[農產品電子商務]系列報導 之十一

網路安全～小心駭客就在你身邊

高雄區農業改良場　鄭文吉
jwj@mail.kdais.gov.tw

※本文已於2002年5月發表於農業世界雜誌225期56-64頁※

前言

上期大致介紹了電子商務網站實際運作時，在資訊流、物流與金流等三大基本商業行為上面可能遇到的問題，以及一些因應之道。由於物流與金流都必須靠資訊流來加以聯繫，但由於網路傳輸太方便了，任何人都可以輕易的傳送資訊，如果買賣雙方彼此無法相互信任，確定所收到的訊息是對方寄出來的，那麼生意就作不成了。因此，關於網路安全與保密的重要性，隨著電子商務的逐漸風行，也開始為大家所重視。

要談網路安全，不可避免的將會牽扯到許多的電腦專業術語。因此小弟不打算搞得太艱澀，而盡量舉例說明，希望能讓大家多少有點概念，而不會把大家嚇跑。

在探討網路交易的安全問題前，讓我們先來談談，在日常生活上可能遇到的網路安全問題～駭客入侵。

駭客入侵不是電影情節

一聽到網路安全這個名詞，大概許多人就會聯想到電腦駭客(hacker)，然後腦海裡就浮現出電影裡的情節：駭客在家裡隨便按幾個鍵，就可以透過網路任意進出任何人的電腦。大至美國國防部，小到老百姓家裡的個人電腦，甚至連街上的交通號誌、銀行的提款機，甚至被害者日常生活的一舉一動，都難逃被駭客操控的命運。

當然，這是電影的情節，實際上並沒有那麼恐怖～至少交通號誌和家裡的音響應該沒有上網吧，駭客若連這些都能遙控，那也太神奇了點。但是如果你以為，傳說中的駭客都是一些神出鬼沒、身懷絕技、遙不可及的藏鏡人，應該只對美國國防部這類重要機關裡的機密文件有興趣，怎麼會找上我這個平凡老百姓的麻煩呢?而且，一般人家裡的電腦又沒有什麼機密資料，駭客應該沒有興趣來光顧我家的電腦吧?好吧，就算給他進來了，反正也沒有什麼好看的，應該也沒什麼關係吧?

老實說，以前小弟也是這麼想，因此從來也沒有去關心這類的問題。直到

改良場安裝了防火牆，看著每小時上千次的攔截紀錄(相當於每台電腦每小時都有數十人次的駭客嘗試入侵)，才當場傻眼(如圖1)。顯然如果沒有防火牆的話，等於是把家裡的門窗打開，歡迎駭客隨便進來玩。

