如何自我偵毒(利用 Pc-cillin) – 個人電腦防毒篇（二）

資料整理自『PC 防毒/防駭 急救手冊 chap.3』學貫 鮑友仲著

一、電腦中毒可能徵兆

系統感染電腦病毒是非常危險的事，因為你不知道病毒發作時會對系統做出哪些破壞，所以在電腦有出現中毒可能徵兆時，務必要檢測電腦是否感染了電腦病毒，以免病毒發作時後悔莫及。

到底有哪些徵兆是代表電腦可能中毒呢?以下筆者就舉幾點狀況提醒大家注意：

■電腦執行速度越來越慢

電腦病毒會在背後傳染、散佈自己，所以會耗用系統的資源，使得電腦執行速度越來越慢，因此當你發現系統無緣無故變慢時，有可能是感染電腦病毒，建議對系統執行偵毒工作。

■原本可以執行的檔案無緣無故不能執行

檔案型電腦病毒會將自己寄生在執行檔內，可能發生檔案被病毒感染後就無法執行的錯誤，所以這時不妨對系統執行偵毒工作，看看這些程式檔案是否已經中毒。

■系統常常無緣無故當機

電腦病毒感染系統是不分對象，它可能會感染 windows 系統的一些重要檔案，當系統重要檔案被感染時，windows 系統會變得非常不穩定，甚至常常當機，所以要找出當機原因，先檢查系統足否已經中毒。

■網路無端出現資料傳輸狀態/網路速度變慢

現在很多新的電腦病毒會利用網際網路散佈(如特洛依木馬程式會讓駭客從網路入侵)，當這類程式感染系統，你會發現連上網際網路時雖沒執行任何程式，但是網路連線狀態卻一百出現資料傳輸的燈號。

這時很可能你的系統已經感染電腦病毒或特洛依木馬程式，它們正在透過網路往外四處傳播。接下來若發現網路傳輸速度越來越慢，那電腦中毒的機率就非常高，請儘快對系統執行偵毒工作。

當你使用數據機撥接上網或是計時制的 ADSL 服務，連上網路會看見視窗右下角出現一個類似 的連線圖示  ，每當利用網際網路傳輸資料，這個 圖示會出現不一樣的顏色燈號  ，你可以藉此得知自己電腦是否正和外界傳遞資料。如果沒有執行接收電子郵件、瀏覽網頁、下載檔案.…等任何網路服務，卻看到燈號一直顯示妳的電腦正和外界聯繫，這時千萬要小心，有可能是駭客利用特洛依木馬竊取你電腦資料某個程式正偷偷利用網路傳輸資料，或是電腦病毒利用網路四處傳遞，請儘快執行偵毒工作。

■資料夾無緣無故多出一些重複檔案

像類似 Nimda 娜妲病毒，它曾透過區域網路或網際網路，感染有提供寫入權限的電腦，在大量感染後，會發現電腦許多資料夾下都多出一個名為「desktop.eml」的檔案。

所以哪天你打開資料夾，發現許多資料夾下都莫名奇妙多一個檔名重複的檔案，很可能病毒已經入侵你的系統，謂趕緊執行偵毒動作。

以上雖然提了幾點中毒徵兆供大家判斷，但現在電腦病毒數量如此繁多，每隻病毒入侵後徵兆都不一樣，所以除了上述中毒徵兆外，我建議你最好養成至少每個禮拜掃毒一次的習慣，這樣就算不幸感染到電腦病毒，也能及早發現、及早治療，降低災害到最小的程度。

二、如何自我偵毒

對於已經購買防毒軟體的讀者來說，自我偵毒的方法非常簡單，只要執行防毒軟體就會自動執行偵毒工作。但是對於沒安裝防毒軟體的人來說，要如何偵毒可是個大問題?講真的，目前電腦病毒數量這麼的多，總不能每隻病毒都寫個中毒特徵，然後要你按照書中描述一一去偵測吧，別說你覺得累人，就算要我收集這些資料就可能要了我老命，所以當然不可能在這裡介紹這種笨方法來偵毒囉！I

因此考量了許多沒有安裝防毒軟體的讀者，根據不同狀況，在特別介紹了三種不同方法來偵毒:

■「HouseCall 網路即時偵/解毒」: 最方便的偵毒方法，只要上網， 利用 Internet Explorer 瀏覽器就能夠偵毒。

■「建緊急開機片偵/解毒」: 若無法上網，則利用它台可上網的電腦建立緊急開機掃毒片，並用裡面的程式來偵毒。

■「透過別台電腦偵/解毒」:針對辦公室區域網路，如果有某台電腦 有安裝防毒軟體，可以透過它偵測網路其它電腦的中毒情形。

系統本身已有安裝防毒軟體的讀者，請自行參考購買軟體的使用手冊來偵毒。

建議使用「Hous eCall 網路即時偵/解毒」雖然這裡介紹了三種方法 DIY 偵毒，但建議你採用第一種「HouseCall 網路即時偵/解毒」，因為這個方法是直接使用趨勢科技的網站服務，病毒碼及病毒掃描技術一定是最新、最即時的，它們研發的木馬殺手還可以直接砍掉記憶體中的特洛依木馬程式和蠕蟲病毒，加上不用事先安裝任何程式，只要透過 Internet Explorer 瀏覽器就可以操作，真的是非常方便又有效率的一種偵毒方式。

三、使用趨勢科技 Housecall 網站即時偵/解毒

1. HouseCall 偵毒有分收費，不收費兩種

網際網路的出現真足帶給我們許多便利，它可以讓你線上看影片、線上買

電影票、線上報稅，當然也包括線上掃毒囉！為了提供許多上網族偵毒的服務，趨勢科技研發了所謂的網站偵毒技術 HouseCall，利用 Internet Explorer 瀏覽器讓你上網直接執行病毒的偵/解毒動作，不用事先安裝任何防毒軟體，不需更新病毒掃描引擎，也不怕病毒碼太舊找不到新病毒(趨勢自己網站用的病毒碼，當然一定是它們的最新版本囉)，真的是非常便利。

