惡意程式入侵的安全鑑別與防制---以 Trojan Horse 為例

Security Forensics and Empirical Strategies for Preventing from the Intrusion of Trojan Horse

王旭正
中央警察大學資訊管理研究所
sjwang@sun4.cpu.edu.tw

高大宇
刑事警察局偵九隊
dayu@email.cib.gov.tw

摘要

近期視窗型 Trojan Horse 快速流行，對電腦使用者存有負面的安全危機，為協助電腦使用者阻擋外來的侵入攻擊，適時採行合宜的防制措施，降低受攻擊者的侵害程度，因此我們藉由收集相關 Trojan Horse 進行實驗模擬，以因應網路資訊犯罪的惡意程式行為。本文嘗試解讀視窗型 Trojan Horse 的運作特質與實質內容，萃取出較為顯著的攻擊特徵，再透過探討程式的感染實作細節，鑑別出攻擊過程事前、事中及事後不同時期的防護措施，以歸納出共通的標準安全檢核表，作為爾後識別新型惡意 Trojan Horse 的主要依據。此外，亦藉由觀察相關應用程式及通訊埠的連線目的方式，能事先知道異狀乃入侵之徵兆，以阻斷可疑的入侵事件，進而研擬提升追緝技能的方法，有效解決相關案例發生之處置效能。

Abstract

In recent years, the program of Trojan horse on the platform of window system has been emerging in the Internet applications. While the kind of such program is subject to the malicious program to risk the networked computer usage. In this paper, we propose the strategies to curb and lessen the influences when the computer working programs infected by the Trojan horse. The way to compass our conclusions is the collections of a sequence of experimental results. We analyze the execution of the Trojan and the aftermath infected by the Trojan on the window system of PC, in such a way that there are a number of remarkable characteristics of the running Trojan are featured in the course of elaborate experiments. Accordingly, the secure criterion tables are summarized to effectively predict, detect and deter from the possible threats in the three periods of before, middle and after happening. Besides, the relevant application programs and network communication ports open to the user connection in networks are also investigated, in the manner that the feasible mechanisms to withstand the attacks issued from the kinds of malicious programs are then kept trace. The explorations will profit the seizure of computer crime caused from malicious programs.

關鍵詞：電腦駭客、電腦安全、惡意程式、Trojan Horse、安全鑑別

壹、簡介

隨著網際網路開放原始碼(Open Source)的資訊共享特性發展，許多免費的安全防護軟體及攻擊程式也相繼蓬勃發展，只要有心蒐集與研讀不難了解其間的差異與特質。也因網路地下駭客組織討論的漸趨熱絡，使網路程式設計師改寫新型 Trojan Horse 的困難度迅速降低，對不同 Trojan Horse 作者而言，更有盡情揮灑設計能力的空間。而隨著設計者背景與時間的先後不同，在感染、啟動、識別或攻擊的手法效果上，亦有不同程度的變化應用。網際時代裡新型變種視窗型 Trojan Horse 的出現，不僅提供遠端存取電腦資訊的另一管道，也引發網路上不安的攻擊事件，若再輔以惡意程式(Malicious Program)的不易識別，將更衍生防護軟體的誤判率。

在本論文中，我們藉由較知名視窗型 Trojan Horse 的實驗模擬過程，瞭解攻擊、防衛與偵查過程的相關細節，進而透過攻擊與防衛之實驗觀摩，尋求可相互抗衡的方式。在實驗過程期間，為避免可能衍生的法律問題，均使用本實驗室的電腦，進行測試、觀摩與解讀木馬入侵程式的實作細節及攻擊方式的多變性，藉此得以研究其侵入技術及差異效果。而在受害主機部分除檢核相關處理程序的啟動與運作外，我們解析入侵徵兆的安全鑑別(Secure Forensic)方式，作為防衛模式的反制主軸，降低被入侵破壞的機率。其中，所謂的「安全鑑別」(Secure Forensic)指的是透過「事前防備設定」、「事中防護措施」與「事後稽核紀錄」等三個不同期間之防護過程，檢核是否存在惡意攻擊事實的過程，進而從電腦資訊設備中採集相關資訊作為爾後法院審理的證據參考。

在本研究論文中，我們先對 Trojan Horse 的觀念與防護做基本說明與介紹，再藉由模擬實驗的輸出結果進行分析與表列，以清楚釐定常見 Trojan Horse 的各項特徵、行為、反制與偵查方式，並透過實際案例來引證我們所提模式的具體性效果，以綜合本篇研究的結論。

