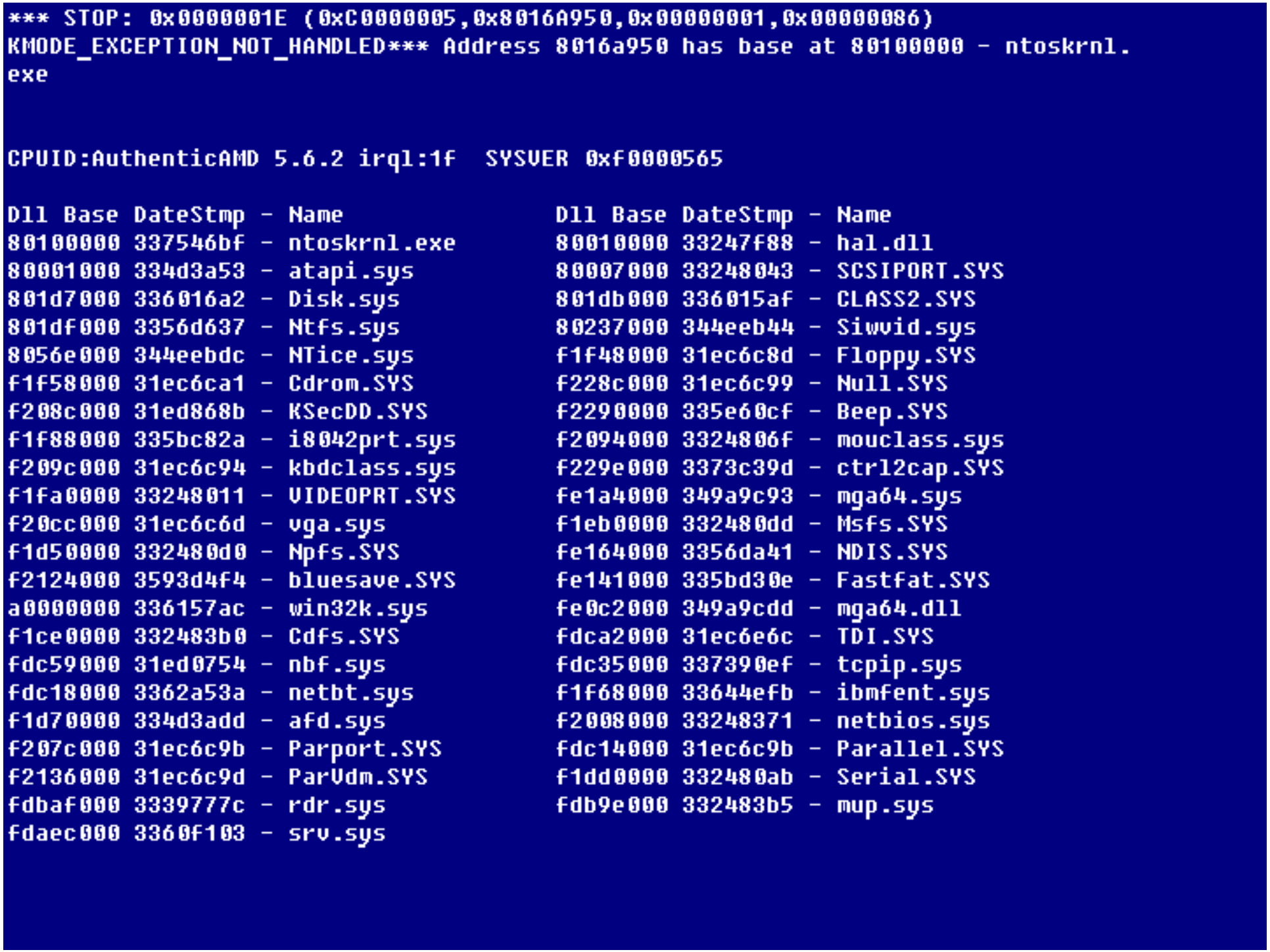
惡意程式防護介紹

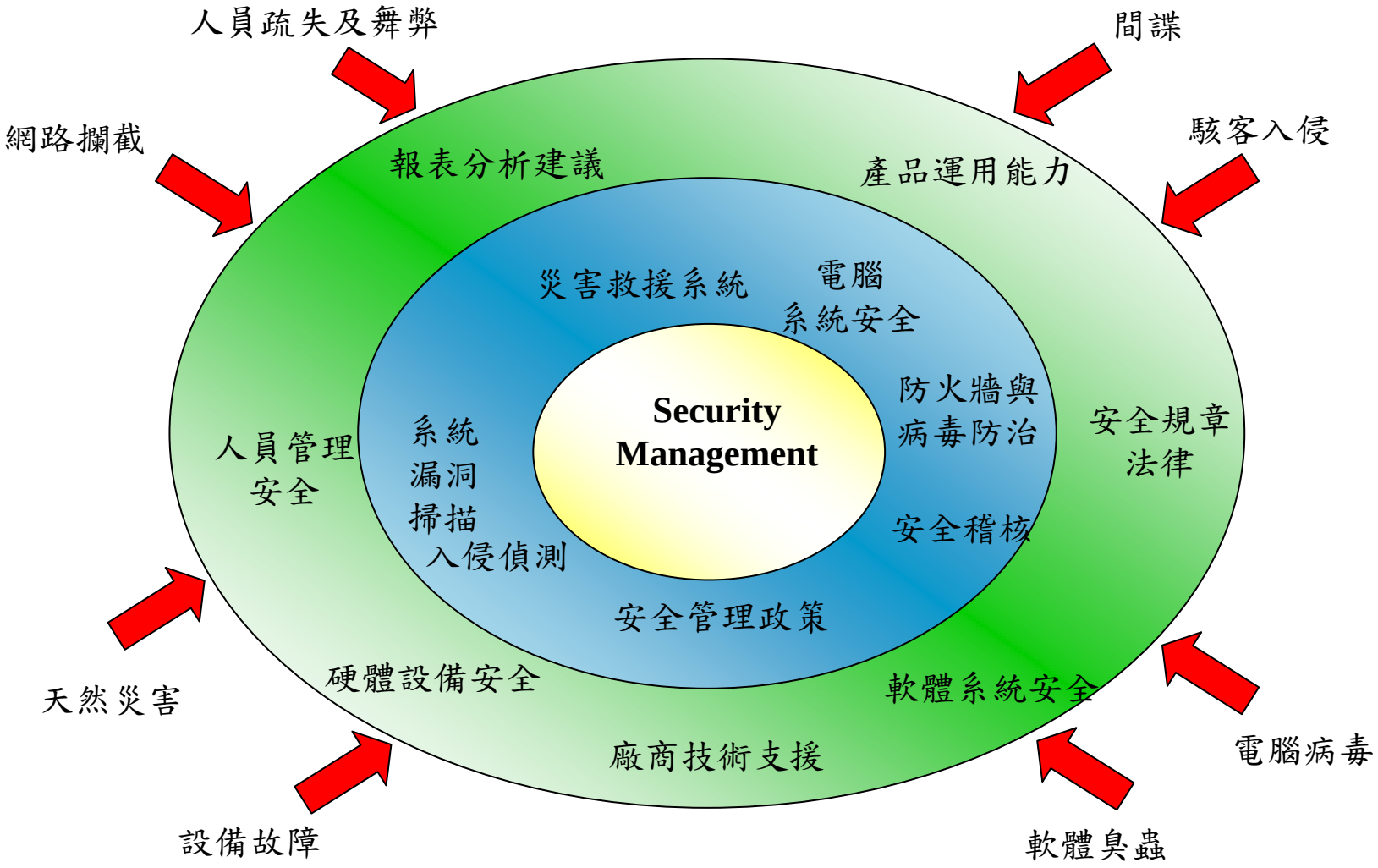
大綱

- 資訊安全威脅來源
- 電腦病毒概念說明
- Demo – 木馬程式所帶來的威脅
- 如何佈署防毒軟體
- 如何防範惡意程式
- 如何發現未知惡意程式
- 問題與討論

資訊安全威脅來源


*** STOP: 0x0000001E (0xC0000005,0x8016A950,0x00000001,0x00000086)
KMODE_EXCEPTION_NOT_HANDLED*** Address 8016a950 has base at 80100000 - ntoskrnl.
exe
CPUID:AuthenticAMD 5.6.2 irql:1f SYSVER 0xf0000565
Dll Base DateStmp - Name
80100000 337546bf - ntoskrnl.exe
80001000 334d3a53 - atapi.sys
801d7000 336016a2 - Disk.sys
801df000 3356d637 - Ntfs.sys
8056e000 344eebdc - NTice.sys
f1f58000 31ec6ca1 - Cdrom.SYS
f208c000 31ed868b - KSecDD.SYS
f1f88000 335bc82a - i8042prt.sys
f209c000 31ec6c94 - kbdclass.sys
f1fa0000 33248011 - VIDEOPRT.SYS
f20cc000 31ec6c6d - vga.sys
f1d50000 332480d0 - Npfs.SYS
f2124000 3593d4f4 - bluesave.SYS
a0000000 336157ac - win32k.sys
f1ce0000 332483b0 - Cdfs.SYS
fdc59000 31ed0754 - nbf.sys
fdc18000 3362a53a - netbt.sys
f1d70000 334d3add - afd.sys
f207c000 31ec6c9b - Parport.SYS
f2136000 31ec6c9d - ParVdm.SYS
fdbaf000 3339777c - rdr.sys
fdaec000 3360f103 - srv.sys
Dll Base DateStmp - Name
80010000 33247f88 - hal.dll
80007000 33248043 - SCSIPORT.SYS
801db000 336015af - CLASS2.SYS
80237000 344eeb44 - Siwvid.sys
f1f48000 31ec6c8d - Floppy.SYS
f228c000 31ec6c99 - Null.SYS
f2290000 335e60cf - Beep.SYS
f2094000 3324806f - mouclass.sys
f229e000 3373c39d - ctrl2cap.SYS
fe1a4000 349a9c93 - mga64.sys
f1eb0000 332480dd - Msfs.SYS
fe164000 3356da41 - NDIS.SYS
fe141000 335bd30e - Fastfat.SYS
fe0c2000 349a9cdd - mga64.dll
fdca2000 31ec6e6c - TDI.SYS
fdc35000 337390ef - tcpip.sys
f1f68000 33644efb - ibmfent.sys
f2008000 33248371 - netbios.sys
fdc14000 31ec6c9b - Parallel.SYS
f1dd0000 332480ab - Serial.SYS
fdb9e000 332483b5 - mup.sys

