數聯資安股份有限公司
Information Security Service Digital United, Inc.

# 惡意程式分析與鑑識

數聯資安(ISSDU)
主講者：張裕敏

# 講師簡介

- 現任－數聯資安副總經理兼資安長
- 學歷：
  - 清華大學資訊科學研究所
- 經歷：
  - 數聯資安副總經理
  - 鈺松國際研發經理/協理/處長/副總
- 資安相關證照
  - CEH, CHFI, CERT/CC, ECSA/LPT
- 專長
  - SCADA/智慧電網/雲端安全研究
  - 駭客攻防技術與駭客趨勢研究
  - 數位鑑識與蒐證研究

# 大綱

- 何謂惡意程式
- 重大漏洞及病毒介紹
- 病毒趨勢
- 如何分辨並清除惡意程式
- 惡意程式分析
- 總結



本課程下半節課有眾多惡意樣本分析示範

# 惡意程式

- 病毒(Virus)
  - 進入主機並未經授權執行的程式。
- 網蟲(Worm)
  - replicates itself over a computer network
- 木馬(Trojan horse)
  - 執行時呈現普通程式結果，實際上暗中進行了惡意活動。
- 後門(Back Door)
  - 秘密管道，藉以在未經認證的情況下使用電腦資源。

# 病毒與蠕蟲

- 技術持續改進
- 數量劇增
- 多重感染途徑
  - 軟碟
  - 電子郵件
  - 網路芳鄰
  - 網站與系統弱點
- 快速散佈
- 變種繁多


# 後門與木馬

- 偽裝檔案
- 釣魚網站
- 竊取資料、佔領主機
- 防毒軟體不負責

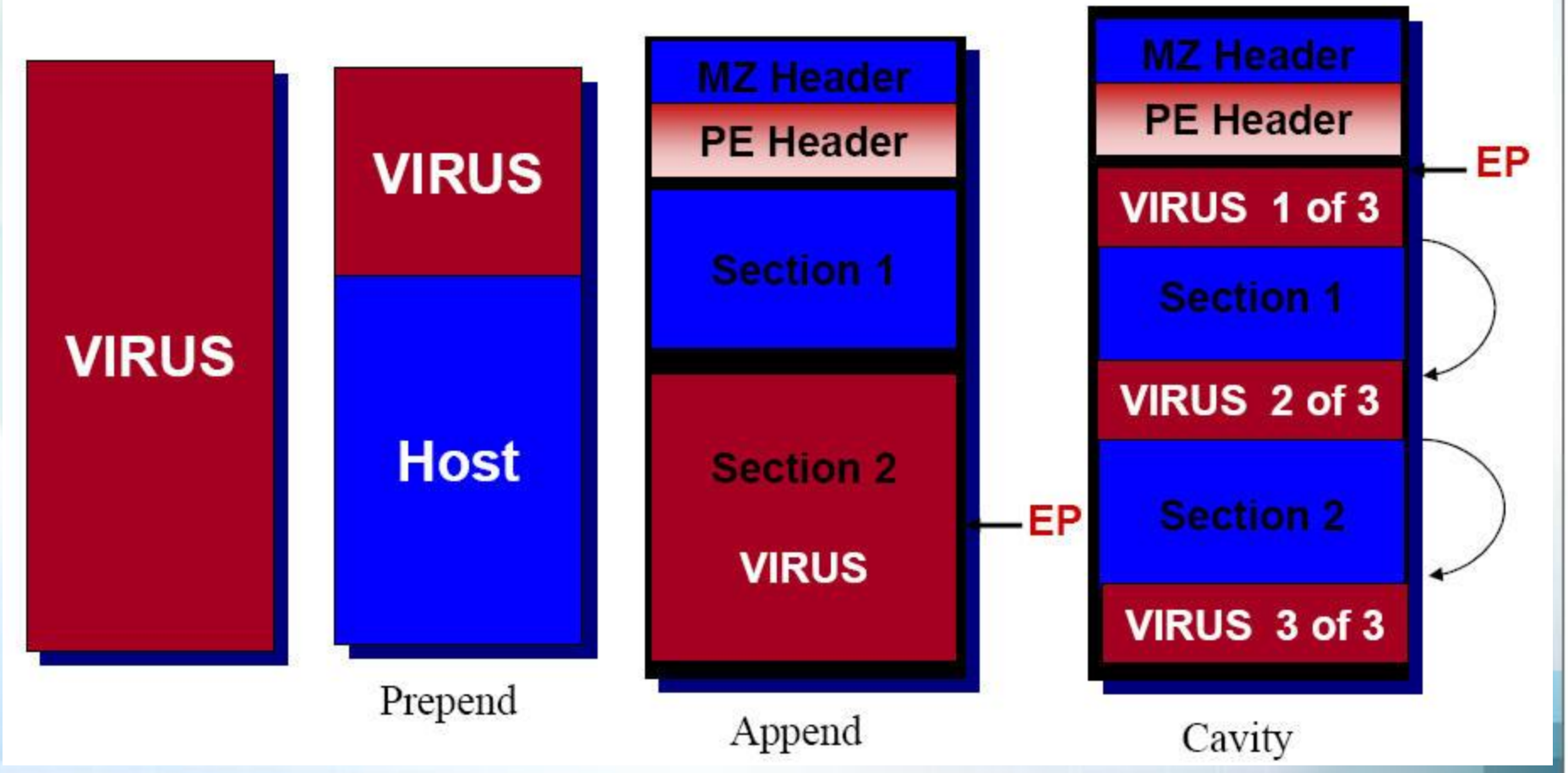
# 後門與木馬(續)

- 只是上網瀏覽網頁、安裝應用程式、觀看HTML郵件時便可植入電腦！
- 監視你的按鍵內容，秘密蒐集資料，然後「打包回家」！
- 綁架IE的首頁！
- 出現大量的廣告，意圖造成混亂。
- 消耗系統資源！

# 惡意程式的差異

| | 病毒 | 木馬 | 蠕蟲 |
|---|---|---|---|
| 感染其他檔案 | ○ | ╳ | ╳ |
| 被動散播自己 | ○ | ○ | ╳ |
| 主動散播自己 | △ | ╳ | ○ |
| 感染程式數目 | 隨使用檔案數量增加 | 不會增加 | 視網路鏈結數量而定，鏈結愈廣，散佈的範圍越大 |
| 破壞能力 | 視設計者而定 | 視設計者而定 | 網路癱瘓 |

# PE Virus


VIRUS
VIRUS
Host
Prepend
MZ Header
PE Header
Section 1
Section 2
VIRUS
EP
Append
MZ Header
PE Header
EP
VIRUS 1 of 3
Section 1
VIRUS 2 of 3
Section 2
VIRUS 3 of 3
Cavity

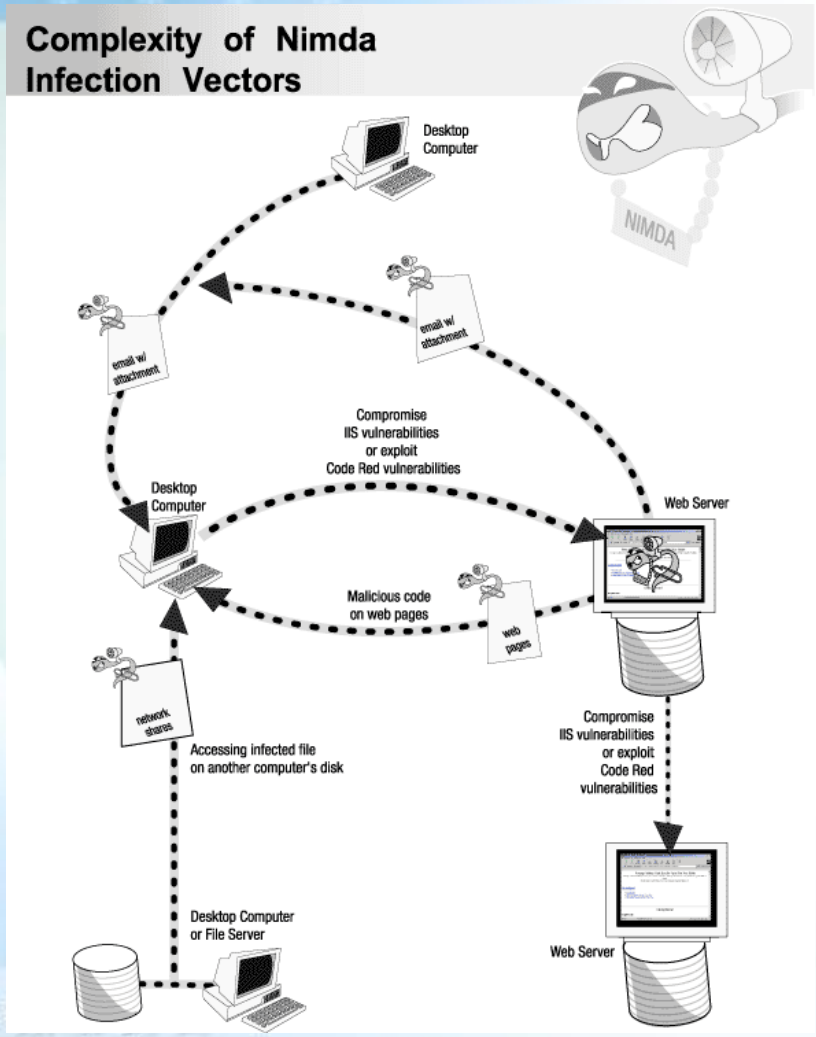
# 重大漏洞與病毒/蠕蟲介紹

# CodeRed

- 2001年7月
- 紅色警戒(Code red)
  - 第一款和駭客程式結合的新型網路病毒，它的主動攻擊方式曾造成歐美等地區網路大範圍癱瘓。它能像生物一樣去主動“覓食”，尋找獵物，迄今爲止共造成12億美元的經濟損失。
- Windows漏洞與病毒結合的轉戾點
- **CodeRed**為利用**IIS Indexing Service DLL**弱點惡意程式碼
- 利用**IIS**伺服器所產生的安全性漏洞導致此一網蟲能輕易入侵沒有修補過的**IIS WEB**伺服器
- 可讓攻擊者得以執行系統上的任意程式


- 目標：
  Microsoft IIS 4.0/5.0
- 漏洞：
  MS01-033
- 間接受害：
  Cisco Router

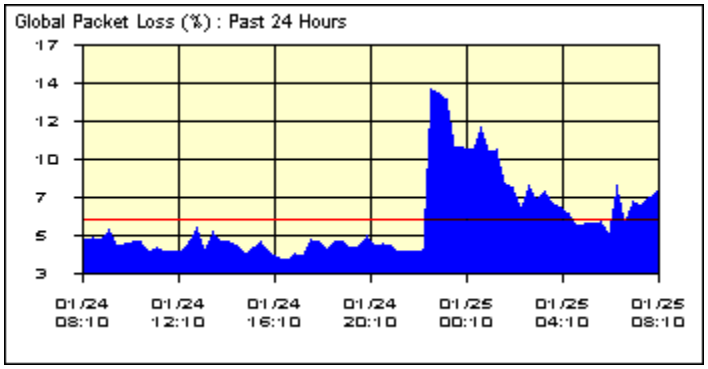
# Nimda

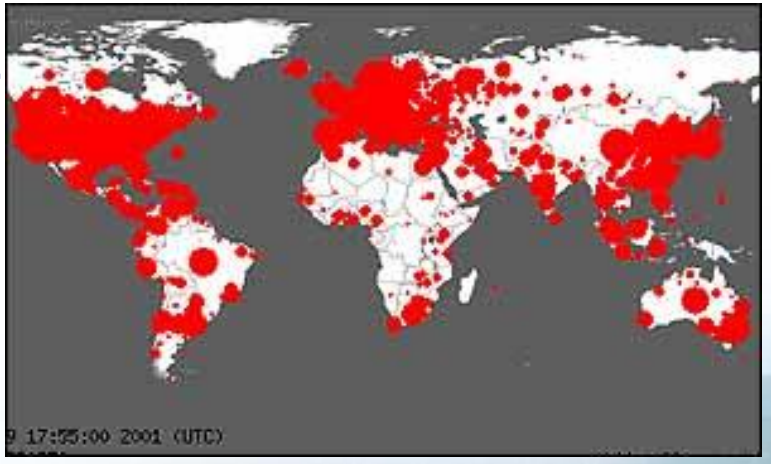



- 2001年9月
- 通過網際網路傳播的新型“蠕蟲”病毒（並不毀壞資料,但會大量佔用硬碟空間,降低主機的處理速度）。2001年出現，是在歷史上造成最大危害的病毒，。由於它狡猾多端，且極其隱蔽，至今在全球範圍內未被根除。
- Nimda病毒所使用的弱點可以讓攻擊者得以執行系統上的任意程式，而遭Nimda病毒感染的系統，則會繼續攻擊其它的網站，而Nimda病毒的感染方式有以下多重感染路徑
- 目標：
  - Microsoft IIS 4.0/5.0
  - 電子郵件
  - 網路分享
  - 惡意網頁
  - CoreRed殘遺程式
- 漏洞：
  - MS01-020
  - MS01-044

# Slammer

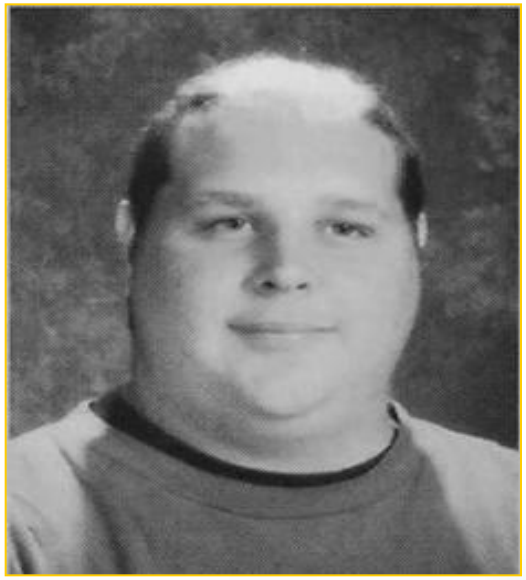
- 2003年1月
- 最小、最快的網蟲之一
- 100 Mbps 的網路每秒能發出高達約 30000 次擴散攻擊
- 目標：
  - Microsoft SQL Server
  - MSDE
- 漏洞：
  - MS02-039
  - MS02-061
- 間接受害：
  - Cisco Router



# Blaster疾風病毒

- 第一種把病毒技術與駭客技術結合起來的網路蠕蟲病毒。2003年8月11日開始橫掃全球，24小時內全球有140萬台電腦被入侵。微軟公司甚至懸賞500萬美元捉拿疾風病毒病毒製造者。
- 18歲的明尼蘇達州少年傑佛雷·帕爾森因製造“疾風病毒二代”(Blaster.B) 病毒已於03年8月29日被FBI逮捕。圖爲帕爾森在Hopkins High School所拍的照片。



# Blaster


- 2003年8月
- 個人PC成為目標
- 目標：

  Windows
- 漏洞：

  MS03-026

  MS03-039

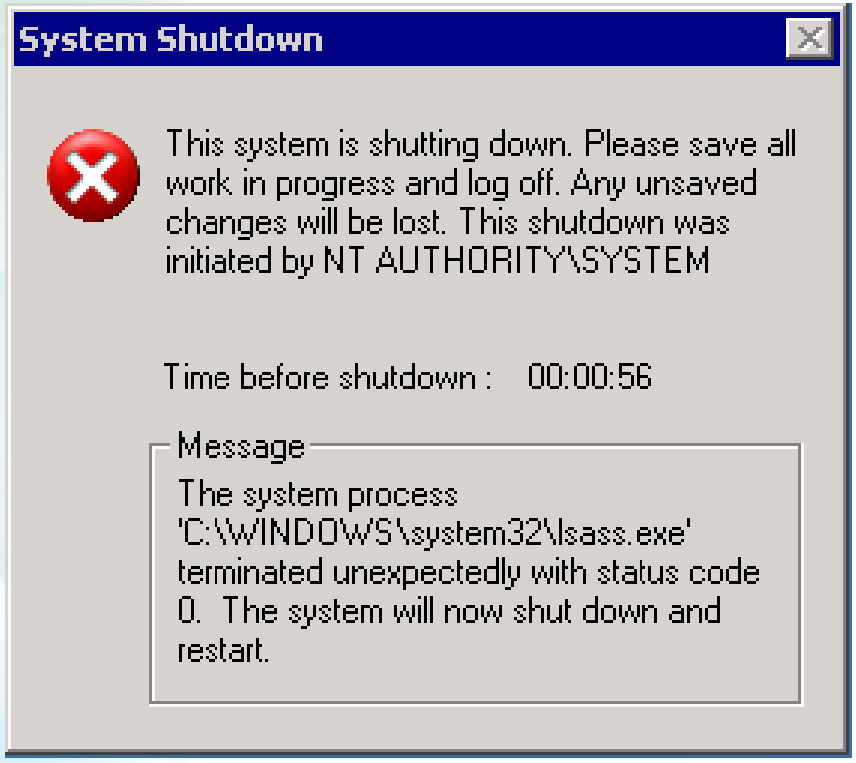
# Sasser殺手病毒

- 這隻來勢洶洶的病毒，仍是針對微軟WindowsNT、2000、XP及2003作業系統進行漏洞攻擊，微軟4月13日曾發布重大安全訊息通知，建議用戶更新修正程式MS04-11，，若已經下載安全補充程式者，將免於受到攻擊，若尚未下載者，出現LSASS.exe錯誤訊息的彈跳視窗畫面，就表示已經中毒。
- 新聞資料(20040501)
  - 中華郵政全台電腦今天上午420個電腦窗口終端機癱瘓，包括大台北地區、台中、高雄等地區全部被入侵，讓各家郵局櫃檯忙成一團。中華郵政表示，初步排除是電腦駭客入侵，仍在追查中毒來源。
  - 中華郵政表示，今天上午10時左右，全台1300個郵局中發現約有420個郵局，近三分之一郵局都出現電腦異常現象，不斷出現重複開關症狀，電腦資訊人員判斷是感染了最新電腦病毒「殺手」。

# 殺手病毒作者

- 爲追查病毒製造者，美國聯邦調查局和中情局出動了大批人馬。最後，德國警方在下薩克森州羅滕堡縣的瓦芬森——一個只有600名居民的小鎮上抓到了“殺手病毒”的製造者：一個叫做斯萬·賈斯查因（Sven Jaschan）現年18歲的孩子，技術學校的學生。賈斯查因可能在6月以“電腦破壞罪”接受審訊，這項罪名最高可判五年監禁。不過賈斯查因可能不會被判這麼重，因爲他4月底才滿18歲，寫“殺手病毒”病毒時只有17歲。

# Sasser




- 2004年4月
- 郵局ATM大當機
- 目標：

  Windows
- 漏洞：

  MS04-011

# 熊貓燒香

- 熊貓燒香”病毒是一個能在電腦操作系統上運行的蠕蟲病毒。採用“熊貓燒香”頭像作為圖標。它的變種會感染EXE可執行檔，被病毒感染的檔圖標均變為“熊貓燒香”。該病毒會在中毒電腦中所有的網頁檔尾部添加病毒代碼。

# 熊貓燒香

- 新聞資料
- http://www.epochtimes.com/b5/7/2/13/n1621522.htm
- http://www.epochtimes.com/b5/7/2/12/n1621057.htm

# 熊貓燒香

- 2007年1月
- 個人PC成為目標
- 目標：
  - Windows
  - Ghost檔案
- 漏洞：
  - 多種版本

# USB病毒

- USB病毒的增加主要是因為個人使用行動裝置的比例提升，如手機、照相機、甚至GPS導航都成為儲存裝置。若設定這些外接裝置可自動執行（autorun），惡意程式也就隨之自動下載至使用者電腦中。

# USB病毒

- 2007年8月大量爆發
- 目標
  - Windows
- 利用自動播放功能
- 例：KAVO.exe, info.exe

# 病毒趨勢

- 快速：檔案小、散布快
- 隱匿：不再破壞檔案與主機
- 惡意：以後門與rootkit為主
- 即時：利用0-Day弱點

# 感染途徑趨勢

- USB隨身碟
- 全新硬碟
- 惡意網頁
- 詐騙郵件
- 即時通訊軟體
- P2P下載軟體
- 網路釣魚

# 新聞及實例

今日要聞
頭版新聞
焦點新聞
政治新聞
社會新聞
生活新聞
國際新聞
自由言論
爆料投訴
愛心暖流
財經新聞
體育新聞
教育新聞
健康醫療
地方新聞
影視名人
流行消費



# 全新硬碟 被植木馬程式 個人資料 瞬間流向北京

〔記者楊國文、何瑞玲／台北報導〕全新、國際知名大廠品牌、大容量的可攜式硬碟，驚傳已被植入木馬程式病毒，一旦安裝使用，電腦中的資料就會幾乎不知不覺被竊取傳送到在中國北京的兩個網址。

## 泰國生產 在台出貨約兩千台

這批生產地寫著泰國的國際知名品牌Maxtor三點五吋、500G可攜式硬碟，在台灣出貨約有兩千台，在接獲調查局通知後，代理商及通路商都已全面緊急下架，並將接受退貨回收，且已立即換成相近類型但不含病毒的產品上架。

這種全新產品即遭植入木馬程式事件，連電腦專家都表示聞所未聞，但卻真的發生在台灣。


國際知名大廠Maxtor全新的三點五吋可攜式硬碟，竟被植入木馬程式，消費者購入安裝後，電腦內資料可能被竊取機密到北京的網址。調查局調查發現，這極可能是中國網軍竊密的手法。代理進口商與銷售業者昨天緊急宣布會進行下架與回收的動作。圖為這款出問題硬碟的外裝盒。（記者楊國文攝）

