建立間諜程式執行特徵分類之研究

作者　陸軍通信電子資訊學校教官　廖秀華上尉

提　要

一、在資訊化的發展下，雖帶給了人們便利的生活，但也隱藏著許多的危機。賽門鐵克公司從「網路安全威脅報告」(Internet Security Threat Report)中指出，近幾年的網路威脅以間諜程式(高達499,811個)居多，比上一次報告成長了81%。由此可見，間諜程式(Spyware)已成為使用者中最嚴重的資安威脅之一。

二、依據微軟對間諜程式的見解，則認為它是專門在用戶不知情或未經用戶准許的情況下，收集用戶的個人資料。所以若無有效的防護間諜程式的入侵，外洩的不僅是個人的資料，更有可能是國家安全的機密資訊。

三、在國軍全力推動資訊化及面對間諜程式的挑戰下，要如何有效偵測間諜程式，是當前國軍資安政策值得深入研究的議題。

關鍵詞：間諜程式、執行特徵、分類

前　言

隨著資訊技術的蓬勃發展，電腦在現今生活中扮演著相當重要的角色。資訊化的社會一方面帶給人們相當便利的生活，但另一方面，也為資訊安全及個人隱私帶來相當多的隱憂。每當打開電腦開關，或許也同時開啟一雙監視自己隱私資訊的眼睛。[1]

1　搜狐新聞，〈警惕間諜軟件威脅國防信息安全〉，http://news.sohu.com/20080403/n256077191.shtml，西元2008年，頁1。

根據資通安全會報所提供的數據得知，超過半數以上的公、民營機構曾經遭受過間諜程式的感染，其中包含駭客攻擊、遭植入後門程式、資料遭竊或被破壞等。[2]甚至在2011年美國所發表的一份報告中指出，美國國防部電腦系統，上半年度遭到駭客攻擊的次數高達21, 124次，平均每次攻擊耗資150萬美元。這些數據均透露出目前政府機構及企業經營，正面臨到相當嚴重的難題，那就是資訊資產保存及個人資料隱私洩露的問題。[3]因資訊技術的發展，導致了社會對網路的依賴，連國防領域也不例外。而間諜程式的發展是從早期的技術炫耀，到現今以利益導向(商業、政治、軍事機密)為目的，就軍事角度來看，網路攻防技術已成為一種全新的軍事作戰手段。利用間諜程式刺探、竊取對方的國防機密，破壞對方的網路系統，一旦攻擊成功將會給對方造成不可預期的傷害，甚至導致全面崩潰的局面。另一方面隨著國軍高科技設備建置及資訊化轉型的發展，國防需求的資訊設備數量正逐年增加，這對建軍備戰而言，是有相當大的助益，但對國防資訊安全來說，卻是相當頭痛的問題。現有的資訊安全政策是採軍、民網實體隔離，但實際上，我們經常使用的各種免費軟體工具，以及新下載的各種版本的升級軟體或安裝程式，都很有可能是一個綑綁「間諜程式」的載體。國軍內部使用人員往往沒有意識到這個問題，他們只注重對外安全保密和電腦實體隔離的問題，而忽略「間諜程式」對內部資訊安全的危害。

文獻探討

一、間諜程式概說

間諜程式通常在未經用戶許可的情況下，採用一系列的技術(例如鍵盤錄製、掃瞄用戶電腦上的檔案或是錄製用戶連線網際網路的執行方式)來搜集用戶個人訊息的電腦程序。而「間諜程式」這個名詞首次在1994年出現，但是到2000年才開始被廣泛使用，並且和廣告軟體及惡意軟體互換使用。其實間諜程式本身就是一種惡意軟體，而且是在用戶沒有許可的情況下，有意或無意的對用戶電腦系統和隱私權進行破壞。依據微軟對間諜程式的見解，則認為間諜程式是一種專門在用戶不知情，或未經用戶准許的情況下，蒐集用戶的個人資料，而所蒐集的資料範圍包含盜竊用戶的網路帳號和密碼，或該用戶平日瀏覽的網站等。[4、5、6、7]

二、間諜程式分類

間諜程式通常分成廣告程式及資料竊

2 行政院科技顧問組，〈2008資通安全政策白皮書〉(臺灣)，西元2008年，頁60～63。

3 搜狐新聞，〈間諜軟件已成危害國防信息安全頭號殺手〉，http://mil.news.sohu.com/20071019/n252735004.shtml，西元2008年，頁1。

4 維基百科，〈Spyware〉，http://en.wikipedia.org/wiki/Spyware，西元2012年，頁1。

5 中國知網，〈間諜軟件危害日深，網絡恐怖暗流湧動〉《中國學術學報》(中國)，第3期，西元2005年，頁1。

6 袁順波，〈信息安全新威脅：網絡間諜軟件〉《中國信息專報》(中國)，第1期，西元2005年，頁49、50。

7 趙有才、劉克勝、楊智丹，〈間諜軟件及其防護策略〉《中國學術學報》(中國)，第1期，西元2007年，頁47～60。

取程式兩大類。

(一)廣告程式

廣告程式是一個套裝軟體，一旦它被安裝於用戶端的電腦，便會在螢幕上自動顯示廣告資料，甚至會不定時的向用戶端傳遞廣告訊息，蒐集該用戶的上網瀏覽習慣。而部分廣告程式(瀏覽器綁架程式)則會改變瀏覽器設定(例如Internet Explorer 的預設首頁及預設搜尋引擎)，導致瀏覽器可能會被重新導向到一個不明的網頁，進而消耗系統資源或網路頻寬，而使得電腦效能降低。

(二)資料竊取程式

資料竊取程式是一個在未經用戶同意下被安裝在用戶端電腦上的間諜程式，然後透過網路將蒐集到的資料傳送給第三者，所產生的威脅如下：

1.資料洩漏

資料竊取程式會在受感染的電腦系統尋找「有用的」資料，它可以是任何檔案或程式，例如業務計畫、原始碼、財務記錄、用戶通訊錄內的電子郵件地址及其他受版權保護的資料，這些被選取的資料可以透過網路秘密地傳送給其他人。

2.鍵盤輸入記錄及螢幕監控

鍵盤輸入記錄功能，可以記錄用戶端所有鍵盤輸入的資訊。而被記錄的資料(如該用戶在網路銀行所輸入的登入名稱及密碼)可以在用戶不知情的情況下傳送給第三者。雖然有部分的網路交易網站採用了動態鍵盤輸入，但仍有些程式可以監控被害者的螢幕，然後記錄鍵盤的輸入位置。

整體來說，間諜程式通常是具有雙重特性，表面上具備實用性及吸引力的基本功能，像是影音播放程式、更新軟體套件、實用的工具及小遊戲等。但事實上卻是暗中夾藏一個間諜程式。當電腦被植入了間諜程式後，使用者的作業系統幾乎和正常的電腦沒什麼差別，但使用者的個人隱私和重要的資訊，都會被間諜程式暗中蒐集，嚴重的話，可能會被開啟後門，變成駭客的操縱工具。在2006年11月美國海軍戰爭學院遭到中共駭客的入侵，其目的是蒐集美國海軍演習資料，而迫使該網站關閉數週之久，但這種情況只是冰山一角而已，更讓人憂心的是目前間諜程式結合後門、木馬、Rootkit[8]等複合技術的發展趨勢。[9]

三、程式分析技術 —— 卡斯敦威廉斯沙盒 (Carsten Willems Sandbox, CWSandbox)

在所研讀的文獻中，有一篇是針對程式執行分析的文章，[10]內容提到目前防護軟體偵測技術，大部分是利用特徵碼來判別間諜程式，但現今駭客的技術及入侵工具，已無法單純用特徵碼機制來防禦，而且特徵碼僅能對已知的間諜程式來進行偵測，但對未知及新型態的間諜程式卻是束手無策。文獻中所用的技術是

8 Rootkit通常指的是在滲透到系統之後，會隱藏登錄項目、檔案或處理程序等資源的一種軟體。因此這種軟體會隱匿系統中的攻擊者行蹤，方便他們隨時存取系統。

9 趙洪彪，〈惡意代碼的特徵與發展趨勢〉《中國學術學報》(中國)，第1期，西元2003年，頁49～51。

10 Carsten Willems, "Toward Automated Dynamic Malware Analysis Using CWSandbox," SECURITY&PRIVACY, IEEE, Valume_5, Issue_2, April 2007, pp.32-39.