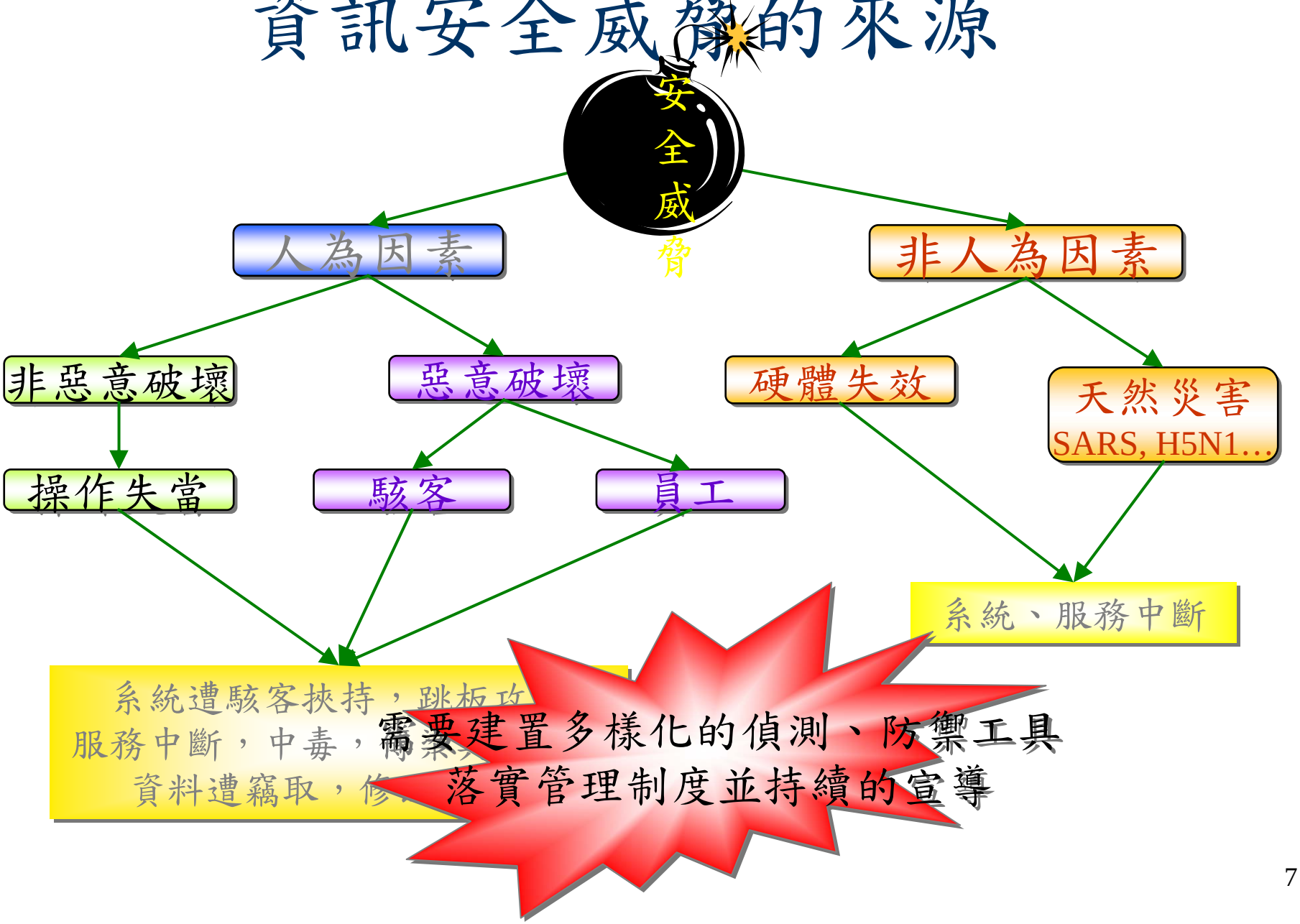
各式各樣的資訊安全問題



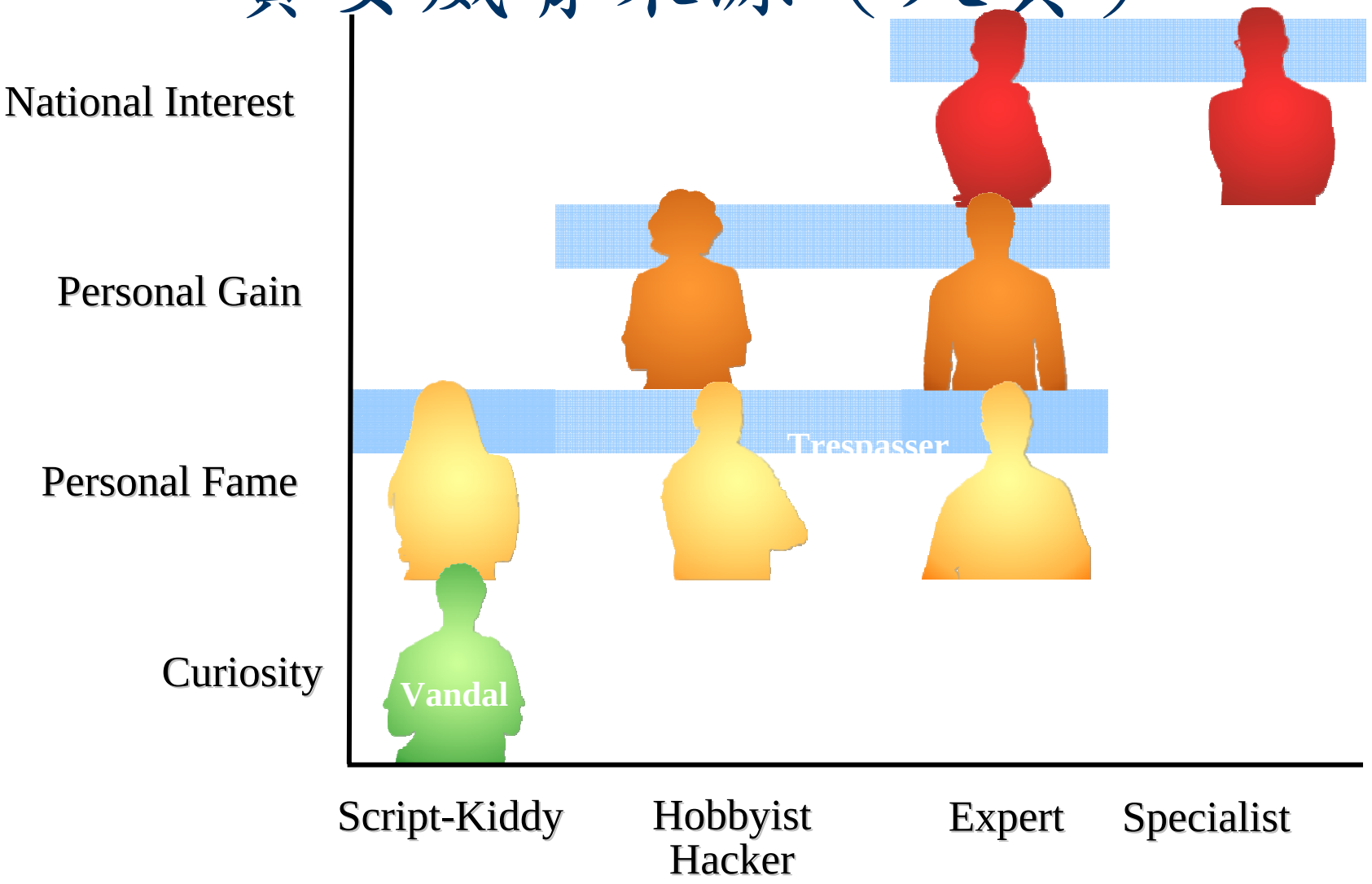
安全威脅同時來自於

- 內部問題
  - 內部濫用
  - 內賊
  - 非法使用
  - 當機
- 外部問題
  - 入侵
  - 病毒

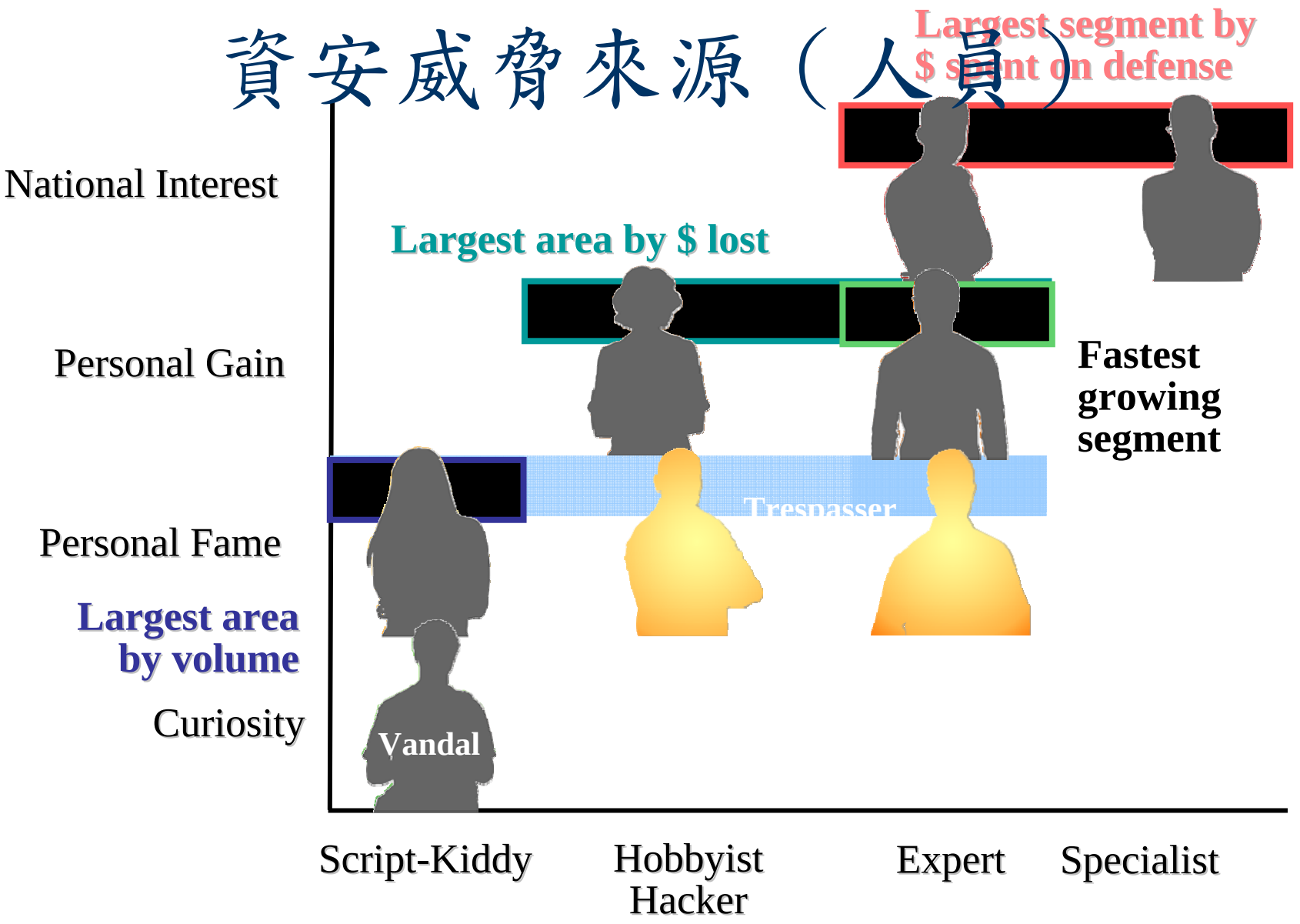
資訊安全威脅的來源


安全威脅
人為因素
非人為因素
非惡意破壞
惡意破壞
硬體失效
天然災害
SARS, H5N1…
操作失當
駭客
員工
系統、服務中斷
系統遭駭客挾持，跳板攻
服務中斷，中毒，
資料遭竊取，修
需要建置多樣化的偵測、防禦工具
落實管理制度並持續的宣導

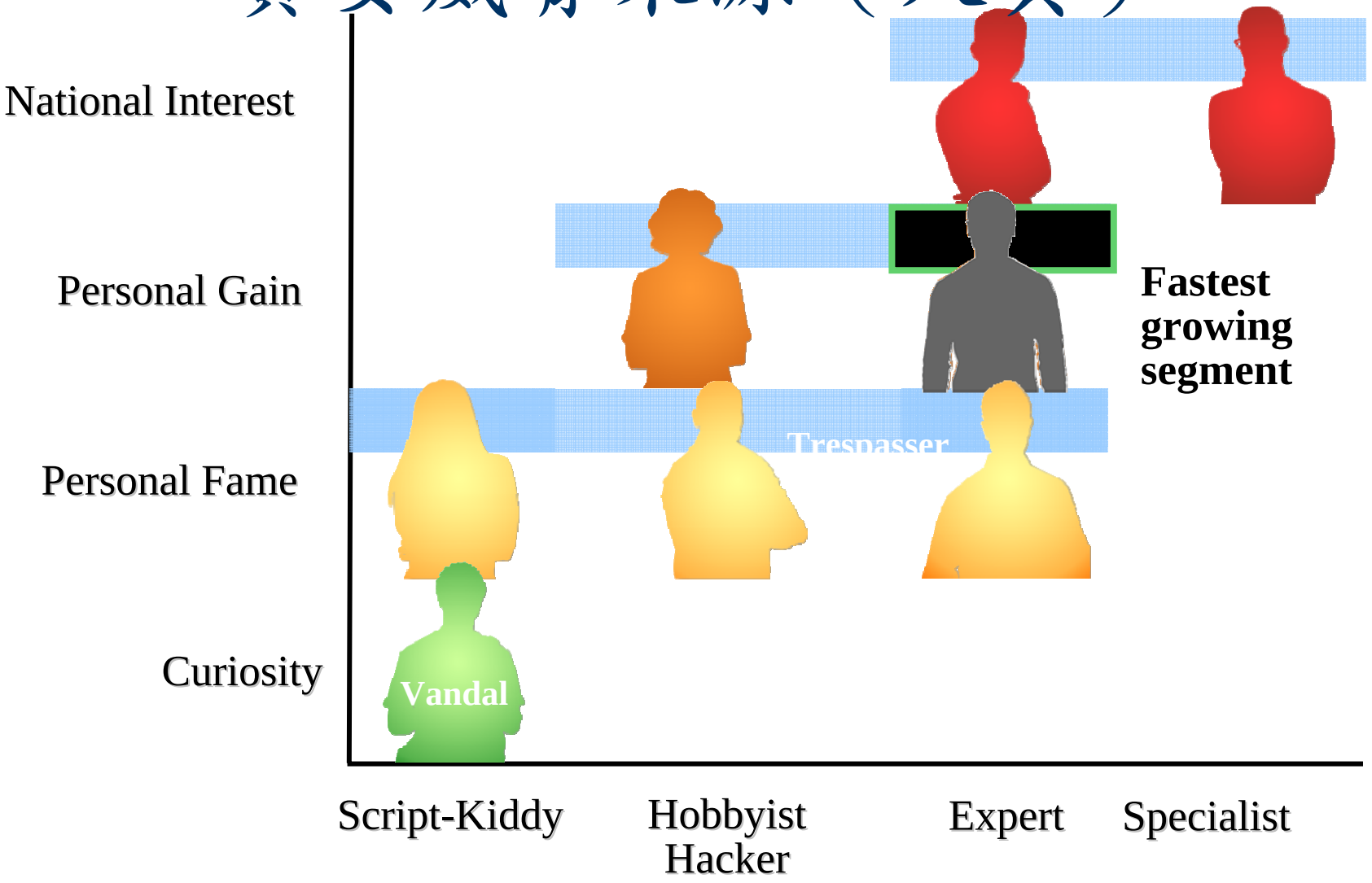
資安威脅來源（人員）


National Interest
Personal Gain
Personal Fame
Curiosity
Trespasser
Vandal
Script-Kiddy
Hobbyist Hacker
Expert
Specialist

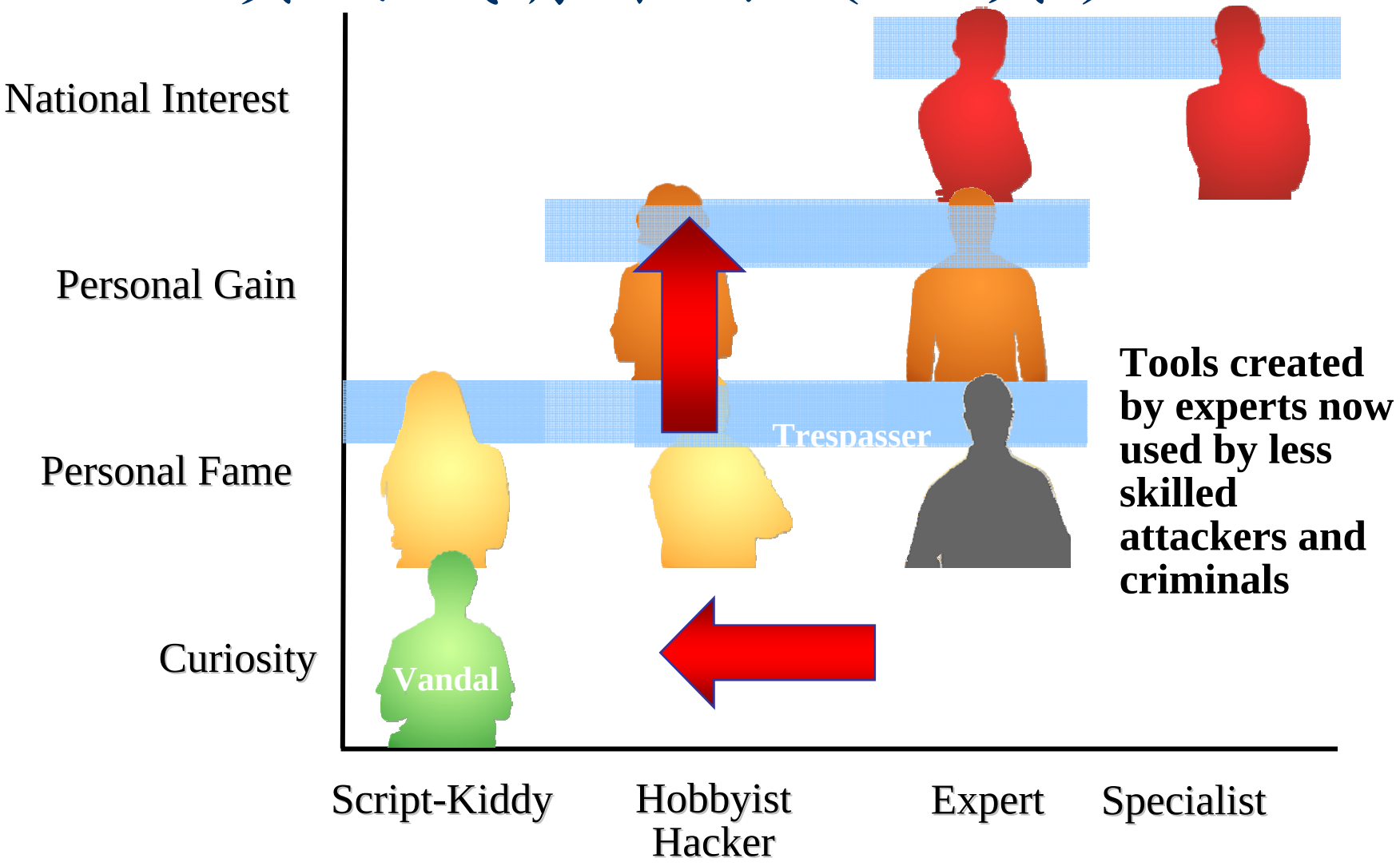
資安威脅來源（人員）


Largest segment by
$ spent on defense
National Interest
Largest area by $ lost
Personal Gain
Fastest
growing
segment
Trespasser
Personal Fame
Largest area
by volume
Curiosity
Vandal
Script-Kiddy
Hobbyist
Hacker
Expert
Specialist

資安威脅來源（人員）


National Interest
Personal Gain
Personal Fame
Curiosity
Fastest growing segment
Trespasser
Vandal
Script-Kiddy
Hobbyist Hacker
Expert
Specialist

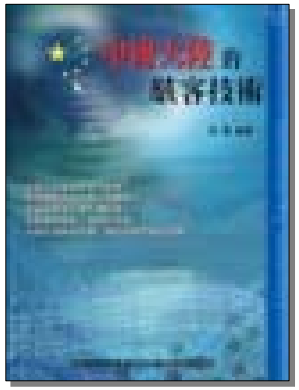
資安威脅來源（人員）

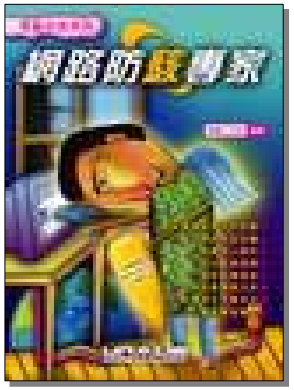

National Interest
Personal Gain
Personal Fame
Curiosity
Trespasser
Vandal
Tools created by experts now used by less skilled attackers and criminals
Script-Kiddy
Hobbyist Hacker
Expert
Specialist


