麟瑞科技
RING LINE CORPORATION

惡意程式分析

Solutions

Services

系統整合、資訊服務的第一選擇

Agenda

- 惡意程式介紹
- 惡意程式手法分析
- 惡意程式分析工具
- USB 病毒攻擊手法分析
- 實際案例探討
- 從郵件安全角度看惡意程式
- 如何預防惡意程式
- 結論

惡意程式介紹

存在於電腦和網路中的威脅

- 惡意軟體
- 系統弱點
- 資源分享
- 非法軟體
- 防毒軟體
- 廣告軟體
- 垃圾郵件
- 釣魚網站
- 駭客攻擊
- 操作習慣

惡意程式 (Malware)

惡意程式是由電腦程式或一段可卸除程式碼(Code)所組成，並試圖攻擊、侵入、破壞電腦系統、 存取相關資源，但確未經使用者授權或是未提示及通知使用者的行為。

惡意程式的演進

Malware History

1985	Virus
1995	Macro Virus
1999	Internet Worm Backdoor
2005	Bots
2007	Spyware

惡意程式的特性

- 自我複製與感染物件
- 刪除檔案
- 強制安裝且難以移除
- 首頁綁架(hi jacking)與廣告彈出
- 搜集使用者與系統資訊
- 移除用戶端程式
- 干擾電腦運作與影響系統網路效能

惡意程式的類型

- 電腦病毒 (Computer Virus)
- 蠕蟲 (Worms)
- 木馬 (Trojans)
- 殭屍電腦(Bot)
- 隱碼程式(Rootkit)
- 駭客工具與其它惡意程式
  (Hacker Utilities and other)

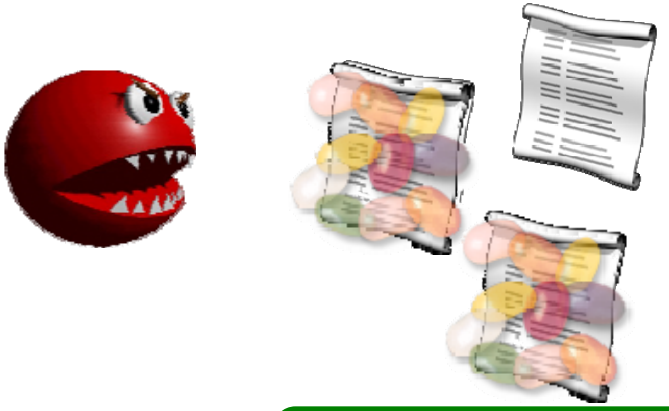
電腦病毒（Computer Virus）

早期的電腦病毒

名稱	年代	描述
Darwin	1962	達爾文，含有「物競天擇，適者生存」的意思。雙方各寫一支程式，叫有機體(organism)，這兩個程式在電腦裡爭鬥不休，直到把另一方殺掉而取代之，便算分出勝負
PERVADE	1975	會感染「動物遊戲」(要玩家聯想一種動物，接著就發問，要玩家提供那一型生物的線索)，並讓遊戲自我複製
Elk Cloner	1982	史上第一支PC病毒，針對Apple II電腦
Core Ware	1984	磁蕊大戰， Darwin遊戲的一種版本，因為遊戲程式在電 腦的記憶磁蕊中遊走,因此得到了磁蕊大戰之名
Brain	1986	由巴基斯坦的二兄弟所撰寫，是第一個MS-DOS病毒，會感染磁片開機區
Virdem	1986	早期MS-DOS病毒，會感染磁片.com檔案

電腦病毒的特性

自我複製

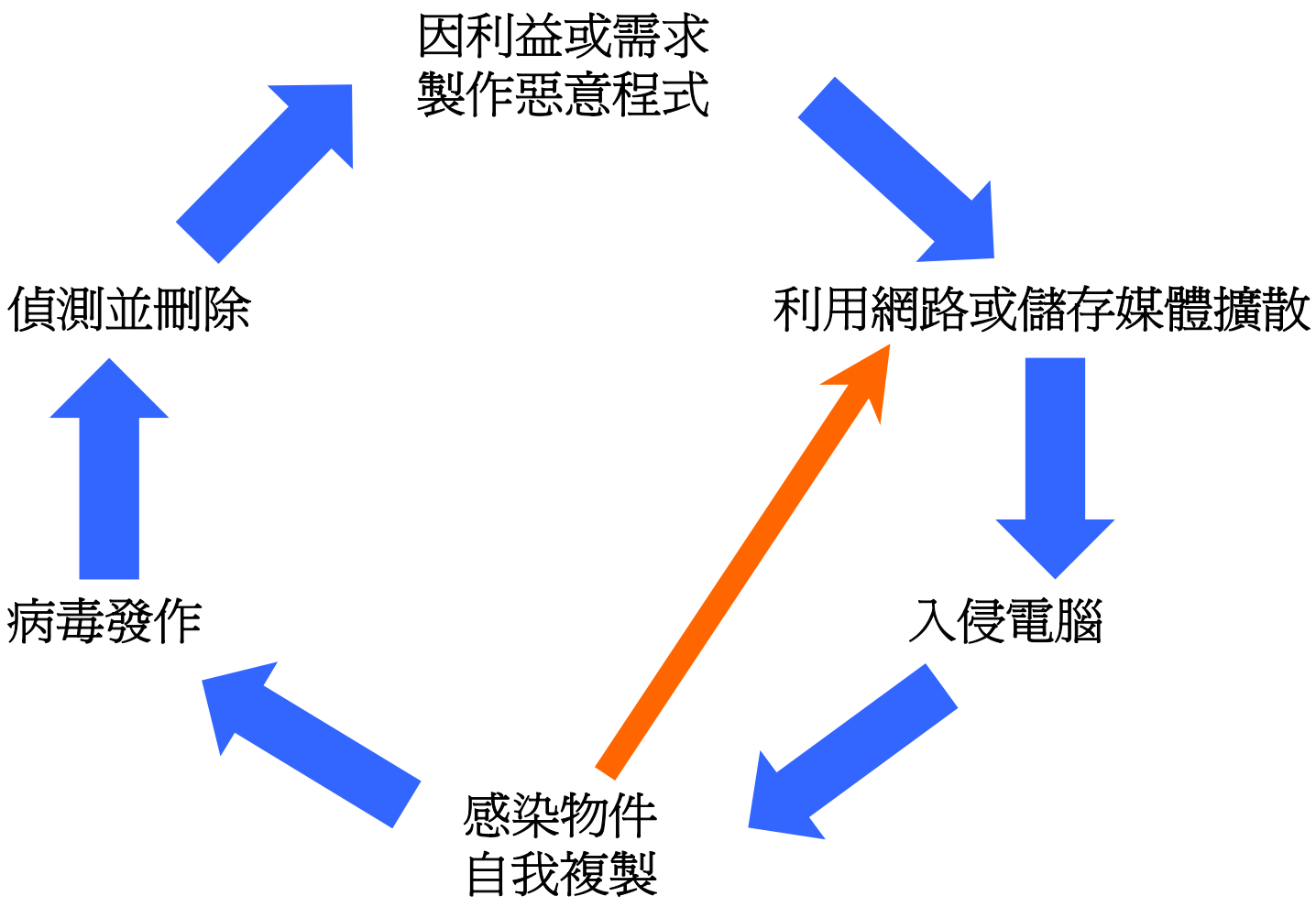


感染檔案

破壞系統檔案

特定時間觸發

電腦病毒的生命週期



電腦病毒的危害

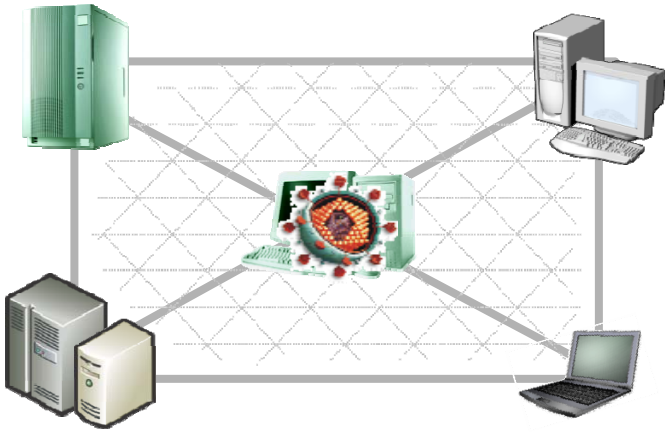
- 降低電腦效能
- 影響電腦操作
- 影響應用程式執行
- 破壞檔案關聯性
- 破壞檔案
- 無法開機
- 刪除系統磁區所有檔案

蠕蟲 (Worms)

蠕蟲的特性

自我複製

感染檔案



攻擊其他電腦

利用程式傳播

惡名昭彰的蠕蟲

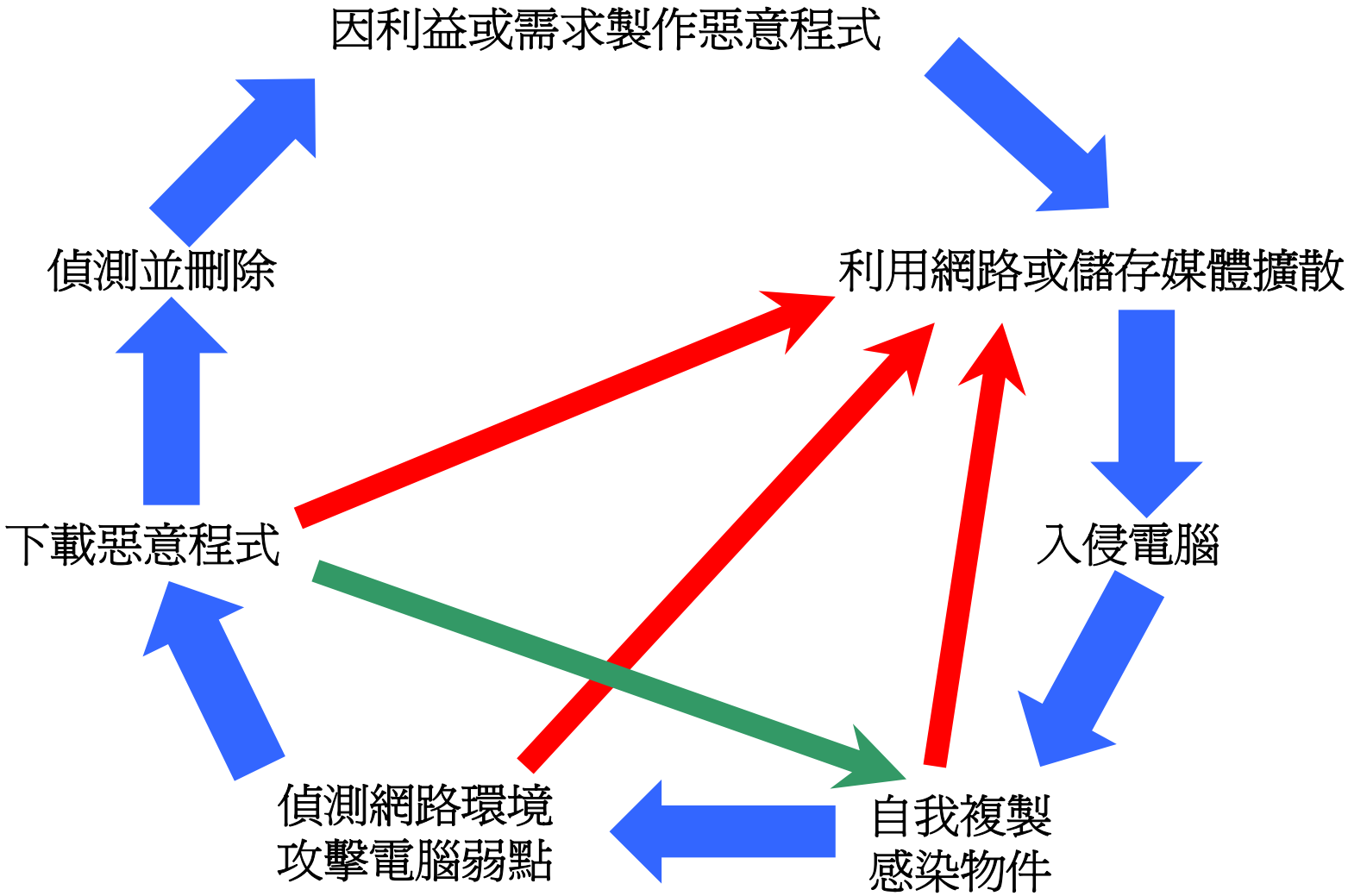
蠕蟲名稱	出現時間	感染平台
Morris Worm	1988/11	UNIX
Melissa	1999/03	微軟Outlook
The Love Bug	2000/05	微軟Outlook
Ramen	2001/01	Linux
Code Red	2001/07	微軟IIS伺服器
Nimda	2001/09	微軟IE, Outlook, IIS, 檔案分享
Klez	2002/01	微軟IE, Outlook, 檔案分享
Slapper	2002/09	Linux+Apache+OpenSSL
SQL Slammer	2003/01	微軟SQL資料庫

蠕蟲的特性

蠕蟲相似於電腦病毒，具備一些共性，能探測系統弱點取得電腦控制權、偵測網路環境透過網路服務找尋其他電腦再入侵、結合其他惡意程式持續攻擊，依其行為可區分以下種類：

- IM-Worms
- IRC-Worms
- P2P-Worms
- NET-Worms
- Email-Worms

蠕蟲的生命週期


因利益或需求製作惡意程式
利用網路或儲存媒體擴散
入侵電腦
自我複製
感染物件
偵測網路環境
攻擊電腦弱點
下載惡意程式
偵測並刪除

蠕蟲的危害

- 降低電腦安全
- 降低電腦效能
- 降低網路效能(區域／廣域網路效能)
- 影響電腦操作
- 結合木馬(Trojans)與後門(Backdoors)竊取資訊
- 遭受DoS、DDoS(Distributed Denial of Service)攻擊
- 當成惡意程式傳播或攻擊主機，網域遭到國際組織列入黑名單，或可能遭受巨大求償

木馬 (Trojans)

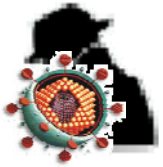
特洛伊木馬

- 斯巴達國王美內勞斯因為其太太被帕里斯所帶走，因此向希臘各城邦求助，共同出兵特洛伊。但特洛伊因為有亞馬遜女戰士和黎明女神兒子梅農的幫忙，與維納斯暗中協助，所以能抵抗希臘聯軍。
- 但因為雅典娜得不到金蘋果，所以不願放過特洛伊，而且指示奧德修斯向希臘聯軍獻上木馬屠城之計。
- 有一天，希臘聯軍突然撤退，並留下一隻木馬，特洛伊人將其當作戰利品帶回城內。在當天晚上，當特洛伊士兵為勝利而慶祝時，藏匿在木馬中的希臘兵悄悄打開城門，將城外的軍艦迎進，在一夜間消滅特洛伊城，城內男丁悉數被殺。

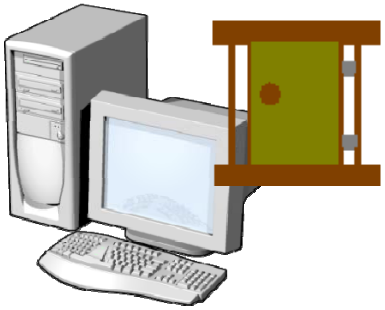
木馬程式的特性

竊取資訊

偽裝



下載更新程式



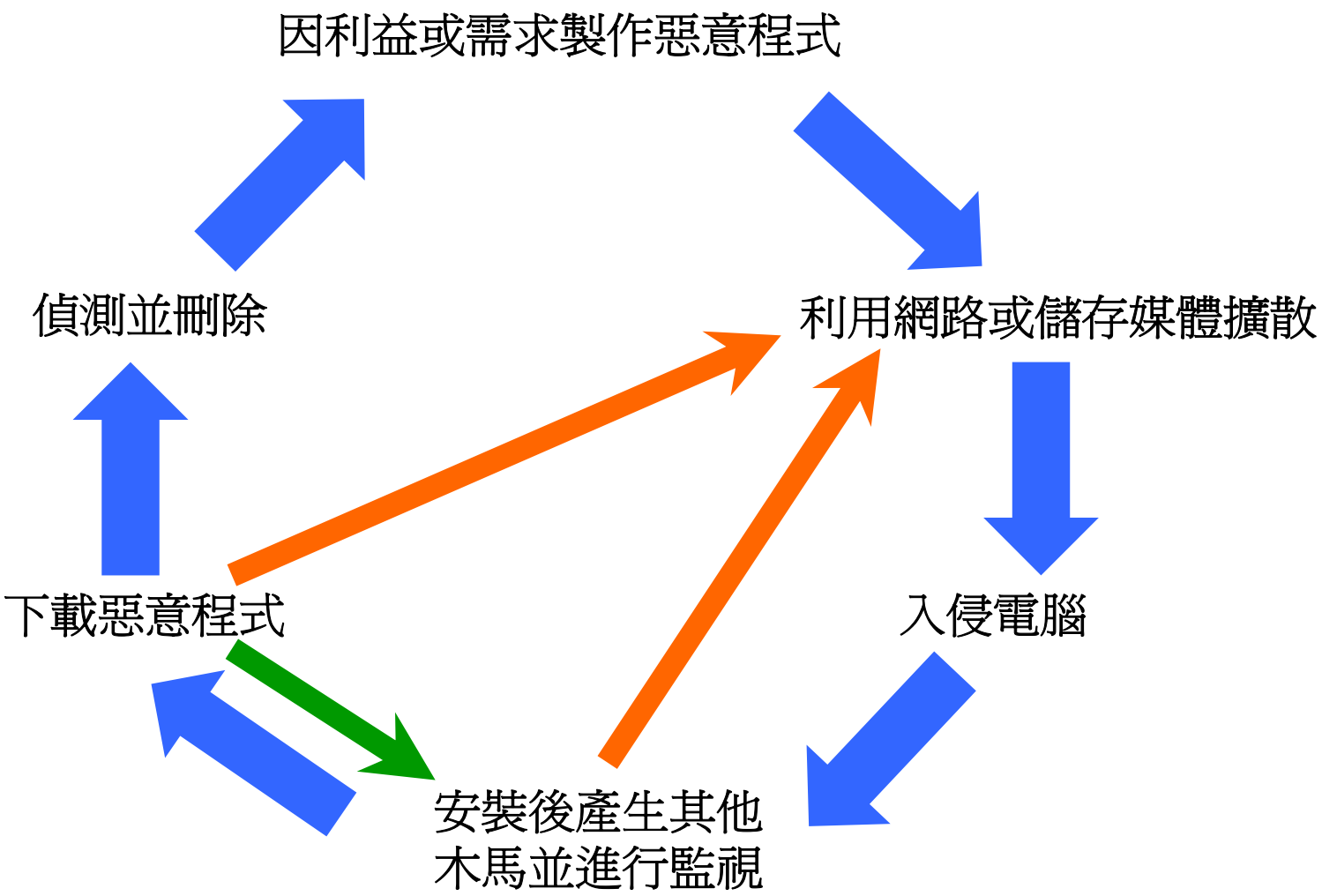
開啟連接埠

木馬程式的特性

與蠕蟲的分別，不會自行複製與感染檔案，而會衍生出關連性木馬檔案，安裝後即進行監視，只要木馬被刪除立即產生。木馬程式依其在受害電腦的行為區分以下種類：

- Backdoors
- General Trojans
- PSW Trojans
- Trojan Clickers
- Trojan Downloaders
- Troja Droppers
- Trojan Proxies
- Trojan Spies
- Trojan Notifiers
- Rootkits

木馬程式的生命週期


因利益或需求製作惡意程式
利用網路或儲存媒體擴散
入侵電腦
安裝後產生其他
木馬並進行監視
下載惡意程式
偵測並刪除

木馬程式的行為

- 中止防毒軟體運作
- 發動緩衝區溢位攻擊(Buffer Overflow)
- 產生關連性木馬檔案並隱藏，進行監視
- 偽裝系統或應用程式檔案名稱、圖示或執行程序
- 阻止安裝防毒軟體及使用防駭工具
- 竊取並傳送個人可識別資訊(PII)
- 開啟連接埠(後門)
- 入侵電腦成為網路攻擊代理主機(Agent)
- 結合蠕蟲(Worms)其他惡意程式，持續進行攻擊

木馬程式的危害

- 降低電腦安全
- 降低電腦效能
- 影響電腦操作
- 竊取資訊
- 結合間諜程式與垃圾信件，遭受網路詐騙機會增加
- 發送垃圾信件，網域遭到國際組織列入黑名單
- 當成惡意程式傳播或攻擊主機，可能遭受具大求償

殭屍電腦， 網路(Bot，NetWork)

BotNet簡介

- 殭屍電腦(Zombie)
  - 指被植入bot遙控程式的電腦，可被駭客任意擺佈。

- 殭屍網路(Botnet)
  - 由被殭屍程式所控制的電腦所組成的網路，而攻擊者可由遠端透過這些受控制的殭屍電腦發動分散式阻斷服務攻擊(DDOS)、散佈垃圾郵件或作為匿名代理器。

BotNet特性

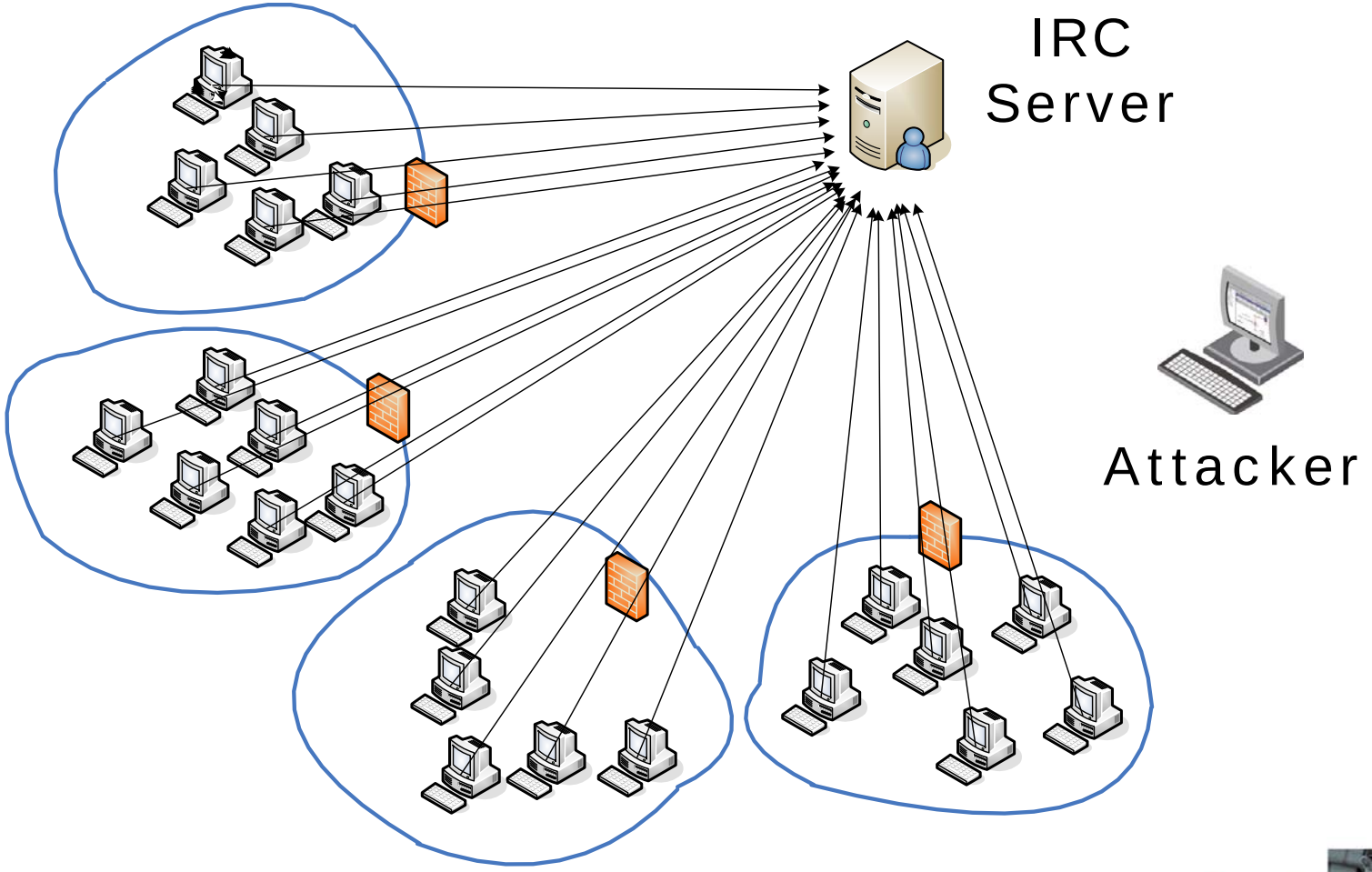
- 針對有漏洞的主機,會自行展開攻擊
- 會自動變種且自我複製
- 隱藏能力高不易被發覺
- 可在短時間內造成大規模感染
- 具有自動刪除功能

BotNet的生命週期

Botnet的產生	Botnet的擴散	Botnet的遷移	Botnet的升級	Botnet的活動	Botnet的消失
Exploit *Worm* *Social Engineer*	利用*Bot*來進行掃瞄及攻擊	*Botmaster*定期轉換*C&C*的位置	更新*Bot*程式，以降低被防毒軟體偵測的可能	接受*Botmaster*命令，進行*DDOS*攻擊、竊取資料、散佈廣告信等	防毒軟體清除*Bot*程式 使用者刪除*Bot*程式 *Botnet*間互相競爭，侵佔彼此控制權

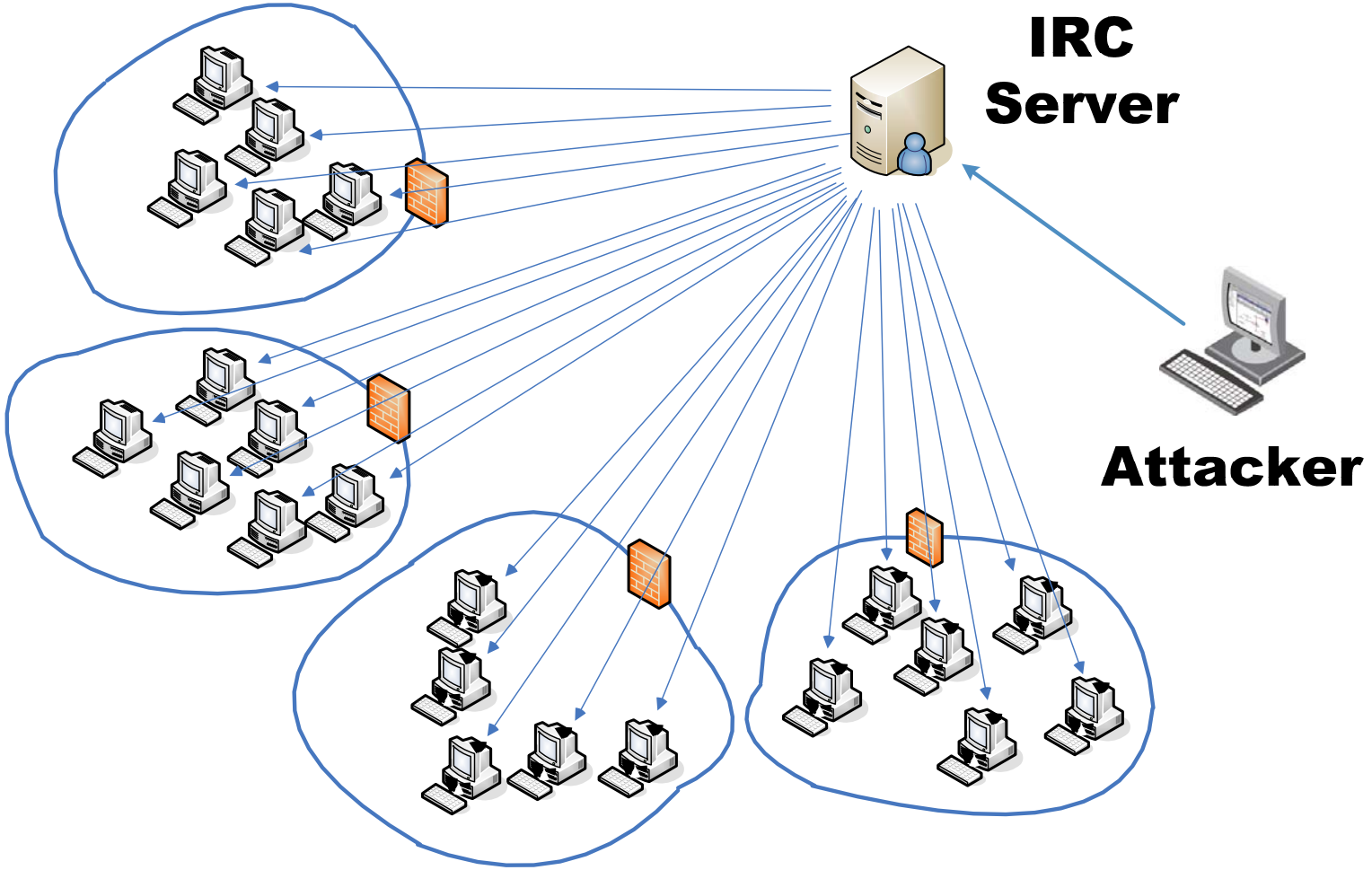
IRC Bot Net架構

殭屍電腦: 嗨！我是殭屍電腦第XX號，我已經受到感染，向指定IRC伺服器報到註冊



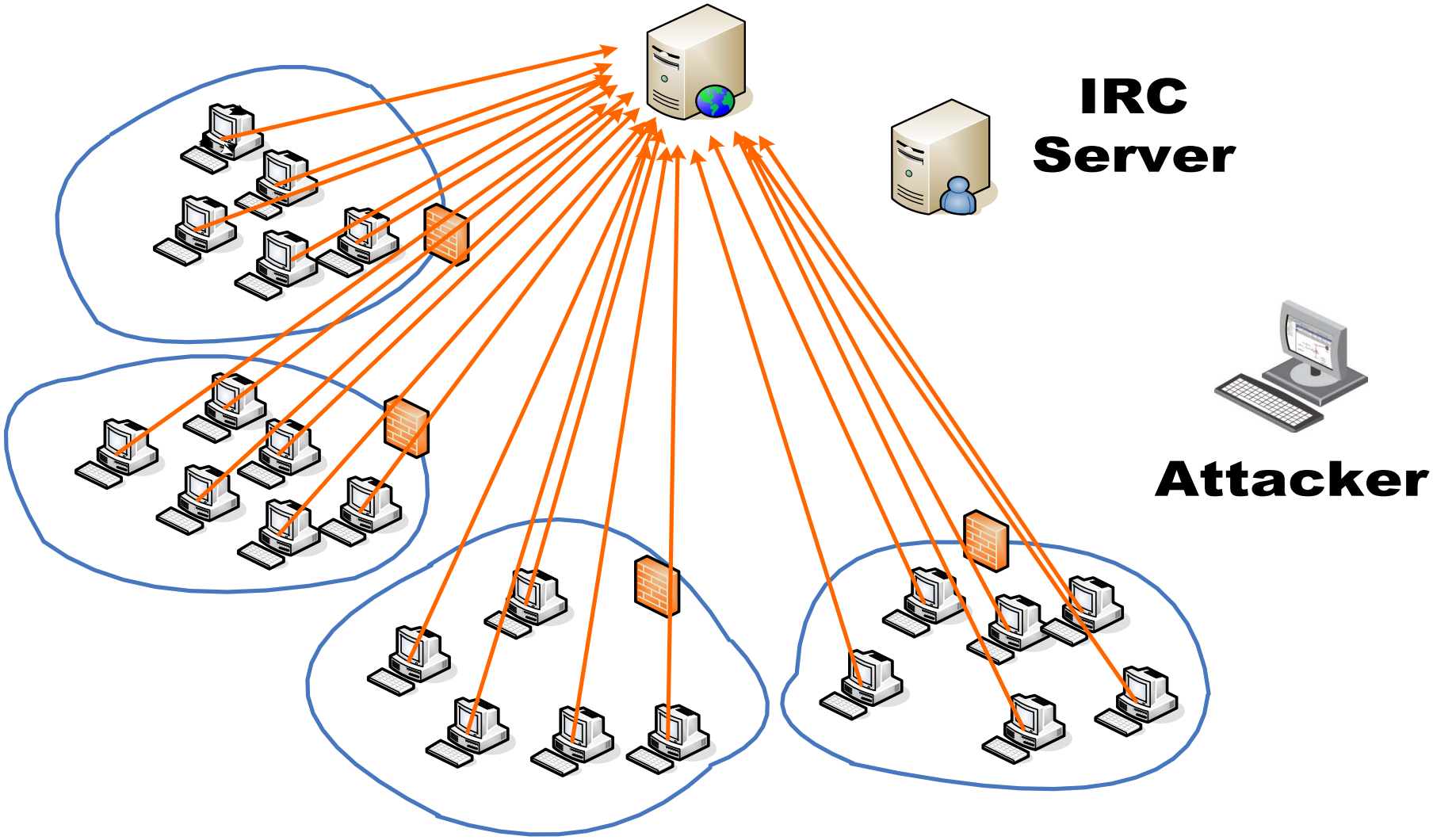
IRC Bot Net架構

Attacker: 向 x.x.x.x 電腦發動DDoS攻擊



IRC Bot Net架構

無辜第三者遭到大量殭屍電腦的DDoS攻擊！！



Bot的感染途徑與惡意行爲模式

- 電子郵件
  - 社交工程
- 網頁流覽
  - 網頁重導, 釣魚網站
- 未修補的漏洞
- P2P軟體
  - 免費工具軟體
- 即時通軟體
  - MSN Messenger
- 其它
  - 後門軟體