運用沙盒(Sandbox)來分析程式執行特徵，以字面上的意義來說，就是用完即丟，重開即還原的意思。因此，本篇利用程式在Sandbox的環境中執行，並運用應用程式介面掛鉤(Application Programming Interface Hook, API Hook)及動態連結資料庫注入(Dynamic Link Library Injection, DLL Injection)方式實現Rootkit技術追蹤，及監控全部系統的系統呼叫(System Calls)來達成分析及記錄程式在執行期間更動系統的資訊。以Windows為例，kernel32.dll是每個程式啟動執行時必定會呼叫的檔案，所以CWSandbox利用kernel32.dll這個特性，運用以上兩種技術監控記錄欲執行程式在系統內所有的特徵，達到分析程式的目的。[11、12]

CWSandbox的分析報告內容包含以下項目(如圖一)。

(一)程式執行時產生或修改那些檔案。

(二)程式執行或修改那些登錄檔 。

(三)程式執行前載入那些DLL檔。

(四)虛擬記憶體那個區域被存取。

(五)產生那些新的程序(Process)。

(六)打開那些網路連線和傳送那些資訊。

(七)安裝那些服務或核心驅動程式。

(八)可分析程式執行後產生的子程式(分析關聯程式的執行方式)。

研究方法

一、研究流程

本篇論文架構(如圖二)，先是從相關網站蒐集間諜程式及正常程式的樣本，做為間諜程式偵測用資料集，接著分析所擷取的樣本特徵，最後再以分析的結果定義動態特徵的執行方式。

(一)蒐集樣本

因目前探討間諜程式偵測的文獻，並沒有相關資料集可做為參考，故本研究是從相關網站蒐集間諜程式及正常程式的樣本，做為間諜程式偵測用資料集。蒐集的間諜程式包括監偵型間諜程式、木馬、鍵盤側錄及後門等執行類似的間諜程式，但不包括執行特性與間諜程式差異太大的惡意程式，例如以破壞系統為目的的病毒程式及蠕蟲程式。正常程式樣本蒐集則包括網路工具、系統校調、系統程式、檔案轉換、登錄檔工具、微軟修補檔等類型共計12項。

(二)定義分類特徵

依據間諜程式特性及參考相關文章，初步訂定間諜程式可能在系統內部產生的執行模式：[13、14、15、16、17、18]

1.系統開機自動啟動

依據間諜程式需要植入被駭端電腦自動執行之特性。而間諜程式自動啟動的方式，大致可概分為以下幾種：(1)將程式置於啟動資料夾；(2)利用註冊表鍵值啟動；(3)應用程序關聯啟動；(4)修改系統啟動文件；(5)註冊新的系統服務；(6)其他方式。

11 惡意程式研究室，〈Spyware & Malware Information〉，http://research.sunbelt-software.com/WhatYouShould Know.aspx，西元2012年，頁1。

12 GFI SandBox, "Dynamic malware analysis," http://www.cwsandbox.org, 2012, p.1.

13～18 於下頁。

圖一　分析報告

資料來源：Malware Research Labs, http://www.cwsandbox.org, Jul, 2011.

上述動作大都由修改註冊表完成，只有極少數的間諜程式會將執行檔放在啟動資料夾內，達到自動啟動的目的。另外，有些間諜程式可以透過修改系統檔案，造成系統啟動設定「初始狀態」時引發自動啟動事件，如修改WINSTART.bat、WIN.ini、System.ini等檔案(如表一)。

2.修改檔案系統(新增、刪除、改變)

13　孫淑華、馬恒太、張楠、卿斯漢，〈內核級木馬隱藏技術研究與實踐〉《微電子學與計算機》(中國)，第21卷3期，西元2004年，頁76～80。

14　朱明、徐騫、劉春明，〈木馬病毒分析及其檢測方法研究〉《計算機工程與應用》(中國)，第39卷28期，西元2003年，頁176～179。

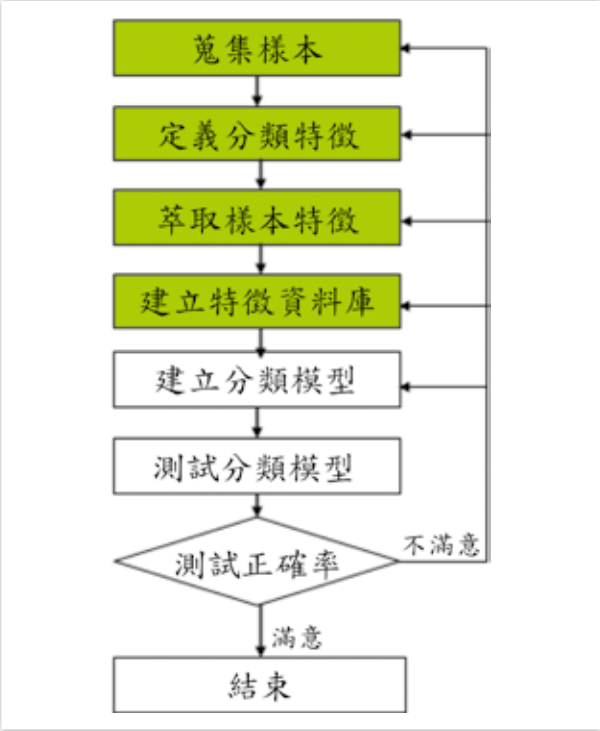
15　張健華，〈剖析特洛伊木馬的隱藏技術〉《水利電力機械》(中國)，第26卷6期，西元2004年，頁53～55。

16　楊珂，房鼎益，陳曉江，〈間諜軟件和反間諜軟件的分析與研究〉《微電子學與計算機》(中國)，第23卷8期，西元2005年，頁46～52。

17　程秉輝、John Hawke，《網路釣魚+側錄+間諜+詐騙+毒駭》(臺灣：旗標出版，西元2004年)，頁4.37～4.66。

18　劉吉與柳靖，《駭客攻防實戰詳解》(臺灣：松岡出版，西元2007年)，頁23～30。

圖二　研究流程



資料來源：作者整理

依據間諜程式需要搜集資料之特性。其間諜程式本身不屬於作業系統預設的程式，為了啟動和工作上的方便，會挑選某一資料夾當做藏身之所。同時為了達到隱蔽功能也常會替換或修改某些檔案，而這些檔案通常為系統檔案。在此將以Windows 及System32兩項系統預設目錄為主，並觀察間諜程式執行後，檔案系統中有無產生檔案。

3.隱藏執行方式

依據間諜程式需具有的隱蔽性。通常間諜程式為了掩人耳目，達到隱藏的目的，除了常使用一些跟系統預設的相近名稱(如rundll32.exe、rund1132.exe)，或跟系統檔相同的名字並放在不同資料夾內等混淆視聽的方法外，還有很多間諜程式利用DLL-Injection的技術來隱藏執行程序與Rootkit技術。其隱藏執行方式的對象包括運行中的程序、檔案、註冊表及系統所開啟的網路通訊埠(Port)等。針對上述執行方式，初步共歸納出14項執行特徵(如表二)。但經分析後發現，前期所使用的程式，其執行特徵產出的結果未如預期中理想，原因在於14項執行特徵中有許多特徵的分辨性不佳，如F14對於正常與間諜程式的執行特徵來說，所產生的執行比例是相近的。其次是部分的特徵屬性類似，如F1～F7特徵同屬自動啟動特性，F12與F13亦同屬更動系統資料夾。基於執行特徵分類，必須能夠清楚明確的表示，才能使初學者或管理者容易分類，且不易混淆。在此將依下列所述三個時期重新修訂執行特徵分類項目：

(1)尚未執行時期

依據目前大部分間諜程式會透過加殼(Packer)的程序，將原程式的特徵碼重新編排過，目的是為了躲避特徵碼掃瞄防毒軟體的偵測，所以將此新特徵納入執行特徵分類項目中。

(2)程式部署時期

在間諜程式執行初期，會在系統中部署所要使用的檔案或程式，目的在找出程式運用何種方式啟動，及系統資料夾內是否產生檔案或遭變更、特徵項目中部分是融合前期執行特徵，如合併F1、F2、F3、F4、F6、F7等6項，統一訂定為「自動啟動」特徵，另外F12、F13則合併為「更動系統目錄」特徵項目，最後的F14(產生新檔案)則修訂為「產生可執行檔」。

(3)程式常駐執行時期

在這時期所要分析的是程式執行後的方式，在執行特徵選定部分如隱藏的執行，除了沿用前期執行特徵F8、F9、

表一　自動啟動方式對照

Feature 1	Registry Run and RunOnce Keys
	HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\RunOnce HKEY_LOCAL_MACHINE\ Software\Microsoft\CurrentVersion\RunOnceEx HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\RunOnce
Feature 2	更動系統配置檔案
	Autoexec.bat, Win.ini, System.ini
Feature 3	藉助磁碟自動執行功能
	AutoRun.inf
Feature 4	更動Winlogon鍵值
	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Feature 5	利用Registry鍵值自動執行DLL-injection
	HEKY_LOCAL_MACHINE\Software\Microsoft\Windows NT \CurrentVersion \Windows\ AppInit_DLLs
Feature 6	利用Internet Explorer執行
	HEKY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Toolbar HEKY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ Browser Helper Objects
Feature 7	SHELL狀態更動
	HKEY_CLASSES_ROOT\exefile\shell\open\command HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command