網路犯罪實錄


完全攻擊秘技


網路駭客手冊




網路防駭專家

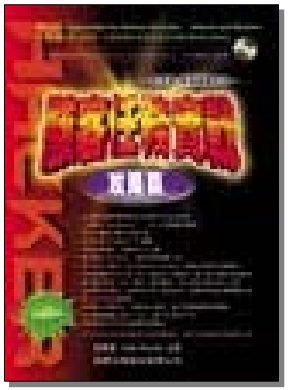

本馬屠城記


小心駭客


GOTOP
駭客入侵不求人


馬上學會
駭客入侵


輕鬆防駭，電腦永保安康




駭客解凍




網路獵殺



企業的郵件都需面對大量的危機

- 病毒信件
- 垃圾信件
- 不當的郵件
- 利用郵件傳送公司機密
- 不穩定的作業系統 影響公司信件收發



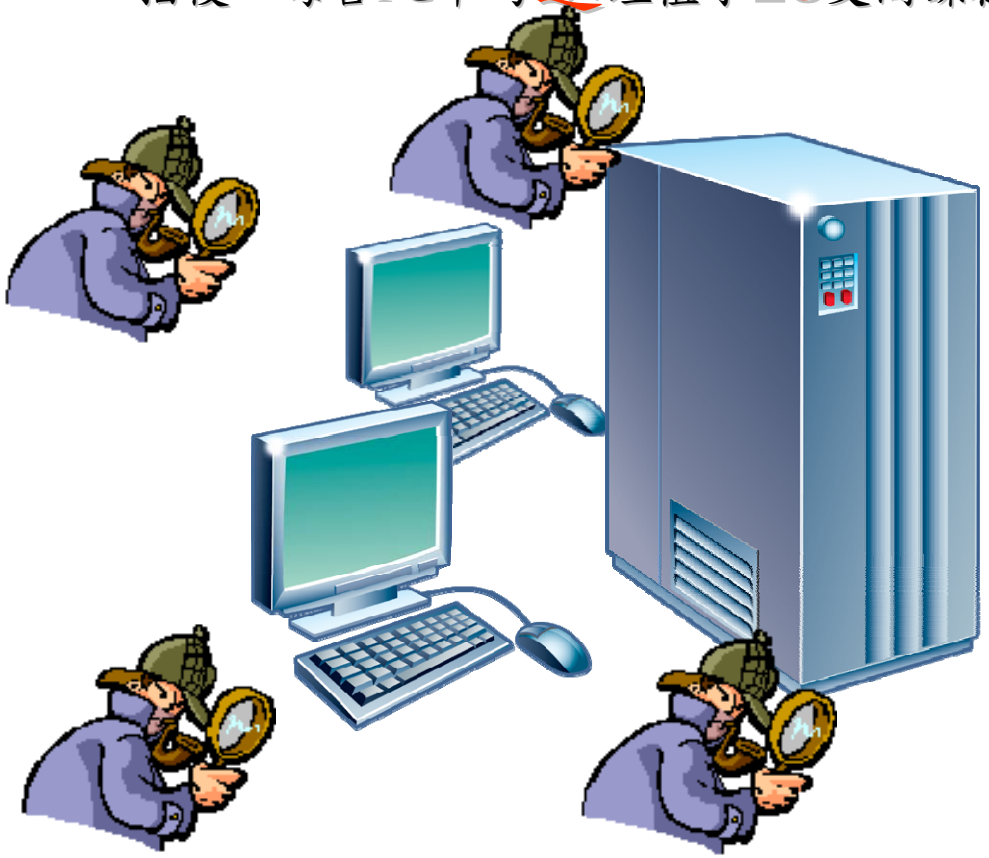
病毒信件的威脅

- 根據 ICSA 調查 86% 的病毒來自 e-mail
- 82% 的 IT 管理者都必須處理病毒的事件



除了防毒還要防偷防搶

安全服務領導廠商EarthLink指出，經過了病毒掃描後，每台PC平均還埋植了28支間諜程式



電腦病毒概念說明

電腦病毒與惡性程式

- 惡性程式 (Malware) - 具有不良企圖的程式

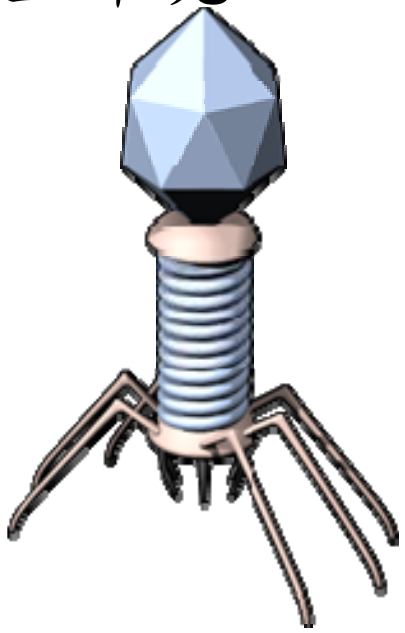


為什麼會有惡意程式

- 惡意程式的來源
  - 創新理論的實驗？！
  - 新科技的發展？！
  - …
- 惡意程式都是有害的嗎？
  - 是的！！！
- 以上所提到的創新被有心人士利用了！

常見電腦病毒發作症狀

- 電腦動作比平遲鈍
- 程式載入比平常花更多的時間
- 不尋常的錯誤訊息出現
- 當你沒存取磁碟時，但磁碟指示燈卻亮
- 系統記憶體突然大減
- 磁碟空間變少了
- 檔案奇怪消失了
- 沒有連線，可是網路流量增加



認識防毒軟體專有名詞

- 何謂病毒碼？
  - 犯人指紋
  - 獨一無二的二進位的病毒程式碼
  - 決定可以偵測到的病毒數目
- 何謂掃毒引擎？
  - 防毒軟體的核心技術(Core-Technology)
  - 真正影響防毒軟體速度及偵測率的主要關鍵
  - 決定可以偵測到的病毒種類及檔案格式
    - 例如:巨集病毒，Java病毒，被ZIP壓縮過的檔案
- 何謂主程式
  - 防毒軟體的介面及功能

電腦病毒

- 電腦病毒 (Virus)
  - 電腦病毒是一種電腦程式，設計有特定的功能，並且會感染寄生或附著在別的電腦程式或文件檔案裡面。有些電腦病毒就只有自我複製這個單一的功能與目的，有些電腦病毒則會破壞電腦裡面的資料，甚至會破壞電腦系統(如：CIH)。

電腦蠕蟲

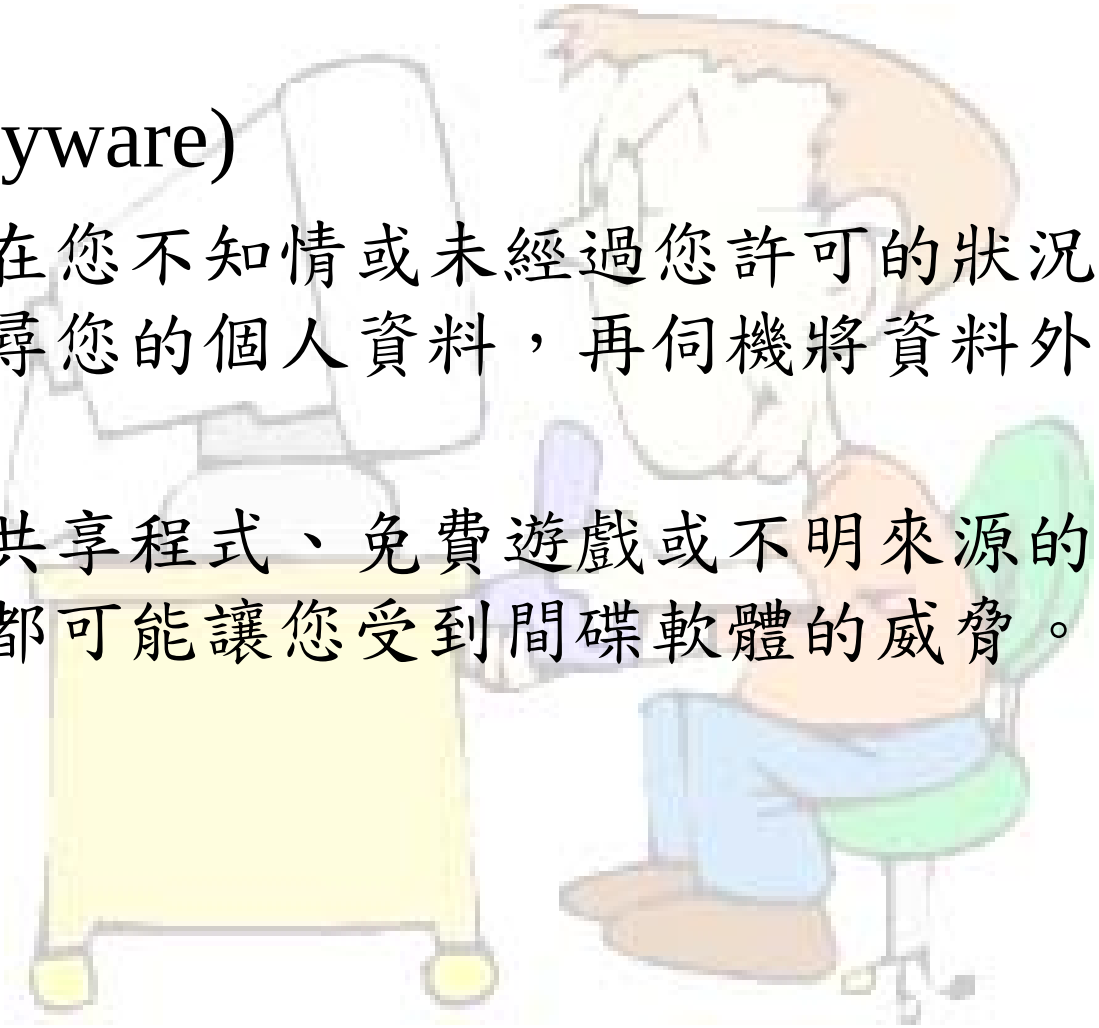
- 電腦蠕蟲 (Worm)
  - 電腦蠕蟲也可說是電腦病毒的一種，與病毒不同的是，蠕蟲不會感染寄生在其他檔案。蠕蟲的主要特性是會自我複製並主動散播到網路系統上的其他電腦裡面。就像蟲一樣在網路系統裡面到處爬竄，所以稱為「蠕蟲」。

特洛伊木馬

- 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。一般定義上，特洛伊木馬不會自我複製，也不會主動散播到別的電腦裡面。

間碟軟體

- 間碟軟體 (Spyware)
  - 間碟軟體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，再伺機將資料外傳。
  - 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。



惡作劇程式

- 除了干擾使用者的正常作業之外，不會有任何感染行為或造成任何損害
- 通常很難停止或中斷該程式
- 滑鼠或鍵盤等周邊裝置出現暫時異常現象

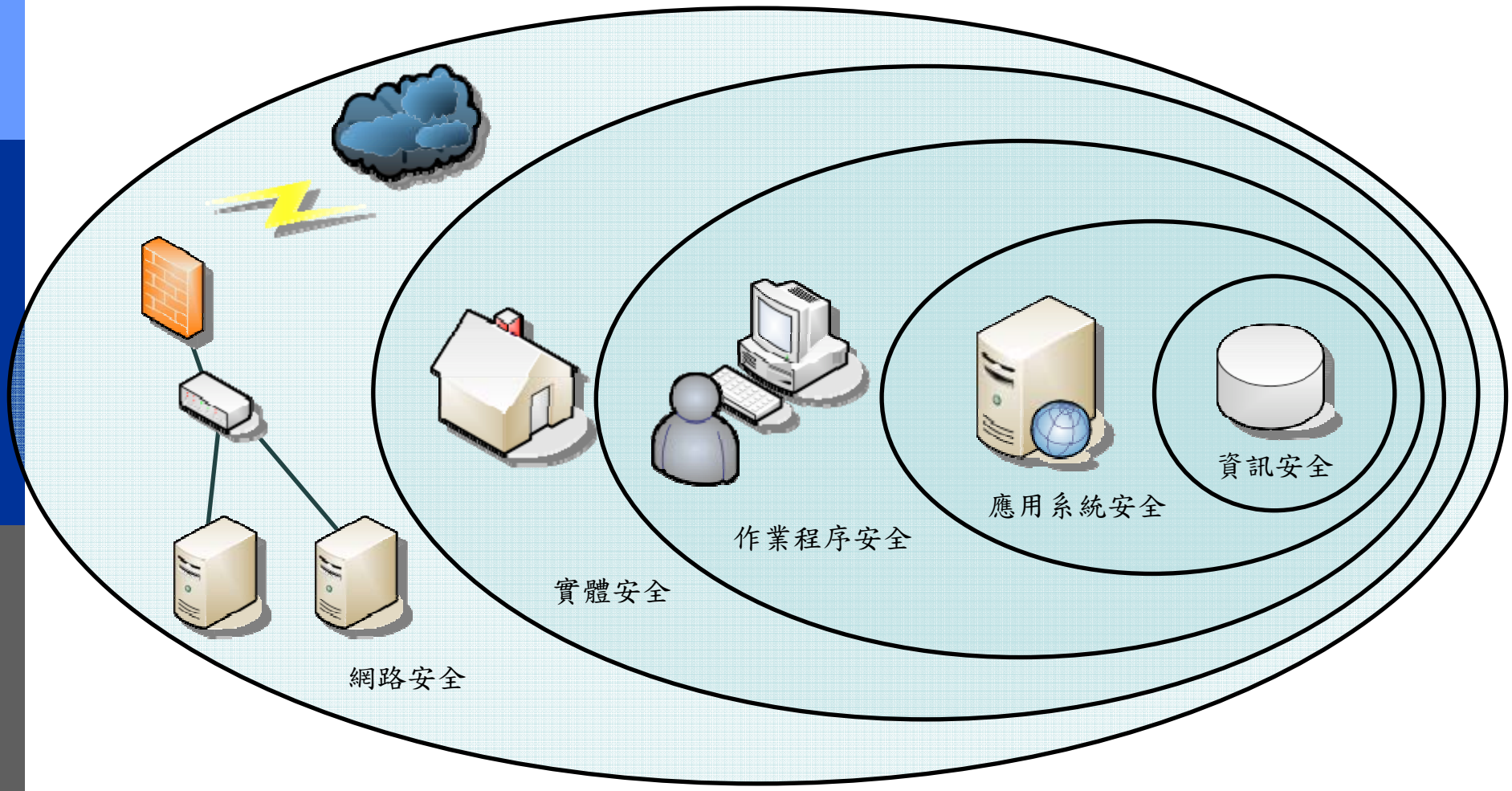
謠言/玩笑

- 網路上經常流傳著一些電子郵件，並且鼓勵你再把這些警告訊息轉寄給你的親朋好友。
  - 『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...』
- 事實上，這種訊息絕大多數都是所謂的「謠言耳語」。
- 藉由查詢各防毒軟體公司的網站，可以分辨大部份的網路謠言。