訂戶登入

登入帳號：

登入密碼：

登入 取消

綜合文章

- IT應用新聞
- IT應用專題
- 應用案例
- 專欄
- 特別企劃
- 研討會／座談會報導
- 人物
- 活動與課程
- 產品情報
- 廠商動態

話題新聞

# 新購隨身碟也可能暗藏木馬病毒！儲存裝置的安全管理應更爲徹底

(寄信給作者) 2007/10/25

耿慧茹／台北

日本廠商Buffalo於日前證實，該公司所製造的隨身碟，在出廠前疑似因控管失當，被植入專門竊取帳號密碼的木馬病毒，爲了不損及消費者權益，該公司決定以免費交換新品，以及提供防毒軟體進行檢測，作爲補償。



這起事件提醒企業的隨身碟安全管理必須再關注另一環節：即對於新隨身碟也應進行掃毒。Flash技術發展成熟，隨身碟的贈送已經很普遍，商務人士在外，其實有相當多機會可取得免費的隨身碟，舉例來說，在各大研討會、資訊展覽、行銷活動裡，就常將大容量的隨身碟作爲吸引群眾的贈品。

# 駭客散佈連接YouTube假網址誘使用戶中毒

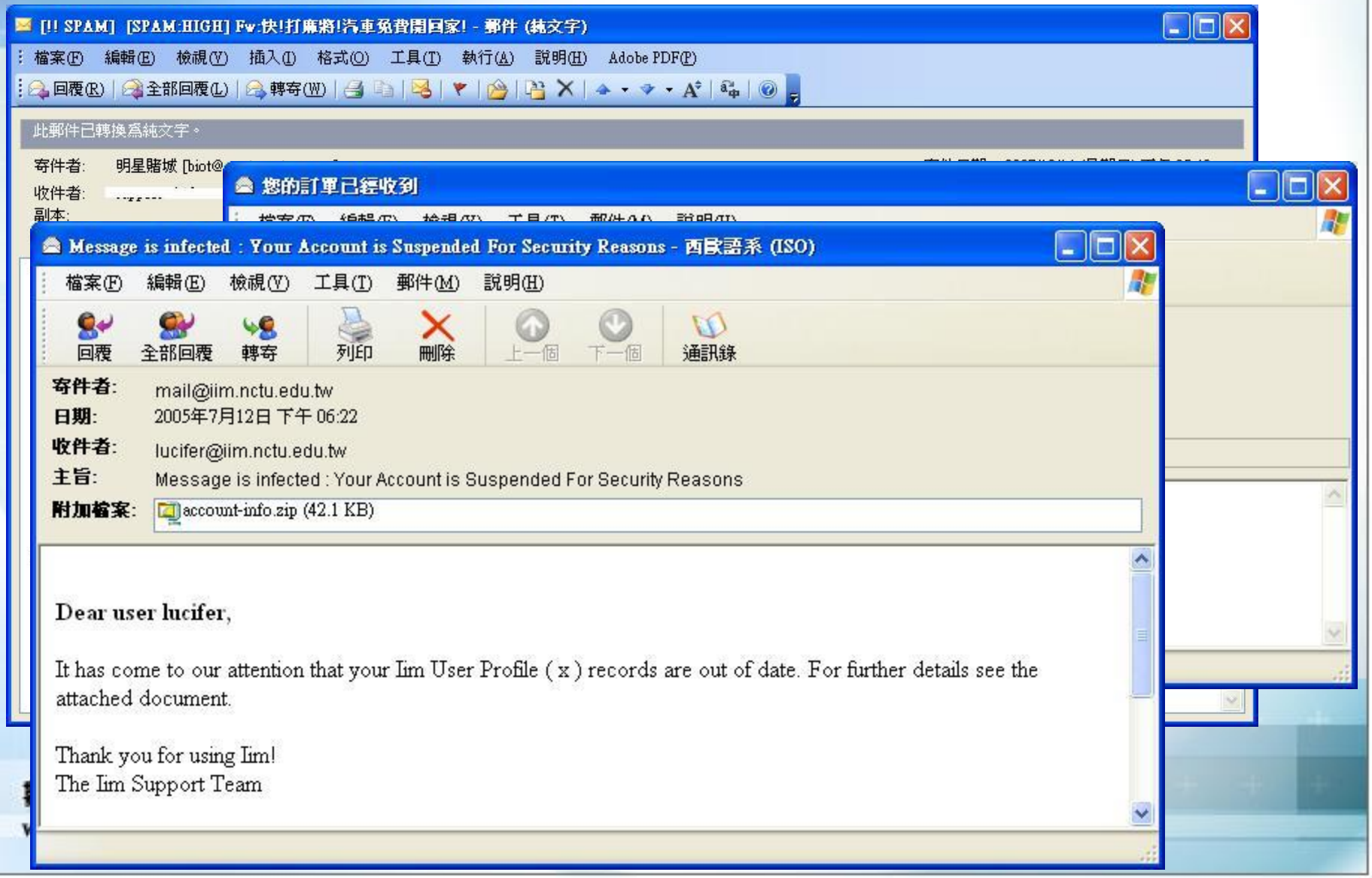
中央社 (2007-08-29 23:35)

轉寄好友 列印

（中央社記者康世人新加坡二十九日專電）英國SophosLabs全球網路安全研究中心今天警告網路用戶，要注意駭客散佈一封提供假YouTube Video網址下載影片的電子郵件，這封電子郵件會誘使網友連接含有惡意軟體或木馬程式的網站，必須提高警惕。

SophosLabs指出，駭客組織利用最近當紅的YouTube數位影片分享網站，大量寄發標題爲「Dudeyour gonna get caught，lol」、「LOL，dude

# 誘人廣告或連結


[!! SPAM] [SPAM:HIGH] Fw:快!打麻將!汽車免費開回家! - 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) Adobe PDF(P)
回覆(R) 全部回覆(L) 轉寄(W)
此郵件已轉換爲純文字。
寄件者: 明星賭城 [biot@
收件者:
副本:
您的訂單已經收到
Message is infected : Your Account is Suspended For Security Reasons - 西歐語系 (ISO)
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: mail@iim.nctu.edu.tw
日期: 2005年7月12日 下午 06:22
收件者: lucifer@iim.nctu.edu.tw
主旨: Message is infected : Your Account is Suspended For Security Reasons
附加檔案: account-info.zip (42.1 KB)
Dear user lucifer,
It has come to our attention that your Iim User Profile ( x ) records are out of date. For further details see the attached document.
Thank you for using Iim!
The Iim Support Team

# 網路詐騙新手法 假買家附件 夾帶木馬程式

由 blue 於 週一, 11/05/2007 - 14:53 發表 ::

Yahoo!奇摩拍賣最近又出現新的詐騙手法。盜取帳號的駭客看上Yahoo!拍賣的人潮，利用盜取的帳號假冒買家寄信給賣家詢問商品，卻在電子郵件中夾帶釣魚網站，或以附件夾帶木馬程式，賣家若開啓此附件，則可能被植入木馬，盜取電腦裡的個人資料。Yahoo!奇摩近期在拍賣討論區內特別發出警告，要求賣家請勿任意開啓買家信中的附件，以免中毒。(記者王珮華／特稿)

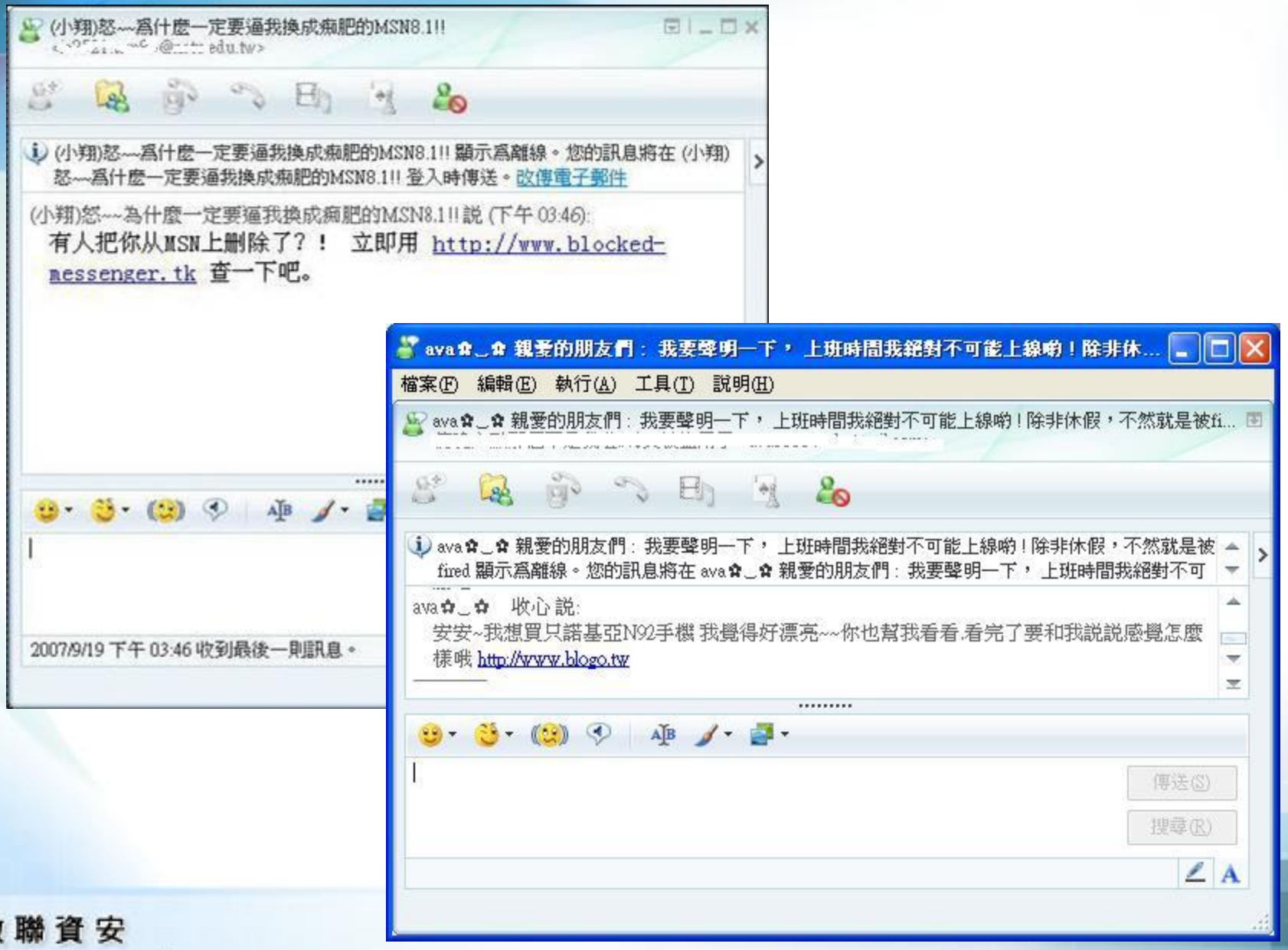
最近不少網拍賣家反映，收到買家寄送的匯款通知信件，內容僅說明自己得標的商品與附件檔案，由於賣家在信中沒看到匯款資料，往往下意識會去開啓附件，甚至附件名稱就被命名爲「匯款明細」，一旦開啓附件，即被植入木馬，帳號密碼都會被駭客所側錄。近期許多帳號被盜，進而開設詐騙賣場的案件，都是來自於這類的釣魚網站或木馬程式。

也有賣家莫名其妙收到買家詢問的電子郵件，內容不外是「我想要買這件商品」，或者是「我想買這個賣場的東西，如果不是被盜用的話我就下標了」，之後附上網址，吸引賣家點入，由於該網址爲釣魚網站，若點進去的話，很可能會被植入木馬，盜走帳號密碼。

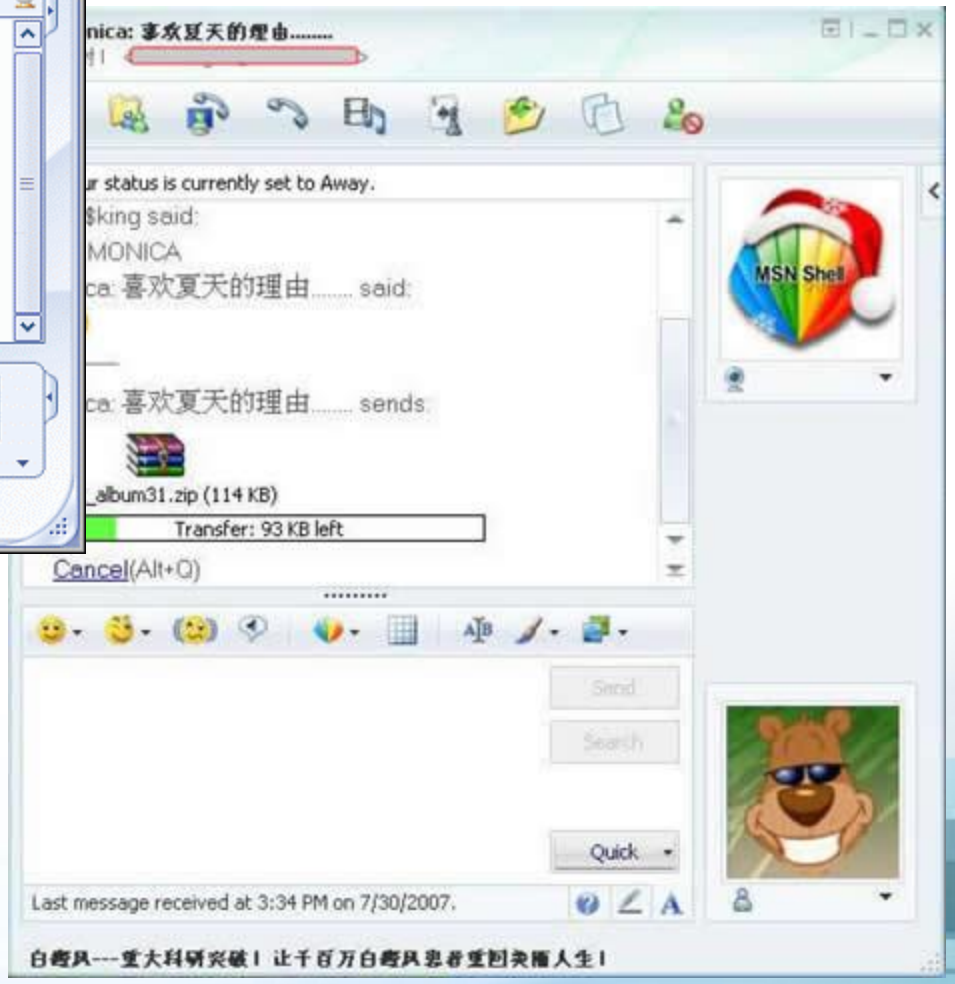
最可怕的是，駭客透過網頁以假亂真的技術越來越強，部份釣魚郵件所附上

資安新聞連結
- 趨勢科技提供免費Sony PS3安全軟體
- Windows防拷驅動程式存漏洞可取得電腦存取權
- Salesforce員工遭網釣攻擊洩漏客戶資訊
- Apple 修正七項 Quicktime 漏洞
- 趨勢宣布推出企業行動裝置安全防護方案
- 併購Vontu 賽門鐵克拓展安全防護領導地位
- McAfee新版ePO管控台納入資料防漏技術

更多資安新聞


(小翔)怒~~為什麼一定要逼我換成痴肥的MSN8.1!!
(小翔)怒~~為什麼一定要逼我換成痴肥的MSN8.1!! 顯示為離線。您的訊息將在 (小翔)怒~~為什麼一定要逼我換成痴肥的MSN8.1!! 登入時傳送。改傳電子郵件
(小翔)怒~~為什麼一定要逼我換成痴肥的MSN8.1!! 說 (下午 03:46):
有人把你从MSN上删除了？！ 立即用 http://www.blocked-messenger.tk 查一下吧。
2007/9/19 下午 03:46 收到最後一則訊息。
ava✿_✿ 親愛的朋友們：我要聲明一下，上班時間我絕對不可能上線喲！除非休...
檔案(F) 編輯(E) 執行(A) 工具(T) 說明(H)
ava✿_✿ 親愛的朋友們：我要聲明一下，上班時間我絕對不可能上線喲！除非休假，不然就是被fi...
ava✿_✿ 親愛的朋友們：我要聲明一下，上班時間我絕對不可能上線喲！除非休假，不然就是被fired 顯示為離線。您的訊息將在 ava✿_✿ 親愛的朋友們：我要聲明一下，上班時間我絕對不可
ava✿_✿ 收心 說:
安安~我想買只諾基亞N92手機 我覺得好漂亮~~你也幫我看看.看完了要和我說說感覺怎麼樣哦 http://www.blogo.tw
傳送(S)
搜尋(R)


sunmooncn@sina.com - 对话
文件(F) 编辑(E) 操作(A) 工具(T) 帮助(H) Plus!
msn
邀请(I) 发送文件(N) 网络摄像机(W) 音频(U) 活力地带(L)
收件人：
Jason_ _西湖歌舞几时休。 说：
明天我请客！
说：
为什么？？？？
Jason_ _西湖歌舞几时休。 发送：
明天我请客.scr (28 KB)
双击此处开始传输
接受 (Alt+C) 另存为... (Alt+S) 拒绝 (Alt+D)
字体(O) 背景(B)
发送(S)
最后一条消息收于 2003-12-11，16:26。


r status is currently set to Away.
$king said:
MONICA
喜欢夏天的理由..... said:
喜欢夏天的理由..... sends:
album31.zip (114 KB)
Transfer: 93 KB left
Cancel(Alt+C)
Send
Search
Quick
Last message received at 3:34 PM on 7/30/2007.
MSN Shell

# 防毒特報／MSN病毒變種快　會火星文、注音文還會對話...

ETtoday

更新日期:2007/08/14 10:20

「千萬別開我傳的網址或檔案！」MSN病毒肆虐情況愈來愈嚴重，實在讓人很抓狂，據防毒專家指出，MSN病毒變種的速度愈來愈快，常見手法除了傳送木馬程式，還會傳釣魚網站的網址，並夾帶中文、表情符號、注音文或火星文，甚至直接跟你對話，簡直防不勝防。

當朋友突然用MSN傳「photos.zip」、「PictureAlbum2007.zip」等壓縮檔給你時，你可能還有點警覺心，識破這是木馬程式搞的鬼；但若朋友傳了一串網址給你，叫你去看笑話，或說：「這是我新申請的部落格，有一些照片，可以去看看喔！」可要注意了，這些都是釣魚網站，會竊取你的帳號、密碼。

賽門鐵克個人消費性產品事業部系統工程師王世煜表示，MSN病毒最主要有兩種擴散手法，最常見的是傳木馬程式，另一種則是傳送釣魚網站，連上網後要求你輸入帳號、密碼或其他個人資料，並立刻透過你的帳戶傳檔案給別

# 惡意程式、內容冒充外洩筆錄鑽進Foxy用戶PC

記者馬培治／台北報導　18/04/2007

PRINT　EMAIL　SAVE

專家警告，有假檔案搭著警方筆錄外洩新聞事件順風車，利用FOXY散佈，建議使用者仍應小心。

上週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，資安專家一度建議使用者在真相未明前先刪除該軟體。而刑事局則發現，有部份以「刑案筆錄」等文字爲檔名的假檔案，在新聞熱潮下透過FOXY傳散，實際內容則爲援交訊息、護膚按摩廣告甚至內含惡意程式，警方呼籲使用者不要因好奇下載來路不明的檔案。

「這種手法相當常見，」CA（組合國際）技術顧問林宏嘉指出，檔名與實際內容不符的假檔案，在P2P軟體上相當常見，也是駭客散佈惡意程式的途徑之一，他表示，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。

而值得注意的是，此次引起話題的FOXY軟體，用戶竟以上班族且在上班時間使用占最大宗。據林宏嘉觀察，上班時間是FOXY使用高峰，他

# 關鍵字廣告


YAHOO! 奇摩 新聞
會員登入
新使用者？立即註冊
搜尋網頁
服務首頁 | 服務說明 | Yahoo!奇摩
新聞首頁 政治 社會 地方 國際 財經 科技 運動 健康 教育 藝文 影劇 旅遊 生活
資訊3C | 科學發展 | 自然環境 | 照片故事 | 專輯 | 民調中心
2007/03/03(星期六) 農曆(丁亥)正月十四日
新聞首頁 > 科技 > 資訊3C > 中時電子報
寄給朋友 | 友善列印
別亂點關鍵字廣告 兩岸駭客用假網頁盜個資詐財
中時電子報 更新日期：2007/02/08 04:09 記者： 吳俊陵／台北報導
兩岸駭客聯手在大型搜尋網站買下「關鍵字廣告」行銷，置入「網路銀行」、「航空公司」、「旅行社」、「電腦科技公司」、「人力銀行」等五十多個假網頁，趁民眾誤點的機會植入木馬程式，竊取個人信用資料和帳號密碼，進行盜轉存款、預借現金、小額付費、網路購物等盜領洗錢犯罪。
兩岸駭客以「釣魚網頁」植入木馬，造成國內上百家公司企業和不計其數的民眾電腦遭到入侵，駭客手上掌握的個人資料達數十萬筆，數百筆網路銀行客戶的帳號密碼遭盜取，進行預借現金和信用卡盜刷購物，初估有十多家網路銀行損失數百萬元，金額還在擴大之中。
請輸入搜尋關鍵字
搜尋新聞
廣 告
Yahoo!奇摩星相
從掌紋分析職場性向
大師幫你解析
Yahoo!奇摩拍賣 推薦最愛商品 發表使用心得
美容大王
最愛睫毛膏討論區
沙龍護髮產品大推薦討論區


