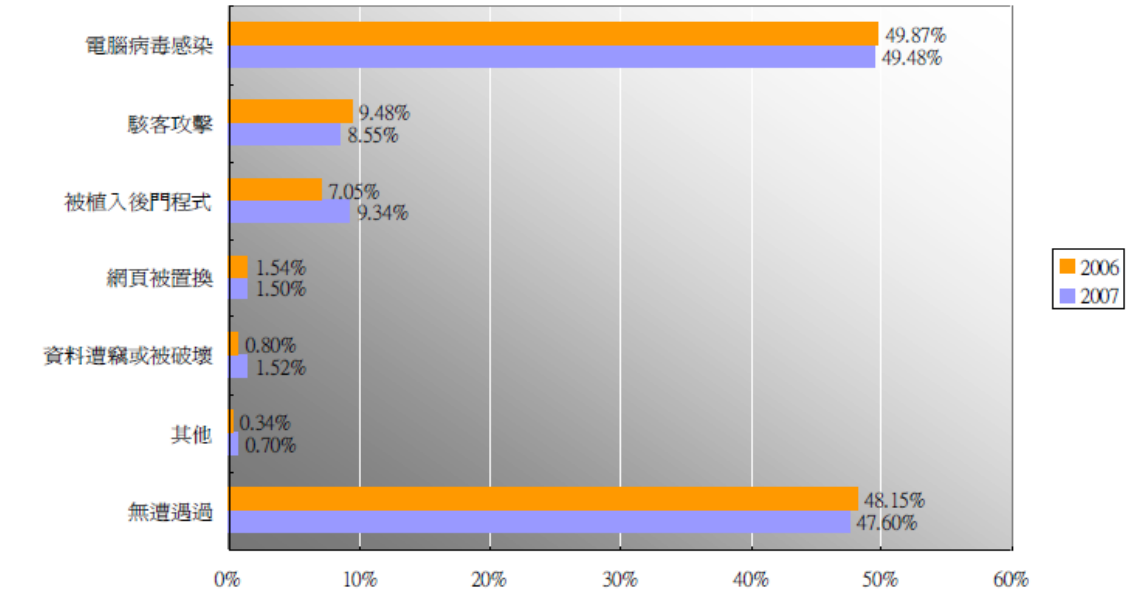
關貿第 22 期電子報

哈燒話題：打擊病毒流竄－USB 自助式掃毒檢測平台

文: 邱華名 課長、林恆生 工程師

關貿網路資安服務課

近年來國內各企業爲反應國際快速變化之環境需求，紛紛導入企業電子化機制，並投入大量電腦及網路資源，然而近年來企業常遭遇「電腦病毒」、「網路攻擊」或「資訊洩露」等危機，依據台經院資安調查報告指出，我國電腦病毒所造成的風險居高不下，但國內企業投入資安資源經費卻相對少很多，而資安人力投入部分亦差異甚大。以我國行政院資通安全會報及主計處今年(98)所做的調查，目前台灣遭遇的主要風險包括電腦病毒感染、駭客攻擊、被植入後門程式、網頁被置換及資料遭竊或被破壞。由此可見，電腦病毒感染應是企業首要必須解決的資安問題。如圖所示。



資料來源：行政院主計處2007年電腦應用概況報告，2008年10月

(圖：資訊安全統計報告)

病毒擴散利用的途徑非常多也通常是多管道並行的，其中包含瀏覽惡意網站造成感染病毒、或瀏覽所謂的掛馬網站等。開啓惡意的病毒郵件、詐騙郵件或是透過中毒電腦對內部網路進行傳播，而最近較爲嚴重的問題就是利用 USB 隨身碟傳播病毒等。病毒在企業內部傳播與擴散，輕微者造成網路塞車影響員工作業，嚴重的導致主機伺服器服務中斷，甚至有可能洩露出重要的機密資訊。所以，完整的縱深防護機制才能將該項風險降至最低。

