電腦病毒防護與問題排除

Agenda

1. 電腦病毒&惡意程式的種類
2. 病毒相關資訊查詢方式及清除程式介紹
3. 病毒建議清除程序及系統安全調校
4. 未知型病毒的建議檢測程序

TREND MICRO

電腦病毒&惡意程式的種類

TREND MICRO

電腦病毒(Virus)

電腦病毒(Virus)

- 一個小程式，通常4K 到10K（1K = 1024 bytes）
- 會將自己的程式依附在其它程式(寄主程式)上
- 透過寄主程式的執行，伺機將病毒程式傳出去
- 有特定潛伏期，於一定條件成立時，會進行破壞行動(如：CIH)

TREND MICRO

電腦病毒(Virus)


e want you!

找份好工作

元 績優廠商 徵才資訊

自由

陳盈豪坦承 製作

應訊供稱設計病毒是要防毒軟體公司賺錢

TREND MICRO

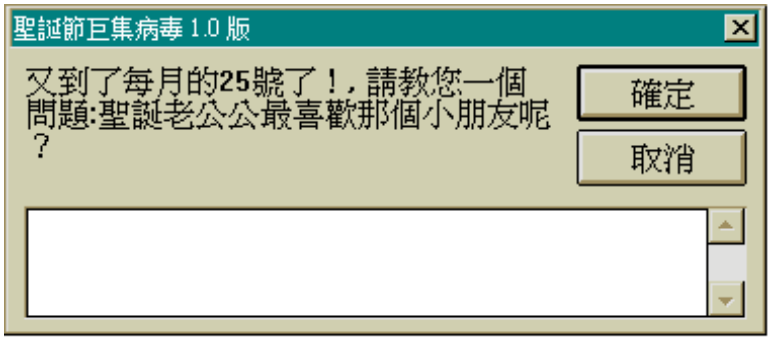
巨集病毒(Macro Virus)

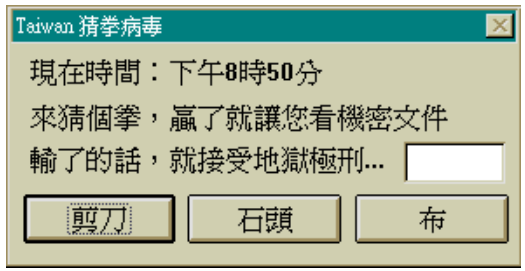
巨集病毒(Macro Virus)

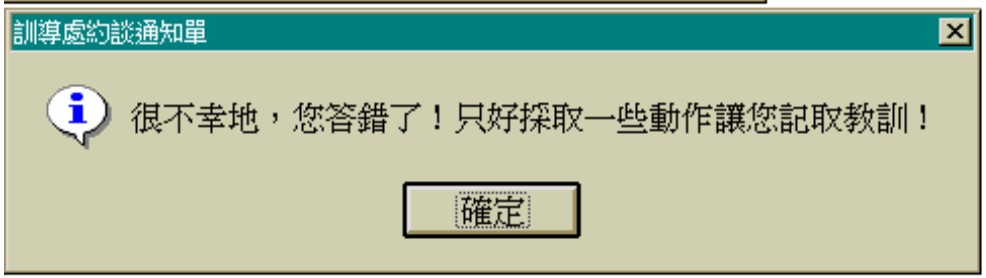
➢利用文書處理軟體內部的巨集功能，使得此文件檔可進行複製感染及破壞，此種病毒是大型且多樣化的病毒，它主要是利用軟體本身所提供的巨集能力來設計病毒， 所以凡是具有寫巨集能力的軟體都有巨集病毒存在的可能， 如Word，Excel， AmiPro都相繼傳出巨集病毒危害的事件， 在台灣最著名的例子正是Taiwan NO.1 Word巨集病毒

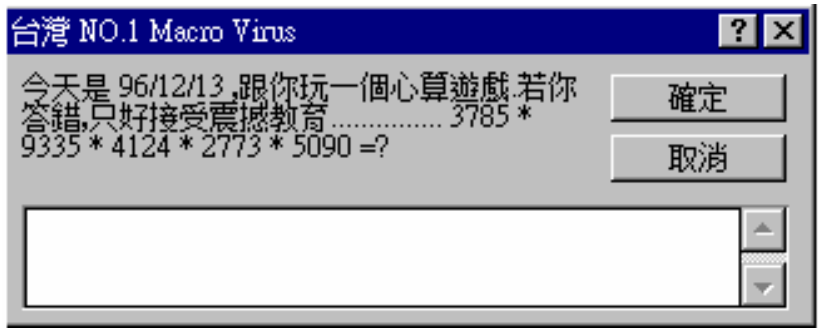
TREND MICRO

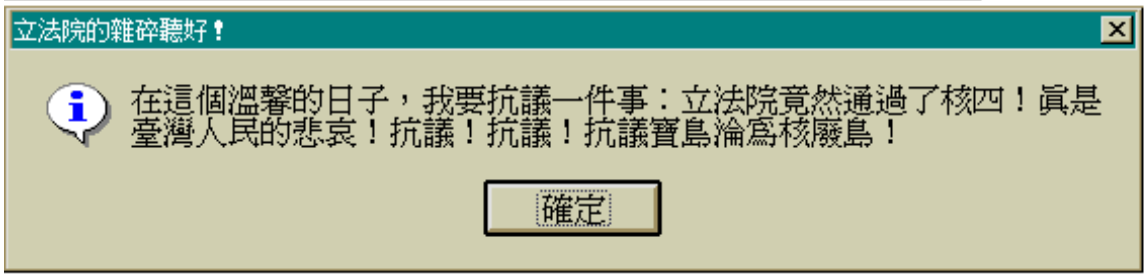
巨集病毒(Macro Virus)











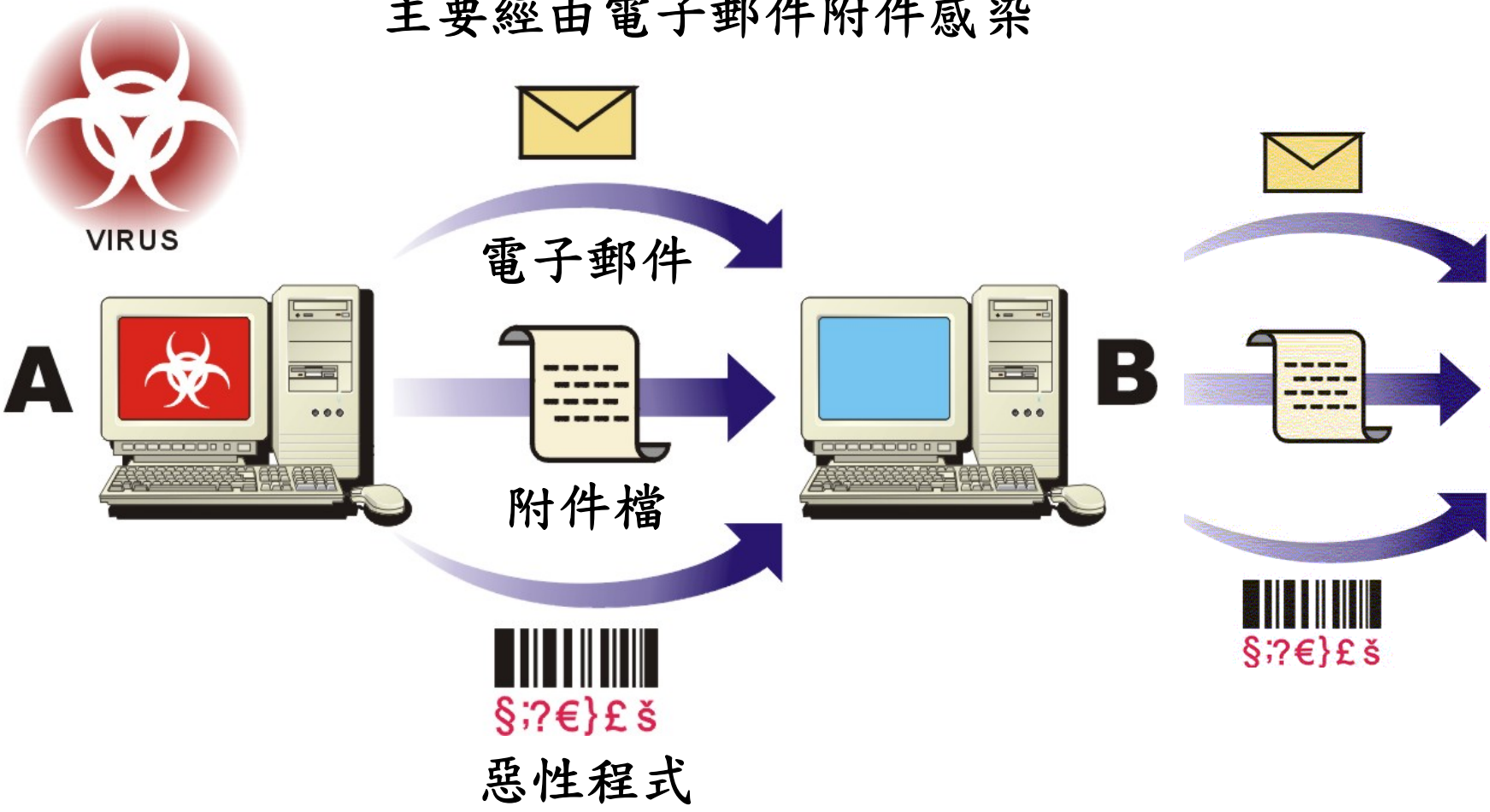
TREND MICRO

網際網路改變了病毒的定義

- 和傳統電腦病毒的觀念不同
- 不需要寄主程式...
- 利用Java / ActiveX / VB Script等技術，潛伏在網頁的HTML頁面裡面，在使用者上網瀏覽時觸發
- 可以結合傳統電腦病毒
- 跨作業平台 - Windows、Linux、Set-top Box、IA等

傳統的病毒傳播方式與行為

主要經由電子郵件附件感染



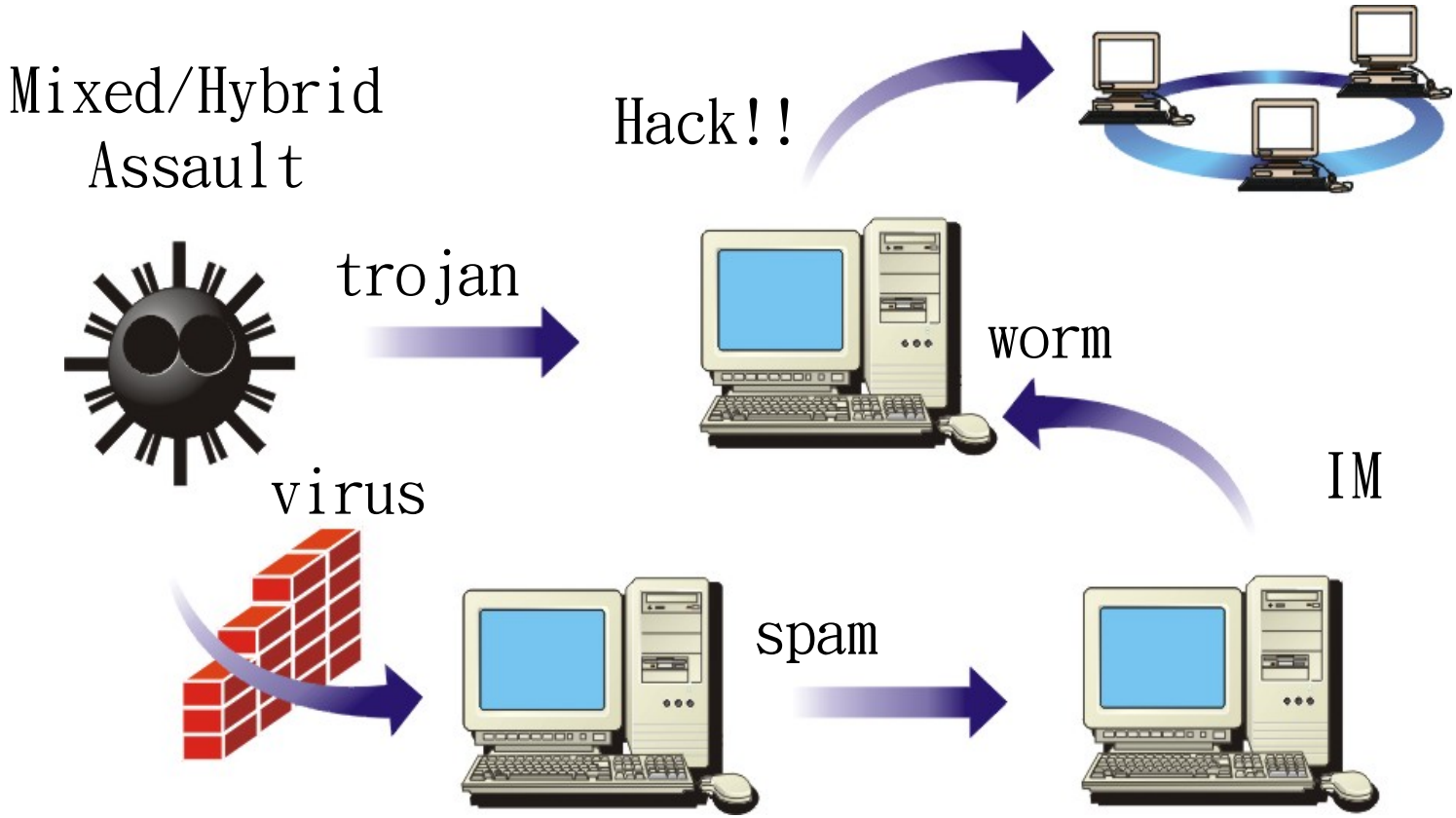
TREND MICRO

新型態病毒的傳播與感染

- 具備病毒的破壞能力
  - 常駐在記憶體
  - 難以偵測的秘密行爲
- 具備駭客的攻擊行爲
  - 阻絕服務(DoS)
  - 採用遠端控制入侵企業組織網路
- 具備郵件炸彈的傳送手法(SPAMMING)
  - 造成一傳十、十傳百的無限迴圈式感染災情

TREND MICRO

網路病毒的行為模式



TREND MICRO

新舊型病毒的侵害力比較

傳統病毒

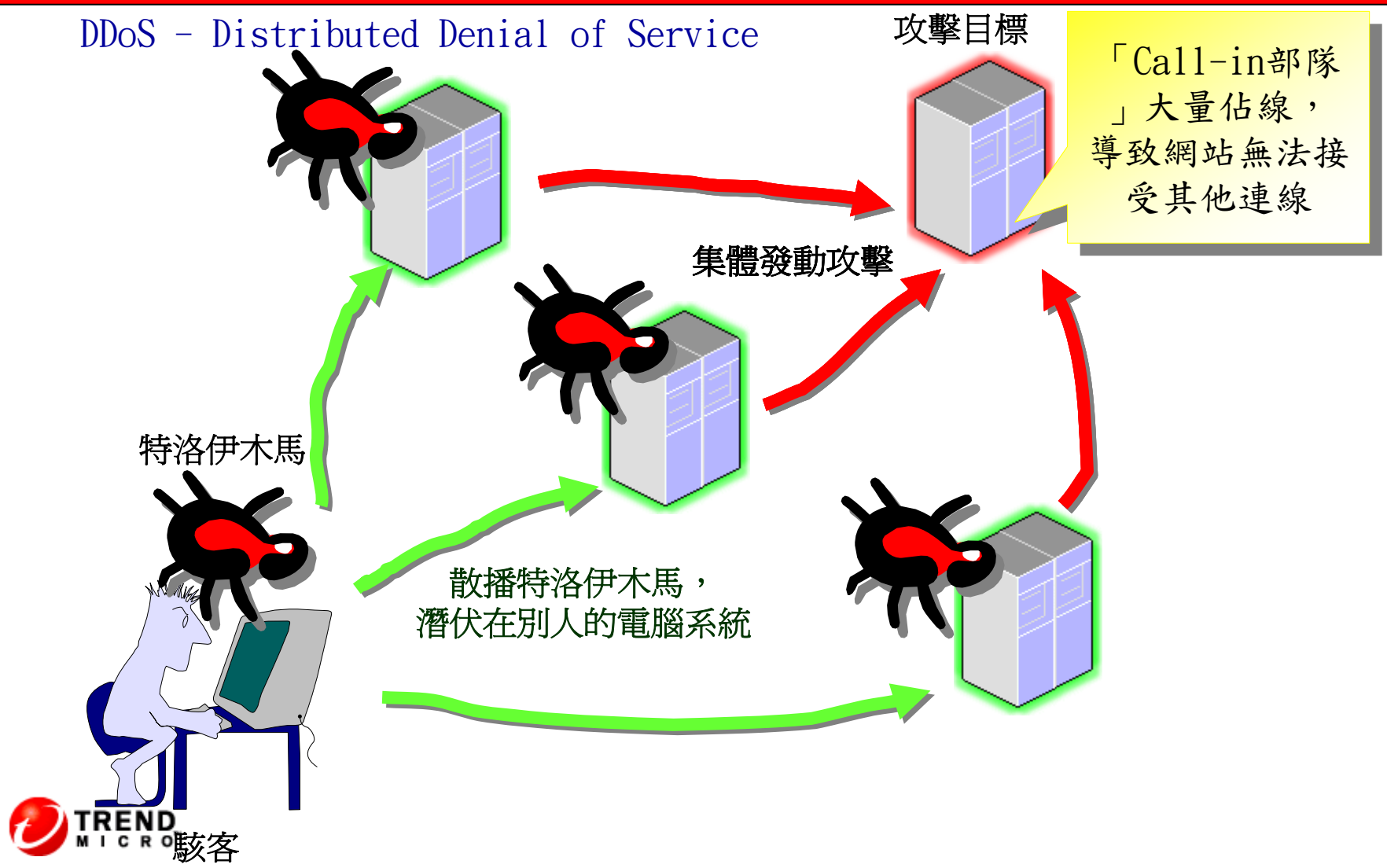
- 單一電腦毀損
- 硬碟資料損壞
- 郵件伺服器灌爆

新型態病毒

- 感染網頁伺服器
- 遠端遙控/駭客攻擊
- 整個網路停擺
- 以級數方式降低生產力

TREND MICRO

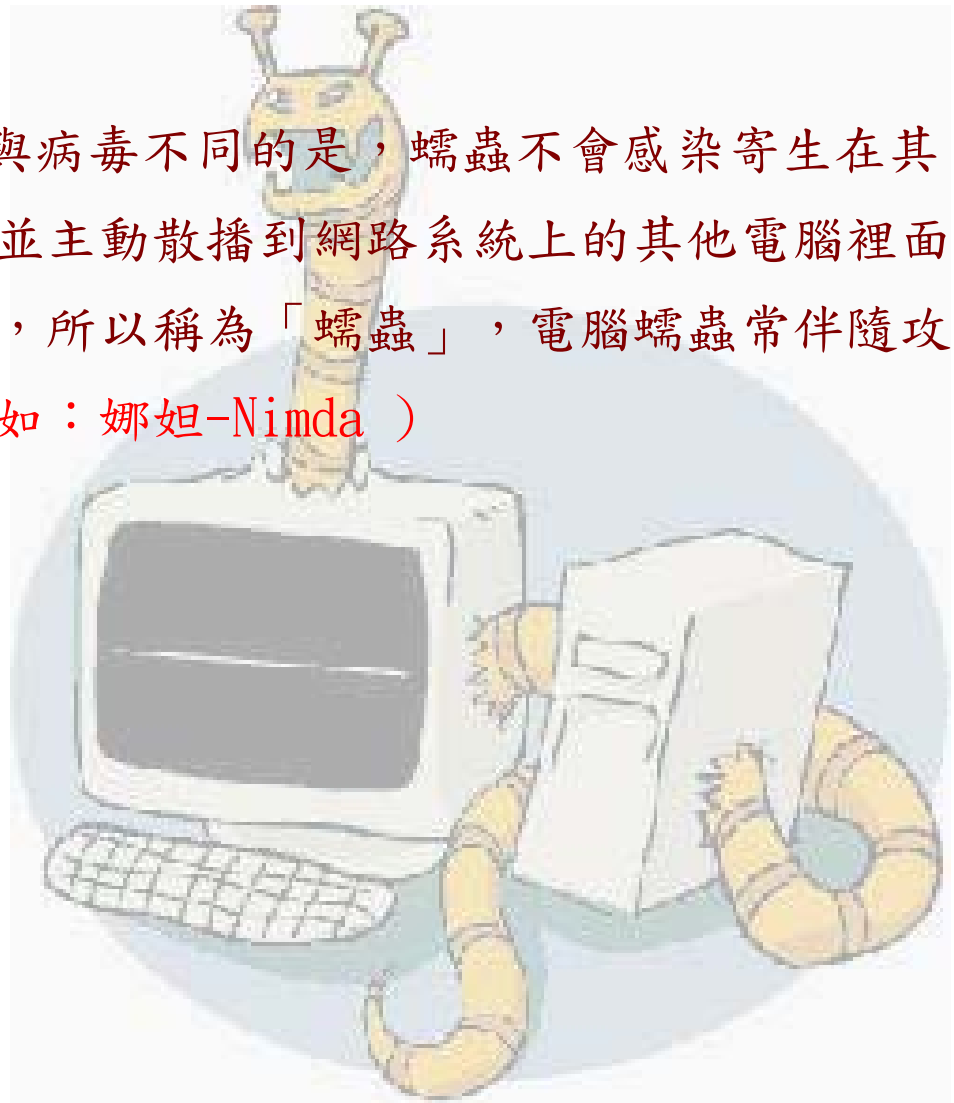
什麼是DDoS-分散式阻絕服務攻擊？



電腦蠕蟲(Worm)