- **分散式阻斷攻擊**
  - **SYN Flood,UDP Flood**
- **竊取使用者資料**
  - **側錄程式**
  - **銀行帳號,信用卡卡號**
- **散佈垃圾郵件**
  - **蒐集通訊錄中電子郵件**
- **恐嚇或綁架檔案**
  - **DDOS**
  - **將重要檔案加密**

Bot與其他惡意程式比較

	可控性	竊秘性	危害等級
病毒	一般沒有	一般沒有	感染檔案:中
蠕蟲	一般沒有	一般沒有	網路流量:高
間諜程式	一般沒有	有	資訊洩漏:中
木馬程式	可控	有	全部控制:高
殭屍程式	高度可控	有	全部控制:高

Bot偵測工具

- 網路連線狀況
  - TcpView
- 網路封包解析
  - tcpdump
- 特徵值
  - PE Table
- 行為分析
  - 登錄檔,系統呼叫,攔截API
- 差異性比對
  - Tripwire
- Rootkit檢查程式
  - IceSword

Botnet預防

- **部署IPS系統**
  - 防止Bot 利用系統漏洞入侵擴散
  - IPS解析應用層封包內容，可發掘並阻擋可疑的IRC登入及連線行為
  - 管理IM/P2P使用，減少惡意軟體擴散管道
  - 隔離受感染的電腦
- **定期弱點掃瞄，安裝修補程式**
- **在主機端安裝防毒軟體，加強主機端防護**
- **加強使用者資訊安全認知教育：**
  - 不任意開啟Email附件檔
  - 不任意依據Email或IM所提供的URL下載執行檔案
  - 採用強密碼，防止Bot透過破解懶人密碼擴散

隱碼程式(Rootkit)

Rootkit簡介

- 它源自於UNIX電腦系統，原本是一組指令，是一種可以獲得電腦系統root存取權限的軟體工具組（kit），因此稱為rootkit；root是UNIX系統權限最高的帳號，也就是系統管理者帳號的名稱。rootkit最重要的特性，就是會想盡一切辦法隱匿攻擊者的所有行為，不能被發現已經被植入或正在執行rootkit；因為只要被發現，管理者當然就會想盡辦法要移除rootkit。

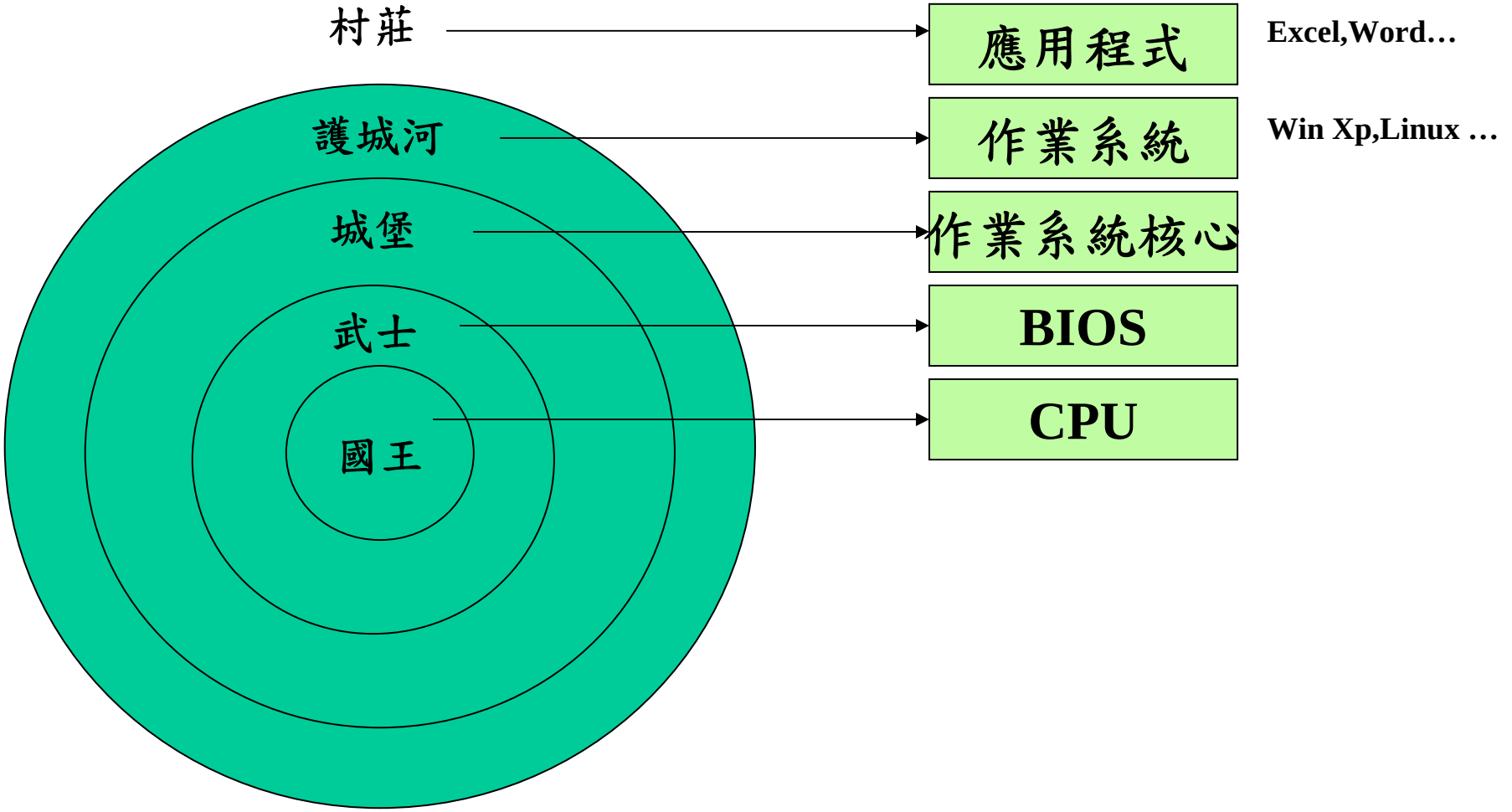
Rootkit特性

- 能偽裝成一般正常的程式，把正常程式換掉
- 能完全隱藏入侵痕跡並保留後門讓攻擊者可以再一次進入
- 可提供攻擊者 telnet、shell 與 finger等服務，並可用來清理登入資料

RootKit類型

- 應用層（application level）
  - 會以假冒的程式換掉一般的正常程式，或者利用hook等各種方法更改正常程式的功能。
- 核心層（kernel level）
  - 會更換或更改系統核心，因此需要利用驅動程式（Windows）或可載入模組。
  - 取代系統中的library(程式庫)，使得使用到這些 library 的程式相當於都有潛在的問題。
  - 較難編寫，但也更不易偵測。

不同層次的惡意程式


村莊
護城河
城堡
武士
國王
應用程式
作業系統
作業系統核心
BIOS
CPU
Excel,Word…
Win Xp,Linux …

不同層次的惡意程式

程式名稱	影響層次	動作	比喻	範例工具
後門程式	應用程式	略過安全機制	入侵者在牆上挖洞	Netcat,vnc
木馬程式	應用程式	表面有用,私下執行惡意動作	入侵者假裝是和善的村人	NetBus, SubSeven
使用者模式 Rootkit	作業系統	替換指令,隱藏蹤跡	入侵者躲入護城河	Windows AFX Rootkit
核心模式 Rootkit	作業系統核心	修改核心,隱藏蹤跡	入侵者登上城堡,改變階級	Window NT Rootkit
Bios層次 惡意軟體	BIOS	BIOS啟動系統時將惡意程式載入	入侵者命令武士蓋城堡	CIH
惡意的 microcode	BIOS及CPU	修改Bios及cpu微碼	入侵者強迫國王妥協, 交出控制權	N/A

RootKit偵測方式

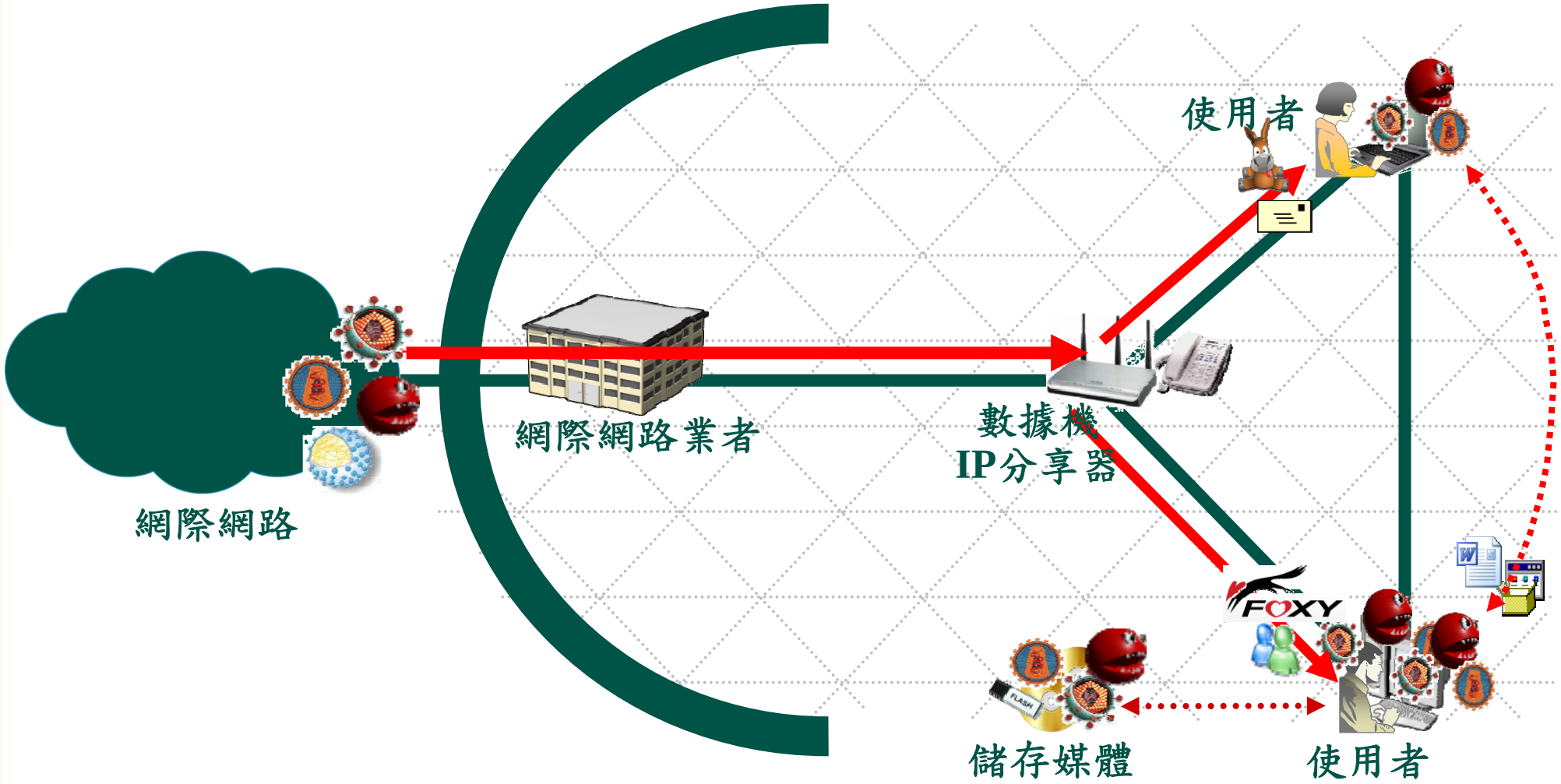
- 特徵辨識（signature-based）
  - 找出已知rootkit程式的一段二進位碼作為辨識特徵。
  - 與掃毒程式利用病毒碼辨識病毒的方式類似。
- 行為辨識（behavior-based）
  - 搜尋rootkit程式隱藏的元素，包括檔案或記錄。

RootKit偵測工具

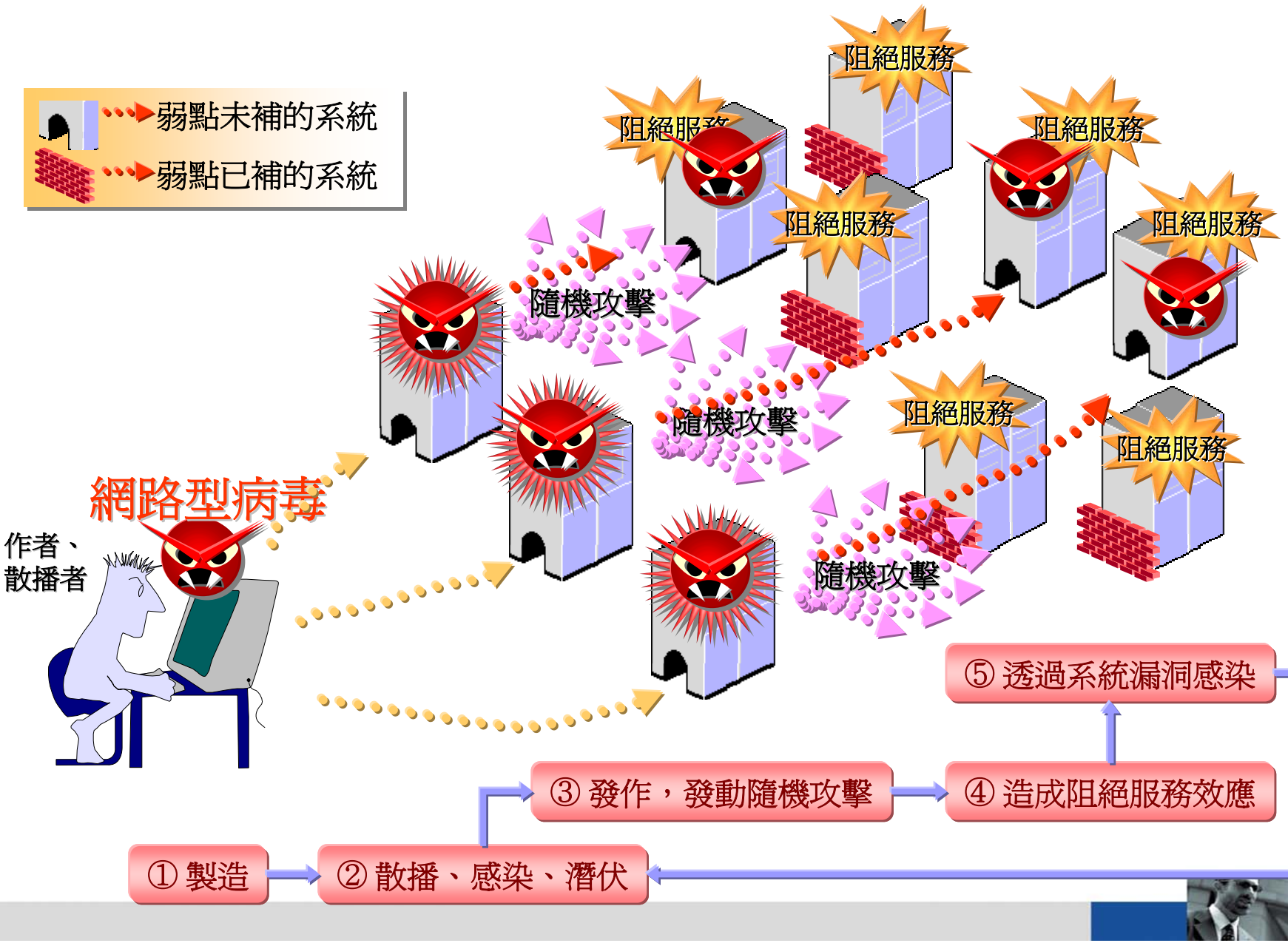
- Tripwire
  - 提供許多演算法如 MD5 / Snefu / SHA 等，可以驗證檔案是否被竄改，如果與原先的檔案不符，將提醒管理者。
  - 參閱 http://www.tripwire.org/
- chkrootkit
  - chkrootkit 提供許多工具檢查是否被植入 rootkits，
  - 例如 chkrootkit 會檢查幾個可能被竄改過的系統程式，以及檢查是否有 rootkits 常使用的工具。

惡意程式手法分析

惡意程式入侵的方式



惡意程式入侵的方式


弱點未補的系統
弱點已補的系統
阻絕服務
阻絕服務
阻絕服務
阻絕服務
阻絕服務
阻絕服務
隨機攻擊
隨機攻擊
隨機攻擊
網路型病毒
作者、
散播者
⑤ 透過系統漏洞感染
③ 發作，發動隨機攻擊
④ 造成阻絕服務效應
① 製造
② 散播、感染、潛伏

駭客犯罪常用策略

密碼是否簡單

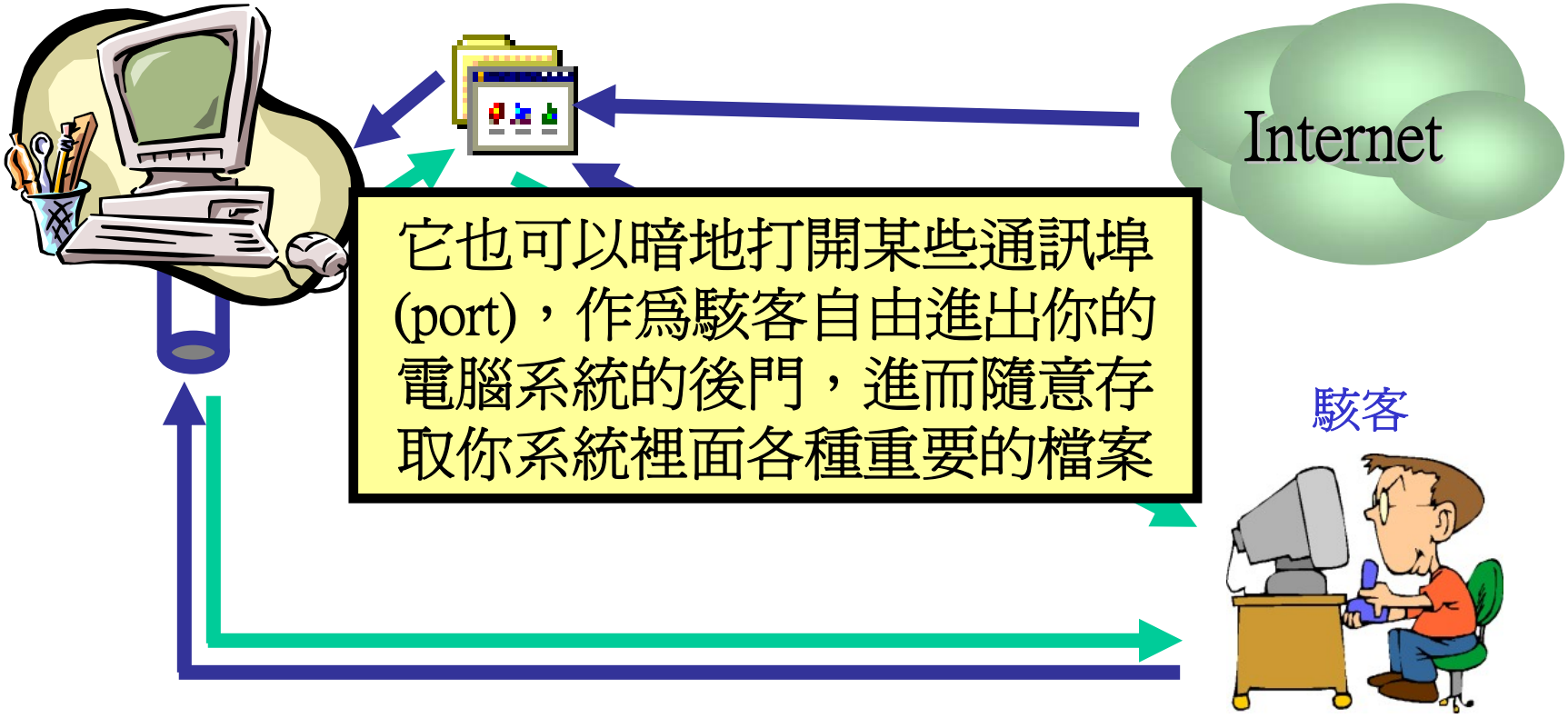
- 方法一：人工方式猜密碼
- 方法二：利用自動化工具竊取密碼

提供那些服務

該服務是否有漏洞

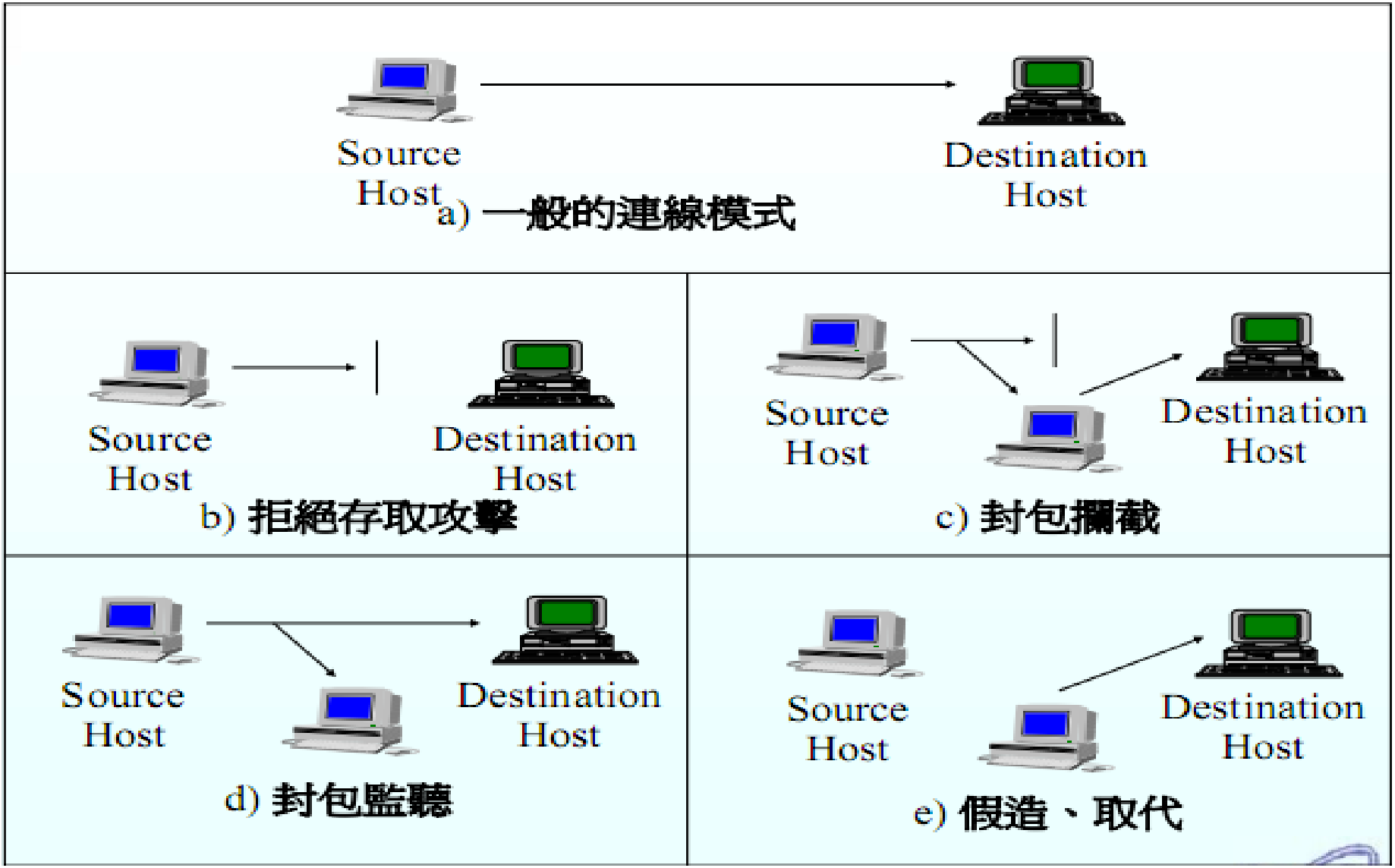
獲取系統資訊並分析內容

惡意程式入侵手法



駭客工具是一種具有特殊目的惡性程式，它可以設計來做遠端遙控或挖掘某些系統的後門等等。

惡意程式常用攻擊手法


Source Host
Destination Host
a) 一般的連線模式
Source Host
Destination Host
b) 拒絕存取攻擊
Source Host
Destination Host
c) 封包攔截
Source Host
Destination Host
d) 封包監聽
Source Host
Destination Host
e) 假造、取代

駭客會怎麼做

第1階段：
入侵前的準備
(資料收集、掃瞄等)

第2階段：
入侵系統，取得受害主機控制權，並安裝後門程式以建立管道進入受害單位內部網路

第3-1階段：
擴散受害範圍

第3-2階段：
持續維護所取得之存取控制權

第3-3階段：
竊取重要資料及檔案

時間軸

入侵前的準備

- 收集目標單位的資訊
  - E-Mail、News、Whois、討論區、搜尋引擎等

http://216.239.51.104/search?q=cache:fwEL0vfMESYJ:ht.24go.com.tw/...

