因此有愈來愈多的攻擊者入侵公開網站，將他們所撰寫的惡意軟體隱藏其中，讓毫無戒心的用戶在下載含有惡意軟體的檔案後，就會觸發多重的感染。此外，攻擊活動除具大規模外，還可迅速轉移，當混合式威脅變得愈來愈狡詐，將使威脅爆發的方式變得十分不同，而偵測、復原所投入的成本亦將倍增。

五、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。以下整理吾人上網時特應避免的行為，籲請網友注意：

不隨意開啟不明來源之電子郵件。

不隨意執行郵件內夾帶之檔案或連結。

避免下載免費軟體或圖檔。

不隨意點擊網頁內的連結網址。

不隨意點擊彈出式廣告或不明內容視窗。

避免使用點對點（P2P）軟體分享檔案

不使用盜版軟體或破解程式。

不使用網路駭客工具。

避免點擊即時通或部落格內不明的網路連結。

避免依安全警告訊息點擊或開啟視窗。

上列危險動作，僅提供網友自我檢查，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。

除了上述個人應注意的事項外，企業組織在架構對外的防禦機制之餘，應思考前端防禦除病毒防護、修正程式派送外，尚可強化各個終端抵抗深度攻擊的能力、加裝反間諜程式，並適當攔阻與管控威脅等，藉多重防護機制應可避免災損擴大。而在後端，則應強化內部存取控制、制訂身分識別機制，同時應定期對於內部網路流量、連線行為等實施追蹤與分析，如此將有助於即早預警及攔阻隱藏性的攻擊行為，並能防止內部人員的攻擊或竊取機密資訊。

六、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，除應廣擴網路安全防禦的縱深外，如何有效蒐證鑑識以訴諸法律行動，又屬另一個研究之範疇。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。

註 1：「魚叉式網路釣魚」（spear phishing）攻擊，是指駭客鎖定特定組織成員每天瀏覽固定網頁之習慣，在網頁或是受害系統中置入病毒自動下載器，並持續更新病毒變種到受害系統謂之。

（本文摘自政風司網頁/吳文進）

※隨手做、順手做、用心做

一、密件資料應妥慎管理保存，辦公桌抽屜及公文櫥櫃必須確實關鎖，嚴防被盜印或竊取。

二、經辦之密件資料，不得隨意散置桌面，下班或臨時離開時應妥為收起，以免被人翻閱窺視而洩密。

三、密件資料在內部傳遞如陳送或會辦時，應當面親交，如主管或當事人不在，應原件帶回下次再送，不可逕置桌上自行離去，以減少他人翻閱窺視甚至遺失之機會。

四、辦公用之廢棄文稿、複寫紙、影印紙等，應即清理銷燬（用碎紙機碾碎），嚴防散落外洩。

五、由職務知悉之機密公務，未經長官核准或有合法依據，不得在任何場合與人談論，更不得擅自對外提供資料。

六、密件資料非經主管核准，嚴禁複印或傳真發送，傳真機禁止傳送私人文件資料。

七、遵守門禁管理視定，非有公務必要，不要讓外客進入辦公室洽談，如發現不明外人闖入辦公室，應即主動加以詢問，並報告主管處理。

八、重要會議資斜，應編號分發，會後收回，其有帶走必要者，應予登記。有關會議內容，在尚未公開之前，與會人員應嚴格保密。

九、個人職務上持有之密件資料，未經奉准嚴禁攜出於外，尤不得攜帶至公共場所或友人處所。個人演講、寫作、授課、通信、日記等，不得涉及公務機密事項。

＊刪除不明電子郵件，慎防網路釣魚

根據國際組織「反網路釣魚工作小組（APWG）」的定義，網路釣魚（Phishing）是利用偽造的網站或是電子郵件作為誘餌，利用使用者一時不察進入偽造網站後後，騙取您的個人基本資料、銀行帳戶密碼或信用卡號碼等資料。