貳、木馬的定位與防護觀念

2.1 基本觀念

Trojan Horse 程式，又稱為木馬程式或特洛伊程式，主要的意義為*「隱藏未授權程式碼並執行使用者不想或不知道功能的程式」*，其特徵具有短小、精幹、安裝方便、不意被察覺等特點[3][6]。對於網路系統而言，類似 Trojan Horse 的許多惡意程式潛藏著影響系統安全的危機。也因為個人電腦使用與連接網際網路的日益普遍，未來發生入侵的頻率將更為頻繁，如何有效識別來意不善的惡意程式，並有效保全個人電腦的使用，也成為安全防護專家及軟體設計時之自我防護機制的努力目標。就惡意程式之 Trojan Horse 的廣泛意義而言，隨著作業系統在使用者操作介面的趨導下有了大幅度的演進，此趨勢亦促使 Trojan Horse 的攻擊方式隨之調整腳步。在 UNIX 系統中，Trojan Horse 指的是一支看起來具正常用途的程式，卻企圖讓使用者在無意間執行特定程序達成攻擊者的侵入目的[2][11]。該程式可以隱藏於已編譯好的被附寄二位元執行檔中，使其不易閱讀、不易察覺與難以偵測。在 Window 視窗環境下的 Trojan Horse，如 Netspy、NetBus、BO(Back Oriffice)、BO2K(Back Oriffice 2000)、Subseven 及 Birdspy 等[4][14][17]，本身具執行過程隱形化功能加深其神秘性，甚至可讓使用者執行強大的遠端檔案存取功能。其中，Netspy、NetBus 及 BO 等三種 Trojan Horse 出現較早，Subseven 及 BO2K 等二種 Trojan Horse 功能

較強且使用率較高，而 BirdspyTrojan Horse 為第一種國人設計的 Trojan Horse。雖然程式本身不會讓電腦系統軟體癱瘓，然因它擁有強悍的資訊掌控功能，使電腦系統一但感染這種 Trojan Horse，便存在隨時被入侵攻擊的危機與風險。因此，在 Window 視窗環境下的視窗型 Trojan Horse 便為本文所探討的主題。

一般而言，視窗型 Trojan Horse 主要區分為客戶端、伺服端和組態設定等三部份，客戶(Client)程式安裝於管理員(或攻擊者)的電腦上，以實現遠端控制的目的。而伺服(Server)程式安裝於被控制者(受攻擊者)的電腦上，對來自客戶程式的攻擊要求做出反應，因而實現攻擊者的目的。一般而言，伺服程式實際體積細小，執行時沒有任何表面反應，不會於工作列或關閉視窗顯示且很難自動停止，感染執行後亦會透過變更檔名或修改系統啟動設定等方式降低被察覺的可能性[4][16][17]。最後在組態設定部分，指的是攻擊者為確保被控制者的電腦僅受攻擊者專用，蓄意攻擊者皆會針對通訊埠、密碼、感染方式、登錄設定鍵值(Registry Key)及啟動檔名方面做特殊的修改設定。根據上述，我們可知由於 Trojan Horse 在植入、感染程序的多變化，使得一般網路使用者對 Trojan Horse 感到恐懼、好奇與驚嘆。