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛

網址(D) http://216.239.51.104/search?q=cache:fwEL0vfMESYJ:ht.24go.com.tw/%E6%9C%83%E5%93%A1%E5%90%8D%E5%9 移至

搜尋 醒目提示 選項 允許快顯視窗 Hotmail Messenger 我的 MSN

這是 Google 的 快取 的 http://ht.24go.com.tw/%E6%9C%83%E5%93%A1%E5%90%8D%E5%96%AE/%E6%9C%83%E5%93%A1%E5%90%8D%E5%96%AE2006.htm，擷取日期在 200

Google 已先行預覽各網站，在資庫儲放各網頁的存檔。

此網頁可能有更新的版本，請按此處檢視新版。

此快取頁可能參照無法再使用的圖片。請按這裡，查閱快取文字。

若要連結至此網頁或加入書籤，請使用此網址：http://www.google.com/search?q=cache:fwEL0vfMESYJ:ht.24go.com.tw/%E6%9C%83%E5%93%A1%E5%90%8D%E5%96%AE/%E6%9C%83%E5%93%A1%E5%90%8D%E5%96%AE2006.htm

Google 和網頁作者無關，對網頁的內容恕不負責。

您的查詢字詞都已標明如下： a11068

這些查詢字詞只有在網頁的連結中出現: allintext

會員名單

序號	會員編號	會員姓名	身份證字號	入會日期	序號	會員編號	會員姓名	身份證字號	入會日期	序號	會員編號	會員姓名	身份證字
1	A10002	呂	E102	900920	34	A10055	曹	S200	901114	67	A10116	林	T102
2	A10004	宋	E121	900920	35	A10056	黃	T101	901115	68	A10120	陳	E201
3	A10005	宋	E202	900920	36	A10058	陳	X200	901115	69	A10121	陳	Q200
4	A10006	呂	E202	900920	37	A10059	陳	E120	901115	70	A10125	許	D200
5	A10015	洪	E202	900928	38	A10061	楊	T101	901119	71	A10127	王	E201
6	A10016	李	S201	900928	39	A10062	宋	S200	901119	72	A10131	陳	E200
7	A10017	李	D100	900928	40	A10065	何	L201	901120	73	A10133	吳	E221
8	A10019	邱	T101	900930	41	A10067	鍾	T100	901121	74	A10135	謝	R221
9	A10020	丁	E101	900928	42	A10068	李	T100	901122	75	A10136	劉	R120
10	A10021	丁	E210	900928	43	A10071	潘	T221	901126	76	A10137	董	E102
11	A10023	張	R220	901010	44	A10072	陳	S201	901126	77	A10144	劉	E200
12	A10025	蔡	E201	901016	45	A10073	陳	R100	901126	78	A10146	黃	Q101
13	A10026	金	S101	901022	46	A10074	何	N101	901126	79	A10151	李	Q101

標誌

```
#echo "GET /" | nc www.microsoft.com 80 | grep Server:
Server: Microsoft-IIS/5.0
#echo "GET /" | nc www.sun.com 80 | grep Server:
#
```

預設的通信埠

```
53/tcp      open        domain
88/tcp      open        kerberos-sec
135/tcp     open        loc-srv
139/tcp     open        netbios-ssn
389/tcp     open        ldap
445/tcp     open        microsoft-ds
464/tcp     open        kpasswd5
593/tcp     open        http-rpc-epmap
636/tcp     open        ldapssl
```

作業系統及版本

```
[root@mdk ~]# nmap -sS -O 10.1.1.4

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap
Interesting ports on  (10.1.1.4):
(The 1520 ports scanned but not shown below are in state: closed)
Port       State       Service
111/tcp    open        sunrpc
515/tcp    open        printer
1024/tcp   open        kdm

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=2550070 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14

Nmap run completed -- 1 IP address (1 host up) scanned in 28 seconds
[root@mdk ~]#
```

開機多久(uptime)

```
Starting nmap V. 2.54BETA29 ( www.insecure.org/nmap/ )
Interesting ports on  (10.1.1.254):
(The 1547 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

Remote operating system guess: OpenBSD 2.9-beta through release (X86)
Uptime 5912.083 days (since Mon Jul  8 09:35:58 1985)

Nmap run completed -- 1 IP address (1 host up) scanned in 19 seconds
```

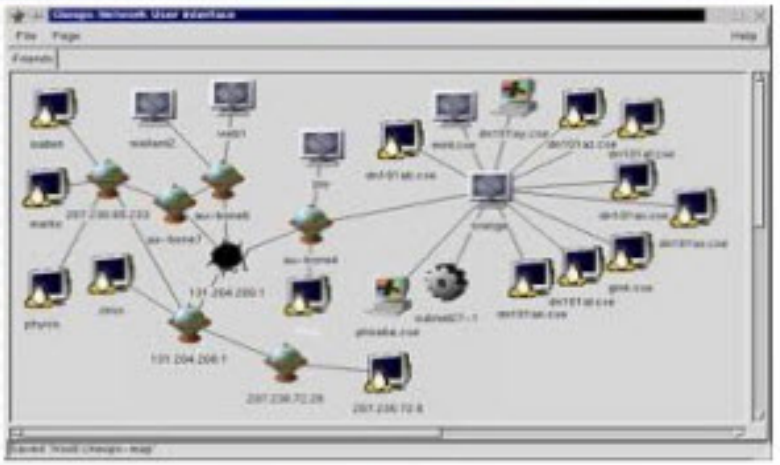
標誌

```
#echo "GET /" | nc www.microsoft.com 80 | grep Server:
Server: Microsoft-IIS/5.0
#echo "GET /" | nc www.sun.com 80 | grep Server:
#
```

預設的通信埠

```
53/tcp      open        domain
88/tcp      open        kerberos-sec
135/tcp     open        loc-srv
139/tcp     open        netbios-ssn
389/tcp     open        ldap
445/tcp     open        microsoft-ds
464/tcp     open        kpasswd5
593/tcp     open        http-rpc-epmap
636/tcp     open        ldapssl
```

入侵前的準備



- 系統掃瞄
  - 獲取系統及網路資訊
    - ➢判斷目標系統是否運作中
    - ➢判斷作業系統類別及版本
    - ➢偵測開啟的網路服務，如Web、E-Mail、FTP、網路芳鄰等
    - ➢工具包括Nmap、Cheops等
  - 獲取系統弱點資訊
    - ➢Nessus、HScan、流光、SuperScan等
      - ✓用來偵測系統可能的弱點

入侵系統

- 在第2階段中，駭客開始對目標系統或網路進行攻擊以取得控制權，根據以往的駭客入侵事件，歸納出駭客可能採用的手法如下：

1. 利用掃瞄過程中發現的系統弱點直接對目標系統進行攻擊，以取得系統控制權。由駭客使用的工具可發現駭客會利用系統不當的權限設定、WebDAV、RPC等弱點來取得系統控制權。

   攻擊對象：系統

入侵系統

2. 寄送含有惡意程式之E-Mail至目標單位人員的E-Mail帳號，以欺騙使用者執行惡意程式，藉此駭客可取得系統之控制權。

攻擊對象：End-User (社交工程攻擊)

E-mail欺騙

資訊通告 - 2005 年 2 月份 MICROSOFT 安全反應中心公告發行 - 郵件

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 表格(A) 視窗(W) 說明(H)

傳送(S) | 選項(P)... | HTML

寄件者... Microsoft

收件者...

副本...

主旨: 資訊通告 - 2005 年 2 月份 MICROSOFT 安全反應中心公告發行

附件... 修補方法.doc (93 KB) 附件選項(M)...

Verdana | 10

資訊通告
2005 年 2 月 9 日

2005 年 2 月 MICROSOFT 安全性公告發行

本通告的內容為何？

新發行的更新程式
Microsoft 將發行 12 個安全性公告，解決 Microsoft Windows、Microsoft .NET Framework、Microsoft Windows SharePoint Services、SharePoint Team Services、Windows Media Player、Microsoft MSN Messenger 和 Microsoft Office 中最近發現的弱點。

最高嚴重性	公告編號	受影響的產品	影響
重要	MS05-004	Microsoft .NET Framework	資訊洩漏，以及可能發生權限提高
重大	MS05-005	Microsoft Office	遠端執行程式碼
中度	MS05-006	Microsoft Windows SharePoint Services、SharePoint Team	遠端執行程式碼

E-mail欺騙

- Microsoft安全性公告 MS07-060

Microsoft Word 中的弱點可能會允許遠端執行程式碼

發佈日期：2007 年 10 月 9 日

影響的軟體：

Microsoft Word 2000 Service Pack 3、Microsoft Word 2002 Service Pack 3

- 如果使用者開啟蓄意製作、其中含有格式錯誤字串的 Word 檔案，此弱點可能會允許從遠端執行程式碼。 系統上帳戶使用者權限較低的使用者，其受影響的程度比擁有系統管理權限的使用者要小

入侵系統

3.寄送會利用IE瀏覽器弱點攻擊使用者之網站連結至目標單位人員的E-Mail帳號，欺騙使用者進入該網站，藉此駭客得以利用IE弱點於使用者端安裝惡意程式，進而取得系統之控制權。

攻擊對象：End-User (社交工程攻擊)

惡意網站攻擊

WORM_NETSKY.Y天網變種病毒通告

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄

寄件者:
日期: 上午 12:12
收件者:
主旨: WORM_NETSKY.Y天網變種病毒通告

病毒名稱：「WORM_NETSKY.Y」天網變種病毒
『天網』駭客現身，若收到主旨爲『Delivery failure notice ID-XXX』，請直接刪除，以免不慎中毒。並即刻更新最新病毒碼以免病毒入侵！
病毒移除步驟 http://xxx.xxx.com.tw/index.html

病毒特性：

1.天網變種病毒，透過e-mail電子郵件方式快速傳播，中毒以後會開啓82 port後門以便駭客於後端遙控操作，中毒電腦會在 發動DoS阻斷式攻擊某些網站造成該網站癱瘓。

2.此病毒針對熔果病毒而來，由於這一隻病毒信有固定郵件主旨，若看到『Delivery failure notice ID-XXX』爲主旨的郵件，請直接刪除該信件，以免不慎中毒。

惡意網站攻擊

- Microsoft 安全性公告 MS08-024

  由於 Internet Explorer 處理資料流的方式，導致其中存在遠端執行程式碼的弱點

  原始發佈日期：2008 年 4 月 9 日

  受影響的軟體：

  Microsoft Internet Explorer 5.01 、Microsoft Internet Explorer 6.0 、Microsoft Internet Explorer 7.0

- 攻擊者可蓄意製作網頁以利用此弱點，當使用者檢視網頁時，此弱點可能會允許遠端執行程式碼。 成功利用此弱點的攻擊者可以取得與登入使用者相同的使用者權限

網路釣魚攻擊

Darling Msn user,

During one of our regular automated verification procedures we've encountered a some problem caused by the fact that we could not verify the info that you provided to us.

Please, give us the following information so that we could fully verify your identity.

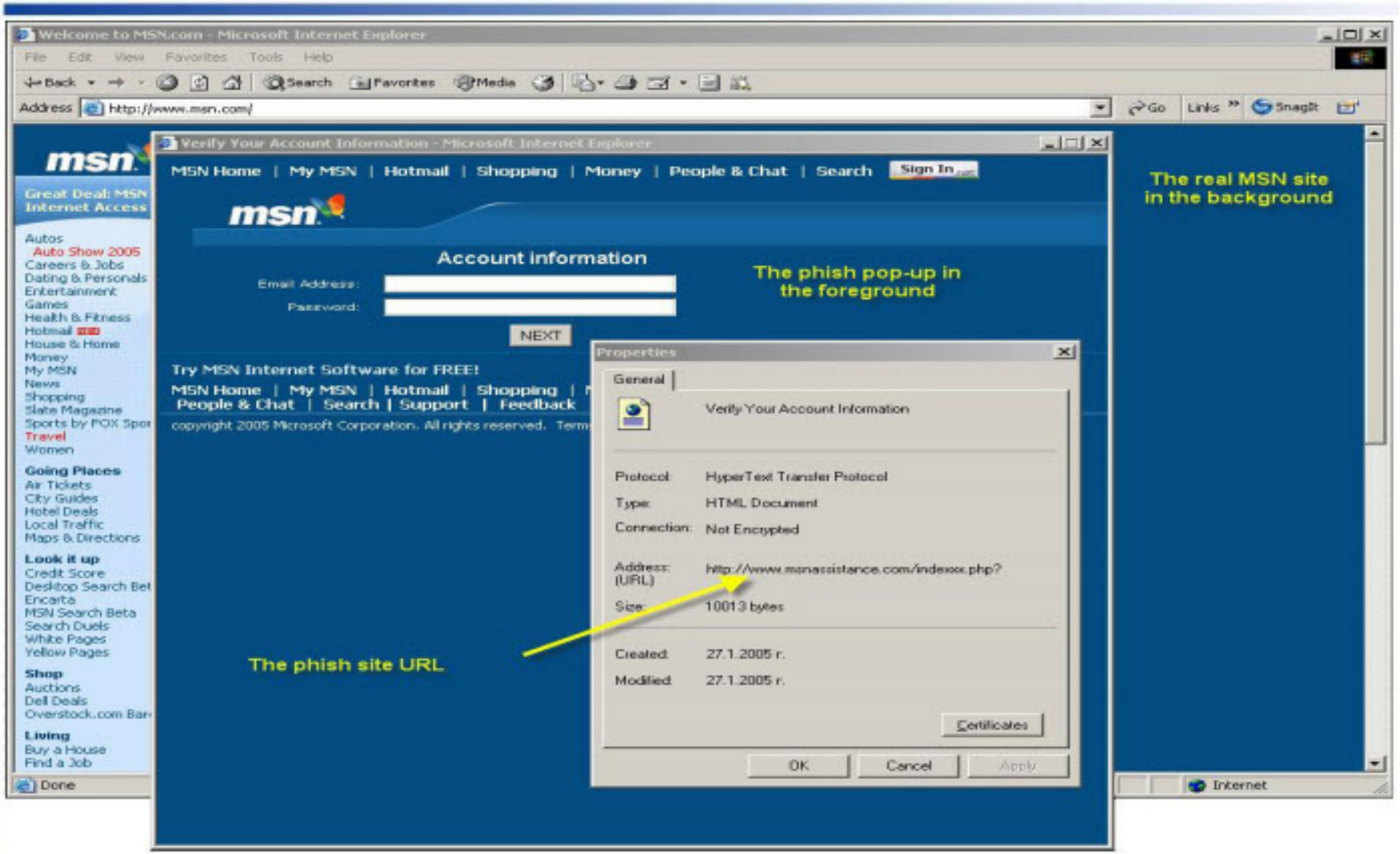
Otherwise your access to MSN services will be closed.

To verify your information please http://www.msnassistance.com/index.php follow this link.

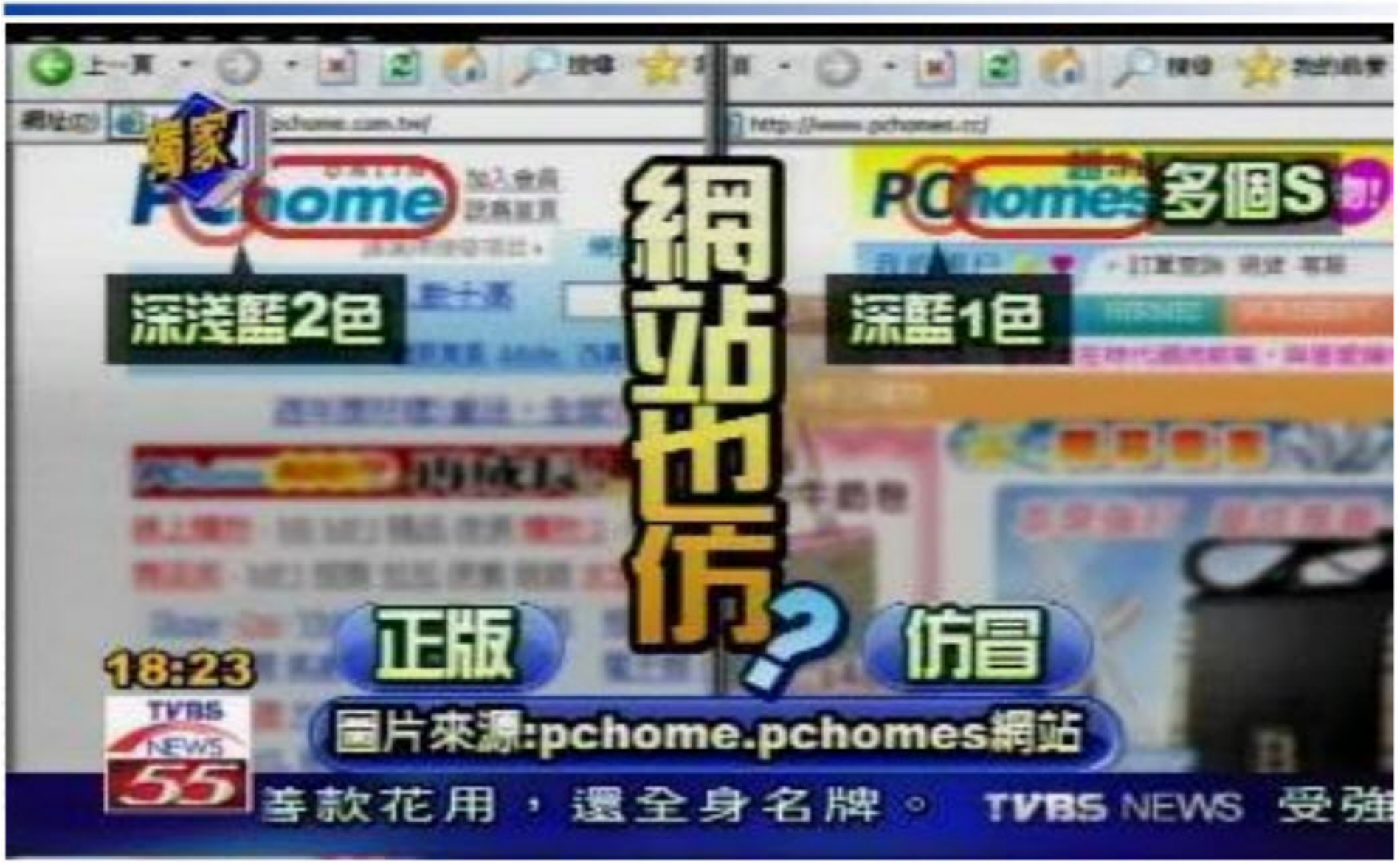
Thanks for using MSN.

MSNWeb Access Supporting.

網路釣魚攻擊


Welcome to MSN.com - Microsoft Internet Explorer
Verify Your Account Information - Microsoft Internet Explorer
The real MSN site in the background
The phish pop-up in the foreground
The phish site URL
Properties
General
Verify Your Account Information
Protocol: HyperText Transfer Protocol
Type: HTML Document
Connection: Not Encrypted
Address: (URL) http://www.monassistance.com/indexxx.php?
Size: 10013 bytes
Created: 27.1.2005 r.
Modified: 27.1.2005 r.
Certificates
OK
Cancel
Apply
Account Information
Email Address:
Password:
NEXT
Try MSN Internet Software for FREE!

網路釣魚攻擊


獨家
深淺藍2色
深藍1色
網站也仿？
正版
仿冒
18:23
TVBS NEWS 55
圖片來源:pchome.pchomes網站
等款花用，還全身名牌。
TVBS NEWS

網路釣魚攻擊

- 利用各種手法來取得您的私密資料
  - 聲稱能為您查詢您的朋友是否將您「封鎖(Blocked)」
  - 輸入MSN帳號密碼後即可查詢。
  - 輸入後，您的帳號密碼即被偷走。

擴散受害範圍

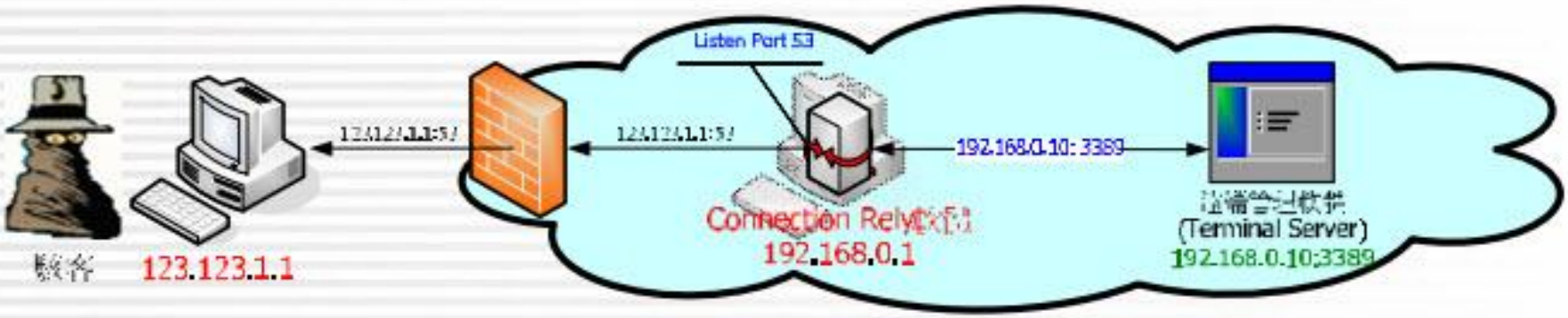
- 一旦內部被入侵成功時，會採用篡改網頁的方式或置放後門程式來加速擴大受害範圍
- Ex. 駭客入侵內部應用系統網站，由於每人每天都需要上此系統登錄資料，如此只要是沒有執行系統修補(Patch)的用戶端電腦，即會在連線至該系統時被植入後門程式
- Ex. 政府單位網站上的網頁如被置換，所有瀏覽該網頁且沒有執行系統修補的用戶端電腦，將被植入後門程式

持續維護所取得的存取控制權

- 為維持所取得的控制權及掌握狀況，駭客安裝後門程式外，亦會安裝下列程式：
  - Keylogger：能記錄使用者所開啟的程式及鍵入的指令，進而可攔截如網路交易、POP3、SMTP、FTP等的帳號/密碼
  - Winlogon密碼側錄程式：能截錄由圖形介面登入的帳號、密碼
  - Password Dump程式：可配合密碼攻擊來取得系統上所有user的帳號及密碼
  - Rootkit：用以隱藏駭客所執行的程序及連線，以防止被系統管理者發現

持續維護所取得的存取控制權

- 一般情況下，透過後門主動建立的連線駭客只能獲得命令列模式的操作界面，但透過Connection Relay軟體的幫助，駭客可使用遠端管理軟體(如Terminal Service、R_Server、Dameware Remote Control、VNC、PCAnywhere等)連上受害主機，取得視窗操作界面，如此駭客可更方便的維護所取得之受害主機的控制權。



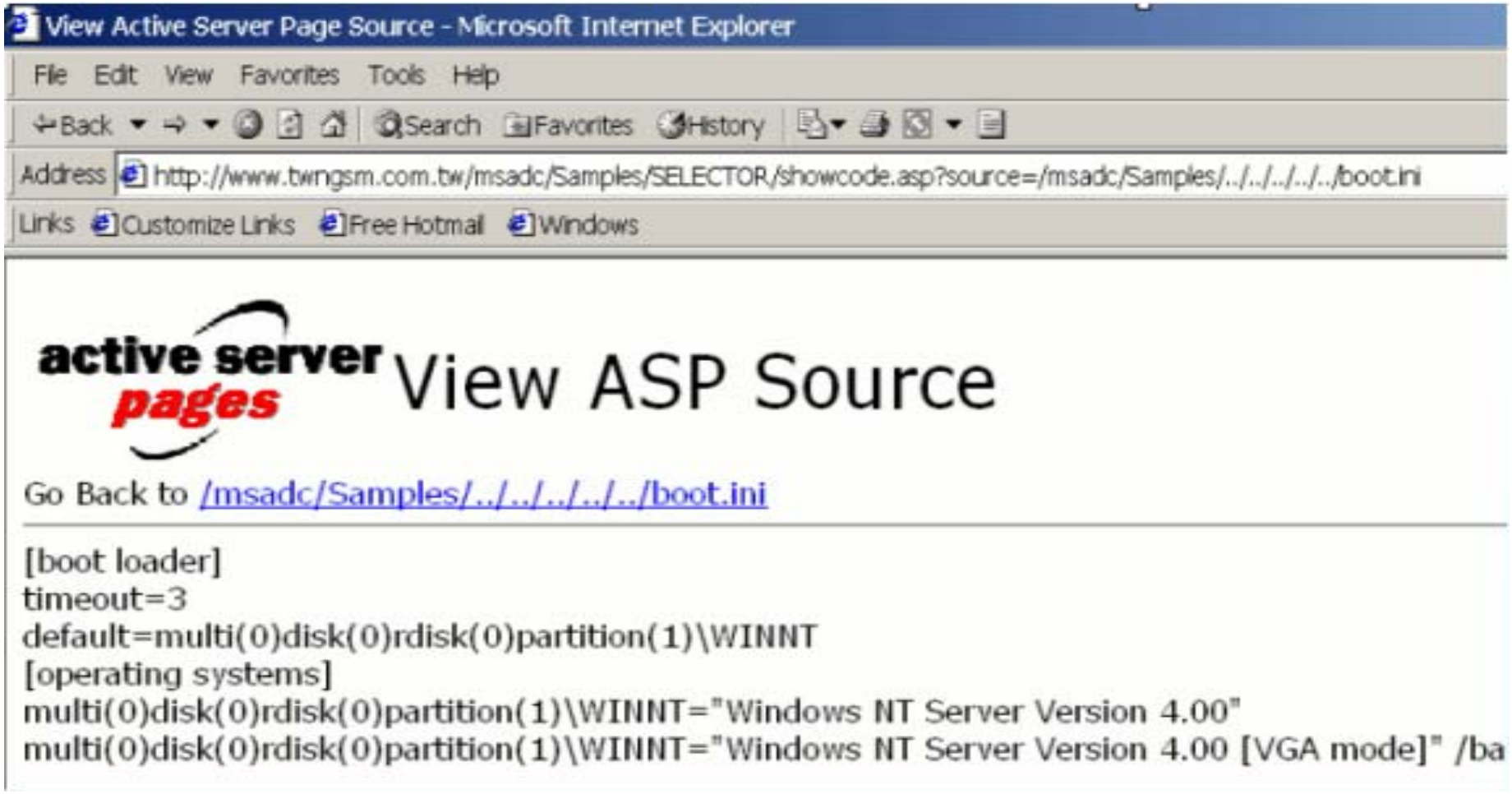
竊取重要資料及檔案

- 在擴散受害範圍及維護駭客所取得之控制權的同時，駭客亦可透過遠端管理軟體於受害主機上或透過網路芳鄰進行快速瀏覽、搜尋及竊取重要檔案及資料

常見的攻擊手法I

- 使用現成的攻擊工具
- 猜測密碼法
  - Remote Password Guessing
  - Local Password Cracking
- 設定錯誤、設定不詳盡的系統
  - 預設帳號、密碼
  - 存取設定錯誤（NFS）
  - 安裝系統時，自動安裝的不必要程式（showcode.asp）

http://www.???gsm.com.tw/??????????/
showcode.asp?source=/msadc/Samples/../../../../../../boot.ini



常見的攻擊手法II

- 程式本身的設計缺陷
  - Buffer Overflow
  - 路徑檢查不嚴謹（../../../etc/passwd）
  - 參數檢查不嚴謹（例如 phf）
- 監聽網路上的封包（Sniffing）
- 搜尋順序的問題
  - 安裝木馬（陷阱）
  - 動態函式替代法
- 安裝後門程式

Buffer OverFlow

- 藉由輸入過長的資料給固定長度的buffer造成buffer overrun。
- 實例：
  - NCSA httpd buffer overflow
    - NCSA’s httpd v1.4 的 MAX_STRING_LEN 只能容忍 256 個字元
    - Crack : 當一個 client 連到server的port 80，利用GET command 輸入超過256字元，server 便會要求結束程式。

Buffer OverFlow

- POP3d
  - Buffer overflow with 'USER username'
    - »username > 152字元
  - Buffer overflow with 'PASS passwd'
    - »password > 104字元
- SMTPd
  - Buffer overflow with 'HELO hostname'
    - »hostname > 471字元
  - Buffer overflow with 'HELP topic'
    - »topic > 514字元

CGI:PHF檢查參數不嚴格

http://theatre.nia.edu.tw/cgi-bin/phf?Qalias=x /bin/cat /etc/passwd - Micros

File Edit View Favorites Tools Help

Back Search Favorites History

Address http://theatre.nia.edu.tw/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

Links Customize Links Free Hotmail Windows

Query Results

/usr/local/bin/ph -m alias=x /bin/cat /etc/passwd

```
root:x:0:0:Super-User:/:/bin/csh
sysadm:x:0:0:System ¥ Administration:/usr/admin:/dev/null
diag:x:0:996:Hardware Diagnostics:/usr/diags:/dev/null
daemon:x:1:1:daemons:/:/dev/null
```

常見的攻擊手法III

- 利用通訊協定的弱點（SYN-Flood、SMTP）
- 假造 IP 位址（IP Spoofing）
- 偽造 DNS 資訊（DNS Spoofing）
- 攔截、替代封包（Session Hijack）
- 偽裝 Client 或 Server
- 遠端掃瞄（Port Scanning）

常見的攻擊手法IV

- 針對個人（Windows）的攻擊
  - 存取未經限制的資源分享
  - 電子郵件、資料檔、網頁（夾帶病毒、巨集、程式碼）
  - Web Bomb、ICQ Bomb、Mail Bomb
  - 程式的漏洞（MSIE、ICQ、FTP）
  - OOB、IGMP（一擊必殺）
  - Bo2k（後門程式）