電腦蠕蟲(Worm)

➢電腦蠕蟲也可說是電腦病毒的一種，與病毒不同的是，蠕蟲不會感染寄生在其他檔案。蠕蟲的主要特性是會自我複製並主動散播到網路系統上的其他電腦裡面。就像蟲一樣在網路系統裡面到處爬竄，所以稱為「蠕蟲」，電腦蠕蟲常伴隨攻擊作業系統漏洞的方式進行攻擊&散播(如：娜妲-Nimda)



TREND MICRO

電腦蠕蟲(Worm)

網 中度警訊：米塔病毒化身廣告再現身

作者：王婷儀 5/31/2005

相關報導 讀者意見

趨勢科技在5月31日針對變種米塔病毒(WORM_MYTOB.AR)發佈中度風險病毒警訊。此病毒發現至今已有超過一百隻變種現身，傳播方式及引誘網友上勾手法與之前發現的米塔病毒甚爲相同，係假藉郵件信箱管理員爲名透過outlook express通訊錄發送電子郵件，以告知網友電子帳號資訊爲藉口誘使網友點選附件而感染中毒，並會卸載電腦中的防毒軟體使得安全門戶洞開。但不同於以往發現的病毒症狀，此隻變種病毒利用微軟安全弱點(Microsoft Security Bulletin MS04-011)開起後門並植入一間諜程式(TSPY_AGENT.H)與一廣告程式(ADW_MEDTICKS.A)，透過此間諜程式將可記錄網友被感染的案例供駭客做爲日後研究病毒的參考，更甚的是會經由廣告程式的執行在電腦營幕上不斷彈跳出一廣告網站Media Tickets" (www.mediatickets.net).的視窗畫面以吸引網友點選，藉此記錄網友的上網行爲及使用習慣記錄。

趨勢科技技術總監王應達表示，除了傳統的病毒危害如開啓後門竊取資訊安全資料的行徑之外，駭客透過病毒侵襲以達到獲取商業利益的手法已越來越成熟，網友除了要提防不明電子郵

TREND MICRO

特洛伊木馬(Trojan Horse)

特洛伊木馬(Trojan Horse)

➢特洛伊木馬(或簡稱 Trojan)是一種電腦程式，偽裝成某種有用的或有趣的程式，比如螢幕保護程式、算命程式、電腦遊戲等，但是實際上卻包藏禍心，暗地裡做壞事；它可以破壞資料、騙取使用者的密碼等等。在定義上，特洛伊木馬不會自我複製，也不會主動散播到別的電腦

(如：TROJ_LINEAGE.A-天堂木馬)

TREND MICRO

特洛伊木馬(Trojan Horse)

木馬偷密碼 台

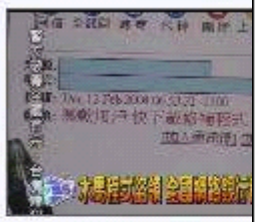
木馬偷密碼 台
國內首度出現網路
目前有台新與富邦
約定帳戶」轉帳功

木馬入侵 就像
網路族如何避免遭
式掃描電腦外，最
件，因爲僅僅可能
導致「木馬程式」

駭客功力高 追
台新及富邦銀行傳
竊取被害人網路銀
偵九隊查出，多名
罪集團勾結國內不

TREND MICRO

木馬程式盜領

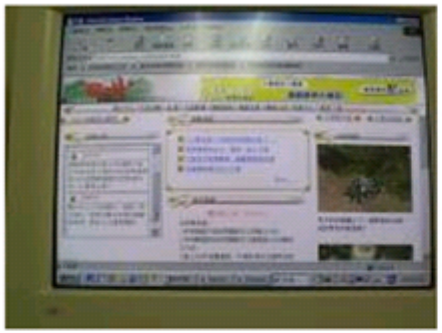


中。警方估計，全
網路安全性幾乎已

有人寄給你這麼美
微軟公司寄來的防
些信件，您的帳號
來就是要盜領你在
銀行用戶遭殃。

刑事局偵九隊長李
們估計基本上全國
取得上千筆資料，
了。」

網路遊戲「天幣」遭竊　警方追查困難 2001/6/25 14:14



記者吳慧玲／台北報導

台灣熱門網路遊戲「天堂」，日前發生玩家「天幣」、「裝備」失竊案，被害人不甘虛擬世界的損失憤而報警，難倒了現實生活的警察。台北市警局刑警大隊接獲數名被害人報案，懷疑有駭客專門找「天堂」玩家下手，偷走「天幣」、「裝備」再轉賣圖利。（記者吳慧玲／攝）

警方說，偷竊「天幣」是否構成犯罪，實務上可能仍有爭議，不過，目前警方偵辦有實際的困難，原因在於警方無法掌控所有玩家的資料，無從得知被害人的「天幣」被哪一個玩家偷走，況且，大部分玩家的資料可能是僞造的。

警方不排除是駭客所爲，研判駭客利用「天堂」熱門搶手，竊取「天幣」、「裝備」再賤賣獲利。

警方表示，被害人所說的「天堂網路遊戲」在國內的版權是由遊戲橘子數位科技股份有限公司取得，該遊戲屬於會員制的線上遊戲，提供玩家一個團隊互動遊戲的空間，玩家需先購買150元的150點或300元的300點儲值卡，取得儲值卡後，再以該儲值卡密碼進入橘子網站登錄開卡，接著自己可選用一組個人密碼和帳號來設立自己的帳戶。

手機病毒(Mobile Virus)

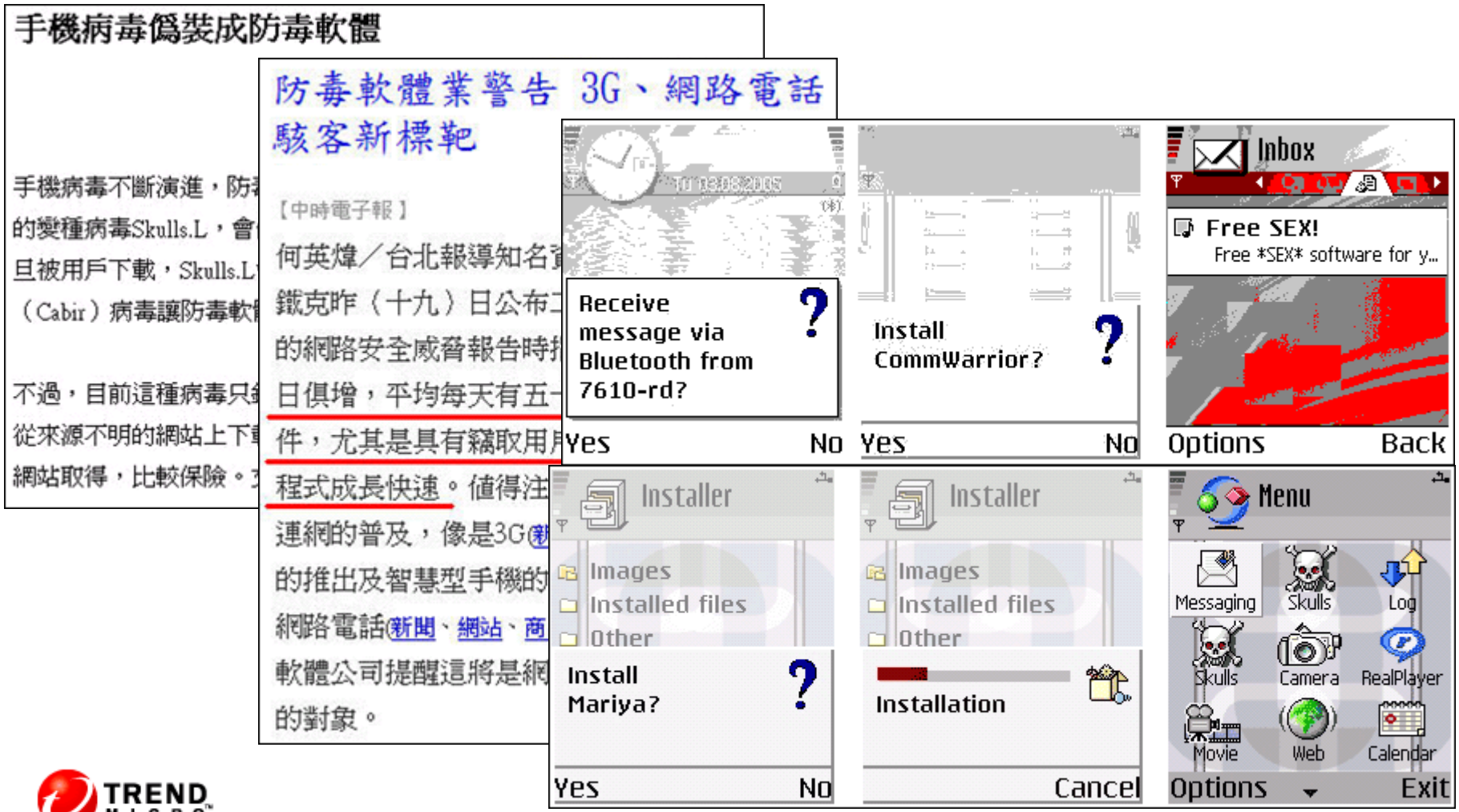
手機病毒(Mobile Virus)

➢隨著智慧型手機的連線用戶不斷增多，各防毒廠商預測病毒作者的目標很快就會轉向這些行動裝置

➢手機病毒最早出現於2004年6月，是病毒作者在智慧型手機上的概念型病毒，為的是展示他們有能力寫出Symbian作業系統的惡意程式碼。很快的，第一隻Pocket PC系統與智慧型手機病毒「Duts」出現。之後又出現幾隻手機上的木馬程式，手機病毒數目持續成長

TREND MICRO

手機病毒(Mobile Virus)

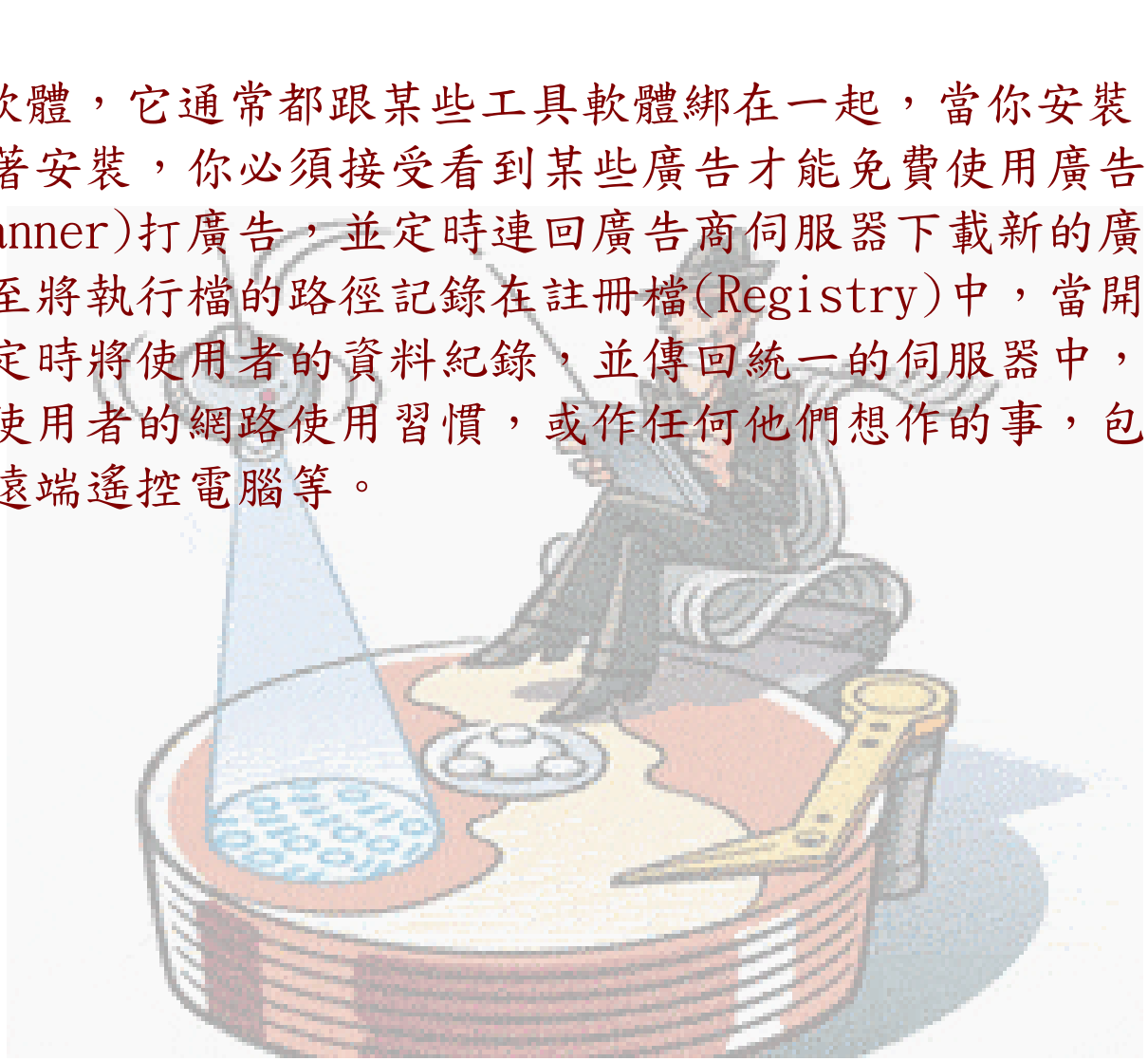


TREND MICRO

廣告軟體(Adware)

廣告軟體（Adware）

➢廣告軟體(Adware)是一種軟體，它通常都跟某些工具軟體綁在一起，當你安裝這些軟體後，廣告軟體也跟著安裝，你必須接受看到某些廣告才能免費使用廣告軟體運行時，會秀出看板(banner)打廣告，並定時連回廣告商伺服器下載新的廣告儲存在使用者的硬碟，甚至將執行檔的路徑記錄在註冊檔(Registry)中，當開機時，軟體就跟著被執行，定時將使用者的資料紀錄，並傳回統一的伺服器中，將這些資料用在分析與統計使用者的網路使用習慣，或作任何他們想作的事，包含竊取網路銀行帳號密碼、遠端遙控電腦等。



TREND MICRO

廣告軟體(Adware)

從網路下載軟體 小心 Adware

天底下沒有白吃的午餐，網路上可供免費下
但在安裝前請先搞清楚是否暗藏玄機，尤其喜
尋寶的人

Adware，儘管不會任意回傳用戶資料，但不時
令人不勝其擾，例如之前介紹過、可增加電腦
Hotbar，讓你在Email底圖加上個性化圖案或表
瀏覽器的介面花樣，但安裝Hotbar之後拖慢系
IE瀏覽器上網時會不時跳出的廣告網頁更是惱

雖然Hotbar.com網站上宣稱其絕對不是Adwar
網頁，不是詢問是否要付費升級軟體，就是推
只要有人花錢購買訂閱，研發Hotbar的公司就
維護軟體。

TREND MICRO

二月病毒 廣告軟體居榜首

【大紀元3月8日報導】(中央社記者韋樞台北八日電)資訊安全廠商Fortinet公佈二月病毒報告顯示，廣告軟體 (Adware)已逐漸成爲電腦使用者頭號網路威脅。Fortinet全球用戶偵測回報統計，二月份偵測到的網路威脅中，廣告軟體BetterInternet高居榜首佔10%，廣告軟體首次列名網路威脅排行榜首位。

Fortinet大中華區技術總監黃志輔表示，廣告軟體是一個必須持續關注的網路威脅趨勢，廣告軟體將成爲未來主要的網路威脅之一。

此外，大量郵件程式的散佈策略已逐漸演化，病毒作者改採一整個月持續小量的散佈模式，而非一次性的大量爆發。這種方式有助於增加感染主機的數量，而且可避免太多媒體的關注以及網路犯罪部門的偵查。

黃志輔指出，廣告軟體與其它蒐集網路使用者行爲的惡意程式已困擾電腦使用者多年。在不經意的情況下，瀏覽網頁或HTML的電子郵件，都有可能被自動安裝此類程式。

廣告軟體BetterInternet首次高居網路威脅榜首，反映了以往被使用者忽略，卻日益嚴重的網路威脅趨勢，電腦使用者必須對這些網路危害有所警覺。

RootKit

什麼是RootKit？

➢RootKit 有部分人士誤認為這是一套可以讓攻擊者取得特殊權限的攻擊程式，其實不然。如同他的字面意義， RootKit 指的是一套程式集，裡面包含了特洛依木馬程式、工具程式、以及可以隱藏攻擊者行蹤的程式。上面提到的工具程式指的是方便入侵者進行他想要進行的動作的程式。

➢由於是屬於程式集，因此也代表著擁有彈性。使用者可以根據自身的需要來修改 RootKit 的功能，例如：增加或刪除某些功能。甚至於當其中部分功能可能因為系統的更新，或是管理者無意間修改了其所利用的 bug，而造成無法運作的情形，只要針對該部分進行修改，即可繼續運作。也因為如此的彈性，從RootKit出現至今，技術發展非常迅速，應用越來越廣泛，偵測困難度也越來越大。

TREND MICRO

RootKit

➢目前世界上比較廣為使用的作業系統，如：*NIX、Windows NT 都有針對其所發展出來的 RootKit。而在 *NIX 系統下運作的 RootKit ，運作原理大致上都是一樣的。但是，因為其散佈方式幾乎都是透過原始碼進行，因此，改良的速度也非常的快速。而且越多使用者的 *NIX，如：Linux、SunOS，針對這兩個家族所發展出來的 RootKit 版本更是驚人。