Demo
木馬所帶來的威脅

如何佈署防毒軟體

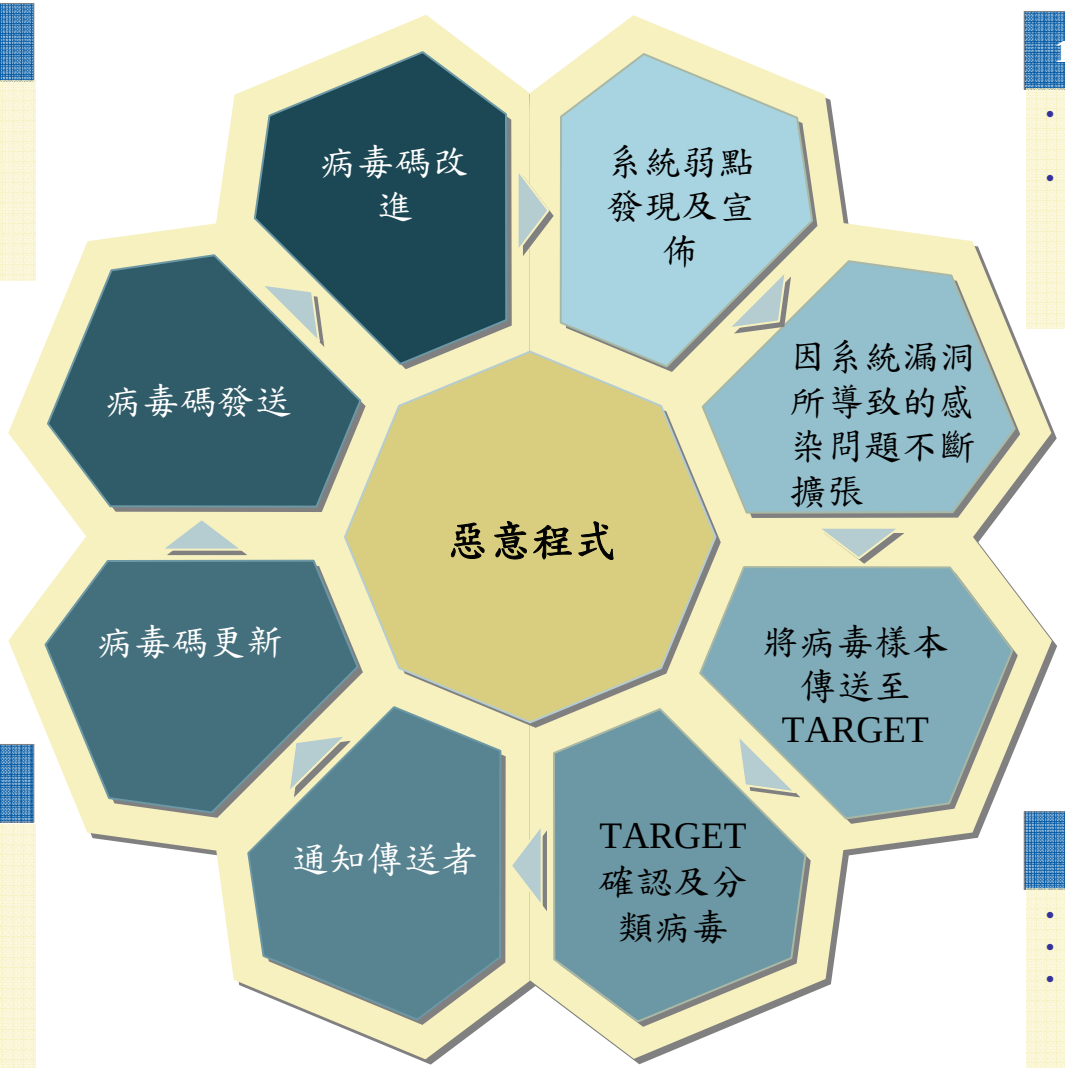
以數位疆界為概念的多層防護



病毒生命週期

4. 病毒碼改進

- 針對變種的病毒及蠕蟲重新定義及更新及發佈病毒碼
- 發佈及更新病毒的清除方式



1. 新的系統漏洞擴張/散佈

- 惡意程式利用系統漏洞散佈及擴張
- 發現因系統漏洞所引發的惡意程式攻擊

3. 病毒碼

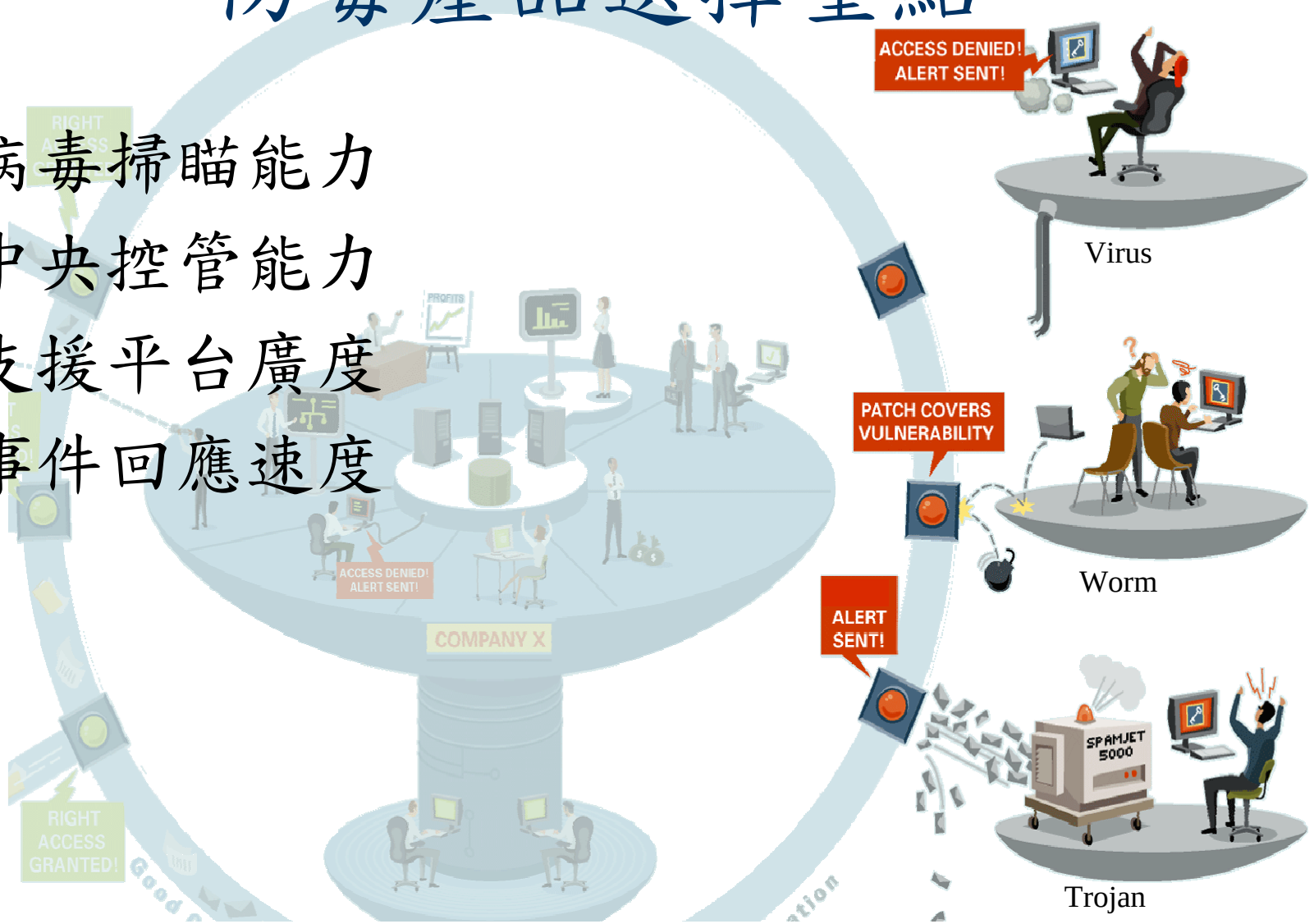
- TARGET 更新病毒碼
- 通知傳送者及傳送病毒碼至傳送者
- 病毒碼部署至客戶企業

2. TARGET 研發團隊

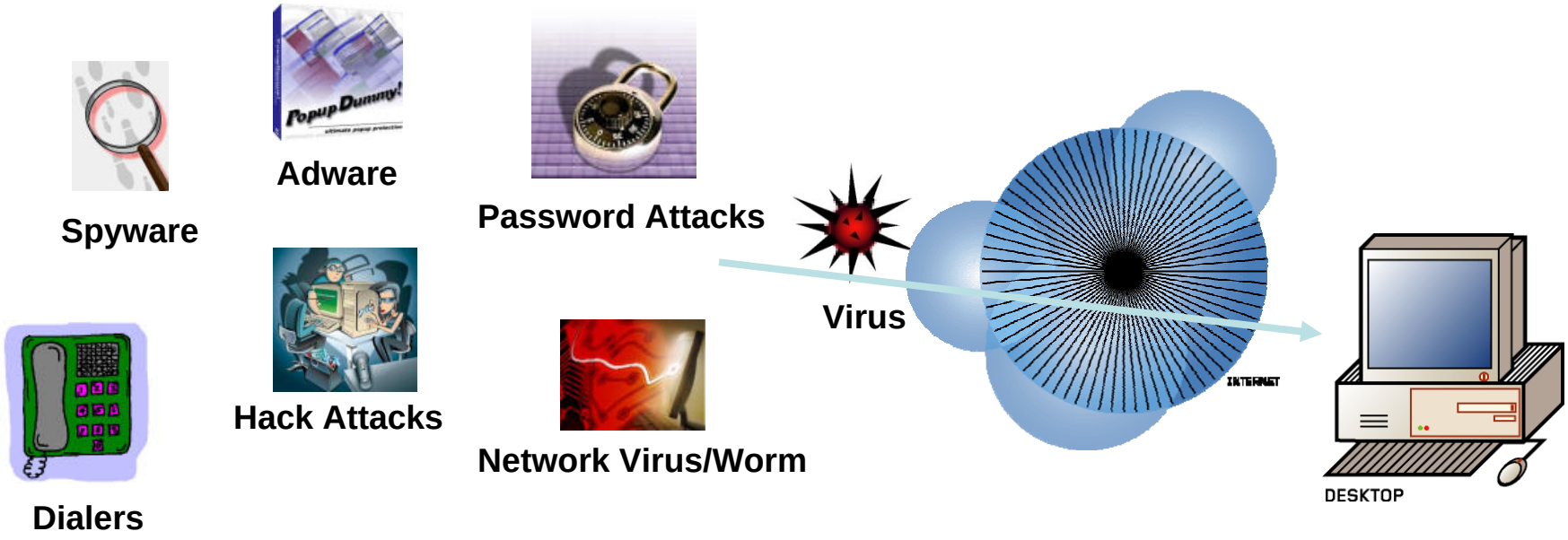
- 分析樣本
- 確認潛在的威脅
- 定義威脅的種類

防毒產品選擇重點

- 病毒掃瞄能力
- 中央控管能力
- 支援平台廣度
- 事件回應速度

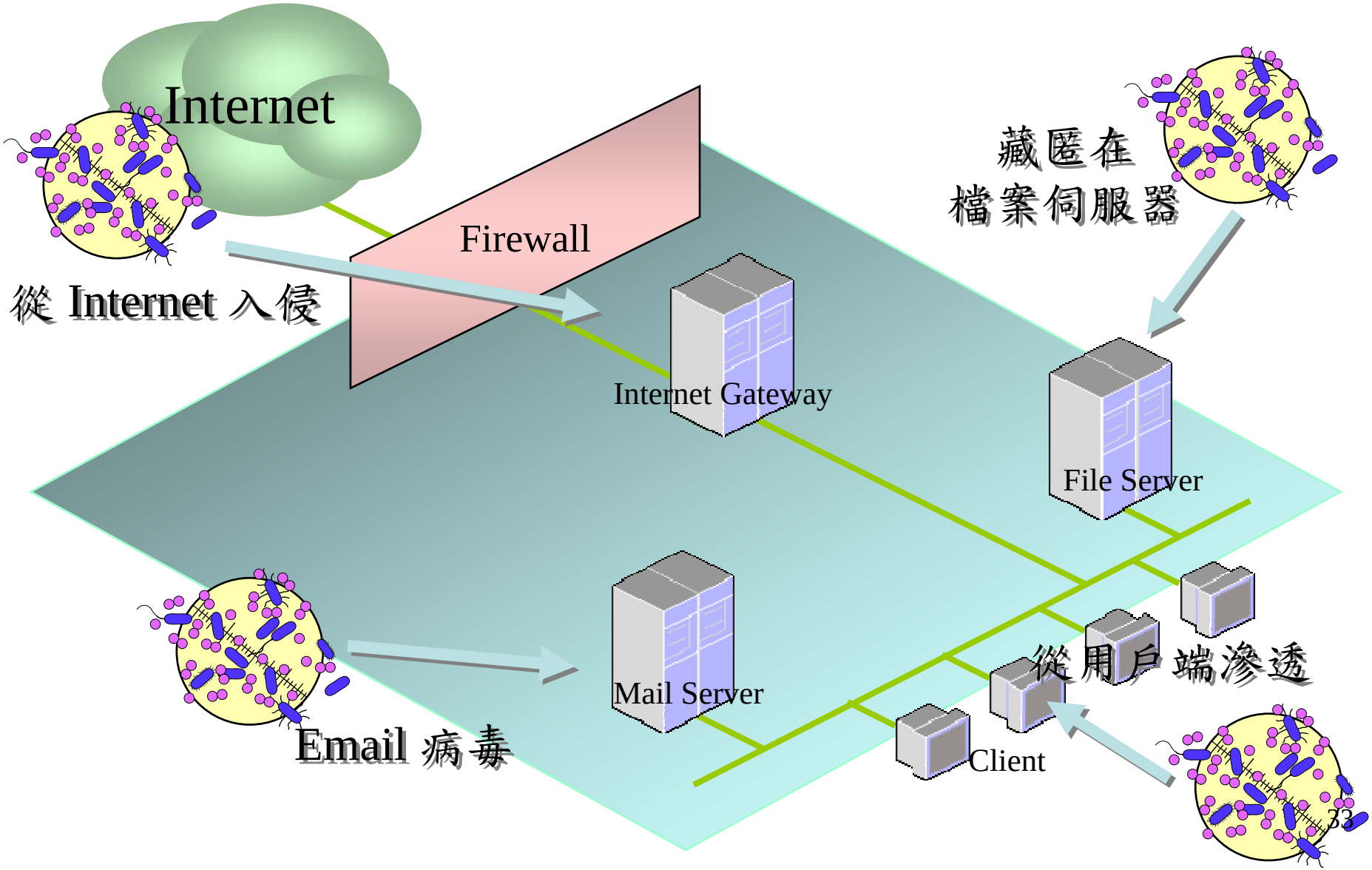


多元化的惡意程式攻擊方式

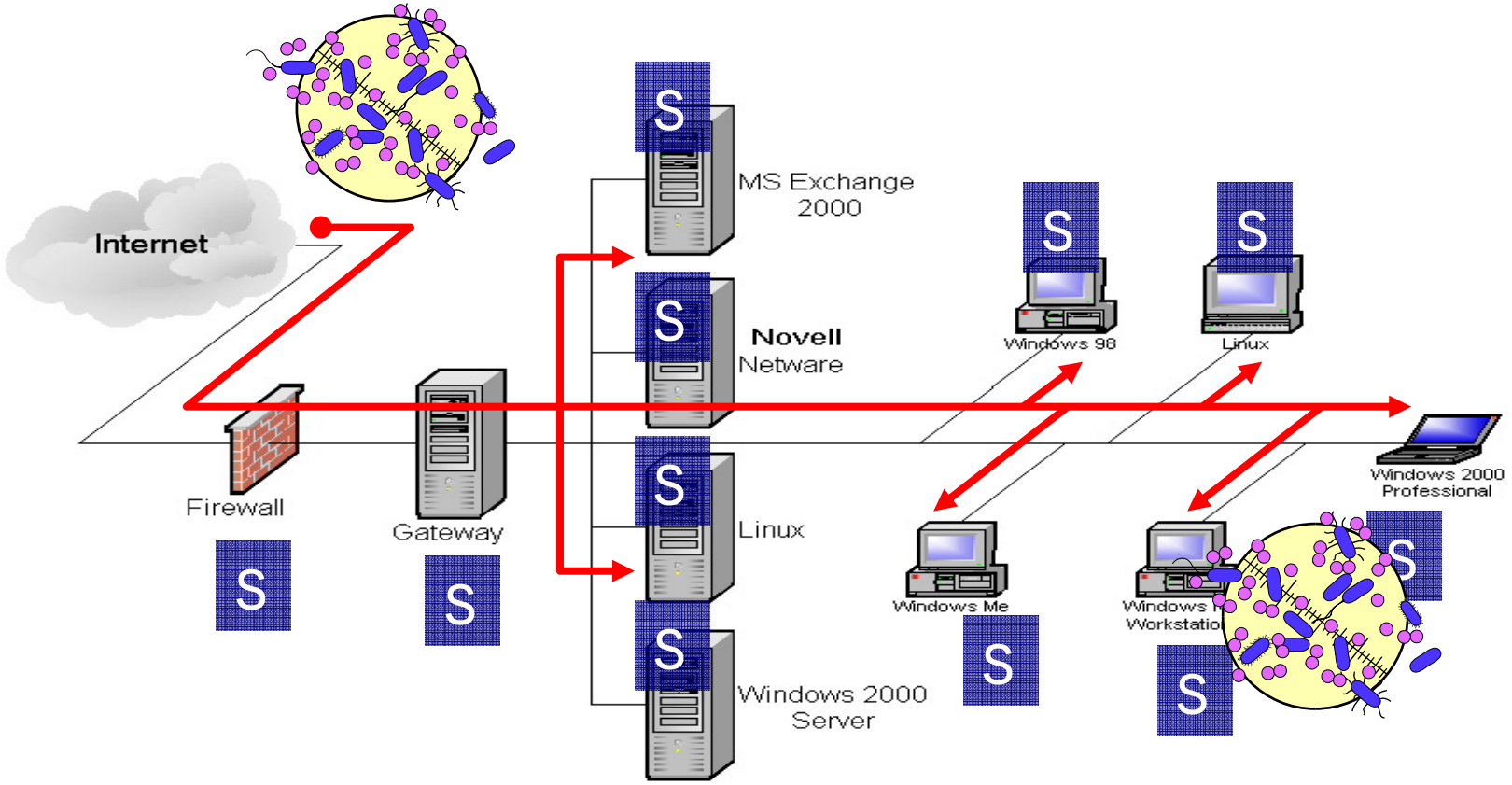


企業或機關正面臨多元化的惡意程式攻擊viruses, spyware, adware, hackers, dialers, password attacks

多元化的惡意程式攻擊管道

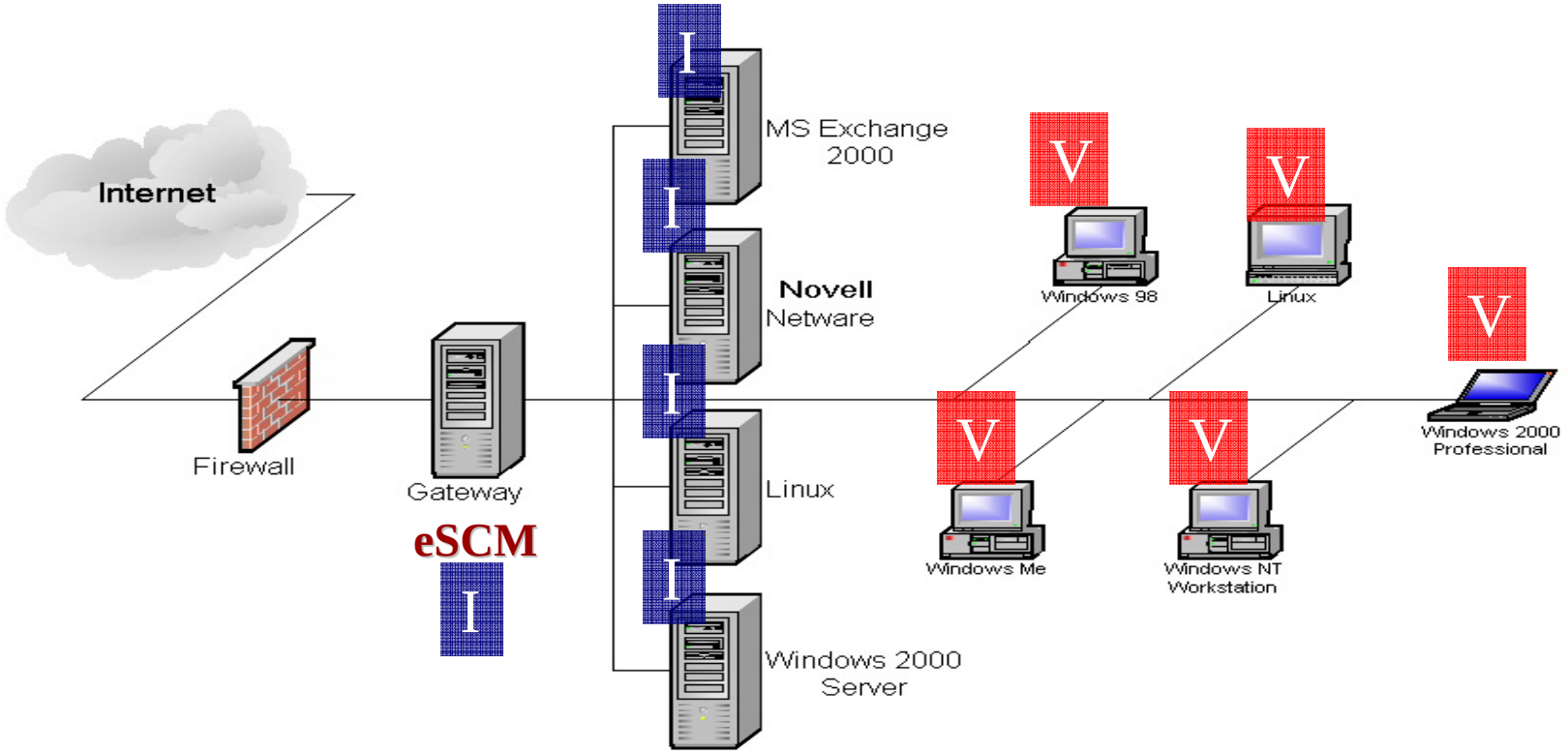


為什麼還有中毒事件？？？



只有單一掃毒引擎，病毒一旦攻破閘道大門，必定輕鬆長驅直入....