破壞防毒軟體防護－電腦病毒、木馬程式

- 修改系統日期
- 停止防毒(防駭)軟體及安全性服務
- 修改系統登錄值

偽裝－蠕蟲、木馬程式

- 圖示
- 檔名
- E-amil
- 服務及驅動程式
- 網站

惡意程式攻擊手法分析

自動執行－電腦病毒、木馬程式、蠕蟲

- 修改登錄值
- 掛載(替換)驅動程式
- 載入服務
- 啟動項目
- 執行程式侵入
- 利用系統特性(功能)結合登錄值

其它惡意行為－電腦病毒、木馬程式、蠕蟲

- 隱藏程序、鍵盤側錄、網路探測、竊取資訊…

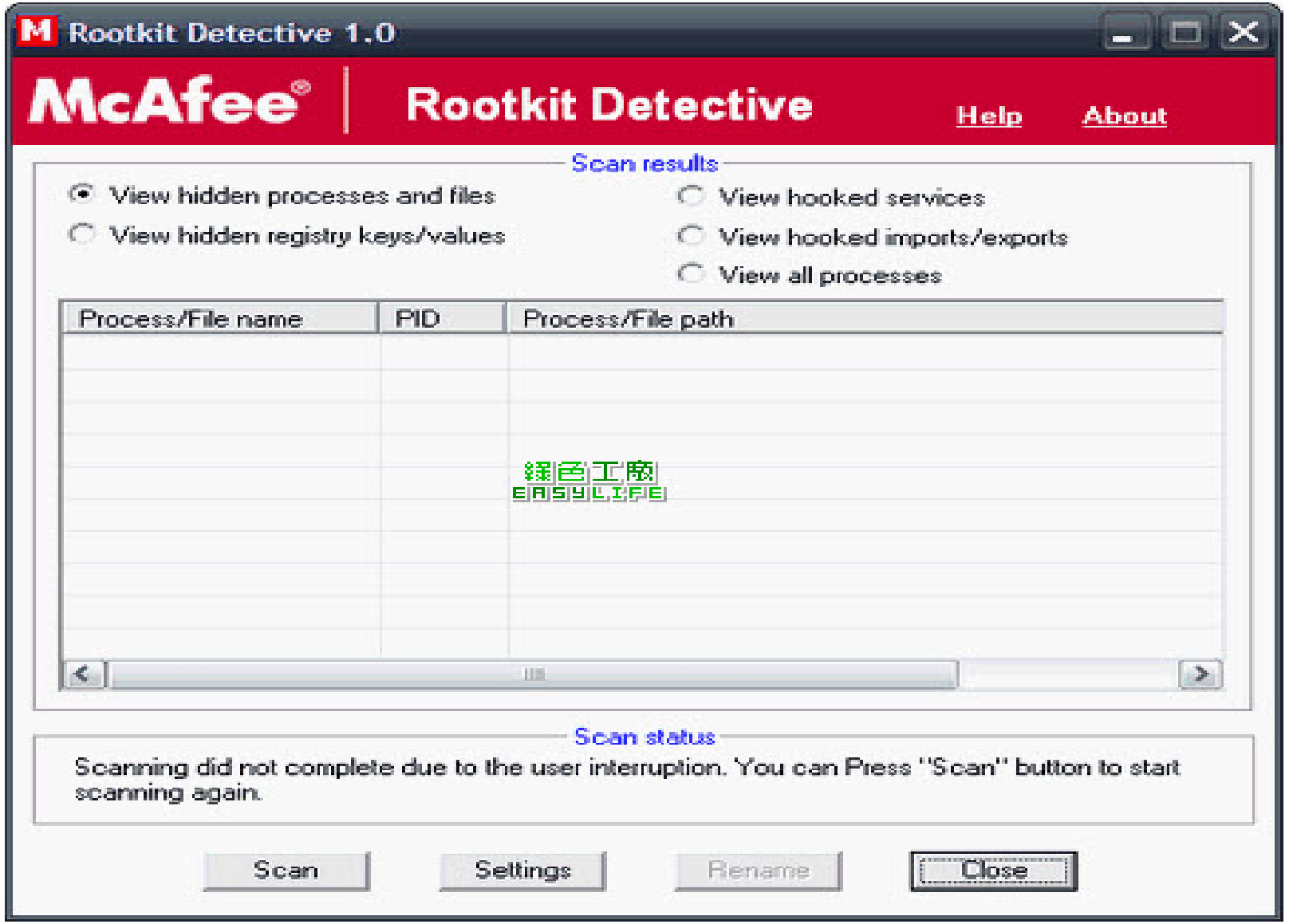
惡意程式分析工具

惡意程式分析工具

- RootKit Detective
- Process Explorer (Procexp)
- TCP/UDP endpoint Viewer (Tcp view)
- RootkitRevealer
- NPASCAN
- GetSystemInfo
- HijackThis
- System Repair Engineer (SREng)
- RootKit Buster

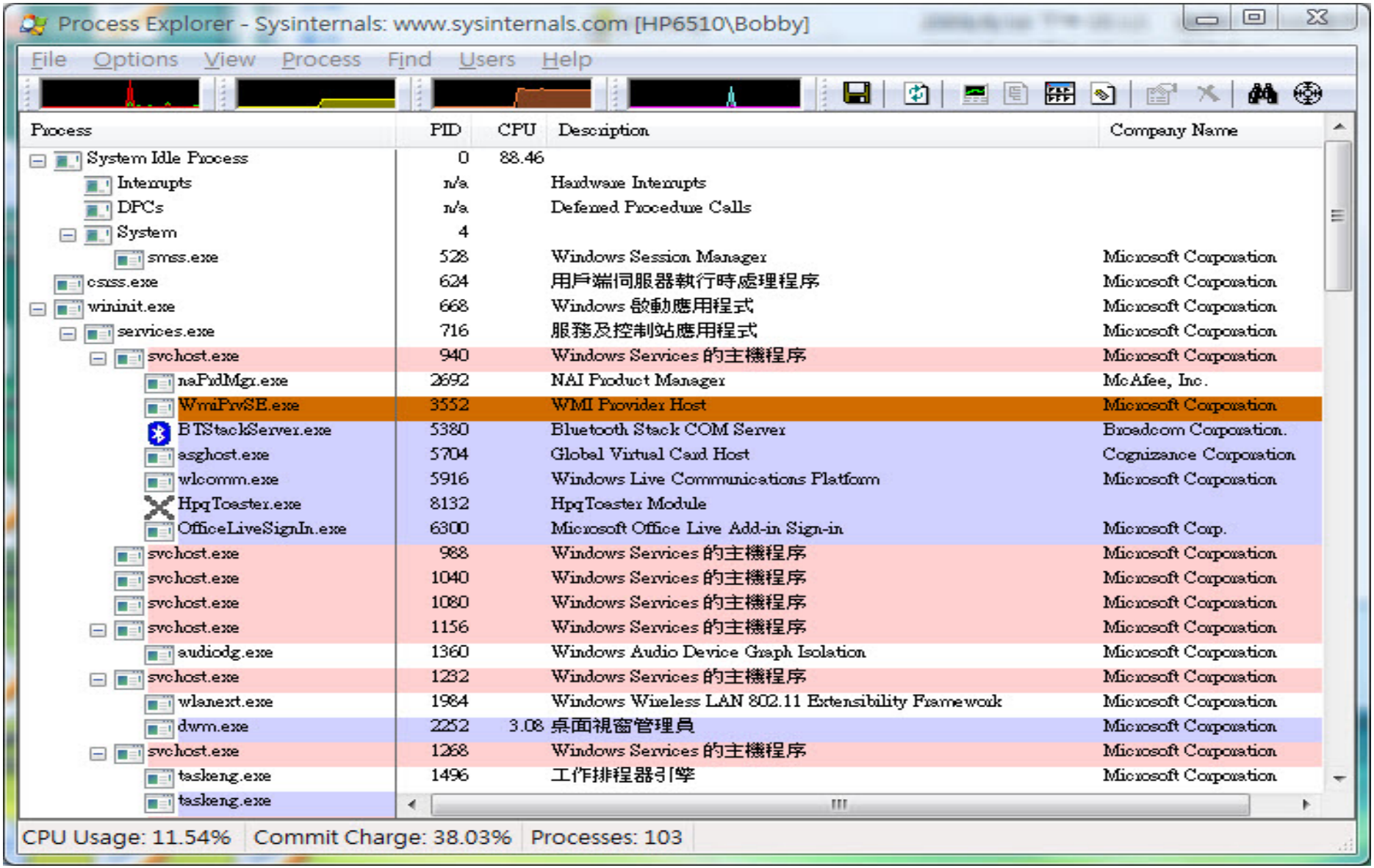
RootKit Detective

- 掃瞄系統中的RootKit


Rootkit Detective 1.0
McAfee
Rootkit Detective
Help
About
Scan results
View hidden processes and files
View hidden registry keys/values
View hooked services
View hooked imports/exports
View all processes
Process/File name
PID
Process/File path
綠色工廠
EASYLIFE
Scan status
Scanning did not complete due to the user interruption. You can Press "Scan" button to start scanning again.
Scan
Settings
Rename
Close

Process Explorer（Procexp）

- Sysinternals開發免費工具
- 檢視系統執行程序與相關即時資訊及存檔
- 刪除、暫停、重新啟動執行程序與除錯
- 調整執行程序優先權
- 線上查詢執行程序相關資訊
- 調整執行程式的使用者權限


Process Explorer - Sysinternals: www.sysinternals.com [HP6510\Bobby]
File Options View Process Find Users Help
Process PID CPU Description Company Name
System Idle Process 0 88.46
Interrupts n/a Hardware Interrupts
DPCs n/a Deferred Procedure Calls
System 4
smss.exe 528 Windows Session Manager Microsoft Corporation
csrss.exe 624 用戶端伺服器執行時處理程序 Microsoft Corporation
wininit.exe 668 Windows 啟動應用程式 Microsoft Corporation
services.exe 716 服務及控制站應用程式 Microsoft Corporation
svchost.exe 940 Windows Services 的主機程序 Microsoft Corporation
naPrdMgr.exe 2692 NAI Product Manager McAfee, Inc.
WmiPrvSE.exe 3552 WMI Provider Host Microsoft Corporation
BTStackServer.exe 5380 Bluetooth Stack COM Server Broadcom Corporation.
asghost.exe 5704 Global Virtual Card Host Cognizance Corporation
wlcomm.exe 5916 Windows Live Communications Platform Microsoft Corporation
HpqToaster.exe 8132 HpqToaster Module
OfficeLiveSignIn.exe 6300 Microsoft Office Live Add-in Sign-in Microsoft Corp.
svchost.exe 988 Windows Services 的主機程序 Microsoft Corporation
svchost.exe 1040 Windows Services 的主機程序 Microsoft Corporation
svchost.exe 1080 Windows Services 的主機程序 Microsoft Corporation
svchost.exe 1156 Windows Services 的主機程序 Microsoft Corporation
audiodg.exe 1360 Windows Audio Device Graph Isolation Microsoft Corporation
svchost.exe 1232 Windows Services 的主機程序 Microsoft Corporation
wlanext.exe 1984 Windows Wireless LAN 802.11 Extensibility Framework Microsoft Corporation
dwm.exe 2252 3.08 桌面視窗管理員 Microsoft Corporation
svchost.exe 1268 Windows Services 的主機程序 Microsoft Corporation
taskeng.exe 1496 工作排程器引擎 Microsoft Corporation
taskeng.exe
CPU Usage: 11.54% Commit Charge: 38.03% Processes: 103

TCP/UDP endpoint Viewer(Tcpview)

- Sysinternals開發免費工具
- 檢視已開啟連接埠即時狀態
- 檢視與終止已開啟連接埠系統執行程序
- 儲存目前系統開啟連接埠資訊

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Proc...	Protocol	Local Address	Remote Address	State
iexplore.ex...	TCP	hp6510:59926	74.217.50.10:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59935	74.217.50.10:http	ESTABLISHED
iexplore.ex...	UDP	HP6510:60375	*:*	
iexplore.ex...	UDP	HP6510:59155	*:*	
iexplore.ex...	UDP	HP6510:65148	*:*	
iexplore.ex...	UDP	HP6510:58806	*:*	
iexplore.ex...	TCP	hp6510:59938	72.14.213.104:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59939	74.125.155.101:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59943	207.46.16.252:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59944	207.46.16.252:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59946	203.69.113.32:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59947	203.69.113.32:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59948	203.69.113.26:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59949	203.69.113.18:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59950	203.69.113.18:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59952	203.69.113.18:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59953	65.55.15.122:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59954	203.69.113.18:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59955	65.55.15.243:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59956	207.46.19.190:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59961	203.69.113.11:http	ESTABLISHED
iexplore.ex...	TCP	hp6510:59962	65.55.15.125:http	ESTABLISHED

Endpoints: 125 | Established: 41 | Listening: 25 | Time Wait: 1 | Close Wait: 1

RootkitRevealer

- 掃瞄電腦系統中的RootKit

RootkitRevealer - Sysinternals: www.sysinternals.com

File Options Help

Path	Timestamp	Size	Description
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\HackerDefender100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\HackerDefender100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HACKERDEFENDER100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HACKERDEFENDERDRV100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\HackerDefender100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\HackerDefenderDrv100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API.
C:\WINDOWS\hxdef100.2.ini	3/7/2005 5:57 PM	3.61 KB	Hidden from Windows API.
C:\WINDOWS\hxdef100.exe	3/7/2005 5:57 PM	68.50 KB	Hidden from Windows API.
C:\WINDOWS\hxdef100.ini	3/7/2005 5:57 PM	3.78 KB	Hidden from Windows API.
C:\WINDOWS\hxdefdrv.sys	3/7/2005 5:57 PM	3.26 KB	Hidden from Windows API.
C:\WINDOWS\Prefetch\HXDEF100.EXE-1BF5F48A.pf	3/7/2005 5:57 PM	6.14 KB	Hidden from Windows API.

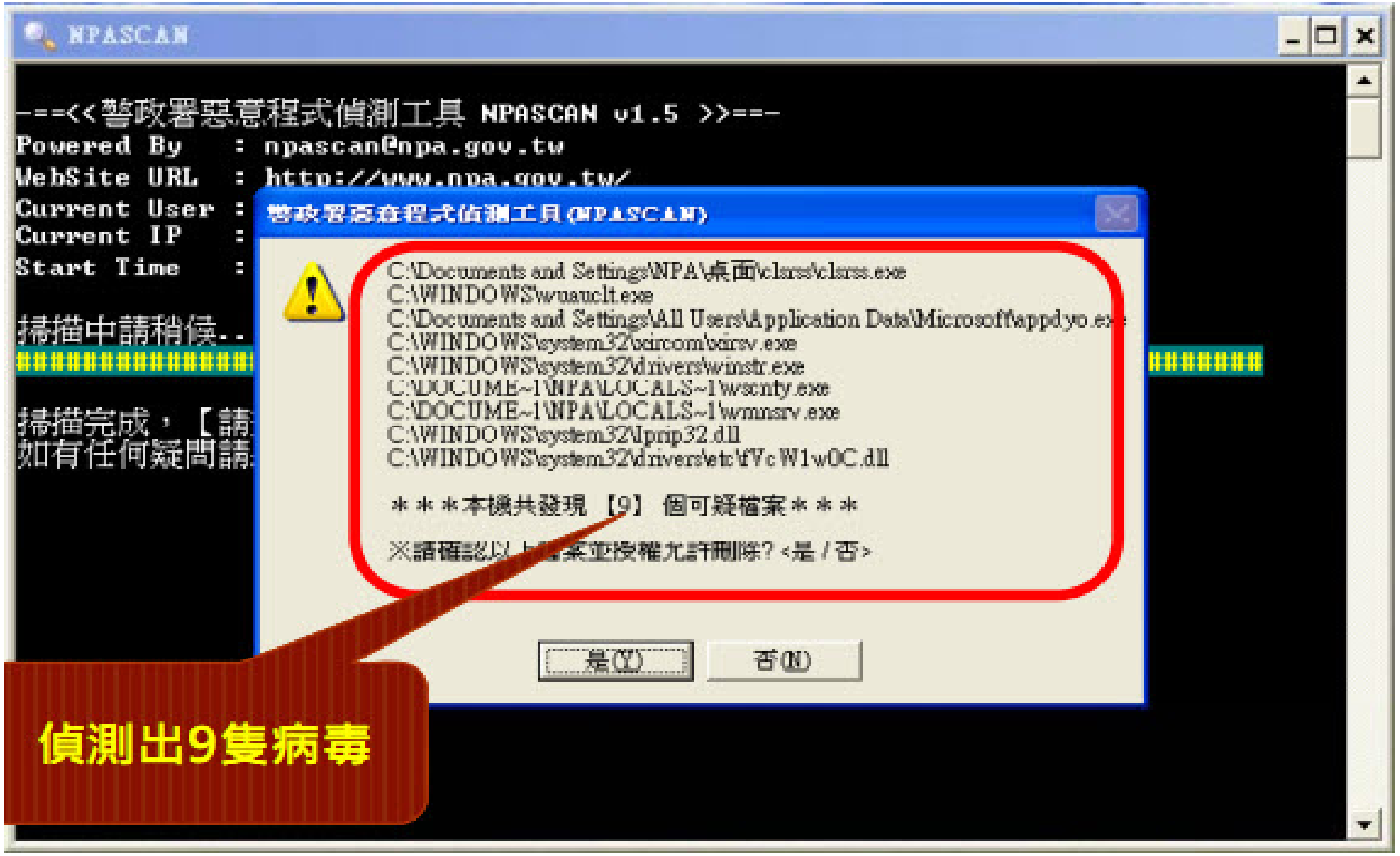
Scan complete: 11 discrepancies found

Scan

惡意程式分析工具

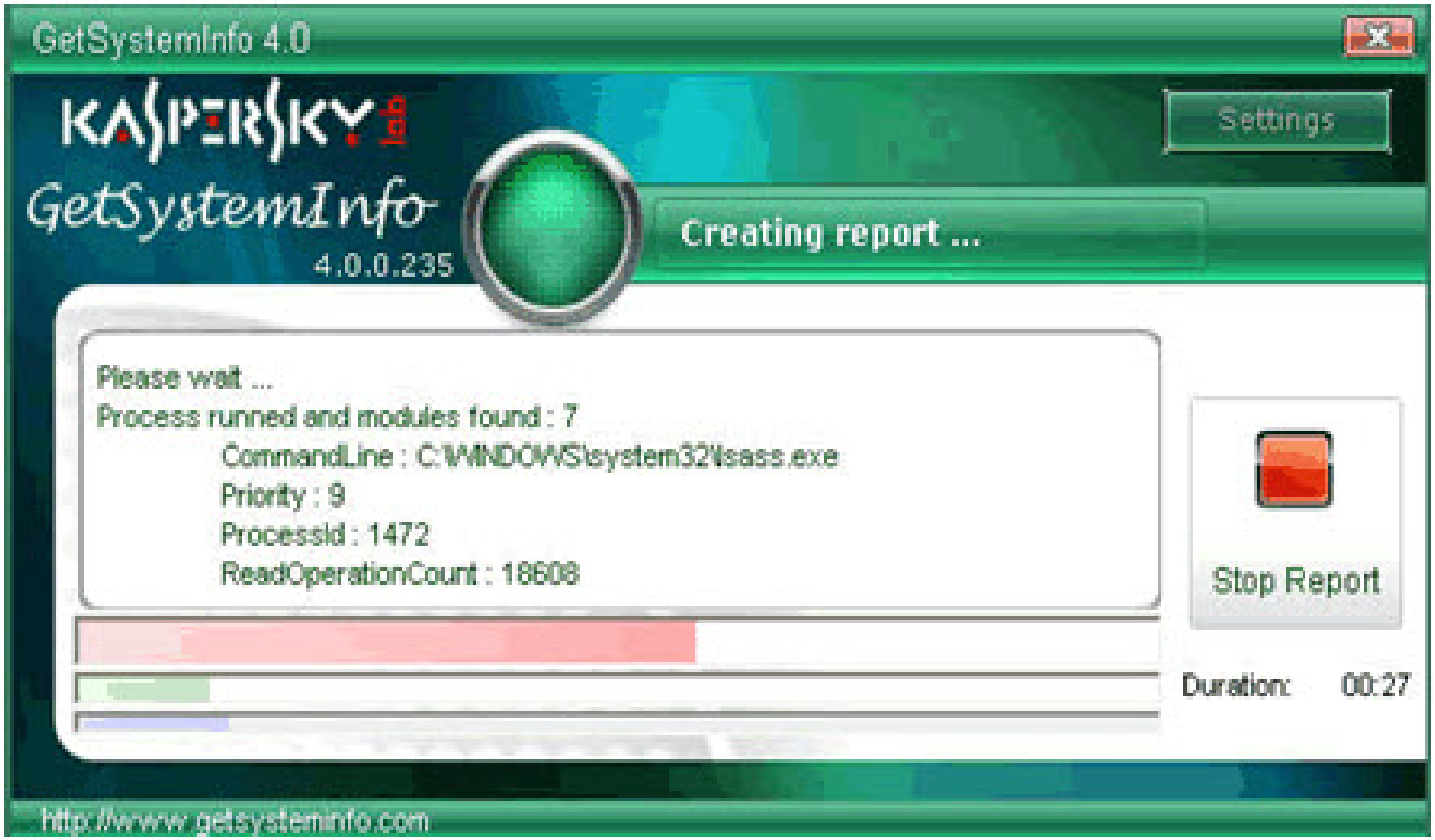
NPAScan

- 掃瞄電腦系統中所有啟動的項目
- 辨識檔案是否為可疑程式
- 可移除掃瞄後的檔案


NPASCAN
---<<警政署惡意程式偵測工具 NPASCAN v1.5 >>---
Powered By : npascan@npa.gov.tw
WebSite URL : http://www.npa.gov.tw/
Current User :
Current IP :
Start Time :
掃描中請稍候..
掃描完成，【請
如有任何疑問請
警政署惡意程式偵測工具(NPASCAN)
C:\Documents and Settings\NPA\桌面\vclass\vclass.exe
C:\WINDOWS\wuauclt.exe
C:\Documents and Settings\All Users\Application Data\Microsoft\appdyo.exe
C:\WINDOWS\system32\oircom\oirsv.exe
C:\WINDOWS\system32\drivers\winstr.exe
C:\DOCUME~1\NPA\LOCALS~1\wscnty.exe
C:\DOCUME~1\NPA\LOCALS~1\wmnsrv.exe
C:\WINDOWS\system32\lprip32.dll
C:\WINDOWS\system32\drivers\etc\tYc W1w0C.dll
＊＊＊本機共發現 【9】 個可疑檔案＊＊＊
※請確認以上檔案並授權允許刪除? <是 / 否>
是(Y)
否(N)
偵測出9隻病毒

GetSystemInfo

- 收集系統資訊


GetSystemInfo 4.0
KASPERSKY lab
GetSystemInfo
4.0.0.235
Settings
Creating report ...
Please wait ...
Process runned and modules found : 7
CommandLine : C:\WINDOWS\system32\lsass.exe
Priority : 9
ProcessId : 1472
ReadOperationCount : 18608
Stop Report
Duration: 00:27
http://www.getsysteminfo.com

惡意程式分析工具

HijackThis

- 收集使用者系統中的資訊與設定
- 管理與觀察目前系統運作中的Process

Trend Micro HijackThis - v2.0.2

O23 - NT Services...

O1 - Hosts: ::1 localhost
O2 - BHO: SnagIt Toolbar Loader - {00C6482D-C502-44C8-8409-FCE54AD9C208} - C:\Program Files\TechSm
O2 - BHO: (no name) - {5C255C8A-E604-49b4-9D64-90988571CECB} - (no file)
O2 - BHO: scriptproxy - {7DB2D5A0-7241-4E79-B68D-6309F01C5231} - C:\Program Files\McAfee\VirusScan
O2 - BHO: Windows Live ID 登入協助程式 - {9030D464-4C02-4ABF-8ECC-5164760863C6} - C:\Program Fi
O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files\Google\
O2 - BHO: Google Toolbar Notifier BHO - {AF69DE43-7D58-4638-B6FA-CE66B5AD205D} - C:\Program Files
O2 - BHO: McAfee SiteAdvisor BHO - {B164E929-A1B6-4A06-B104-2CD0E90A88FF} - C:\Program Files\McA
O2 - BHO: Google Dictionary Compression sdch - {C84D72FE-E17D-4195-BB24-76C02E2E7C4E} - C:\Progra
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program File
O2 - BHO: Credential Manager for HP ProtectTools - {DF21F1DB-80C6-11D3-9483-B03D0EC10000} - c:\Progr
O3 - Toolbar: McAfee SiteAdvisor - {0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064} - C:\Program Files\McA
O3 - Toolbar: SnagIt - {8FF5E183-ABDE-46EB-B09E-D2AAB95CABE3} - C:\Program Files\TechSmith\SnagIt
O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files\Google\Goo
O4 - HKLM\..\Run: [QlbCtrl.exe] C:\Program Files\Hewlett-Packard\HP Quick Launch Buttons\QlbCtrl.exe /Start
O4 - HKLM\..\Run: [SynTPEnh] C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
O4 - HKLM\..\Run: [McAfeeUpdaterUI] "C:\Program Files\McAfee\Common Framework\udaterui.exe" /StartedFr
O4 - HKLM\..\Run: [UnlockerAssistant] ; "C:\Program Files\Unlocker\UnlockerAssistant.exe"
O4 - HKLM\..\Run: [vmware-tray] "C:\Program Files\VMware\VMware Workstation\vmware-tray.exe"
O4 - HKLM\..\Run: [WowUSBSecurity] C:\Program Files\WowUSBProtector\start.bat
O4 - HKLM\..\Run: [QuickTime Task] "C:\Program Files\QuickTime\QTTask.exe" -atboottime
O4 - HKLM\..\Run: [iTunesHelper] "C:\Program Files\iTunes\iTunesHelper.exe"
O4 - HKCU\..\Run: [swg] "C:\Program Files\Google\GoogleToolbarNotifier\GoogleToolbarNotifier.exe"
O4 - HKCU\..\Run: [msnmsgr] "C:\Program Files\Windows Live\Messenger\msnmsgr.exe" /background

Scan & fix stuff
Scan | Fix checked
Info on selected item...

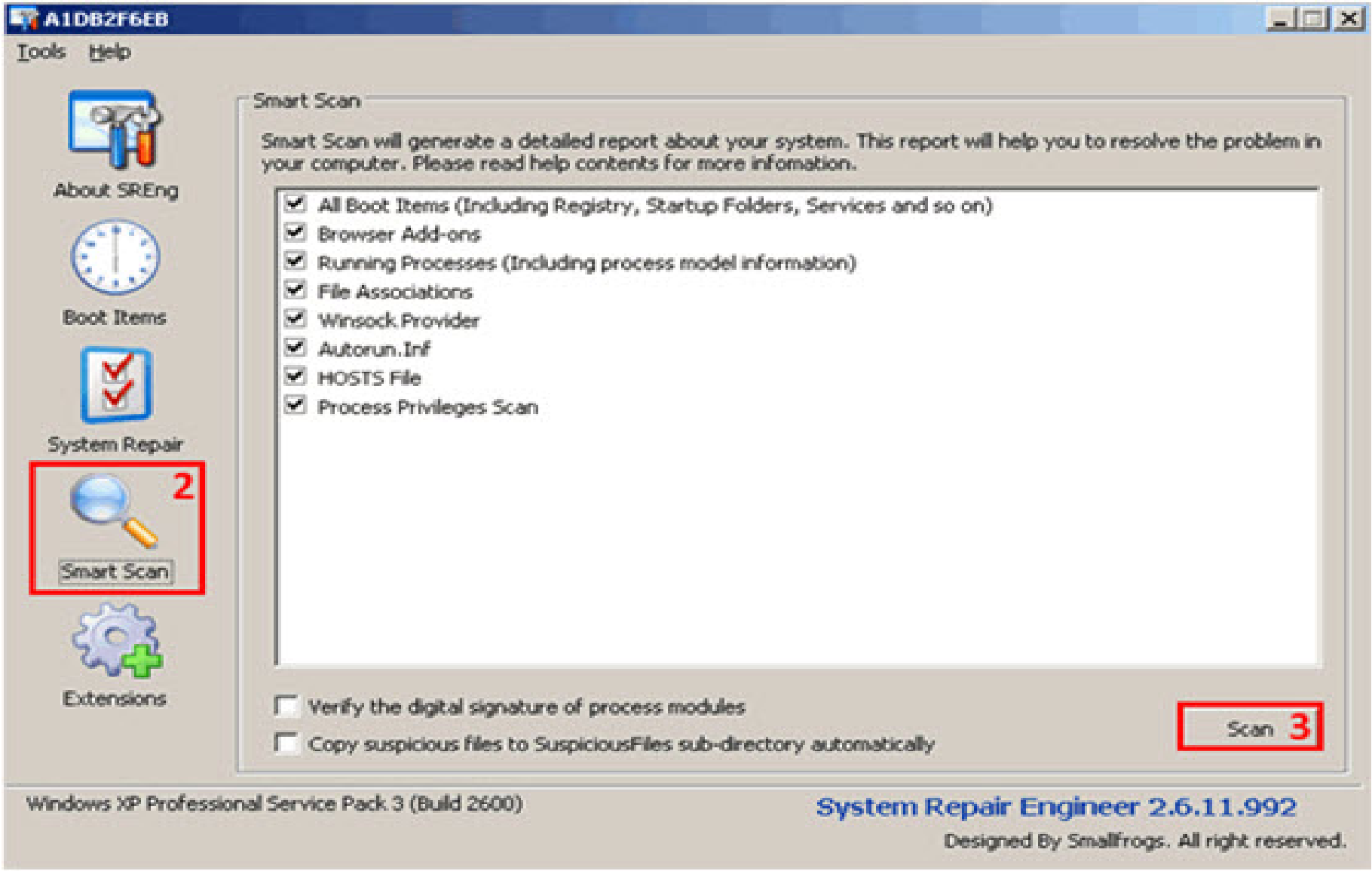
AnalyzeThis
Upload to TrendSecure
Main Menu

Other stuff
Info... | Config...
Add checked to ignorelist

惡意程式分析工具

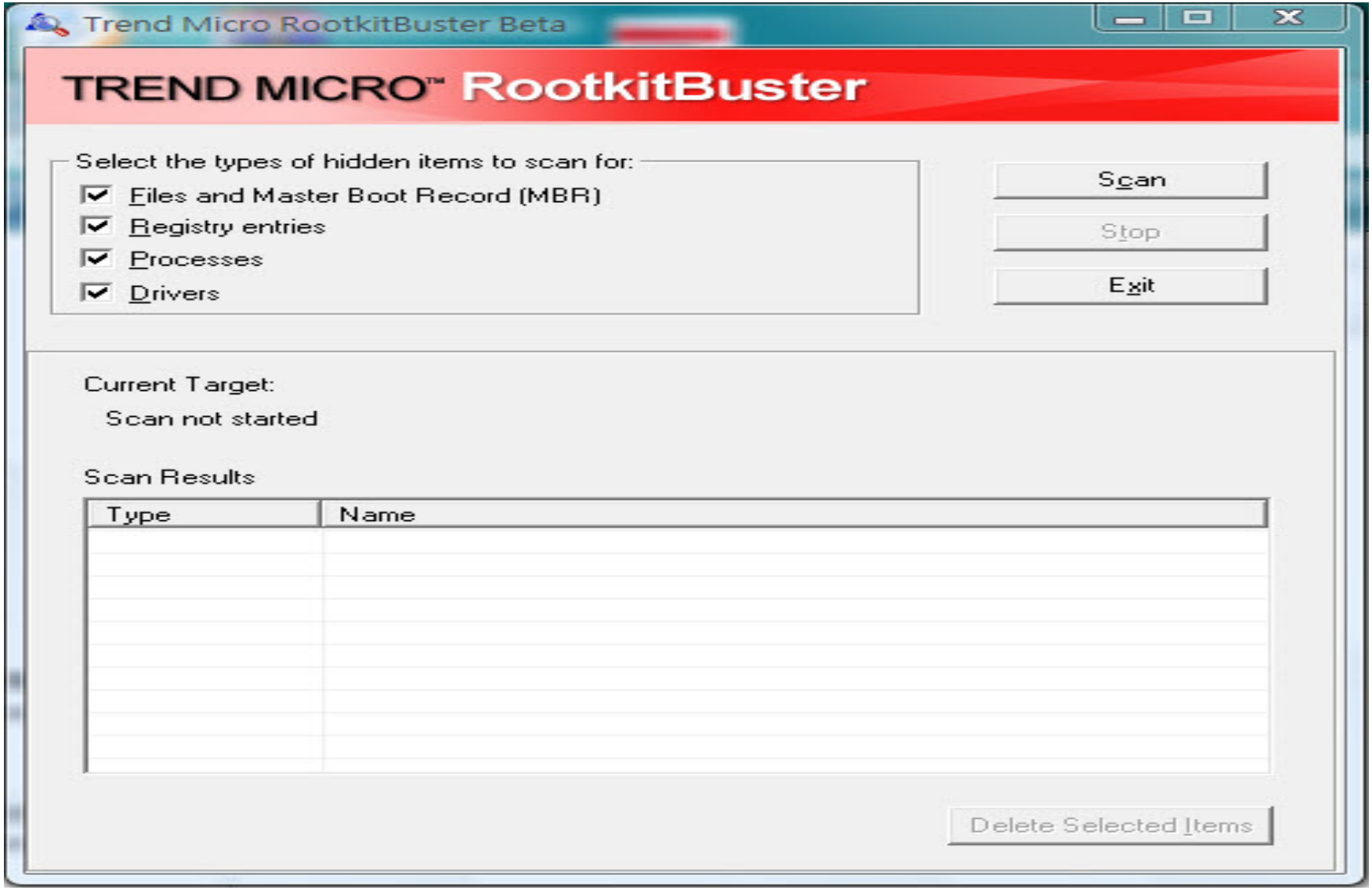
System Repair Engineer(SREng)

- KZTechs.com網站作者Samllfrogs開發免費工具
- 收集系統資訊
- 系統維護與修復
- 主要診斷未經簽署的程序與被修改的登錄資訊
- 資訊較少約15至40kb，分析簡易迅速


A1DB2F6EB
Tools Help
About SREng
Boot Items
System Repair
2
Smart Scan
Extensions
Smart Scan
Smart Scan will generate a detailed report about your system. This report will help you to resolve the problem in your computer. Please read help contents for more information.
All Boot Items (Including Registry, Startup Folders, Services and so on)
Browser Add-ons
Running Processes (Including process model information)
File Associations
Winsock Provider
Autorun.Inf
HOSTS File
Process Privileges Scan
Verify the digital signature of process modules
Copy suspicious files to SuspiciousFiles sub-directory automatically
Scan 3
Windows XP Professional Service Pack 3 (Build 2600)
System Repair Engineer 2.6.11.992
Designed By Smallfrogs. All right reserved.