RootKit 主要的使用目的？

➢當一位惡意使用者成功入侵目標主機，除了他的目的是癱瘓或是破壞該主機之外，否則為了安全起見，首要目標就是抹掉他入侵系統的相關紀錄，以及隱藏自身的行蹤。rootkit 的主要用途，就是提供入侵者達到上述目的。甚至於，大多數的rootkit 還提供了竊取密碼、監聽網路流量、建立後門的程式。

TREND MICRO

RootKit

- 由此看來，若一系統被植入rootkit，一般的管理者將不容易發現所管理的系統已經遭到入侵，細心一點的管理者或許能察覺出系統怪怪的，但是也不知道哪裡出了問題。但是對於入侵者而言，他卻可以輕易的控制系統，取得他想取得的資訊，而且通行無阻。

- 因此，rootkit 的主要功能，就是修改紀錄、隱藏蹤跡、竊取密碼、以及建立方便日後進出之後門。

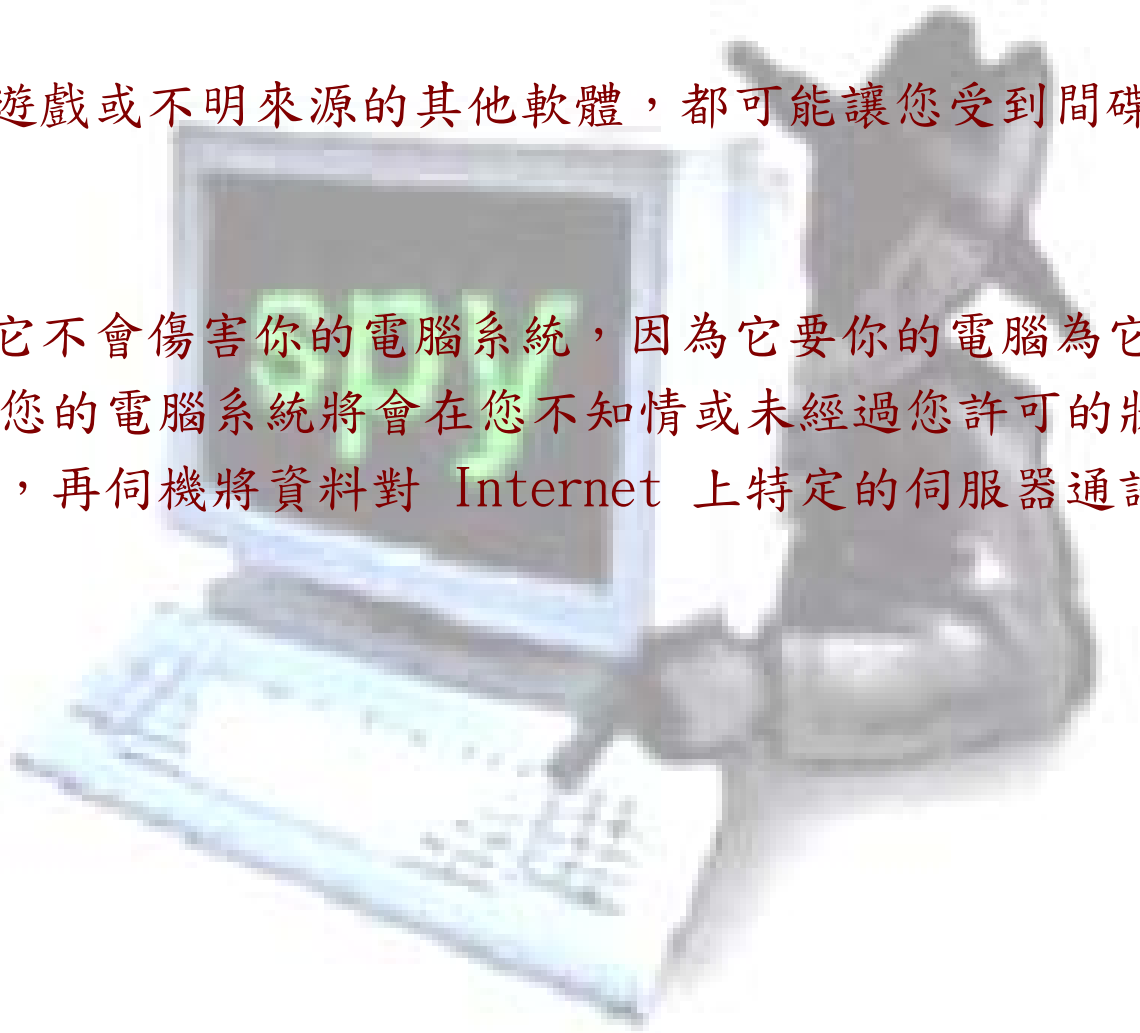
TREND MICRO

間碟軟體(SpyWare)

間碟軟體（Spyware）

➢下載未知的共享程式、免費遊戲或不明來源的其他軟體，都可能讓您受到間碟軟體的威脅。

➢間諜軟體與病毒不同之處是它不會傷害你的電腦系統，因為它要你的電腦為它所用。通常感染間諜軟體後，您的電腦系統將會在您不知情或未經過您許可的狀況下，擅自搜尋您的個人資料，再伺機將資料對 Internet 上特定的伺服器通訊並傳送。



TREND MICRO

Spyware Threat

- 什麼是間諜軟體
  - 所謂的「間諜軟體」是一個統稱，泛指會在未經使用者同意的情況下進行廣告、收集私人資訊，或修改電腦設定等行為的軟體

- 間諜軟體的特徵
  - 我不斷看到廣告視窗
  - 我的設定遭到更改，而且無法恢復原本的設定
  - 我的網頁瀏覽器出現額外的元件，但我並不記得下載過這些元件
  - 我的電腦變得反應遲緩甚至當機

TREND MICRO

Spyware Threat

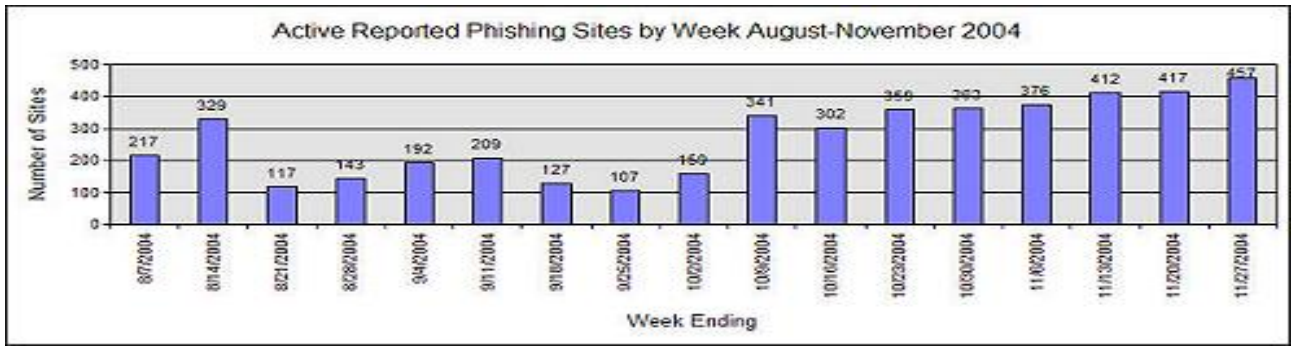
- 如何移除間諜軟體
  - 下載並安裝移除工具
  - 執行工具，掃描電腦是否含有間諜軟體和其他有害軟體
  - 檢查工具程式發現的檔案是否為間諜軟體或其他有害軟體
  - 依工具程式的指示，選取可疑的檔案進行移除
  - 移除有害軟體後，可能無法繼續使用與其一併安裝的免費軟體

  - Lavasoft Ad Aware
  - Spybot Search & Destroy (S&D)
  - Windows AntiSpyware
    Microsoft在2004 年 12 月買下購由 GIANT Company Software， Inc. 所建立的反間諜軟體技術，目前是試用版(Beta)

TREND MICRO

Spyware Threat

- 分析公司 IDC 在 2004 年 11 月所做的研究，估計大約百分之 67 的消費者 PC 都已受到某種型式的間諜軟體的感染



Phishing.org Info

- 間諜軟體可獲得利益，所以氾濫情形日益嚴重
- 並非所有的間諜軟體都有明確的違法行為
  - 使用者常常無心的同意免費軟體的 EULAs

TREND MICRO

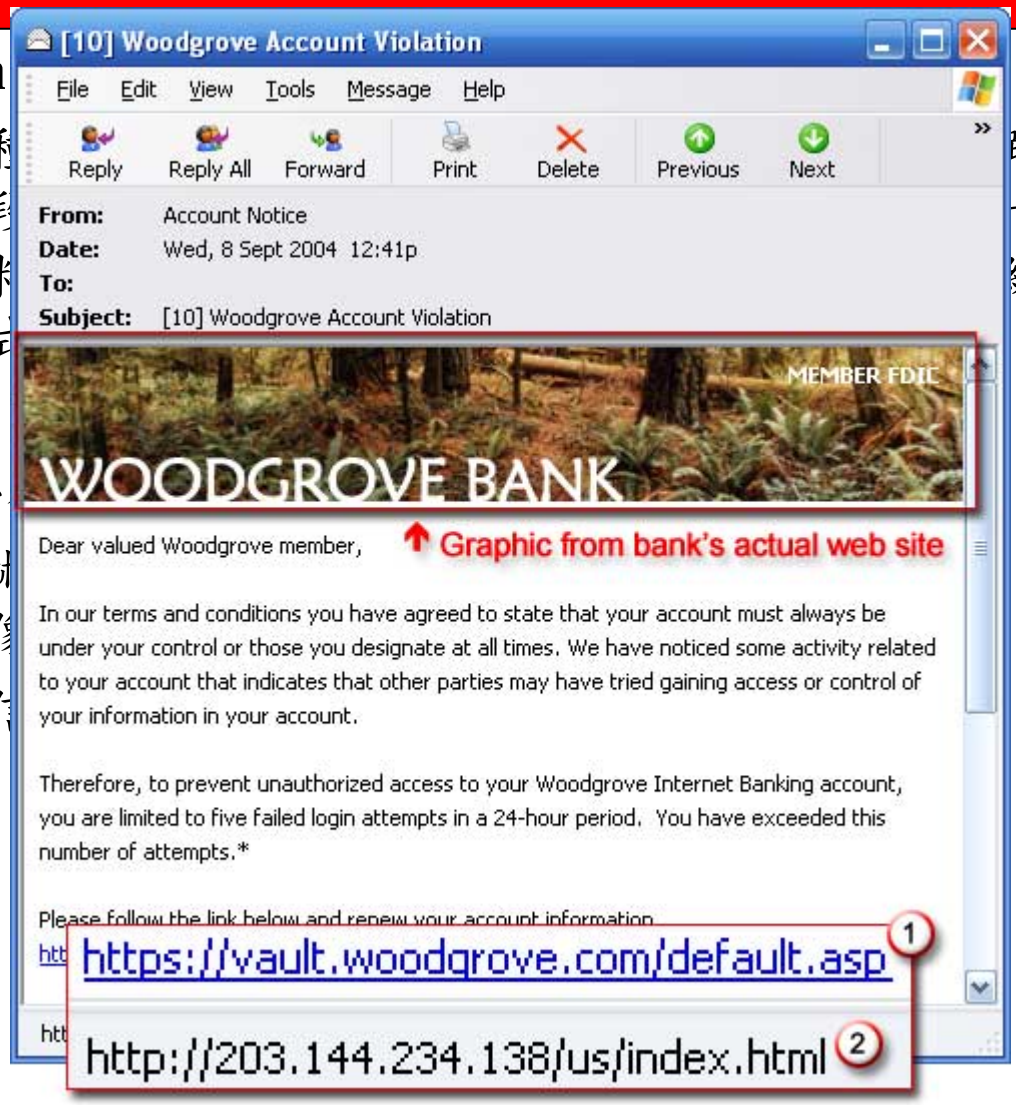
Phishing Threat

- 何謂網路釣魚（ph
  - 網路釣魚是一種
    用各種矇騙手段
    帳號或其他資料
    圾信件或彈跳式

路釣魚手法，利
卡號碼、密碼、
線上則是經由垃

- 網路釣魚詐騙的外
  - 騙子的詐騙技術
    官方網頁的圖像
  - 網路釣魚詐騙作

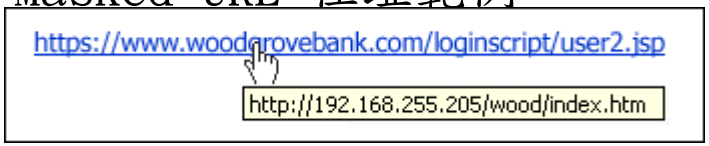
。他們通常複製



TREND MICRO

Phishing Threat

- 網路釣魚 (phishing)詐騙的電子郵件特徵
  - 確認您的帳號
  - 如果您不在 48 小時內回覆，您的帳號將被關閉
  - 親愛的重要客戶
  - 按一下以下連結來存取您的帳號
    - Masked URL 住址範例



- 對於可疑信件的應變方式
  - 檢舉可疑信件
  - 點選電子郵件中的超連結時請小心
  - 使用您個人書籤或直接在網址列上輸入網址
  - 當您在網站輸入個人或金融資料前確認安全簽章(SSL)
  - 不要在跳出視窗中輸入個人或金融資料
  - 經常檢查您的信用卡與銀行明細

TREND MICRO

駭客工具(Hacker's Tool)

駭客工具(Hacker's Tool)

- 駭客用的工具程式，樣式繁多，最近熱門的有 TFN2K、Mstream等可供有心人利用作為 DDoS - 分散式阻斷服務攻擊 的工具程式。其他還有騙取使用者密碼，以便駭客用來假冒使用者身分入侵網路或讀取/篡改機密資料等

- 任何人都可以輕易在網路上獲得或買到這種程式

駭客工具(Hacker's Tool)

刑事局查獲國內大規模駭客入侵植入木馬案

作者：編輯部 5/31/2004

刑事局偵九隊日前宣佈
首次以刑法第三十六章

由於日前發現有多家高
情形非常嚴重，經查後
及PeepBrowser.exe（檔
能使其電腦所儲存的機
檔等資料）被悉數竊取
式原始碼被公開於網路
及查殺，導致該軟體在
惡意程式仍繼續以各種

警方調查發現，王嫌程
士交換原始木馬程式檔
已知全世界少數可植入
片卡之同時，若遭植入
不堪設想。

駭客入侵 外交機密遭竊

記者李順德／台北報導 07/01 03:18

友善列印 寄給朋友 加入評論

外交部網站傳出遭駭客入侵植入木馬程式，許多機密資料遭竊取。駭客像遇綠燈般的輕鬆進入外交部。記者曾吉松／攝影

外交部電腦日前遭駭客入侵，竊取高官出訪、談判事宜等機密資料及外交文件。外交部長陳唐山獲悉後震怒，指示追查、懲處失職官員，等他四日返國後即核定懲處案。

官員懷疑，這可能是中共透過木馬程式入侵外交部電腦。

行政院資訊通訊安全會報昨天決議，未來各部會將增設「資訊安全長」，由各部會副首長兼任，專責處理、協調資安事宜。另外，開發「安全郵件」系統也列爲行政院資通的未來投資重點，以確保國家機密的安全。

主管官員透露，外交部這起事件是以駭客入侵的木馬程式，藏在電子文件及資料檔中，只要官員開啓電腦，檔案即被竊取。這次被竊取的資料具有高度機密性，外交部已展開補救，一一變更檔案，或作廢，並建置更好的防火牆。

TREND MICRO

鍵盤側錄程式(Key-logger)

鍵盤側錄程式(Key-logger)

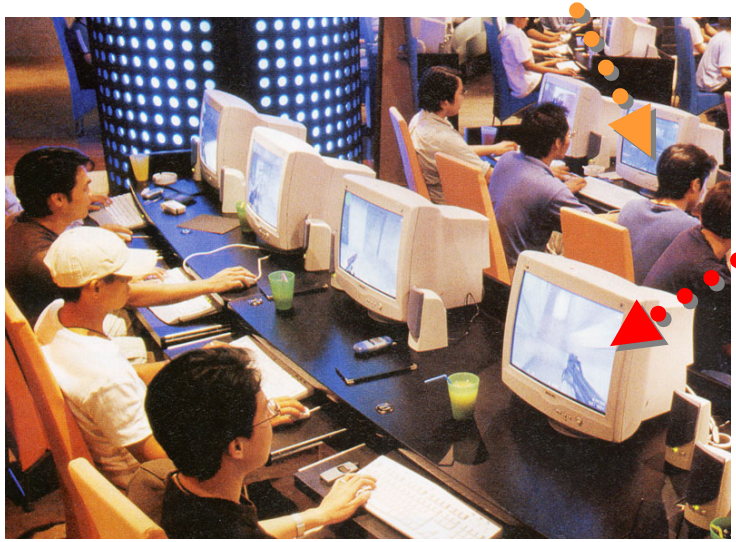
➢Key-logger程式可側錄所有自鍵盤輸入之字元，並將其存入一記錄檔(log file)之中為持續記錄鍵盤輸入，key-logger程式同一般應用程式，須載入Registry，且常駐記憶體當中執行駭客可藉由植入key-logger程式，側錄電腦使用者鍵入之網路帳號、金融密碼、甚至於個人機密文件；然後只須取得記錄檔(log file)，即可竊取各種電子資料

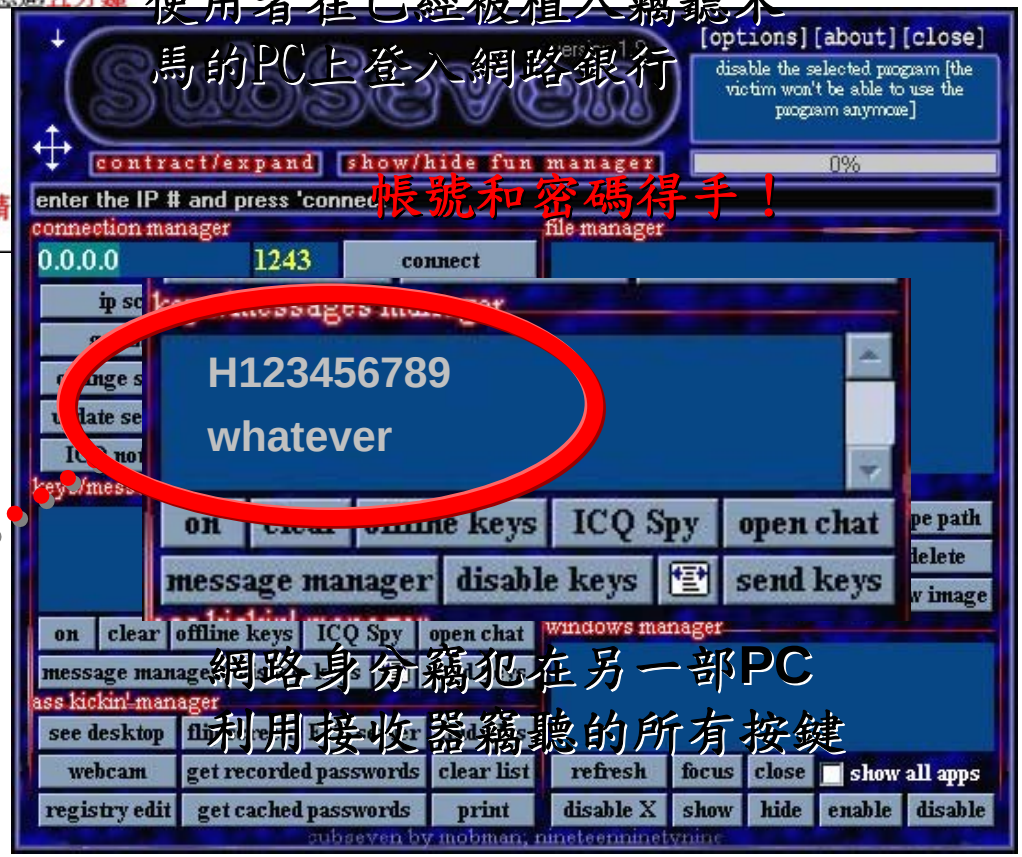
TREND MICRO

鍵盤側錄程式(Key-logger)