拍賣 - Google 搜尋 - Windows Internet Explorer
拍賣 - Google 搜尋
Jean.MT@gma
所有網頁 圖片 新聞 網上論壇 更多 »
Google
拍賣
搜尋
進階搜尋 | 使用偏好
搜尋所有網站 搜尋所有中文網頁 搜尋日文 和 法文 和 英文 和 繁體中文 和 簡體中文
所有網頁
個人化 關於拍賣大約有3,640,000 頁日文 和 法文 和 英文 和 繁體中文 和 簡體
Yahoo!奇摩拍賣
www.bids-yahoo.com
物品交換中心,提供中古、新品、收藏品 完整拍賣教學 買家/賣家購物保障
贊助廠商
Yahoo!奇摩拍賣:拍賣,包括:精品,電腦,手機,數位相機,mp3,美容,中古車 ...
什麼都有、什麼都賣，名牌精品、電腦、手機、數位相機、電玩遊戲、中古車二手車、mp3、
美容保養品，歡迎來網拍拍賣！
tw.bid.yahoo.com/ - 62k - 頁庫存檔 - 類似網頁 - 加入筆記本
Yahoo!奇摩拍賣:拍賣,包括:精品,電腦,手機,數位相機,mp3,美容,中古車 ...
小心匯款通知Email附件 · 賣家好康:買家結帳你賺錢，免抽獎送現金 Timberland拍賣獨享五折起
· 美人館 · OL館 · 3C館 · 家電館 · Motor館 · 玩FUN館 · 我要賣東西 · 我的拍賣 · 討論區/公告 · 求
助. 關鍵字, 商店名稱, 賣家帳號, 拍賣編號 ...
tw.bid.yahoo.com/tw - 63k - 頁庫存檔 - 類似網頁 - 加入筆記本
[ tw.bid.yahoo.com 的其它相關資訊 ]

艾克索夫實驗室 » 查天堂，找天堂，讓你電腦上天堂 - Microsoft Internet Explorer

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 媒體

網址(D) http://x-solve.com/blog/?p=98 移至 連結

Google 開始 書籤 5 已攔截 拼字檢查 翻譯 傳送到 設定

3.另是否我不玩線上遊戲、也不用網拍你能奈我何?有這種想法的朋友現在可能要改變一下了:P，駭客與詐騙集團是不會原地踏步的(他們也是講求創新、殺手級應用的:P)，大家搜尋引擎有用過吧? 例如:Google、yahoo搜尋、拍賣、知識+等應是民眾經常使用的搜尋引擎，這些搜尋引擎除了提供最符合(排名)使用者查詢之關鍵字網站外，當然對於付費的使用者會把他們的網址排在較顯著的位址:P (例如:購買Yahoo、Google等關鍵字廣告)，假如你(妳)是個遊戲玩家或是一位虔誠的基督徒，應該有搜索過”天堂”的關鍵字經驗吧:XD，某知名引擎搜尋結果如下:


**位居於前五名的網站www(dot)2uo(dot)com(dot)tw(千萬不要嘗試)，它會是一些瀏覽者進入天堂的不錯管道(印證了好的網站帶你上天堂:))。**

網際網路

新 聞
新 聞 專 題
即 時 新 聞
新 聞 簡 訊
技 術
產 品 報 導
技 術 專 題
IT 書 訊
IT管理

# 美國求職網站被植木馬 竊取使用者資料

文/陳曉莉 (編譯) 2007-08-20

**研究人員發現，駭客開始在今年5月於各大人力銀行網站放置惡意廣告，一但使用者點選該惡意廣告就會受到木馬程式感染。**

資訊安全業者SecureWorks的兩名研究人員Joe Stewart及Don Jackson在上周五（8/17）提出警告，發現有一台駭客專門用來儲存資料的伺服器存放了4.6萬名使用者的個人資料，而這些資料是駭客透過在人力銀行網站上所置放的惡意廣告，讓使用者電腦感染Prg Trojan木馬程式所竊取而來。

研討會訊息
- Data de-duplicat
- 微軟 BizTalk Se 上市發表會
- Microsoft Tech
- Microsoft MIX(

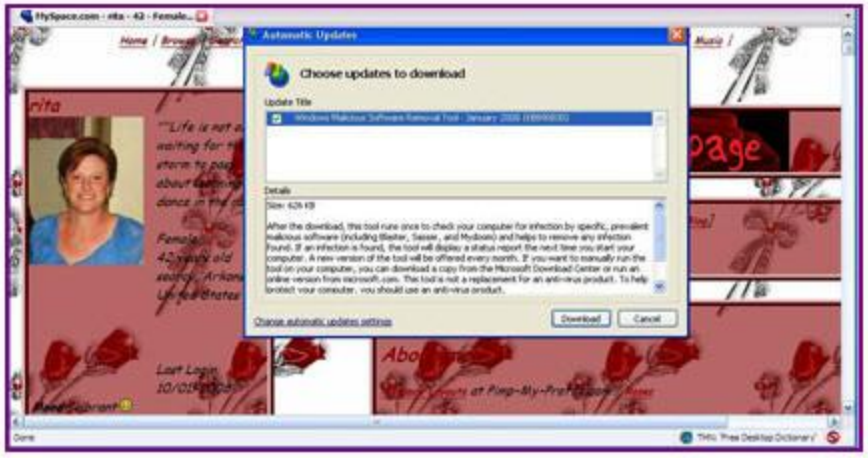
Blog

# ITinternals

## 木馬偽裝成Windows Update 潛伏在MySpace頁面

一月 14th, 2008 | 張貼者： ITinternals | 51Views

McAfee研究人員發現，熱門社交網站MySpace的某些頁面被植入惡意程式碼，此惡意程式偽裝(或)成微軟的Windows Update，藉以分散受害者的注意力，讓受害者誤以為是真的Windows Update，而執行此程式。




(圖片來源：The Register)

### 文章存檔

- 2008 年 一月
- 2007 年 十二月

### 文章分類

- AntiRootkit (1)
- 一般新聞 (1)
- 國內資安新聞 (12)
- 國外資安新聞 (19)
- 垃圾郵件 (4)
- 安全更新 (2)
- 安全漏洞 (10)
- 惡意程式 (7)
- 檔案誤判 (1)
- 資安法律 (1)
- 身分盜賊 (1)
- 駭客入侵 (3)

# 假造網站(1)


個人金融理財網 - 臺灣銀行 - Microsoft Internet Explorer
http://www.my-bot.com/
銀行
個人金融理財網
首頁 | 網站導覽
首頁 網路銀行 理財資訊 理財規劃 服務據點 線上客服
電子化服務
信用卡服務
存款服務
貸款服務
外匯服務
信託服務
證券理財
票券理財
境外金融
保管箱
法拍屋訊
客戶通訊
若您無法看到FLASH效果,可連結此按鈕
INSTALL NOW
證券下單/融資利率 超優惠
人性化介面、貼心的服務、即時的資訊,
讓您即時掌握理財方向
Easy pass
使用說明
電子銀行服務
網路銀行
證券下單
學雜費服務網
就學貸款服務網
代理收付保險費
金融行情查詢
即時金融行情
即時財經新聞
即時股市新聞
台股走勢圖
牌告價格查詢
牌告匯率
歷史匯率
新台幣存放款利率
外匯存款利率
消費者貸款利率
短期票券利率
公債附條件交易利率
可轉讓存單牌告利率
最新推薦
行動理財大樂透! 理財達人大募集!!
全民理財總動天!一起加入理財的行列,趕快參加行動理財王票選、行動樂透王抽獎活動、X-Box 360、香港迪士尼來回機票等豐富大獎等你拿 ....more
"幸福" 留給準備好的人
給自己及所愛的人一個安心的保障,輕鬆的人生,夠闊的未來、、、享受沒有壓力的生活,就在彈指之間 ....more
中信局betacare倍得康購物網站照顧您的健康
「betacare倍得康健康美容網站」產品嚴選有保障,您可輕鬆購買中信局優質的保健美容產品,更可享有紅利積點及換金回饋等多重優惠 ....more
網頁發生錯誤。
網際網路


Whois.Net
DOMAIN-BASED RESEARCH SERVICES
WHOIS information for my-bot.com:
[whois.dns.com.cn]
Domain Name..... my-bot.com
Creation Date..... 2006-05-14 10:37:12
Registration Date.... 2006-05-14 10:37:12
Expiry Date..... 2007-05-14 10:37:12
Organisation Name.... xinf
Organisation Address. XM
Organisation Address.
Organisation Address. X M
Organisation Address. 361000
Organisation Address.
Organisation Address. CN
中國

# 你分的出來嗎?






# 你分的出來嗎?


104人力銀行~不只找工作，為你找方向！104人力銀行以"全職、獵
http://www.104.com.tw/
104人力銀行~不只找工作，為你找方向！104...
104家族
人力銀行
人脈銀行
家教網
外包網
人才派遣
加入最愛
104 動態
104中國
104 人 力 銀 行
.com.tw
www.104.com.tw
CIGNA International
104最新消息
新手上


104人力銀行~不只找工作，為你找方向！104人力銀行以"全職、獵
http://www.104.com.tw/
104人力銀行~不只找工作，為你找方向！104...
104家族
人力銀行
人脈銀行
家教網
外包網
人才派遣
加入最愛
104 動態
104中國
104 人 力 銀 行
.com.tw
www.104.com.tw
CIGNA International
104最新消息
新手上


104人力銀行~不只找工作，為你找方向
http://www.104.com.tw/
104人力銀行~不只找工作，為你找方向

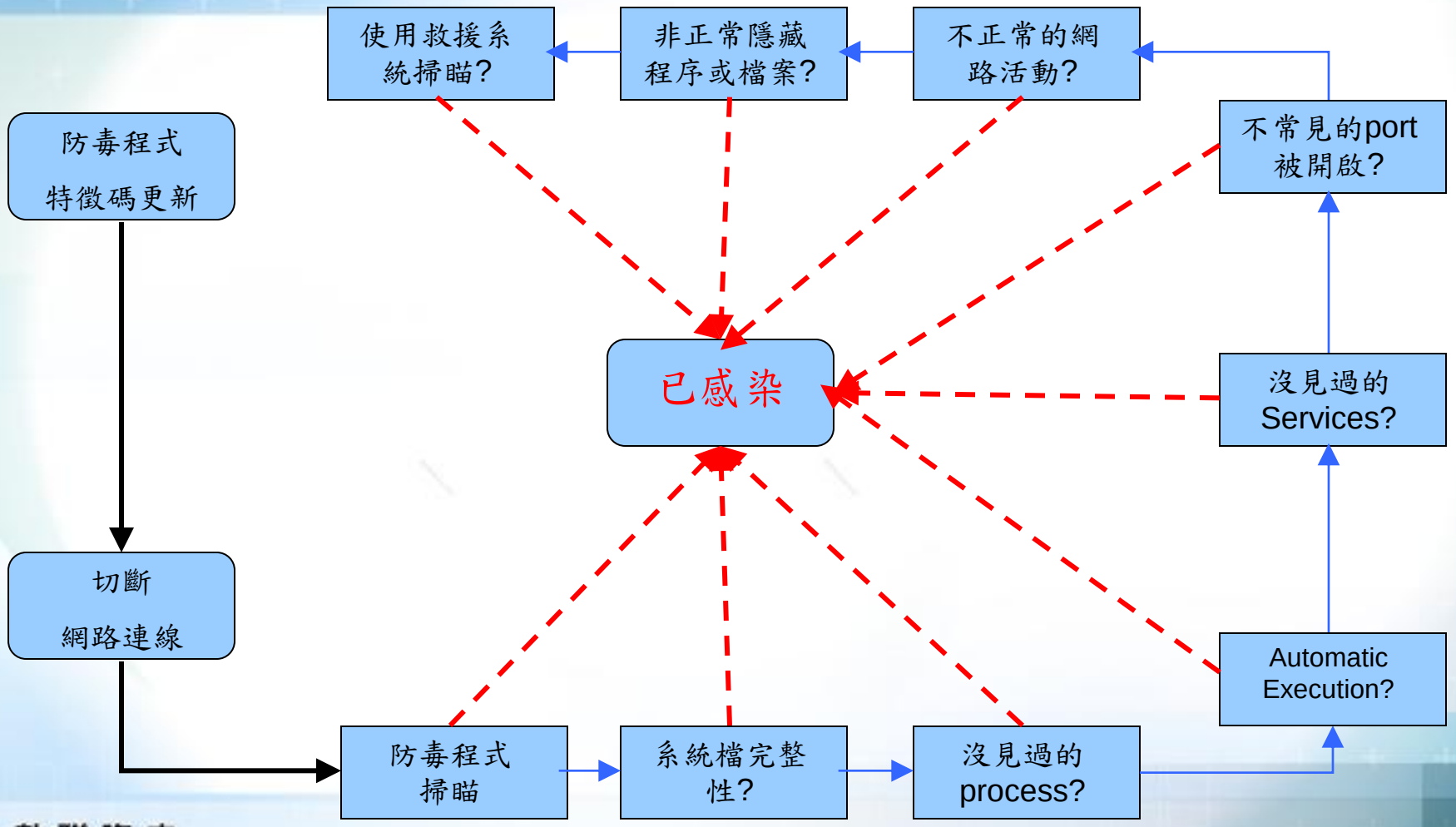

104人力銀行~不只找工作，為你找方向
http://www.104.com.tw/
104人力銀行~不只找工作，為你找方向

# 如何判斷是否中獎

- 網路異常的緩慢
- 硬碟燈閃不停
- 程式莫名的自行關閉
- 防毒程式無法啟動
- 防毒程式無法更新
- C槽無法開啟...
- .....

# 如何分辨並清除惡意程式

# 如何確定是否已遭感染


防毒程式
特徵碼更新
切斷
網路連線
防毒程式
掃瞄
系統檔完整
性?
沒見過的
process?
Automatic
Execution?
沒見過的
Services?
不常見的port
被開啟?
不正常的網
路活動?
非正常隱藏
程序或檔案?
使用救援系
統掃瞄?
已感染

# Checklist:辨識是否為惡意程式

| 流程 | 工具 | 結果 |
|---|---|---|
| 更新特徵碼及切斷網路連線 | | |
| 防毒程式完整掃瞄 | Antivirus/Antispyware | |
| 檢查系統檔案完整性 | MD5 / Tripwire | |
| 檢查running processes | Process Explore | |
| 檢查Automatic Execution部份 | | |
| 檢查Services部份 | Service Control Manager | |
| 檢查listening port | Netstat / Port Monitor | |
| 檢查網路活動 | Network Monitor / Wireshark | |
| 檢查是否有隱藏程序或檔案 | IceSword / RootkitRevealer | |
| 透過救援系統檢查 | WinPE / BartPE | |

# 如何清除惡意程式

- 刪除或更名惡意程式新增之物件
  - Service
  - Process
  - BHO (Browser Helper Object)
  - Registry
  - 其它相關檔案
- 使用救援系統
  - 若無法直接更動檔案時
  - 記得將原系統的登錄檔刪除
- 重新檢查系統是否已恢復正常

# 惡意程式分析與採樣

# 大綱

- 惡意程式偵測, 找尋與採樣
  - 線上採樣
  - 記憶體採樣
- 分析
  - 動態分析
  - 靜態分析
  - 沙盒分析
  - 線上沙盒分析

# 線上採樣

# 線上採樣

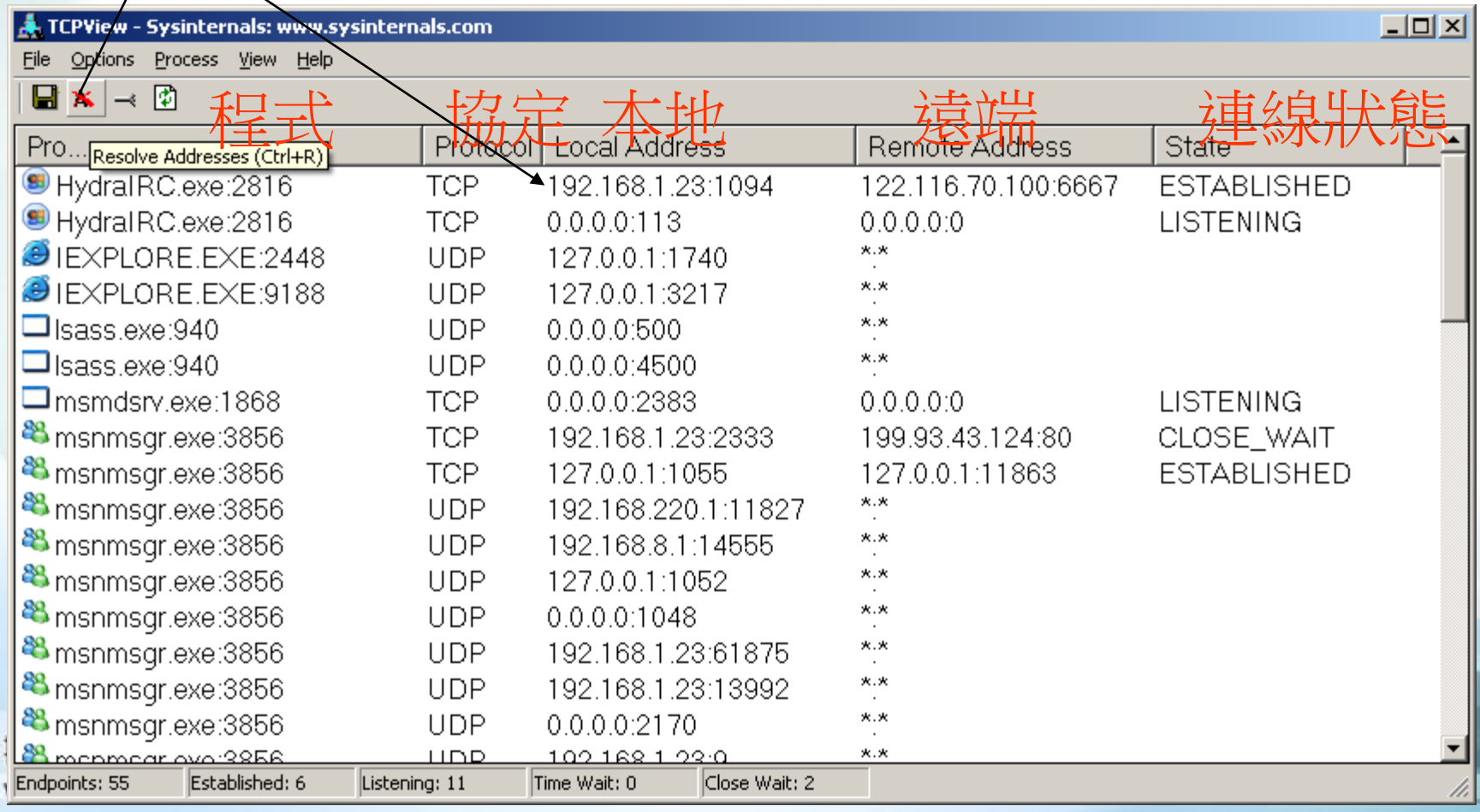
- 要採樣那些?
- 人工採樣
  - TCPVIEW/Procexp/procmon/regcheck/autoruns/gmer…
- 程式自動採樣(issduscan)

# 人工採樣

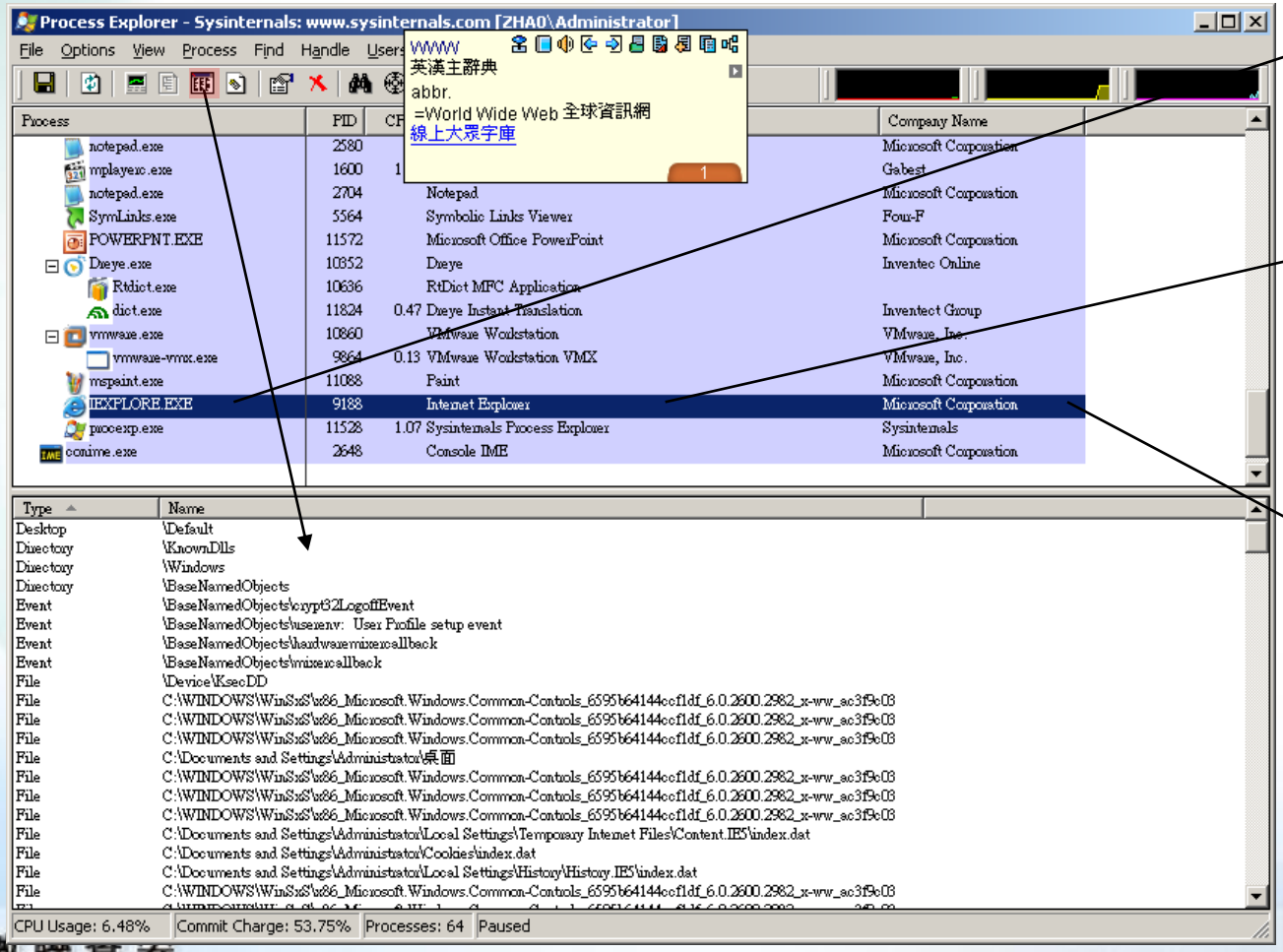
- 採樣項目
  - Process
  - File
  - Registry
  - Service
  - Port
  - Network Activity
  - etc....