資料來源：作者整理

F10 外，再增加「隱藏服務」、「自我保護」及是否有監視系統某視窗的「Hook特徵」，而原先的「隱藏通訊埠」則更明確的定義為「是否開啟通訊埠」。

新修訂的特徵項目共計有12項(如表三)，比前期執行特徵分析少了2項，但分析的內容及範圍皆比前期分析來得更深入、更容易辨識。

(4)網路執行模式(下載、上傳、轉送)

除了在系統內部的執行外，間諜程式必須對外通聯，達到傳送資訊給第三者的目的。

上述四項執行模式，也就是本研究對間諜程式所訂定的基本原則，初步分析主要是針對前三項執行特徵模式，網路執行模式現階段暫不納入特徵分析中。

二、程式執行分析工具

程式執行特徵分析所使用的主要工具軟體介紹如下：

(一) ProcessXP(如圖三)

功能：可以查看目前正在運作的程式及移除運作的程序(Windows工作管理員無法看到的隱藏的程序)。

目的：查看Windows工作管理員所看不到的系統內部程序運作，判別是否有不正常的程式在運作。

(二) IceSword(如圖四)

功能：屬於核心模式系統檢查工

表二　前期執行特徵分類

編號	執行特徵描述
F1	更動登錄檔(Run、RunOnce key)
F2	更動系統配置檔案(win.ini、system.ini..)
F3	藉助自動執行功能(Autorun.inf)
F4	更動登錄檔(Winlogon key)
F5	有無DLL Injection執行
F6	更動登錄檔(IE_Toolbar key)
F7	更動關聯檔
F8	隱藏登錄檔
F9	隱藏檔案
F10	隱藏執行程序
F11	隱藏通訊埠
F12	更動Windows資料夾
F13	更動System32資料夾
F14	產生新檔案

資料來源：作者整理

具，能檢查電腦系統內所有參數資料。

目的：查看執行完後，惡意程式更改系統底層的資訊，如系統服務描述表 (System Service Descriptor Table, SSDT)、瀏覽器說明物件(Browser Helper Object, BHO)及隱藏在工作管理員無法監看到的程序。

(三) AutoRun(如圖五)

功能：列出系統所有從開機自動啟動執行的程序，及相關檔案。

目的：監看執行過後的惡意程式，有無變更系統自動啟動項目。

(四)Winalysis(如圖六)

功能：系統快照軟體可比對作業系統在某個時間點運作產生的前後差異。

目的：針對執行惡意程式前、後的作業系統，使用該軟體能將整個系統的變動完整的顯示出來。

(五)Rootkit Revealer(如圖七)

功能：查找Rootkit程序的免費軟體，運用非作業系統程序的技術，可以掃瞄出隱藏在系統中的文件及登錄檔。

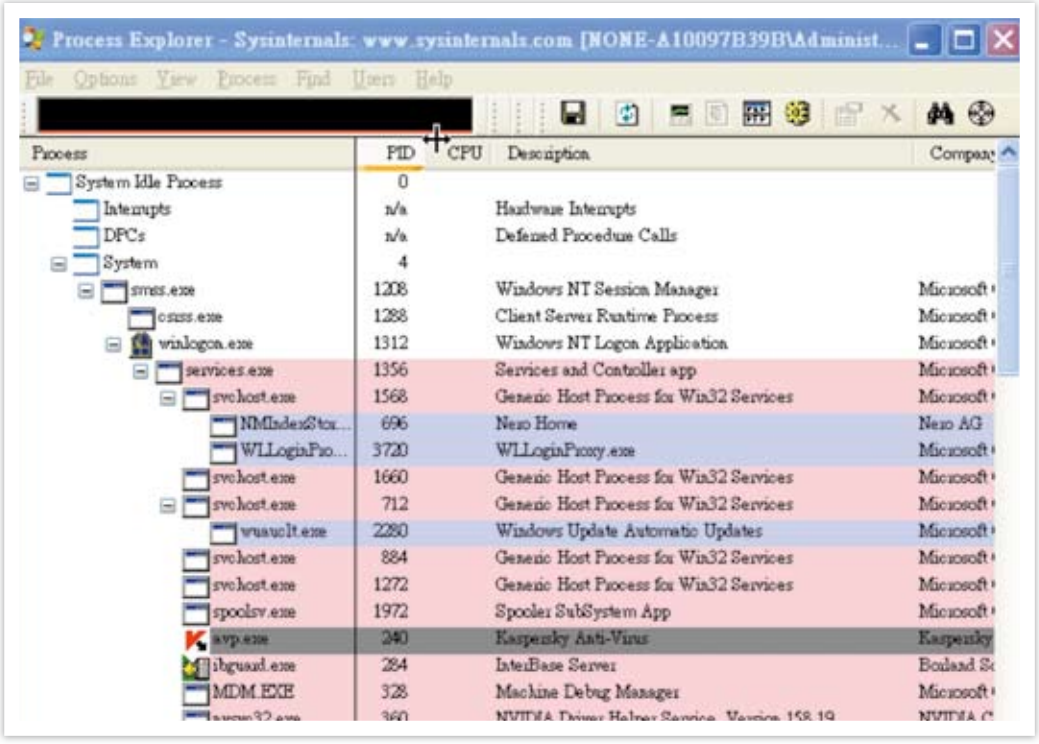
目的：找出隱藏在作業系統內的檔案及登錄資料。

表三　前期與後期執行特徵分類與對照

後期特徵行為描述		前期特徵項目修訂對照
F1	是否加殼	新增項目
F2	自動啟動	整合F1,F2,F3,F4,F6,F7
F3	DLL Injection	沿用F5
F4	更動系統目錄	合併F12,F13
F5	產生可執行檔	修正F14
F6	隱藏檔案	沿用F9
F7	隱藏註冊表	沿用F8
F8	隱藏程序	沿用F10
F9	隱藏服務	新增項目
F10	是否開啟通訊埠	修正F11
F11	自我保護	新增項目
F12	Hook行為	新增項目