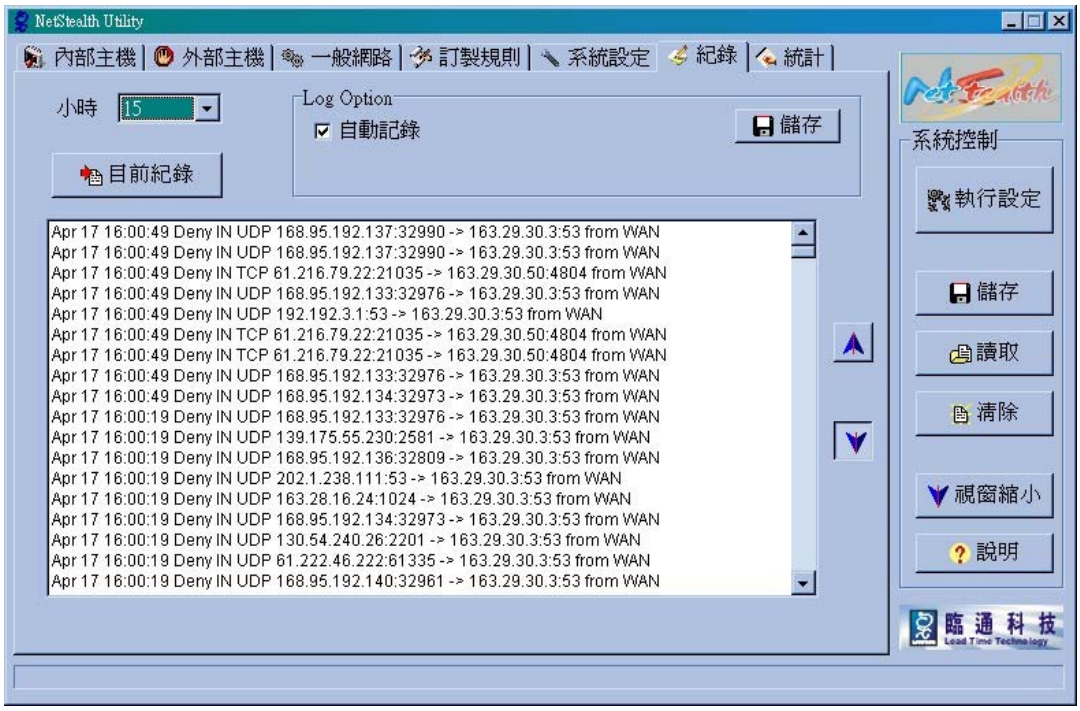

圖1.防火牆的攔截紀錄。顯示在一分鐘內，就有30幾個來自不同來源的使用者嘗試連結改良場裡的電腦。

或許你會好奇，哪來那麼多的駭客啊?其實，當我們連上網路時，就可以到全世界任何一個網站查閱資料；然而相對的，這時候我們的電腦也成爲網際網路的一部份，因此全世界任何一個使用者也可以與我們連線，「查閱」我們電腦裡的資料。這個道理，就跟你家裡裝了電話機，就可以打到全世界任何一個地方，而任何人只要有你家的電話號碼，就可以打電話給你是一樣的。試想，連劫機撞大樓這種事都有人作得出來了，全世界有幾百幾千萬個人在上網路，其中出現幾個神經病會來搞這種事，應該也不足爲奇才對。

況且，就像我們會透過網路收集和分享各種資訊，駭客們其實也會架設網站，彼此分享入侵網路的技術和心得。因此任何人只要對這方面有興趣，就可以透過網路查詢到一大堆的資料。就算你不想花那麼多時間去研究這些網路漏洞，只要隨便到一家書店裡，就可以找到一堆教你如何當駭客的書籍(不信?自己去書店看看就知道了)。而且這些書往往還附上光碟，提供各種現成的入侵程式，讓你可以現學現賣。

因此，現在就有一大堆搞不清楚狀況的小朋友，拿著這些現成的駭客程式到處試驗。反正他們也不是有什麼特殊目的專程要去入侵某個網站，只是隨便亂玩～套句日式的講法是「無差別攻擊」，而台式的講法則是「看到黑影就開槍」。一旦給他找到沒有設防的倒楣網站(例如我們家裡的電腦)，就自以爲是個「駭客」了。對於這種只會拿現成軟體來胡亂使用，本身對於網路原理完全不懂的人，實在不配稱之爲駭客。個人以爲，應該改稱爲clicker(只會按按鈕的

人)比較適合。

所以，現在駭客的攻擊與入侵行爲是沒有一定的道理可循的。只要是連上網路的電腦，都可能是駭客的下手對象。過去大家都用數據機撥接上網時，通常是有需要才上網，資料查完就掛電話離線，這樣駭客可能比較沒有足夠的時間來入侵。就算眞的入侵成功了，當我們掛電話離線後，這個連線就被迫停止，等下次再上網時，因爲ISP業者分配給我們的網址又改變了，駭客就沒有辦法繼續鎖定我們的電腦來攻擊。因此對於撥接上網的使用者來說，遭到駭客攻擊的可能性就很低了。

然而，由於近來按月付錢的寬頻網路日漸普及，許多人的電腦不管有沒有上網，其實都是一天24小時掛在網路上。這時如果沒有適當的防護措施，被駭客攻擊的機率自然就提高了。

因此，駭客入侵可不是電影裡的情節，其實在我們上網時，就隨時都有人在敲門探路的。至於爲何我們好像都沒有感覺?或許對方功力太差，沒有攻進來；或者人家只是敲門敲好玩的，並不是眞的想入侵；或者搞不好人家已經進來了，只是因爲沒有破壞什麼東西，因此你也不知道有人進來過。然而不管是哪一種情形，我們可不能當作沒看到，多作一些防範措施總是好的。

駭客找我幹什麼?