# TcpView主控台

解析 IP 位址



# Process Explorer主控台

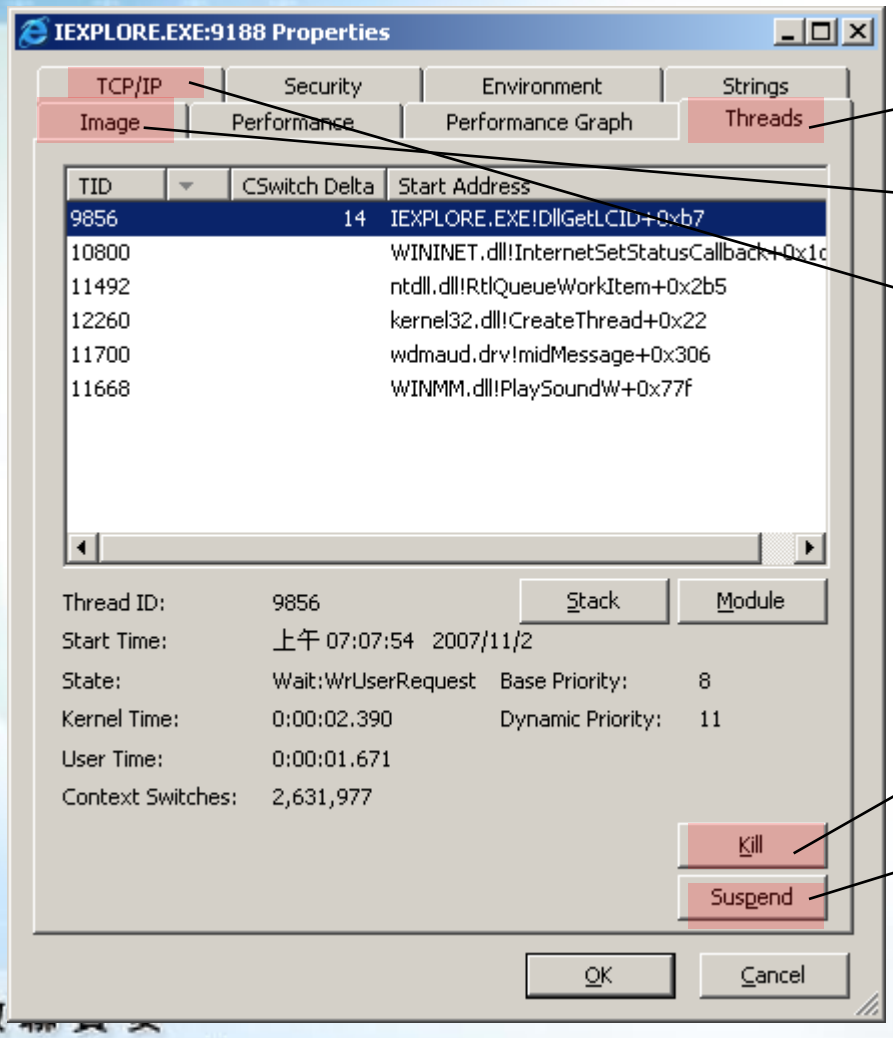



可刪除

按下去可看細節

按兩下可看更多資訊

# Process Explorer分項資訊




Threads : 正在執行的程式區段

Image : 程式檔案路徑

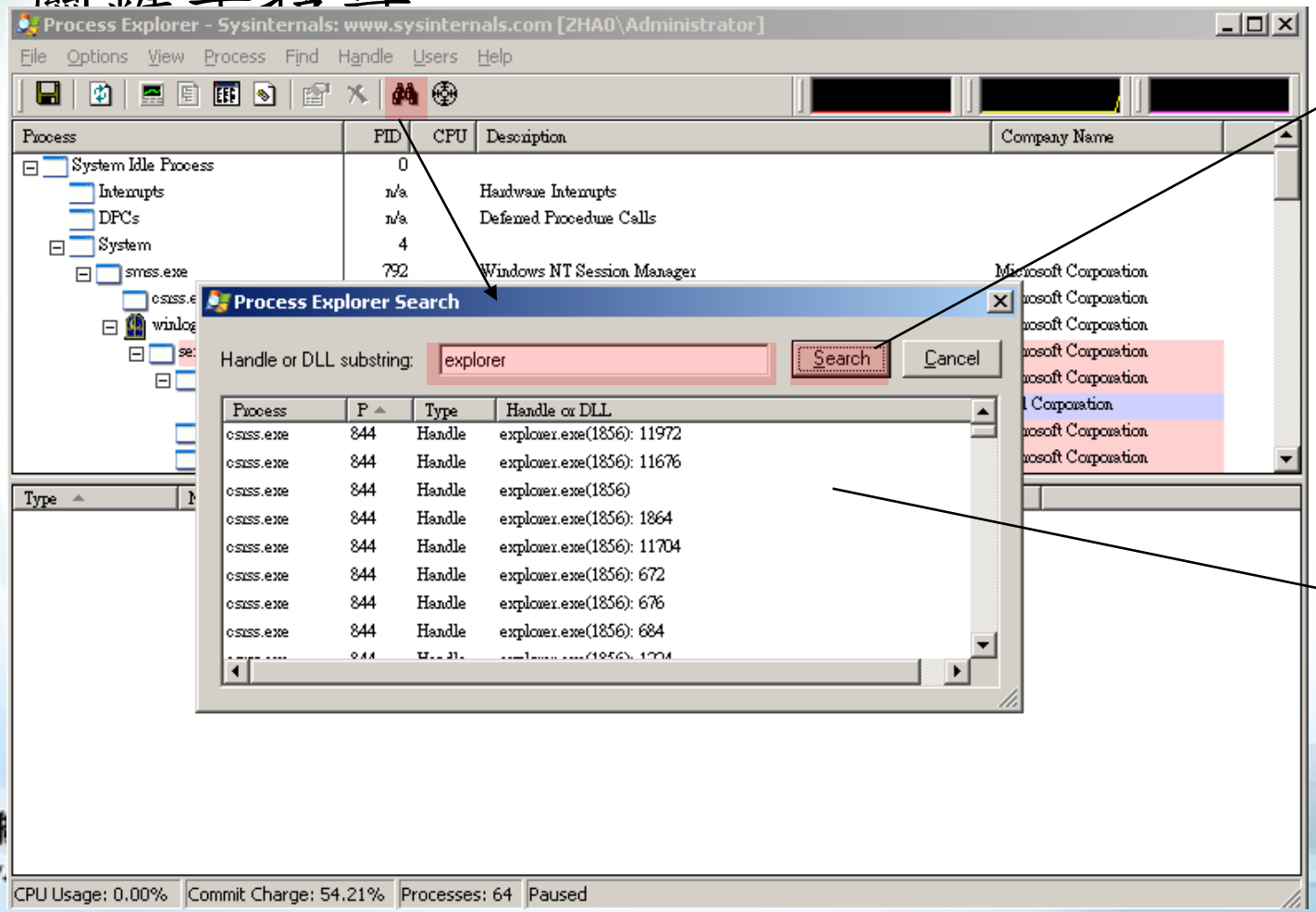
TCP/IP : 網路連線狀態

Kill : 刪除

Suspend : 暫停
Resume :恢復

# Process Explorer資料搜尋畫面

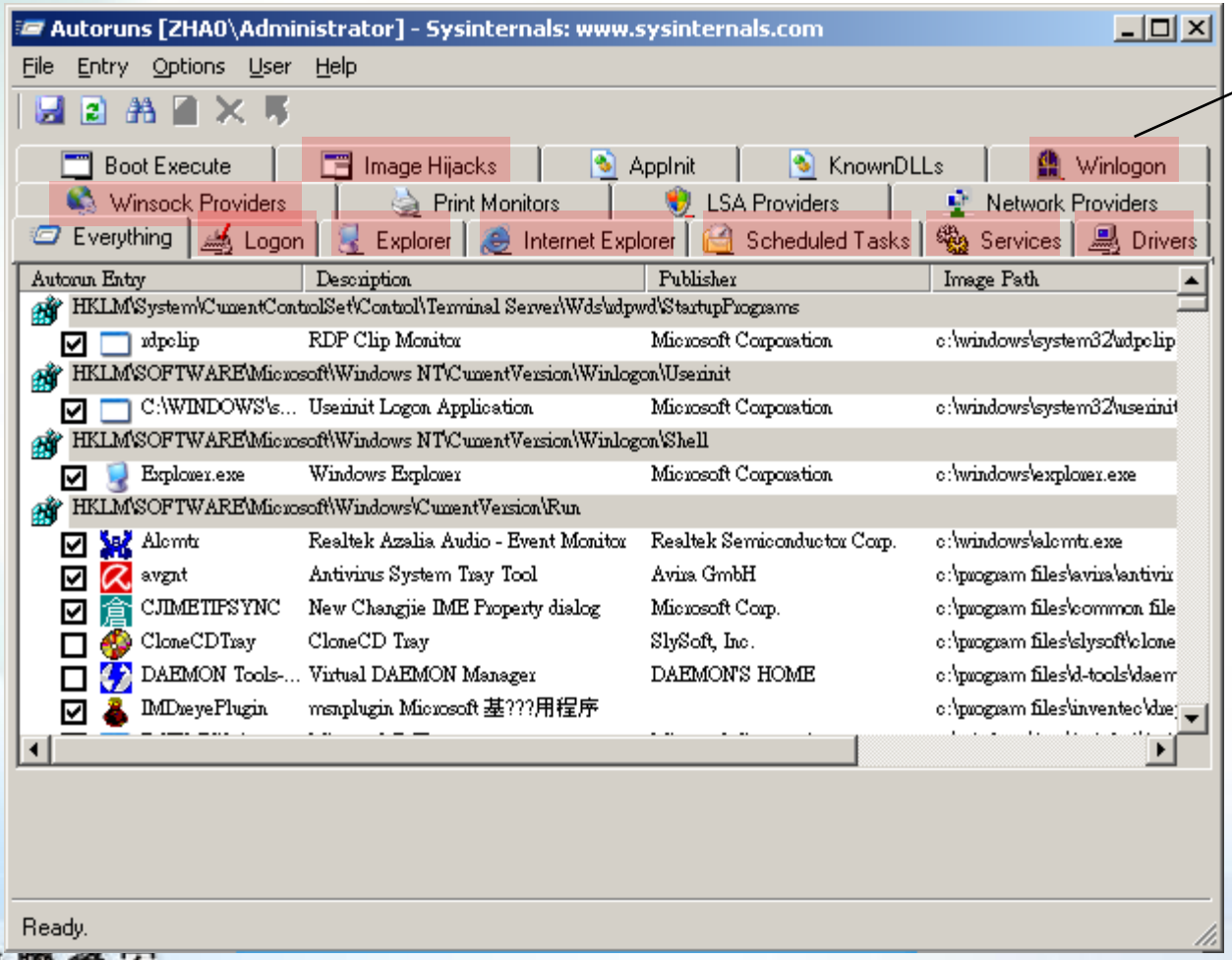
- 關鍵字搜尋




搜尋

結果

# Autoruns主控台




惡意程式常見掛載位址

# 程式自動採樣(Log 收集)

- 如何從log判斷有異常
  - 黑名單
  - 白名單
  - 程式簽章
  - 防毒/線上防毒協助
- 把疑似有問題的檔案採樣後，開始分析

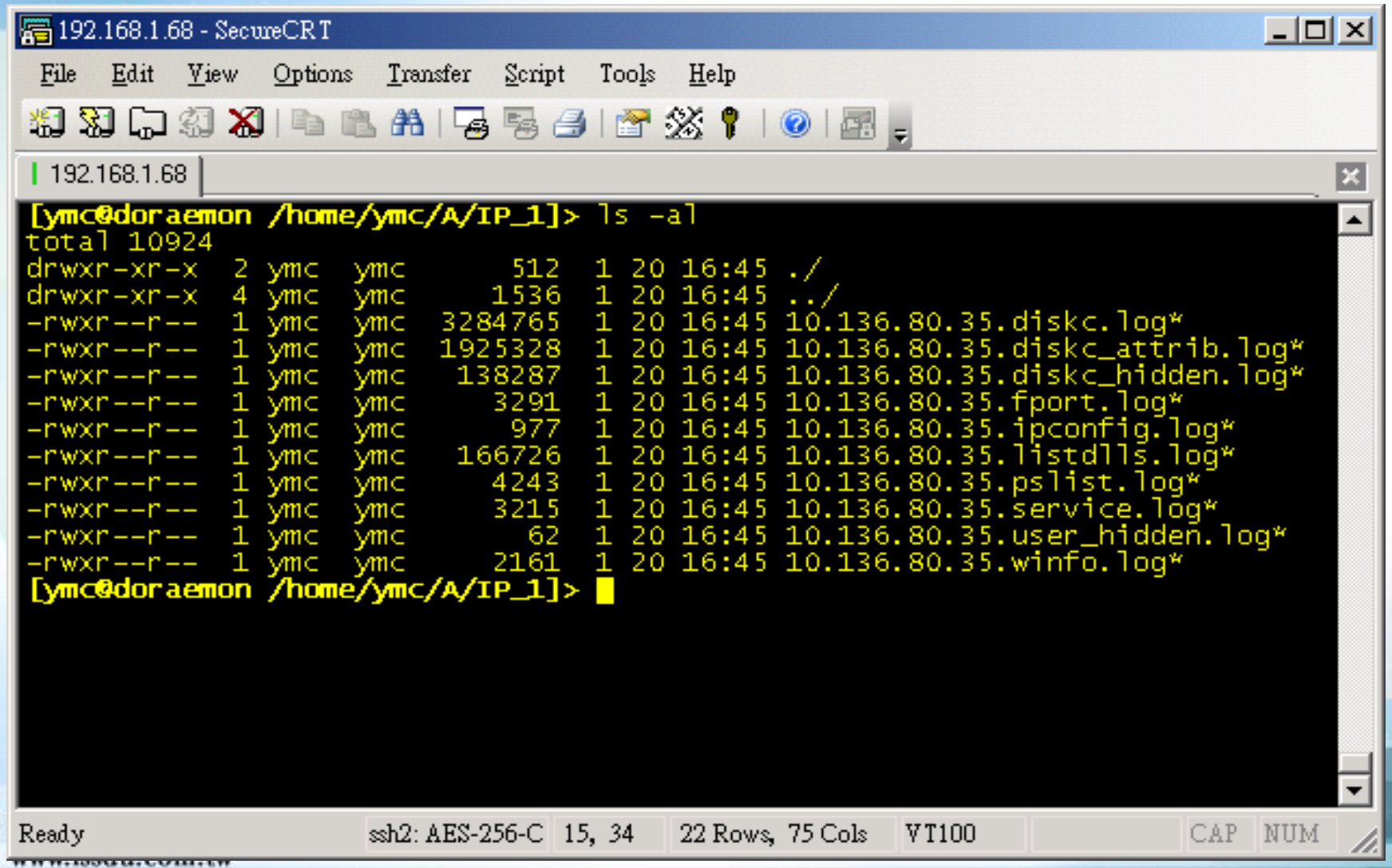


可參考issdu自行研發的線上log收集程式

# 應該收集的系統資訊

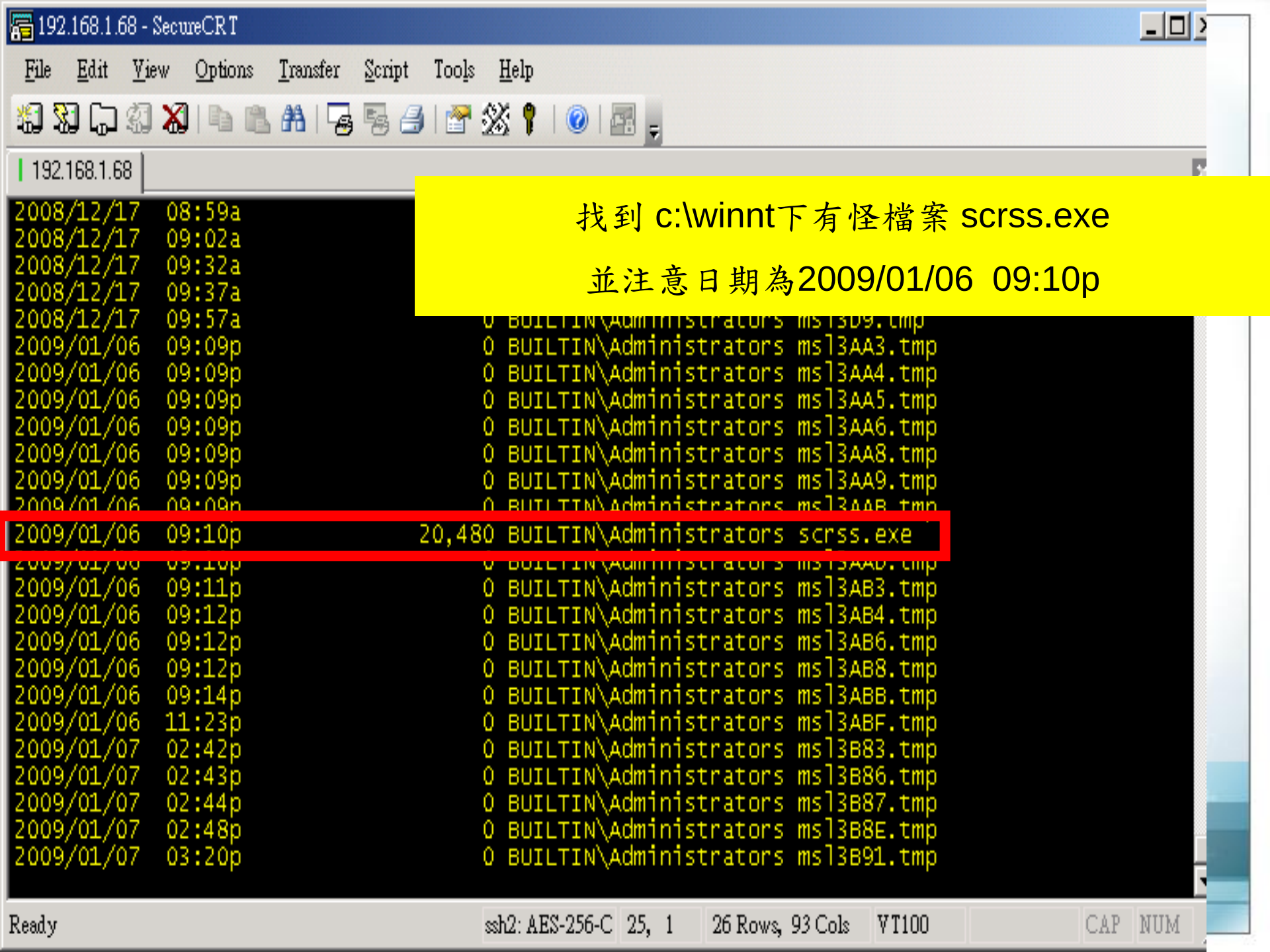
- 機器IP組態資訊
- 系統內的執行程式列表
- 執行程式與配屬的DLL列表
- 硬碟C槽的檔案資訊(檔名,時間,大小,屬性)
- 系統目前開的PORT
- 系統所安裝的服務
- 其他一般系統資訊
- 隱藏的使用者資料