在企業內部針對員工瀏覽惡意網頁造成感染病毒的問題，以網頁信任評比過濾方式避免員工瀏覽不當網頁造成病毒感染，針對惡意病毒郵件及詐騙郵件，利用郵件過濾系統進行攔阻，員工電腦病毒問題則利用防毒軟體及定期漏洞更新來進行防護，減少員工電腦感染病毒的機率。

但是隨著 USB 隨身碟的便利與普及，越來越多人使用 USB 隨身碟作爲電子資料攜帶的器具，然而衍伸出來的問題除了資料外洩的控管問題外，USB 隨身碟也成爲病毒傳播的最佳載具。所以近年來，不管是公務機關、私人企業等都飽受 USB 病毒之苦，甚至還有軍事單位因爲此原因，限制使用 USB。科技、便利與安全，往往無法面面俱到，其解決方式也不見得一定全面封殺，應在其中取

得一個平衡點才是因應之道。

關貿網路作爲服務供應商的角色，爲客戶提供優質與便利的服務是我們的宗旨，但與客戶或夥伴間的業務往來頻繁，確也造成了一些病毒透過 USB 隨身碟流竄進入公司內部的網路，也因此造成同仁日常作業上的影響。爲了享受 USB 隨身碟的便利性，也避免外出洽公的同仁，返回公司的同時，將 USB 病毒攜帶回公司。關貿網路的資安團隊規劃了病毒的防護策略，首先，於公司的櫃檯出入口處放置一自行開發與整合的**『USB 自助式掃毒檢測平台』**（同仁們口中戲稱的 USB 病毒終結者），讓進出公司的同仁能夠簡易的對自己的 USB 隨身碟進行檢查。再來是透過安裝在同仁機器上的防毒程式、網路入侵偵測防禦器（IPS）以及 7x24 資安監控中心進行病毒入侵的監控作業，最後再利用資安政策對同仁的 USB 碟使用進行規範，並透過教育訓練讓同仁了解與養成良好與正確的 USB 隨身碟使用習慣。在公司使用了該平台之後，成功的發現近三成的訪客攜入的 USB 隨身碟是含有病毒的，並經過檢測台全部徹底的刪除病毒，成功的阻絕可能在內部發生的病毒擴散。

目前資訊安全採用多層防護措施的觀念，從 SOC 資安防護監控、弱點掃描、滲透測試、源碼檢測、防毒掃描、網頁異常監控、電子郵件警覺性測試到 USB 病毒掃描，採取的是縱深防禦的架構，越是及早進行防護，所造成的影響是越小。所以，針對病毒隨 USB 攜入的防護，我們在員工與訪客經常出入的櫃台設置 USB 檢測站，提供進出同仁及來賓訪客所攜入的 USB 隨身碟進行病毒消除的服務，以避免病毒自外部進入企業內部造成營運上的影響。此外，本公司配合 7x24 資安監控中心（SOC）即時監控是否有病毒在內部擴散，及整合入侵偵測及預防系統(IDS/IPS)的防禦措施，讓病毒感染後的擴散行爲能及時被發現及時處理，以避免災情擴散造成的企業損失。

圖：關貿網路 USB 自助式掃毒檢測平台簡易操作介面

『USB 自助式掃毒檢測平台』在病毒防護縱深中，扮演著第一道防線的重要角色。本產品具有以下幾項特色：

- 操作簡易：要讓公司每一位同仁或外部訪客都能夠輕易操作，放置於公司櫃檯的自助式檢測平台才能發揮最大的效益，因此我們設計的操作步驟，全部僅需二個步驟而已。一、插入 USB 隨身碟，二、輸入員工編號啓動掃瞄，然後就結束完成掃毒動作
- 有效阻斷：不僅對已知的病毒進行清除，更對病毒常用的擴散手法進行攔阻，對無法辨識的新型病毒，至少能切斷其擴散與感染的途徑，避免病毒被攜入企業內部造成內部感染
- 強化抵抗：利用植入唯讀 Autoruns.inf 資料夾，爲 USB 產生"抗體"，避免病毒透過 USB 進行擴散
- 可信任的服務：透過程式執行清單管制技術，確保自助式掃毒檢測平台不受病毒的感染，提供使用者安心可信任的掃毒平台