當然你會說，我的電腦裡又沒有什麼機密資料，駭客入侵我的電腦要作什麼?其實，駭客會入侵人家的電腦，除了竊取機密外，還可能有下列幾種目的：

1. 無聊：

前面提過，現在有一堆現成的程式和書籍，只要會按滑鼠按鈕就好了，完全不需要任何電腦功力，連小孩子都會使用。所以許多人閒閒沒事就喜歡拿這些程式來到處惡搞，這也是目前網路駭客氾濫的主因，絕大部分所謂的駭客，其實都是這種半吊子的無聊人士。碰上了這種以惡整別人爲樂的人，你也只能自嘆倒楣了。

2. 拿來當跳板：

如果是眞正的駭客，在他要入侵一個重要的目標，例如政府機關或公司企業的電腦主機時，因爲擔心自己的來源位置被追蹤到，就會先找其他的電腦做爲「跳板」。也就是先入侵你的電腦，然後再用您的電腦去入侵眞正的目標。如果事跡敗漏，人家追查來源，就會追查到你這邊來，而你就成了駭客的替死鬼了。因此不要以爲自己沒有什麼機密資料，就算讓駭客入侵也沒關係。等哪天有人請你去調查局喝咖啡，那時就來不及了。就算最後終於證明你的清白，那也是會搞得烏煙瘴氣的。

3. 測試自己寫的程式或系統漏洞：

當駭客寫出了一個攻擊程式、或者發現了作業系統的某項漏洞可供入侵，總要先試驗一下實際應用的可行性，順便炫耀一下自己的功力。這時候，網路上成千上萬的電腦，就成了他最理想的實驗對象。這時，如果你也連上網路，就很有可能成爲人家眾多的實驗品之一。

4. 挾怨報復：

由於現在當駭客已經不需要什麼專門知識，因此這年頭，駭別人的電腦已成了最新的報復方式。如果你不小心得罪了別人，搞不好人家就偷偷入侵你的電腦，把你的檔案殺光光，或者把你信箱裡的私人信件公諸於世，或者用你的名義隨便發信件給別人等等，給你造成一大堆麻煩。尤其現在學校有宿舍網路、公司有內部區域網路，大家的電腦平時都連在一塊。就算有再好的防火牆，也頂多只能擋住外來的駭客，如果有內賊出現，還是難逃毒手。

如何防範駭客入侵?

前面講得這麼恐怖，我想很多人都會問，要如何防範駭客入侵呢?

其實，這就跟如何防止小偷入侵你家差不多。記得小弟搬新家時，曾跟一位鐵窗師傅聊過這個問題。基本上，我們裝鐵窗，設保全監視系統等等，甚至還加上電網，其實都不能「絕對」保證不會遭小偷。只要小偷的技術夠好、帶的工具夠齊全，就算你的鐵窗再粗、用的鎖再複雜，最後還是有可能會被打開的。設鐵窗和大鎖的目的，其實只是在於拖延小偷打開所需的時間而已，讓他覺得，要開你家的門鎖得花上非常長的時間，而你家又沒有金山銀山，花這麼大的時間和精力，一點都不划算。當然，如果你家眞的有金山銀山，搞不好小偷還眞的會在你家牆壁挖洞。

同樣的，面對駭客入侵也是如此。道高一尺、魔高一丈，沒有人能保證他的電腦系統萬無一失，絕對不可能被駭客入侵。遇到眞正的高手，再完善的防範措施也不一定有用。試想，連美國國防部都可以被駭客像在逛自家廚房一樣的來去自如，更何況是一般的老百姓?