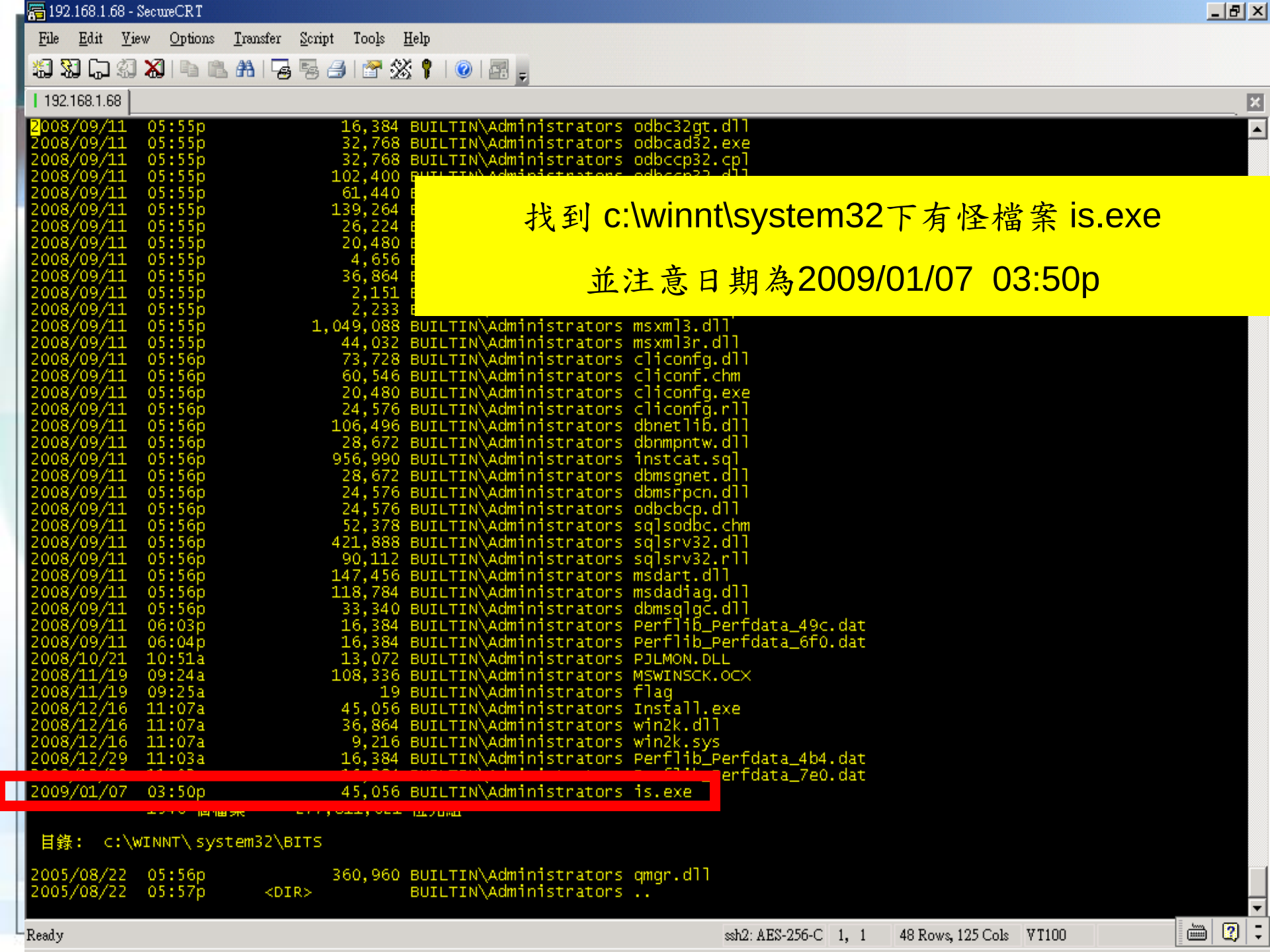
# 收集到的資訊列表


192.168.1.68 - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.68
[ymc@doraemon /home/ymc/A/IP_1]> ls -al
total 10924
drwxr-xr-x 2 ymc ymc 512 1 20 16:45 ./
drwxr-xr-x 4 ymc ymc 1536 1 20 16:45 ../
-rwxr--r-- 1 ymc ymc 3284765 1 20 16:45 10.136.80.35.diskc.log*
-rwxr--r-- 1 ymc ymc 1925328 1 20 16:45 10.136.80.35.diskc_attrib.log*
-rwxr--r-- 1 ymc ymc 138287 1 20 16:45 10.136.80.35.diskc_hidden.log*
-rwxr--r-- 1 ymc ymc 3291 1 20 16:45 10.136.80.35.fport.log*
-rwxr--r-- 1 ymc ymc 977 1 20 16:45 10.136.80.35.ipconfig.log*
-rwxr--r-- 1 ymc ymc 166726 1 20 16:45 10.136.80.35.listdlls.log*
-rwxr--r-- 1 ymc ymc 4243 1 20 16:45 10.136.80.35.pslist.log*
-rwxr--r-- 1 ymc ymc 3215 1 20 16:45 10.136.80.35.service.log*
-rwxr--r-- 1 ymc ymc 62 1 20 16:45 10.136.80.35.user_hidden.log*
-rwxr--r-- 1 ymc ymc 2161 1 20 16:45 10.136.80.35.winfo.log*
[ymc@doraemon /home/ymc/A/IP_1]>
Ready
ssh2: AES-256-C
15, 34
22 Rows, 75 Cols
VT100
CAP
NUM

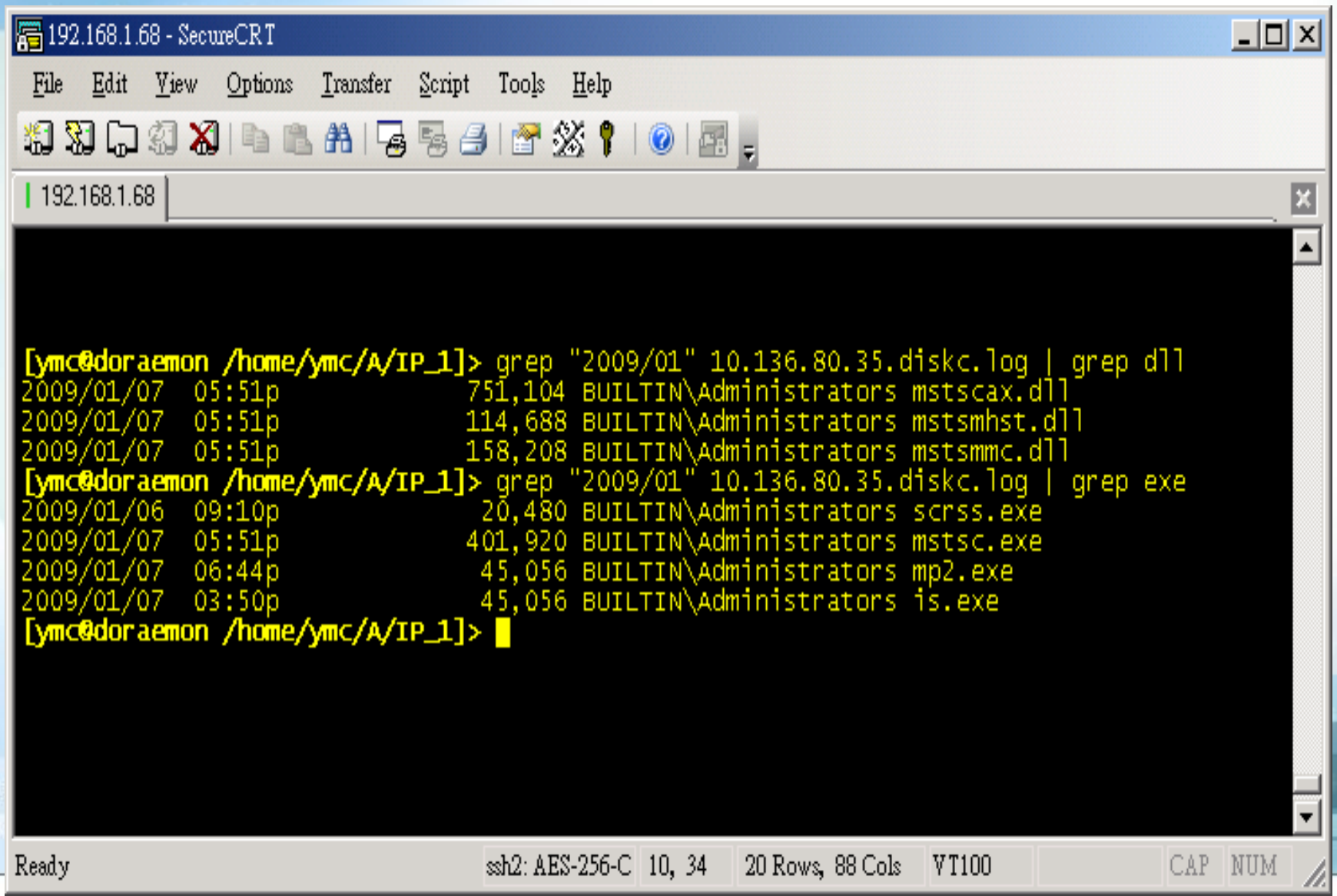
# Ctc.log

- 檔案內容
  - 硬碟C槽的檔案列表
- 查看重點
  - 沒見過的檔案(如果有前一次的資料, 可以做差異比對)
  - 特定日期的找尋
  - %systemroot% 與 %systemroot%\system32 目錄的查看

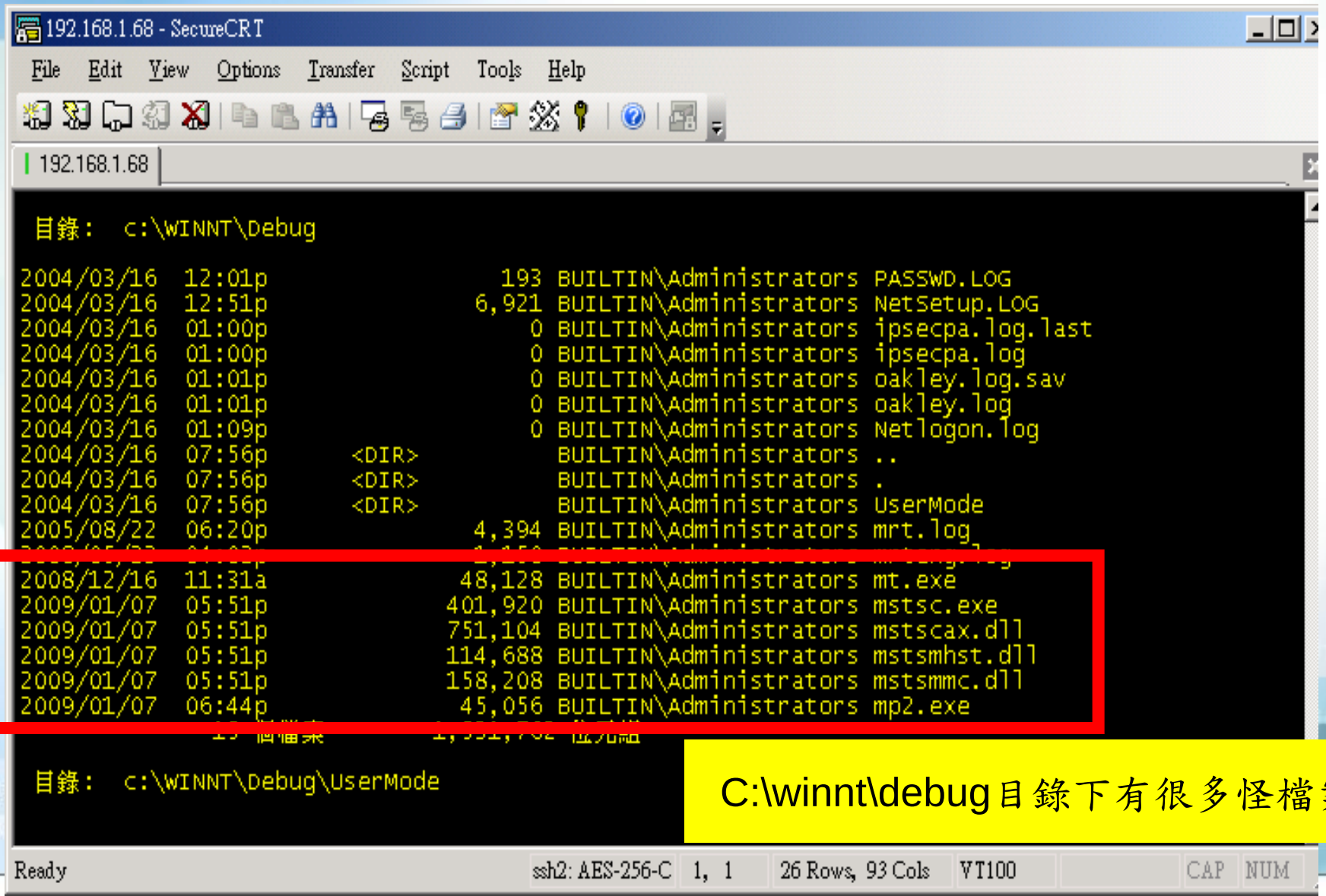

192.168.1.68 - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.68
找到 c:\winnt下有怪檔案 scrss.exe
並注意日期為2009/01/06 09:10p
2008/12/17 08:59a
2008/12/17 09:02a
2008/12/17 09:32a
2008/12/17 09:37a
2008/12/17 09:57a
2009/01/06 09:09p 0 BUILTIN\Administrators msl3AA3.tmp
2009/01/06 09:09p 0 BUILTIN\Administrators msl3AA4.tmp
2009/01/06 09:09p 0 BUILTIN\Administrators msl3AA5.tmp
2009/01/06 09:09p 0 BUILTIN\Administrators msl3AA6.tmp
2009/01/06 09:09p 0 BUILTIN\Administrators msl3AA8.tmp
2009/01/06 09:09p 0 BUILTIN\Administrators msl3AA9.tmp
2009/01/06 09:10p 20,480 BUILTIN\Administrators scrss.exe
2009/01/06 09:11p 0 BUILTIN\Administrators msl3AB3.tmp
2009/01/06 09:12p 0 BUILTIN\Administrators msl3AB4.tmp
2009/01/06 09:12p 0 BUILTIN\Administrators msl3AB6.tmp
2009/01/06 09:12p 0 BUILTIN\Administrators msl3AB8.tmp
2009/01/06 09:14p 0 BUILTIN\Administrators msl3ABB.tmp
2009/01/06 11:23p 0 BUILTIN\Administrators msl3ABF.tmp
2009/01/07 02:42p 0 BUILTIN\Administrators msl3B83.tmp
2009/01/07 02:43p 0 BUILTIN\Administrators msl3B86.tmp
2009/01/07 02:44p 0 BUILTIN\Administrators msl3B87.tmp
2009/01/07 02:48p 0 BUILTIN\Administrators msl3B8E.tmp
2009/01/07 03:20p 0 BUILTIN\Administrators msl3B91.tmp
Ready
ssh2: AES-256-C 25, 1 26 Rows, 93 Cols VT100
CAP NUM


192.168.1.68 - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.68
2008/09/11 05:55p 16,384 BUILTIN\Administrators odbc32gt.dll
2008/09/11 05:55p 32,768 BUILTIN\Administrators odbcad32.exe
2008/09/11 05:55p 32,768 BUILTIN\Administrators odbccp32.cpl
2008/09/11 05:55p 102,400
2008/09/11 05:55p 61,440
2008/09/11 05:55p 139,264
2008/09/11 05:55p 26,224
2008/09/11 05:55p 20,480
2008/09/11 05:55p 4,656
2008/09/11 05:55p 36,864
2008/09/11 05:55p 2,151
2008/09/11 05:55p 2,233
2008/09/11 05:55p 1,049,088 BUILTIN\Administrators msxml3.dll
2008/09/11 05:55p 44,032 BUILTIN\Administrators msxml3r.dll
2008/09/11 05:56p 73,728 BUILTIN\Administrators cliconfg.dll
2008/09/11 05:56p 60,546 BUILTIN\Administrators cliconf.chm
2008/09/11 05:56p 20,480 BUILTIN\Administrators cliconfg.exe
2008/09/11 05:56p 24,576 BUILTIN\Administrators cliconfg.rll
2008/09/11 05:56p 106,496 BUILTIN\Administrators dbnetlib.dll
2008/09/11 05:56p 28,672 BUILTIN\Administrators dbnmpntw.dll
2008/09/11 05:56p 956,990 BUILTIN\Administrators instcat.sql
2008/09/11 05:56p 28,672 BUILTIN\Administrators dbmsgnet.dll
2008/09/11 05:56p 24,576 BUILTIN\Administrators dbmsrpcn.dll
2008/09/11 05:56p 24,576 BUILTIN\Administrators odbcbcp.dll
2008/09/11 05:56p 52,378 BUILTIN\Administrators sqlsodbc.chm
2008/09/11 05:56p 421,888 BUILTIN\Administrators sqlsrv32.dll
2008/09/11 05:56p 90,112 BUILTIN\Administrators sqlsrv32.rll
2008/09/11 05:56p 147,456 BUILTIN\Administrators msdart.dll
2008/09/11 05:56p 118,784 BUILTIN\Administrators msdadiag.dll
2008/09/11 05:56p 33,340 BUILTIN\Administrators dbmsglgc.dll
2008/09/11 06:03p 16,384 BUILTIN\Administrators Perflib_Perfdata_49c.dat
2008/09/11 06:04p 16,384 BUILTIN\Administrators Perflib_Perfdata_6f0.dat
2008/10/21 10:51a 13,072 BUILTIN\Administrators PJLMON.DLL
2008/11/19 09:24a 108,336 BUILTIN\Administrators MSWINSCK.OCX
2008/11/19 09:25a 19 BUILTIN\Administrators flag
2008/12/16 11:07a 45,056 BUILTIN\Administrators Install.exe
2008/12/16 11:07a 36,864 BUILTIN\Administrators win2k.dll
2008/12/16 11:07a 9,216 BUILTIN\Administrators win2k.sys
2008/12/29 11:03a 16,384 BUILTIN\Administrators Perflib_Perfdata_4b4.dat
erfdata_7e0.dat
2009/01/07 03:50p 45,056 BUILTIN\Administrators is.exe
目錄： c:\WINNT\system32\BITS
2005/08/22 05:56p 360,960 BUILTIN\Administrators qmgr.dll
2005/08/22 05:57p <DIR> BUILTIN\Administrators ..
找到 c:\winnt\system32下有怪檔案 is.exe
並注意日期為2009/01/07 03:50p
Ready
ssh2: AES-256-C 1, 1 48 Rows, 125 Cols VT100