根據資訊安全的木桶理論－由許多塊長短不同的木板箍成的木桶，決定其容水量大小的並非是其中最長的那塊木板或全部木板長度的平均值，而是取決於其中最

短的那塊木板，如果我們各項防護都進行了，安裝了 IPS、IDS、防毒程式…等。卻忽略防堵 USB 病毒擴散的管道，那仍然有可能讓病毒被帶入公司造成內部的感染與擴散，所以除了配合公司資安政策對 USB 使用的宣導以及內部資安意識的教育訓練外，在進出口處設置的防護機制，在技術上也提供多一層的防護措施，完整的病毒防護縱深才會讓企業遠離病毒的夢魘。

新聞播報：

第五屆歐亞無紙化貿易聯盟高峰會議於吉隆坡圓滿結束

第五屆歐亞電子商務無紙化貿易聯盟（Asia Europe Alliance for Paperless Trade, ASEAL）高峰會議，於 1 月 18 -19 日在馬來西亞召開。此次高峰會議由馬來西亞主辦，參與的國家包含：德國、韓國、英國、法國、塞內加爾、挪威、香港、中國、利比亞、哥倫比亞及亞洲開發銀行(ADB)，台灣則由經濟部國際貿易局徐純芳副局長率同關貿網路公司參加。

馬國貿工部次長拿督 Mukhriz Tun Mahatir 於致詞中表示無紙化貿易爲平衡安全供應鏈及貿易便捷化之工具，ICT（資通迅科技）協助創造經濟實績，並強調電子商務推動需要政策之協調及區域間之合作。

ASEAL 現任主席法國 France eCI 之總裁 Mr. Jean-Marc Dufour 致詞中表示目前全球景氣已逐漸復甦，強調民間企業的參與使整體商務環境更便捷及有效率，對景氣復甦有極大助益。同時也感謝於上屆在台灣的高峰會議中選定的歐洲及亞洲常設秘書處，由英國 SITPRO 及台灣關貿網路公司，負責推動跨境無紙化工作及跨區域合作成果顯著。

高峰會議中，各經濟體成員就各國電子商務及跨境合作之發展作充分的說明及討論，台灣關貿網路史蘭亭經理亦就「台韓電子產證交換」合作案例於會中分享。另外也說明台灣爲馬國第三大投資國，馬國台商自台灣進口原物料，在馬國加工生產後外銷世界各地。若能促成台馬無紙化貿易合作，對促進台馬間貿易將有極大幫助。此項建議亦獲馬國正面回應。

ASEAL(Asia Europe Alliance for Paperless Trade)於民國 93 年 9 月成立，其宗旨爲以安全、便捷的電子化方式串連歐洲及亞洲各國之跨境貿易。此聯盟成員之加入皆得該國政府之全力支持，以確保聯盟跨國貿易無紙化服務之中立性及可靠性。至於貿易業者，只需透過當地之通關網路公司，即可安全、快速的與其他國家合作夥伴進行連線交易。


A-EAL

e 卡掌握　數位生活

-RFID 應用發表會-

隨著無線射頻辨識(RFID)技術的日益成熟與穩定，在不同領域中的應用也越來越廣泛，由這小小晶片帶來的巨大商機，已成爲近年來的熱門話題，從身分識別延伸到服務自動化，乃至跨業付款等，不僅是日常生活的廣泛應用，更帶來產業供應鏈的革新。

商業司爲充分展現推動成效，持續推動台灣 RFID 產業的成長，並使一般大眾了解計畫與年度成果，特整合 RFID 加值應用旗艦示範計畫 (關貿網路公司執行)、加工食品流通履歷追蹤計畫、智慧型陳列架展示銷售服務計畫等，於 1 月 22 日假台北國際會議中心 1 樓舉行聯合成果發表會，今年的主題定爲「e 卡掌握數位生活」，揭露未來的智慧化數位生活，只要一張內置 RFID 晶片的 e 卡就可以完全掌握而暢行無阻。