問題是，前面也說過，眞正的高手其實不多，絕大部分所謂的「駭客」，其實只是一些窮極無聊、只會拿現成軟體來用的半調子。這些人對於網路傳輸和電腦運作的原理並不了解，因此如果他手中所用的程式沒法進入某個網站，他就不知道該如何解決，只能放棄轉換其他目標了。對這種程度的駭客，其實只要作一些簡單的防範措施，就可以加以防制。

那麼，駭客究竟是如何來攻擊我們的電腦呢?其實，由於設計作業系統或者應用程式的軟體廠商爲了想要趕快推出新的軟體來賣，有時在設計上會有一些考慮不周詳的地方，使得程式在某些狀況執行時，會出現一些意想不到的結果。例如在瀏覽網站時，在網址後面加上某些奇怪的字句，就可以直接看到對方網站內的硬碟資料，或者啓動網站裡的程式，甚至讓電腦當機，而使對方整個網站停擺～這些都是可以說是電腦安全上的漏洞。

當衣服有破洞沒法直接縫合起來時，我們通常會剪一小塊布來補這個破洞。同樣的，當作業系統或者程式的設計師發現有安全上的漏洞時，也會發布公告訊息，並提供修改的小程式來補這些漏洞。就跟補衣服的小布塊一樣，這些小程式通常也被稱之爲patch(補丁)。

問題是，對一般人來說，通常我們並不會主動去看這些公告訊息；就算看了，往往也不知道該怎麼去補這些漏洞，因而讓駭客有可趁之機。前面提到的

駭客工具程式，通常也都是針對這些安全漏洞設計的偵測軟體。任何人只要有這些程式，就可以隨意的偵測網路上的電腦是否有洞可鑽，根本不需要知道其中的原理。

一般來說，小偷要偷東西前，往往會先打電話或按門鈴，看看主人在不在家，以便決定哪一家可以下手。然後，再勘查一下目標的環境，確定這户人家的防盜措施怎樣，有沒有什麼漏洞，例如門窗忘記關緊，或者門鎖好不好開等等。最後，才眞正下手潛入屋內偷東西。同樣的，駭客攻擊電腦網站，大致也會有下面幾個步驟：

1. 首先掃描某區段內所有網路位置，看看現在有哪些電腦或網站有連上網路，以便確認目標。這種做法有點像小偷不知道人家實際的電話號碼，所以就用當地的電話號碼位置，然後末三碼從000打到999，連打一千通電話，看看哪些電話號碼是有人用的。這看起來似乎很麻煩，因爲在現實生活中如果眞的打一千通電話，可能會累死人，大概不會有小偷這樣做；但駭客使用網路掃描程式，連續掃描一千個網路位址，可能還不用幾分鐘，因此並不是什麼麻煩的事。
2. 當發現有某部電腦連上網路後，就進一步掃描那部電腦有開放哪些服務。按理，我們的個人電腦又不是網站，然而，有時候作業系統也會預設開放這些服務(Windows系統最常搞這種飛機)；如果這些服務又有漏洞，就會讓駭客有可趁之機。
3. 當發現某部電腦有開放某些有漏洞的服務時，駭客就可以利用這些漏洞進入電腦，再設法取得更高的使用權限，最後你的電腦就等於被駭客「接管」了。這時，他要把你的資料檔案殺光光，或者用你的電腦來作他想做的壞事，都隨他高興。

由上面的步驟看來，如果我們可以把自己隱藏起來，讓駭客掃描不到我們這台電腦的存在，就能在第一個階段防止駭客的入侵。這樣不管我們的網路服務是不是關了，或者系統上的漏洞有沒有補起來，都沒有關係了。當然，爲預防萬一，如果漏洞能順便補起來，還是比較安全一點。