2.2 防護觀念

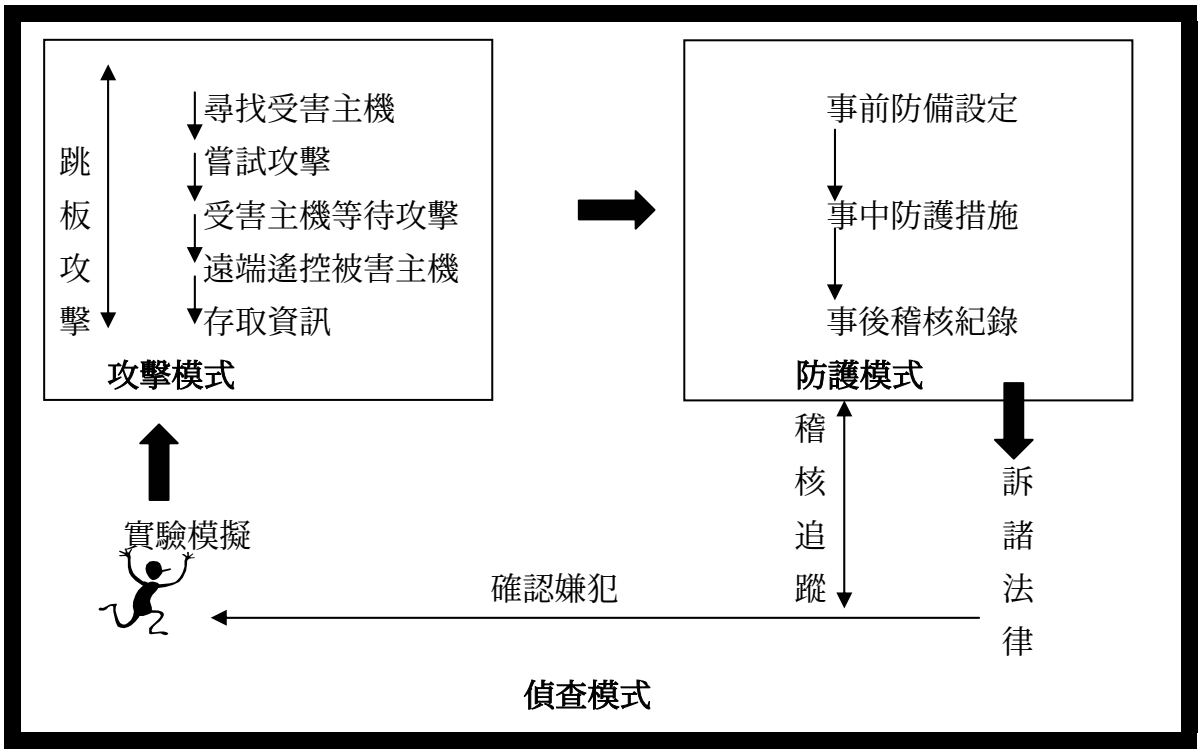
不論是 Trojan Horse、病毒或電腦蟲等惡意攻擊程式，大多有一定的特徵，這些特徵為特有的連續位元識別碼或特定的感染程序方法[1][6][7][12][15]。事實上，不論發作效果如何，其行為勢必影響電腦資產的安全性。對於防護觀念的了解，可先由 Trojan Horse 設計方式來逐一建立。早期 Trojan Horse 的設計需要懂得組合語言才能撰寫此程式，現在藉由易用的程式化工具，可較輕易地寫出破壞性強大的惡意程式，諸如 Trojan Horse。另也因相關感染程序與手法，類似正在運作的系統程式或通訊協定，間接提高 Trojan Horse 偵測發現的困難度。而磁碟作業系統(DOS)或視窗環境(Windows)下並無針對檔案存取做特殊保護，也未內建反病毒的能力，這些不利的環境皆加速了 Trojan Horse 的猖獗。在種種限制之下，截至目前為止，在消極面的防護是以借助額外開發程式或安裝防護軟體才能防衛電腦資產的安全性[2][5][11]。

雖然許多人未注意電腦安全措施，甚至被入侵也不覺得驚奇與害怕[10][8]，但如所屬電腦成為駭客攻擊轉接站，一旦攻擊事件發生，如何讓自己法外於攻擊事件後的相關單位偵查，即為防護觀念重要之所在。也就是說，這樣類似直接或間接轉接被攻擊事件的發生，皆在強調防護必須是建立在使用電腦即需有安全必要的認知上。

參、模式建立：攻擊、防衛與偵查

網路使用者在拜訪網站或下載共享軟體的過程中，可能連帶植入特定 Trojan Horse 而不自知[3][9]，網路攻擊者只要掃描不特定網路網址範圍便可輕易地查出已遭植入的電腦，此時根本不需要額外的技術處理。也就是說，當受害者電腦被植入伺服程式時，其電腦便會開啟某個特定通訊埠等待攻擊者的連線侵入，而這樣的通訊埠並非固定不變，所以，在使用者欲識別是否真有 Trojan Horse 上有其困難度。然視窗型 Trojan Horse 的通訊效果就像主從(Client-Server)架構一樣，只要攻擊者在多方嘗試下，一找到入侵的通訊窗口，伺服端即會提供客戶端所有需要的資訊。在本篇研究中，我們即以一個視窗型 Trojan Horse 的可能攻擊與如何去防制攻擊並進行事後偵查的角度，來為此網路惡意程式