經濟部商業司司長葉雲龍在開幕致詞中表示：「RFID 的未來性已經明確地揭露，也有許多企業嗅出端倪並走在趨勢的前端，我們希望今天的成果能帶來更新的局面。也期許未來 RFID 產業的規模與產值，隨著應用層面的擴大，大規模提升」。

發表會中除有靜態的成果展示，還特別設置一個 RFID 未來智慧生活的體驗區，讓與會者透過手上與悠遊卡結合的出席證，完成食品或服飾的消費結帳流程、社區家戶的門禁展示，也可上網查詢電子發票、登入共享平台使用電子書或愛卡啦等消費紀錄，甚至結合安全照護系統記錄日常的體溫血壓等，都可以由一張 RFID 卡串接完成。

關貿網路執行經濟部商業司推動的「RFID 加值應用旗艦示範計畫」已達三年，98 年度運用前期執行的成果與便利應用情境，擴大推動協助北、中、南共 12 所學校導入智慧化校園建置，從基礎的發卡、身分識別，進而與校務資訊系統整合，讓多元的 RFID 應用服務透過簡單的註冊及登錄，與校務系統緊密結合，並藉由卡片的應用管理，導入電子消費機制，延伸擴充生活消費儲值與扣款功

能。未來更將近一步整合校園內及周邊商圈的電子錢包應用，達到推廣 RFID 便利生活圈，帶動 RFID 推廣效益示範之目的。

在智慧化社區推廣建置上，今年持續於台北市木柵二期重劃區，選擇具有資訊基礎的社區與社區型安養護中心，進行智慧化社區應用服務的建置與導入，並與已完成建置的社區進行跨區域合作與整合，讓智慧化社區的服務平台實際運作，並逐步完成建構智慧化社區藍圖的目標，達成 RFID 便利生活圈的理想，期望讓校園的學生與社區的居民從生活中享受 RFID 帶來的便利，進而擴散全面提升 RFID 的加值應用，期望透過加值應用服務的推廣，從消費需求端的提升，來帶動 RFID 相關產業的發展。

活動快遞：

ECFA 架構下兩岸物流運籌及中國物流基盤調研與內需「品牌」戰略佈局研討會

ECFA 簽約在即，爲讓物流運籌產業進一步了解其對產業的發展與衝擊，特邀請交通部及國貿局長官出席闡釋及東莞台商協會葉會長分享 ECFA

對於台商的影響狀況爲何?可以讓大眾對於 ECFA 有更的了解。

爲了解大陸物流基礎建構數據，特別邀請大陸福建省福州大學副校長王健來台就海西物流基盤調研進行發表，可以讓大眾了解海西蘊藏多少商機。

最後我們也邀請到兩岸連鎖經營協會王理事長來分享【流通業前進中國內需市場如何進行「品牌」戰略佈局】，活動內容如下，竭誠歡迎各界踴躍參與。

一、時間：2010/2/26(五)1330~1800

二、地點：交通部運輸研究所國際會議廳(台北市敦化北路 240 號 B1)

三、費用：免費參加,名額有限,請先報名

四、主辦單位: 台灣全球運籌發展協會(GLCT)

五、活動聯結：http://www.glct.org.tw/Train/train.asp?vid=46

服務新知：

美國海運預申報服務

繼 911 事件後，美國海關爲了能對全球進口至美國的貨物進行安全控管，於 2004 年 2 月 2 日起在全球實施「裝船前 24 小時申報艙單規則（24hr Rule）」，要求進口美國的船運公司（Carrier）及出口國貨運代理（Forwarder）須在貨物裝船前二十四小時，將艙單資料傳輸至美國海關。