要在網路上隱藏自己有很多種方法，防火牆(Firewall)的設置，就是最常用的做法。

防火牆的原理

什麼叫防火牆呢?基本上，防火牆就跟家裡的圍牆一樣，把房子圍起來，讓外面的人看不到房子裡有什麼東西，住些什麼人，作些什麼事。以免錢財露白，吸引小偷的注意和覬覦。外面的人除非有主人的同意，否則是無法進來的。

簡單來說，防火牆是一種放在你的電腦和網路之間的過濾設備。它可以讓你設定什麼樣的人才能通過，如果不是預設範圍內的動作，就通通視爲非法而攔截下來。例如，一般我們家裡或辦公室的電腦都是平常工作使用的，並不是網站，也不會提供什麼網頁給人家看，所以也根本不需要讓人家知道我們的存

在。如果有外面的人居然試圖連上我們的電腦來要求「開網頁」，除了網址打錯的糊塗蛋之外，顯然就是駭客了。

因此防火牆最基本的功能，就是把公司或企業裡所有的電腦全部隱藏起來，只有幾台眞正的網站不得不開放。而且，即使是網站，也只開放某些特定的服務，例如全球資訊網站就只開放讓人家瀏覽網頁、電子郵件伺服器就只提供郵件收發，其他不用的功能就通通關閉，以減少被人家入侵的可能性(如圖２)。

舉例來說，圖１是改良場所設置的防火牆攔截到駭客掃描時的紀錄畫面。由於一般員工的電腦並不是網站，所以也沒有必要開放給外人隨便亂看。因此外來的使用者若想查閱它的資料，或者只是單純測試這部電腦是否有開機而已，都會被防火牆視爲不合法而攔截下來。這麼一來，對駭客來說，我們的電腦等於是不存在的，因而可以免去被他鎖定作進一步攻擊的危險。

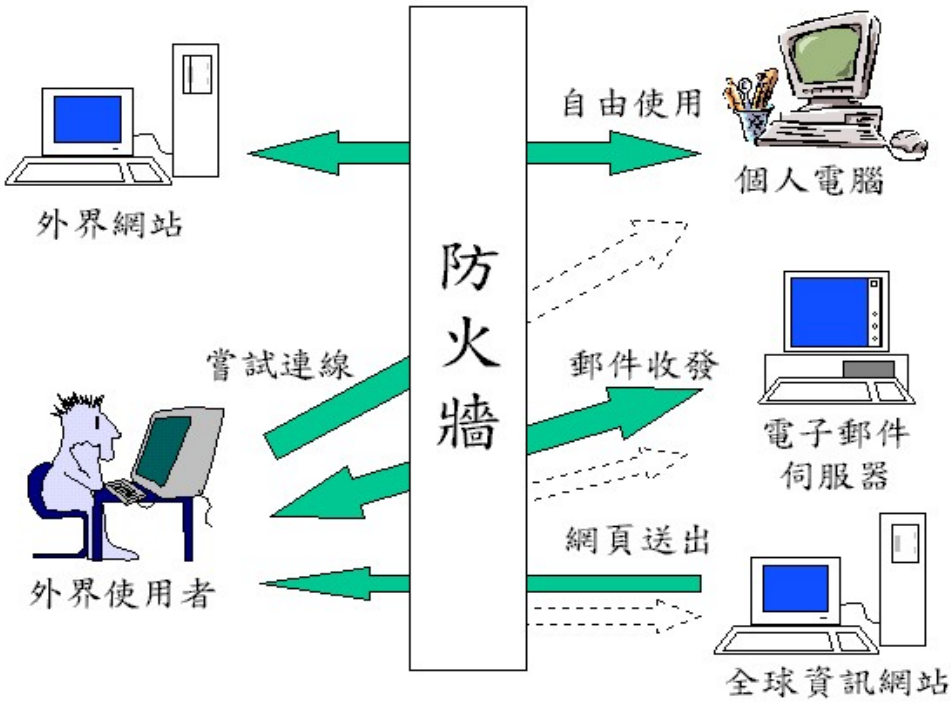

圖2.防火牆的原理。外界使用者只能取得經過許可的資訊，例如收發電子郵件或者瀏覽全球資訊網頁，至於其他的用途及一般使用者的個人電腦則不准進入。但內部的員工則可以自由瀏覽外界的網站，不受限制。