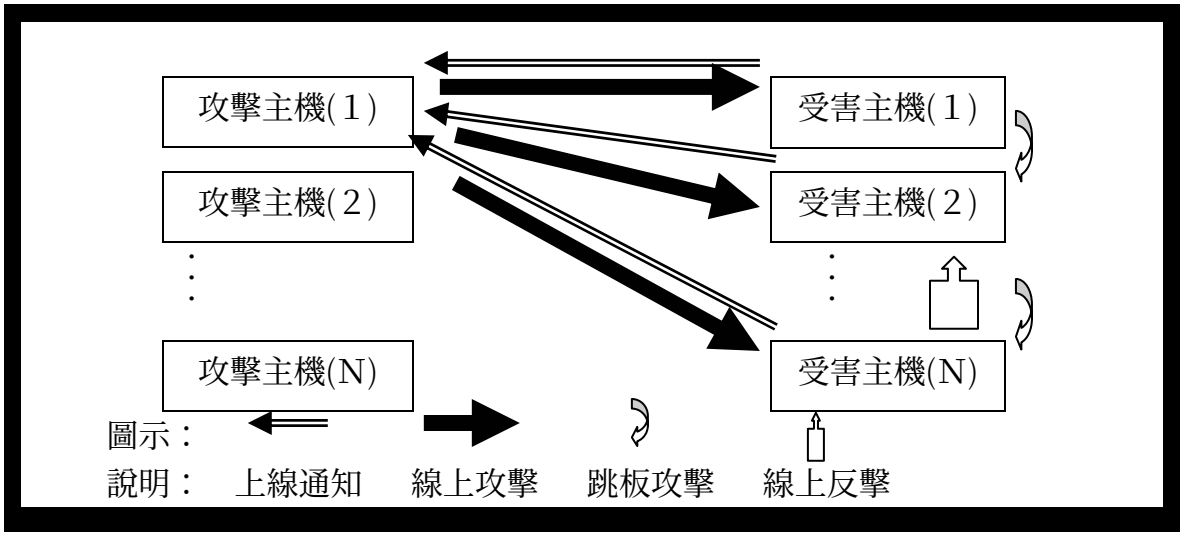
行為建立一個研究機制，並透過如圖一的架構圖來逐一說明我們的研究方向與討論。在圖一中，實驗模式包括攻擊模式及防衛模式，最後依據稽核資料而擬定偵查模式。



圖一：視窗型 Trojan Horse 的研究架構

3.1 實驗模擬

為模擬與解析視窗型 Trojan Horse 的實驗過程，我們建立如圖二的實驗架構圖。在圖二中，主要電腦設備分為攻擊主機與受害主機。攻擊主機嘗試藉由偽裝圖像檔或應用程式合體執行檔等散播途徑，讓不同的受害主機植入不同 Trojan Horse 之伺服程式，因而主動開啟某特定通訊埠，接著即等待攻擊主機的連線侵入。在模擬侵入過程中，單一攻擊主機除使用不同感染手法外，亦使用不同 Trojan Horse 試圖侵入受害主機，以觀察跳板攻擊與線上反擊的實驗效果。藉由此實驗的進行，我們亦嘗試在受害主機採行不同的防衛措施，以研析反制作法的阻絕效果。



圖二：視窗型 Trojan Horse 的實驗架構圖

3.2 模式分析

為清楚解讀不同視窗型 Trojan Horse 的感染效果，在本節中，我們以具有不同特質之 Netspy Trojan Horse (出現較早)、Subseven Trojan Horse (功能較強且使用率較高)及 Birdspy Trojan Horse (國人設計)等三種木馬程式的公開版本為依據，透過實驗過程，從攻擊模式、防衛模式及偵查模式角度，研究視窗木馬程式相關事件的安全鑑別、防制策略與法律追訴[1]。

A.攻擊模式

在攻擊特徵方面，謹就 Netspy 等三種 Trojan Horse 常見的攻擊特徵作一整理、分類與說明，並就攻擊手法的特徵，透過表列方式比較其差異性(如表一)。其中，Netspy Trojan Horse 由於出現較早，謹具備基本的檔案上下傳等遠端管理功能，在攻擊感染手法與方式上較固定單純。至於 Subseven Trojan Horse 因原設計作者為提升攻擊效果，不斷加強功能至新版本中，使得該程式廣受網路玩家的喜愛。最後 Birdspy Trojan Horse 因出現時期較晚，感染原理方面尚未公開，然而在跳板攻擊功能、上下傳檔案、上線通知功能、伺服程式密碼保護、伺服程式大小的變更、伺服程式檔名的多變化及組態設定的多變化方面，則依然延續眾多 Trojan Horse 的特徵。

表一：視窗型 Trojan Horse 攻擊特徵的比較

特徵 / 種類	感染原理公開	跳板攻擊功能	上下傳檔案	上線通知功能	伺服程式密碼保護	伺服程式大小的變更	伺服程式檔名的多變化	組態設定的多變化
Netspy	○		○					
Subseven	○		○	○	○	○	○	○
Birdspy		○	○	○	○	○	○	○

一般而言，如果「感染原理未公開」或「組態設定的多變化」(指通訊埠、處理程序名及啟動設定方式等組態是否提供攻擊者自由性的選擇)出現在 Trojan Horse 的使用上，則移除 Trojan Horse 之程序的困難度便較高。此外，對於 Trojan Horse 版本的提升，一般著重在人性化介面、縮小程式大小或強化攻擊效能等攻擊特徵方面，這些功能的提升往往是 Trojan Horse 作者為掩飾其行為的藏匿作為。但無論如何，舉凡奇怪視窗的出現、電腦日期時間的異常變動、電腦系統的自我啟動、鍵盤或滑鼠的失效或滑鼠被遙控，均為視窗型 Trojan Horse 常見的徵兆，當遇到這些事件發生時，便需要尋求相關的移除資訊，以強化電腦的安全保護措施。