# 使用找到的時間點再次找尋

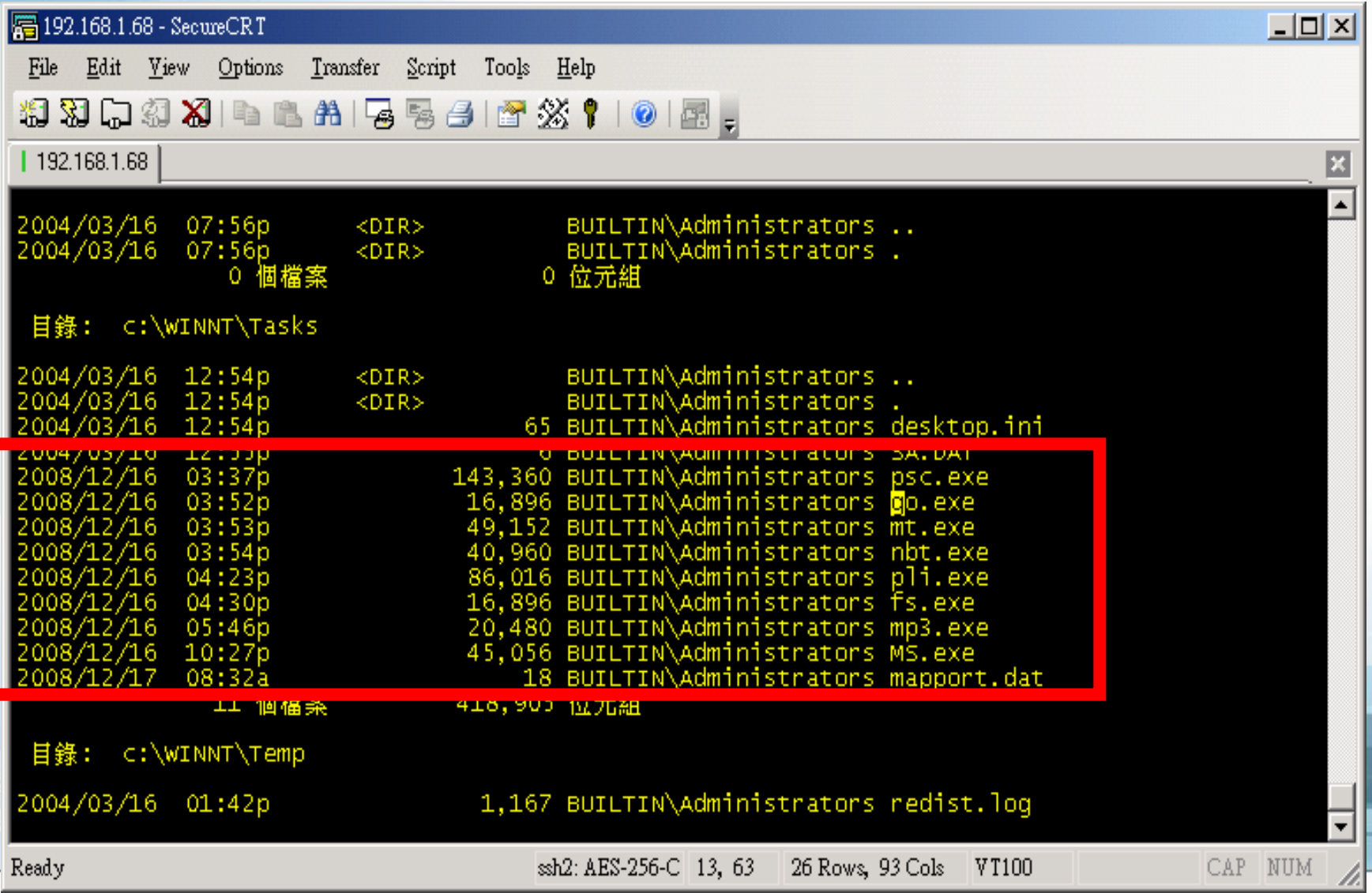


# 看看這些程式都在哪個目錄下




C:\winnt\debug目錄下有很多怪檔案

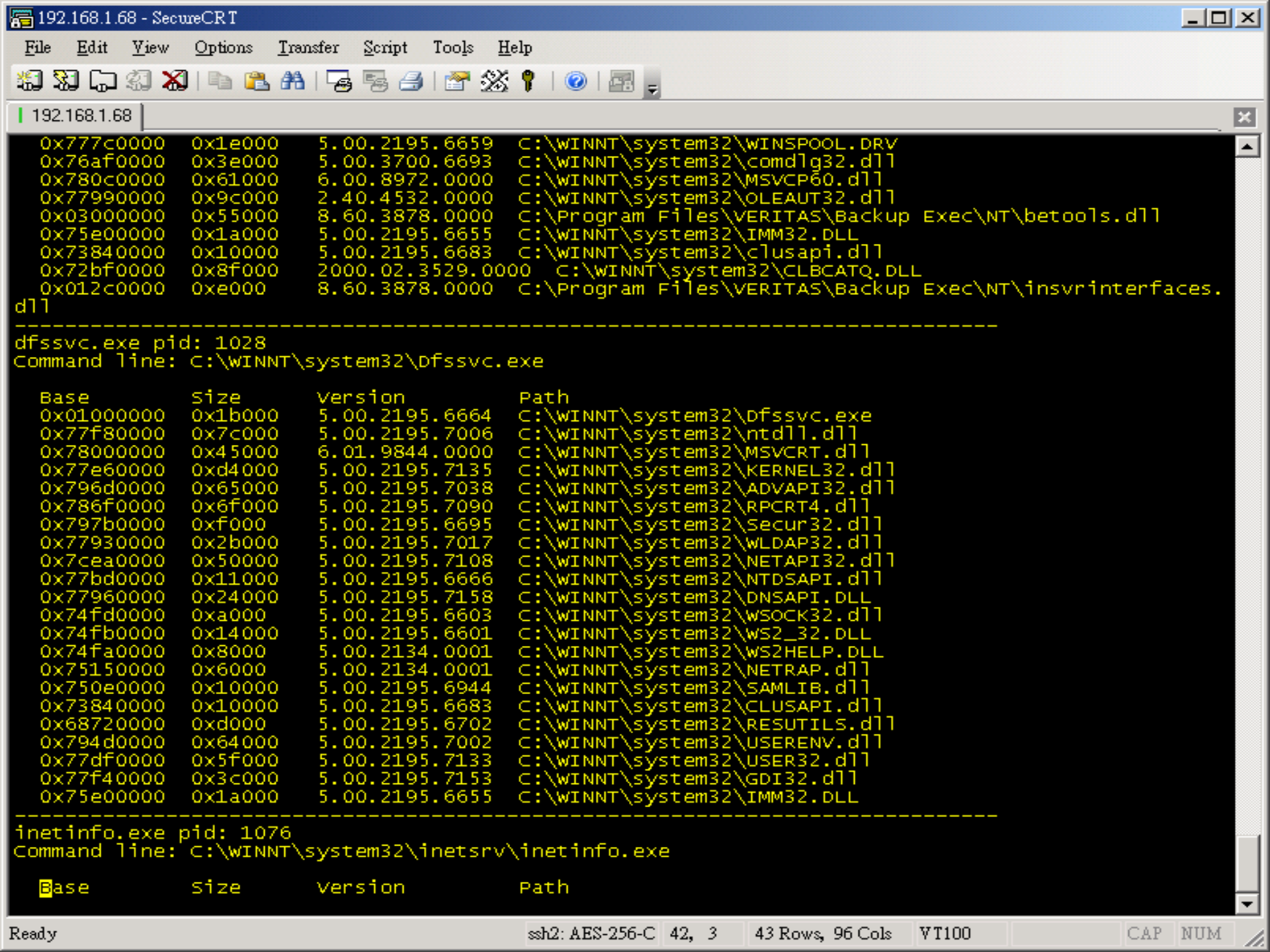
# 再次使用時間點找尋

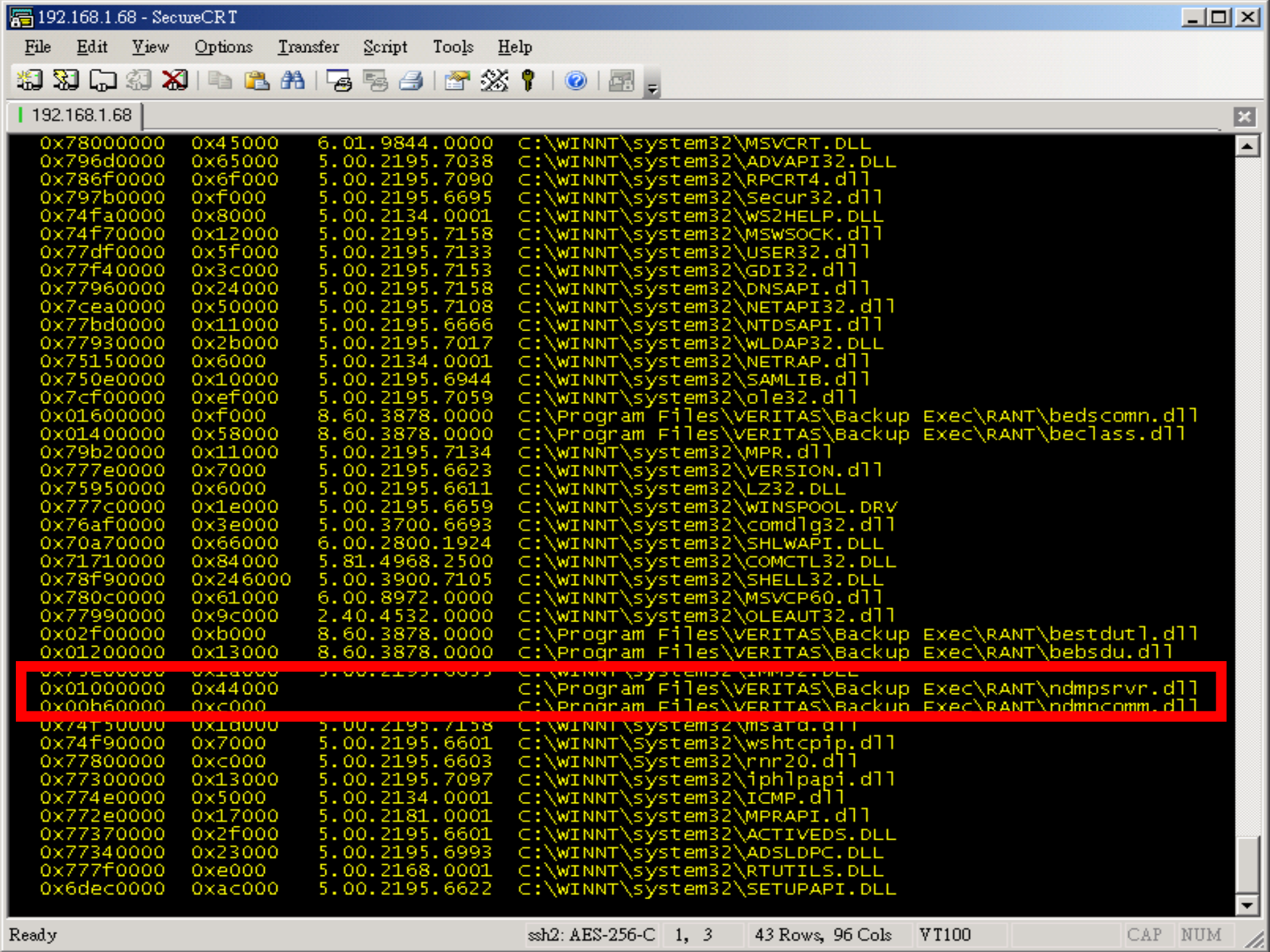

192.168.1.68 - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.68
2004/03/16 07:56p <DIR> BUILTIN\Administrators ..
2004/03/16 07:56p <DIR> BUILTIN\Administrators .
0 個檔案 0 位元組
目錄: c:\WINNT\Tasks
2004/03/16 12:54p <DIR> BUILTIN\Administrators ..
2004/03/16 12:54p <DIR> BUILTIN\Administrators .
2004/03/16 12:54p 65 BUILTIN\Administrators desktop.ini
2008/12/16 03:37p 143,360 BUILTIN\Administrators psc.exe
2008/12/16 03:52p 16,896 BUILTIN\Administrators qo.exe
2008/12/16 03:53p 49,152 BUILTIN\Administrators mt.exe
2008/12/16 03:54p 40,960 BUILTIN\Administrators nbt.exe
2008/12/16 04:23p 86,016 BUILTIN\Administrators pli.exe
2008/12/16 04:30p 16,896 BUILTIN\Administrators fs.exe
2008/12/16 05:46p 20,480 BUILTIN\Administrators mp3.exe
2008/12/16 10:27p 45,056 BUILTIN\Administrators MS.exe
2008/12/17 08:32a 18 BUILTIN\Administrators mapport.dat
目錄: c:\WINNT\Temp
2004/03/16 01:42p 1,167 BUILTIN\Administrators redist.log
Ready ssh2: AES-256-C 13, 63 26 Rows, 93 Cols VT100 CAP NUM

# Process .listdlls.log

- 檔案內容
  - 執行程式與配屬的DLL列表
- 查看重點
  - 沒有見過的DLL
  - 空白的版本資訊
  - 比對之前的資料

DLL Injection 攻擊
Listdlls.exe


192.168.1.68 - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.68
0x777c0000 0x1e000 5.00.2195.6659 C:\WINNT\system32\WINSPOOL.DRV
0x76af0000 0x3e000 5.00.3700.6693 C:\WINNT\system32\comdlg32.dll
0x780c0000 0x61000 6.00.8972.0000 C:\WINNT\system32\MSVCP60.dll
0x77990000 0x9c000 2.40.4532.0000 C:\WINNT\system32\OLEAUT32.dll
0x03000000 0x55000 8.60.3878.0000 C:\Program Files\VERITAS\Backup Exec\NT\betools.dll
0x75e00000 0x1a000 5.00.2195.6655 C:\WINNT\system32\IMM32.DLL
0x73840000 0x10000 5.00.2195.6683 C:\WINNT\system32\clusapi.dll
0x72bf0000 0x8f000 2000.02.3529.0000 C:\WINNT\system32\CLBCATQ.DLL
0x012c0000 0xe000 8.60.3878.0000 C:\Program Files\VERITAS\Backup Exec\NT\insvrinterfaces.dll
dfssvc.exe pid: 1028
Command line: C:\WINNT\system32\Dfssvc.exe
Base Size Version Path
0x01000000 0x1b000 5.00.2195.6664 C:\WINNT\system32\Dfssvc.exe
0x77f80000 0x7c000 5.00.2195.7006 C:\WINNT\system32\ntdll.dll
0x78000000 0x45000 6.01.9844.0000 C:\WINNT\system32\MSVCRT.dll
0x77e60000 0xd4000 5.00.2195.7135 C:\WINNT\system32\KERNEL32.dll
0x796d0000 0x65000 5.00.2195.7038 C:\WINNT\system32\ADVAPI32.dll
0x786f0000 0x6f000 5.00.2195.7090 C:\WINNT\system32\RPCRT4.dll
0x797b0000 0xf000 5.00.2195.6695 C:\WINNT\system32\Secur32.dll
0x77930000 0x2b000 5.00.2195.7017 C:\WINNT\system32\WLDAP32.dll
0x7cea0000 0x50000 5.00.2195.7108 C:\WINNT\system32\NETAPI32.dll
0x77bd0000 0x11000 5.00.2195.6666 C:\WINNT\system32\NTDSAPI.dll
0x77960000 0x24000 5.00.2195.7158 C:\WINNT\system32\DNSAPI.DLL
0x74fd0000 0xa000 5.00.2195.6603 C:\WINNT\system32\WSOCK32.dll
0x74fb0000 0x14000 5.00.2195.6601 C:\WINNT\system32\WS2_32.DLL
0x74fa0000 0x8000 5.00.2134.0001 C:\WINNT\system32\WS2HELP.DLL
0x75150000 0x6000 5.00.2134.0001 C:\WINNT\system32\NETRAP.dll
0x750e0000 0x10000 5.00.2195.6944 C:\WINNT\system32\SAMLIB.dll
0x73840000 0x10000 5.00.2195.6683 C:\WINNT\system32\CLUSAPI.dll
0x68720000 0xd000 5.00.2195.6702 C:\WINNT\system32\RESUTILS.dll
0x794d0000 0x64000 5.00.2195.7002 C:\WINNT\system32\USERENV.dll
0x77df0000 0x5f000 5.00.2195.7133 C:\WINNT\system32\USER32.dll
0x77f40000 0x3c000 5.00.2195.7153 C:\WINNT\system32\GDI32.dll
0x75e00000 0x1a000 5.00.2195.6655 C:\WINNT\system32\IMM32.DLL
inetinfo.exe pid: 1076
Command line: C:\WINNT\system32\inetsrv\inetinfo.exe
Base Size Version Path
Ready
ssh2: AES-256-C
42, 3
43 Rows, 96 Cols
VT100
CAP
NUM


192.168.1.68 - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.1.68
0x78000000 0x45000 6.01.9844.0000 C:\WINNT\system32\MSVCRT.DLL
0x796d0000 0x65000 5.00.2195.7038 C:\WINNT\system32\ADVAPI32.DLL
0x786f0000 0x6f000 5.00.2195.7090 C:\WINNT\system32\RPCRT4.dll
0x797b0000 0xf000 5.00.2195.6695 C:\WINNT\system32\Secur32.dll
0x74fa0000 0x8000 5.00.2134.0001 C:\WINNT\system32\WS2HELP.DLL
0x74f70000 0x12000 5.00.2195.7158 C:\WINNT\system32\MSWSOCK.dll
0x77df0000 0x5f000 5.00.2195.7133 C:\WINNT\system32\USER32.dll
0x77f40000 0x3c000 5.00.2195.7153 C:\WINNT\system32\GDI32.dll
0x77960000 0x24000 5.00.2195.7158 C:\WINNT\system32\DNSAPI.dll
0x7cea0000 0x50000 5.00.2195.7108 C:\WINNT\system32\NETAPI32.dll
0x77bd0000 0x11000 5.00.2195.6666 C:\WINNT\system32\NTDSAPI.dll
0x77930000 0x2b000 5.00.2195.7017 C:\WINNT\system32\WLDAP32.DLL
0x75150000 0x6000 5.00.2134.0001 C:\WINNT\system32\NETRAP.dll
0x750e0000 0x10000 5.00.2195.6944 C:\WINNT\system32\SAMLIB.dll
0x7cf00000 0xef000 5.00.2195.7059 C:\WINNT\system32\ole32.dll
0x01600000 0xf000 8.60.3878.0000 C:\Program Files\VERITAS\Backup Exec\RANT\bedscomn.dll
0x01400000 0x58000 8.60.3878.0000 C:\Program Files\VERITAS\Backup Exec\RANT\beclass.dll
0x79b20000 0x11000 5.00.2195.7134 C:\WINNT\system32\MPR.dll
0x777e0000 0x7000 5.00.2195.6623 C:\WINNT\system32\VERSION.dll
0x75950000 0x6000 5.00.2195.6611 C:\WINNT\system32\LZ32.DLL
0x777c0000 0x1e000 5.00.2195.6659 C:\WINNT\system32\WINSPOOL.DRV
0x76af0000 0x3e000 5.00.3700.6693 C:\WINNT\system32\comdlg32.dll
0x70a70000 0x66000 6.00.2800.1924 C:\WINNT\system32\SHLWAPI.DLL
0x71710000 0x84000 5.81.4968.2500 C:\WINNT\system32\COMCTL32.DLL
0x78f90000 0x246000 5.00.3900.7105 C:\WINNT\system32\SHELL32.DLL
0x780c0000 0x61000 6.00.8972.0000 C:\WINNT\system32\MSVCP60.dll
0x77990000 0x9c000 2.40.4532.0000 C:\WINNT\system32\OLEAUT32.dll
0x02f00000 0xb000 8.60.3878.0000 C:\Program Files\VERITAS\Backup Exec\RANT\bestdutl.dll
0x01200000 0x13000 8.60.3878.0000 C:\Program Files\VERITAS\Backup Exec\RANT\bebsdu.dll
0x01000000 0x44000 C:\Program Files\VERITAS\Backup Exec\RANT\ndmpsrvr.dll
0x74f90000 0x7000 5.00.2195.6601 C:\WINNT\System32\wshtcpip.dll
0x77800000 0xc000 5.00.2195.6603 C:\WINNT\System32\rnr20.dll
0x77300000 0x13000 5.00.2195.7097 C:\WINNT\system32\iphlpapi.dll
0x774e0000 0x5000 5.00.2134.0001 C:\WINNT\system32\ICMP.dll
0x772e0000 0x17000 5.00.2181.0001 C:\WINNT\system32\MPRAPI.dll
0x77370000 0x2f000 5.00.2195.6601 C:\WINNT\system32\ACTIVEDS.DLL
0x77340000 0x23000 5.00.2195.6993 C:\WINNT\system32\ADSLDPC.DLL
0x777f0000 0xe000 5.00.2168.0001 C:\WINNT\system32\RTUTILS.DLL
0x6dec0000 0xac000 5.00.2195.6622 C:\WINNT\system32\SETUPAPI.DLL
Ready
ssh2: AES-256-C 1, 3 43 Rows, 96 Cols VT100
CAP NUM

# 程式碼簽章

- 簽章是否沒過
  - 懷疑是惡意程式
- 工具
  - Sigcheck.exe
  - Sigverf.exe
- 用法
  - Sigcheck –a *.* (找出簽章資訊)
  - Sigcheck –u –a *.exe (找出簽章沒過的資訊)
  - Sigcheck –u –a –r c:\ (找出整個硬碟簽章沒過的資訊)

# 記憶體採樣

# 記憶體採樣與分析

- Memory dump (記憶體傾印)
  - Pmdump
  - Win32dd
- Memory 分析
  - volatility

# Volatility功能

- The Volatility Framework currently provides the following extraction capabilities for memory samples
- Image date and time
- Running processes
- Open network sockets
- Open network connections
- DLLs loaded for each process
- Open files for each process
- Open registry handles for each process
- A process' addressable memory
- OS kernel modules
- Mapping physical offsets to virtual addresses (strings to process)
- Virtual Address Descriptor information
- Scanning examples: processes, threads, sockets, connections,modules
- Extract executables from memory samples
- Transparently supports a variety of sample formats (ie, Crash dump, Hibernation, DD)
- Automated conversion between formats

https://www.volatilesystems.com/default/volatility

# 適用系統

- 32bit Windows XP Service Pack 2 and 3
- 32bit Windows 2003 Server Service Pack 0, 1, 2
- 32bit Windows Vista Service Pack 0, 1, 2
- 32bit Windows 2008 Server Service Pack 1, 2 (there is no SP0)
- 32bit Windows 7 Service Pack 0, 1

# 範例下載

- https://code.google.com/p/volatility/wiki/FAQ#Are_there_any_public_memory_samples_available_that_I_can_use_for

Images from The Malware Analyst's Cookbook

| Description | url | OS |
|---|---|---|
| be2.vmem.zip | be2.vmem.zip | XP SP2 |
| coreflood.vmem.zip | coreflood.vmem.zip | XP SP2 |
| laqma.vmem.zip | laqma.vmem.zip | XP SP2 |
| prolaco.vmem.zip | prolaco.vmem.zip | XP SP2 |
| sality.vmem.zip | sality.vmem.zip | XP SP2 |
| silentbanker.vmem.zip | silentbanker.vmem.zip | XP SP2 |
| tigger.vmem.zip | tigger.vmem.zip | XP SP2 |
| zeus.vmem.zip | zeus.vmem.zip | XP SP2 |
| spyeye.vmem.zip | spyeye.vmem.zip | XP SP2 |

Other Images

| Description | url | OS |
|---|---|---|
| Stuxnet image | stuxnet.vmem.zip | XP SP3 |
| NIST | http://www.cfreds.nist.gov/mem/memory-images.rar | XP SP2 |
| Hogfly's malware memory samples | http://cid-5694a755c9c6a175.skydrive.live.com/browse.aspx/Public | ? |
| Moyix's Fuzzy Hidden Process Sample | http://amnesia.gtisc.gatech.edu/~moyix/ds_fuzz_hidden_proc.img.bz2 | XP SP3 |
| Honeynet Banking Troubles Image | https://www.honeynet.org/challenges/2010_3_banking_troubles | XP SP2 |
| NPS 2009-M57 | http://domex.nps.edu/corp/scenarios/2009-m57/ram/ | Various XP / Vista |
| Dougee's comparison samples | before and after infection | XP |
| Shylock Sample | Shylock vmem | XP |

# 惡意程式分析

# 惡意程式分析

- 動態分析(Dynamic Analysis)
  - 觀察惡意程式之活動
- 靜態分析(Static Analysis)
  - 了解惡意程式之編碼內容
- 沙盒分析
- 線上沙盒分析

# 動態分析

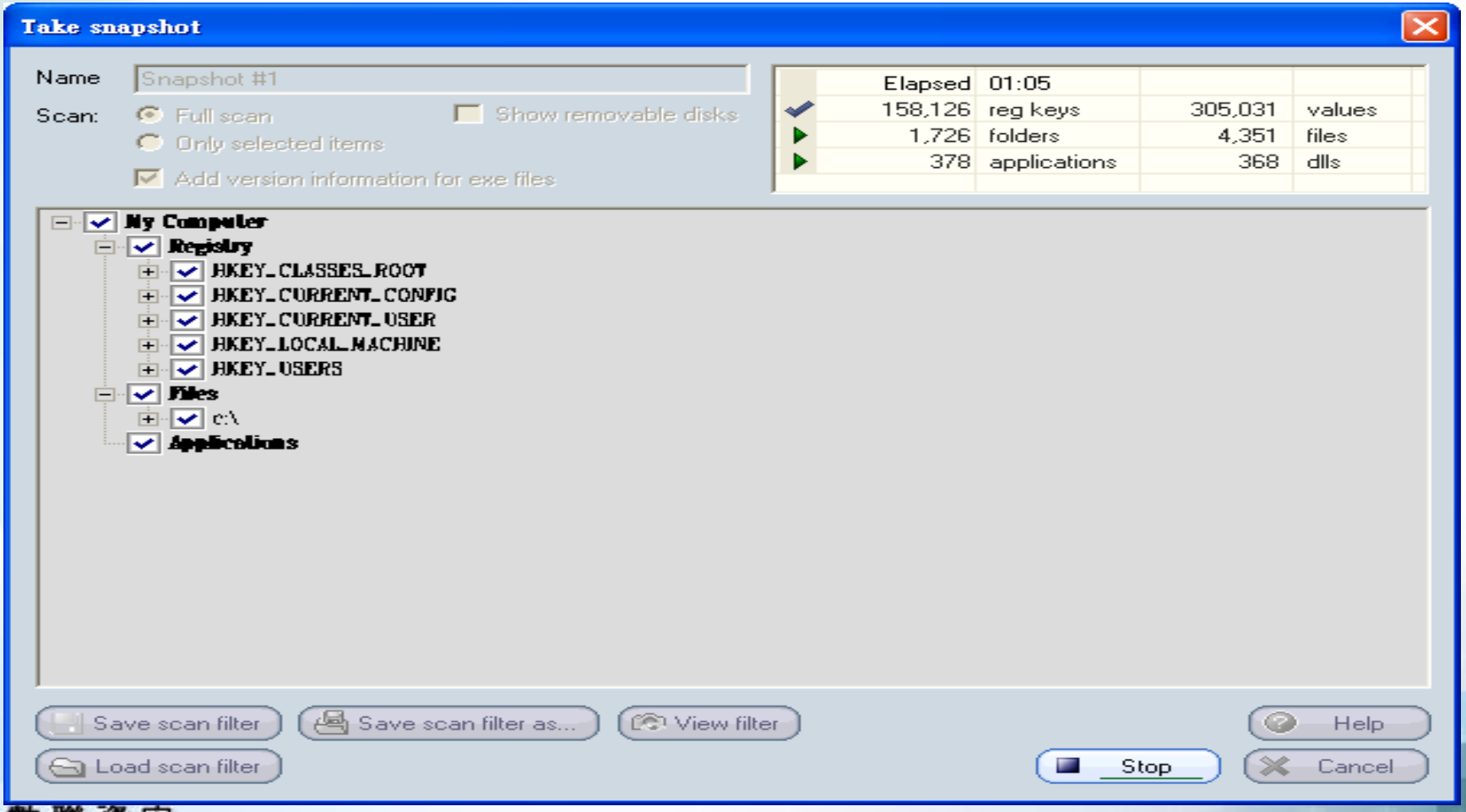
- 使用Debug工具
  - Windbg
  - Ollydbg
  - immunity debugger
  - Gdb(unix)
- 使用沙盒
  - Vmware+工具
  - VirtualBox +工具