人人可用的個人防火牆

前面所介紹的，是以公司企業或機關學校爲對象的防火牆。這類防火牆通常是架設在機關內部網路的前端，以過濾外部網際網路的使用者不能任意進入內部的電腦。因此它所要服務的對象很多，包括內部和外部的使用者與電腦；而要處理的狀況也比較複雜，有些可以通行，有些則必須攔截。因此這種企業用的防火牆，通常其價位也不便宜，往往要花十幾萬甚至上百萬才行。對於一般人來說，專程買一個防火牆來照顧家裡的一台個人電腦，似乎不太划算。

其實對一般使用者來說，網路大多只是用來上網查閱資料以及收發電子郵件而已。就算眞的有人想架設網站，通常也都是像先前介紹過的那樣，直接使用現成的免費網站空間來架設。大概很少人會拿自己的電腦當作網站，然後提供資訊給人家查詢。因爲要這樣做，你的電腦必須一天24小時開機並保持在上網的狀態。而且，如果有人要查詢你的網站資料，就會佔用你的網路頻寬和電腦效能，這樣就會影響你本身的使用～除非你的電腦自己根本不用，就是專門拿來當網站用的。所以，對一般人來說，我們只要保護一台個人電腦就好了，這樣問題就變的比較單純。這時，我們只要去安裝所謂的「個人防火牆」軟體，就可以達到保護自己的要求。

目前市面上這類個人防火牆軟體很多，功能也各有不同。例如以ZoneAlarm這套軟體(如圖3)來說，它只對企業使用者收費，如果是個人使用這套軟體則是免費的。而它運作的原理大致如下：