B.防衛模式

為解析前述三種 Trojan Horse 的防衛對策，我們先瞭解如表一之各 Trojan Horse 的攻擊行為特徵後，再觀察啟動與執行期間的通訊方式，以尋求反制發作效果的解決方法。在反制作法上，我們依序採行「避免存取執行 Trojan Horse 伺服程式」、「通訊埠的監看」、「啟動設定的檢核」、「網路狀態的監看」及「處理程序的監看」等防範措施(如表二)，期望確實達成阻斷 Trojan Horse 的攻擊效果。

不過，因為這些程式原始碼的公開化與本身兼具攻擊者自行變更組態設定的功能，造成各 Trojan Horse 的程式檔名、通訊埠、啟動設定及處理程式名稱等內容，不局限於表二中的各已知資料上[14][17]。而藉由識別監控攻擊者入侵方式，保留攻擊者連線資料，除可識別其他可疑變種 Trojan Horse 存在的可能性外，亦可追查連線攻擊之當時使用者，作為未來調查與追緝的參考。藉由本研究機制所提出的「事前防備設定」、「事中防護措施」與「事後稽核紀錄」等三個不同期間之防護檢核措施，在 Trojan Horse 的防制上，應能基本防止不良惡意 Trojan Horse 的侵入行為。

表二：視窗型 Trojan Horse 特徵反制的比較

第一項 反制作法 / Trojan Horse	避免存取執行木馬伺服程式
Netspy	避免 999.exe、procspy.exe 或 xspy.exe 等程式的執行。
SubSeven	避免 server.exe、server2.exe、rundll6.exe、systray.dl、task_bar_exe、FAVPNMCFEE.dll、MVOKH_31.dll,dllnodll.exe 或 watching.dll 等程式的執行。
BirdSpy	避免 winstart.bat、winbmf.scr、papa.exe、smile.exe、netdrv.exe、smile.scr、Netdrv.exe、EasyBird.exe、ems.exe、Netdrv.exe、goofylinux.exe、ems32.exe、wintssb.exe、acklex.exe 或 wintx.exe 等程式的執行。
第二項 反制作法 / Trojan Horse	通訊埠的監看
Netspy	刪除 1024、1033、7306 或 7308 等通訊埠的處理程序。
SubSeven	刪除 1243、1999、2773、6667、6711、6712、6713、6776、7215、16959、27374、27573 及 54283 等通訊埠的處理程序。
BirdSpy	刪除 3576、6200、6789、7891、19999 或 31229 等通訊埠的處理程序。
第三項 反制作法 / Trojan Horse	啟動設定的檢核
Netspy	移除登錄編輯器中之 Run 目錄中 netspy 的登錄鍵值。
SubSeven	移除 c:\windows\Win.ini 中 "load=XYZ.exe" 或 "run=XYZ.exe"、c:\windows\ system.ini 中 "shell=exprorer XYZ.exe"、c:\autpexec.bat 及程式集之啟動設定，或移除登錄編輯器中之 RunServices 或 Run 目錄中 ABC 的登錄鍵值。
BirdSpy	刪除 a1676、doggy20、internetDrv、DefaultScr、InternetDrv、EasyVet、qwer、internetDrv、client、Winsys32、NetKernel、papaya 或 Initail 等登錄鍵值。
第四項 反制作法 / Trojan Horse	網路狀態的監看
Netspy	注意 1024、1033、7306 或 7308 等通訊埠的網路狀態。
SubSeven	注意 1243、1999、2773、6667、6711、6712、6713、6776、7215、16959、27374、27573 及 54283 等通訊埠的網路狀態。
BirdSpy	注意 1219、6789、6200、19999、3576、7890、7891 或 31229 等通訊埠的網路狀態。
第五項 反制作法 / Trojan Horse	處理程序的監看
Netspy	注意 netspy.exe 程式所啟動的處理程序。
SubSeven	注意 server.exe、server2.exe、rundll6.exe、systray.dl、task_bar_exe、FAVPNMCFEE.dll、MVOKH_31.dll,dllnodll.exe 或 watching.dll 等程式所啟動的處理程序。
BirdSpy	注意 winstart.bat、winbmf.scr、papa.exe、smile.exe、netdrv.exe、smile.scr、Netdrv.exe、EasyBird.exe、ems.exe、Netdrv.exe、goofylinux.exe、ems32.exe、wintssb.exe、acklex.exe 或 wintx.exe 等程式所啟動的處理程序。