RootKit Buster

- 掃瞄電腦系統中的RootKit，並予以刪除


Trend Micro RootkitBuster Beta
TREND MICRO™ RootkitBuster
Select the types of hidden items to scan for:
Files and Master Boot Record (MBR)
Registry entries
Processes
Drivers
Scan
Stop
Exit
Current Target:
Scan not started
Scan Results
Type
Name
Delete Selected Items

USB病毒分析與處理

1. USB 病毒的演進
2. 感染症狀、感染過程
3. 解毒的迷思
4. 如何預防USB病毒

USB病毒的演進

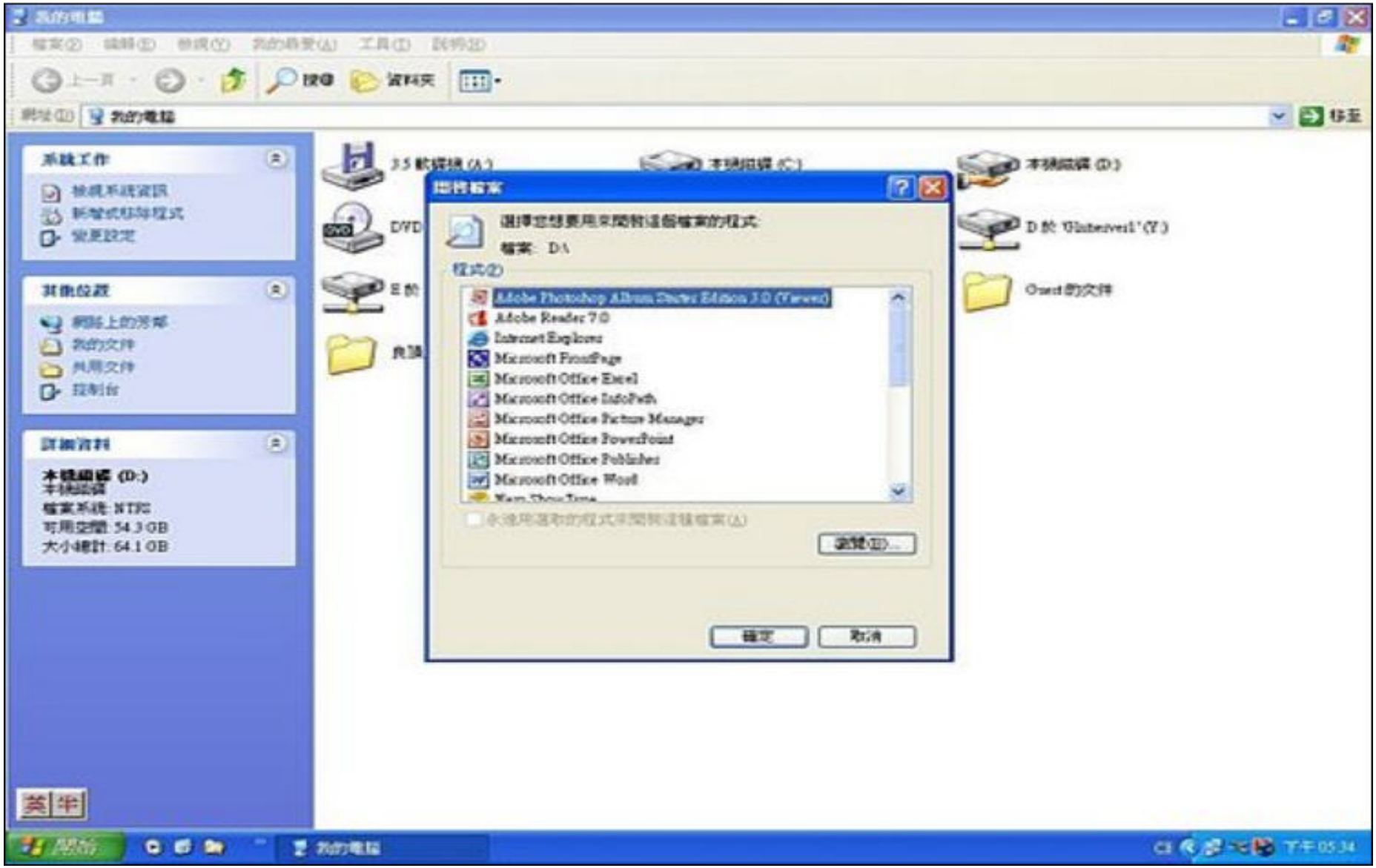
USB病毒的演進

- 2006年開始出現相關的報導：MP3隨身聽、拇指碟、記憶卡、全新的硬碟…
- 2007年七月台灣開始大量散播 （地區性）
- 主要目的：竊取線上遊戲的帳號和密碼
- 傳染途徑：USB裝置
- 損害：系統效能變慢、無法檢視隱藏檔或開啟磁碟

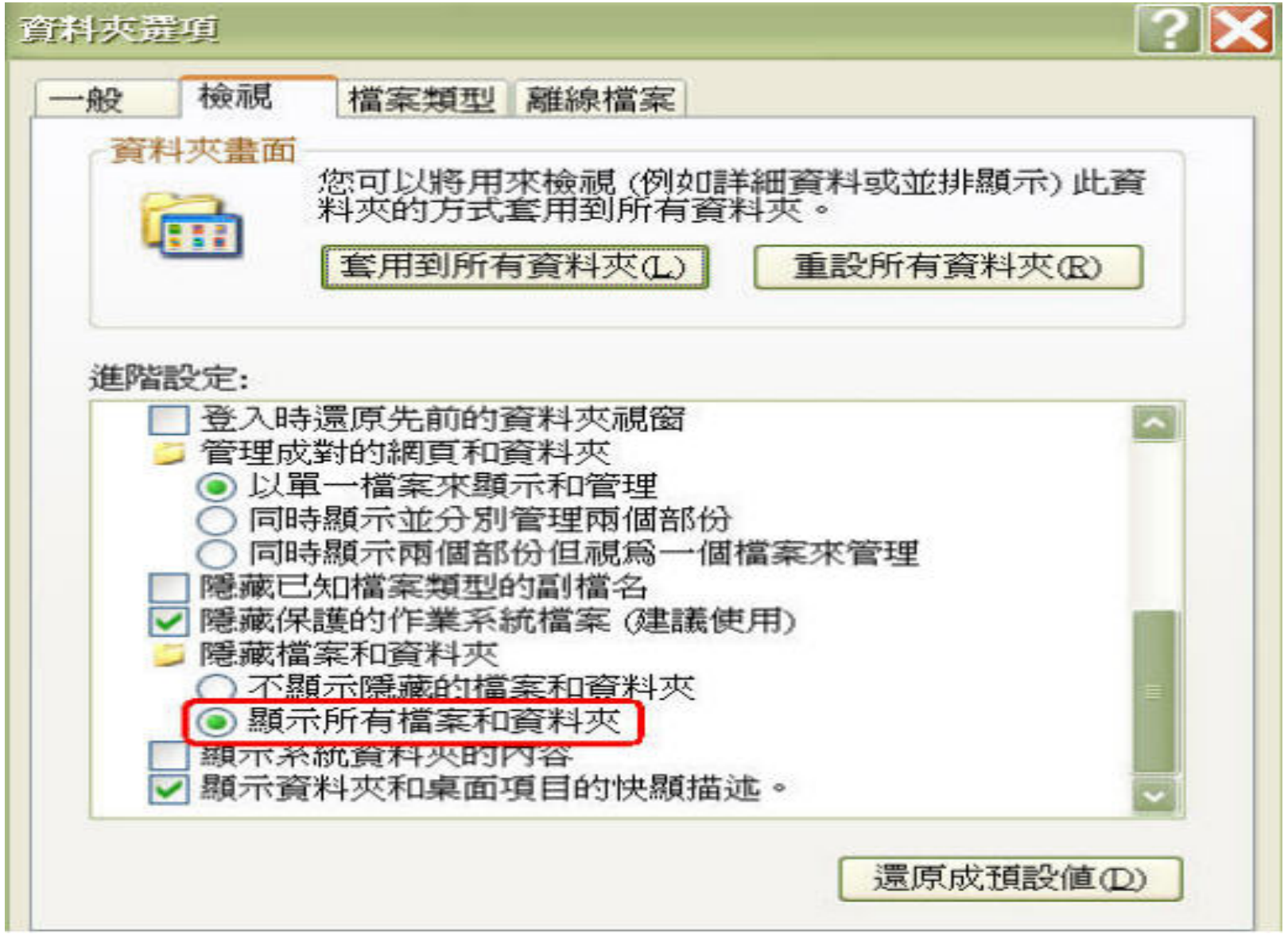
USB病毒的演進

- 新手法：看門狗、自動隱藏、自動更新、社交工程…
- 附加破壞：破壞網路裝置（網路中斷）、無法進入安全模式、停用防毒軟體、無法執行某些程式…
- 其他傳染途徑：網路磁碟、執行檔、郵件附件檔都可能感染

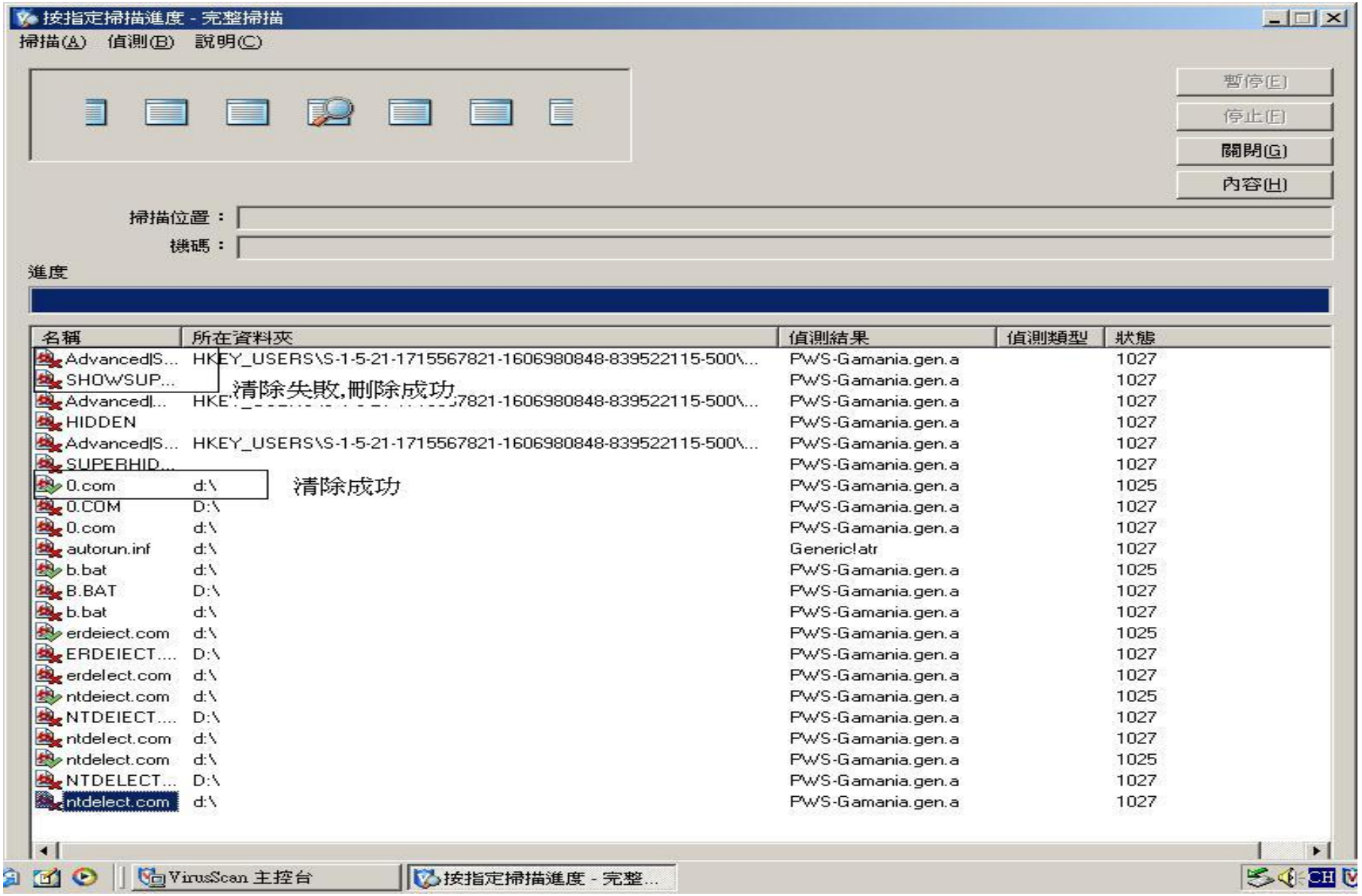
USB病毒中毒畫面


我的電腦
系統工作
其他位置
詳細資料
開啟檔案
選擇您想要用來開啟這個檔案的程式:
檔案: D:\
程式(P)
Adobe Photoshop Album Starter Edition 3.0 (Viewer)
Adobe Reader 7.0
Internet Explorer
Microsoft FrontPage
Microsoft Office Excel
Microsoft Office InfoPath
Microsoft Office Picture Manager
Microsoft Office PowerPoint
Microsoft Office Publisher
Microsoft Office Word
瀏覽(B)...
確定
取消
英半
開始

USB病毒中毒畫面


資料夾選項
一般
檢視
檔案類型
離線檔案
資料夾畫面
您可以將用來檢視 (例如詳細資料或並排顯示) 此資料夾的方式套用到所有資料夾。
套用到所有資料夾(L)
重設所有資料夾(R)
進階設定:
登入時還原先前的資料夾視窗
管理成對的網頁和資料夾
以單一檔案來顯示和管理
同時顯示並分別管理兩個部份
同時顯示兩個部份但視爲一個檔案來管理
隱藏已知檔案類型的副檔名
隱藏保護的作業系統檔案 (建議使用)
隱藏檔案和資料夾
不顯示隱藏的檔案和資料夾
顯示所有檔案和資料夾
顯示系統資料夾的內容
顯示資料夾和桌面項目的快顯描述。
還原成預設值(D)

USB病毒中毒畫面


按指定掃描進度 - 完整掃描
掃描(A) 偵測(B) 說明(C)
暫停(E)
停止(T)
關閉(C)
內容(H)
掃描位置：
機碼：
進度
名稱 所在資料夾 偵測結果 偵測類型 狀態
AdvancedIS... HKEY_USERS\S-1-5-21-1715567821-1606980848-839522115-500\... PWS-Gamania.gen.a 1027
SHOWSUP... PWS-Gamania.gen.a 1027
清除失敗,刪除成功
AdvancedI... HKE...7821-1606980848-839522115-500\... PWS-Gamania.gen.a 1027
HIDDEN PWS-Gamania.gen.a 1027
AdvancedIS... HKEY_USERS\S-1-5-21-1715567821-1606980848-839522115-500\... PWS-Gamania.gen.a 1027
SUPERHID... PWS-Gamania.gen.a 1027
0.com d:\ 清除成功 PWS-Gamania.gen.a 1025
0.COM D:\ PWS-Gamania.gen.a 1027
0.com d:\ PWS-Gamania.gen.a 1027
autorun.inf d:\ Generic!atr 1027
b.bat d:\ PWS-Gamania.gen.a 1025
B.BAT D:\ PWS-Gamania.gen.a 1027
b.bat d:\ PWS-Gamania.gen.a 1027
erdeiect.com d:\ PWS-Gamania.gen.a 1025
ERDEIECT.... D:\ PWS-Gamania.gen.a 1027
erdelect.com d:\ PWS-Gamania.gen.a 1027
ntdeiect.com d:\ PWS-Gamania.gen.a 1025
NTDEIECT.... D:\ PWS-Gamania.gen.a 1027
ntdelect.com d:\ PWS-Gamania.gen.a 1027
ntdelect.com d:\ PWS-Gamania.gen.a 1025
NTDELECT... D:\ PWS-Gamania.gen.a 1027
ntdelect.com d:\ PWS-Gamania.gen.a 1027
VirusScan 主控台
按指定掃描進度 - 完整...
CH

感染症狀、過程

感染症狀

- 破壞作業系統：程式執行發生錯誤、系統當機（BSOD）、系統日期錯誤
- 破壞防毒軟體：防毒軟體無法運作，或部份元件無法執行
- 網路裝置元件故障：無法上網及更新
- 解毒後可能無法直接開啟磁碟機，或是出現程式執行錯誤的提示訊息

感染過程

第1階段：木馬程式開始執行

1. 在%tmep%資料夾產生DLL格式的木馬程式
2. 替換系統驅動程式檔案vga.sys，造成防毒軟體元件損毀，無法進入安全模式
3. 產生隱藏屬性的檔案，例如：kxvo.exe、kxvoX.dll（X為累加數）
4. kxvoX.dll插入explorer.exe執行程序，並持續惡意行為

感染過程

第2階段：IExplorer.exe自動下載惡意軟體

1. IExplorer.exe自動下載木馬程式cc.exe至 %temp% 下，此惡意軟體一直變種，名稱為 Trojan-GameThief.Win32.OnLineGames.xxxx
2. IExplorer.exe會持續在 %temp% 路徑刪除與建立 cc.exe

感染過程

第3階段：cc.exe自動執行

1. cc.exe執行後會破壞防毒軟體
2. 替換tdi.sys。造成網路裝置無法使用
3. 產生隱藏屬性的檔案，例如：j3ewro.exe、jwedsfdo0.dll
4. 新增登錄檔，以便在登入系統後自動執行
5. 由jwedsfdo0.dll持續惡意行為，cc.exe即停止運作

第4階段：IExplorer.exe自動下載惡意軟體

1. IExplorer.exe自動下載木馬程式ff.exe至 %temp% 路徑，此惡意軟體經常變種
2. IExplorer.exe會持續在 %temp% 路徑刪除與建立 ff.exe

第5階段：惡意軟體藉由explorer.exe執行程序進行惡意攻擊

1. 刪除 %temp% 路徑下cc&ff.exe惡意軟體
2. 持續修改登錄檔，藉以隱藏惡意檔案
3. 新增登錄檔：當使用者透過「我的電腦」開啟任何磁碟區，就會觸發惡意軟體執行
4. 持續在磁碟根目錄刪除與建立autorun.inf及對應的執行檔

感染過程

第6階段：ff.exe自動執行

1. 如同cc.exe，ff.exe會下載tdi.sys並置換
2. 產生隱藏屬性的檔案，例如：kxvo.exe 、kxvoX.dll
3. 新增登錄檔，以便在登入系統後自動執行
4. 由kxvoX.dll持續惡意行為，ff.exe即停止運作

第7階段：惡意軟體在開機時自動啟動及更新

若未即時解毒，即會產生新的變種病毒

感染手法補充

增加以下登錄值，開機後即自動執行kxvo.exe

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run

“tasoft"= "C:\WINDOWS\SYSTEM32\kxvo.exe “

“jvsoft"= "C:\WINDOWS\SYSTEM32\j3ewro.exe “

持續修改以下登錄值，無法顯示所有檔案和資料夾

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL

"CheckedValue"=dword:00000000（正常為1）

解毒的迷思

解毒的迷思

- USB病毒讓許多使用者和MIS頭痛不已，因為它防不勝防，殺了又中、中了再殺
- 無止盡的變種病毒更讓防毒軟體防不勝防
- 抓不到病毒成了防毒軟體的原罪！
- 專殺工具、民俗療法真的有效嗎？

解毒的迷思

坊間常見的「民俗療法」

網路偏方	效果	說明
建立 Autorun.inf 資料夾 停用 Autorun 功能	部份有效	可以暫緩病毒發作。新的變種病毒會先刪除舊有的 Autorun.inf 資料夾或檔案，或是自行啟動 Autorun 功能。 建議移除該資料夾安全性頁籤中的所有使用者及群組，才能防止被竄改。
按住 Shift 鍵開啟隨身碟	無效	只能關閉 Autoplay，無法關閉 Autorun。
在隨身碟上按右鍵開啟檔案總管	部份有效	透過「我的電腦」去點選，仍會遭感染。若正確地透過「檔案總管」來開啟，則不會感染。
啟用隨身碟的唯讀功能	無效	若是隨身碟已感染病毒，只要能執行，就可以感染作業系統。
軟體限制原則	部份有效	能阻止病毒從 USB 裝置擴散，但無法防範從網路磁碟或郵件附件檔執行。
禁用 USB 裝置	部份有效	能阻止病毒從 USB 裝置擴散，但無法防範從網路磁碟或郵件附件檔執行。
USB 病毒專殺工具	短期有效	若未定期更新，只能清除舊病毒。而且工具來源不一定安全。

感染症狀

為什麼防毒軟體無法提供有效的防護呢？

- 防毒軟體屬於被動防護，必須要有病毒特徵碼，才能偵測與解毒
- 現今病毒都是小區域暴發，不易收集樣本（之前是全球大規則暴發）
- 化被動為主動，善用新的防護技術（免疫防護、啟發式分析、HIPS）才能偵測未知病毒

如何預防USB病毒

如何防範USB類型病毒？ （預防勝於治療）

- 不要因為一時好奇，而任意開啟或執行來路不明的檔案
- 在開啟檔案之前，建議先以防毒軟體進行掃瞄
- 定期更新防毒軟體、並執行完整掃瞄
- 將磁碟或USB外接式儲存媒體轉換為NTFS格式，在根目錄設置Autorun.inf目錄並移除所有權限
- 透過教育訓練灌輸使用者正確防護概念與良好電腦操作習慣

實際案例探討

Sony DRM Rootkit

2003年發現Sony DRM Rootkit的是一位知名軟體工程師、講師、顧問和作家Mark Russinovich

Russinovich測試自己創作的RootkitRevealer時，赫然發現自己的其中一部電腦竟然藏著rootkit程式，但在確定電腦所安裝的程式來源無誤，也找不出rootkit程式來源

後來經過反覆的測試， Russinovich發現Rootkit來源竟然是從亞馬遜網站買了一張Sony BMG發行的音樂光碟

Sony DRM Rootkit

這張光碟有一種稱為XCP的內容保護技術，用Google查詢才得知，有好幾家唱片公司都採用了這家公司的XCP技術，作為音樂光碟的數位版權管理

這張光碟在電腦上只能以光碟內建的程式播放，而且限制只能複製三次。Russinovich以Process Explorer檢視光碟內建的程式播放，發現程式是來自Macromedia，但是當開始播放音樂之後，sysDRMServer.exe的CPU使用率就越來越高，而這支程式就是之前找到的rootkit所附帶的程式

Sony DRM Rootkit

這起事件引發了相當多的效應，除了隱私權和電腦控制權之外，系統管理者可能又得多擔心一項資安威脅的入侵管道：原本非常單純的播放音樂光碟，沒想到竟然可以植入rootkit程式。

這個rootkit會隱藏任何名稱是sys開頭的行程、檔案、資料夾或登錄資料庫機碼，而目前也已經出現利用這個rootkit達到隱藏效果的惡意軟體。

Seagate Trojan

2007 年 8 月之後購買 Maxtor Basics Personal Storage 3200 產品，該產品可能已遭到病毒感染。

Seagate 提出警示，已在至少一套 Maxtor Basics Personal Storage 3200 產品中發現一種病毒。

根據 Kaspersky 的資料，該病毒名為 Virus.Win32.AutoRun.ah，這種竊密病毒會搜尋線上遊戲的密碼，然後傳送到位於中國的伺服器。此外，它還會刪除其他竊密軟體，並且停用病毒偵測軟體。

Asus Trojan

ASUS公佈於日本出售的 Eee BOX B202 桌面電腦產品，被發現被感染病毒需全面回收及更換新品，而搭配 Eee PC 出貨的 30G USB 外接式硬碟配件亦同樣發現感染病毒。

這次感染的是「W32.SillyFDC」， 也就是俗稱『隨身碟病毒』的蠕蟲程式。 這次的病毒是存在於D槽的「Recycled.exe」， 並且也有「autorun.inf」。所以只要一打開D槽，病毒立即開始感染擴散， 只要做儲存媒體的讀寫動作，或使用USB隨身碟，都會造成病毒的感染！

So-net網站遭駭

2007年臺灣So-net網站遭駭客入侵，會員個人資料外洩，導致信用卡被盜刷約1,840張

經警方調查，駭客來自中國大陸，係以俗稱「釣魚網站」的假網頁，藉由郵寄電子郵件、圖檔等方式夾帶木馬程式入侵，So-net員工甚至高層幹部都不知自己的電腦已中毒。

警察機關使用P2P軟體洩密事件

2007年4月爆發警察機關因員警違規使用P2P分享軟體FOXY，而導致內部筆錄外洩的新聞事件，刑事局則發現，有部份以「刑案筆錄」等文字為檔名的假檔案，在新聞熱潮下透過FOXY傳散，實際內容則為援交訊息、護膚按摩廣告甚至內含惡意程式。

在P2P軟體上，檔名與實際內容不符的假檔案相當常見，也是駭客散佈惡意程式的途徑之一，類似的社交工程手法本身雖不算新，但常會利用熱門新聞事件的話題性，引誘使用者下載、點選，導致木馬上身。