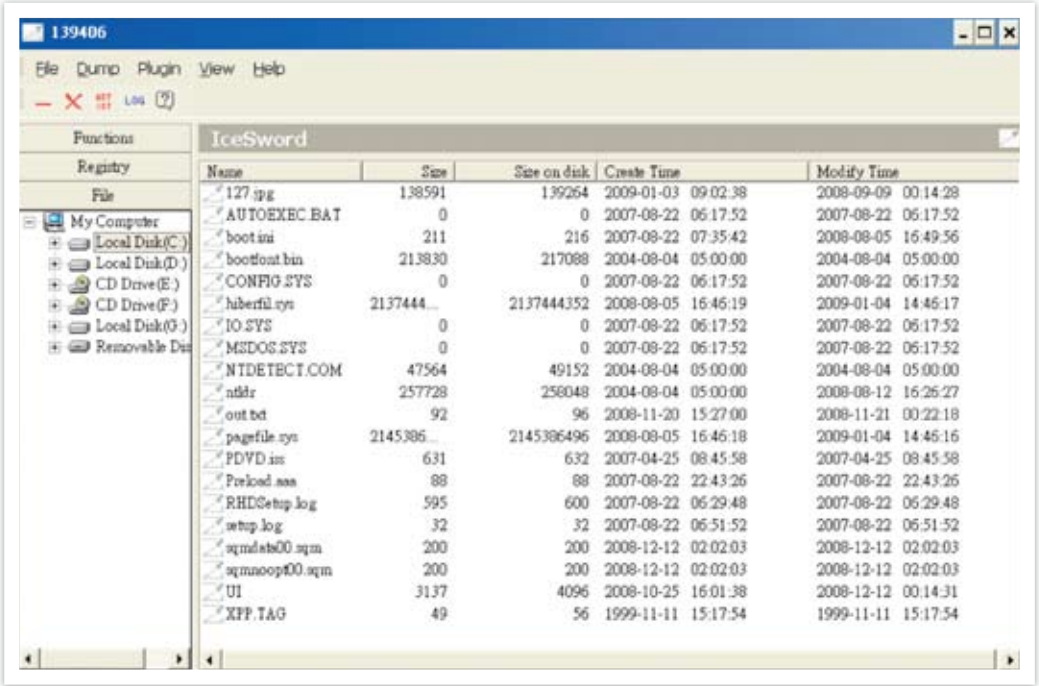
資料來源：作者整理

圖三　ProcessXP 執行畫面



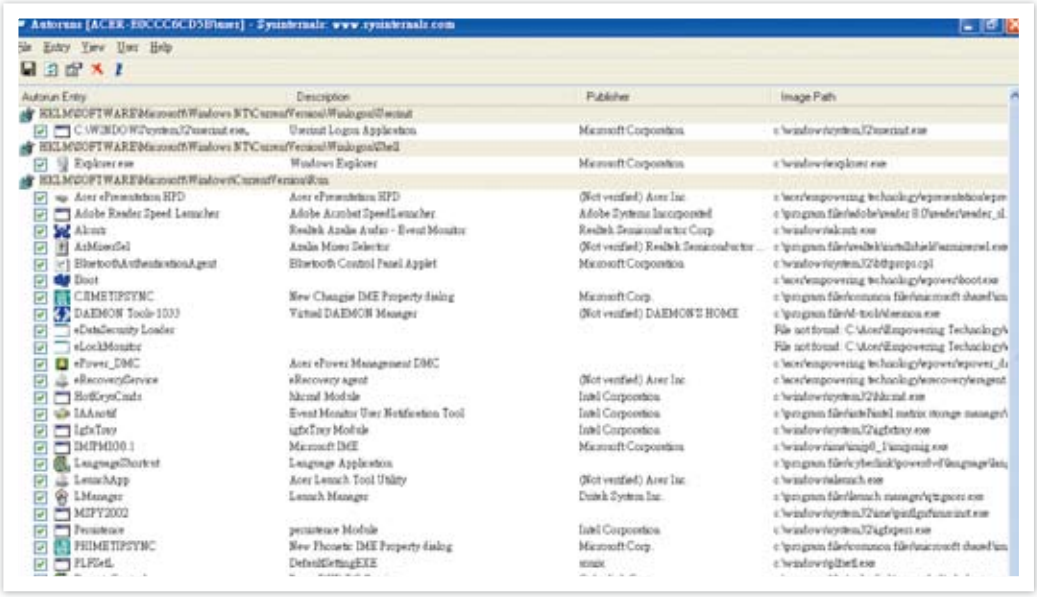
資料來源：作者整理

圖四　IceSword 執行畫面



資料來源：作者整理

圖五　AutoRun執行畫面



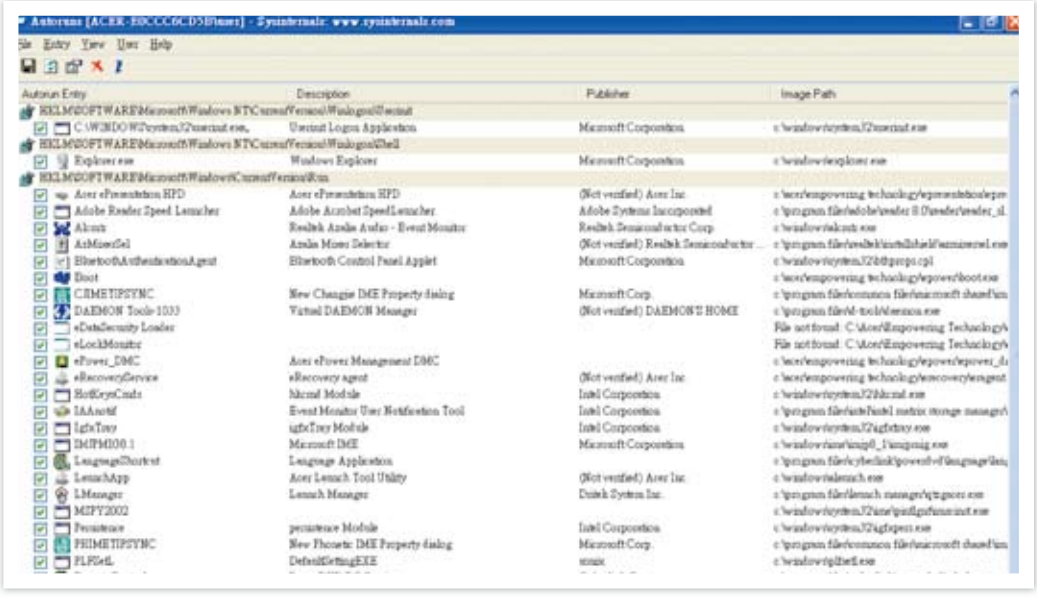
資料來源：作者整理

(六)Fport(如圖八)

功能：可以檢測出所有開放的傳輸控制協定/網際網路協定(Transmission Control Protocol/Internet Protocol, TCP/IP)及使用者資料報協定(User Datagram Protocol, UDP)的通訊埠並對應到可能是那些應用程式在使用這些通訊埠。在知道有那些通訊埠是暴露在外後，可以將不需要開放的通訊埠關閉，以防攻擊。

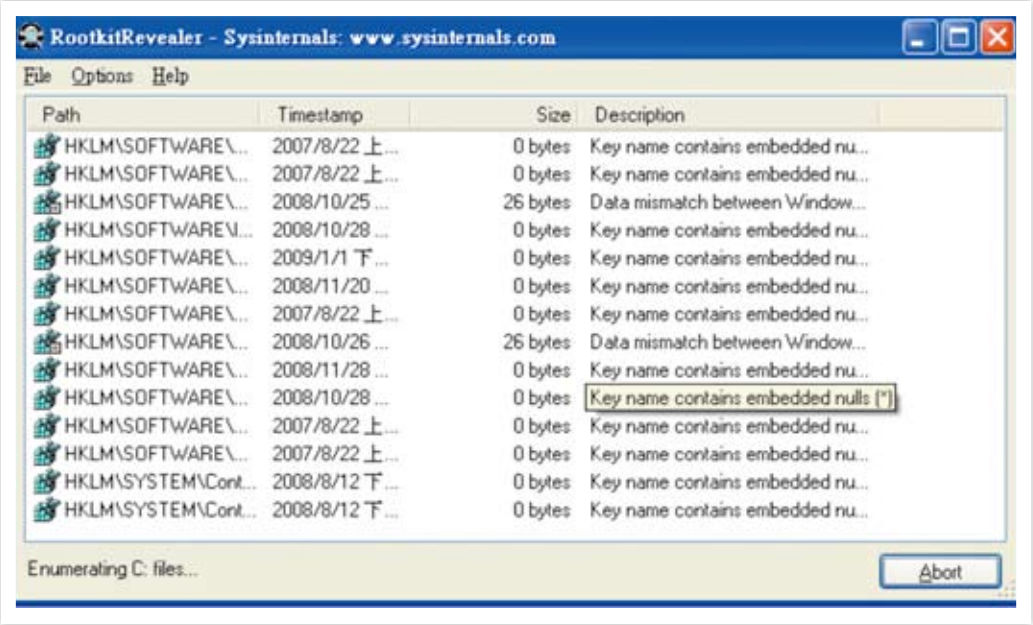
目的：查看惡意程式在系統中所

圖六　Winalysis執行畫面



資料來源：作者整理

圖七　Rootkit Revealer執行畫面



資料來源：作者整理

開啟的通訊埠。

(七)PEiD(如圖九)

功能：PEiD目前可以偵測超過多種的檔案加殼(Packer)器、加密器及編譯器，也可識別出執行檔案是用何種語言編寫的，如VC++、Delphi或VBi 等，另外，PEiD也能夠偵測出幾乎所有被打包、掩藏和編譯的檔案。

目的：偵測樣本檔案是否經過加殼(Packer)程序。

圖三～圖八為前期分析所使用的工具，程式執行特徵與工具對照如表四。在後期程式執行特徵分析，新增加使用PEiD查殼工具，所分析使用的工具與執行特徵比對如表五。

三、分析標準作業程序制定

當蒐集數量到達預定目標之後，接下來就是要訂定分析的流程及相關細節，因為分析工具皆是獨立的個體，必須將分析過程訂定成標準，以利未來在分類過程中才有依據可循(如圖十)。

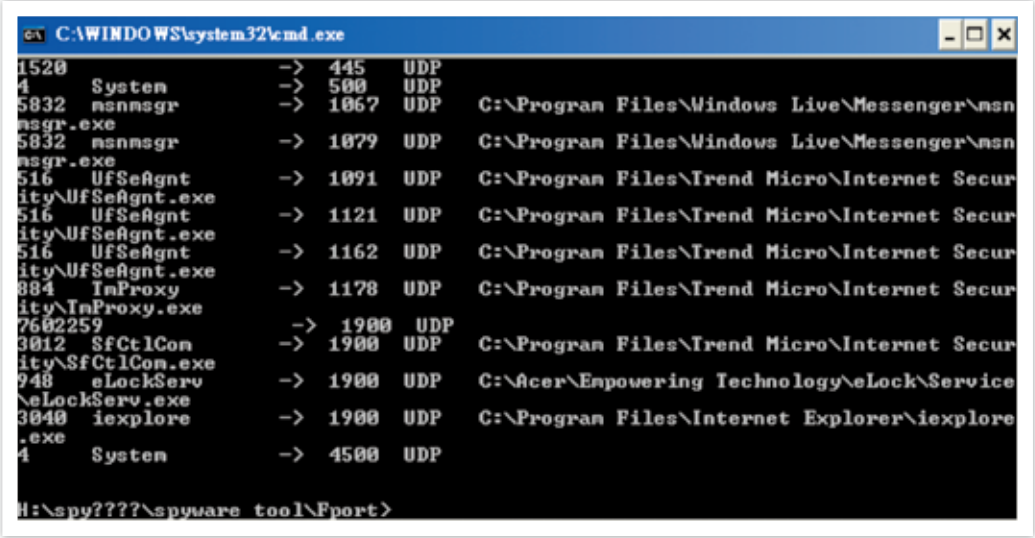
(一)資料篩選

程式資料庫的前置處理，是將所蒐集到的程式中多餘的雜訊要先過濾，使正常程式資料庫中無間諜程式的摻入，以確保分析資料的可用性。目前運用的前置處理方式是將蒐集的程式，利用數家知名的防毒(間諜)軟體計有Kaspersky、F-Secure、Symantec、Trend Micro及SpywareDetector做掃瞄過濾，讓樣本資料庫更具可靠度，其流程(如圖十一)。