使用者在已經被植入竊聽木馬的PC上登入網路銀行

帳號和密碼得手！





網路身分竊犯在另一部PC利用接收器竊聽的所有按鍵

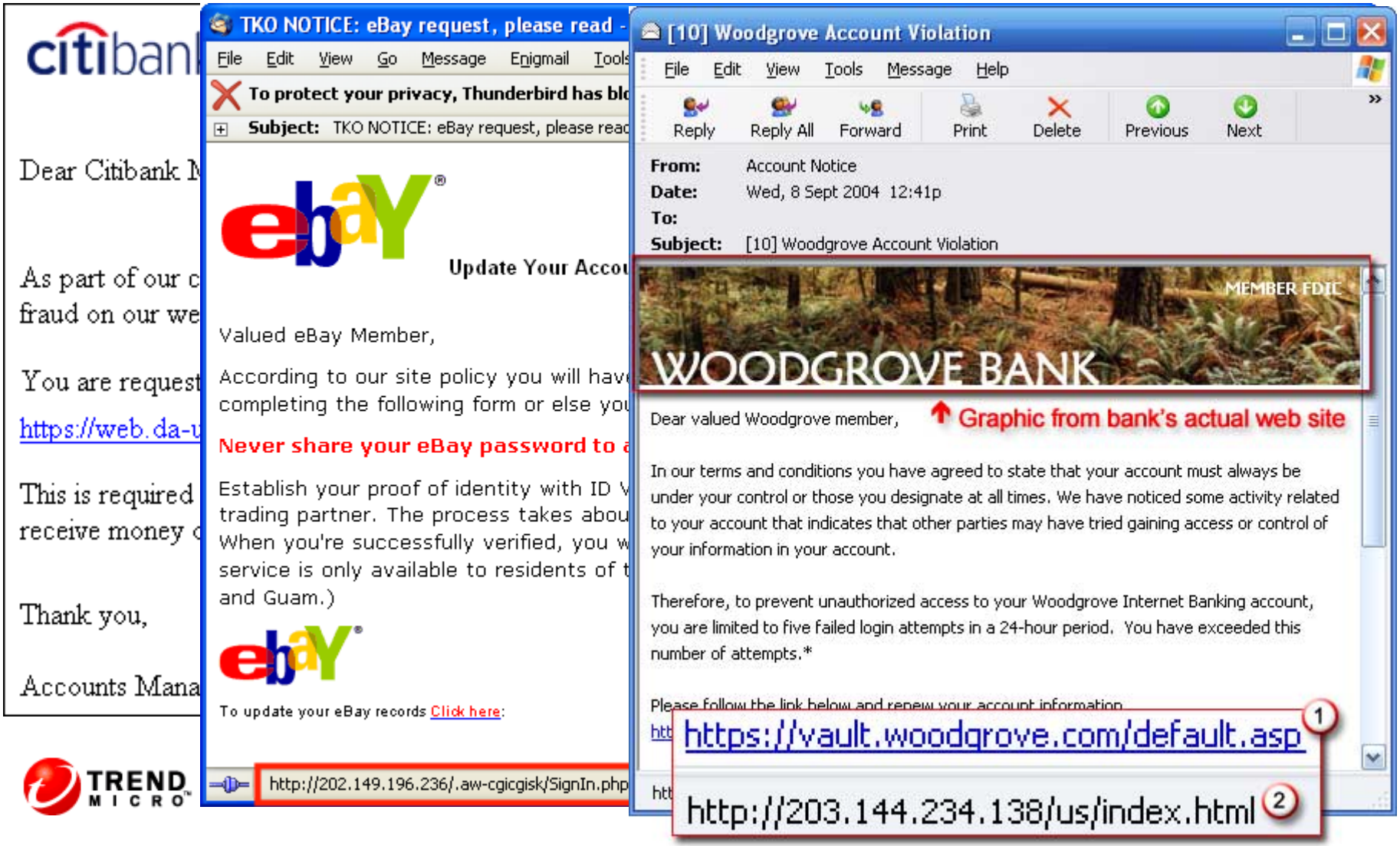
網路釣魚(Phishing)

網路釣魚（phishing）

➢phishing是以社會工程學（也就是騙術）結合電腦科技的新犯罪手法，以「願者上勾」方式騙取受害人之個人金融資料，如帳號、密碼、身分證號碼、存款或信用卡等資料。歹徒取得資料後，可使用受害人名義貸款、申用信用卡、線上轉帳、以及盜刷等違法行為，以致受害人信用破產通常詐騙的信件都會偽造自己是某知名的網站，根據統計，偽造的身分網路銀行佔81%，入口網站佔9%，線上零售商約佔10%。由此可知，大部份phishing的最終目的就是要騙取受害人的銀行存款與盜刷信用卡。

TREND MICRO

網路釣魚 (Phishing)



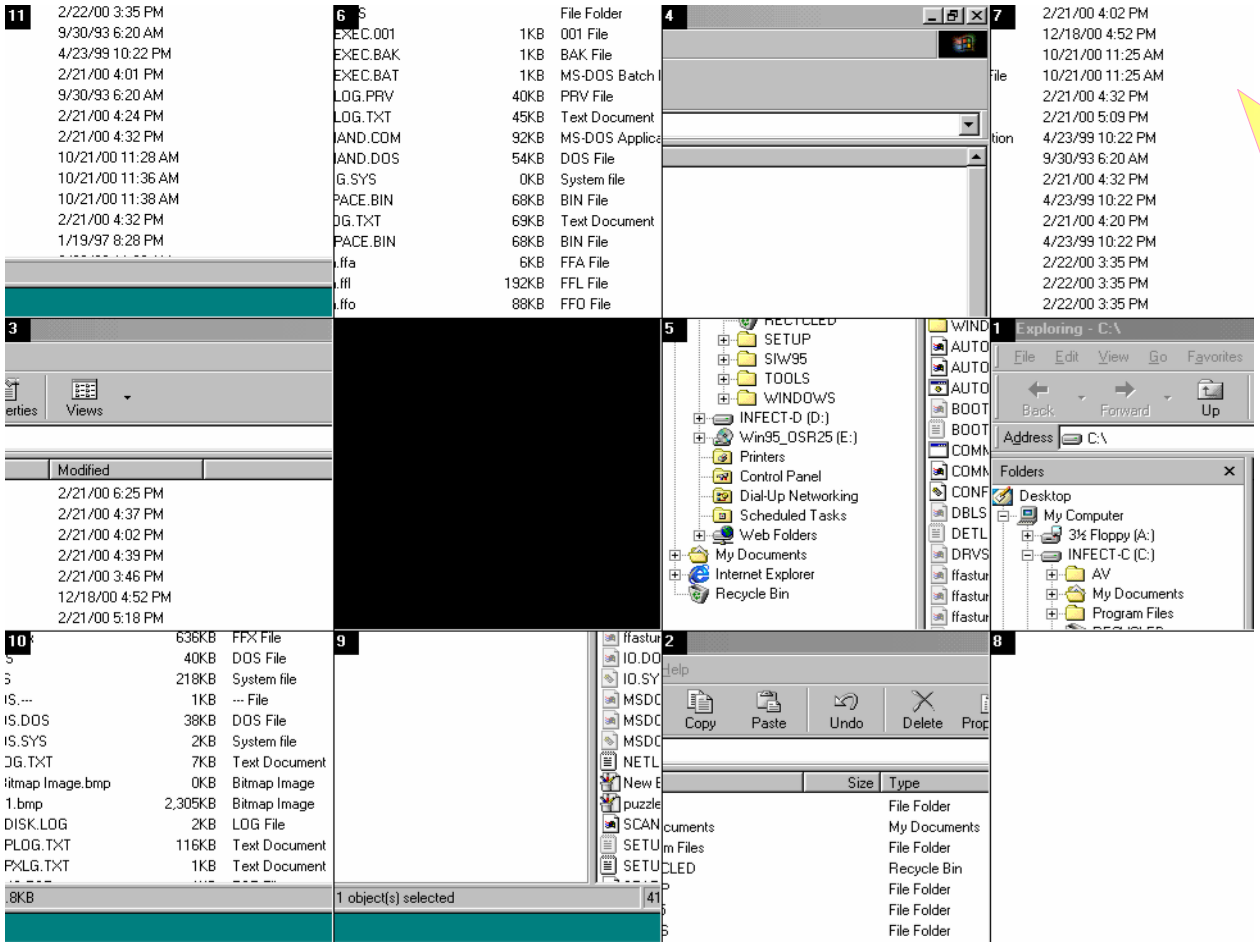
謠言/玩笑/惡作劇(Hoax)

謠言/玩笑/惡作劇(Hoax)

- 網路上一直流傳著一些電子郵件，內容是告訴你『最近發現最新電腦病毒…如果你收到主旨為…的email，請立刻把它刪除，否則你的資料通通會被刪掉！這個訊息已經由 IBM、Microsoft、CIA確認』並且鼓勵你再把這封警告訊息轉寄給你的親朋好友，事實上，這種訊息大多數都是所謂的「謠言耳語」，就像921之後，網路上充斥著各種謠言說何時又何時還會有更大的地震等等(如：Joke_Ghost 貞子病毒)

TREND MICRO

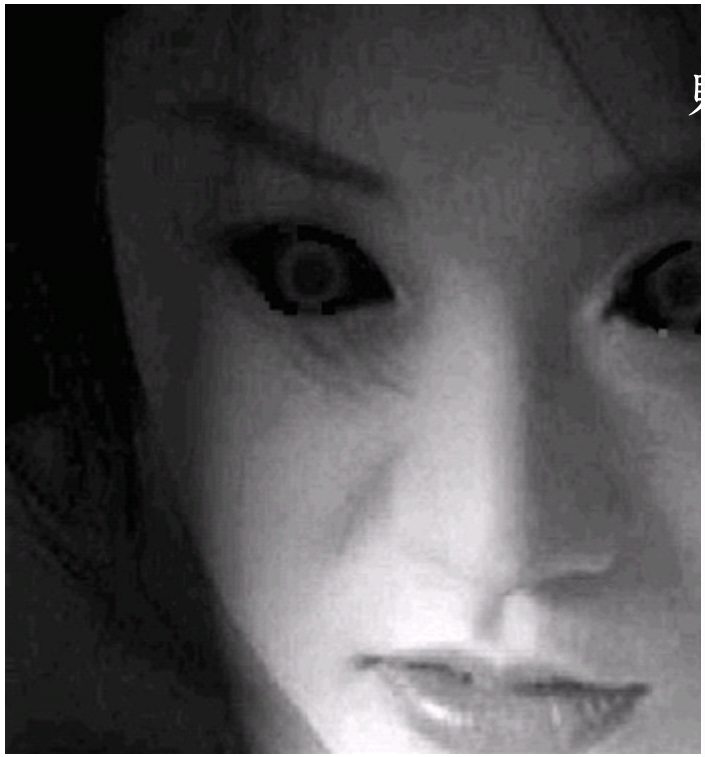
謠言/玩笑/惡作劇(Hoax)



使用者必須解完遊戲後，才能繼續操作電腦，回到原來的作業

TREND MICRO

謠言/玩笑/惡作劇(Hoax)



伴隨淒厲的
造成3名女

TREND MICRO

首頁 | 產品訊息 | 採購指南 | 技術支援 | 網路安全百科 | 經銷商專區 | 關於趨勢

病毒新訊
病毒百科查詢
惡作劇信件
全球病毒即時監控中心
病毒常識
毒害新聞
TrendLabs - R&D

首頁 > 網路安全百科 > 病毒查詢 > 惡作劇信件

惡作劇信件

查詢

- " Lets watch TV "(來看電視)
- "Economic Slow Down in US" Email Hoax
- #90 Cell Phone Warning Hoax
- 文化的也脫了
- 手機病毒
- 火車遊戲
- 水晶玫瑰
- 火燄挑戰者
- 小孩不要說髒話
- 可怕的汽球
- 可愛青蛙螢幕保護程式
- 仙蒂病毒
- 台灣土產的中文病毒
- 此網頁千萬不要去
- 江蕙-再相會或孫燕姿-風箏
- 危險網站通告！叫Smart Boy的人會四處發放病毒!!

TREND MICRO

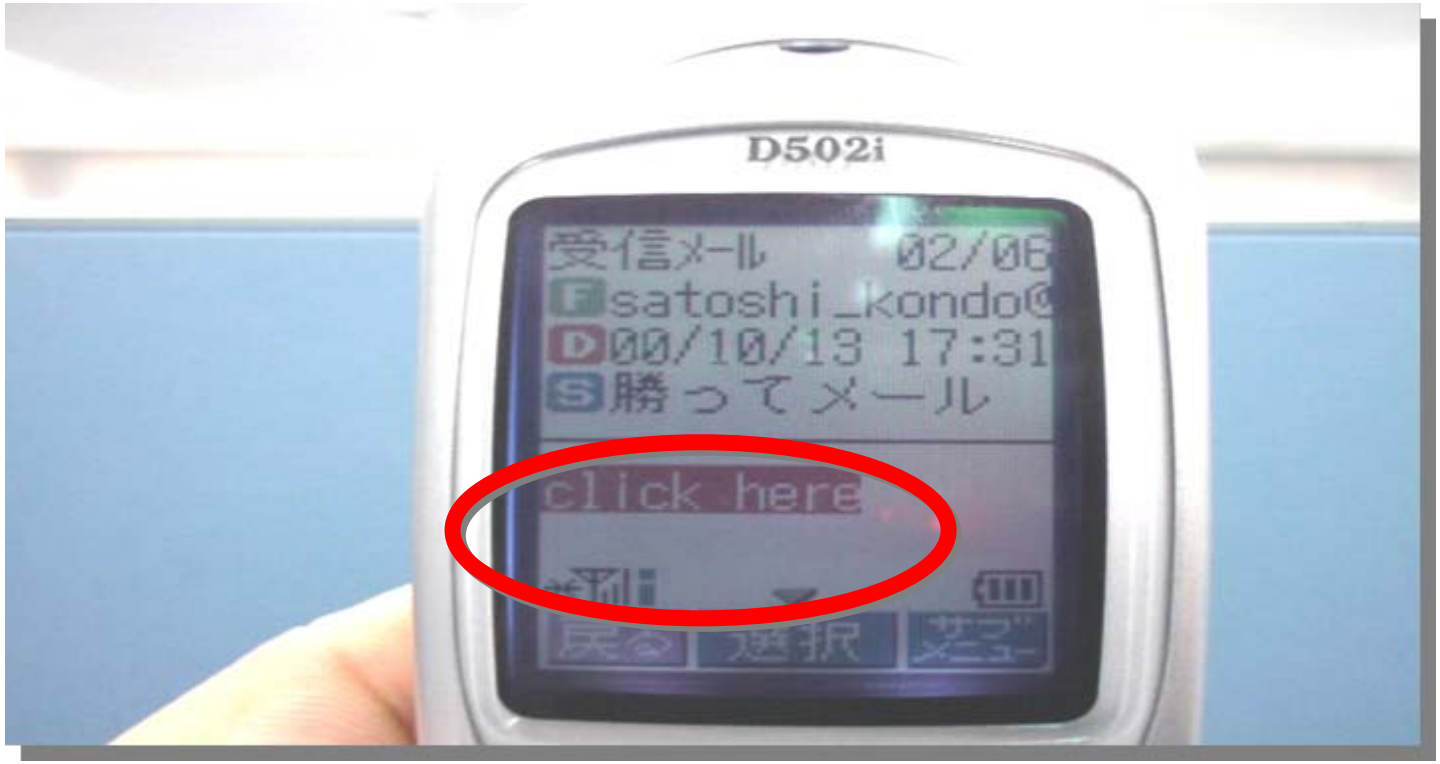
Instant Messaging

- IM 已成爲另一個病毒感染的管道
- 2005 Q1就發現 3隻此類病毒

Malware	level	date	propagation medium
WORM_BAGLE.AZ	Yellow	January 27	email, shared folders
WORM_BROPIA.F	Yellow	February 2	instant messenger
WORM_MYDOOM.BB	Yellow	February 16	email
WORM_BAGLE.BE	Yellow	March 1	email (downloaded by a Trojan)
WORM_KELVIR.B	Yellow	March 7	instant messenger
WORM_FATSO.A	Yellow	March 7	instant messenger, peer-to-peer

TREND MICRO

日本 NTT DoCoMo iMode 手機案例



iMode使用者收到病毒寄發的惡作劇郵件，不知情而按下郵件裡面的超連結後，手機會自動撥號到110緊急報案電話

TREND MICRO

殭屍病毒

- 微軟最新安全報告說，自遠端遙控的惡意軟體，仍是Windows PC最嚴重的威脅之一。
- 微軟在23日公布的「安全情報」報告中指出，2006上半年發現的殭屍病毒(zombies)新變種總計超過43，000種，可謂最活躍的惡意軟體。
- 早在6月間，微軟就把殭屍病毒列為最猖獗的Windows PC安全威脅。
- 微軟在報告中寫道：「攻擊者一心想牟利，顯然專注於開發這種惡意軟體。」

TREND MICRO

殭屍病毒(續)

- 上半年微軟發現，共有400萬台Windows PC感染某種惡意軟體，其中大約200萬台已被遠端遙控的惡意軟體入侵。微軟是透過免費下載的Windows惡意軟體移除工具蒐集到上述資料；每當使用者安裝微軟新發布的安全性更新程式，該軟體就會執行檢查，並移除所發現的惡意軟體。

- 儘管為數依然可觀，但被發現的殭屍病毒總數其實已比2005年上半年減少。去年上半年，有68%的中毒PC被植入後門木馬程式(Trojan)。

- 此外，駭客現在更大費工夫，企圖用最新的、以全球資訊網為據點的手法，讓被綁架的電腦在不被察覺的情況下運作。

TREND MICRO

殭屍病毒(續)

- 被這種木馬程式綁架的電腦，通常稱為「殭屍電腦」(zombie PC)，可能被網路惡徒用來組成「殭屍網路」(network of bots；botnet)，大量傳發垃圾郵件(spam)和發動網路攻擊。駭客通常也會竊取受害者的個人資料，並在電腦上安裝間諜程式與廣告軟體，藉此向間諜程式或廣告軟體業者收取回扣。