不要以為只有利用電話才能詐財，最近流行的「網路釣魚」更令人防不慎防。其詐騙的過程，大多是偽造各種賺大錢、聳動、博人同情的新聞或假冒各大金融機構、網路購物、拍賣網站的通報、促銷電子郵件，在取得使用者信任後，利用郵件中的假連結，誘騙受害者前往幾乎 100%相似的仿冒假官方網站，主動鍵入信用卡號、金融帳戶帳號密碼，甚至伺機植入木馬或間諜軟體等惡意程式。

提醒您：

1. 不要任意開啟或點選不明電子郵件中的附件檔案或連結。
2. 使用網路購物、拍賣或網路銀行時，最好盡量用 key in 的方式鍵入網址。
3. 接到不尋常或太好康的訊息時，應思考內容的可靠性，寧可去電查證而不要點選來信所附的連結。

＊為酒店護航 派出所副主管洩密起訴

3 分局土城派出所副主管王○秋，與酒店負責人高女交往密切，被督察室鎖定為加強考核對象，去年六月警方臨檢時，他竟以行動電話發送簡訊告知高女，被依洩密罪移送法辦，並經檢察官提起公訴。

台南市警局表示，督察室靖紀小組，是在去年底接獲民眾檢舉，指土城派出所副主管王○秋，經常前往轄區內富爺俱樂部酒店喝酒，

而且和負責人高女頗有交情，督察人員乃在去年底調閱王員通聯紀錄分析，查知王員涉有洩密罪嫌。

經調查後，證實王○秋在去年六月中，3 分局要前往富爺俱樂部臨檢時，他竟發送簡訊給負責人高女，今年一月卅一日調查完畢後，將他依洩密罪移送台南地檢署偵辦，並立刻將他調整服務地區，調至 1 分局警備隊，同時，督察員又查出，王員另於勤餘時間，涉足該不正當場所，並召女陪侍，馬上記過 2 次。

台南地檢署已在六月廿一日，依洩密罪將王某提起公訴，台南市警局將待法院判決確定後，依法將他移付懲戒。

台南市警局說，陳富祥局長到任後，對風紀問題非常重視，近日一再指示督察室和單位主管，對有違法違紀之虞的部屬，除應加強法紀教育和嚴予考核外，並應依法查處違法違紀者案件，絕不姑息、不庇縱，斷然處置，以整飭警察風紀。【中國時報 / 黃文博 / 台南報導】

＊收賄、洩密 員警判刑

警員湯○興等人向盜版光碟業者收取「保護費」、私下查報車籍等，涉貪污、洩密案，花蓮地方法院依收受賄賂罪、洩密罪判處湯○興、繆○國等人分別判處 5 年 2 個月至 5 年 8 個月徒刑。

法院判決，前軒轅派出所警員湯○興涉嫌在查緝時盜版光碟時，與業者達成協議，遇警方查緝時，湯某不予查報或私下發還，收受業者賄款。

警官鍾○憲涉嫌利用警用電腦查系統，為友人查詢車籍資料，涉嫌 洩密罪。

前保二總隊保護智慧財產權警察大隊花東分隊隊員謝○榮，涉嫌

為業者通風報信。

前警員繆○國涉嫌受賄款，對於假結婚的大陸人民進入台灣地區保證書上核章，同時不予查緝。

全案經法院判決：湯○興依貪污罪處 5 年 8 個月徒刑、褫奪公權 5 年，所得財物 45000 元追繳沒收。鍾○憲依洩密罪處 4 個月徒刑，得易科罰金。謝○榮依貪污罪處 5 年 2 個月徒刑，褫奪公權 5 年、所得不當利益應追繳 3400 元。繆○國依貪污罪處 5 年 4 個月徒刑，褫奪公權 5 年、所得財物 10000 元追繳沒收）。另外，保二總隊的花東分隊教官陳○民並無違背職務收受不正利益，判決無罪。

【中國時報 / 簡東源 / 花蓮報導】