(二)程式執行特徵分類

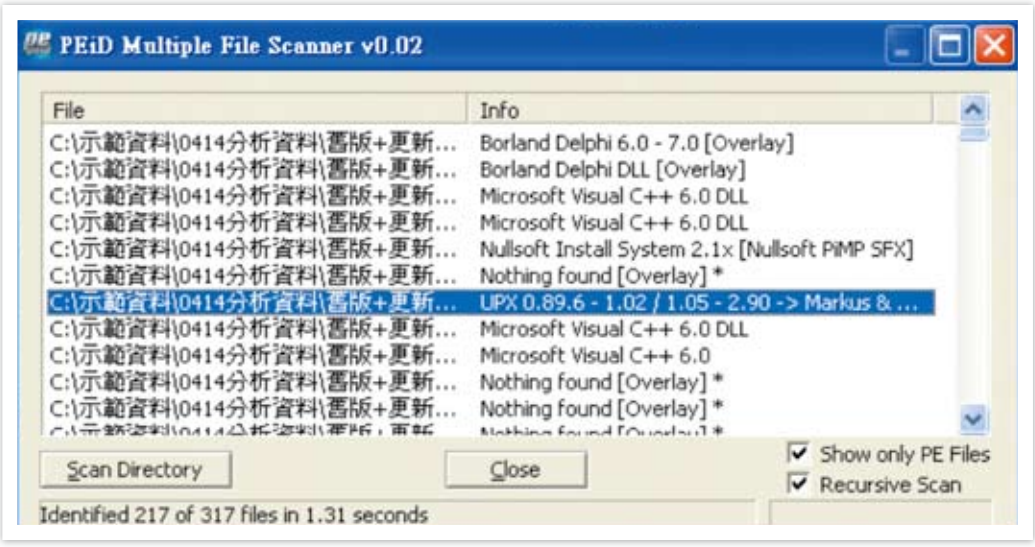
程式執行特徵分類是比較偏向主觀的判斷，每個程式分析人員皆有屬於自己的一套分析程式方法及環境，雖然分析人員擁有相同的程式，但在不同的作業系統環境及分析工具之情況下，分析的結果卻有相當大的差異，這結果對後端使用這些分析數據的人員影響甚鉅，分析結果的好壞，都與前端分析的穩定度及正確

圖八　Fport執行畫面



資料來源：作者整理

圖九　PEiD執行畫面



資料來源：作者整理

性息息相關，所以建立一套分類流程(程序)對未來承接此工作的分析人員是有必要性的。而執行特徵的萃取，是靠不同的分析程式來完成，在此以CWSandbox為例，CWSandbox自動化分析程式執行特徵的網站，提供免費程式上傳分析(網址：http://research.sunbelt-software.com/Submit.aspx)。CWSandbox上傳分析(如圖十二)，分析結果(如圖十三)。

(三)資料核對

資料比對是將手動執行分析的結果與CWSandbox分析的結果實施比對。

表四　前期分析工具與程式執行特徵對照

特徵＼程式名稱	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14
ProcessXP										●				
Ice Sword										●	●			
Auto Run	●		●	●	●									
Wina lvsis	●	●	●	●	●	●	●					●	●	●
Rootkit Revealer								●	●					
Fport											●			

資料來源：作者整理

表五　後期分析工具與程式執行特徵對照

程式名稱＼特徵	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12
PEiD	●											
Wina lvsis				●								
ProcessXP			●								●	●
Auto Run		●	●	●								
Rootkit Revealer					●	●						
Fport									●			
Ice Sword					●	●	●	●	●			

資料來源：作者整理

若比對結果差異性太大，則此筆資料將不列入特徵資料庫內，若兩者分析比對資料相符，則納入特徵資料庫內。

研究成果

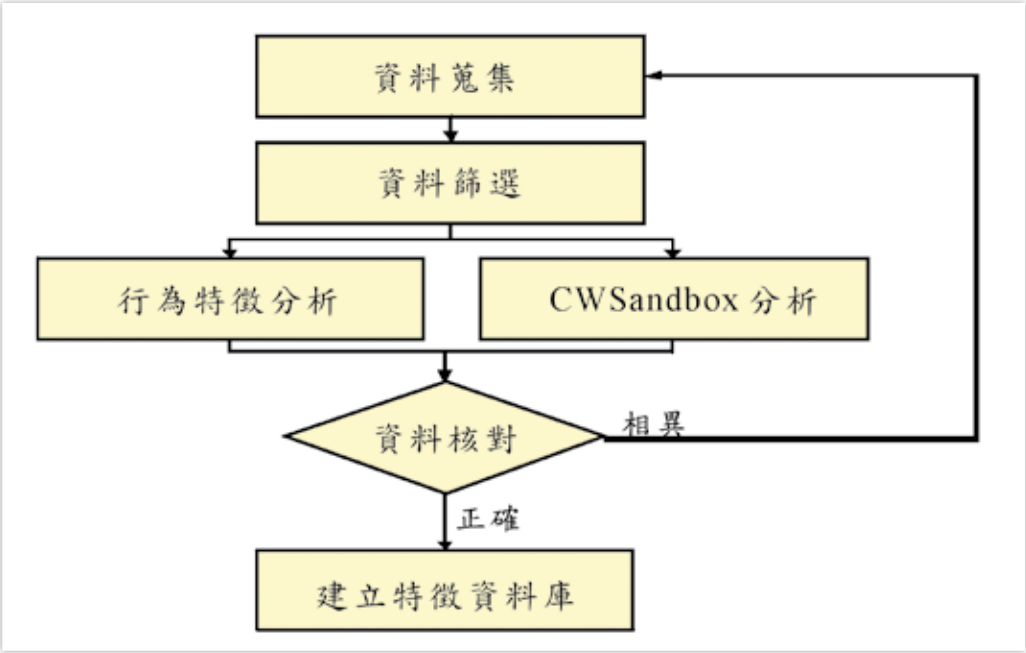
於前期分析結果，所採用間諜程式數為328，正常程式數為525。於後期分析結果，則採用間諜程式數400，正常程式數800。其表六、七、九、十的縱軸為特徵分類項目，橫軸為程式呼叫次數，而所謂的呼叫次數即表示程式執行後，會產生的該類特徵。

一、前期分析結果

前期分析間諜程式的14個執行特徵結果如表六，正常程式特徵分析結果如表七，表八則是將間諜程式與正常程式的特徵組合做綜合分析。若比例相差愈近，則表示間諜與正常程式特徵相依性太高、分辨率差。若比例相差愈大，則表示間諜與正常程式特徵相依性低、分辨率佳。由表六、七的數據可得知間諜程式和正常程式在F1～F14特徵中各占的比重，再進一步採聯集方式，綜合比對兩個類別的特徵關聯如表八。表中的程式執行特徵是採聯集方式所產生，如萃取－程式自動啟動(F1)、隱藏通訊埠(F11)、更動System32資料(F13)、產生新檔案(F14)皆為「1」的間諜及正常程式數目來比較分析。