首先，在「事前防備設定」方面，程序上最好經常性地注意「禁止不明檔案的存取」、「檢查電腦的啟動組態設定」、「檢查處理程序的執行」、「檢核 Trojan Horse 的特徵」、「設定高警戒狀況」及「安裝防護軟體」等六個檢核方式(如表三)，以確保系統資源的合法存取及未中斷的系統運作，提供軟硬體及資料檔案的良好安全防護。此外，藉由防護軟體監看網路狀態外，亦可分析與偵測潛在的攻擊影響，進而產生警告事件的報告資訊，解讀可能的威脅活動。但對於現有個人電腦安全防護軟體而言，大多只能識別已知攻擊方式的入侵警訊，對未知的侵入技巧依然存在不易辨識的現象，也唯有深入解讀 Trojan Horse 的實際感染發作效果，才能有效解決防護軟體識別錯誤的問題。

表三：視窗型 Trojan Horse 的事前安全檢核表

項目	檢核方式	說明
一	禁止不明檔案的存取	來路不明的文件檔(含巨集指令)，圖像檔或執行檔均可能暗藏 Trojan Horse。
二	檢查電腦的啟動組態設定	透過檢查登錄編輯器中之 HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\ Current Version\RunServices\或 HKEY _LOCAL_MACHINE\ Software\Microsoft\Windows\Current Version\Run\目錄、c:\windows \Win.ini、c:\windows\ system.ini、c:\autpexec.bat 及程式集之啟動設定等內容
三	檢查處理程序的執行	透過檢查處理程序方式，關閉不當通訊埠的連結。
四	檢核 Trojan Horse 的特徵	檢視是否存在 Trojan Horse 藉電腦開機時自動執行伺服程式，進而準備接受攻擊指令，如發現應尋找相關資訊，移除該 Trojan Horse。
五	設定高警戒狀況	避免動態網頁的執行，降低內含惡意 Trojan Horse 的潛在危機。
六	安裝防護軟體	隨時監看稽核紀錄，並拒絕來路不明的連線需求。

其次，在「事中防護措施」方面，不論使用何種方式作為檢核 Trojan Horse 的依據，只要是視窗型 Trojan Horse 便會對外通訊，藉由 Pview95 等工具程式可檢查正在執行的處理程序是否有不當或異常的名稱，判斷是否為 Trojan Horse 的執行程序，進而適時移除防止其入侵行為。另亦可透過反組譯編輯軟體檢查是否有奇怪、惡意的字樣(如 Server)出

現，以觀察可疑程式之執行過程中是否存在與外界連通的企圖。為迅速應變、處理與反應突發攻擊事件，最好依序採行「啟動防護軟體」、「Trojan Horse 的掃瞄」、「網路狀態的監看」、「處理程序的監看」、「通訊埠的監看」及「刪除 Trojan Horse 的啟動組態設定」等合宜防堵措施(如表四)，進而阻止 Trojan Horse 的攻擊行為。

表四：視窗型 Trojan Horse 的事中安全檢核表

項目	檢核方式	說明
一	啟動防護軟體	隨時監看稽核紀錄，並拒絕來路不明的連線需求。
二	Trojan Horse 的掃瞄	掃瞄電腦主機中是否存在 Trojan Horse。
三	網路狀態的監看	觀察網路連線對方的身分及執行通訊協定與封包流程。
四	處理程序的監看	透過處理程序的監看，對映是否存在不當通訊埠的連結。
五	通訊埠的監看	觀察是否存在異常通訊埠的開啟。
六	刪除 Trojan Horse 的啟動組態設定	依個別 Trojan Horse 的感染方式，刪除啟動設定。

最後，在「事後稽核紀錄」方面，雖然識別攻擊來源的過程裡，諸如時間、地點、甚而匿名攻擊者身分等資料追查十分困難，但透過事後蒐集分析稽核紀錄方式，依然可歸納研判入侵者的攻擊源，進而了解其企圖、能力與入侵手法。其參考作法上，可依序採行「檢查是否遭受侵入攻擊」、「檢查受損情形」、「檢查稽核紀錄」、「回顧的事件經過」、「電腦系統運作的流程說明」及「復原系統」等檢核措施(如表五)。

表五：視窗型 Trojan Horse 的事後安全檢核表

項目	檢核方式	說明
一	檢查是否遭受侵入攻擊	識別 Trojan Horse 的類型與名稱，以蒐集相關資料，採行合宜處置措施。
二	檢查受損情形	觀察重要資料檔案的現況。
三	檢查稽核紀錄	查看有無異常的刪改紀錄與連線進入。
四	回顧的事件經過	就時間流程做一解後做分類敘述。
五	電腦系統運作的流程說明	簡單扼要地解說相關事件流程。
六	復原系統	移除相關設定及檔案後，從新啟動電腦系統，並加強相關安全措施。