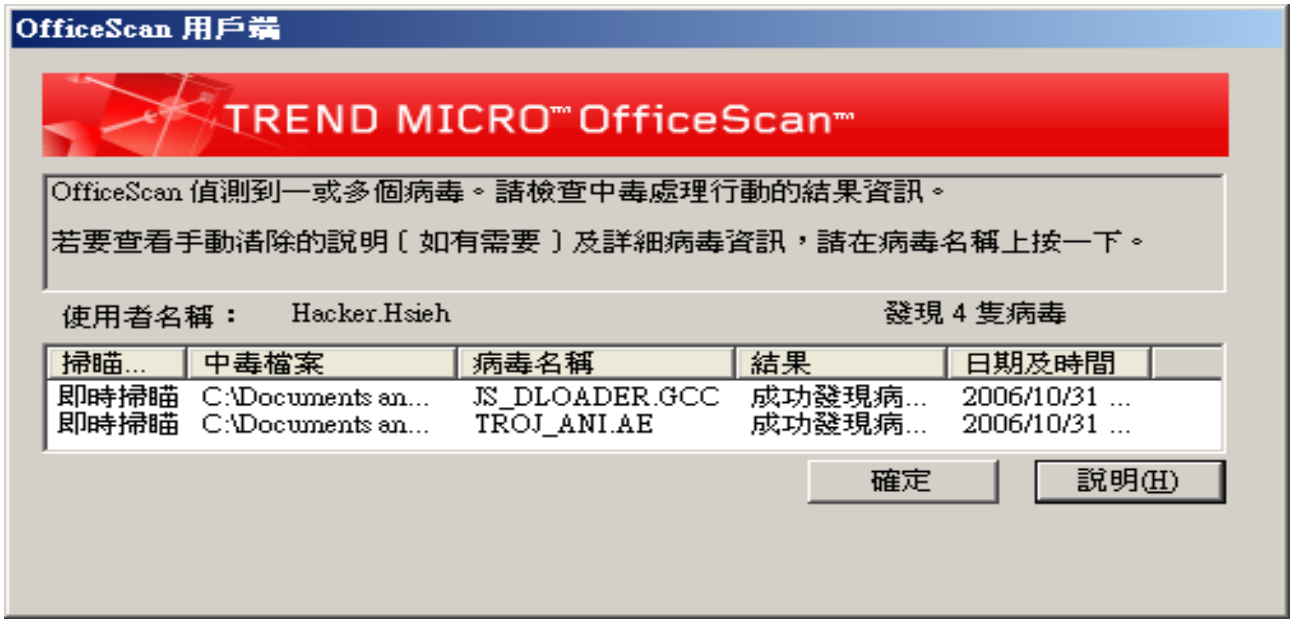
- 另一種常見的威脅則是RootKits，這種軟體擅自修改系統設定，以便窩藏另一種可能不懷好意的軟體。微軟說，今年上半年RootKits攻擊Windows PC的案例已降低50%。

- 微軟自去年1月起定期發布Windows惡意軟體移除工具，每月隨安全公告釋出最新版程式。這個工具的用意是辨認並移除PC上偵測到的常見惡意軟體。

TREND MICRO

殭屍病毒(續)

- 目前已知上述網站含有來自俄羅斯專偷機密資料的木馬，此木馬還會到其它網站下載含有惡意程式的改造圖檔（.jpg），而每一隻下載的病毒又會各自去其他網站下載多隻間諜軟體、木馬等等。一旦系統遭受感染，駭客將取得系統控制權，展開資料竊取、竄改等隱形攻擊 。



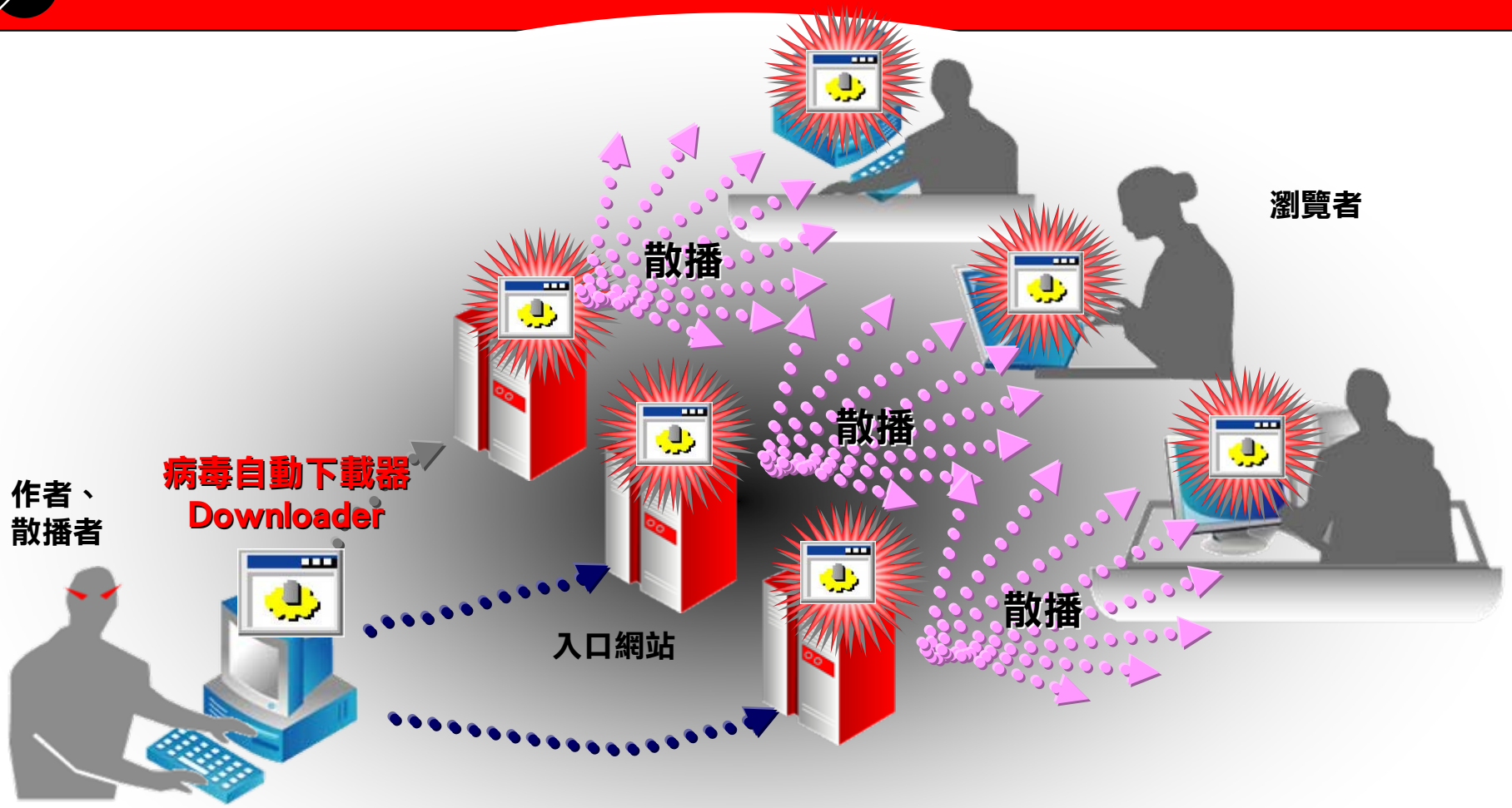
殭屍病毒(續)

- 目前駭客常假造熱門話題頁面(如相片分享網站)，然後將病毒自動下載器(downloader)放置其中，藉由討論區或是 MSN、電子郵件等傳播惡意連結。甚至入侵高知名度官方網站，將網站中的某些圖檔背後悄悄放置病毒自動下載器，一旦瀏覽這些網頁，各式各樣的病毒、惡意程式、間諜軟體就會隨時更新病毒變種到受害電腦中。

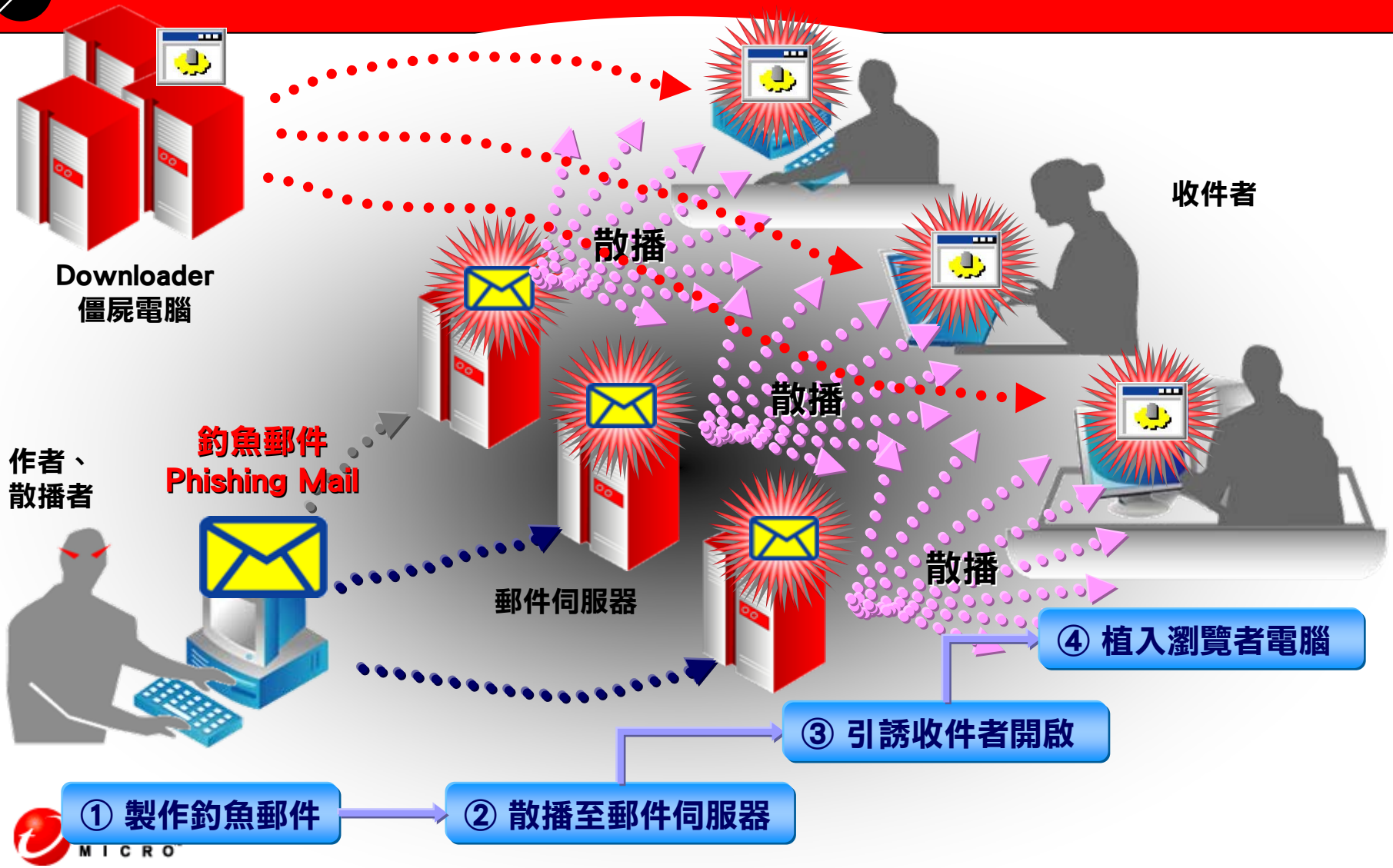
- 變種病毒幾乎每小時都在產生，要及時推出病毒碼更新有困難；而且此類攻擊手法嘗試使用不同的檔案壓縮機制 /加密演算法，以躲避病毒過濾功能。要有效遏止變種病毒透過電子郵件或網頁進入企業網路中，企業應使用如IMSA、IWSA搭配新型的智慧型技術來偵測壓縮檔案，並透過威脅偵測功能來預防未知的威脅。

TREND MICRO

藉由知名網站散播病毒自動下載器



藉由釣魚郵件手法散播病毒自動下載器



病毒相關資訊查詢方式及清除程式介紹

TREND MICRO

病毒資訊查詢方式

- Trend網路安全百科

http://www.trendmicro.com/vinfo/zh-tw/

- 行政院國家資通安全會報技術服務中心

http://www.icst.org.tw/

- 微軟資訊安全網站

http://www.microsoft.com/taiwan/security

- Google萬能資料庫

http://www.google.com

TREND MICRO

Trend Micro網路安全百科

安全資訊

沒有惡意程式警訊
目前沒有中度或高度病毒警訊.

最近的更新
Virus Pattern File 3.473.00 Jun 1
掃描引擎 8.000
› 瀏覽下載中心

惡意程式公告 | 最嚴重的威脅 | 安全性通報

Search Security Info

間諜程式/灰色程式(Grayware)	風險程度	公告日期	病毒碼
TSPY_SINOWAL.BR	Low	May 30, 2006	Scan Pattern: 3.462.01
ADW_WINFIXER.Y	Low	May 24, 2006	Scan Pattern: 372.01
TSPY_POKERFAKE.A	Low	May 17, 2006	Scan Pattern: 3.434.04
TSPY_BANKER.BDD	Low	May 10, 2006	Scan Pattern: 3.416.02
TSPY_LDPINCH.AP	Low	May 5, 2006	Scan Pattern: 3.408.03

TREND MICRO

國家資通安全會報技術服務中心

病毒防護

- 2006-05-29 大量散播郵件的蠕蟲病毒-W32.Areses.F@mm
- 2006-05-29 掩蔽掉與安全相關的視窗的W32.Amirecivel網路蠕蟲
- 2006-05-29 會打開後門和降低電腦安全性的蠕蟲病毒-W32.Mytob.PO@mm
- 2006-05-29 會自動分裂爲多個檔案的W32.Kittyka病毒

漏洞修補

- 2006-05-30 IBM WebSphere伺服器存在可繞過Welcome Page 安全限制之弱點
- 2006-05-30 Mozilla Firefox處理 Deleted Object Reference的 iframe.contentWindow.focus函式有弱點
- 2006-05-30 Macromedia Flash Player具有多項原因不明的安全弱點
- 2006-05-30 Linux核心的USB子系統有阻斷服務的弱點

微軟資安

- 2006-05-11 Microsoft 發布MS06-019安全公告-Microsoft Exchange 中的弱點可能會允許遠端執行程式碼。 威脅等級: 重大
- 2006-05-11 Microsoft 發布MS06-018安全性公告-Microsoft Distributed Transaction Coordinator 的弱點可能會造成拒絕服務。
- 2006-05-11 Microsoft 發布MS06-020安全性公告-Adobe 的 Macromedia Flash Player 中存在的弱點可能會允許遠端執行程式碼。 威脅等級: 重大
- 2006-04-12 Microsoft 安全性公告(MS06-013):Internet Explorer 積存安全性更新。

TREND MICRO

微軟資訊安全

最新資訊安全補充程式

取得最新的軟體補充程式資訊。

- 2006 年 5 月份 Microsoft Windows 和 Exchange 安全性重大更新 New!
- 惡意軟體移除工具 New!
- Microsoft 安全性摘要報告 (916208)：Adobe 安全性公告：APSB06-03 Flash Player 更新可解決安全性弱點 New!
- 您必須知道的 Zotob 消息
- 測驗：保護個人電腦基本知識
- 測驗：間諜軟體基本知識

更多資訊安全更新...

最近發生的事件

瞭解如何協助保護您的電腦免於病毒、駭客和其他安全性問題的侵害。

- ISA Server 2006 新功能一日體驗 New!
- Microsoft 安全性 - 進展更新 New!
- 防範安全性公告 MS05-009 相關的破解程式碼 New!
- Microsoft ASP.NET 通報弱點須知
- 最新病毒通知：Mydoom 蠕蟲 (2004/8/2 更新)

TREND MICRO

Google萬能資料庫

TREND MICRO

病毒清除工具Damage Cleanup

- Trend Damage Cleanup Engine / Template

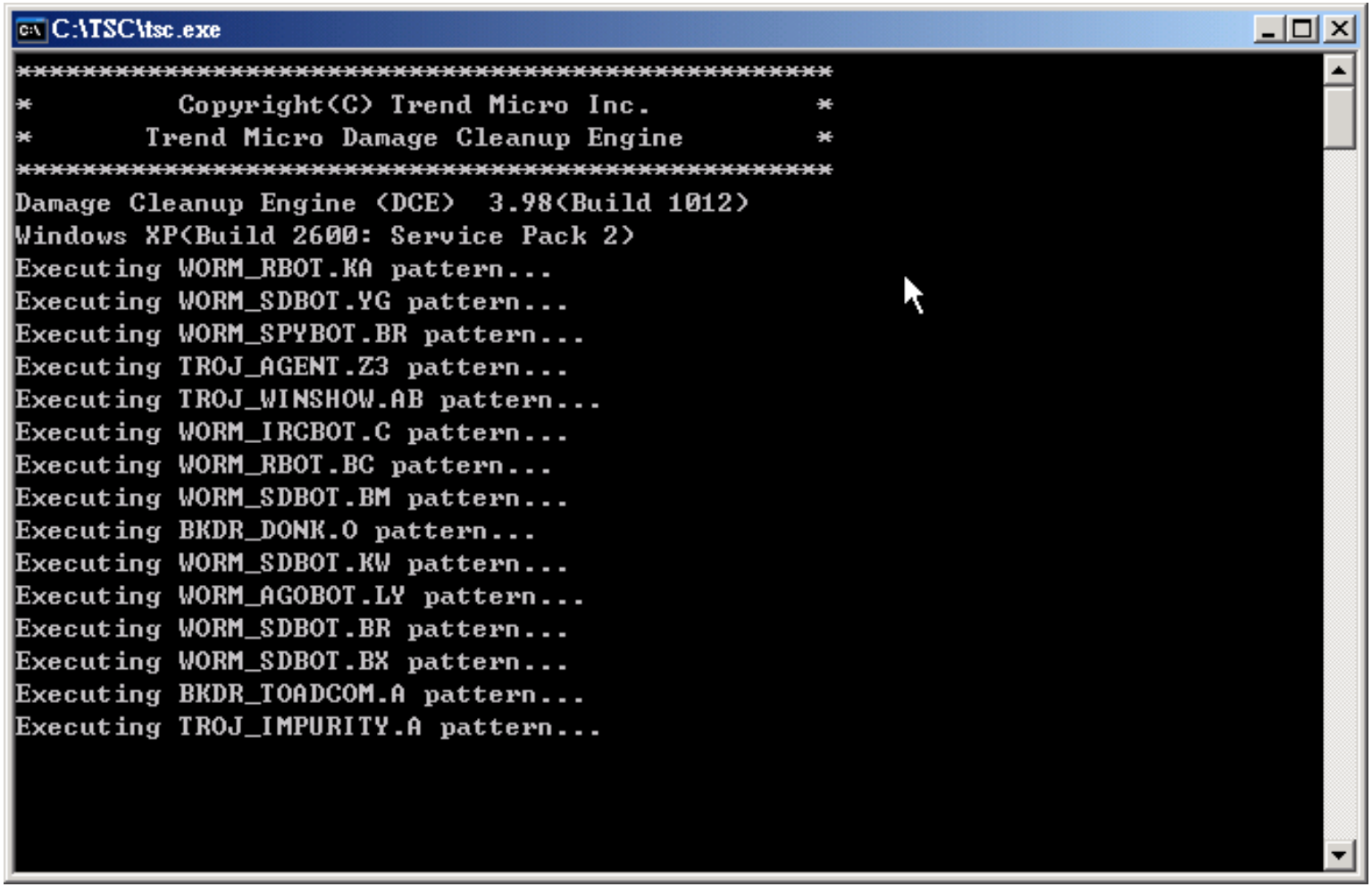
http://www.trendmicro.com/ftp/products/tsc/tsc.zip

Trend Damage Cleanup功能如下：

- 結束所有記憶體裡惡意程式的執行
- 從registry entries裡移除惡意程式
- 從系統檔裡移除惡意程式

TREND MICRO

病毒清除工具Damage Cleanup



TREND MICRO

病毒清除工具System Clean

- Trend System Clean

http://www.trendmicro.com/ftp/products/tsc/sysclean.com

- Sysclean功能如下:

  結束所有記憶體裡惡意程式的執行

  從registry entries裡移除惡意程式

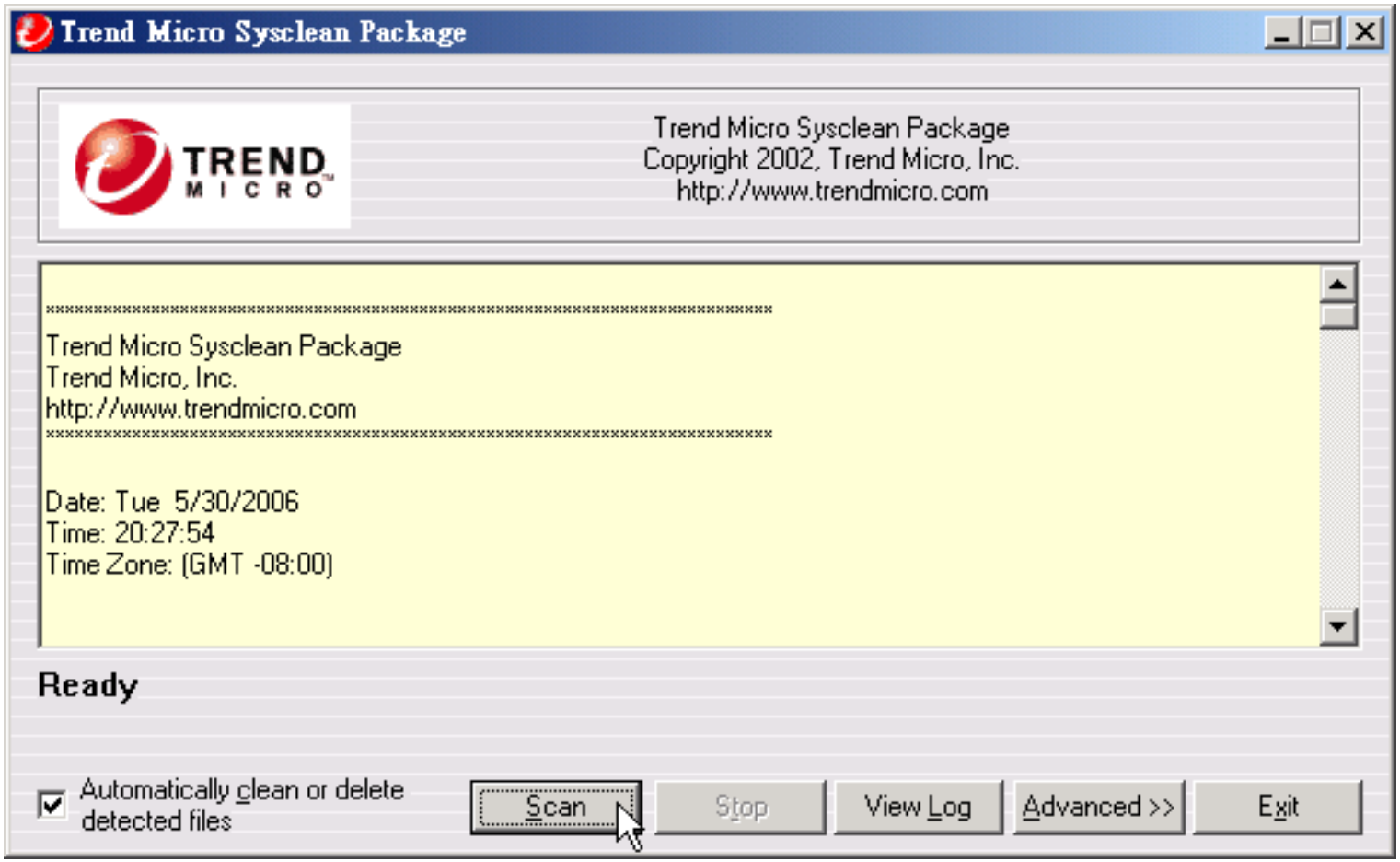
  從系統檔裡移除惡意程式

  掃描並刪除所有硬碟裡的惡意程式

- 要使用Sysclean，客戶必須在執行掃毒工具前下載最新的病毒碼版本(lpt$vpn.xxx)

TREND MICRO

病毒清除工具System Clean



TREND MICRO

HouseCall線上掃毒

- Trend HouseCall線上掃毒

  http://housecall65.trendmicro.com/

- Sysclean功能如下:

  掃毒、反間諜、弱點檢查三效合一

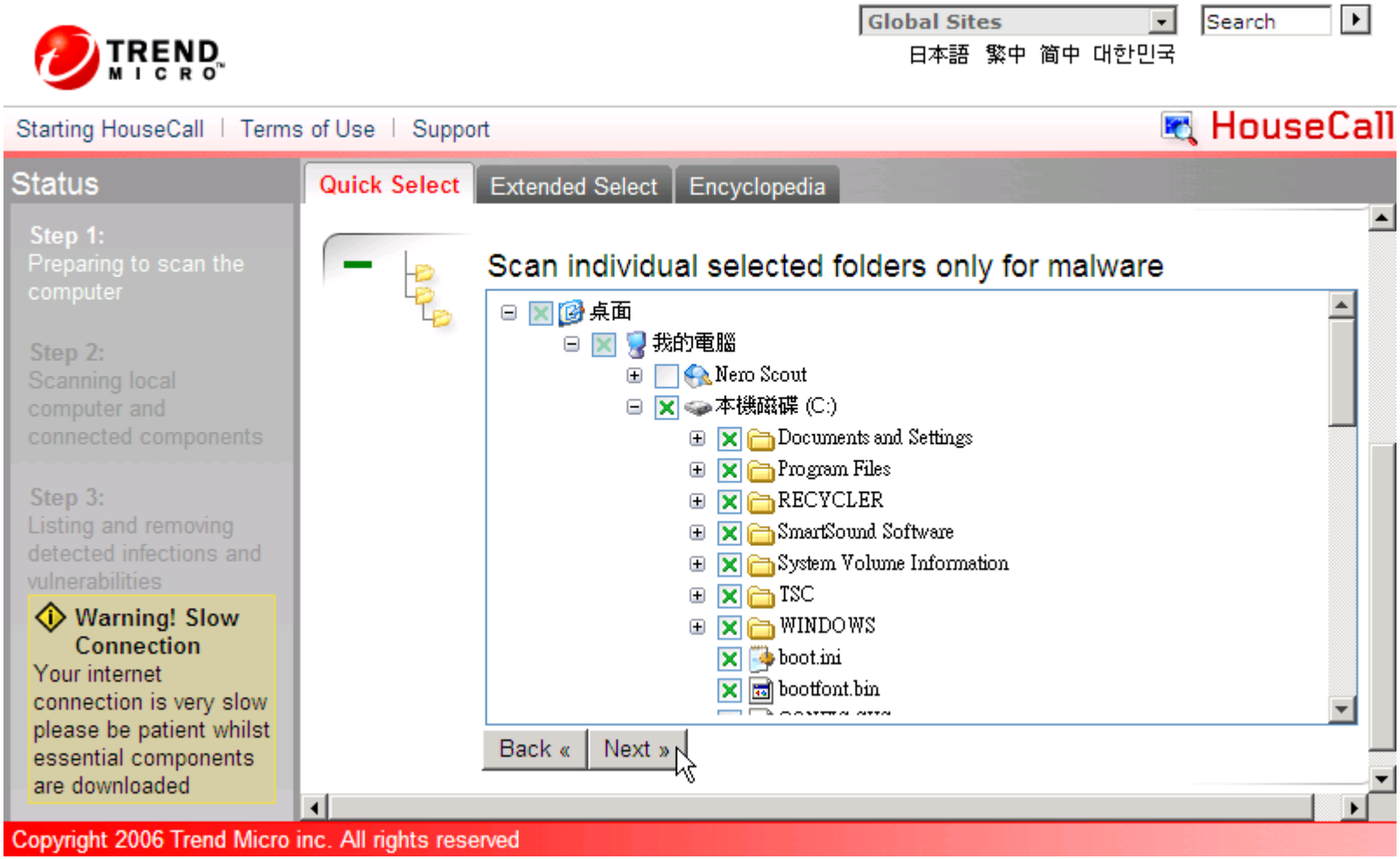
  免更新免等待，病毒碼永保最新

  24小時線上掃毒，不限時地隨心所欲

  免安裝輕鬆上手，系統資源零負擔

TREND MICRO

HouseCall線上掃毒



TREND MICRO

Trend Micro Spyware 線上掃瞄

- Trend Micro Spyware線上掃毒

  http://www.trendmicro.com/spyware-scan/

- Sysclean功能如下:

  快速防制新種間諜程式

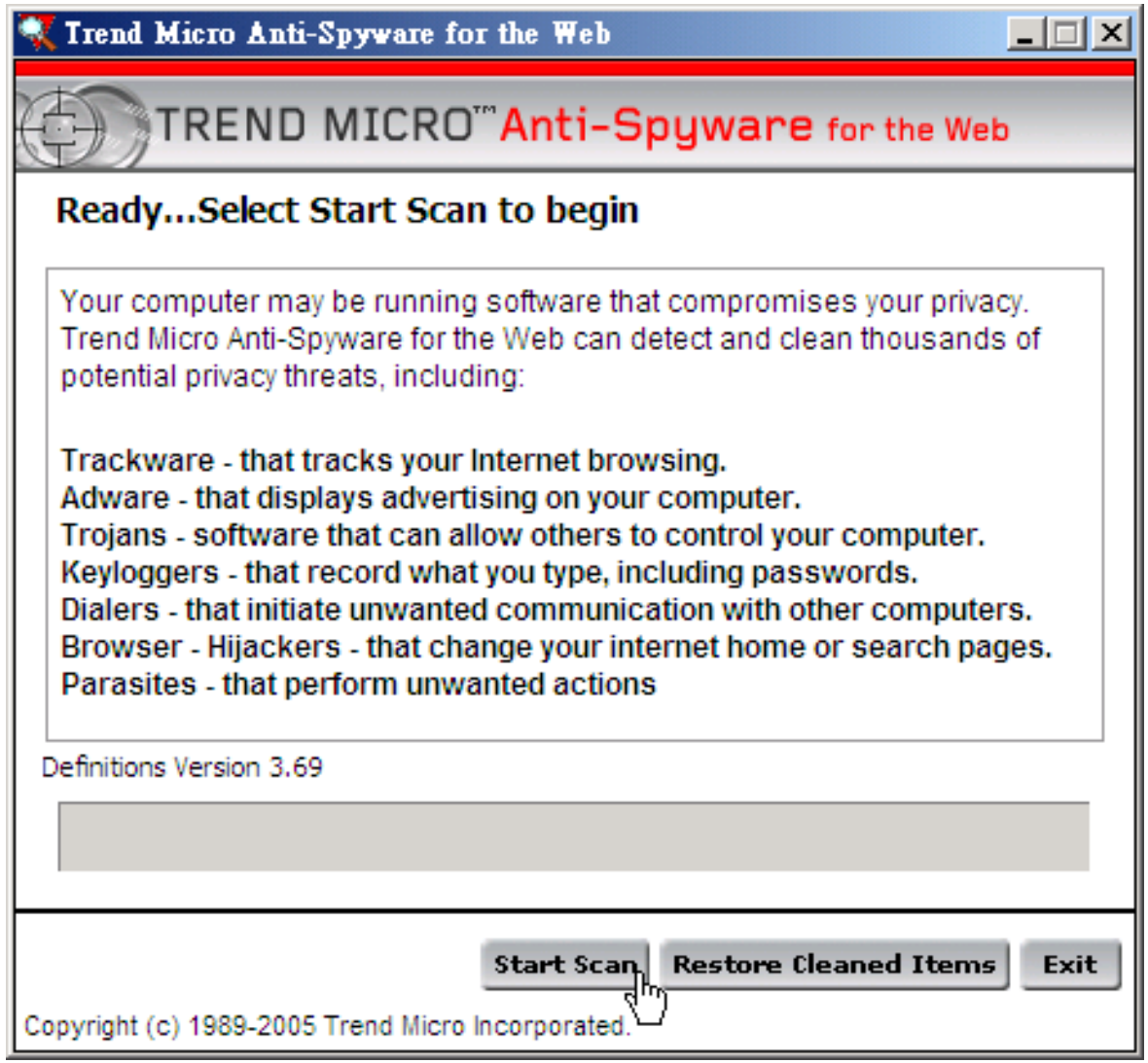
  CoolWebSearch首頁綁架清除功能

  歷史紀錄快速清除，防止資料外洩

  有效掃描與移除間諜程式

TREND MICRO

Trend Micro Spyware 線上掃瞄



X-Cleaner Adware 線上掃瞄

- X-Cleaner Adware 線上掃毒

  http://www.spywareinfo.com/xscan.php

- X-Cleaner Adware 線上掃毒功能如下:

  線上偵測廣告軟體及間諜程式

  有效掃描與移除廣告及間諜程式

TREND MICRO

X-Cleaner Adware 線上掃瞄

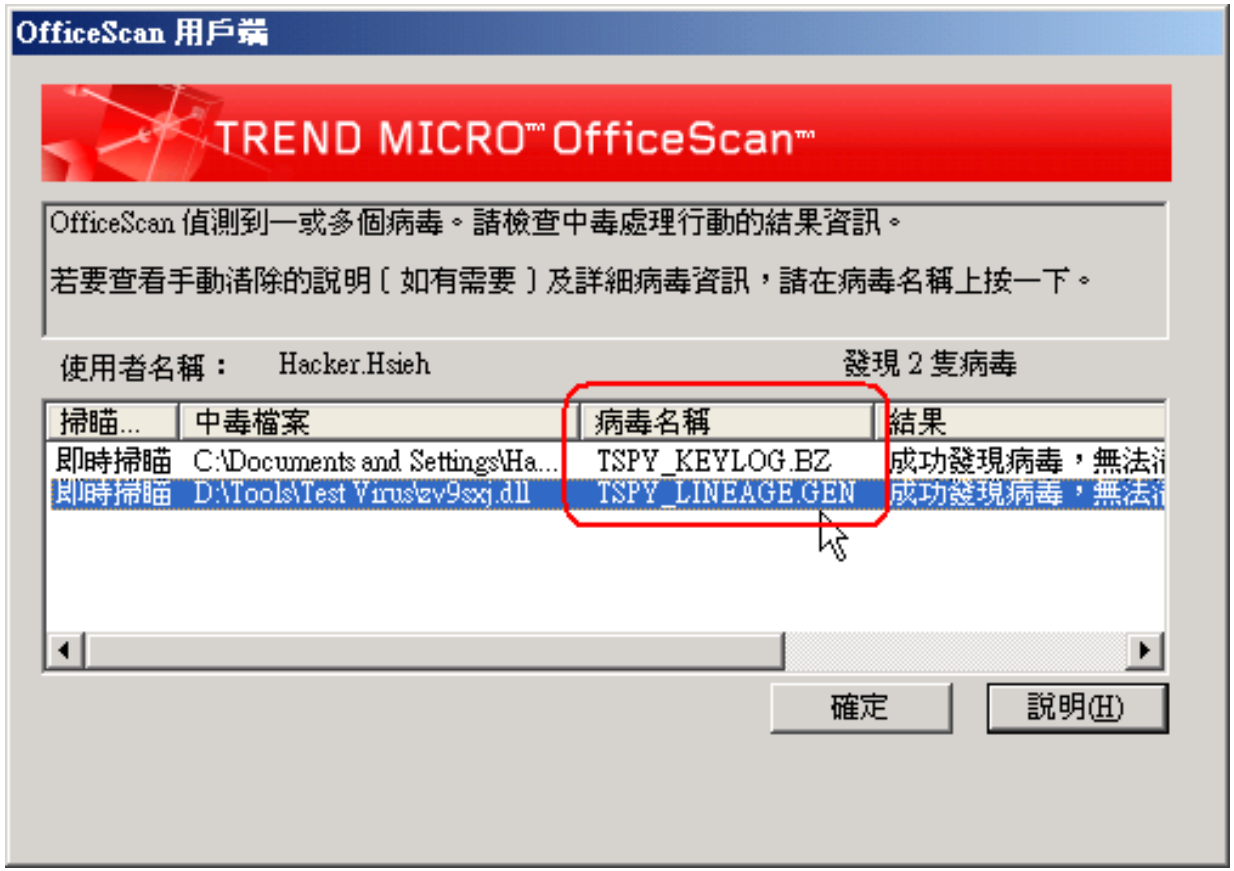
TREND MICRO

病毒建議清除程序及系統安全調校

TREND MICRO

中毒時的建議解毒程序

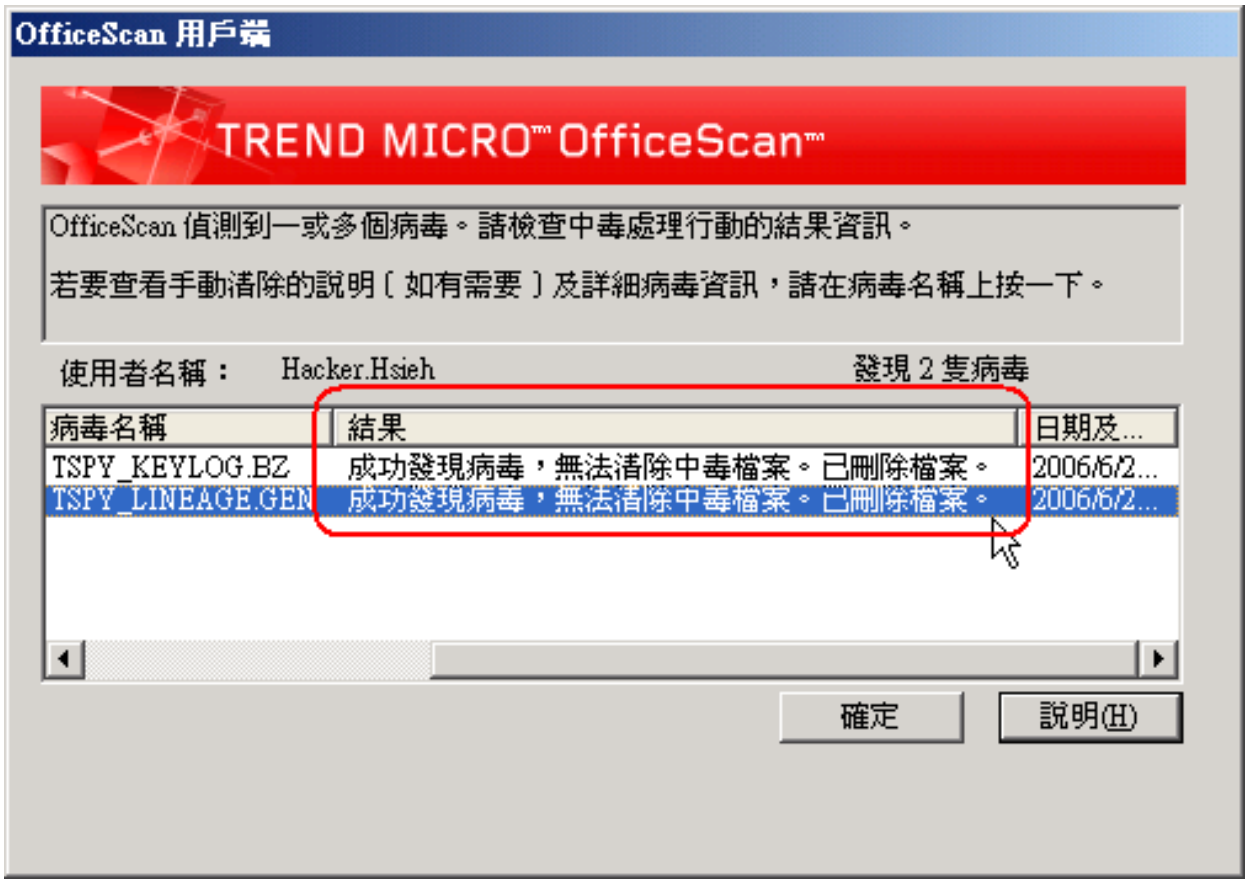
- 檢查目前電腦感染何種類型病毒及名稱為何



TREND MICRO

中毒時的建議解毒程序

- 檢查防毒產品針對此病毒處理程序為何



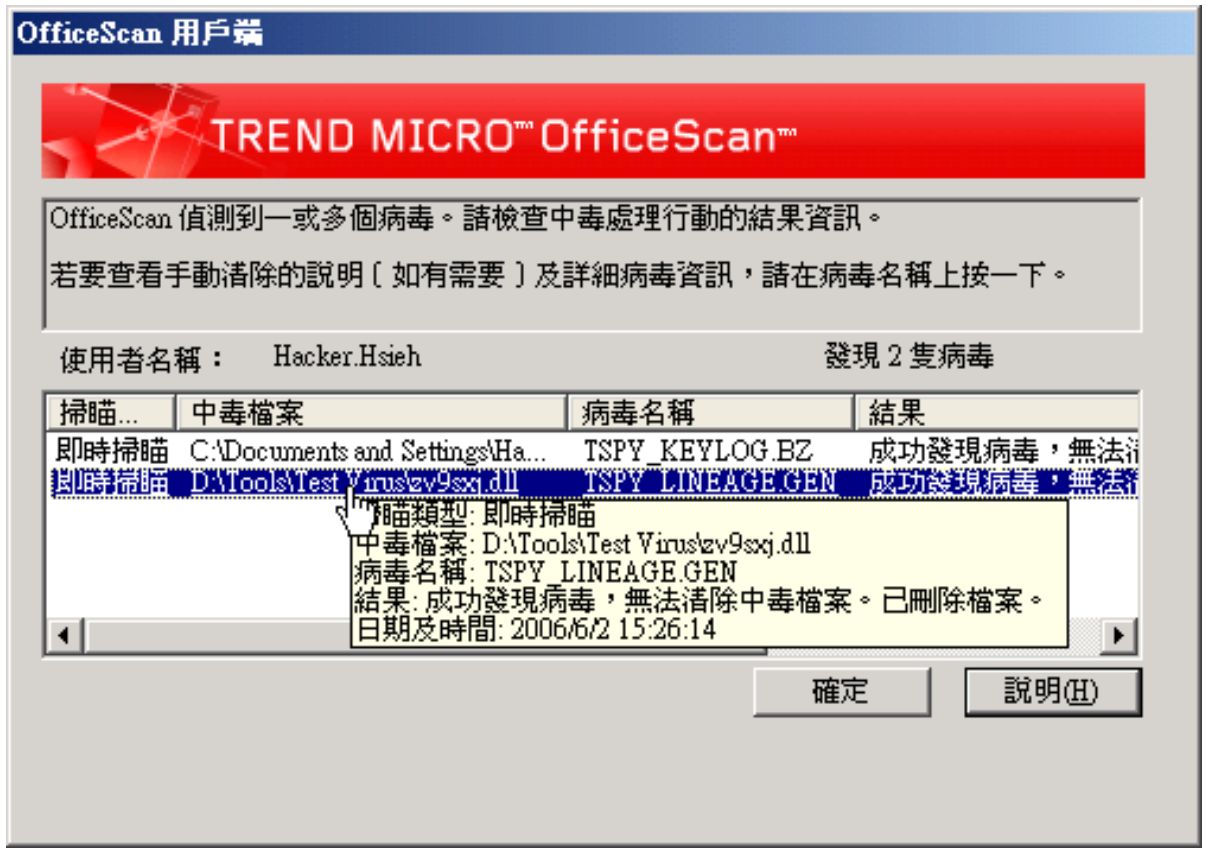
中毒時的建議解毒程序

- 若防毒軟體最後處理結果為已刪除或已隔離檔案，表示防毒產品已可解毒，您只要將解毒工作交給防毒軟體即可
- 若防毒軟體最後處理結果為無法刪除或無法隔離檔案，則需要進一步進行處理，請參照接下來的程序進行解毒程序

TREND MICRO

中毒時的建議解毒程序

- 請點選中毒訊息視窗內的病毒連結查看解決方案



TREND MICRO

中毒時的建議解毒程序

- 依據解決方案裡所述方式或先前所介紹的解毒工具一步步進行解毒

中毒時的建議解毒程序

- 確認感染病毒的名稱，以及病毒是否有攻擊某些系統漏洞，漏洞的名稱為何
- 將相關工具及作業系統漏洞修正程式下載至中毒電腦，確認OfficeScan已更新至最新病毒碼後，將網路線拔除
- 將此電腦系統還原功能關閉，並使用OfficeScan或之前所述的各項清毒工具進行手動全系統掃瞄，將所有偵測為病毒的檔案刪除
- 安裝所下載的微軟作業系統Hotfix

TREND MICRO

中毒時的建議解毒程序

- 至新增移除程式中將所有非必要及未知的程式手動進行移除程序
- 檢查系統相關分享權限，儘可能將分享關閉
- 檢查Guest此本機帳號是否已停用
- 請更改本機管理者密碼，密碼盡量不要設定太過簡易，以及將不必要的其他管理者帳號刪除
- 完成後插回網路現並重新開機，更新所有Hotfix

TREND MICRO

平時需注意的防毒小技巧

- 安裝防毒軟體：定期更新病毒碼、掃毒引擎
- 定期更改帳號與密碼，最好是英文加上數字，並不洩漏予他人
- 不隨意連結不明網站，不隨意下載不明程式
- 宣導安全的上網行為，不上一些奇怪的網站(地下、破解、下載、情色)
- 遠離來路不明的軟體，檔案，磁片及光碟；並隨時注意電腦異常狀況
- 養成安全上網行為不收發及轉寄一些奇怪郵件

TREND MICRO

平時需注意的防毒小技巧

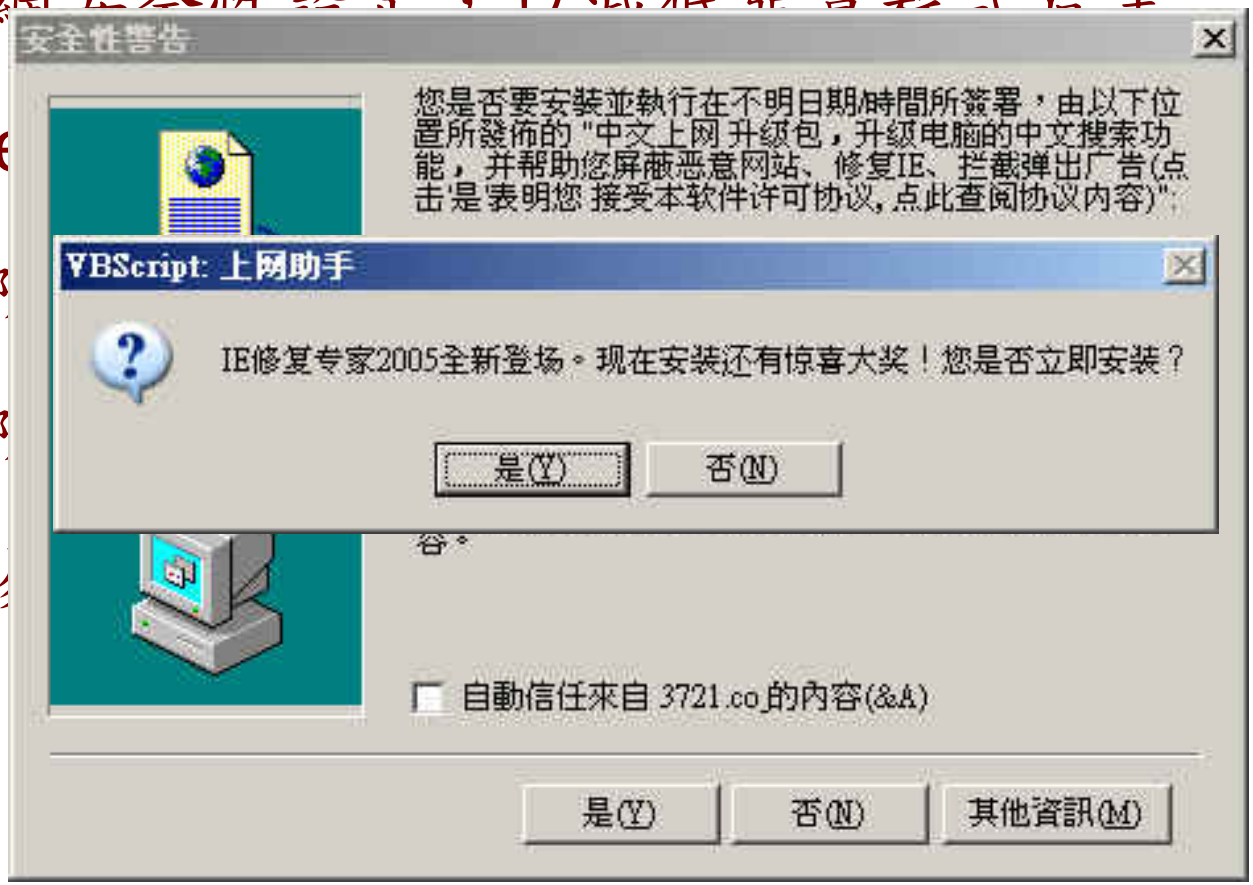
- 密切注意病毒、資訊安全通報等相關最新消息
- 定期更新Windows的弱點程式
- 調整檔案顯示方式，避免誤觸病毒
- 調整IE瀏覽器安全等級
- 嚴謹控管資源分享
- 善用系統還原機制
- 定期備份重要資料

TREND MICRO

系統安全調校-提高上網安全性

調整IE上網安全性設定，以減低惡意程式危害

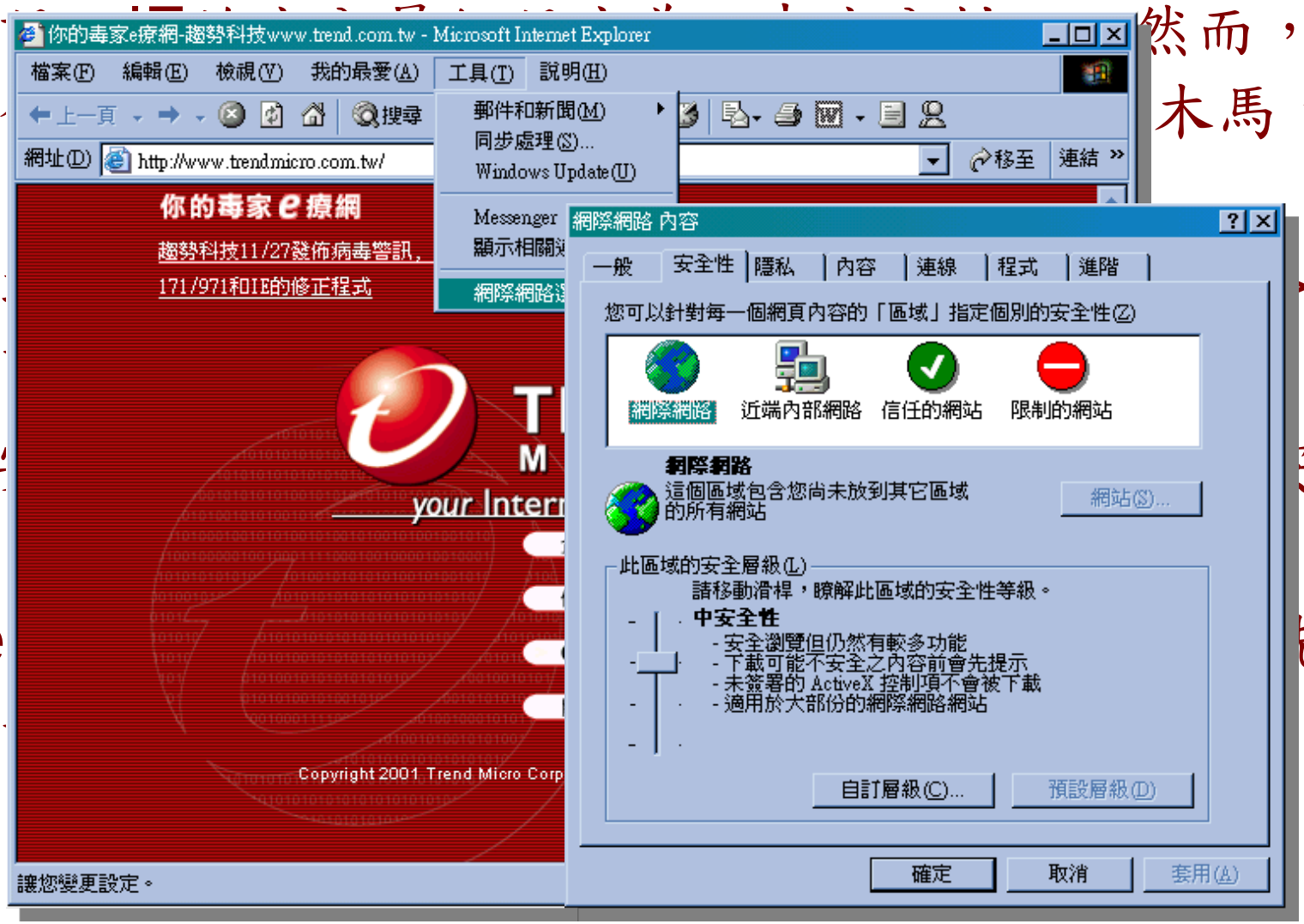
- 設定Inte
- 定期刪除
- 定期刪除
- 不要輕



TREND MICRO

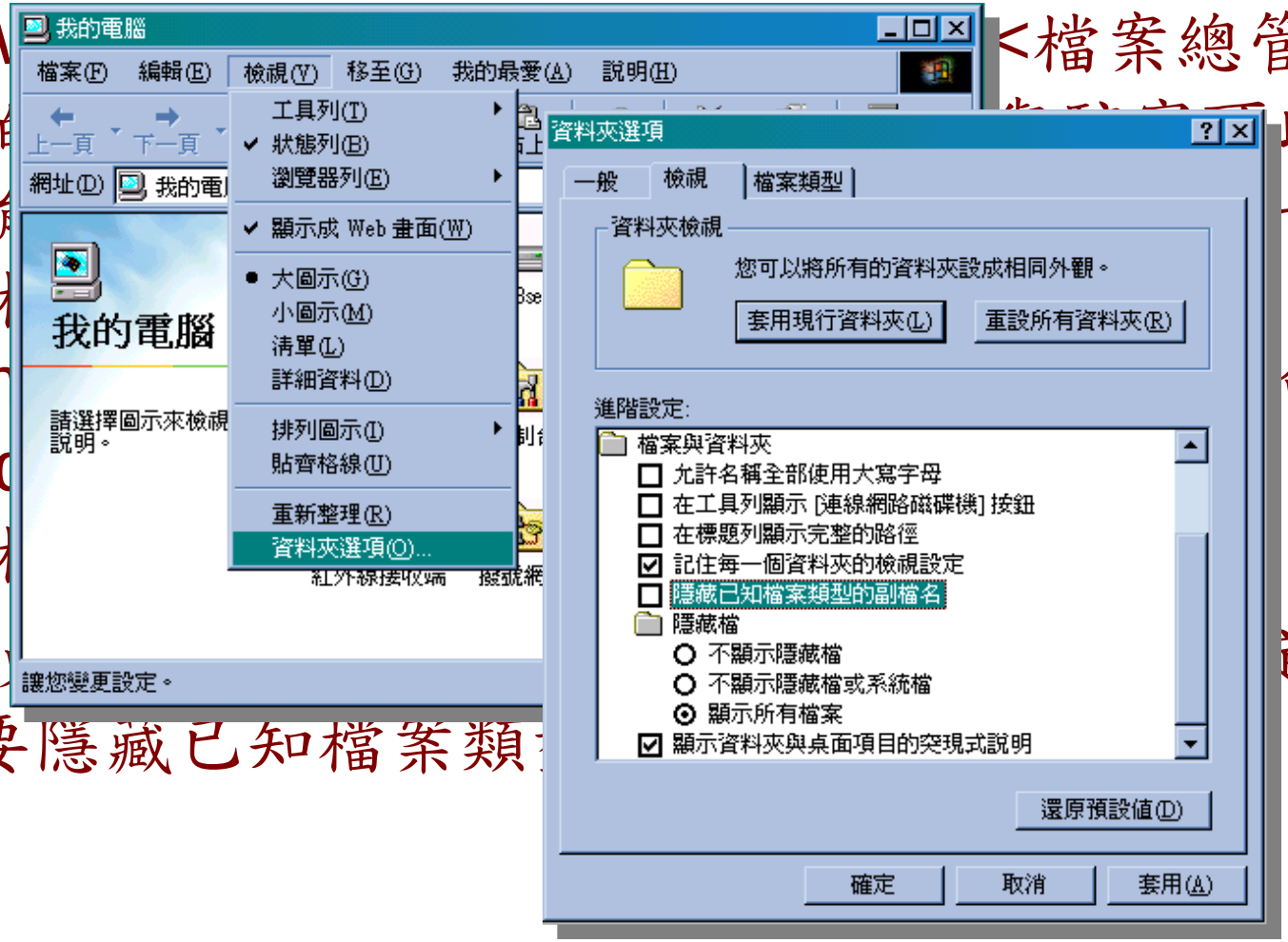
系統安全調校– IE安全層級

- 根據預 然而，我們卻 木馬、或駭客
- 基於這 ，如此
- 在 <中 全的檔
- Interne 先顯示警



系統安全調校-已知檔案副檔名

- 所有的\<檔案總管>中會將已知的 以利用這項功能 音效檔等其他檔 <readm 會顯示成<read 這個「文字」檔
- 為了避免 定變更為<不要隱藏已知檔案類