在不同的環節使用不同的產品



雙重掃毒引擎與病毒碼，有效提昇防毒安全等級

如何防範惡意程式

正確設定 IE 的安全層級

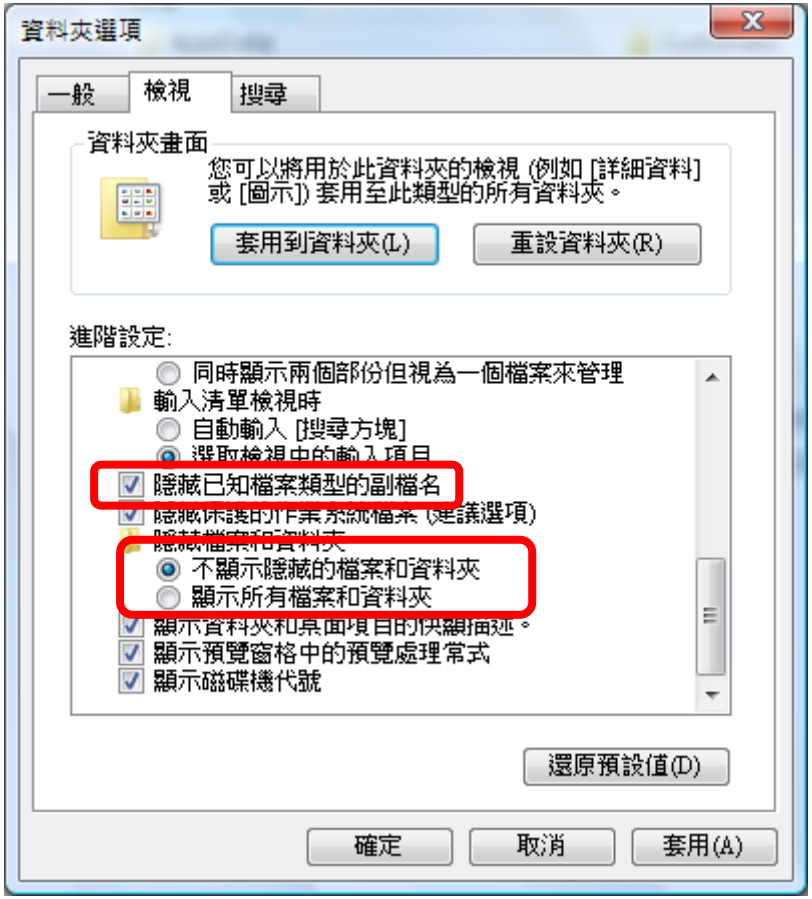
- IE 的安全層級設定至少是 [中安全性]，如此可降低意外執行惡意檔案的風險。
- 在 [中安全性] 的安全層級，Internet Explorer 會在執行內容可能不安全的檔案之前先提示使用者。
- Internet Explorer 也會在執行任何 ActiveX 控制項之前先顯示警告訊息

使用安全的電腦設定



- 有些檔案你可以不了解它的功能，但是
- 你不可以不知道它的存在

使用安全的電腦設定



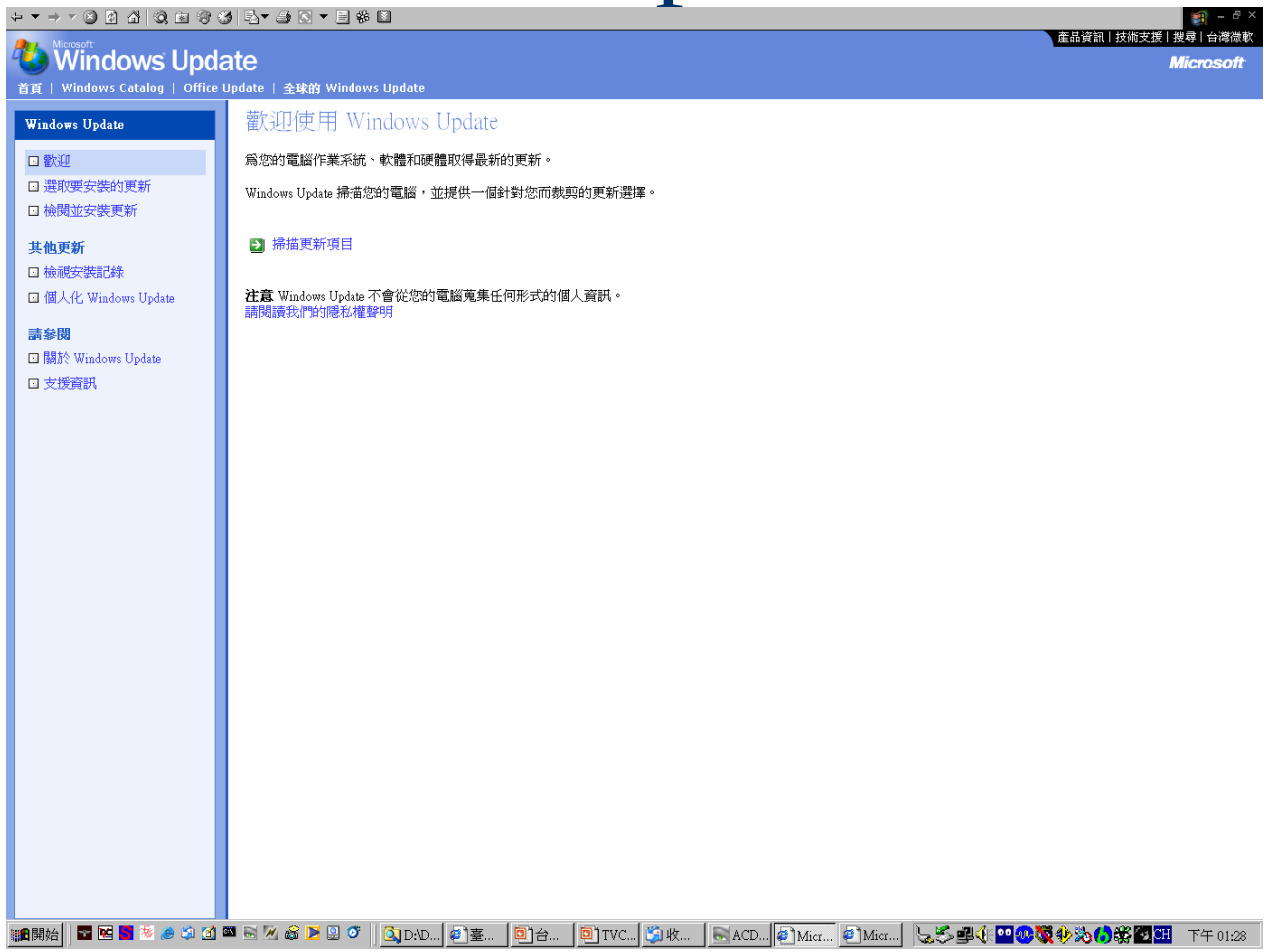
- 請取消「隱藏已知檔案類型的副檔名」
- 請選擇「顯示所有檔案的資料夾」

電腦開機後到底執行了哪些程式？

- 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程式侵擾。



安裝任何產品後請立刻檢查 patch



平時防毒該注意的小秘訣

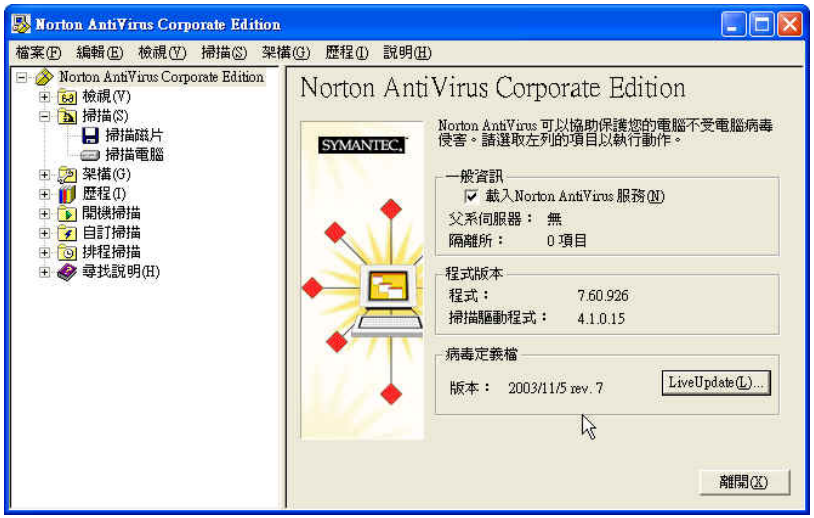
- 定期更改帳號與密碼，最好是英文加上數字，並不洩漏予他人
- 安裝最少的系統元件：降低被入侵的風險
- 遠離來路不明的軟體，檔案，磁片及光碟 ；並隨時注意電腦異常狀況
- 安裝防毒軟體：定期更新病毒碼、掃毒引擎及程式
- 定期備份

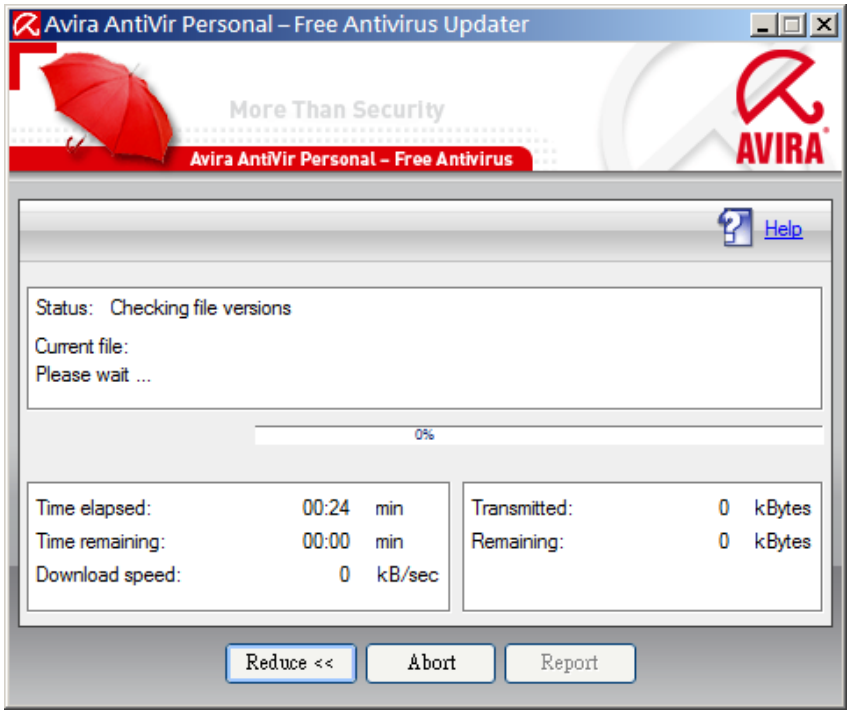
有效的預防措施



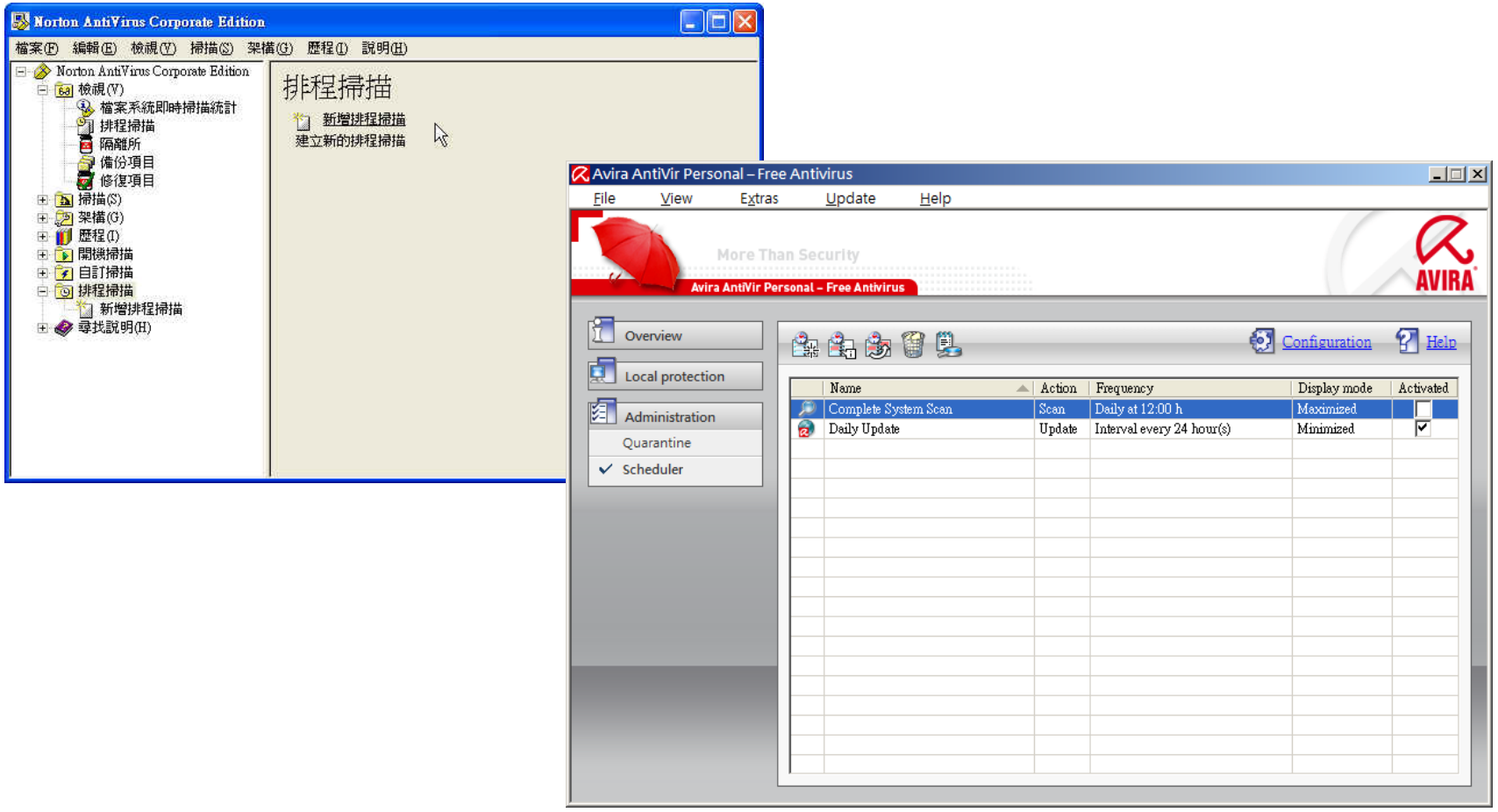
- 安裝防毒軟體來檢查病毒是否存在
- 不要使用來路不明的軟體
- 請勿從論壇或其他網站下載程式
- 定期掃毒
- 作業系統加裝密碼，防止他人隨意使用而中毒
- 觀察系統是否有無法解釋的改變

更新病毒碼


Norton AntiVirus Corporate Edition
檔案(F) 編輯(E) 檢視(V) 掃描(S) 架構(G) 歷程(I) 說明(H)
Norton AntiVirus Corporate Edition
檢視(V)
掃描(S)
掃描磁片
掃描電腦
架構(G)
歷程(I)
開機掃描
自訂掃描
排程掃描
尋找說明(H)
Norton AntiVirus Corporate Edition
SYMANTEC.
Norton AntiVirus 可以協助保護您的電腦不受電腦病毒侵害。請選取左列的項目以執行動作。
一般資訊
載入Norton AntiVirus 服務(N)
父系伺服器： 無
隔離所： 0 項目
程式版本
程式： 7.60.926
掃描驅動程式： 4.1.0.15
病毒定義檔
版本： 2003/11/5 rev. 7
LiveUpdate(L)...
離開(X)


Avira AntiVir Personal – Free Antivirus Updater
More Than Security
Avira AntiVir Personal – Free Antivirus
AVIRA
Help
Status: Checking file versions
Current file:
Please wait ...
0%
Time elapsed: 00:24 min
Time remaining: 00:00 min
Download speed: 0 kB/sec
Transmitted: 0 kBytes
Remaining: 0 kBytes
Reduce <<
Abort
Report

定期自動執行病毒掃描


Norton AntiVirus Corporate Edition
檔案(F) 編輯(E) 檢視(V) 掃描(S) 架構(G) 歷程(I) 說明(H)
Norton AntiVirus Corporate Edition
檢視(V)
檔案系統即時掃描統計
排程掃描
隔離所
備份項目
修復項目
掃描(S)
架構(G)
歷程(I)
開機掃描
自訂掃描
排程掃描
新增排程掃描
尋找說明(H)
排程掃描
新增排程掃描
建立新的排程掃描
Avira AntiVir Personal – Free Antivirus
File View Extras Update Help
More Than Security
Avira AntiVir Personal – Free Antivirus
AVIRA
Overview
Local protection
Administration
Quarantine
Scheduler
Configuration
Help
Name
Action
Frequency
Display mode
Activated
Complete System Scan
Scan
Daily at 12:00 h
Maximized
Daily Update
Update
Interval every 24 hour(s)
Minimized

免費線上掃毒

- Panda
  - http://www.pandasecurity.com/homeusers/solutions/activescan/?