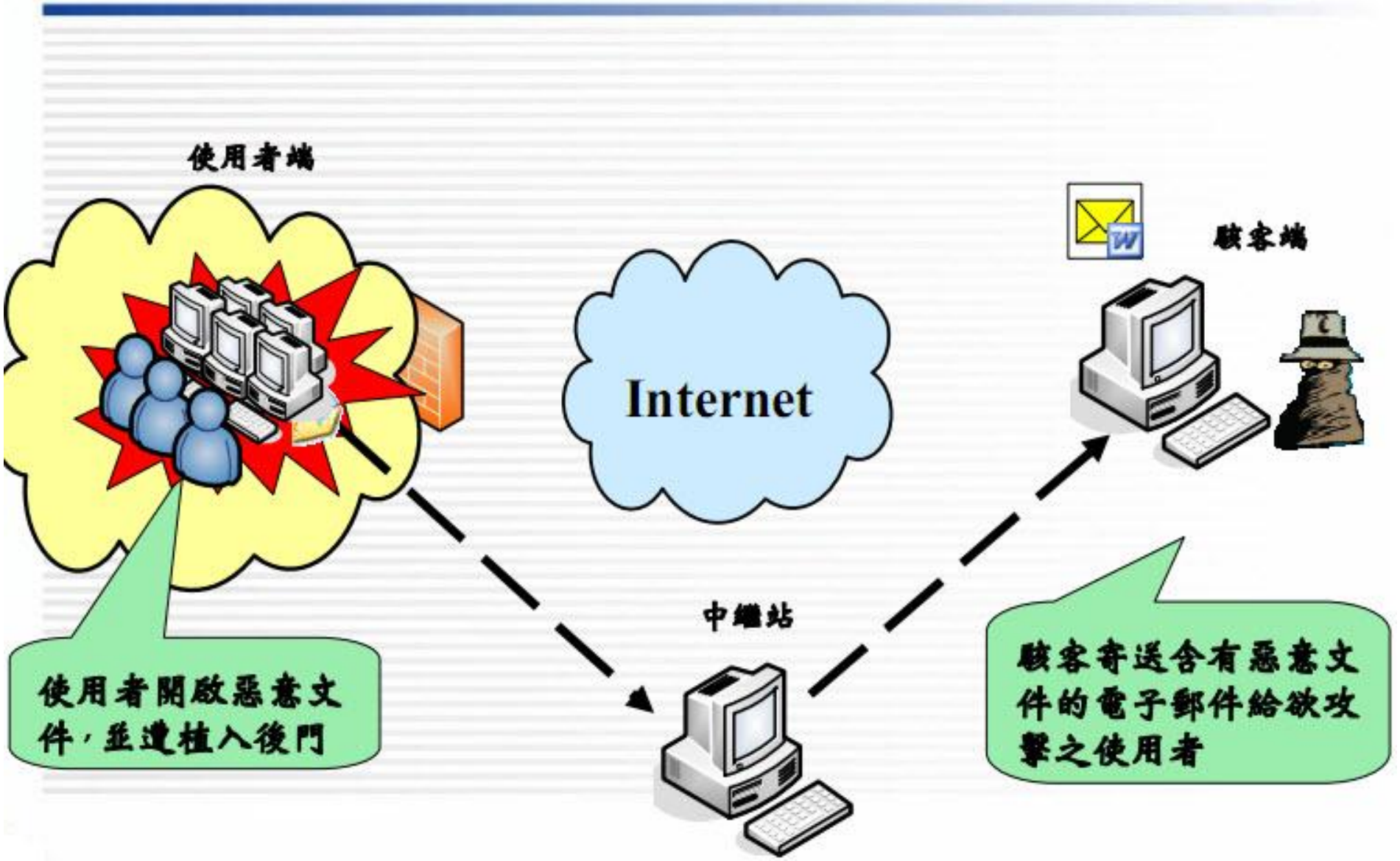
真實案例

- **中國駭客攻擊遊戲網站，脅迫配合宣傳**(2008/05/04)
  - 國內最知名的遊戲討論社群遊戲基地與巴哈姆特，分別遭到DDoS(分散式阻斷服務)攻擊，來自中國大陸的駭客甚至要求網站配合宣傳，否則將繼續攻擊，行徑令業者咋舌。 擁有眾多使用者的巴哈姆特與遊戲基地網站，自前(27)天起分別傳出因同時湧現大量連線要求導致首頁主機當機事件。
  - http://vbb.twftp.org/showthread.php?t=12019

- **首例DDOS攻擊案告破，遐邇防火牆老總羅春被抓**(2007/07/25)
  - 2007年6月10日晚，北京海澱區，完美時空公司總部遭遇駭客攻擊。公司技術部工作人員最先發現異常，大量攻擊數據突然從網上湧來，衝向公司DNS伺服器，隨後網站癱瘓無法打開。
  - http://202.99.120.116:82/gate/big5/jike.it168.com/8876389/viewspace-1793

從郵件安全角度看惡意程式

E-mail社交工程手法

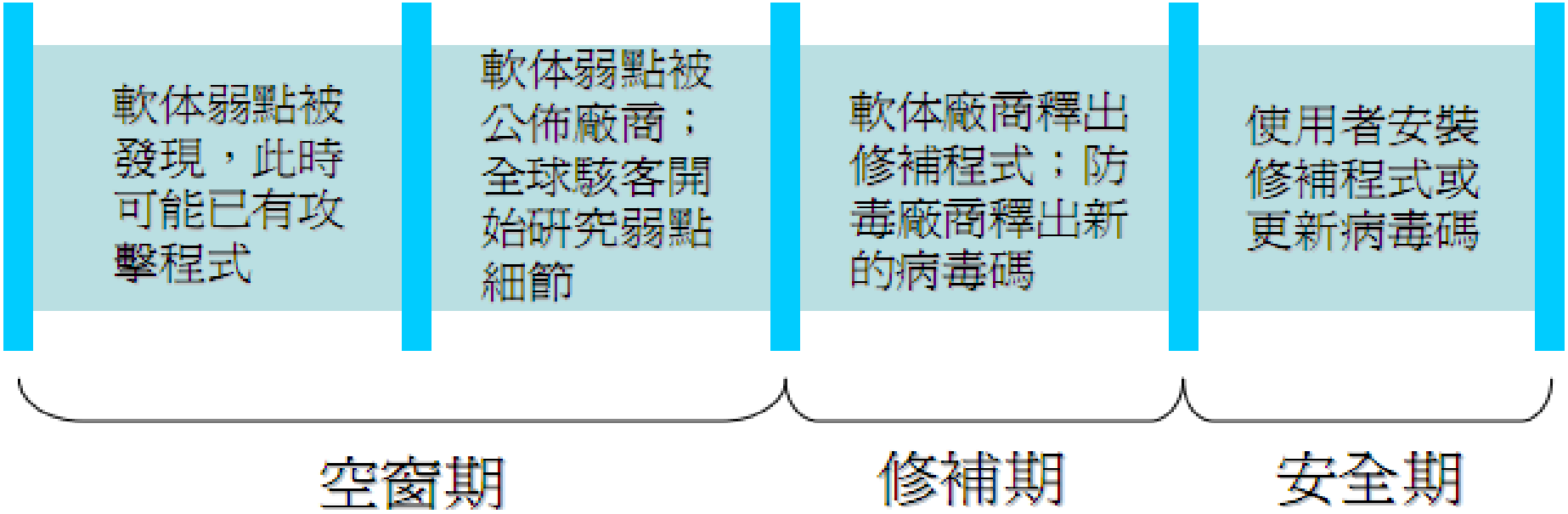


社交工程定義

- 社交工程係操控人類的藝術，使之執行特定的動作或揭露機密資訊，如同精心設計的詐騙或是簡單的欺瞞，通常應用於資訊的搜集或是電腦系統的存取，且大部分的案例中，攻擊者從來不會與受害者面對面（Wikipedia）。
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)
- 可以主動的挑選攻擊對象

軟體弱點與零時差攻擊

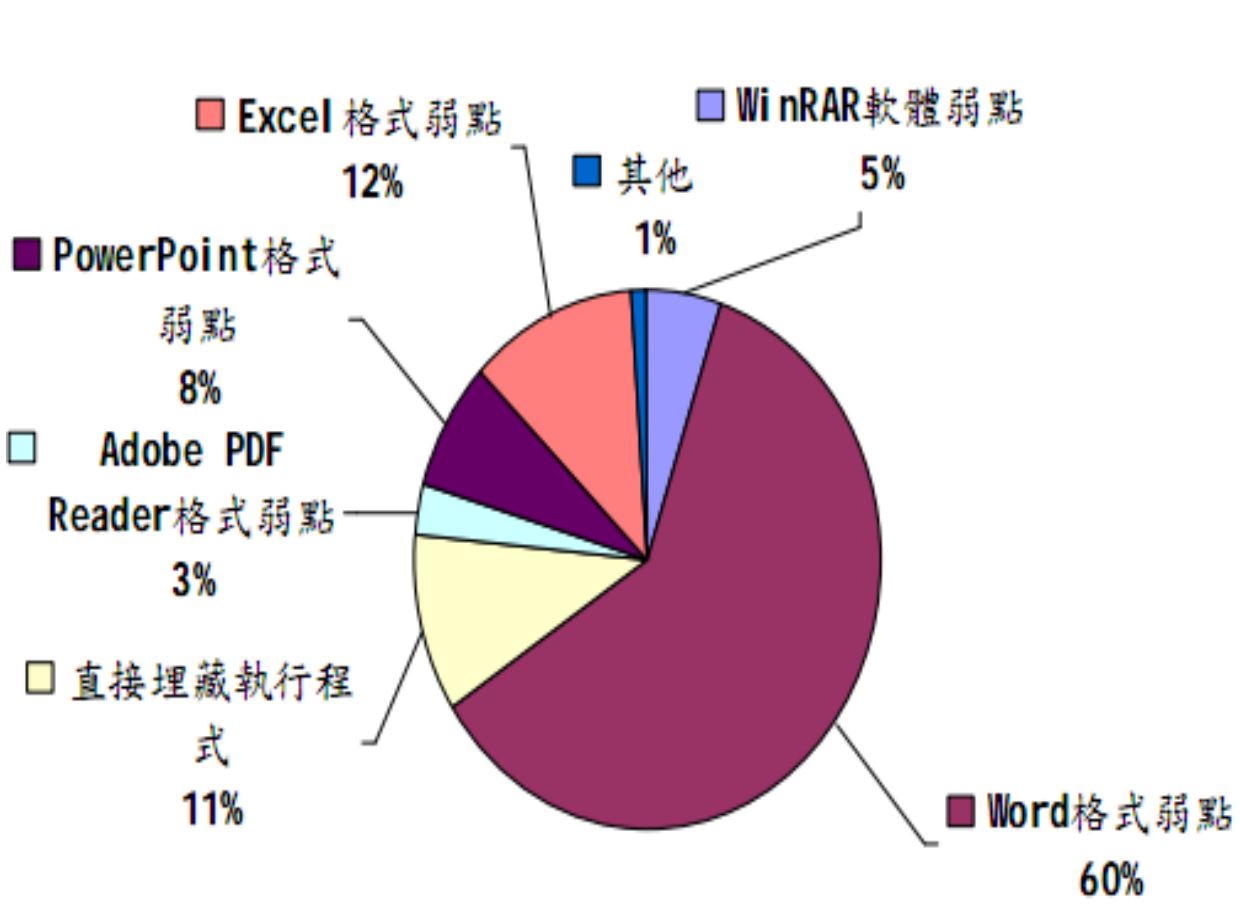
- 只要是軟體即有可能存在弱點，若未能及時修補弱點，即可能讓駭客入侵成功
- 軟體弱點在沒有任何修補方式之前，出現相對應的攻擊行為時，此類攻擊稱為「**零時差攻擊（Zero-day Attack）**」



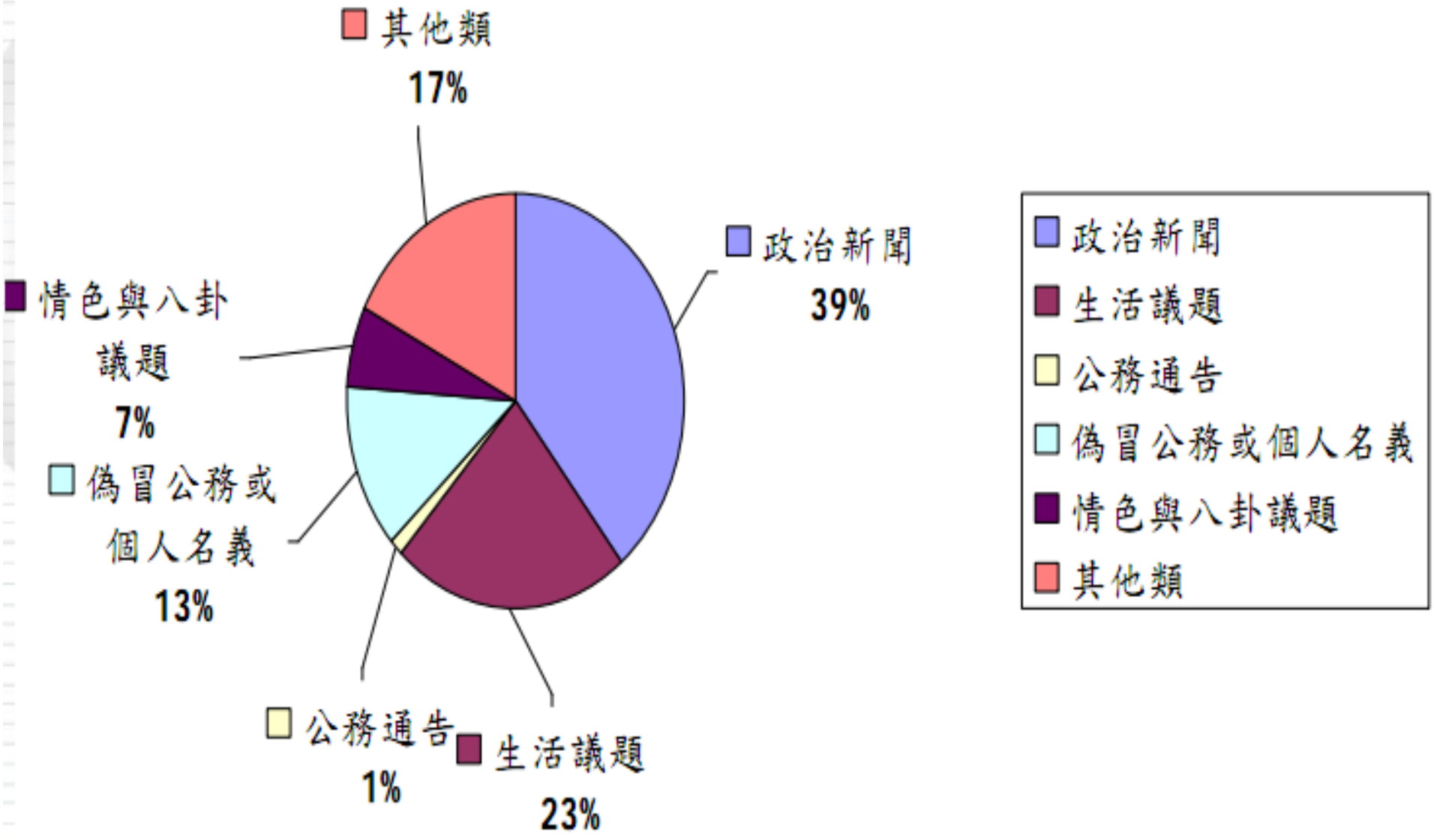
惡意郵件分析

- 組織型駭客多以電子郵件**夾藏惡意程式**之社交工程手法入侵
- 蒐集政府機關可疑電子郵件，分析發現比率約**40.0%**為惡意郵件
- 駭客最常利用弱點
  - **微軟文書處理軟體(Microsoft Office)系統**(因使用普及，造成影響較廣)
  - **常見應用程式(如WinRAR、Adobe Reader and Flash Player等)**相關「軟體弱點」或「脆弱性缺陷」
- 駭客最常運用的社交工程手法
  - **政治新聞**
  - **生活議題**
  - **假冒公務或個人名義**

惡意郵件運用軟體弱點


Excel格式弱點
12%
WinRAR軟體弱點
5%
其他
1%
PowerPoint格式弱點
8%
Adobe PDF Reader格式弱點
3%
直接埋藏執行程式
11%
Word格式弱點
60%
WinRAR軟體弱點
Word格式弱點
直接埋藏執行程式
Adobe PDF Reader格式弱點
PowerPoint格式弱點
Excel格式弱點
其他

惡意郵件內容分析


其他類
17%
政治新聞
39%
情色與八卦
議題
7%
偽冒公務或
個人名義
13%
公務通告
1%
生活議題
23%
政治新聞
生活議題
公務通告
偽冒公務或個人名義
情色與八卦議題
其他類

社交工程手法歸納

- 主要利用電子郵件夾帶**惡意連結**或**惡意附件**進行攻擊
- 惡意電子郵件係針對**入侵對象**精心設計，為主動之針對性攻擊(又稱：魚叉式攻擊)
- 經常利用微軟**Office**軟體或知名之常用軟體弱點，成功入侵**未及時更新弱點之環境。**
- 運用**廣告心理學**，透過**文案**、圖案或**照片**等諸多媒體，藉由電子郵件寄達受害者，誘使受害者開啟郵件，達到入侵之目的。

電子郵件社交工程演練(政治新聞)

中共十七大即將召開，民主開放將成為共產黨存亡的大難題.. - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) 全部回覆(L) 轉寄(W)

寄件者: 兩岸觀察站 [Montague@applepie.serveblog.net] 寄件日期: 2007

收件者: [redacted]

副本:

主旨: 中共十七大即將召開，民主開放將成為共產黨存亡的大難題..

中共十七大前民主開放暗潮洶湧

共十七大代表大會將在年底召開...
而在此時民主開放的思潮已經漫天蓋地的展開...

"改革了，亡黨；不改革，亡國。"

民主開放會在這次十七大投下怎樣的震撼彈... [觀看全文]

電子郵件社交工程演練(影劇新聞)

新片發表會上周潤發表示力挺馬英九選總統!!! - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W)

寄件者: 娛樂大事報 [Laurence@taiwannews.xyles.net]

寄件日期: 2007/7/

收件者: [redacted]

副本:

主旨: 新片發表會上周潤發表示力挺馬英九選總統!!!

周潤發表示力挺[redacted]參選總統

迪士尼強檔新片「神鬼奇航3：世界的盡頭」中扮演新加坡海盜頭子嘯風船長的周潤發，日前在東京出席宣傳活動時，親口表示：「戲里壞人好演、好做，....

.....[redacted].....，如果他選總統，我一定投他一票！」...

電子郵件社交工程演練(色情主旨)

本班女生性感的畢業大頭照 - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W)

寄件者: 小玲 [Devin@wulala.serveblog.net]

收件者: [redacted]

副本:

主旨: 本班女生性感的畢業大頭照

寄件日期: 2007

☆ 本班女生拍的性感畢業照相簿 ☆

電子郵件社交工程演練(政治新聞)

龍應台於台北市文化局長任內的貪污自白!! - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) 全部回覆(L) 轉寄(W)

按這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

寄件者: 政治評不平 [Halbert@applepie.serveblog.net]

寄件日期: 2007/7/17 (星期二) 上午 10:5

收件者: [redacted]

副本:

主旨: 龍應台於台北市文化局長任內的貪污自白!!

附件: 龍應台對[redacted]內的貪污自首告白.doc (58 KB)

龍應台於台北市文化局長任內的貪污自白!! 信件內容: 曾經在[redacted]下擔任文化局局長的龍應台, 在公務首長特別費爭議中的貪污自首告白! 連龍應台這樣高道德標準的人也貪污了嗎?

電子郵件社交工程演練(影劇新聞)

電子郵件社交工程演練(休閒娛樂)

2007宜蘭童玩節來了!! - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W)

寄件者: [redacted]

收件者: [redacted]

副本:

主旨: 2007宜蘭童玩節來了!!

寄件日期: [redacted]

童玩節 12 歲囉！

讓我們大手牽小手 邁開腳步

1 2 1 2 齊步走 ~ 一起向充滿歡笑希望的兒童夢土出發！

今年在冬山河畔，用最快樂的節奏　最熱情的步伐，享受夏日水舞的沁涼，隨著海洋之歌的音符起舞，
7月7日 讓我們跟著小雨和童玩娃娃兵團，展開童玩國度51天的夏日冒險！

[更多活動資訊]

演出	• 【野外劇場】 來自全世界五大洲風俗音樂舞蹈團隊的精采演出 • 【蔚藍舞台】 海洋之歌的曼妙樂符 悠揚於冬山河畔！
展覽	• 【七彩陀螺館】 感受陀螺七彩旋風的魅力！ • 【童玩童食回味屋】 回味兒時童玩童食的時光之旅！ • 【飛行船劇場】 全國首座的球體型可移動式3D立體劇場
	飄浮在半空中的【水母瀑布】，突如其來的多樣水幕瀑布，傾瀉而出，彷彿水母的觸足神

電子郵件社交工程演練(體育新聞)

2007年MLB烏龍球精華節錄 - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W)

寄件者: 體育世界 [redacted]
收件者: [redacted]
副本:
主旨: 2007年MLB烏龍球精華節錄

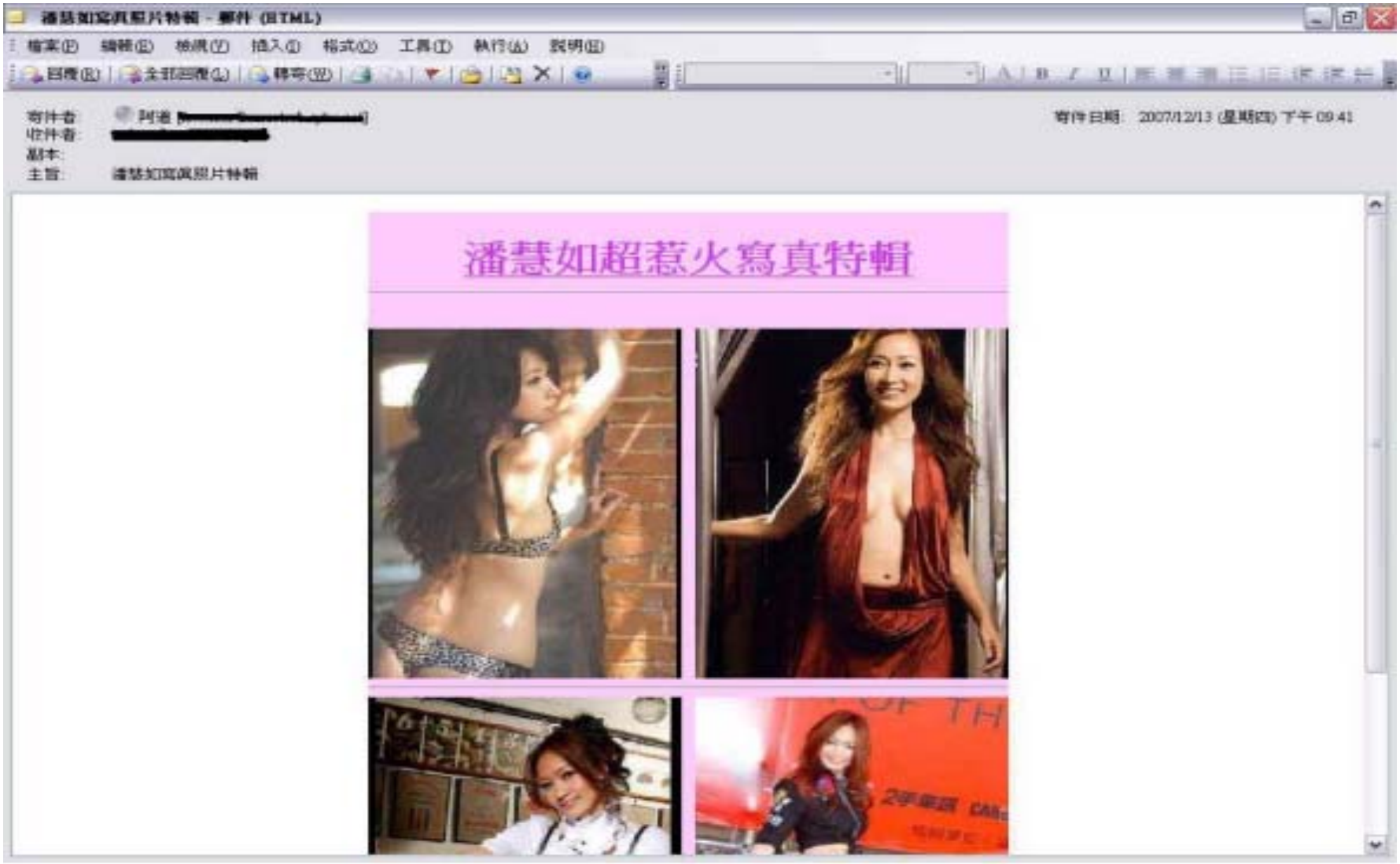
寄件日期: 2007/12/19 (星期三) 下午 04:43

~2007美國大聯盟烏龍球精華~

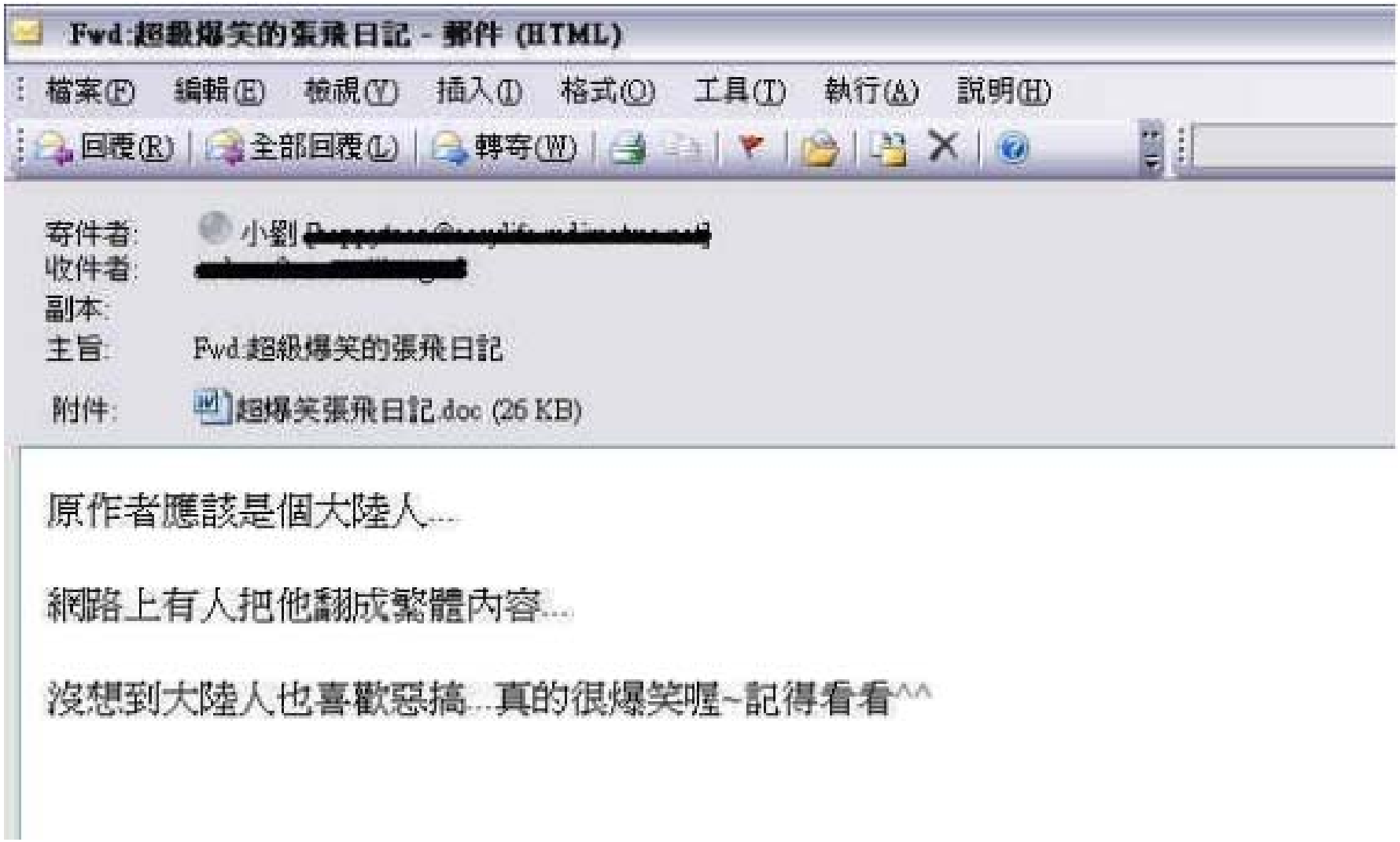
要傳1壘,結果傳到1壘後方觀眾席...