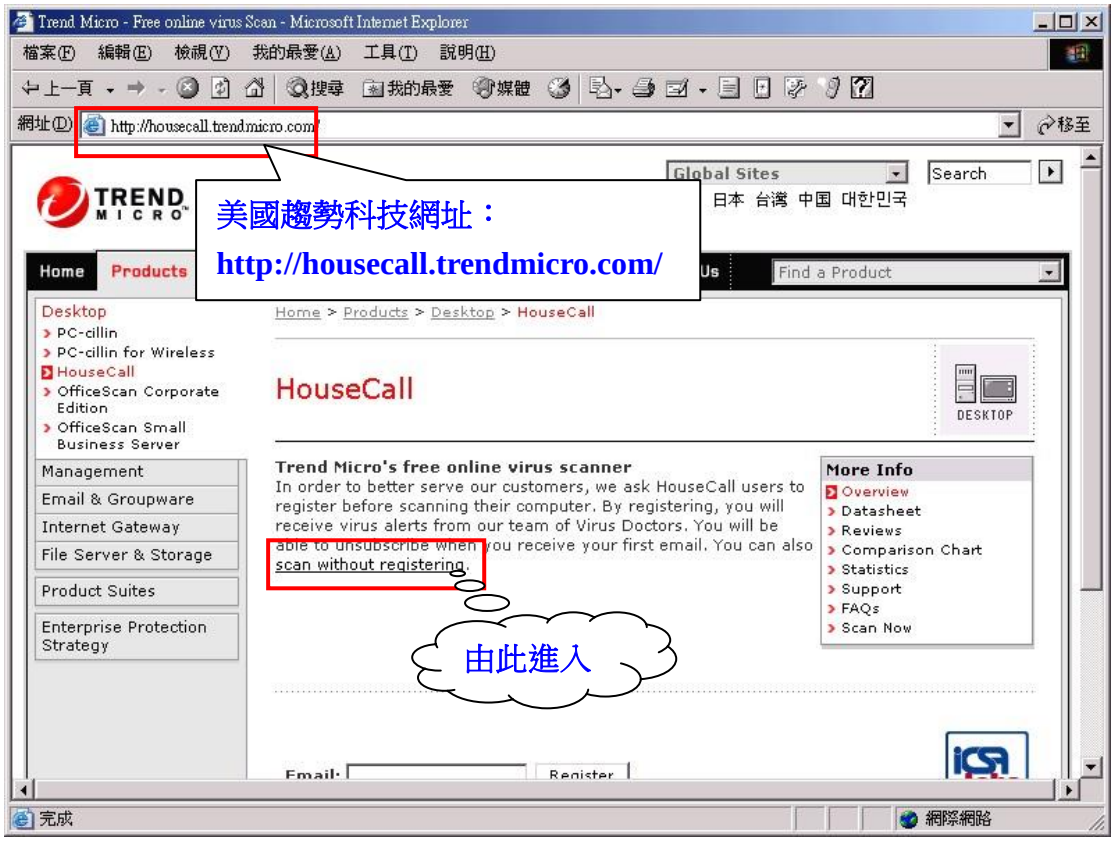
你可至以下網站查詢相關資料：

文中是以美國趨勢提供的免費 HouseCall 線上掃毒服務作為範例，但要提醒各位兩點：

口使用美國趨勢 HouseCall 線上掃毒服務不須付任何費用，但沒有任何 諮詢服務。

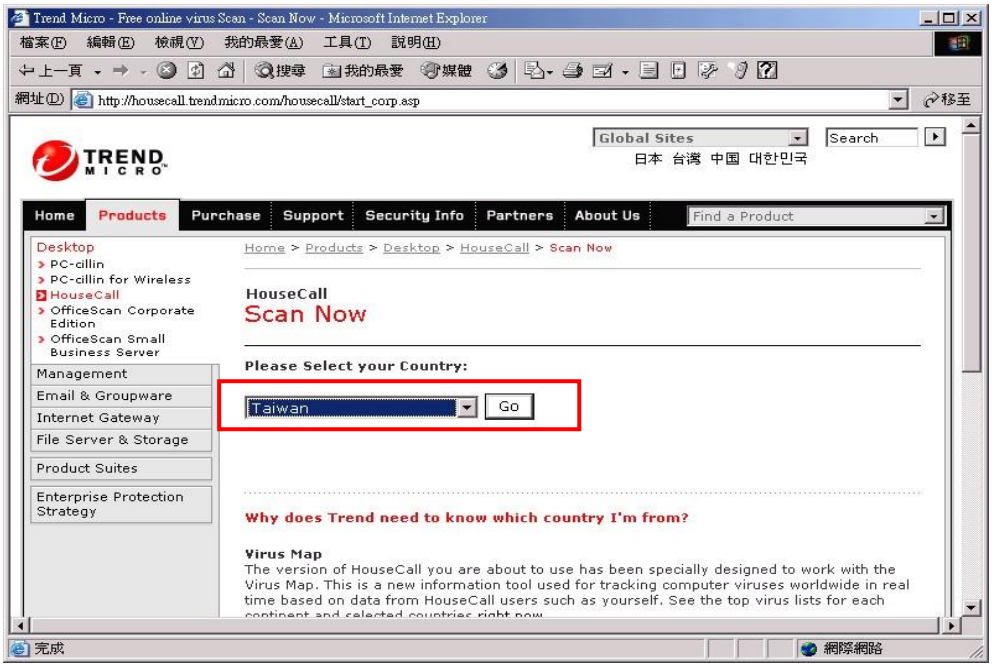
口使用台灣趨勢 HouseCall 線上掃毒服務，雖然每次掃毒要付大約 50 元 新台幣的費用，但是台灣趨勢客服中心支援諮詢服務。