Free online antivirus. Download ActiveScan 2.0 and clean your PC. Panda Security - Windows Internet Explorer

http://www.pandasecurity.com/homeusers/solutions/activescan/?

Free online antivirus. Download ActiveScan 2.0...

Panda Worldwide | About Panda | Contact

PANDA SECURITY — One step ahead.

Home Users | Enterprises | Partners

Products | Downloads | Store | Support | Security Info | Press Center

Home » Home Users » Products » Panda ActiveScan 2.0

Products

- Internet Security 2008
- Antivirus+Firewall 2008
- Antivirus 2008
- Panda Security for Linux
- ActiveScan 2.0
- TruPrevent Technologies
- Panda Services





Panda ActiveScan 2.0

Are you really sure that your PC is not infected?

ActiveScan 2.0 is an advanced online scanner based on Collective Intelligence (scanning in-the-cloud) that detects malware that traditional security solutions cannot detect.

- **Make sure your antivirus is offering you proper protection.**
- **Find hidden threats on your PC, such as rootkits, banker Trojans and malware designed to steal your identity.**
- **Simple, online disinfection of all malware detected on your PC.**

Scan your PC now

It's simple, fast and free.

Click "Scan your PC". And you'll see the benefits of this product immediately. If this is the first time you have used Panda Activescan, you will have to download the ActiveX controls.

Buy ActiveScan 2.0

Complete disinfection of all malicious software on your PC.

Get ActiveScan 2.0 to disinfect all types of malware from your PC.

Product data sheet | More information

Greater detection capacity

Panda ActiveScan 2.0 detects and eliminates more threats than traditional antivirus solutions thanks to its latest generation

網際網路 | 受保護模式: 關閉 100%

開始 下載 惡意程式防護介... 收件匣 - Microso... Free online antivi... 下午 02:43

免費線上掃毒

- Panda
  - http://www.pandasecurity.com/homeusers/solutions/activescan/?
- Kaspersky
  - http://www.kaspersky.com.tw/virusscanner/


KL - Windows Internet Explorer
http://www.kaspersky.com.tw/virusscanner/
Google
KL
KASPERSKY lab
Search
線上病毒掃描 | 下載免費防毒軟體 | 購買防毒軟體
產品介紹
購買資訊
網路威脅
下載專區
服務專區
夥伴專區
關於我們
服務專區
線上病毒掃描
技術支援服務
產品註冊(取得授權)
線上病毒掃描
常見問題解答
訂閱電子報
首頁 / 服務專區
免費線上病毒掃描
卡巴斯基線上病毒掃描 採用 Microsoft ActiveX 來掃描檢查您的電腦中是否存在有惡意程式. 掃描將利用微軟 Internet Explorer 來掃描您的連結在網路上的電腦, 其惡意程式的偵測能力就如同卡巴斯基的產品一樣.
請注意! 卡巴斯基線上掃瞄已經在 2006 年的 8 月 8 日改版. 如果您已經安裝了先前的版本, 則必須 先 移除之前的版本才能進行安裝新版本. 請利用"控制台"中的"新增移除程式"來移除舊版本的線上掃瞄程式。
開始下載安裝
Copyright © 1997 - 2008 Kaspersky Lab
技術支援專線:台灣 (886)(02)2791-5365
連絡我們 | 技術支援 | 可疑病毒回報
網際網路 | 受保護模式: 關閉
100%
開始
下載
惡意程式防護介...
收件匣 - Microso...
KL - Windows Int...
下午 02:45

免費線上掃毒

- Panda
  - http://www.pandasecurity.com/homeusers/solutions/activescan/?
- Kaspersky
  - http://www.kaspersky.com.tw/
- Trend Micro
  - http://tw.trendmicro.com/tw/products/personal/house-call/

HouseCall線上掃毒 - Trend Micro Taiwan - Windows Internet Explorer

http://tw.trendmicro.com/tw/products/personal/house-call/

Google

開始 書籤 拼字檢查 翻譯 傳送到 設定

HouseCall線上掃毒 - Trend Micro Taiwan

網頁(P) 工具(O)

This site is for visitors in **Taiwan** | 全球網站

網站地圖 | 關於趨勢 | 求職專區 | 與我們聯絡

搜尋: Go

TREND MICRO

快速連結 所有產品及解決方案 | 技術支援 | 購買 | 下載專區

首頁 | 個人/SOHO安全防護 | 小型企業安全防護 | 中型企業安全防護 | 大型企業安全防護 | 經銷夥伴

產品訊息/解決方案 | 技術支援 | 資安威脅 | 毒資新聞

- 家庭與個人工作室解決方案
  - HouseCall 線上掃毒
    - 產品功能

列印此頁

HouseCall線上掃毒



新版線上掃毒除駭服務全新上市！對於立即有掃毒解毒需求、擔心電腦暗藏間諜程式和系統弱點的使用者，只要簡單的透過上網，您不但可以快速地針對您的電腦進行線上掃毒、解毒外，新版HouseCall更能幫助您將間諜程式、廣告軟體等惡意程式碼一併掃瞄與移除，避免您的帳號、密碼等隱私資料遭竊！還提供最新的安全弱點偵測功能，可以掃瞄電腦中的系統安全漏洞，協助您立即更新修正程式，避免駭客或網路病毒趁機攻擊入侵電腦，給您一個安全無毒、無駭的上網安全環境。

結合掃毒、保護隱私、安全檢查三效合一，全新上市！

產品特色

擔心電腦中毒、個人帳號密碼遭竊嗎？快來線上掃毒、除駭一下吧！

個人採購資訊

- 線上購買
- 線上續約
- 宅配免運費送到家
- 查詢經銷商
- 聯絡趨勢科技

哪裡直接線上購買？

- HiNet
- PC Home
- Seednet
- 台灣固網
- So-net

相關資訊

- HouseCall線上掃毒除駭包

http://tw.trendmicro.com/tw/home/enterprise

網際網路 | 受保護模式: 關閉 100%

開始 下載 惡意程式防護介... 收件匣 - Microso... HouseCall線上掃... 下午 02:48

免費線上掃毒

- Panda
  - http://www.pandasecurity.com/homeusers/solutions/activescan/?
- Kaspersky
  - http://www.kaspersky.com.tw/
- Trend Micro
  - http://tw.trendmicro.com/tw/products/personal/house-call/
- McAfee
  - http://tw.mcafee.com/root/mfs/default.asp


McAfee – 用於個人電腦的電腦防毒軟體和網際網路安全性產品 - Windows Internet Explorer
http://tw.mcafee.com/root/mfs/default.asp
McAfee – 用於個人電腦的電腦防毒軟體和網際網...
McAfee
全球網站 | 關於 McAfee | 與我們聯絡 | 搜尋
McAfee SECURE
每日認證 7月14日
家庭與家庭辦公室 中小型企業 | 企業 | 合作夥伴
產品 | 病毒資訊 | 支援 | 下載
我的帳戶 | 登入
產品
Total Protection
Internet Security Suite
VirusScan Plus
SiteAdvisor Plus
免費服務
SiteAdvisor
FreeScan
World Virus Map
FreeScan
McAfee FreeScan 可幫助您偵測出電腦上數千種的病毒。以屢獲獎賞的 McAfee VirusScan 引擎為基礎，FreeScan 可搜尋多種病毒 (包括最新發現的「in the wild」病毒)，並可顯示所有已感染病毒的檔案之詳細清單。如果發現病毒，FreeScan 還會提供連結，以提供病毒的詳細資訊，以及您該如何進行清理系統的工作。
使用者授權合約
所有使用者請注意：請仔細閱讀本合約。如果貴用戶 (個人或法人團體) 按一下 [接受] 按鈕或安裝軟體，即表示同意本合約與您簽署的任何書面合約一樣具有可執行性。如果貴用戶不同意接受本合約，請按一下表示不接受本合約條款的按鈕，而且請勿安裝軟體。如果您購買的軟體是存放在實體媒體上 (例如 CD) 而沒有機會檢視本授權，而且您不接受本合約，則在下列條件下，您可以獲得原始付款金額的退款：(A) 沒有使用本軟體，並且 (B) 從購買日起算的三十 (30) 天內，將本軟體及付款證明一
立即掃描
附註：McAfee FreeScan 是給 McAfee 成員的一項附贈服務。
產品資訊
優點與系統需求
如何使用 FreeScan
相關服務
VirusScan Plus
Internet Security Suite
Total Protection
完成
網際網路 | 受保護模式: 關閉
100%
開始
惡意程式防護介...
收件匣 - Microso...
McAfee – 用於個...
個人化
下午 03:11

免費工具

- 趨勢 System Cleaner
  - http://www.trendmicro.com/download/zh-tw/tsc.asp


Trend Micro - Windows Internet Explorer
http://www.trendmicro.com/download/zh-tw/tsc.asp
Google
Trend Micro
This site is for visitors in Taiwan | 全球網站
網站地圖 | 關於趨勢 | 求職專區 | 與我們聯絡
搜尋:
Go
TREND MICRO
快速連結 所有產品及解決方案 | 技術支援 | 購買 | 下載專區
首頁 | 個人/SOHO安全防護 | 小型企業安全防護 | 中型企業安全防護 | 大型企業安全防護
Trend Micro System Cleaner
2008/07/10, 目前最新的TSC病毒碼是 966, 及掃描引擎是 5.32.
趨勢科技的產品使用者 請下載 Trend Micro System Cleaner Patch.
› tsc.zip 2.1MB
適用於 PC-cillin2002 或以上版本, OfficeScan V5.02 或以上版本, ServerProtect 5.x
如何更新 TSC 請參閱下列說明文件
PC-cillin2002或以上版本
OfficeScan 5.x
ServerProtect 5.x
非趨勢科技的產品使用者 請下載 Trend Micro System Cleaner Package.
› SYSCLEAN.COM 4.5MB
MD5 checksum: 360ef072099c8b95c72ca7cfbbeb1f2f
請與病毒碼放至於同一目錄下, 即可執行, 詳細資訊請參閱 readme_sysclean.txt
TSC與SYSCLEAN之差異
完成
網際網路 | 受保護模式: 關閉
100%
開始
惡意程式防護介紹.pptx
收件匣 - Microsoft Ou...
Trend Micro - Windo...
下午 03:07

免費工具

- 趨勢 System Cleaner
  - http://www.trendmicro.com/download/zh-tw/tsc.asp
- Windows Live OneCare
  - http://safety.live.com/site/zh-tw/default.htm

Windows Live OneCare 安全掃描：確保電腦安全的免費線上掃描服務 - Windows Internet Explorer

http://onecare.live.com/site/zh-tw/default.htm

Windows Live OneCare 安全掃描：確保電腦安...

Windows Live™ 首頁 Hotmail Spaces OneCare | MSN 搜尋

OneCare ▸ 安全掃描工具 語言 | 說明

- 安全掃描工具
- 防護
- 清理
- 維護
- 新發行

免費電腦安全掃描，防護個人資訊安全

Windows Live OneCare 安全掃描工具是全新的**免費**服務，協助您全方位防護個人資訊安全。

- 針對電腦病毒、安全漏洞、間諜軟體，提供創新全方位掃描與清除服務
- 偵測與移除老舊無用檔案，並搭配硬碟重組功能，大幅提升電腦系統執行效能
- 有效強化資訊安全，提供個人用戶高效能的資訊安全防護新體驗

最新消息：Windows Vista 使用者，歡迎試用專屬的安全掃描 Beta 版 服務。

修復特定電腦問題

使用完整掃描服務檢查電腦的所有問題。要修復您電腦上的特定問題，請指定以下特定的掃描類型。

ABN·AMRO 荷蘭銀行

在三大時尚通路
刷荷蘭銀行Shop&Dine白金卡
最高 5 倍積點 極速轉動

現在立即申請



體驗更多 Beta 版本產品

試用更多 Beta 版本產品，了解 Windows Live 如何提供更佳的線上服務。 移至 Windows Live 搶鮮版網頁

網際網路 | 受保護模式: 關閉 100%

開始 惡意程式防護介紹.pptx 收件匣 - Microsoft Ou... Windows Live OneCar... 下午 03:07

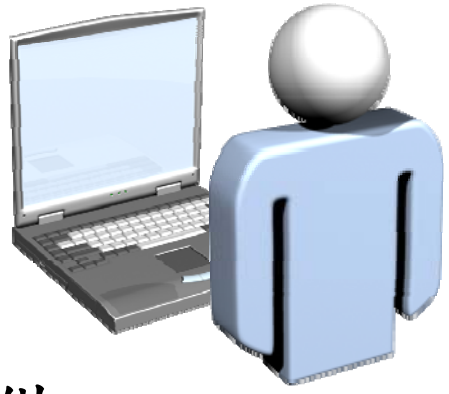
免費工具

- 趨勢 System Cleaner
  - http://www.trendmicro.com/download/zh-tw/tsc.asp
- Windows Live OneCare
  - http://safety.live.com/site/zh-tw/default.htm
- 清除 AdWare 工具
  - Ad-Aware 2008 Free Edition
    - http://lavasoft.com/single/trialpay.php


Get Ad-Aware 2008 Plus for Free with Lavasoft and TrialPay - Lavasoft - Windows Internet Explorer
http://lavasoft.com/single/trialpay.php
Google
Get Ad-Aware 2008 Plus for Free with Lavasoft ...
LAVASOFT
Continue to download
Ad-Aware® 2008 Free
Download
Or...
Get Ad-Aware® 2008 Plus
NOW FREE!
Reg. $26.95
Get Plus for Free
Powered By trialpay
Ad-Aware® 2008 Plus Features
With integrated anti-virus, real-time monitoring, and over 1.2 million threats in detection, Ad-Aware 2008 provides superior protection against the sophisticated
Plus vs Free
Anti-Virus Protection
Extended Threat
完成
網際網路 | 受保護模式: 關閉
100%
開始
下載
惡意程式防護介...
收件匣 - Microso...
Get Ad-Aware 2...
下午 02:53

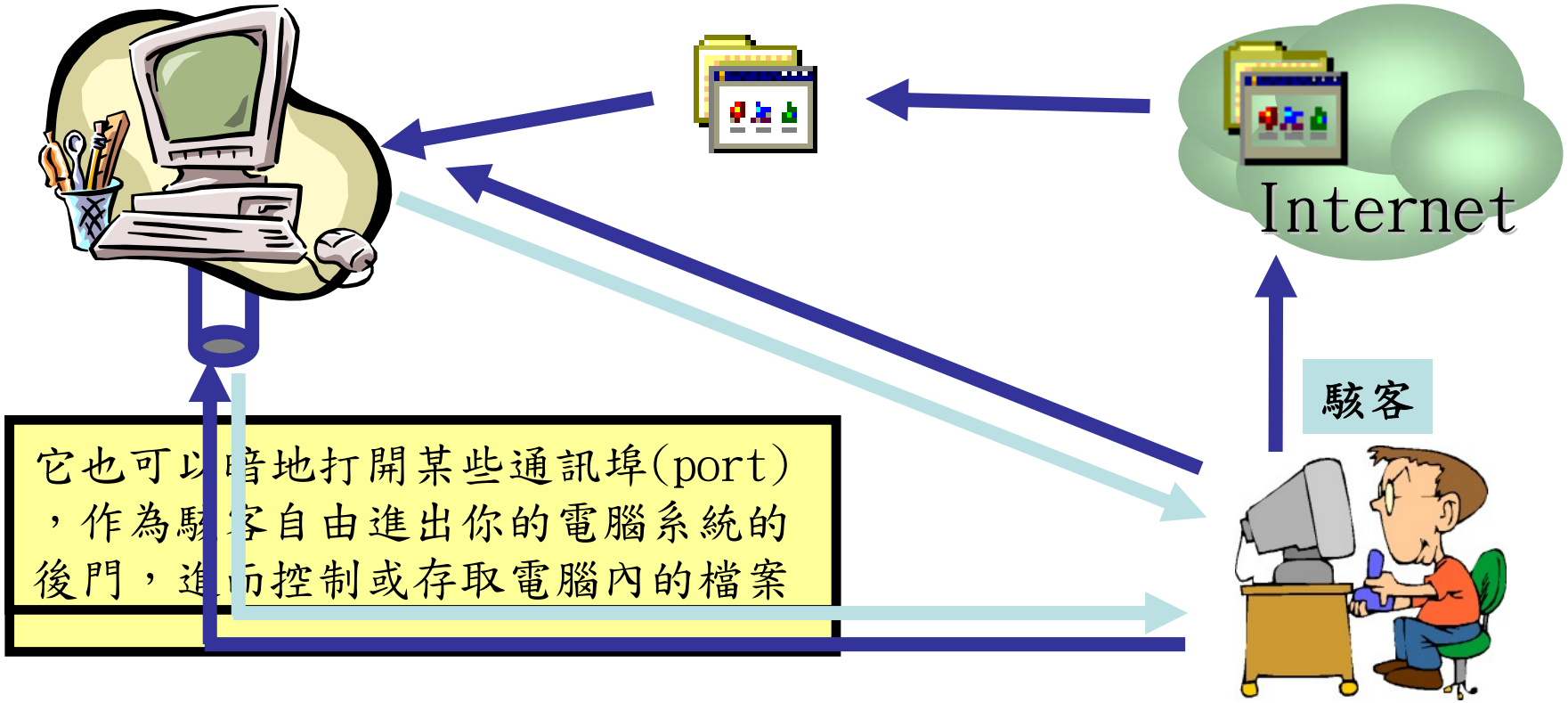
當系統已中毒時，我該怎麼做?