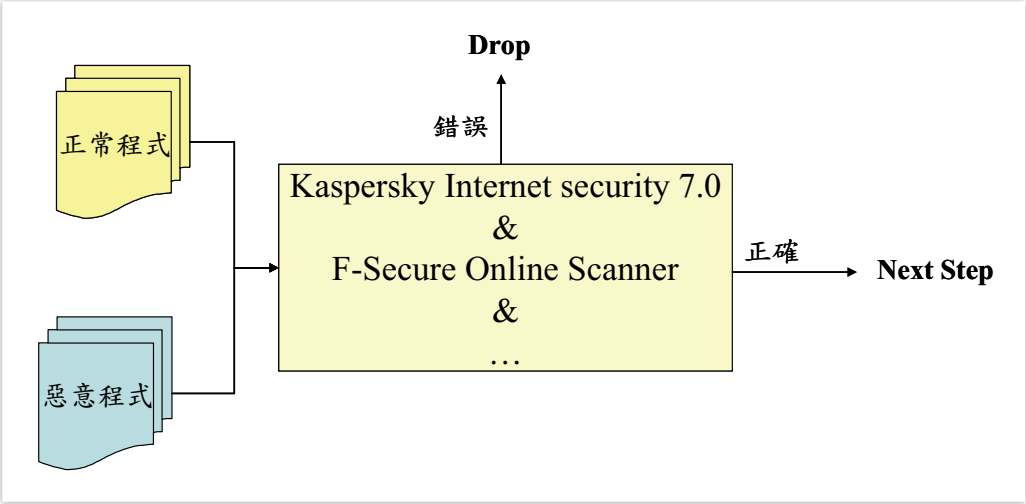
由於現階段並無標準的程式資料庫參考，本研究所分析的間諜程式及正常程式是自行從網路蒐集下載，間諜程式包括病毒郵件、論壇惡意程式樣本，正常程式類別包括系統、網路、程式修補、工具程式等共計12大類。目前的程式執行分析初步

圖十　執行特徵分析流程



資料來源：作者整理

圖十一　資料篩選流程圖



資料來源：作者整理

結果如表八，產出的結果有許多是不如預期的理想，其中遭遇幾項問題及解決方案如下：

(一)執行特徵定義要更明確，目前程式執行分析的14項執行特徵，有些需要再進一步的定義，目的是讓分析程式執行時，避免模糊不清，造成誤判或無法判斷。初期訂定的14項特徵在程式分析過程中，有些部分的執行特徵有再重新修訂過，未來分析的產出結果將以新的執行特徵為基

圖十二　CWSandbox上傳分析

資料來源：Malware Research Labs, http://research.sunbelt-software.com/Submit.aspx, Aug, 2011.

礎。

(二)模擬分析環境的增加，目前分析的環境是在VMware Workstation下建立作業系統(Windows XP sp2)，然而現今的惡意程式攻擊的目標，卻是有針對作業平臺版本而設計，不符合設計的攻擊平臺是無法執行，在初步分析中也遭遇到這類問題，所以在未來分析可計畫增加分析平臺，讓分析數據更臻完善。

二、後期分析結果

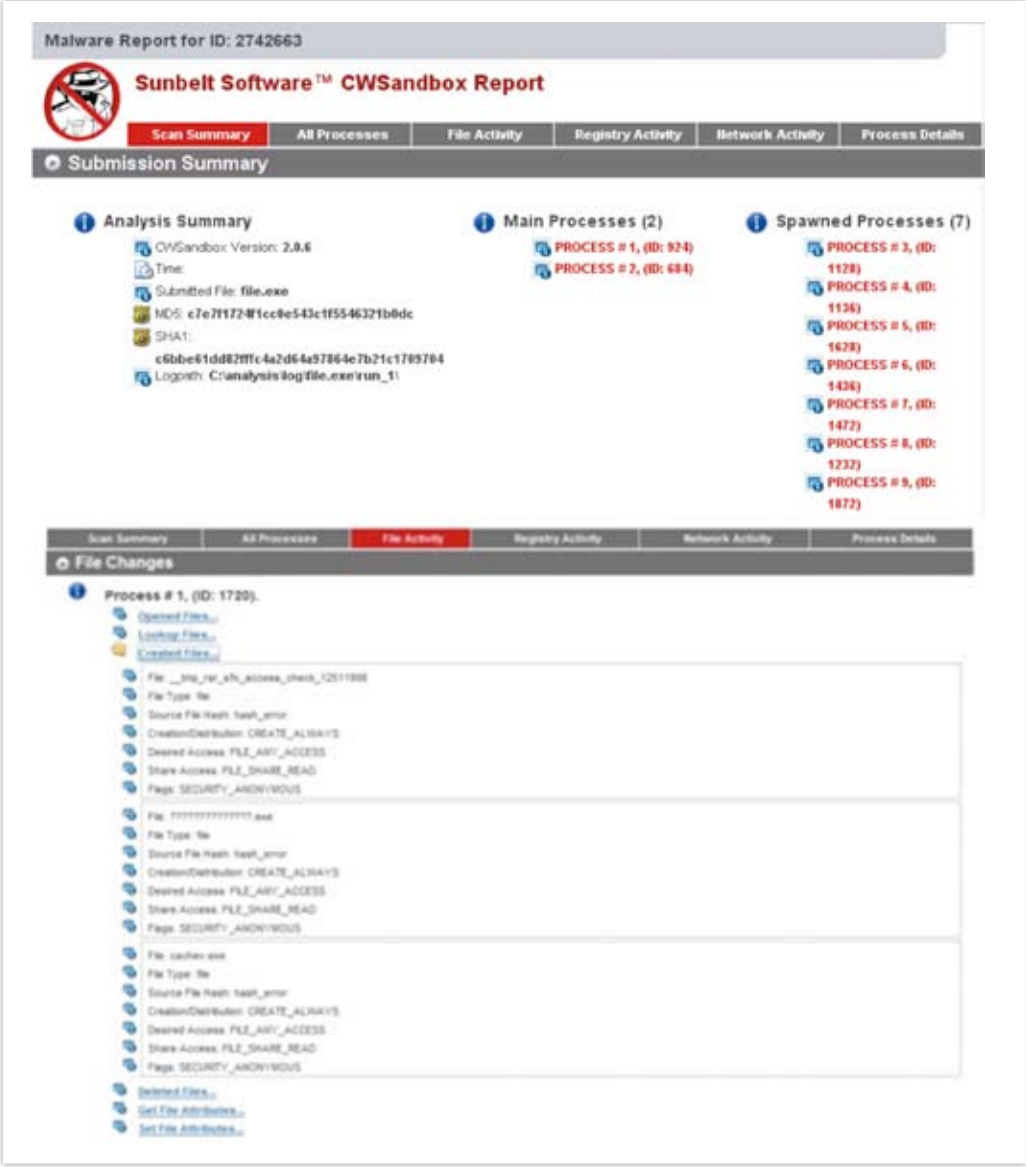
後期分析部分，利用新修訂的程式執行特徵其分析結果：間諜程式分析結果(如表九)，正常程式分析結果(如表十)，特徵綜合比對分析結果(如表十一、十二)。比較表十一、表十二與表八所分析的結果，可看出分辨率的確有提高許多，另一方面靜態API分析也是分辨程式的其中一項重點，後續可利用本研究所修訂的執行特徵分類建立特徵資料庫(如圖十四)，以利管理人員有統一的資料格式可運用。

結　論

隨著網路發展技術的突破，資訊化的社會帶來許多的便利，但相對的危機也愈來愈多，若資訊系統沒有健全的防護機制，將導致個人、企業、國家的資訊資產暴露在危險中。為因應目前間諜程式偵測機制不夠完善，現行的特徵碼比對僅能對已知的間諜程式，進行防護，而對未知及變形的間諜程式則是毫無招架之力，所以，本研究發現必須做到以下幾項：蒐集間諜程式及正常程式樣本；定義間諜程式執行特徵分類；建立程式執行分析程序。

雖然市面上已有許多的反間諜軟體，但礙於種種因素，市面上的反間諜軟體並不會描述實際特徵與執行模式。而目前本研究運用靜態API呼叫並配合程式執行分

圖十三　CWSandbox傳回分析結果

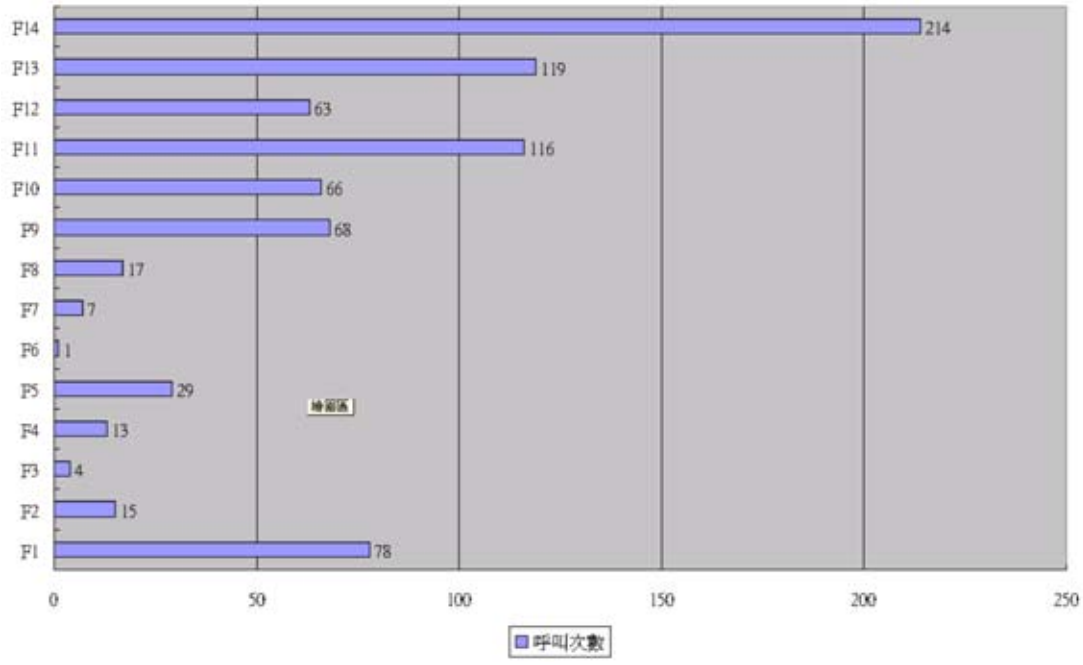


資料來源：Malware Research Labs, http://www.cwsandbox.org, Feb, 2012.