# 靜態分析

- 不真正執行起來, 避免中毒
- 分析惡意程式的結構, 繪出流程圖, 建構出惡意程式的行為
- 工具
  - IDA Pro
  - Dumpbin
  - 其它自製工具

# 沙盒分析

# 使用SysTracer+Vmware
# 作沙盒分析



# 使用Procmon+Vmware作沙盒分析

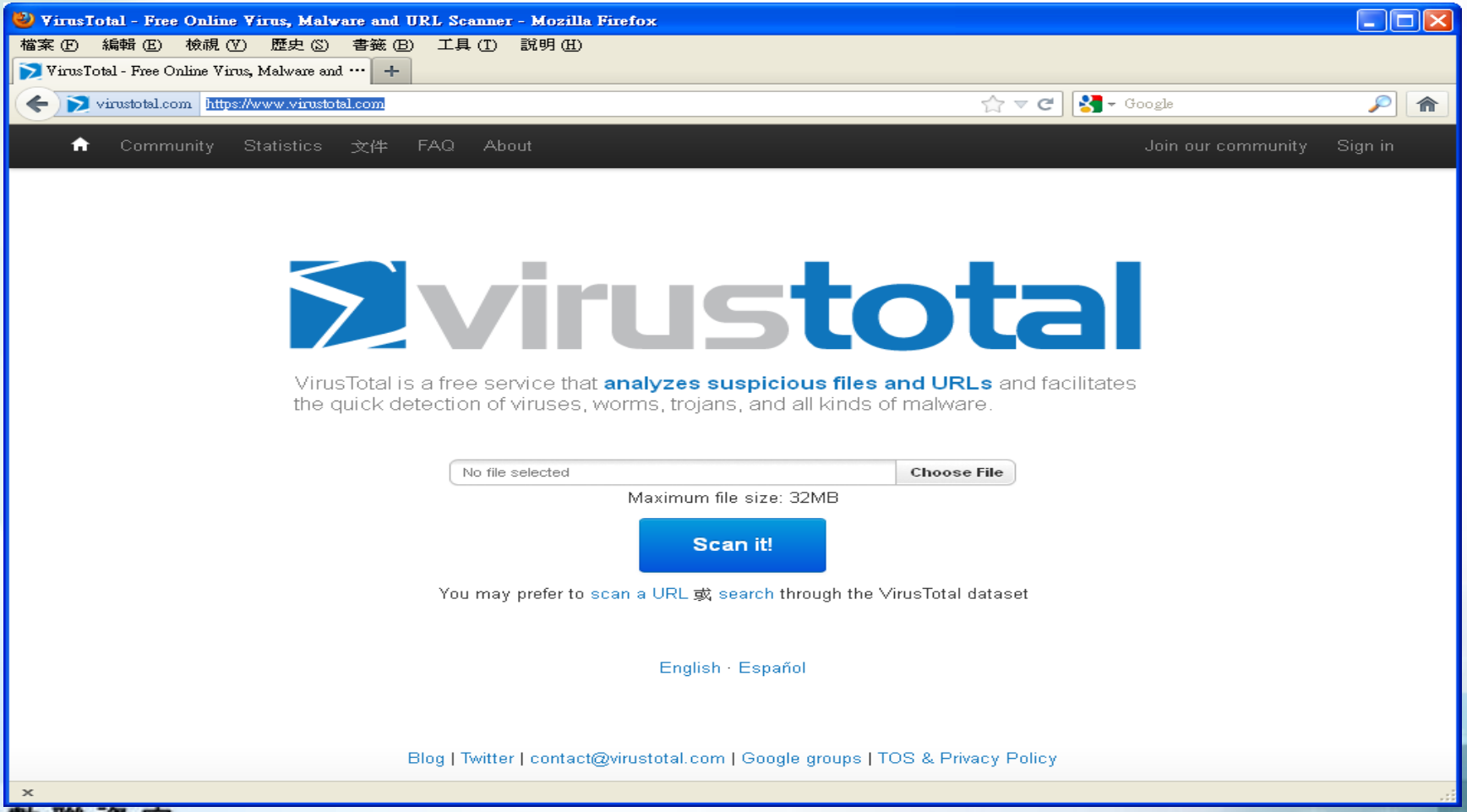
- Procmon 監控系統的
  - 程式執行
  - 檔案存取
  - Registry更動
- Procmon可以設定開機補捉
  - 可以找出部份 rootkit
  - 可以追蹤 MBR型的後門

# 線上沙盒分析

# 線上沙盒分析: Virustotal

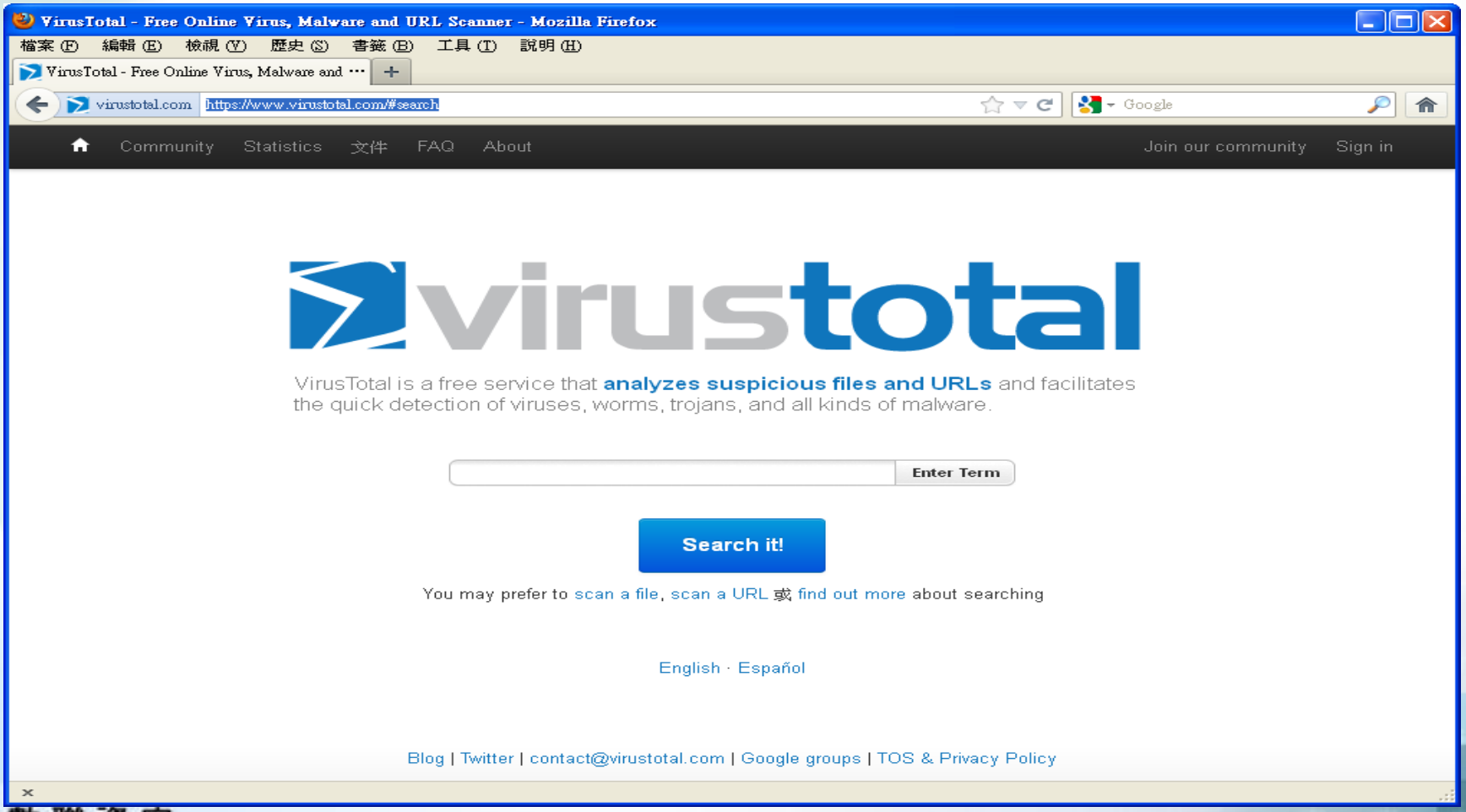
- 全世界最大的惡意程式掃毒網站
- 超過40種以上的防毒
- 提供多種上傳模式
  - 檔案上傳
  - 檢查碼比對(md5, sha,…)