C.偵查模式

偵查程序源起於線索的解析，在入侵事件的追緝過程，稽核資料往往是不可或缺的主要線索，也唯有針對稽核紀錄進行證據蒐集與追蹤的工作，才是緝獲嫌犯的重要成功關鍵。關於此部份，我們將從「訴諸法律」、「稽核追蹤」及「確認嫌犯」等三項程序來解析視窗型 Trojan Horse 偵查模式的施行[1]，茲分述如下：

1. 訴諸法律程序

在決定訴諸法律程序時，首要工作是採集被害證據，由於相關入侵資訊採證不易，案發當時最好能利用工具軟體記錄來源網址、攻擊用帳號、通訊協定、期間、手法、程式及通訊埠等相關稽核資訊，以整理出合宜的入侵事件報表，避免造成事過境遷後未能即時蒐證的遺憾。此外，除了準備這些相關細節文件外，也要有面對煩瑣訴訟程序的心理準備。而在出現視窗型 Trojan Horse 警訊的同時，宜注意相關徵兆的檢核點，查看有無奇怪少見的類似系統檔案名稱，檢視過程中遇有疑難不解之處，可透過網路尋求解答或向資訊專家請求協助，取得被害徵兆的特徵內容，提供檔案資料異常刪改及處理程序啟動 Trojan Horse 的佐證資料，進而確認攻擊事件的發生，提供偵查來源的依據及調查事件分析上的參考。

2. 稽核追蹤程序

因為 Trojan Horse 攻擊態樣多樣化的特質，使得稽核紀錄的誤判率居高不下，常常導致不同採證方式獲得不同觀察結果，不同業者開發的安全防護軟體，也因識別特徵或防護觀點的不同而呈現不同的紀錄內容。在稽核攻擊事件的過程中，可同時採行不同採證工具程式或安全防護軟體，所得綜合結果的真實性亦較為明確。只要細心蒐集與分析稽核紀錄，歸納與研判可疑入侵者的攻擊步驟，可瞭解事件經過問題之所在，進而尋求

改善安全防衛的機制。另外為強化蒐證追蹤的效果，在識別攻擊來源上，應能特別注意入侵者的帳號、密碼、使用程式及通訊埠號碼等資訊，研判攻擊者的攻擊手法、步驟與流程，再依時間經過、攻擊來源、懷疑對象及分項說明等項目內容做一文件化整理說明，作為事後重建入侵流程的模擬參考，將有助於追蹤程序的進行。

3.確認嫌犯程序

因為稽核資料提供訊息並非全然正確，使得確認嫌犯的工作益形重要，視窗型 Trojan Horse 的相關知識及侵入程序非一般人得輕易獲取，嫌犯在進行攻擊行為之前，亦會蒐集一些相關的程式、書籍或文章，以瞭解其運作方式再實行侵入作為，所以，舉凡嫌犯相關之瀏覽器「我的最愛」內容、上網習性、電腦儲存資料、購買書籍、隨手筆記、網站瀏覽紀錄及電腦常識等等，均是驗證嫌犯是否涉案的重要參考依據。

肆、討論分析

近期電腦駭客的攻防與追蹤已成為熱門話題，攻防之間須對電腦系統架構、攻擊程式工具或通訊協定深入了解，才能在執行成效上獲致良好效果[2][18][13]。以下，我們蒐集並列出二個代表性案例，以瞭解視窗型 Trojan Horse 的犯罪手法，透過這些個案方式，也確實驗證我們的防護方法能發揮功效。

<案例一>

民國八十九年八月，刑事警察局查獲苗栗縣三位少年利用別人所開發的 Subseven 及 Netspy 等視窗型 Trojan Horse，以遠端搖控方式侵入他人電腦，取得中華電信數據通信分公司撥接帳號的密碼，在未知會原申請者且未經其同意下以電話撥打中華電信數據分公司撥接代表號方式盜用受害者帳號，使受害者須負擔額外的撥接費用。

<討論一>

在案例一中，為受害者於網路上不慎執行內含視窗型 Trojan Horse 的不明檔案後，電腦系統本身運作並不受影響，致不易察覺其存在，而未施行檢查電腦啟動組態設定及處理程序的防護措施，成為攻擊者的侵入目標。如果受害者定期監看網路狀態、處理程序及通訊埠，便能提早發現 Trojan Horse 的存在，並阻止此一透過下傳檔案攻擊特徵侵入事件的發生。在反向追蹤的過程中，由於被害者在案發期間安裝 Lockdown 個人電腦防護軟體，才能依據稽核資料做後續的追查工作。依此案例，我們可知異狀的觀察與防護軟體的安裝，相當助益於 Trojan Horse 入侵後的查緝工作。 ■