析數據，定義間諜程式執行特徵及建立程式執行分析程序，後續將可依執行特徵分類建立資料庫，進而偵測未知的間諜程式。雖然分析數據不盡完善，尚有待更進一步精進及改善空間，但本研究對於要如何分析已知的攻擊及未知的異常攻擊有了初步方法，可提供未來接手本研究人員有相關參考依據。

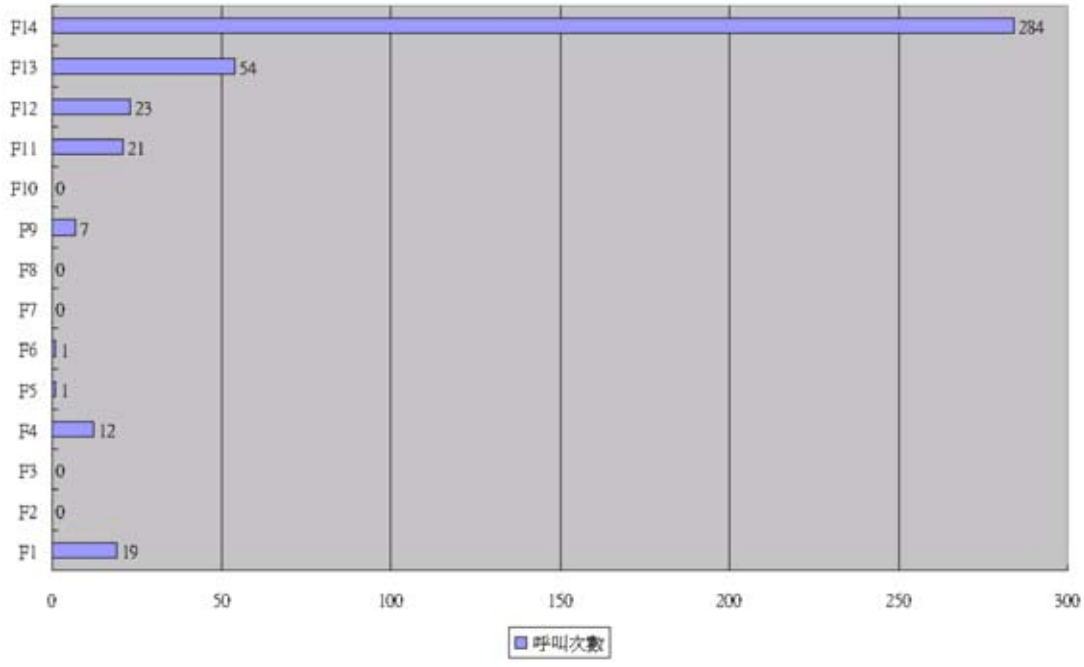
從研究方法中我們確信，只要掌握每個間諜程式的動態執行特徵，運用執行特徵模式去判斷該程式是否具有惡意執行特徵，不但有助於個人用戶加強內部安全防護，更便於程式管理者分析和管理。也可將所掌握的執行特徵製作成一個資料庫，便能在發現新型態或未知的間諜程式時，迅速做進一步的判斷及處置，以便縮短處

表六　間諜程式執行特徵分析



資料來源：作者整理

表七　正常程式執行特徵分析



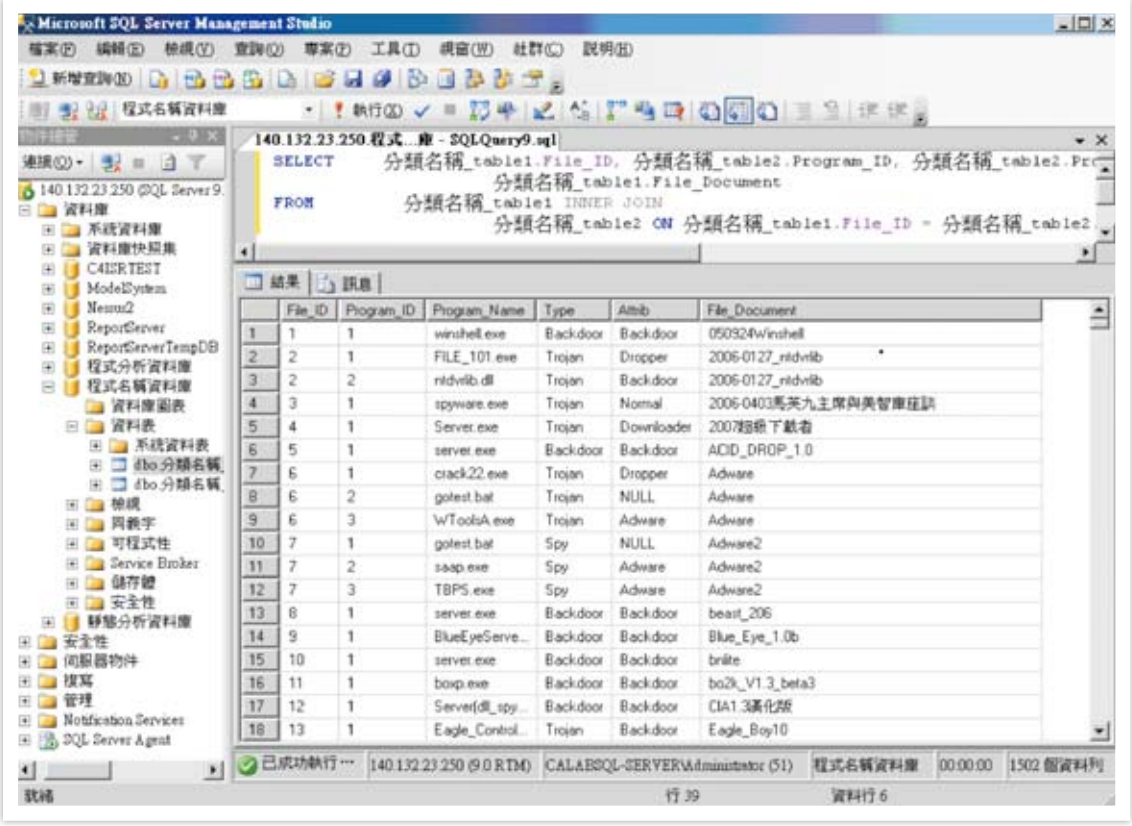
資料來源：作者整理

表八　特徵組合綜合分析

特　徵　組　合	間諜程式	正常程式	比例(間／正)	
All Zero	29.3%	45.0%	不列入考量	BAD
F14=1	65.4%	54.0%	1.2/1	
F1,F11,F13,F14=1	11.3%	0.2%	56.5/1	GOOD!
F12,F14=1	19.2%	4.3%	4.46	
F13,F14=1	36.1%	10.2%	3.5	BAD!
F4,F14=1	3.9%	0.4%	9.75	
F11,F13F14=1	18.6%	1.1%	16.9	
F1,F13,F14=1	17.1%	1.1%	15.5	
F11,F14=1	31.4%	4.0%	7.8	
F1,F11,F14=1	14.3%	0.6%	23.8	
F5,F14=1	28.0%	0.2%	140	GOOD!
F12,F13,F14=1	8.5%	0.2%	42.5	
F1,F14=1	22.3%	3.6%	6.2	
F5,F9,F12,F14=1	2.7%	0.0%	2.7	