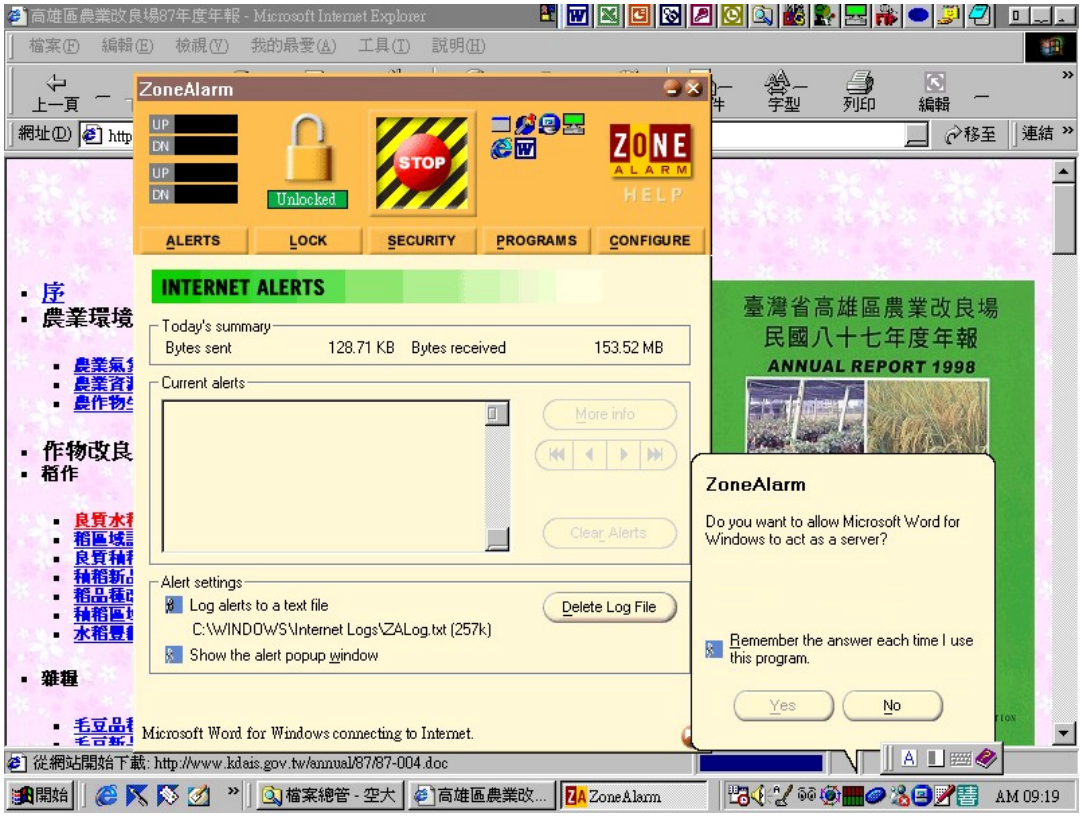

圖3.個人防火牆軟體ZoneAlarm運作的畫面。除了攔截外來的偵測外，當瀏覽網站要求開啓其他的程式時，立刻就出現警告訊息，詢問是否要加以開啓，以確保不會在無意中執行到不當的程式。

1. 先預設關閉所有網路的連線，以確保駭客沒有漏洞可鑽。如果有人想要掃描你的網站是否存在，ZoneAlarm除了將它攔截之外，並且會回報給你做參考。在範例中，由於改良場本身另外有安裝防火牆，因此這些訊息都已經被過濾掉了。在還沒安裝眞正的防火牆之前，ZoneAlarm每天都會回報數十個訊息，看了眞是讓人怵目驚心。
2. 如果你要上網路，當然要執行軟體才行。例如你可能會使用IE來瀏覽全球資訊網站，或者使用Netterm來進入BBS站。這時ZoneAlarm發現有某個程式要對

外連線，就詢問你是否要開放通過。這樣可以避免某些程式(例如電腦病毒)會在未經你的同意下偷偷對外連線。

3. 在你上網路的過程中，有時會因應對方網站設計的需要，而另外開啓其他的程式。例如在圖3的畫面中，小弟查閱高雄改良場87年年報的資料，因爲這些檔案是用word製作的，因此必須另外執行word才能開啓。這時ZoneAlarm就會發出警告，並徵詢你的同意才讓它執行。這樣就可以避免有些不懷好意的網站設計者，故意在網頁中加入某些指令，來啓動你電腦裡具有破壞性的程式(例如Format)。
4. 在程式畫面的左上方有個流量表，可以讓你查看電腦連線傳輸資料的狀況。如果你突然發現，明明自己並沒有使用網路，但流量卻大量湧現，這可能就有問題了。例如很多病毒會透過outlook等郵件軟體，自動散發夾帶病毒的信件，但因爲outlook本身我們自己也會使用，所以會列在ZoneAlarm的許可通行名單中，因而無法被攔截。這時如果你發現寄幾並沒有寄信，但卻有大量資訊向外流出，這時就需要檢查看看了。
5. 萬一你發現有任何異狀，例如前面說的有可疑的流量出現，還有最後的絕招。只要按下中間那個紅色STOP按鈕，就可以立刻暫停所有網路連線，這樣就算駭客已經進來了，因爲沒法繼續遙控你的電腦，所以就來不及收拾入侵的痕跡，而讓人容易察覺出來。如果你檢查後認爲沒有問題，就可以再讓電腦繼續連線，不用重頭開始。

網站的防駭之道

當大家都已經鞏固了自己電腦的安全之後，下一個問題是，那網站該怎麼辦呢?因爲對一般人來說，我們可以用防火牆把所有的掃描全部攔截下來，讓駭客不知道我們這台電腦的存在。但是，那些對外營業的網站卻沒法這樣做，因爲網站本身樹大招風，本來就很容易招來駭客的注意；而且，網站就是要提供資訊傳輸的服務，如果我們也用防火牆把它關起來，那就沒法營業了。因此，網站本身勢必要開放連線才行。