<案例二>

民國九十年一月 Birdspy Trojan Horse 作者因販賣及散佈 Birdspy Trojan Horse 給網路使用者進行遠端侵入的攻擊，遭我國政府之執法機關依違反刑法毀損罪移送，另外原作者亦在試用版本中藉由線上通知方式知悉攻擊者的所在網址，讓程式作者可透過暗藏的後門程式及萬用密碼進入攻擊者的電腦[4]。

<討論二>

此 Birdspy Trojan Horse 在特徵上與其他 Trojan Horse 類似，亦具備前述的跳板攻擊功能、上下傳檔案、上線通知功能及伺服程式密碼保護等特徵，但未使用較特殊的感染啟動設定。只不過為了降低被查覺的機率，將啟動的檔名、處理程序名及通訊埠的內容上，予以個別設定且編譯成執行檔後售給購買者使用，這也使購買者得以專用獨一無二的 Trojan Horse。另外由於 Birdspy Trojan Horse 的使用率不高，部分安全或防毒公司尚未

列入防護對象，使得目前現有的安全防護軟體及防毒軟體尚無法完全阻檔其攻擊，因此此種 Trojan Horse 更淪為網路駭客攻擊的新利器。不過藉由本文所提出的監看網路狀態、處理程序及通訊埠等防制作為，還是可以查覺此一異常程式的存在。

伍、結論

本研究藉由實驗觀察提出視窗型 Trojan Horse 的攻擊特徵，並解析反制與防護的方式，透過實驗與案例討論，我們的防制模式確實可有效監測現有視窗型 Trojan Horse 的攻擊威脅，並緝獲可能攻擊者。即使面對變種 Trojan Horse 依然具備啟動載入執行及對外通訊等特性，只要經常性備份重要資料，刪除來路不明的處理程序，並時時檢核系統啟動設定、網路狀態、處理程序、通訊埠、相關目的網址等電腦主機所有對外的通訊狀況，再觀察異常處理程序之源頭與執行狀態，必可辨識出異常程式之存在。本論文研究期能讓一般電腦使用者與資訊檢疫人員(例檢警單位、專業資訊人員)，在實際面對視窗型 Trojan Horse 的入侵案件時，均能了解防制網路安全所需的觀念與標準程序，並在適當時機實行合宜措施，阻絕不法人士的違法侵害。

參考文獻

[1] 高大宇，”網路駭客與惡意程式入侵之偵查研究”，中央警察大學警政研究所論文，2001：頁53-88。

[2] Anonymous,*Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*,Second Edition,1998.

[3] Bruce, S.,”The Trojan Horse Race”,*Communications of The ACM* ,Vol. 42. No.9 .1999:p 45.

[4] Chiu, J.,”Birdman’s Happy Coding”,http://go.to/birdman/

[5] Cusumano,M. and Selby,R.”How Microsoft Builds Software”, *CACM,* 40,6,1997:pp.53-61.

[6] Denning, E.D.,*Information Warfare and Security*,Addsion- Wesley Longman.Inc.1999.

[7] Denning, E.D. and Denning, P.J.,*Internet Besieged-Countering Cyberspace Scofflaws*,Addison Wesley Publications,1998.

[8] Donn, B.P.,*Fighting Computer Crime-A New Framework for Protecting Information*,Wiley Computer Publications,1998.

[9] Doshelp Intrusion and Attack Reporting Center,http://www.doshelp.com/trojanports.htm,2001.

[10] Douglas, T. and Brian D.L.,*Cybercrime-Law Enforcement ,Security and Surveillance in The Information Age* ,Routledge Publications,2000.

[11] Edward, W.,*Information Warfare Principles and Operation*s,Artech House Publications,1998.

[12] Eoghan, C.,*Digital Evidence and Computer Crime-Forensic Science*,Computer and The Internet,Acadenic Publications,2000.

[13] Grabosky, P. and Smith, R.G.,*Crime in Digital Age:Controlling Telecommunications and Cyberspace Illeagalities*, Thunder’s Mouth Press,1997.

[14] Graphics Accelerator Trojan Horse/Virus Alert, http://www.utexas.edu/cc/ds/alerts/ga_trojan.html, 2001.

[15] Kenneth, S.R.,*High-Technology Crime-Investigating Cases Involving Computers*,KSK Publications,1996.

[16] Remote Control PC 2000,"The Most Powerful PC Monitoring Software on the Internet ,Formerly Known as NETSPY”, http://www.shopsandstuff.co.uk/netspy/rpc.html,2000.

[17] Subseven Official Website,http://www.sub7files.com/faq/general.shtml,2000.

[18] Taylor P.A.,*Hackers-Crime in the Digital Sublime*,Routledge Press,1999.