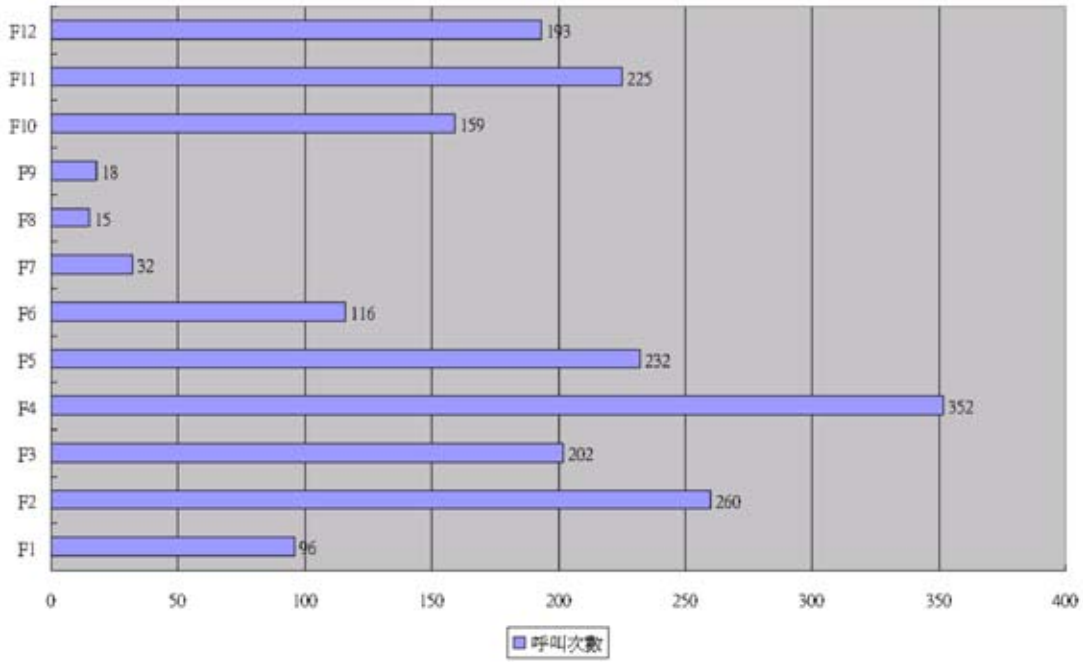
資料來源：作者整理

圖十四　資料庫程式分類



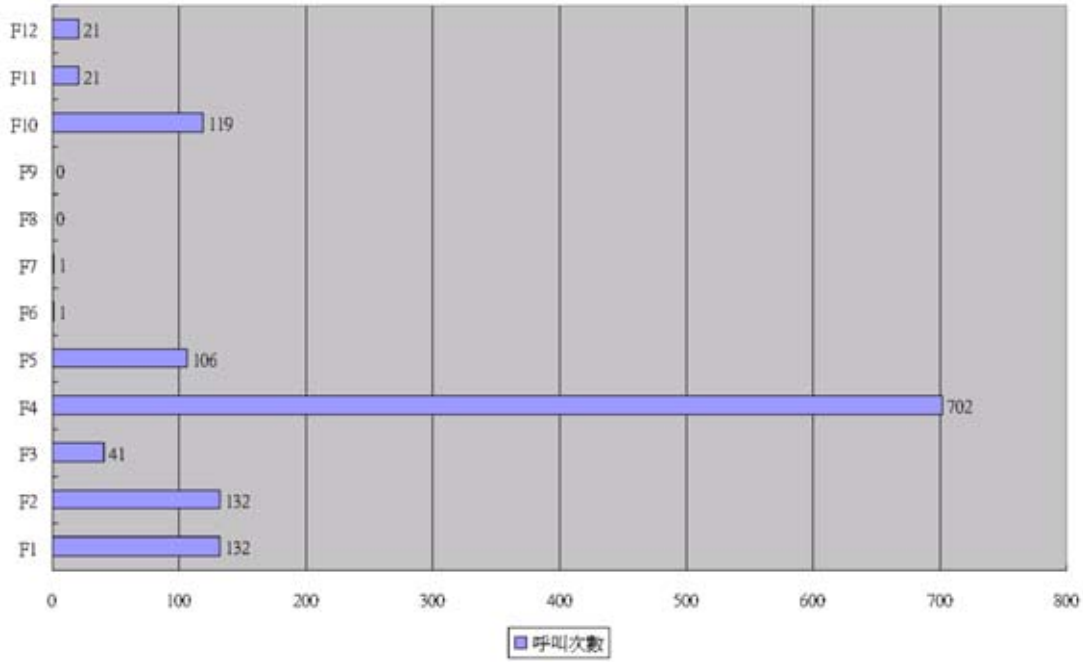
資料來源：作者整理

表九　間諜程式執行特徵分析



資料來源：作者整理

表十　正常程式執行特徵分析



資料來源：作者整理

表十一　單一特徵綜合分析

單一特徵	間諜程式	正當程式	比例(間：正)
F1	24.0%	16.1%	1.5:1
F2	65.0%	16.1%	4:1
F3	50,5%	5.0%	10.1:1
F4	88.0%	85.6%	1:1
F5	58.0%	12.9%	4.5:1
F6	29.0%	0.1%	237.8:1
F7	8.0%	0.1%	65.1:1
F8	3.8%	0.0%	3.8:0
F9	4.5%	0.0%	4.5:1
F10	39.8%	14.5%	2.7:1
F11	56.3%	2.6%	22:1
F12	48.3%	2.6%	18.8:1

資料來源：作者整理

表十二　特徵組合綜合分析

特徵組合	間諜程式	正常程式	比例(間／正)
F2,F3,F4,F5,F11	30/0%	1.0%	30.8
F2,F3,F5,F11	42.3%	1.1%	38.5
F2,F4,F5,	49.3%	4.6%	10.6
F2,F4	60.5%	15.6%	3.9
F2,F5	52.0%	4.6%	11.2
F2,F11	55.3%	13.4%	4.1
F4,F5	54.8%	11.2%	4.9
F4,F11	52.5%	2.4%	21.5
F5,F11	44.8%	1.6%	28.2
F2,F3.F4,F5	36.8%	1.2%	30.1
F2,F3.F4	43.3%	4.3%	10.1
F3,F3.F5	36.5%	1.2%	29.9
F3,F4,F5	37.0%	1.5%	25.3
F3,F4	46.8%	4.8%	9.8
F3,F5	38.8%	1.6%	24.4

資料來源：作者整理

置時間，將風險損失降到最低。

為使分析的數據更具有辨識率及可信度，未來研究方向可朝多平臺系統分析，因為現階段只在單一版本的作業系統分析，故有其分析環境的限制因素，分析數據可能就不能全面適用，故未來可建置不同版本的作業系統如Windows Server 2003、Windows7等，可讓資料庫內的分析數據更具可利用性。另外，在程式分析部分可加入網路執行特徵，如封包分析、網路異常及透過網路連線傳送何種資訊，可讓間諜程式的執行特徵更具完善。

參考文獻

一、搜狐新聞，〈警惕間諜軟件威脅國防信息安全〉，http://news.sohu.com/20080403/n256077191.shtml，西元2008年。

二、行政院科技顧問組，〈2008資通安全政策白皮書〉(臺灣)，西元2008年。

三、搜狐新聞，〈間諜軟件已成危害國防信息安全頭號殺手〉，http://mil.news. sohu.com/20071019/n252735004.shtml，西元2008年。

四、維基百科，〈Spyware〉，http://en.wikipedia.org/wiki/Spyware，西元2012年。

五、中國知網，〈間諜軟件危害日深，網?恐怖暗流湧動〉《中國學術學報》(中國)，第3期，西元2005年。

六、順波，〈信息安全新威脅:網絡間諜軟件〉《中國信息專報》(中國)，第1期，西元2005年。

七、趙有才、劉克勝、楊智丹，〈間諜軟件及其防護策略〉《中國學術學報》(中國)，第1期，西元2007年。

八、趙洪彪，〈惡意代碼的特徵與發展趨勢〉《中國學術學報》(中國)，第1期，西元2003年。

九、惡意程式研究室，〈Spyware & Malware Information〉，http://research. sunbelt-software.com/WhatYouShould Know.aspx，西元2012年。

十、GFI SandBox, "Dynamic malware analysis," http://www.cwsandbox.org,2012.

十一、孫淑華、馬恒太、張楠、卿斯漢，〈內核級木馬隱藏技術研究與實踐〉《微電子學與計算機》(中國)，第21卷3期，西元2004年。

十二、朱明、徐騫、劉春明，〈木馬病毒分析及其檢測方法研究〉《計算機工程與應用》(中國)，第39卷28期，西元2003年。

十三、張健華，〈剖析特洛伊木馬的隱藏技術〉《水利電力機械》(中國)，第26卷6期，西元2004年。

十四、楊珂，房鼎益，陳曉江，〈間諜軟件和反間諜軟件的分析與研究〉《微電子學與計算機》(中國)，第23卷8期，西元2005年。

十五、程秉輝、John Hawke，《網路釣魚+側錄+間諜+詐騙+毒駭》(臺灣：旗標出版，西元2004年)。

十六、劉吉、柳靖，〈駭客攻防實戰詳解〉(臺灣：松岡，西元2007年)。

十七、Carsten Willems, "Toward Automated Dynamic Malware Analysis Using CWSandbox," SECURITY&PRIVACY, IEEE, Valume_5, Issue_2, April 2007.