- 關掉電源，最少等待一分鐘再開機
- 移去所有外接儲存媒體
- 卸除所有的週邊裝置
- 所有的磁片貼上防寫標籤
- 將還原光碟放入光磁機中
- 系統還原後再接上所有的週邊設備



如何發現未知惡意程式

木馬程式運作概念



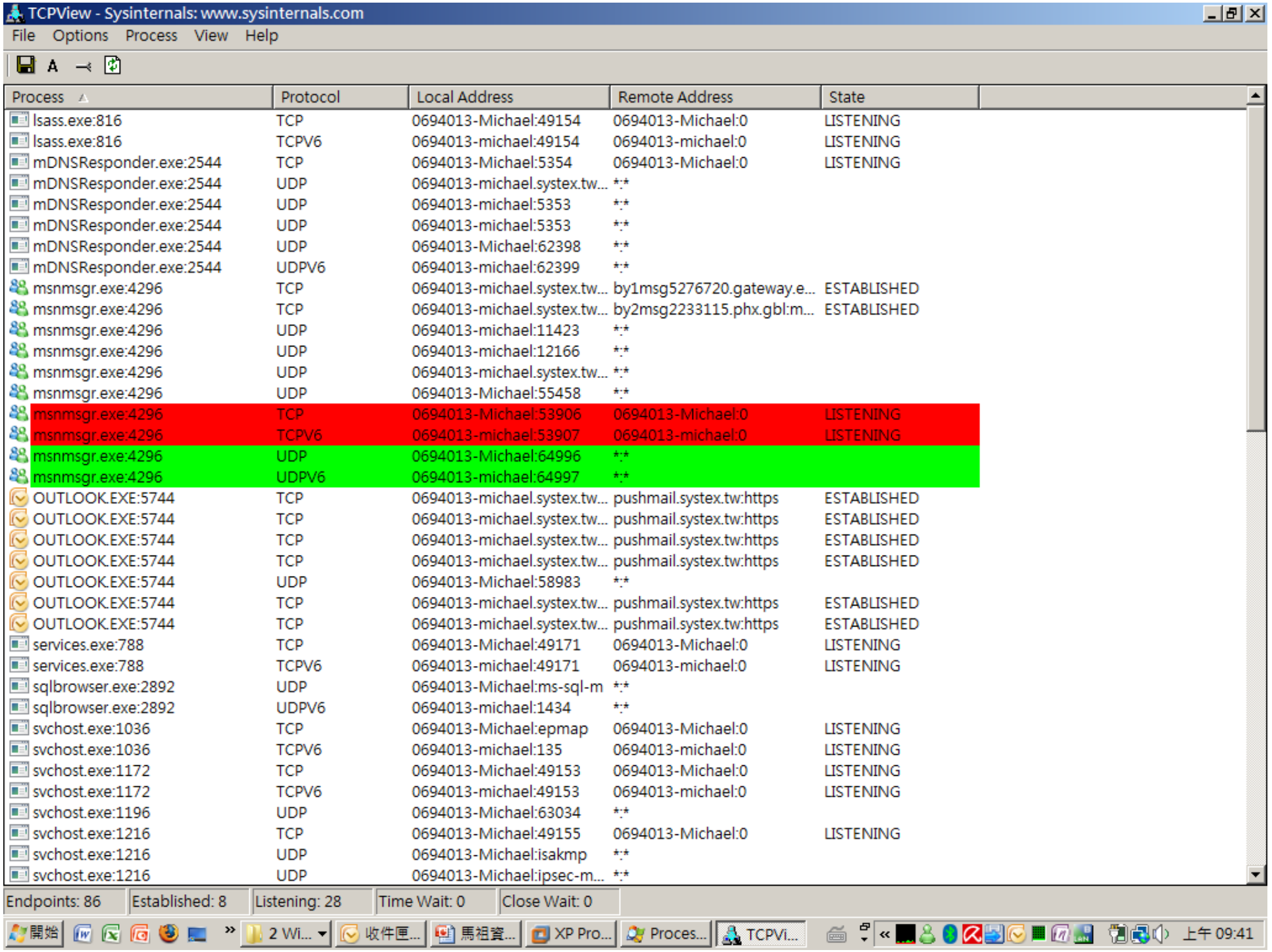
木馬程式：惡意程式的一種，利用開啟被害者電腦後門而達到遙控或竊取資訊的目的。

木馬程式的基本特徵

- 自動執行系統以外的 process
- 對外連線；傳送資料

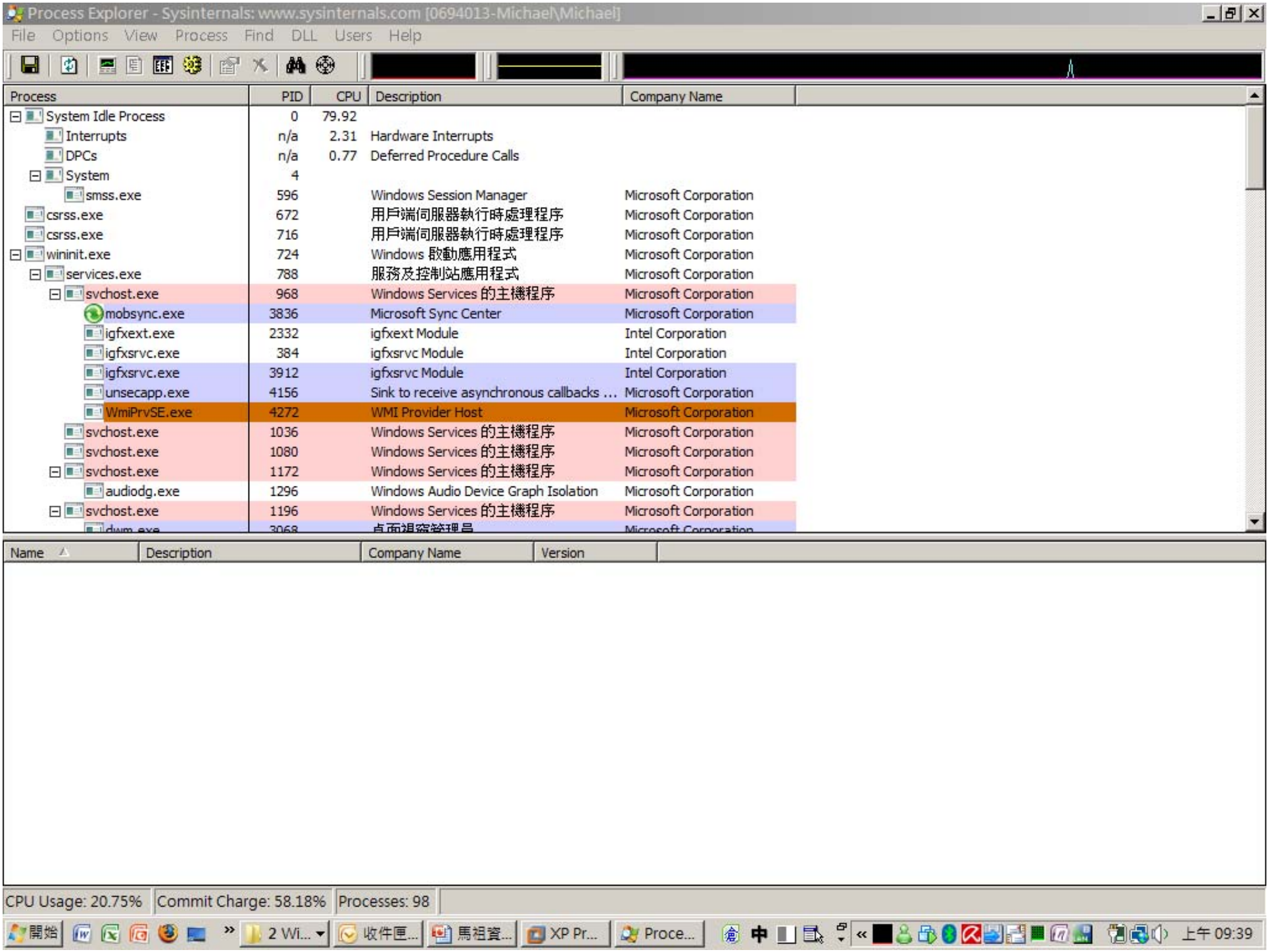
工具介紹

工具類別	工具名稱	參考/下載網址
網路檢測	TCPView	http://www.microsoft.com/technet/sysinternals/Networking/TcpView.mspx
程序檢測	Process Explorer	http://www.microsoft.com/technet/sysinternals/ProcessesAndThreads/ProcessExplorer.mspx
啟動途徑檢測	Autoruns	http://www.microsoft.com/technet/sysinternals/SystemInformation/Autoruns.mspx


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process Protocol Local Address Remote Address State
lsass.exe:816 TCP 0694013-Michael:49154 0694013-Michael:0 LISTENING
lsass.exe:816 TCPV6 0694013-michael:49154 0694013-michael:0 LISTENING
mDNSResponder.exe:2544 TCP 0694013-Michael:5354 0694013-Michael:0 LISTENING
mDNSResponder.exe:2544 UDP 0694013-michael.systex.tw... *:*
mDNSResponder.exe:2544 UDP 0694013-michael:5353 *:*
mDNSResponder.exe:2544 UDP 0694013-michael:5353 *:*
mDNSResponder.exe:2544 UDP 0694013-Michael:62398 *:*
mDNSResponder.exe:2544 UDPV6 0694013-michael:62399 *:*
msnmsgr.exe:4296 TCP 0694013-michael.systex.tw... by1msg5276720.gateway.e... ESTABLISHED
msnmsgr.exe:4296 TCP 0694013-michael.systex.tw... by2msg2233115.phx.gbl:m... ESTABLISHED
msnmsgr.exe:4296 UDP 0694013-michael:11423 *:*
msnmsgr.exe:4296 UDP 0694013-michael:12166 *:*
msnmsgr.exe:4296 UDP 0694013-michael.systex.tw... *:*
msnmsgr.exe:4296 UDP 0694013-Michael:55458 *:*
msnmsgr.exe:4296 TCP 0694013-Michael:53906 0694013-Michael:0 LISTENING
msnmsgr.exe:4296 TCPV6 0694013-michael:53907 0694013-michael:0 LISTENING
msnmsgr.exe:4296 UDP 0694013-Michael:64996 *:*
msnmsgr.exe:4296 UDPV6 0694013-michael:64997 *:*
OUTLOOK.EXE:5744 TCP 0694013-michael.systex.tw... pushmail.systex.tw:https ESTABLISHED
OUTLOOK.EXE:5744 TCP 0694013-michael.systex.tw... pushmail.systex.tw:https ESTABLISHED
OUTLOOK.EXE:5744 TCP 0694013-michael.systex.tw... pushmail.systex.tw:https ESTABLISHED
OUTLOOK.EXE:5744 TCP 0694013-michael.systex.tw... pushmail.systex.tw:https ESTABLISHED
OUTLOOK.EXE:5744 UDP 0694013-Michael:58983 *:*
OUTLOOK.EXE:5744 TCP 0694013-michael.systex.tw... pushmail.systex.tw:https ESTABLISHED
OUTLOOK.EXE:5744 TCP 0694013-michael.systex.tw... pushmail.systex.tw:https ESTABLISHED
services.exe:788 TCP 0694013-Michael:49171 0694013-Michael:0 LISTENING
services.exe:788 TCPV6 0694013-michael:49171 0694013-michael:0 LISTENING
sqlbrowser.exe:2892 UDP 0694013-Michael:ms-sql-m *:*
sqlbrowser.exe:2892 UDPV6 0694013-michael:1434 *:*
svchost.exe:1036 TCP 0694013-Michael:epmap 0694013-Michael:0 LISTENING
svchost.exe:1036 TCPV6 0694013-michael:135 0694013-michael:0 LISTENING
svchost.exe:1172 TCP 0694013-Michael:49153 0694013-Michael:0 LISTENING
svchost.exe:1172 TCPV6 0694013-michael:49153 0694013-michael:0 LISTENING
svchost.exe:1196 UDP 0694013-Michael:63034 *:*
svchost.exe:1216 TCP 0694013-Michael:49155 0694013-Michael:0 LISTENING
svchost.exe:1216 UDP 0694013-Michael:isakmp *:*
svchost.exe:1216 UDP 0694013-Michael:ipsec-m... *:*
Endpoints: 86 Established: 8 Listening: 28 Time Wait: 0 Close Wait: 0
開始
2 Wi...
收件匣...
馬祖資...
XP Pro...
Proces...
TCPVi...
上午 09:41

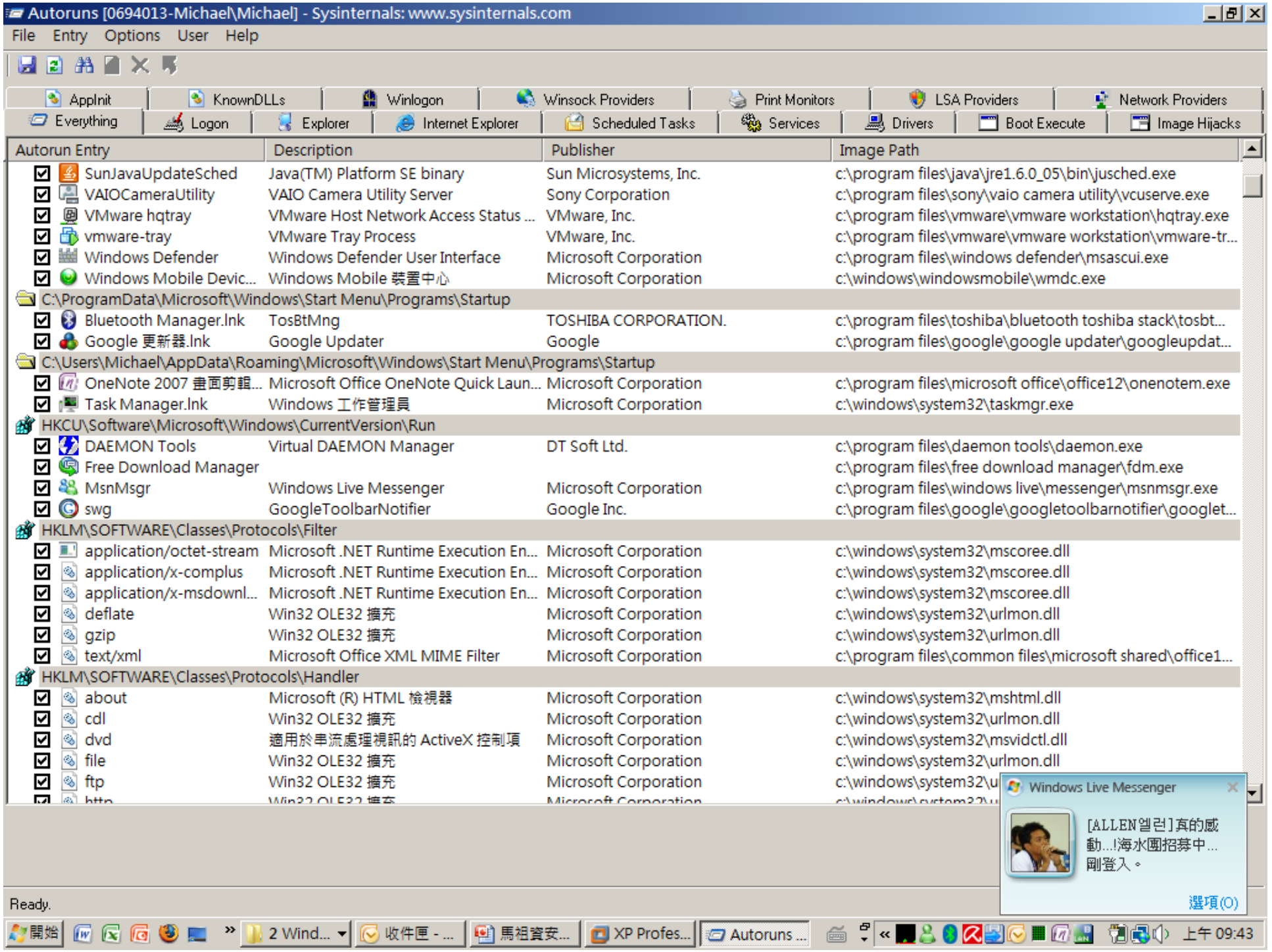
TCPView

- 檢查重點
- 是否有不明的對外連線


Process Explorer - Sysinternals: www.sysinternals.com [0694013-Michael\Michael]
File Options View Process Find DLL Users Help
Process PID CPU Description Company Name
System Idle Process 0 79.92
Interrupts n/a 2.31 Hardware Interrupts
DPCs n/a 0.77 Deferred Procedure Calls
System 4
smss.exe 596 Windows Session Manager Microsoft Corporation
csrss.exe 672 用戶端伺服器執行時處理程序 Microsoft Corporation
csrss.exe 716 用戶端伺服器執行時處理程序 Microsoft Corporation
wininit.exe 724 Windows 啟動應用程式 Microsoft Corporation
services.exe 788 服務及控制站應用程式 Microsoft Corporation
svchost.exe 968 Windows Services 的主機程序 Microsoft Corporation
mobsync.exe 3836 Microsoft Sync Center Microsoft Corporation
igfxext.exe 2332 igfxext Module Intel Corporation
igfxsrvc.exe 384 igfxsrvc Module Intel Corporation
igfxsrvc.exe 3912 igfxsrvc Module Intel Corporation
unsecapp.exe 4156 Sink to receive asynchronous callbacks ... Microsoft Corporation
WmiPrvSE.exe 4272 WMI Provider Host Microsoft Corporation
svchost.exe 1036 Windows Services 的主機程序 Microsoft Corporation
svchost.exe 1080 Windows Services 的主機程序 Microsoft Corporation
svchost.exe 1172 Windows Services 的主機程序 Microsoft Corporation
audiodg.exe 1296 Windows Audio Device Graph Isolation Microsoft Corporation
svchost.exe 1196 Windows Services 的主機程序 Microsoft Corporation
Name Description Company Name Version
CPU Usage: 20.75% Commit Charge: 58.18% Processes: 98
開始
2 Wi...
收件匣...
馬祖資...
XP Pr...
Proce...
上午 09:39