各位可以針對自己的需要，選擇你要使用哪一邊提供的服務，實際執行偵毒工作時，兩邊使用 Housecall 偵毒的步驟都十分類似。



四、使用 HouseCall 即時偵/解毒服務的步驟

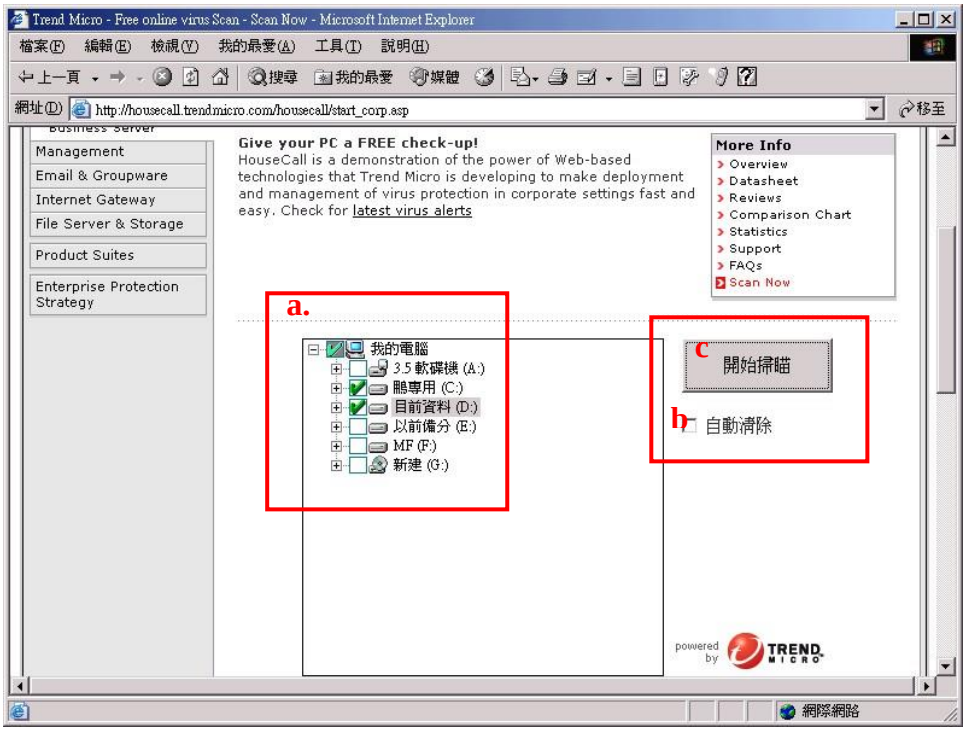
1. 首先連到美國趨勢 HouseCall 網站「**http://housecall.trendmicro.com/**」，如上圖。
2. 在「Please select your country」欄位選擇來自「Taiwan」，這樣會顯示中文訊息，請按下「Go」按鈕繼續下一步驟。如下圖



3. 螢幕會出現一個視窗，詢問是否要安裝來自「Trend Micro Incorporated」研發佈的東西，請選「是(Y)」同意安裝，這樣才可以正確使用 HouseCall 服務。

4. 接著螢幕會出現下載更新檔案的訊息視窗，請耐心等待下載。

5. 下載完畢後，會看到網頁內出現系統「我的電腦」裡面的資訊，請執行：
   a. 選擇要偵測的磁碟、資料夾。
   b. 勾選「自動清除」選項，這樣 Housecall 掃到病毒後會自動執行解毒執行解毒動作。
   c. 按下「開始掃描」按鈕執行偵毒動作。(下圖『自動清除最好打√』



6. 接下來，HouseCall 就會開始執行掃毒動作，它會針對你系統記憶體執行偵毒，如果有發現惡意軟體，螢幕可能會秀出如下圖的畫面。
7. 掃描完記憶體之後，Housecall 會對你選擇的磁碟位置作偵毒動作，接下來會顯示如圖的畫面，在「掃描結果」秀出正在掃描的檔案名稱，與哪些檔案已經被病毒感染了。


趨勢科技線上掃毒程式
你的 Internet 毒家 e 療配方
掃瞄結果： C:\Documents and Settings\ouyang1\Application
已掃瞄檔案數： 693 中毒檔案數： 0
病毒
掃瞄結果
檔案
清除病毒
刪除檔案
如需詳細的防毒資訊, 請洽 :http://www.trendmicro.com
停止掃瞄
(c)1996-2001 Trend Micro Inc. Trend HouseCall v5.50.0
掃毒引擎:6.510-1002 病毒碼:451
關閉

or


趨勢科技線上掃毒程式
你的 Internet 毒家 e 療配方
掃瞄結果： D:\下載軟體\hope\tuxbox-0.2.tar.bz2
已掃瞄檔案數： 128391 中毒檔案數： 3
病毒
掃瞄結果
檔案
TROJ_SPYKIM.A 無法清除 D:\pc active monitor\pca...
TROJ_SPYKIM.A 無法清除 D:\pc active monitor\pca...
TROJ_SPYKIM.A 無法清除 D:\pc active monitor\pca...
TROJ_SPYKIM.A 無法清除 D:\pc active monitor\pca...
清除病毒
刪除檔案
如需詳細的防毒資訊, 請洽 :http://www.trendmicro.com
停止掃瞄
(c)1996-2001 Trend Micro Inc. Trend HouseCall v5.50.0
掃毒引擎:6.510-1002 病毒碼:451
關閉