# Virustotal: 檔案上傳



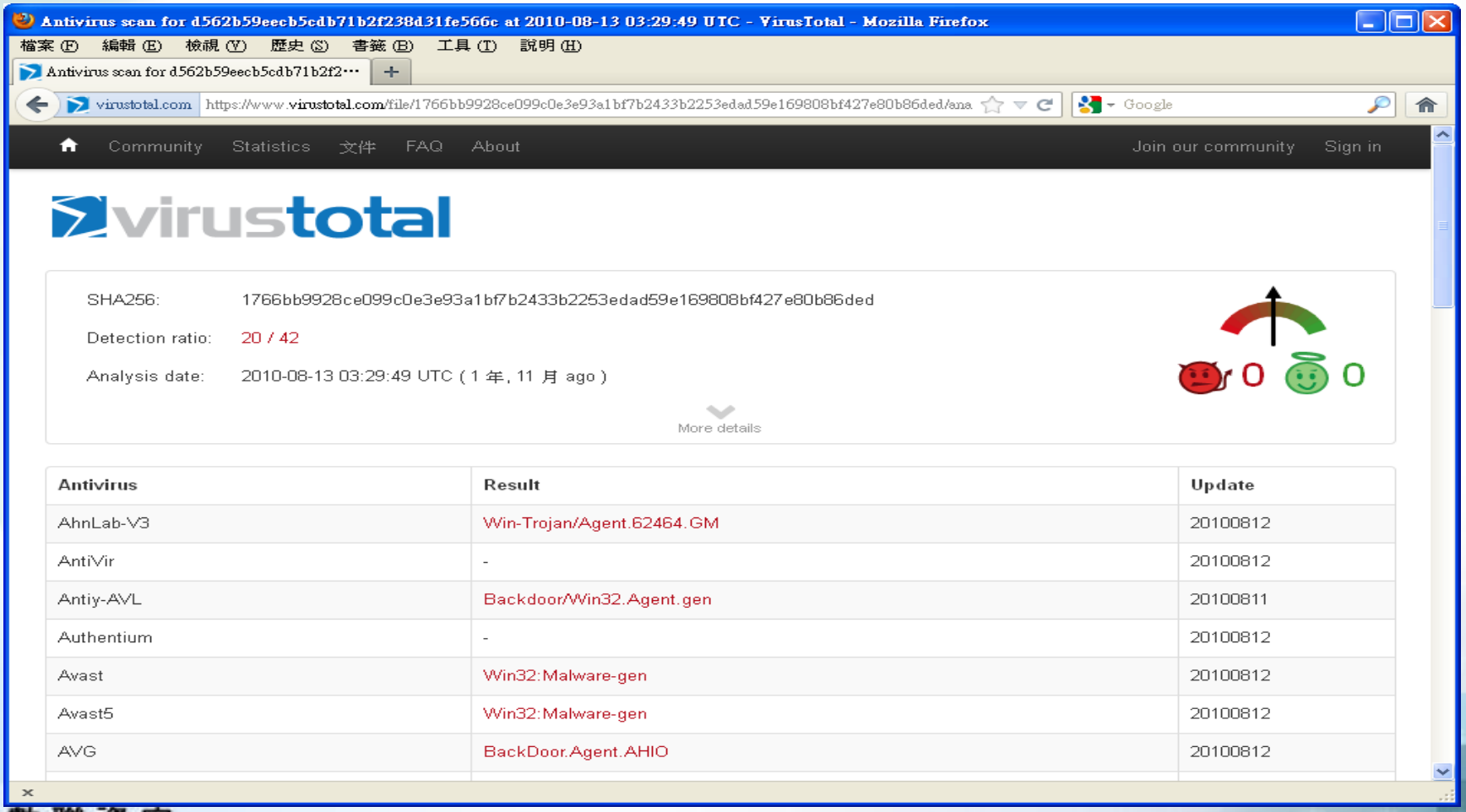

https://www.virustotal.com/

# Virustotal:檢查碼比對



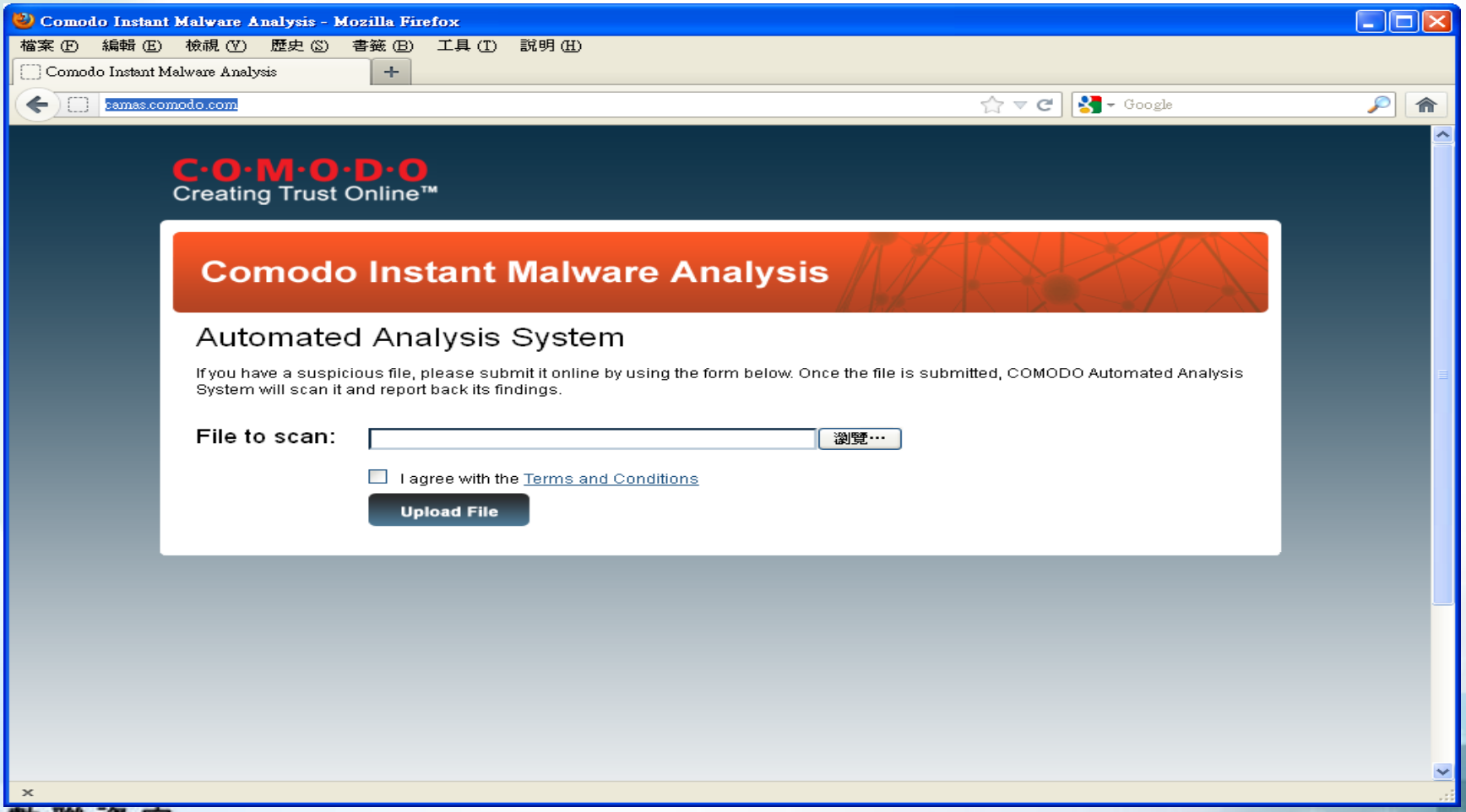

https://www.virustotal.com/#search

# Virustotal:檢查碼比對



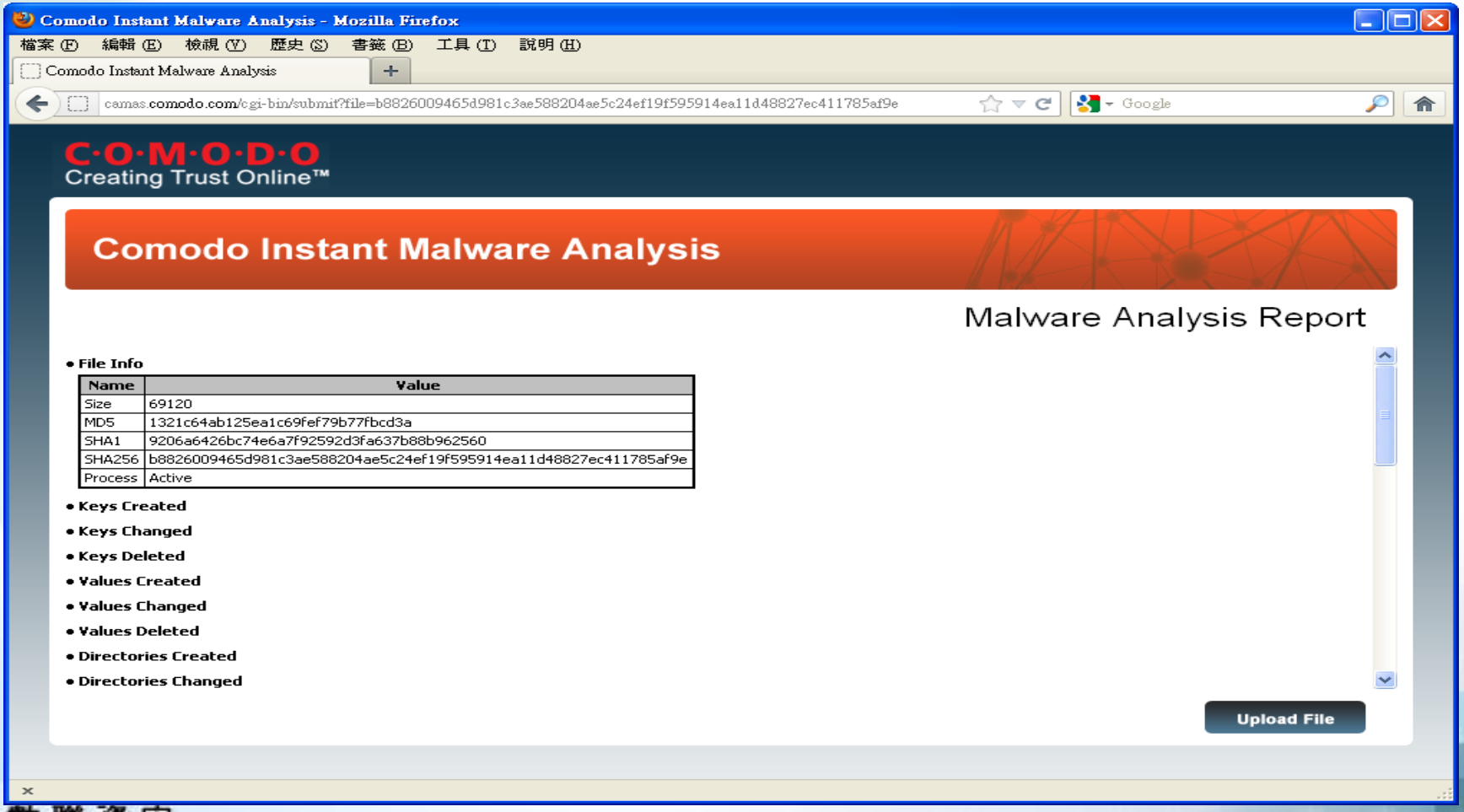

MD5: d562b59eecb5cdb71b2f238d31fe566c

# 線上沙盒分析: comodo

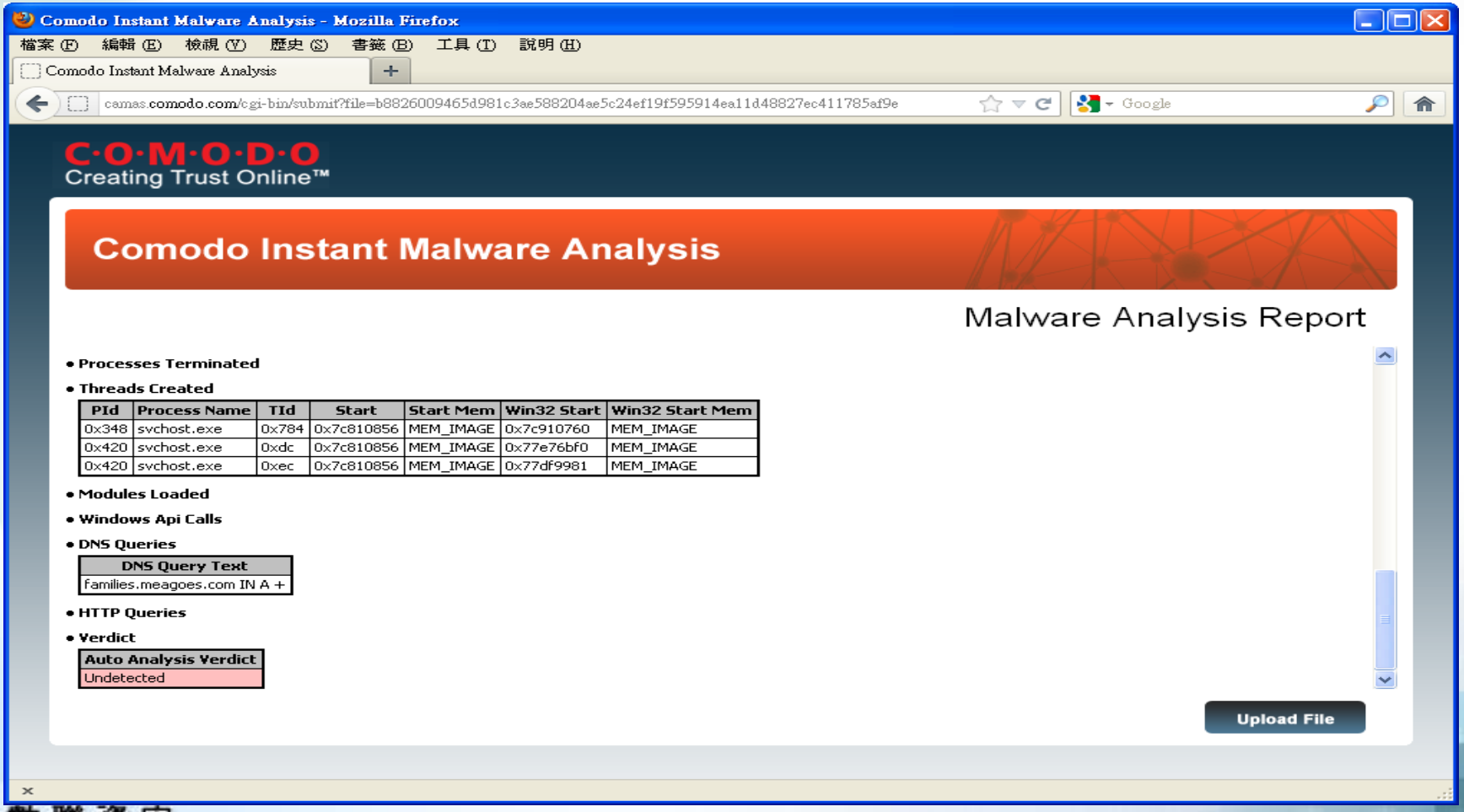



http://camas.comodo.com/

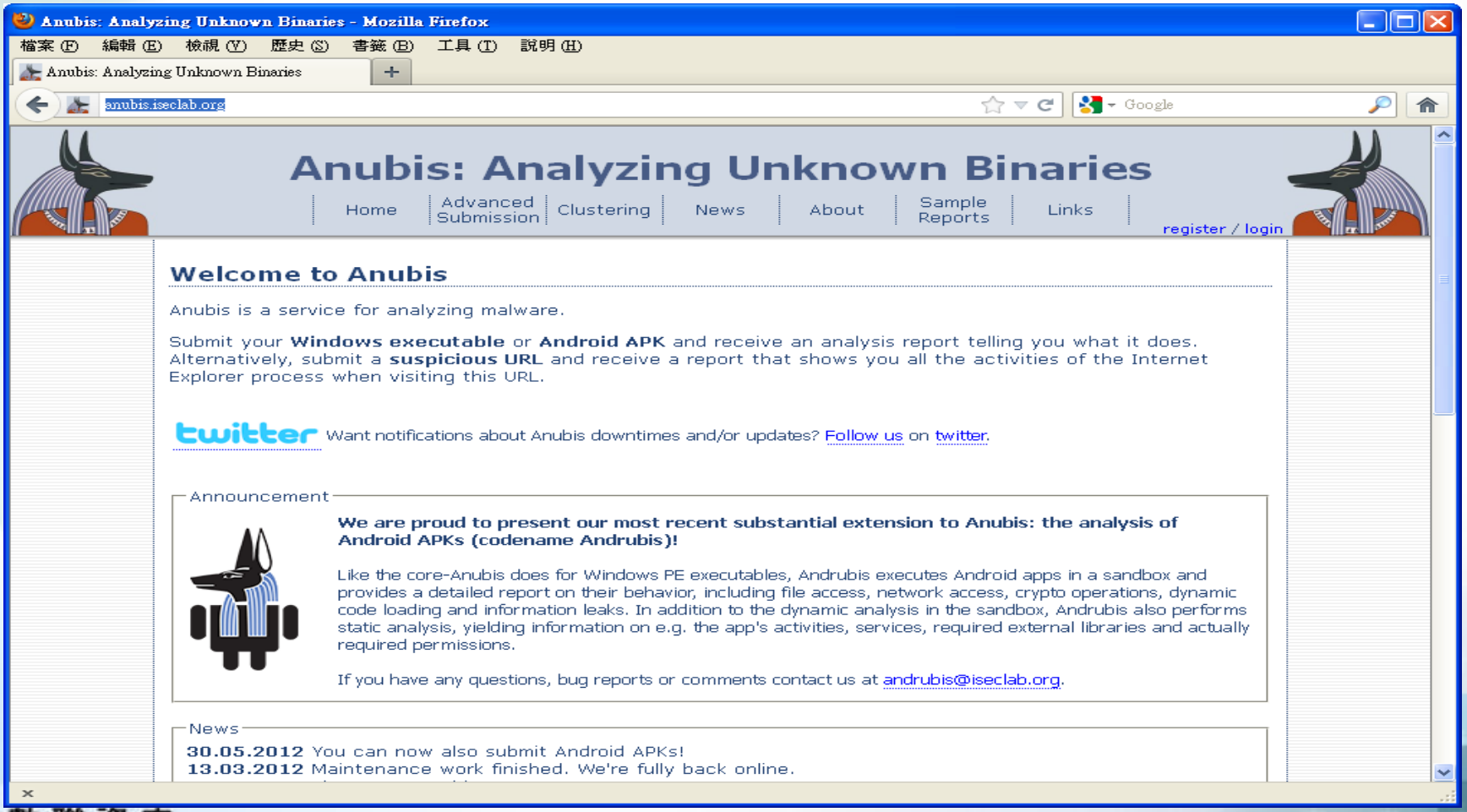
# 線上沙盒分析: comodo



# 線上沙盒分析: comodo

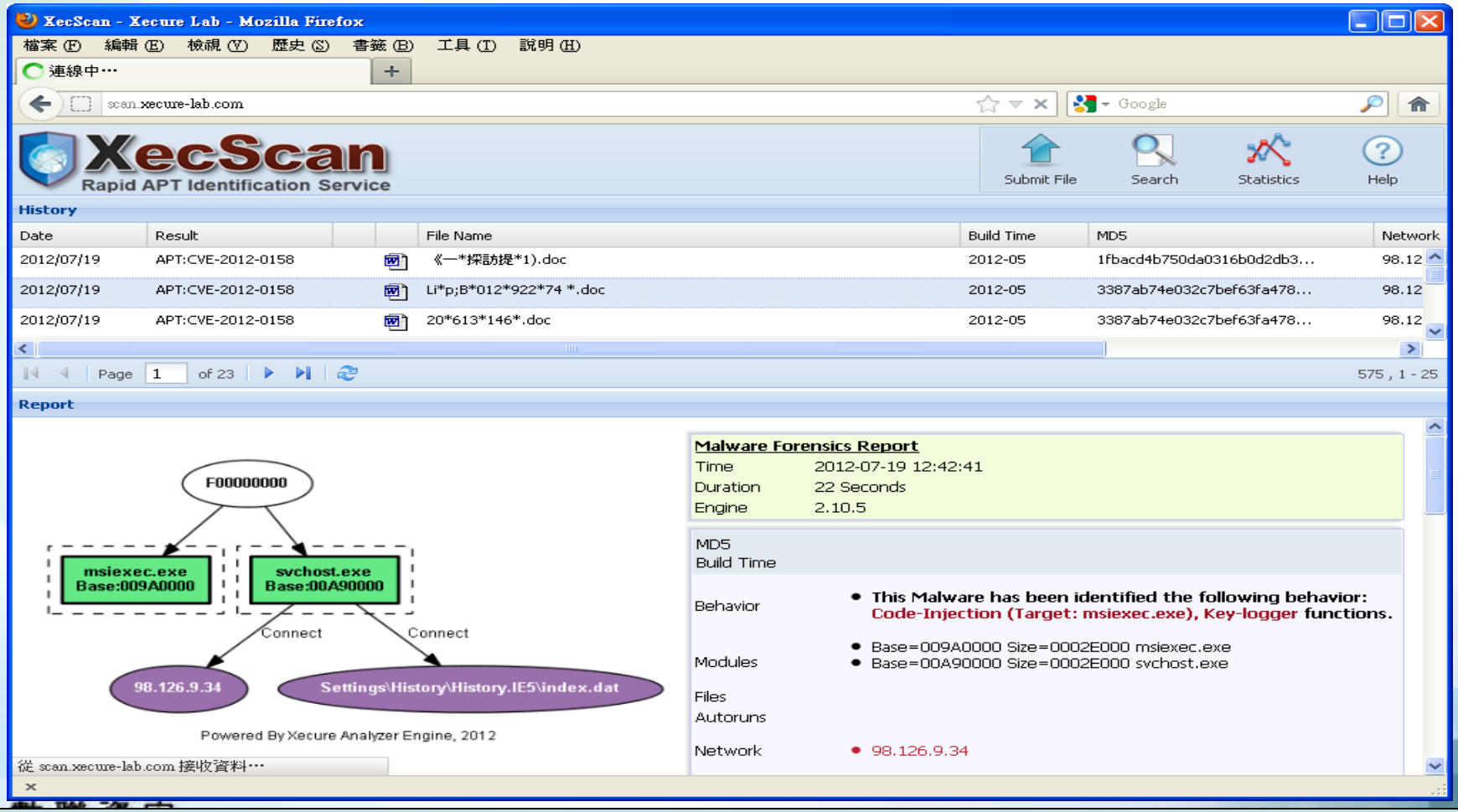


# 線上沙盒分析: anubis




http://anubis.iseclab.org/

# 線上沙盒文件分析




http://scan.xecure-lab.com/

# Q & A

# 附錄

# 惡意程式技術

- Automatic Execution
- Watchdog
- DLL Injection
- Layered Service Provider (LSP)
- Rootkit

# Automatic Execution

- Startup files and folders
- 登錄檔(Registry)
  - System Startup
  - Event Triggered
- 排訂的工作(Task Scheduler)

# Startup files and folders

- Win.ini
  - C:\Winnt\win.ini or C:\Windows\win.ini
- System.ini
  - C:\Winnt\system.ini or C:\Windows\System.ini
- Wininit.ini
  - C:\Winnt\Wininit.ini or C:\Windows\Wininit.ini

# Startup files and folders(cont.)

- Windows 2000
  - C:\Documents and Settings\[user]\Start Menu\Programs\StartUp
- Windows XP & 2003
  - C:\Documents and Settings\[user]\Start Menu\Programs\StartUp
- Windows Vista
  - C:\Users\[user]\Appdata\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

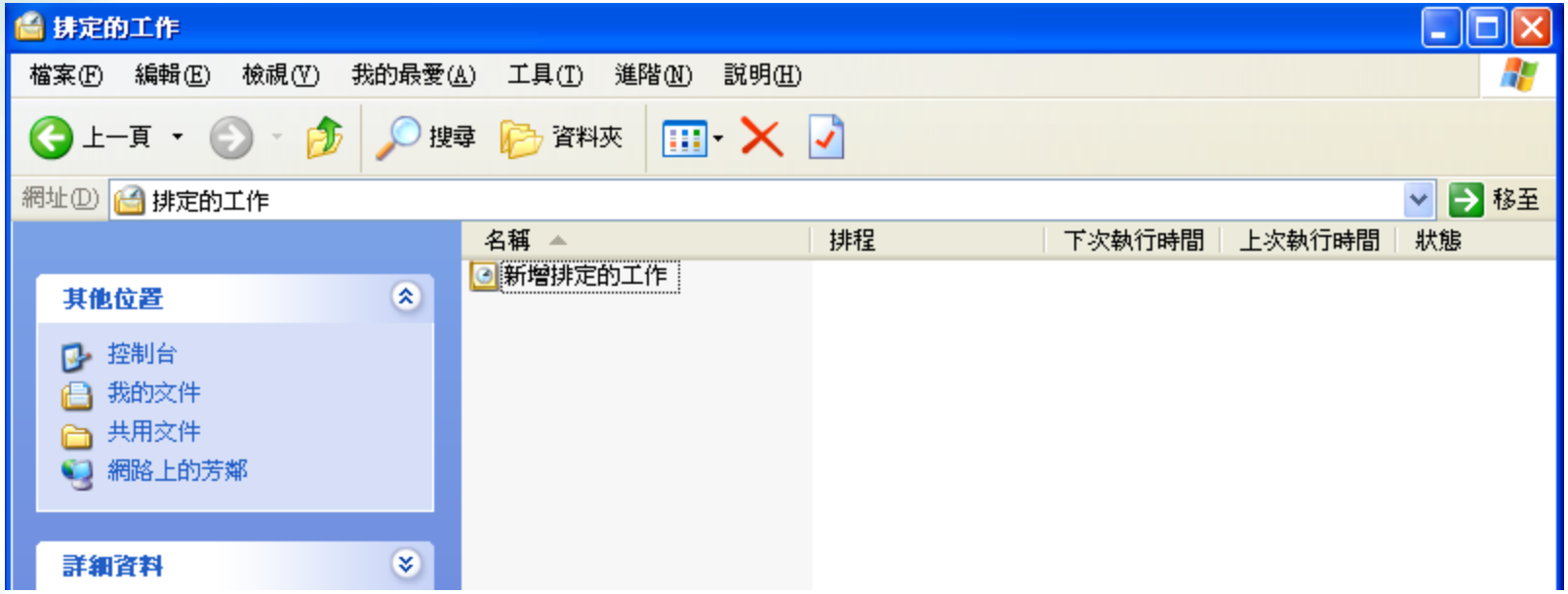
# Registry

- System Startup
  - Run Key
    - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
    - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - Service
    - HKLM\System\CurrentControlSet\Services

# Registry(cont.)

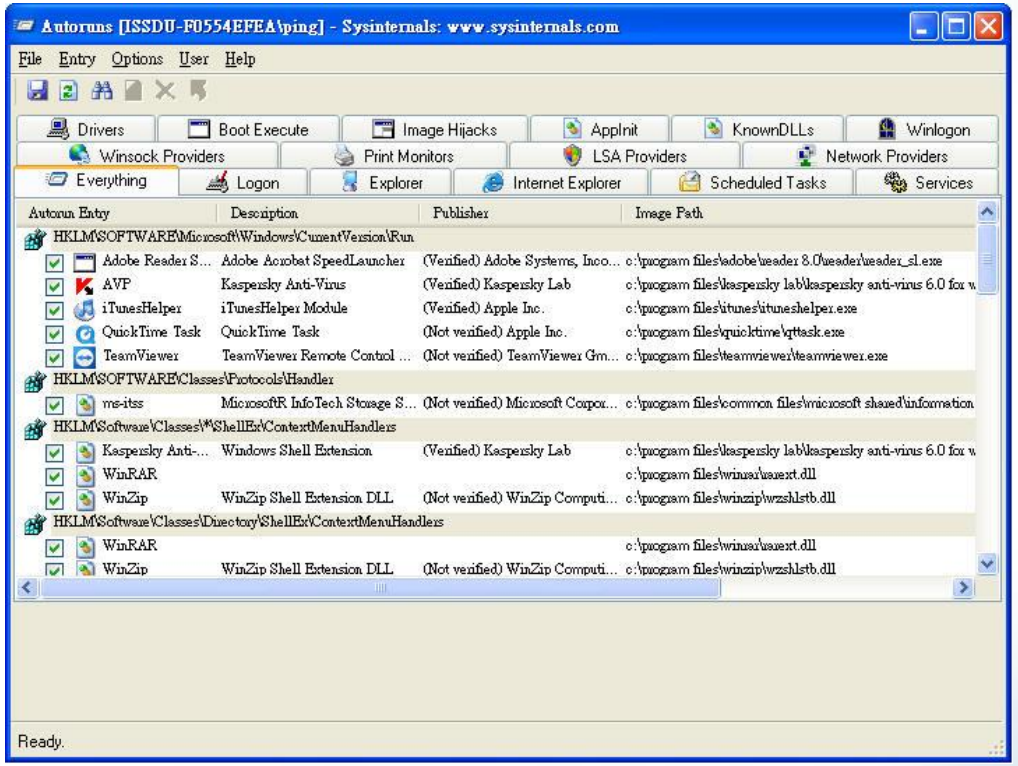
- Event Triggered
  - exe檔案執行關聯
    - HKCR\Shell\Open\Command
  - Program Loader
    - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

# Task Scheduler



# 工具：AutoRuns

- 必需檢查項目
  - AppInit
  - Winsock
  - IE
  - Boot Execute




- Reference
  - http://www.microsoft.com/technet/sysinternals/utilities/Autoruns.mspx

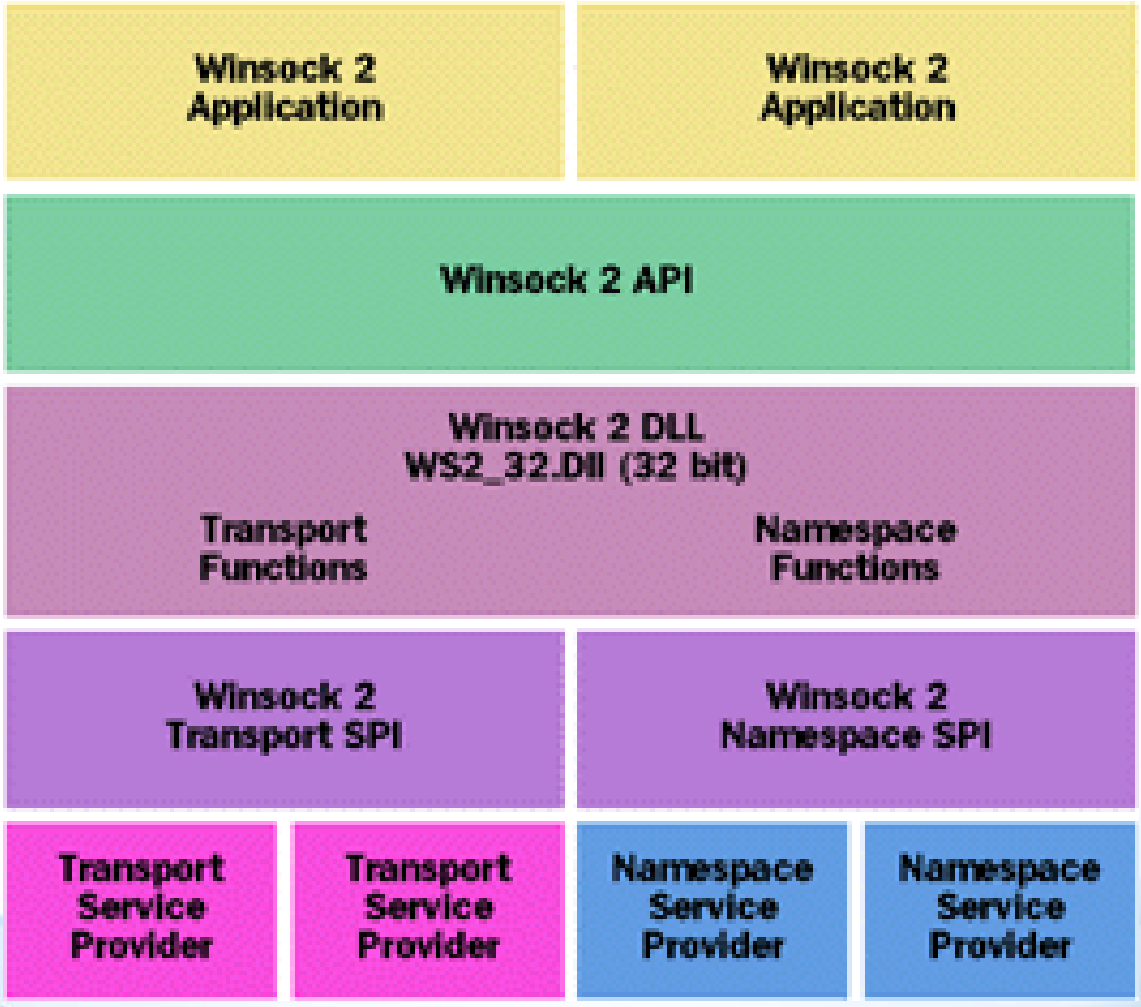
# Watchdog

- Process監控，當該process被停止時，會自動再將其執行
- 主要分為
  - Standalone process
  - Infected process
    - DLL injection
    - Remote thread execution

# DLL Injection

- Registry
- Windows Hooks
- Remote Threads
- Others

# Layer Service Provider(LSP)



# Rootkit

- Rootkit行為
  - Process hiding
  - Loaded drivers hiding
  - File/directory hiding
  - File contents cheating
  - Registry keys/contents hiding
  - Network status(opened port) hiding

# Rootkit (cont.)

- Rootkit techniques
  - User Mode
    - Replacing files
    - Hooking DLL's functions
    - Modifying DLL's functions
  - Kernel Mode
    - Hooking entries in Service Descriptor Table(SDT)/KiService Table
    - Hooking Interrupt Descriptor Table(IDT) 2Eh entry
    - Modifying Kernel Code

# Rootkit Detection

- Looking for Hooks
  - Import address Table (IAT)
  - Service Descriptor Table (SDT)
  - Interrupt Descriptor Table (IDT)
  - Raw Code change
- Detecting Behavior
  - Hidden Processes
  - Hidden Files/Directories
  - Hidden Registry