打擊打到球棒飛出去,打到觀眾席賣東西小販

電子郵件社交工程演練(情色內容)



電子郵件社交工程演練(休閒娛樂)



電子郵件社交工程演練(保健養生)

八多八少的簡單健康觀念 - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W)

寄件者: 賴董 [redacted]
收件者: [redacted]
副本:
主旨: 八多八少的簡單健康概念
附件: 八多八少健康多多病痛少.doc (20 KB)

八多：多運動、多蔬果、、、、、、
八少：少熬夜、少重口、、、、、、

很不錯的健康概念
簡單又容易做~看看吧~

電子郵件社交工程演練(影視八卦)

電子郵件社交工程演練(科技新知)

RE: 求救~~~才重灌完又中毒了~~~~ - 郵件 (HTML)

檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

回覆(R) | 全部回覆(L) | 轉寄(W)

寄件者: 阿強 [redacted]
收件者: [redacted]
副本:
主旨: RE: 求救~~~才重灌完又中毒了~~~~
附件: [轉錄]正確的重灌知識.doc (10 KB)

俗話說重灌的多不如重灌的好，
提供大家正確的重灌方式，
不要再浪費時間搞東搞西囉~~~~

: 電腦才重灌沒多久又中毒了，
: 原因到底出在哪?????
: 我已經重灌好多次了(大哭)

社交工程演練統計

區分	平均		最高	最低
	開啟率	點閱率	開啟率	開啟率
96年度	18.02%	11.46%	58.57%	2.73%
97年度	30.57%	19.81%	100%	1.53%

郵件安全防範策略

- 阻絕連結
- 鑑別身分
- 數位簽章
- 郵件加密

阻絕連結

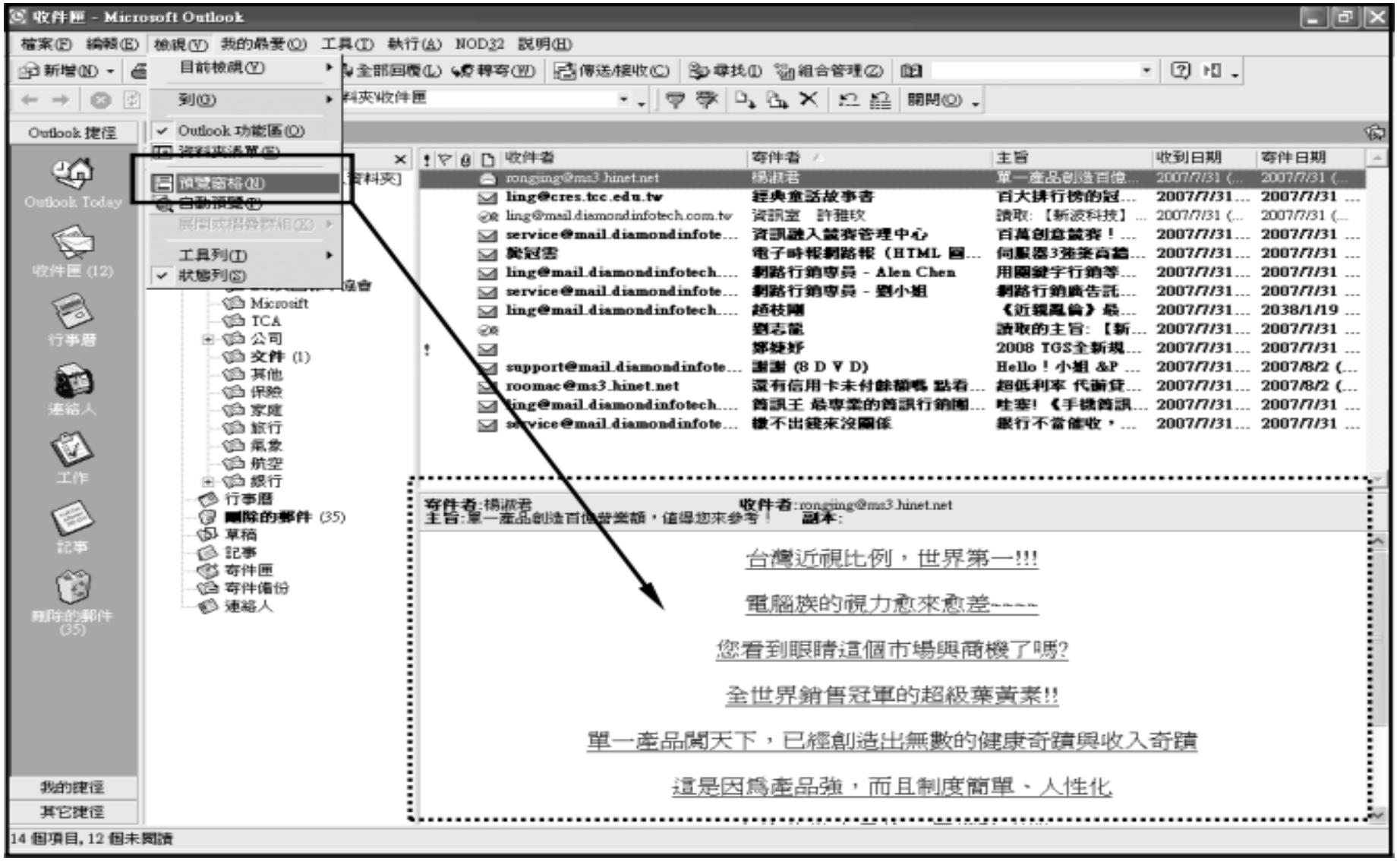
- 設定垃圾郵件過濾機制
- 取消郵件預覽功能
- 以純文字模式開啟郵件
- Webmail環境設定

  — 讀信模式->關閉預覽
  — 去除JavaScript
  — 強制純文字轉換
  — 封鎖外部圖檔

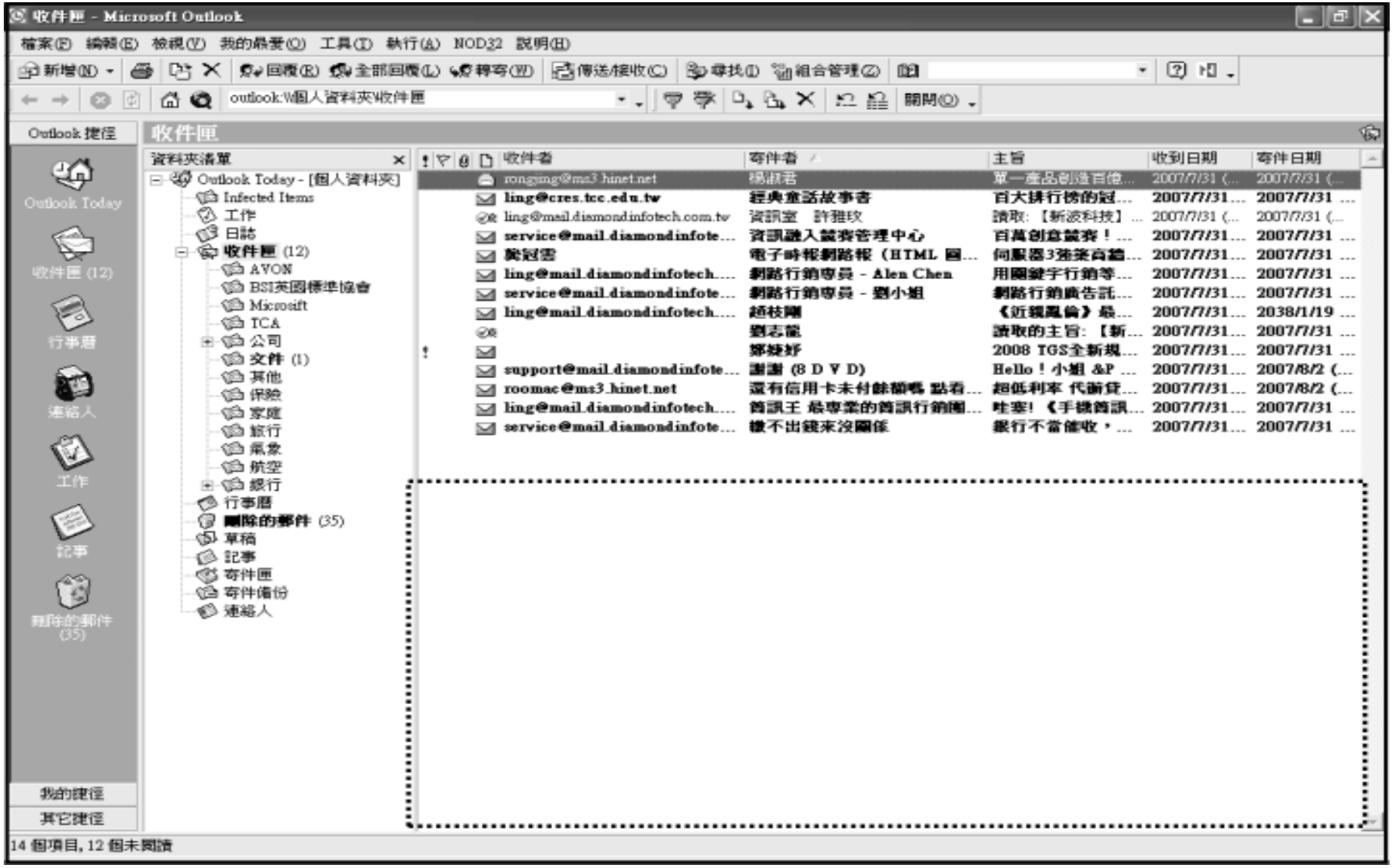
設定郵件過濾機制


型號: CSMG-Unlimited
位置: 郵件防護 > 防垃圾郵件(寄內) > 黑白名單比對
edward | 登出
郵件防護
白名單
黑名單
寄件者 IP 位址白名單:
60.248.122.219
60.248.54.13
寄件者郵件地址白名單:
若 寄件者 IP 在白名單內, 該郵件將不會被垃圾郵件政策限制 (使用換行或逗號分隔)
若 寄件者郵件信箱 在白名單內, 該郵件將不會被垃圾郵件政策限制 (使用換行或逗號分隔)
套用
重設
防中病郵件
防垃圾郵件(寄內)
垃圾郵件政策
Greylist
SPF
RBL 過濾
寄件者驗証
收件者驗証
智慧型內容過濾
黑白名單比對
內容關鍵字比對
關鍵字分類
啟發式規則
防垃圾郵件(寄外)
首頁
系統設定
郵件防護
郵件控管
郵件政策
事件紀錄
設定精靈
關機

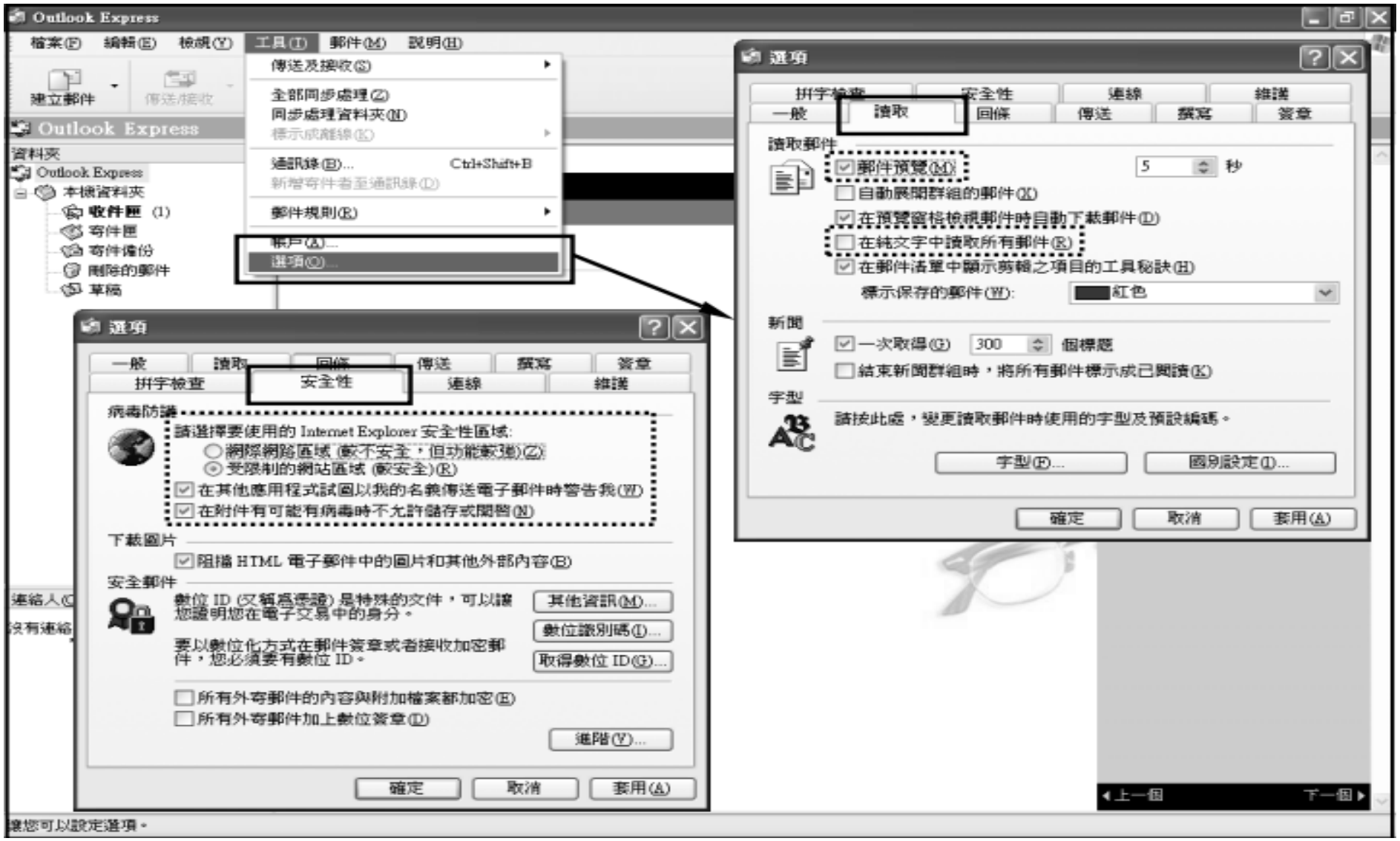
取消郵件預覽功能


收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 我的最愛(O) 工具(T) 執行(A) NOD32 說明(H)
目前檢視(Y)
到(G)
Outlook 功能區(O)
預覽窗格(U)
工具列(T)
狀態列(S)
Outlook 捷徑
Outlook Today
收件匣 (12)
行事曆
連絡人
工作
記事
刪除的郵件 (35)
我的捷徑
其它捷徑
收件者 寄件者 主旨 收到日期 寄件日期
台灣近視比例，世界第一!!!
電腦族的視力愈來愈差~~~~
您看到眼睛這個市場與商機了嗎?
全世界銷售冠軍的超級葉黃素!!
單一產品闖天下，已經創造出無數的健康奇蹟與收入奇蹟
這是因爲產品強，而且制度簡單、人性化
14 個項目, 12 個未閱讀

取消郵件預覽功能


收件匣 - Microsoft Outlook
檔案(F) 編輯(E) 檢視(V) 我的最愛(O) 工具(T) 執行(A) NOD32 說明(H)
新增(N) 回覆(R) 全部回覆(L) 轉寄(W) 傳送/接收(C) 尋找(I) 組合管理(Z) 關閉(O)
outlook:\個人資料夾\收件匣
Outlook 捷徑
Outlook Today
收件匣 (12)
行事曆
連絡人
工作
記事
刪除的郵件 (35)
我的捷徑
其它捷徑
收件匣
資料夾清單
Outlook Today - [個人資料夾]
Infected Items
工作
日誌
收件匣 (12)
AVON
BSI英國標準協會
Microsoft
TCA
公司
文件 (1)
其他
保險
家庭
旅行
氣象
航空
銀行
行事曆
刪除的郵件 (35)
草稿
記事
寄件匣
寄件備份
連絡人
收件者
寄件者
主旨
收到日期
寄件日期
14 個項目, 12 個未閱讀

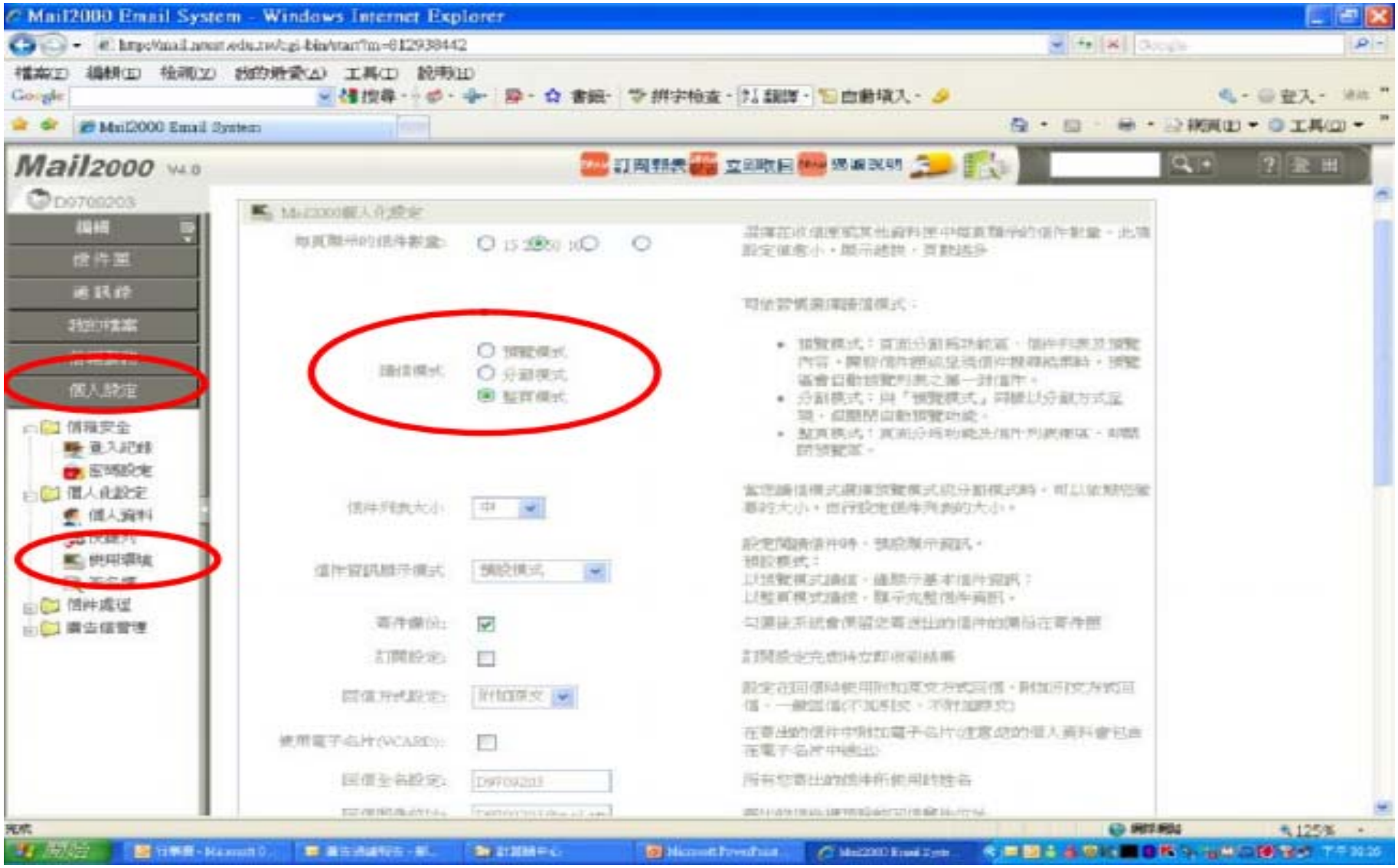
以純文字開啓


Outlook Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
傳送及接收(S)
全部同步處理(Z)
同步處理資料夾(N)
通訊錄(B)... Ctrl+Shift+B
郵件規則(R)
帳戶(A)...
選項(O)...
建立郵件
Outlook Express
資料夾
本機資料夾
收件匣 (1)
寄件匣
寄件備份
刪除的郵件
草稿
選項
一般 讀取 回條 傳送 撰寫 簽章
拼字檢查 安全性 連線 維護
病毒防護
請選擇要使用的 Internet Explorer 安全性區域:
網際網路區域 (較不安全，但功能較強)(Z)
受限制的網站區域 (較安全)(R)
在其他應用程式試圖以我的名義傳送電子郵件時警告我(W)
在附件有可能有病毒時不允許儲存或開啓(N)
下載圖片
阻擋 HTML 電子郵件中的圖片和其他外部內容(B)
安全郵件
數位 ID (又稱為憑證) 是特殊的文件，可以讓您證明您在電子交易中的身分。
其他資訊(M)...
數位識別碼(I)...
要以數位化方式在郵件簽章或者接收加密郵件，您必須要有數位 ID。
取得數位 ID(G)...
所有外寄郵件的內容與附加檔案都加密(E)
所有外寄郵件加上數位簽章(D)
進階(Y)...
確定 取消 套用(A)
選項
一般 讀取 回條 傳送 撰寫 簽章
拼字檢查 安全性 連線 維護
讀取郵件
郵件預覽(M)
5 秒
自動展開群組的郵件(X)
在預覽窗格檢視郵件時自動下載郵件(D)
在純文字中讀取所有郵件(R)
在郵件清單中顯示剪報之項目的工具秘訣(H)
標示保存的郵件(W): 紅色
新聞
一次取得(G) 300 個標題
結束新聞群組時，將所有郵件標示成已閱讀(K)
字型
請按此處，變更讀取郵件時使用的字型及預設編碼。
字型(F)... 國別設定(I)...
確定 取消 套用(A)
上一個 下一個
讓您可以設定選項。

信件開啓範例


「半日租」消遙行 租車價999元起！ - 郵件 (HTML)
和運租車
半日租
車型
VIOS
"半日" 租金
(5小時)
999元
「半日租」消遙行 租車價999元起！ - 郵件 (純文字)

Webmail環境設定

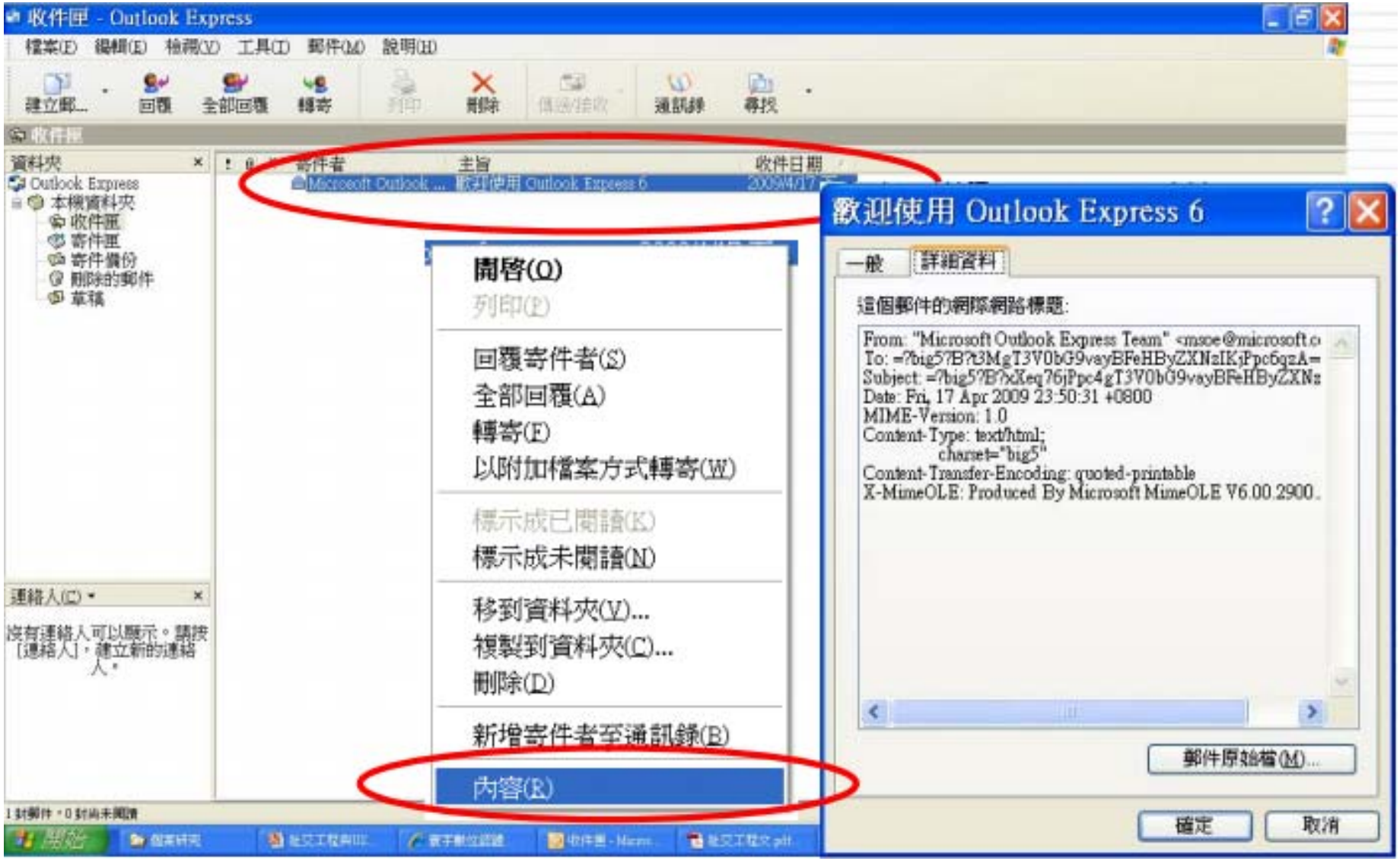


Webmail環境設定

鑑別身分

- 查明信件來源
- 鑑別寄件者身分
- 確認收件者郵件位址

查明信件來源


收件匣 - Outlook Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
建立郵... 回覆 全部回覆 轉寄 列印 刪除 傳送/接收 通訊錄 尋找
資料夾
Outlook Express
本機資料夾
收件匣
寄件匣
寄件備份
刪除的郵件
草稿
寄件者 主旨 收件日期
Microsoft Outlook ... 歡迎使用 Outlook Express 6
開啓(O)
列印(P)
回覆寄件者(S)
全部回覆(A)
轉寄(F)
以附加檔案方式轉寄(W)
標示成已閱讀(K)
標示成未閱讀(N)
移到資料夾(V)...
複製到資料夾(C)...
刪除(D)
新增寄件者至通訊錄(R)
內容(R)
連絡人(C)
沒有連絡人可以顯示。請按[連絡人]，建立新的連絡人。
歡迎使用 Outlook Express 6
一般
詳細資料
這個郵件的網際網路標題:
From: "Microsoft Outlook Express Team" <msoe@microsoft.c
To: =?big5?B?t3MgT3V0bG9vayBFeHByZXNzIKjPpc6qzA==
Subject: =?big5?B?xXeq76jPpc4gT3V0bG9vayBFeHByZXNz
Date: Fri, 17 Apr 2009 23:50:31 +0800
MIME-Version: 1.0
Content-Type: text/html;
charset="big5"
Content-Transfer-Encoding: quoted-printable
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.
郵件原始檔(M)...
確定
取消

驗證寄件者身分

系統管理員: 命令提示字元 - nslookup

```
C:\Users\Bobby>nslookup
預設伺服器:  mail.ringline.com.tw
Address:  172.16.0.2

> set type=mx
> gmail.com
伺服器:  mail.ringline.com.tw
Address:  172.16.0.2

DNS request timed out.
    timeout was 2 seconds.
未經授權的回答:
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google
.com

gmail.com       nameserver = ns4.google.com
gmail.com       nameserver = ns3.google.com
gmail.com       nameserver = ns1.google.com
gmail.com       nameserver = ns2.google.com
ns4.google.com  internet address = 216.239.38.10
ns3.google.com  internet address = 216.239.36.10
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
>
```

免費個人郵件憑證介紹 (Free eMail Certificatese)

- X.509 V3 標準。
- 對稱密鑰長度為 128 位，非對稱密鑰長度為 1024 位。
- 支援目前國際標準的加密和簽章演算法。
- 支持 MS Outlook 、 Outlook Express 、Thunderbird 、Foxmail 、 Netscape Messenger 以及 Frontier 、 Pre-mail 、 Opensoft 、 Connectsoft 、 Eudora 等更安全電子郵件之延伸協議S/MIME的電子郵件軟體。
- 除了可直接純放在電腦外，還包括 USB Key 、 IC 卡等。

請選擇，您想要免費申請的個人郵件憑證 (Free eMail Certificatese) ：

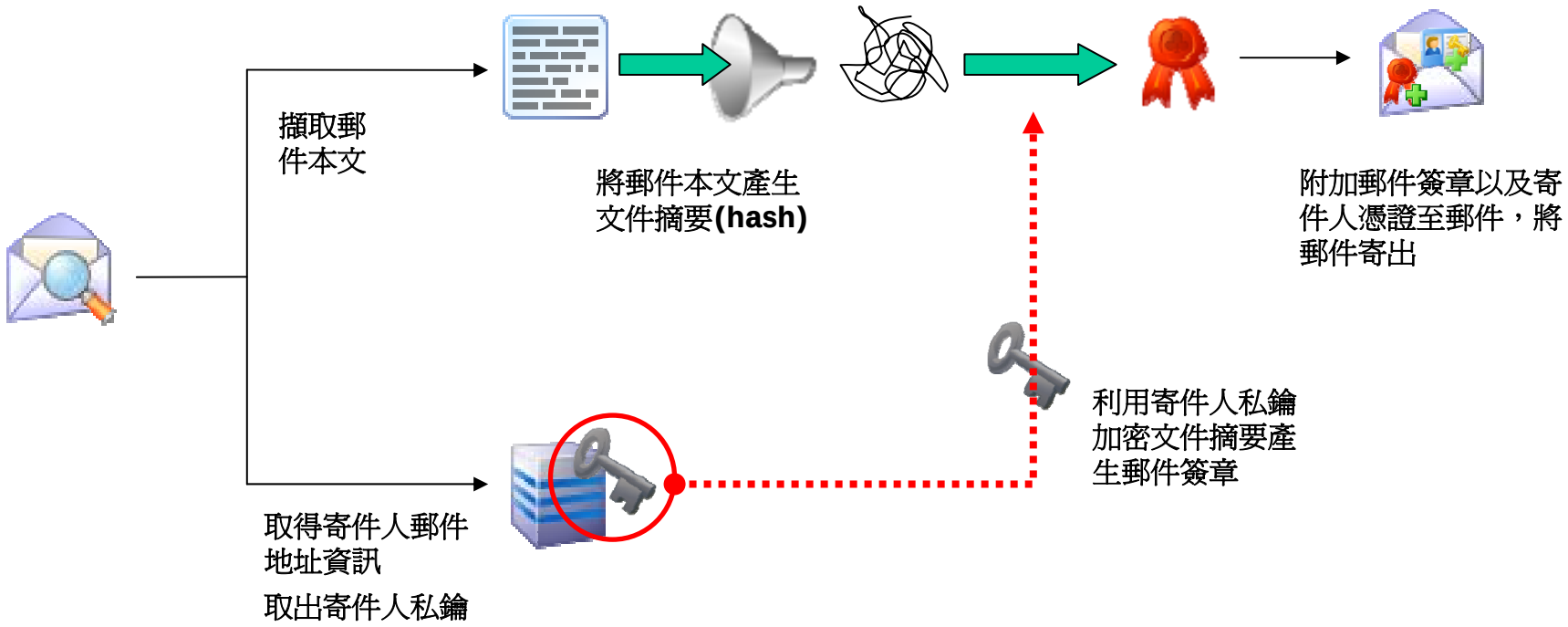
免費個人郵件憑證 (Free eMail Certificatese)