這麼一來，那我們的農產品電子商務網站實際運作時，要如何防範駭客入侵呢?其實，就像鹿鼎記裡韋小寶所說的：「現在江湖上，打悶棍、灑石灰、下蒙汗藥的小毛賊，恐怕比武功高手還多」。現在大部分所謂的「駭客」，其實都是一些只會拿現成駭客工具軟體來亂玩的小毛頭，本身根本不懂什麼網路技術。因此，只要我們將不必要的網路服務關閉，並且經常注意網路安全漏洞的訊息，隨時將已經知道的漏洞補起來，這樣應該就可以防止絕大多數的駭客入侵了。

駭客眞的無法被查到嗎？

前面不斷提到，現在有很多現成的資訊和工具軟體，可以讓任何人都能當駭客。或許有些人也會躍躍欲試，也想去弄來玩玩看。在此，小弟要先警告一

下。如果你以爲只要躲在電腦後面偷偷進行駭客攻擊，就不會被別人抓到，那你就錯了。

套一句電視上常聽到的口頭禪：「凡走過必留下痕跡」。網路世界雖然龐大繁雜，卻也不是毫無脈絡可循。因爲在網站上都會留下連線的紀錄，例如某個時間從某個位置有人連線進來，然後作了什麼動作，如上傳或下載資料，或者是執行了哪個指令或者內部程式等等。網站管理員只要檢查這個紀錄檔案，就可以發現駭客行動的蹤跡。

因此眞正的駭客，在成功進入網站後，都會想辦法將這些紀錄檔清除，讓管理員無法察覺。問題是，如果你對這些原理完全不懂，只會利用現成的駭客軟體進行攻擊，當然就會很容易被察覺出來。

就算你的功力夠高，知道要清掉網站裡的紀錄檔。問題是，我們所進行的網路連線，都必須透過中間許多台電腦主機的轉接，才能讓我們坐在家裡，就能瀏覽美國的網站。而這些轉送的動作，中間每一台電腦主機也都會分別紀錄起來。因此，如果駭客利用電腦上網，就會在所有的網路主機上留下記錄。這樣只要收集足夠的資料，從被入侵的電腦倒著回去追查，就可以查出駭客的源頭。甚至即使駭客遠在地球的另一端，只要各國的警政單位、電信業者、提供上網服務的ISP業者等等全力配合，就能讓駭客無所遁形。許多知名的國際駭客，都是這樣被跨國合作逮捕的。

所以，如果你也想要去「駭人」，可別存著「沒人知道我是誰」的僥倖心理哦。當心人還沒駭到，自己就先進了監獄，那可就不好玩了。

結語

隨著寬頻網路專線的普及，大家使用網路越來越普遍，遭受駭客攻擊的機會也就越來越高。以上大致介紹了駭客入侵電腦的過程和防制之道，希望能給大家一些關於網路安全的基本概念，進而建立一些簡單的防範措施，例如使用個人防火牆軟體，來攔截外來的偵測等等。這些看起來似乎跟我們的主題～農產品電子商務沒什麼關聯，但是卻是攸關大家基本權益的大事。當然，駭客不一定會找上我們，但只要遇上一次，就會讓人傷透腦筋。

老實說，眞正駭客入侵的新聞並不多見。比較常見的，大部分都是資訊機密外洩的問題，例如客户資料被盜賣，或者帳號密碼被猜出來等等。只不過記者們往往搞不清狀況，看到電腦犯罪就自動給它冠上駭客的稱號而已。

由於網路傳輸太方便了，任何人都可以輕易的傳送資訊，但如果買賣雙方彼此無法確定所收到的訊息是對方寄出來的，那麼生意就作不成了。因此，電子商務網站是否能夠經營下去，資訊保密就成爲一大關鍵。如何確定所收到的訊息是對方寄出來的，而且中間不會遭到偷聽或竄改，就成爲大家最關心的問題。下期就讓我們談談這方面的問題，敬請期待。