TREND MICRO

系統安全調校-資源分享的控管

- 在<W… …下您想要分享
- 在<檔…
- 按一… …名稱>。
- 按一… …碼。
- 儘量避… …分享設定為

TREND MICRO

系統安全調校-微軟SP及Hotfix

- 目前的病毒大多透過微軟作業系統本身的漏洞進行攻擊及擴散，故除了防毒產品的防護之外，建議也針對作業系統的漏洞進行修補程序，降低病毒的攻擊管道及為害

TREND MICRO

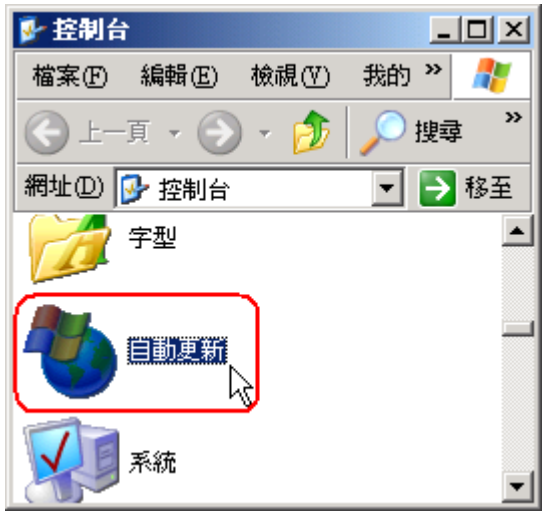
系統安全調校-微軟SP及Hotfix

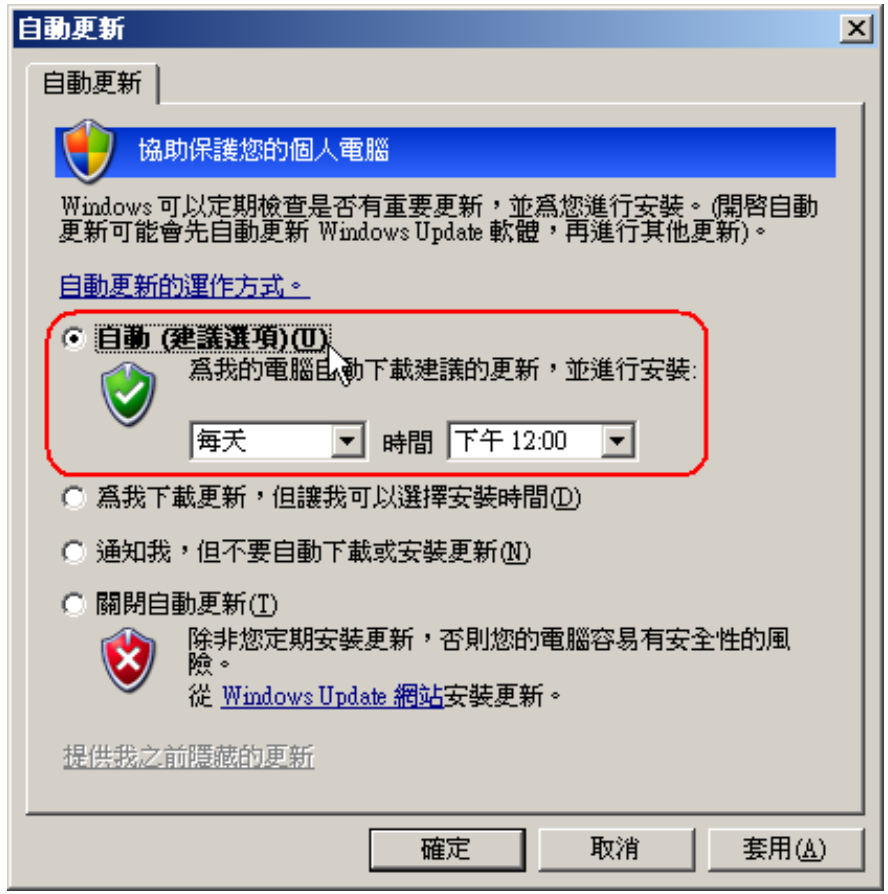
- 於電腦點選[開始]，選擇Windows Update

TREND MICRO

系統安全調校- HotFix自動更新

- 建議調整電腦自動下載更新Hotfix





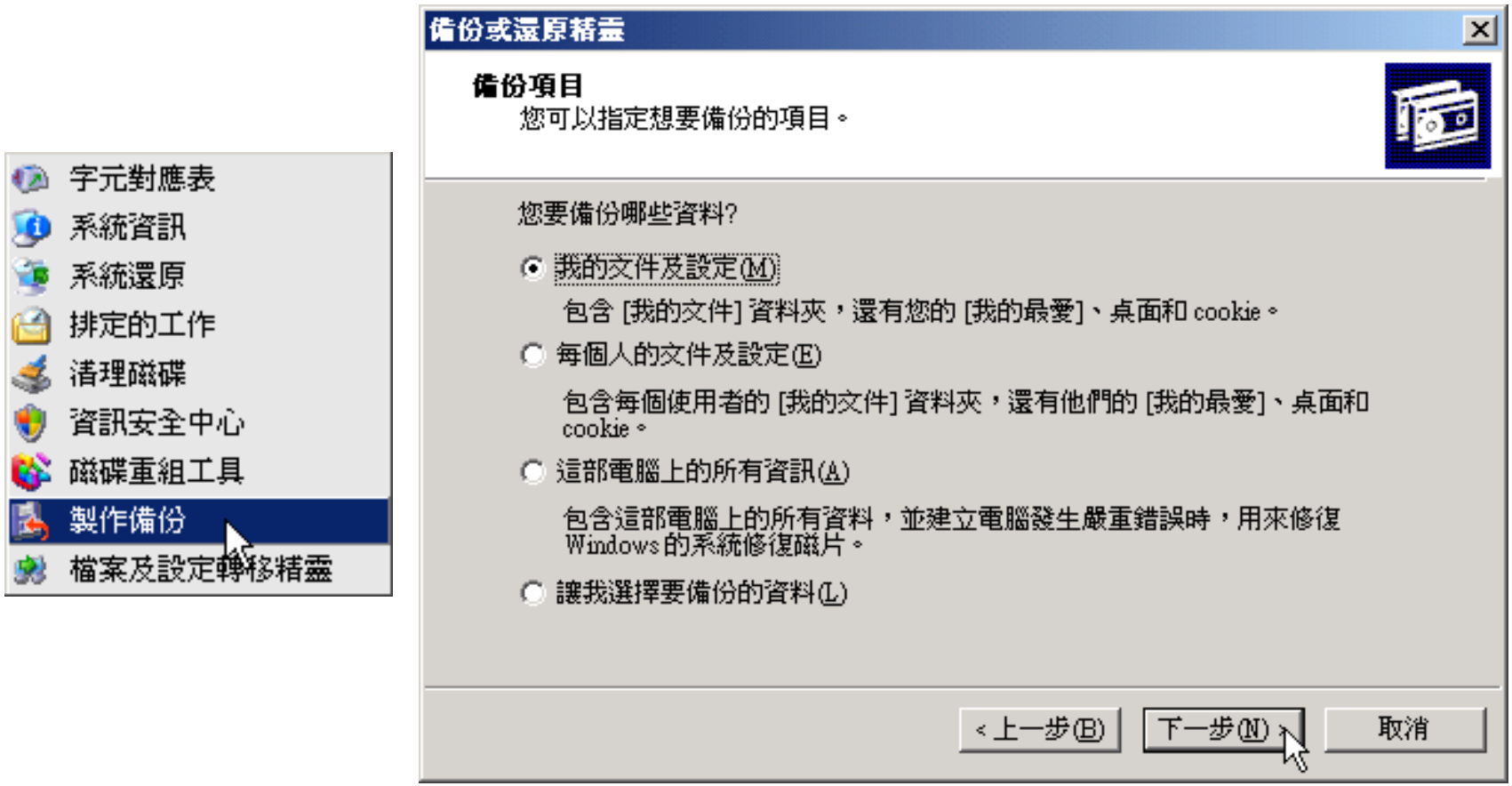
TREND MICRO

系統安全調校-資料備份

- 設定重要資料夾的位置，將個人文件等重要資料放置於特定目錄，定期備份
- 藉由Windows本身提供的程式來進行備份
- Windows的備份工具—「製作備份」
- 備份「我的最愛」和「通訊錄」
- 備份系統設定與重要檔案
- 備份重要資料夾位置
- 善用XP的時光回溯器—「系統還原」

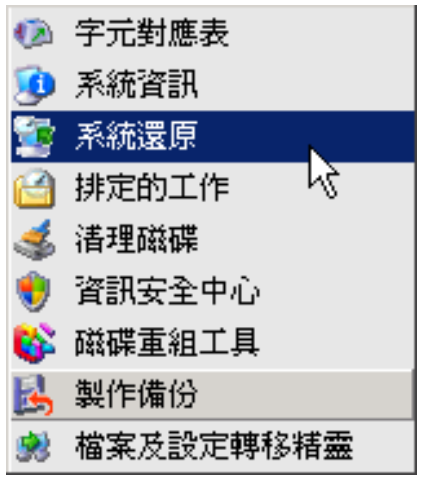
TREND MICRO

系統安全調校-資料備份


字元對應表
系統資訊
系統還原
排定的工作
清理磁碟
資訊安全中心
磁碟重組工具
製作備份
檔案及設定轉移精靈
備份或還原精靈
備份項目
您可以指定想要備份的項目。
您要備份哪些資料?
我的文件及設定(M)
包含 [我的文件] 資料夾，還有您的 [我的最愛]、桌面和 cookie。
每個人的文件及設定(E)
包含每個使用者的 [我的文件] 資料夾，還有他們的 [我的最愛]、桌面和 cookie。
這部電腦上的所有資訊(A)
包含這部電腦上的所有資料，並建立電腦發生嚴重錯誤時，用來修復 Windows 的系統修復磁片。
讓我選擇要備份的資料(L)
< 上一步(B)
下一步(N) >
取消

系統安全調校– 系統還原

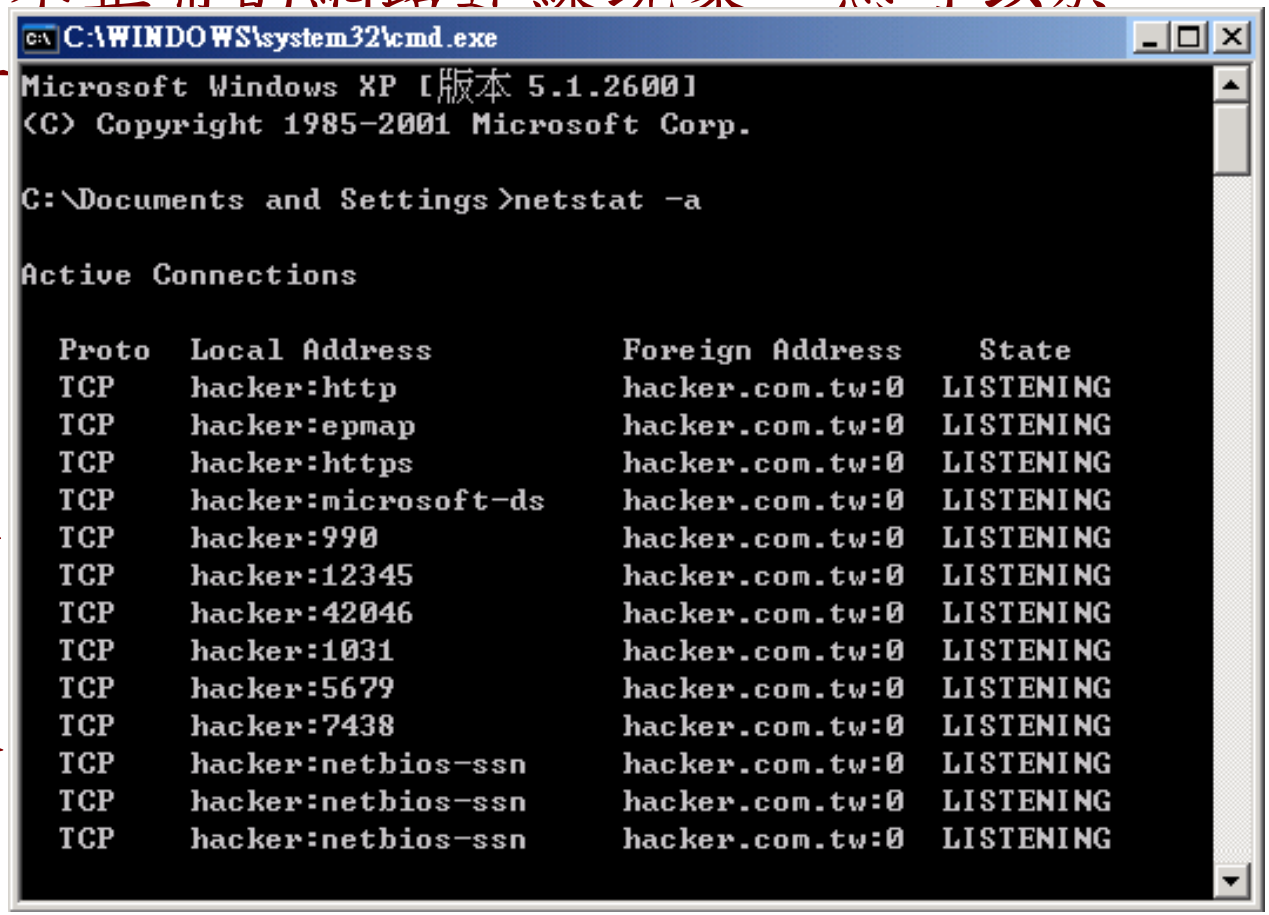
- 部分作業系統 (Windows ME、XP) 或時光回溯軟體也會提供系統還原的功能，只要先建好還原點，若日後系統感染病毒而無法正常運作，我們便可利用系統還原功能，將系統回復到曾建立還原點 (尚未感染病毒的時間點) 的地方。



TREND MICRO

小技巧-誰正在與我的電腦連線

- 若您發覺有不正常的網路連線現象，您可以於DOS模式下建立的所有
- 您可以看到第二欄為您址及通訊埠機所使用的機建立網路



TREND MICRO

小技巧-我的電腦執行了哪些程式

- 您可以利用工作管理員檢視目前正在執行中的程式名稱，是否有您未曾安裝的軟體或執行序，確保您的系統未遭後門或病毒程式侵擾。

TREND MICRO

未知型病毒建議檢測程序

TREND MICRO

系統可疑問題

- 當你發現電腦有異常現象，例如系統運作或網路變得非常緩慢、系統產生了一些奇怪的檔案、電腦操作變得異常、持續偵測到某個dll檔案但無法偵測主程式執行檔、自動打開一些網頁等狀況，有可能你的機器感染病毒了，這個時候請先確定你電腦的防病毒軟體是不是最新的病毒碼和引擎，在進行全系統掃瞄後狀況仍然相同，就可能感染了未知型惡意程式

TREND MICRO

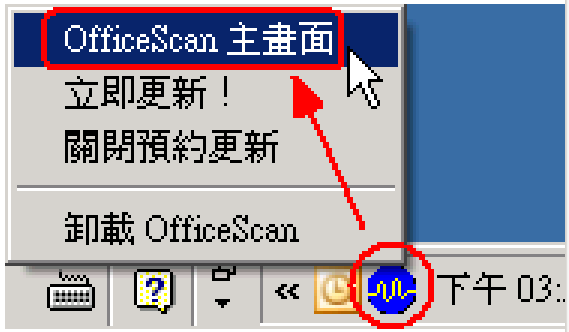
異常程式手動移除

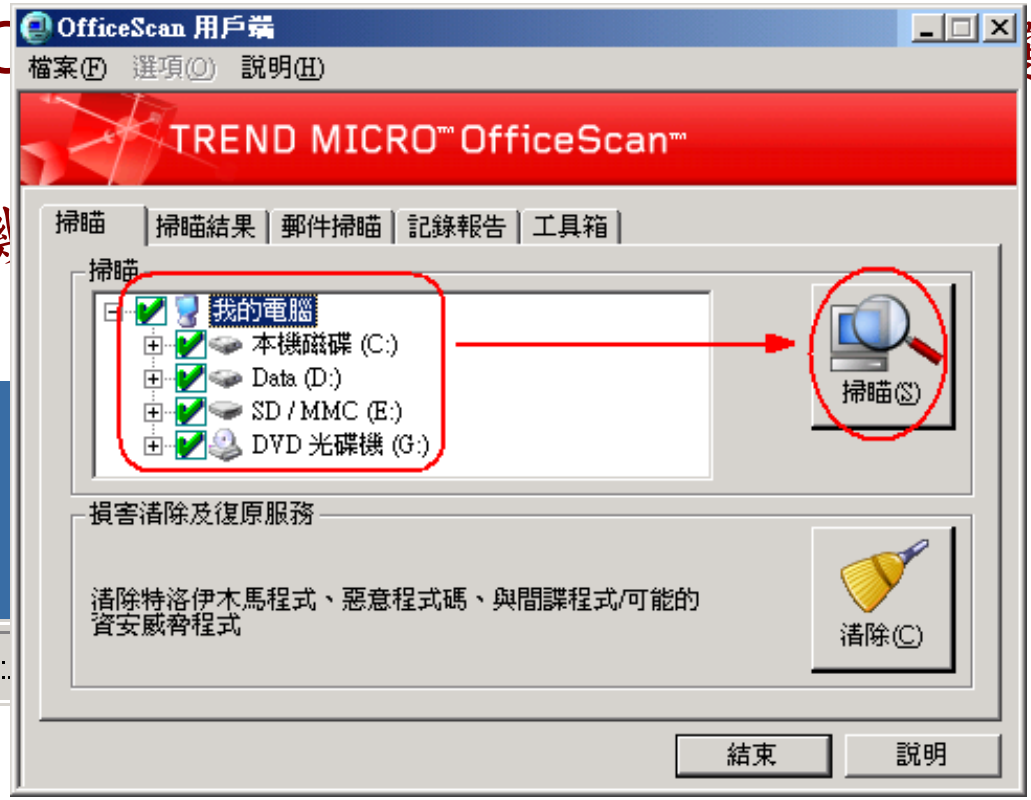
- 建議先於此異常主機之新增移除程式中查詢將非工作相關或非自行安裝的軟體手動移除

TREND MICRO

系統完整掃瞄

- 當您確定此電腦防病毒軟體各元件均已更新到最新版本，您可以對本機進行一次手動掃描，待掃描完成查看掃描的紀錄是否有病毒被發現
- 於工作列OfficeScan C…選 OfficeScan主畫面
- 請選擇要掃描的磁碟機

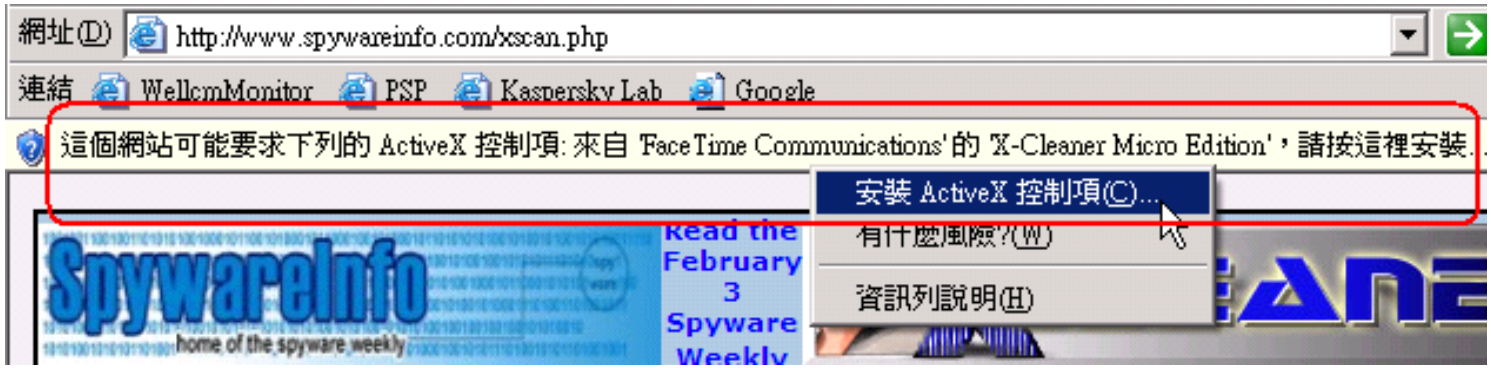




TREND MICRO

X-Cleaner Adware 線上掃瞄

- 首先建議先進行線上Adware/Spyware掃描，看是否有目前OSCE無法偵測的廣告或間諜軟體作怪，開啟瀏覽器輸入：http://www.spywareinfo.com/xscan.php
- 網頁開啟後，因此網頁須利用ActiveX運作，故請於瀏覽器上方點選安裝ActiveX



TREND MICRO

X-Cleaner Adware 線上掃瞄

- 出現以下畫面時請點選安裝

- 安裝完成後便開始進行線上掃瞄

TREND MICRO

System Information Collect

- 如果在進行以上全系統掃瞄並重新開機後發現狀況仍然相同，就可能感染了未知型惡意程式
- 趨勢提供System Information Collect Tool系統資訊蒐集工具，這個程式能把此電腦目前系統資訊蒐集後產生SIC紀錄，請將檔提供給客服人員，客服人員便會進行檔案分析，分析後如確實有疑似病毒程式，將請您把可疑的程式壓縮加密寄回分析，在寄送可疑的檔案之前請加密壓縮，如果分析後確認它是一個病毒檔，便會在一定時間內提供一個新的病毒碼用來偵測此病毒

TREND MICRO

System Information Collect

- SIC使用方法很簡單，下載後將檔案解壓縮至某暫存目錄，請開啟DOS模式，輸入sic -a，等候蒐集程序完成
  http://a928.g.akamai.net/f/928/485/10m/www.trend.com.tw/support/downloads/SIC/SIC_v33_1201.zip

TREND MICRO

System Information Collect

- 蒐集程序完成後，會於SIC主程式相同目錄下產生SICLOG00001.TXT，將此檔案提供給客服人員分析，該檔案包含了系統中絕大多數病毒可能利用的設定以便於診斷

TREND MICRO

Q & A
問題與回答