點選購買品牌	GlobalTrust
憑證名稱	個人電子郵件憑證 Free eMail Certificate
憑證加密	對稱密鑰長度為 128 位，非對稱密鑰長度為 1024 位
國際加密演算法	✓
公司資料認證	✗
重新申請次數	相同的信箱只限申請一次
申請時間	即時申請，即可發放
支援的Email軟體	MS Outlook 、 Outlook Express 、Thunderbird 、Foxmail 、 Netscape Messenger 以及 Frontier 、 Pre-mail 、 Opensoft 、 Connectsoft 、 Eudora 等更安全電子郵件之延伸協議 S/MIME的電子郵件軟件。
線上訂購	Free 免費申請

數位簽章

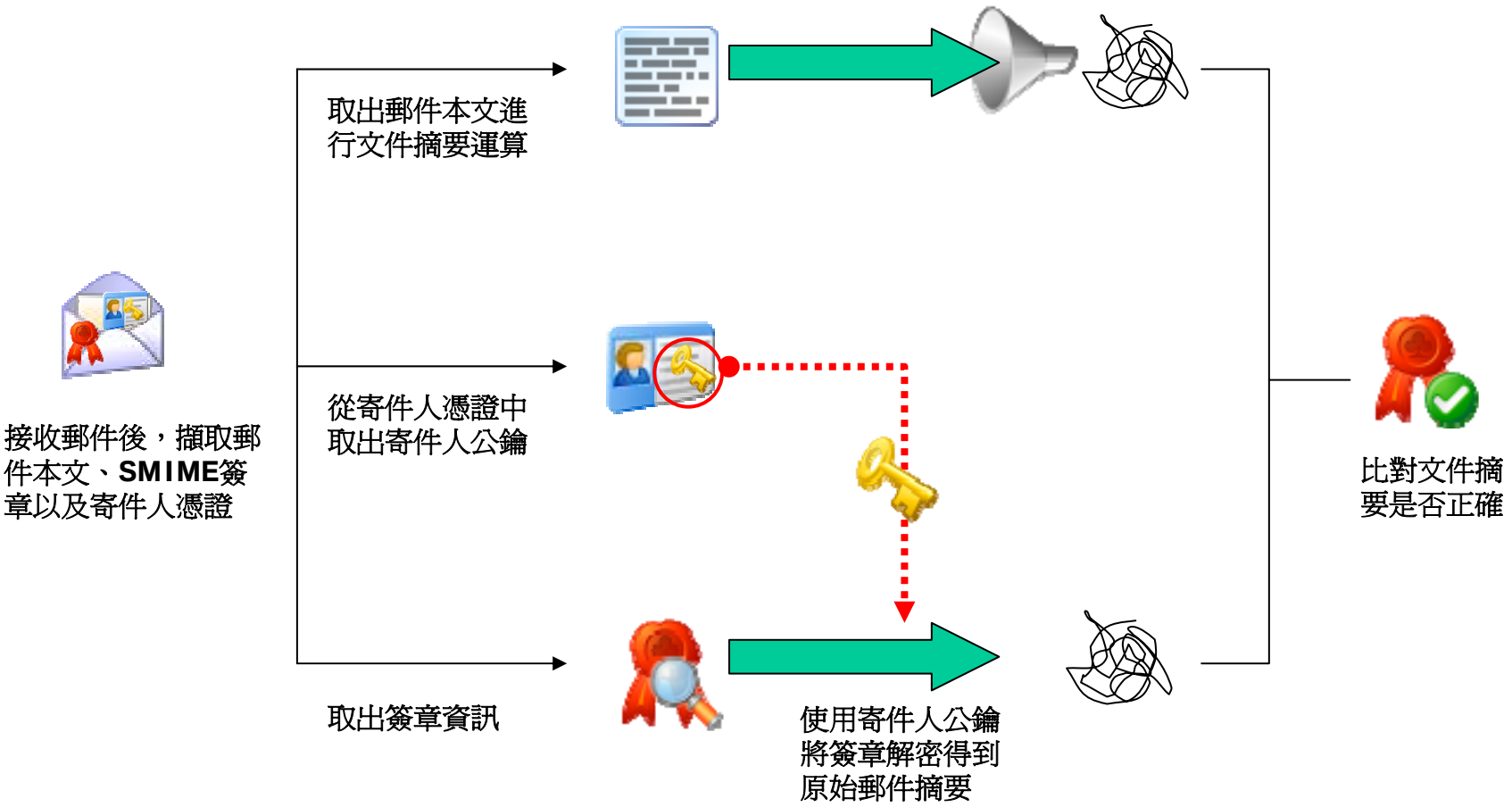

我的新憑證與 gmail 信箱. - 郵件 (純文字)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: 郭秋田 [tonyctkuo@gmail.com]
收件者:
副本: 郭秋田 et gmail
主旨: 我的新憑證與 gmail 信箱
簽名者: tonyctkuo@gmail.com
寄件日期: 2009/4/2 (星期四) 上午 01:55
Dear partners,
Here my gmail address and certificate come. Please check them.
Thanks.
My best regards,
--
Tony C. T. Kuo (郭秋田), Ph. D., CISSP
Assistant Professor, Management & Information Dept.
National Open University
Email: tony@mail.nou.edu.tw, tonyctkuo@gmail.com
Tel: 886-2-22829355x7617
數位簽章: 有效
主旨: 我的新憑證與 gmail 信箱.
寄件者: 郭秋田
簽名者: tonyctkuo@gmail.com
此郵件的數位簽章為 [有效] 且 [受信任的]。
如需有關用於郵件數位簽章憑證的詳細資訊，請按一下 [詳細資料]。
詳細資料(D)...
開啓郵件之前，警告我關於數位簽章電子郵件的錯誤。(W)
關閉(C)
開始

S/MIME簽章寄件端流程



S/MIME簽章收件端流程

寄件人憑證為受信任的憑證授權單位 (CA) 發出，才可正確檢驗
否則收件端必須要信任該憑證授權單位

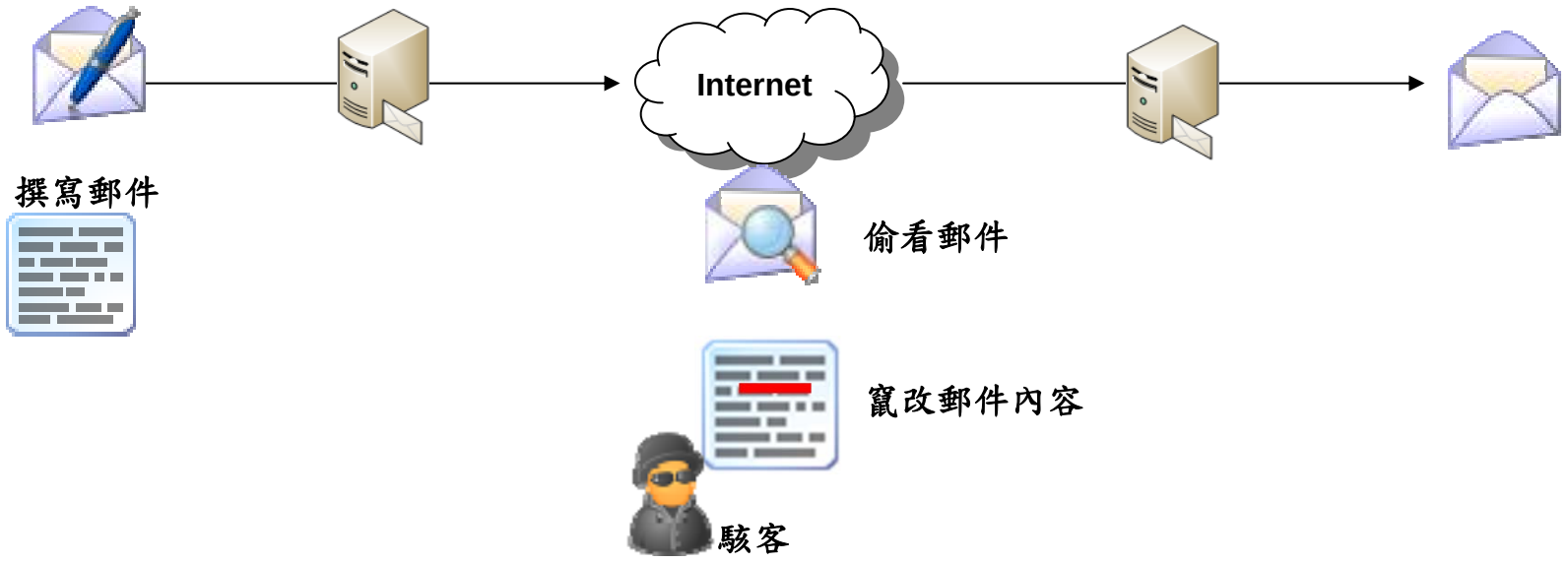


附件檔壓縮,加密

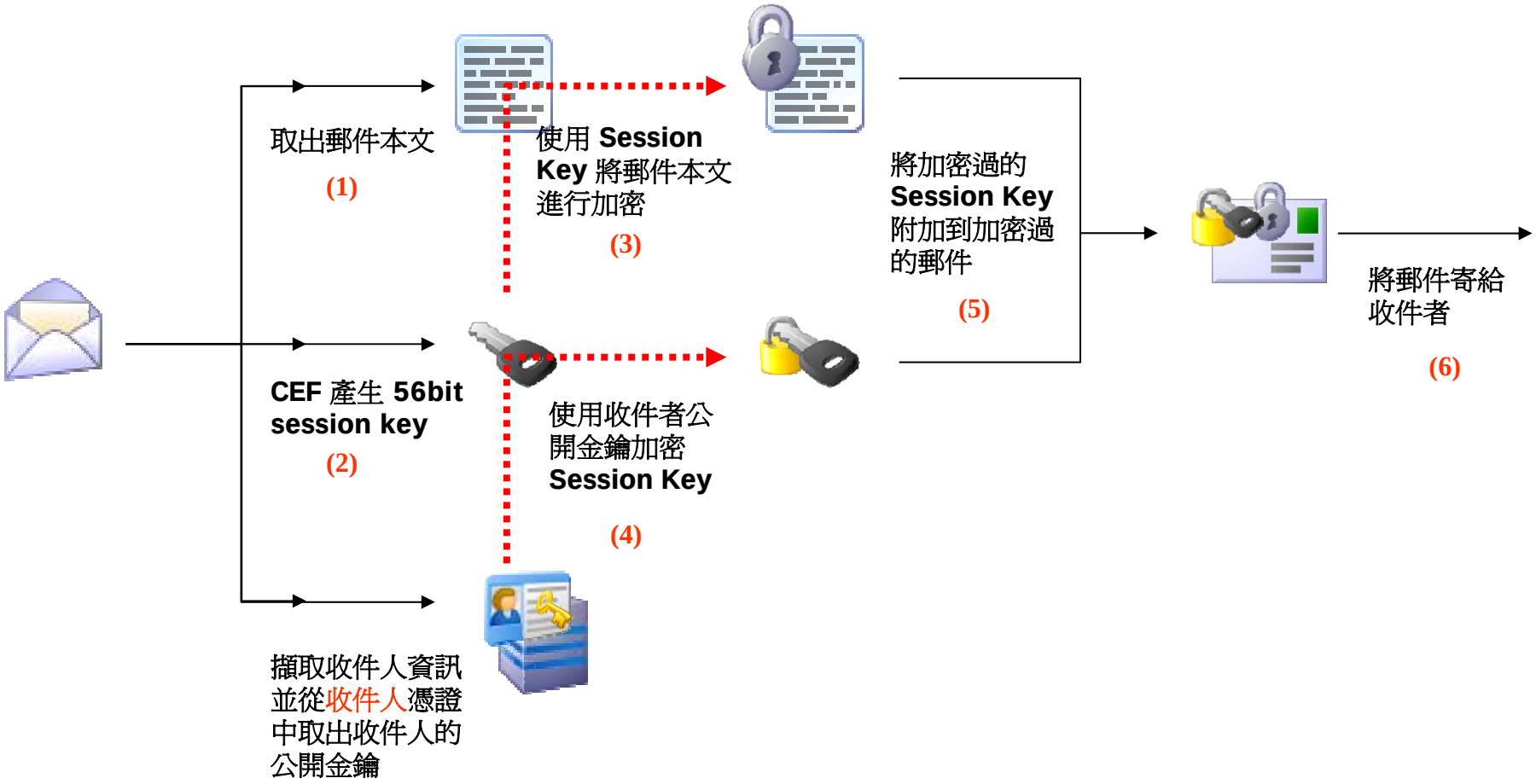

壓縮檔名稱及參數
一般設定
進階設定
檔案
備份
時間
註解
NTFS 選項
儲存檔案安全性(S)
儲存檔案資料流(T)
復原記錄(R)
分割檔
檔案分割操作後先暫停(Y)
套式分割檔命名(L)
個復原分割檔(C)
壓縮設定(C)...
自解檔選項(X)...
設定密碼(P)...
系統
背景壓縮作業(B)
結束時關閉電腦(F)
說明
加密碼的壓縮檔
請輸入密碼(E)
再次輸入密碼來確認(E)
顯示密碼(S)
檔名加密(N)
確定
取消
說明

SMTP Protocol

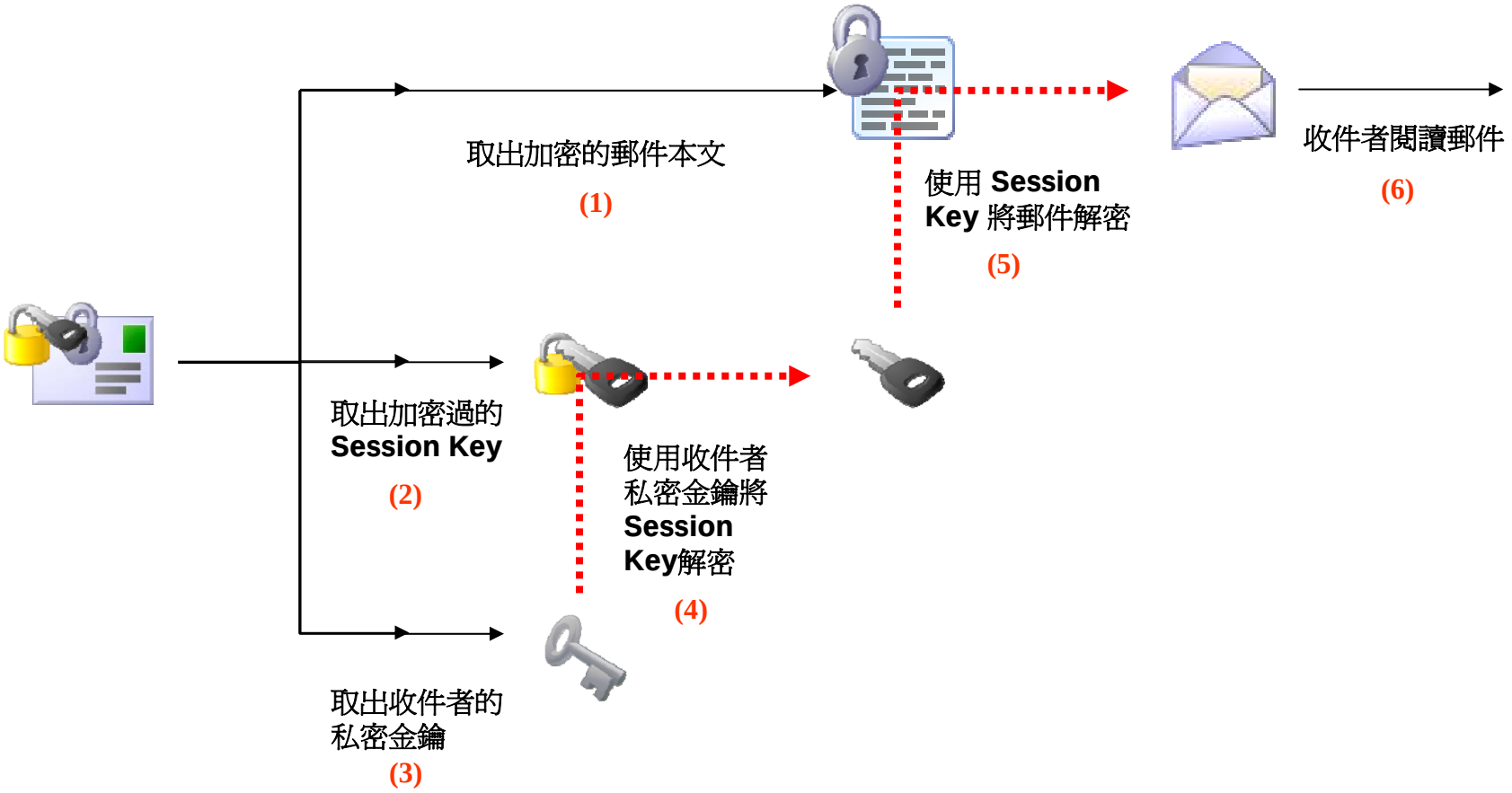
- 一般的電子郵件為明碼傳輸，並不具備安全性，容易被駭客側錄、偷看、竄改內容。



S/MIME寄件端加密流程



S/MIME加密收件端流程



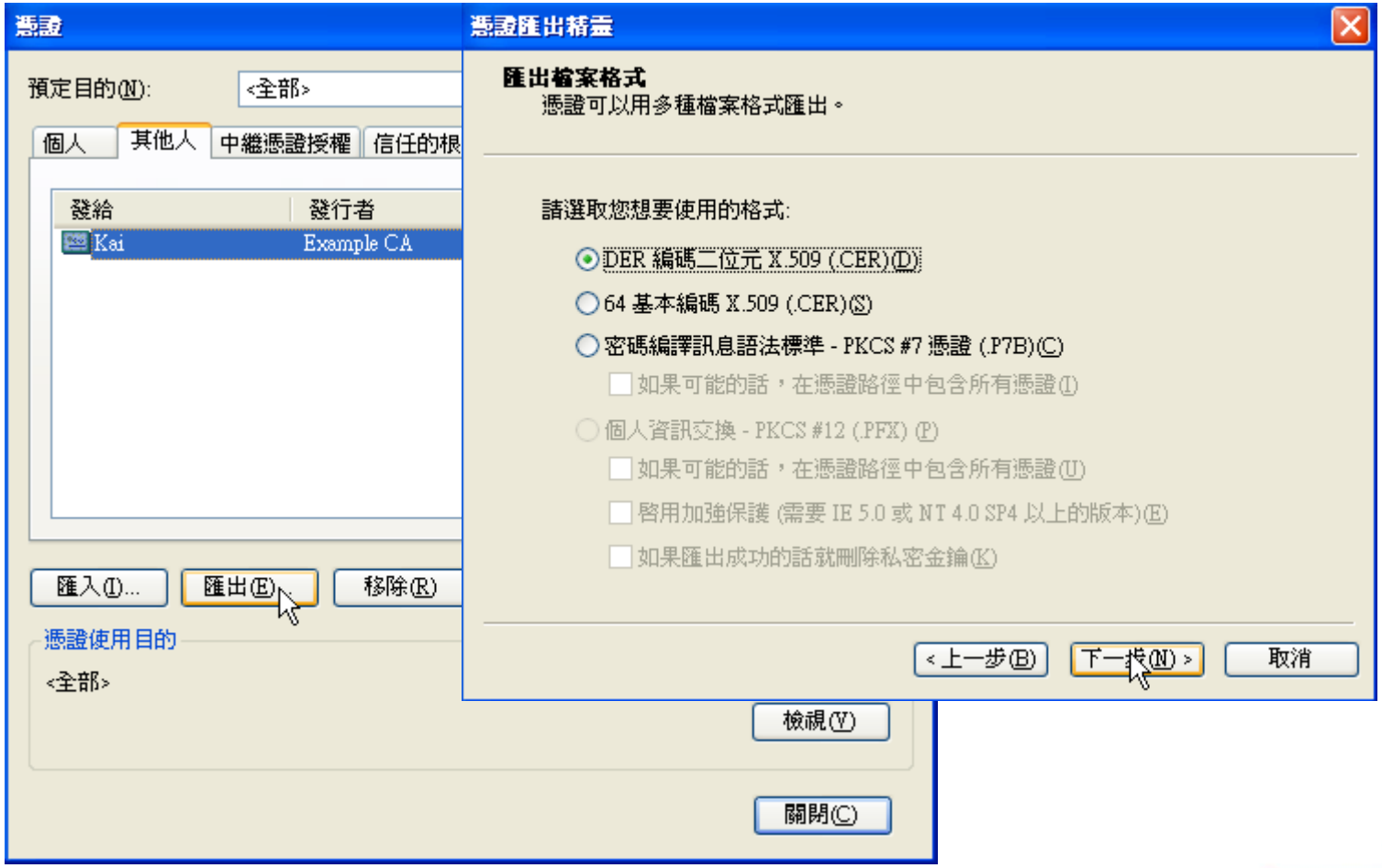
1. 將收件人憑證匯入 CEF Mail Gateway

2. 設定郵件政策，讓寄出的郵件進行 S/MIME 加密

Step1:將收件人憑證匯出

若曾接收有加 S/MIME 簽章的信件，則在憑證管理區會有該寄件人憑證，需把該寄件人的憑證匯出

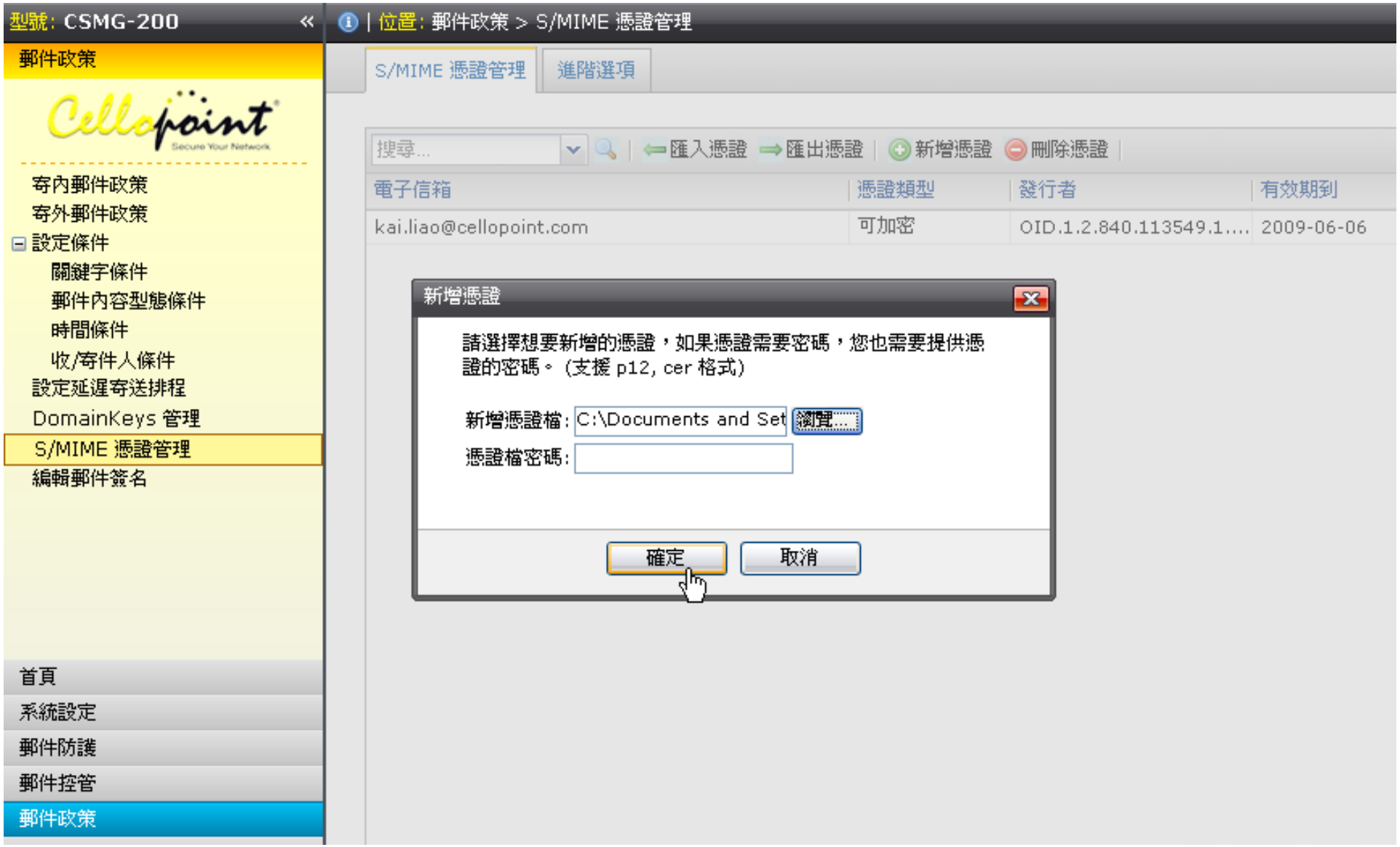
[IE > 工具 > 網際網路選項 > 內容 > 憑證 > 其他人]



麟瑞科技 RING LINE CORPORATION

匯入收件人憑證到Mail Gateway

www.ringline.com.tw



Step2:設定寄外郵件政策

1. 將寄件人條件加入
2. 執行條件選擇 “無”
3. 點選［更多選項 > 安全性 > S/MIME 加密］

Step2:設定寄外郵件政策

www.ringline.com.tw

型號: CSMG-200 «

| 位置: 郵件政策 > 寄外郵件政策 admin | 登出

- 郵件政策
- 寄內郵件政策
- 寄外郵件政策
- 設定條件
  - 關鍵字條件
  - 郵件內容型態條件
  - 時間條件
  - 收/寄件人條件
- 設定延遲寄送排程
- DomainKeys 管理
- S/MIME 憑證管理
- 編輯郵件簽名
- 首頁
- 系統設定
- 郵件防護
- 郵件控管
- 郵件政策

寄外郵件政策總覽 | 編輯 寄外郵件政策 | 寄外政策引擎設定

政策名稱: SMIME_CRY (名稱中不能包含字元 ! [ ] : , & " ' < > + \)

停用這個郵件政策

條件類別: 寄件人

符合 / 不符合 選擇條件:

All from example
all subnet
example.com
peter
user1

>>

<<

篩選條件: Go!

郵件要符合的條件:

寄件人=all subnet

執行動作: 無

更多選項...

記錄事件
S/MIME 加密
關鍵字: 標頭 內文
寄送優先權: 一般

收件人若不具有私密金鑰則無法檢視信件

寄件者: 未指定寄件者
日期: 2008年6月5日 下午 04:49
收件者: kai.liao
主旨: test encry

進行郵件加密時發生錯誤

您無法閱讀這封郵件。

可能是因爲:

- 您可能遺失或刪除了用來加密這封郵件的數位識別碼。
- 您可能已經在其他電腦上安裝了加密這封郵件的數位識別碼。
- 這個寄件者可能將郵件送錯人了。
- 您的電腦上沒有安裝必需的安全性套裝軟體。

Outlook Express

收件人若具有私密金鑰則可以檢視信件

寄件者: kai.liao
日期: 2008年6月5日 下午 04:55
收件者: kai.liao
主旨: Re: test S/MIME Encrypt
安全性: 已加密

----- Original Message -----
From: kai.liao
To: kai.liao
Sent: Thursday, June 05, 2008 4:55 PM
Subject: test S/MIME Encrypt

test S/MIME Encrypt

如何預防惡意程式

預防惡意程式

- 要有正確的資訊安全觀念
- 不隨意開啟或下載郵件或軟體
- 定期做系統更新集資料備份
- 避免使用P2P軟體
- 安裝防毒軟體並定時更新病毒碼
- 不使用來路不明的軟硬體
- 提高警覺，加強危機意識

預防惡意程式

- 定期掃瞄電腦裡的檔案
- 移除電腦中不必要的程式
- 使用者權限的設定
- 不隨便開啟不明的連結或檔案
- 定期更換各種應用程式的密碼，注意密碼複雜度
- 使用個人防火牆，增加系統安全性

結論


DIE HARD 4.0

網路跟現實的世界一樣，處處都是危機，每分每秒都充滿著威脅，時時提高自己的警覺性，不讓威脅靠近自己的身邊

網頁瀏覽、電子郵件、即時通訊這些使我們生活上更便利的工具，一個不小心卻也可能為我們帶來更大的災害；例如自己的網路銀行帳號密碼被竊取等等的事件；要能善用這些工具，同時也能保障自己的安全

使用者應該謹慎的使用網路上的各項服務，並且時時吸收新知，了解目前網路存在著什麼樣新型態的威脅，且避免使用非法軟體，這樣可以盡量避免自己受到新的惡意程式威脅

電腦系統中各種軟體的版本、漏洞都應定時檢查是否有更新或是安裝；並且利用各種防護工具來保持電腦系統隨時都維持在安全無虞狀態下，這樣電腦使用起來也會放心許多

電腦使用習慣要良好，不用時就關機，這樣一來可以避免受到莫名其妙的攻擊，二來也可以為地球節能減碳，平時勤做系統健康的檢查，讓電腦隨持維持在高檔狀態下運作

Reference

- 奕瑞科技
- 國家資通安全會報
- 趨勢科技
- 邁克菲有限公司
- 基點資訊

Thank You