Process Explorers

- 檢查重點
- 列出的 process 中
  - 空白的公司名稱或說明
  - 未知的 process

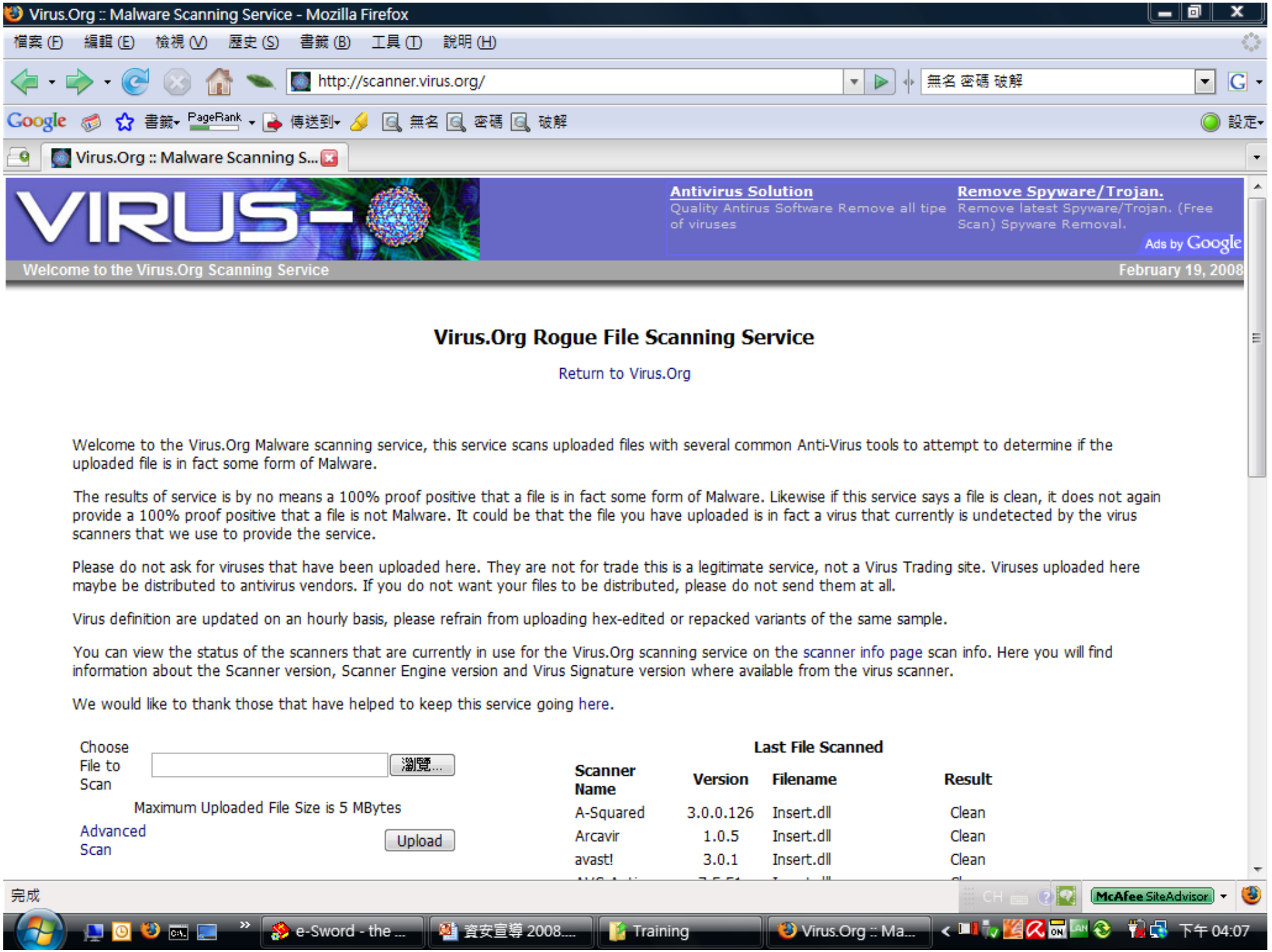

Autoruns [0694013-Michael\Michael] - Sysinternals: www.sysinternals.com
File Entry Options User Help
AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers Network Providers
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Boot Execute Image Hijacks
Autorun Entry Description Publisher Image Path
SunJavaUpdateSched Java(TM) Platform SE binary Sun Microsystems, Inc. c:\program files\java\jre1.6.0_05\bin\jusched.exe
VAIOCameraUtility VAIO Camera Utility Server Sony Corporation c:\program files\sony\vaio camera utility\vcuserve.exe
VMware hqtray VMware Host Network Access Status ... VMware, Inc. c:\program files\vmware\vmware workstation\hqtray.exe
vmware-tray VMware Tray Process VMware, Inc. c:\program files\vmware\vmware workstation\vmware-tr...
Windows Defender Windows Defender User Interface Microsoft Corporation c:\program files\windows defender\msascui.exe
Windows Mobile Devic... Windows Mobile 裝置中心 Microsoft Corporation c:\windows\windowsmobile\wmdc.exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Bluetooth Manager.lnk TosBtMng TOSHIBA CORPORATION. c:\program files\toshiba\bluetooth toshiba stack\tosbt...
Google 更新器.lnk Google Updater Google c:\program files\google\google updater\googleupdat...
C:\Users\Michael\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
OneNote 2007 畫面剪輯... Microsoft Office OneNote Quick Laun... Microsoft Corporation c:\program files\microsoft office\office12\onenotem.exe
Task Manager.lnk Windows 工作管理員 Microsoft Corporation c:\windows\system32\taskmgr.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
DAEMON Tools Virtual DAEMON Manager DT Soft Ltd. c:\program files\daemon tools\daemon.exe
Free Download Manager c:\program files\free download manager\fdm.exe
MsnMsgr Windows Live Messenger Microsoft Corporation c:\program files\windows live\messenger\msnmsgr.exe
swg GoogleToolbarNotifier Google Inc. c:\program files\google\googletoolbarnotifier\googlet...
HKLM\SOFTWARE\Classes\Protocols\Filter
application/octet-stream Microsoft .NET Runtime Execution En... Microsoft Corporation c:\windows\system32\mscoree.dll
application/x-complus Microsoft .NET Runtime Execution En... Microsoft Corporation c:\windows\system32\mscoree.dll
application/x-msdownl... Microsoft .NET Runtime Execution En... Microsoft Corporation c:\windows\system32\mscoree.dll
deflate Win32 OLE32 擴充 Microsoft Corporation c:\windows\system32\urlmon.dll
gzip Win32 OLE32 擴充 Microsoft Corporation c:\windows\system32\urlmon.dll
text/xml Microsoft Office XML MIME Filter Microsoft Corporation c:\program files\common files\microsoft shared\office1...
HKLM\SOFTWARE\Classes\Protocols\Handler
about Microsoft (R) HTML 檢視器 Microsoft Corporation c:\windows\system32\mshtml.dll
cdl Win32 OLE32 擴充 Microsoft Corporation c:\windows\system32\urlmon.dll
dvd 適用於串流處理視訊的 ActiveX 控制項 Microsoft Corporation c:\windows\system32\msvidctl.dll
file Win32 OLE32 擴充 Microsoft Corporation c:\windows\system32\urlmon.dll
ftp Win32 OLE32 擴充 Microsoft Corporation c:\windows\system32\u
Windows Live Messenger
[ALLEN엘런]真的感動...!海水團招募中...
剛登入。
選項(O)
Ready.
開始
2 Wind...
收件匣 - ...
馬祖資安...
XP Profes...
Autoruns ...
上午 09:43

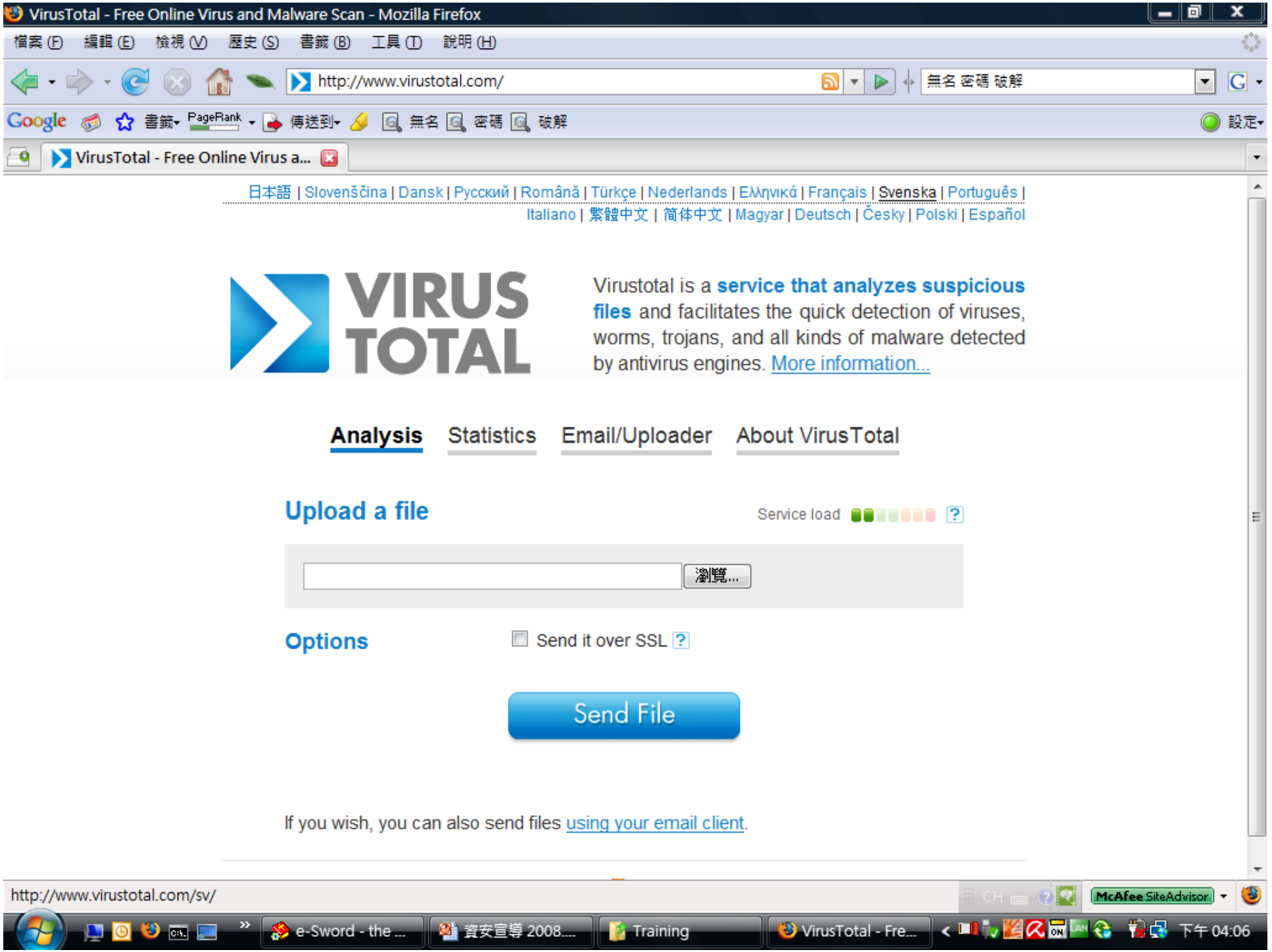
AutoRuns

- 檢查重點
- 開機時，自動執行的程式中，是否有
  - 空白的公司名稱或說明
  - 未知的程式

發現可疑檔案處理方式

- 將檔案交給資訊人員
- 檢查可疑檔案的網站
  - http://scanner.virus.org
  - http://www.virustotal.com


Virus.Org :: Malware Scanning Service - Mozilla Firefox
檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
http://scanner.virus.org/
無名 密碼 破解
Google 書籤 PageRank 傳送到 無名 密碼 破解 設定
Virus.Org :: Malware Scanning S...
VIRUS-
Antivirus Solution
Quality Antirus Software Remove all tipe of viruses
Remove Spyware/Trojan.
Remove latest Spyware/Trojan. (Free Scan) Spyware Removal.
Ads by Google
Welcome to the Virus.Org Scanning Service
February 19, 2008
Virus.Org Rogue File Scanning Service
Return to Virus.Org
Welcome to the Virus.Org Malware scanning service, this service scans uploaded files with several common Anti-Virus tools to attempt to determine if the uploaded file is in fact some form of Malware.
The results of service is by no means a 100% proof positive that a file is in fact some form of Malware. Likewise if this service says a file is clean, it does not again provide a 100% proof positive that a file is not Malware. It could be that the file you have uploaded is in fact a virus that currently is undetected by the virus scanners that we use to provide the service.
Please do not ask for viruses that have been uploaded here. They are not for trade this is a legitimate service, not a Virus Trading site. Viruses uploaded here maybe be distributed to antivirus vendors. If you do not want your files to be distributed, please do not send them at all.
Virus definition are updated on an hourly basis, please refrain from uploading hex-edited or repacked variants of the same sample.
You can view the status of the scanners that are currently in use for the Virus.Org scanning service on the scanner info page scan info. Here you will find information about the Scanner version, Scanner Engine version and Virus Signature version where available from the virus scanner.
We would like to thank those that have helped to keep this service going here.
Choose File to Scan
瀏覽...
Maximum Uploaded File Size is 5 MBytes
Advanced Scan
Upload
Last File Scanned
Scanner Name
Version
Filename
Result
A-Squared 3.0.0.126 Insert.dll Clean
Arcavir 1.0.5 Insert.dll Clean
avast! 3.0.1 Insert.dll Clean
完成
McAfee SiteAdvisor
e-Sword - the ...
資安宣導 2008....
Training
Virus.Org :: Ma...
下午 04:07


VirusTotal - Free Online Virus and Malware Scan - Mozilla Firefox
檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (T) 說明 (H)
http://www.virustotal.com/
無名 密碼 破解
Google 書籤 PageRank 傳送到 無名 密碼 破解 設定
VirusTotal - Free Online Virus a...
日本語 | Slovenščina | Dansk | Русский | Română | Türkçe | Nederlands | Ελληνικά | Français | Svenska | Português | Italiano | 繁體中文 | 简体中文 | Magyar | Deutsch | Česky | Polski | Español
VIRUS TOTAL
Virustotal is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...
Analysis Statistics Email/Uploader About VirusTotal
Upload a file
Service load
瀏覽...
Options
Send it over SSL
Send File
If you wish, you can also send files using your email client.
http://www.virustotal.com/sv/
McAfee SiteAdvisor
e-Sword - the ...
資安宣導 2008....
Training
VirusTotal - Fre...
下午 04:06

問題與討論