於 2010 年 1 月 26 日起，除了原有的「24hr Rule」之外，美國海關將強制執行 Importer Security Filing（進口商安全申報）簡稱 ISF（10+2）新規定。新的法規要求美國的進口商（Importer）或其委託的台灣出口商／承攬業，必須在貨物裝船前二十四小時，將所規定的資料傳輸至美國海關，並將針對以下 4 種情況，對未正確申報的進口商每次最高可被罰款 5,000 美元。

1. 進口商沒有申報 ISF
2. 進口商沒有在登船 24 小時前提出申報
3. 進口商 ISF 申報訊息有誤
4. 進口商誤報的 ISF，未從海關系統刪除乾淨

爲便利各型企業用戶，關貿網路推出【美國海運進口預申報服務】，協助承攬業者及進出口商申報 ISF (Importer Security Filing)、AMS (Automated Manifest System)資料。

您可透過 Web 登打方式，也可經由既有承攬系統或 ERP 以 EDI 檔案傳輸方式進行申報作業，並即時獲取美國海關回應訊息掌握申報狀態。

DM 下載

資安小常識：

何謂電腦鑑識

伴隨著資訊化程度及資訊安全要求程度不斷地提升，資訊與法律成爲各大企業管理者、技術長(Chief Technology Officer，簡稱 CTO)所要面對的議題，也因爲資訊事件層出不窮，電腦鑑識學開始成爲一門熱門的學問，而日漸受到重視。

維基字典對電腦鑑識的定義是一門從資訊設備、數位儲存媒體中尋找不法證據的鑑識科學，當企業或個人遇到資訊緊急事故時，如何像 CSI 鑑識人員一樣還原事件真相，即可歸屬於電腦鑑識範疇。鑑識作業四大主要元素：

1. 數位證據的保存：

此階段是整個鑑識流程的第一步，在鑑識過程中，爲確保資料及保持所蒐集證物的完整性，不會因關機、重新啓動、人爲有意或無意地破壞等外在因素發生，導致原料資料損毀，所以優先步驟就是管制現場，並透過諸如 LiveDector、RealDector、Helix 等數位工具將數位證物建立完整映像檔及 MD5 檔，以確保證物的完整性及不可否認性。爲避免後續識別及蒐集過程中發生意外，導致原始資料損毀，在此一階段通常會再複製多份，以供識別及蒐集過程使用。

2. 數位證據的識別及蒐集：

犯罪者通常會在犯罪後，將證據或工具予以湮滅，鑑識人員透過了解資訊設備種類、作業系統種類、資訊設備儲存在著什麼樣的資料、證據可能存放處，進而決定要採用的工具及細部作業流程以協助還原證據，提高資料可讀性、可用性，所以此階段是爲後續各階段執行預做準備。

3. 數位證據的分析：

由於電腦系統中所儲存的資料是以位元型式儲存，無法被人所理解，因此被擷取出來的數位證據需要進一步處理。透過電腦軟體的輔助，鑑識人員才能理解、分析內容。除此之外，鑑識人員也會透過分析及檢驗證據的結果，確認數位證據是否可以明確指向特定嫌犯，藉以證明或推斷嫌犯的行爲或用意，進而建立相關證物與嫌犯間存有不可否認性的關係。

4. 數位證據的呈現：

此階段爲電腦鑑識最終階段，由於數位證據相當抽象，加上司法人員對於電腦鑑識相關知識程度不如專業人員的深入，因此本階段分成二部份，一爲報告的撰寫，一爲數位證據的呈現，透過報告詳盡的說明，結合數位證據的可信度、解讀者的專業程度與分析、鑑識過程的品質保證，將事件真相真實且詳實地還原，進而建立報告的不可否認性。

電腦鑑識發展至今已十餘年，伴隨著資訊犯罪案件數量漸增、資訊安全重視程度的增加及鑑識報告具有法律效力等等原因，造成電腦鑑識需求程度漸增，如何建立電腦鑑識專業能力及相關作業程序，成爲資訊安全重要課程之一。