從 Code Red 癱瘓學術網路看校園網路主機管理問題

陳伯榆
國立中正大學電訊傳播研究所
g8837001@ccu.edu.tw

摘要

Code Red 在今年 8 月蔓延全球，衝擊網路相關服務，更讓台灣相關主機數量登上受害國家第四名，不僅僅是民間 ISP 業者受害，當然也包含了台灣學術網路（TANet），讓網路主要節點的呈現癱瘓的問題。更麻煩的是 Code Red 變種所夾帶駭客後門，更讓資訊網路陷入更大的危機中，在本篇文章將不去深究 Code Red 的入侵與破壞技術，而是從這次的事件中，發現幾個重要的問題，需要被充分的提出討論，包含：一、Code Red 事件所突顯出新的網路安全問題。二、校園管理網路主機架設的制度結構問題及其改善建議。三、則對這段混亂時期，對主機架設管理的建議，來彌補整體大環境不足的缺陷，作為本篇文獻的三個主軸。來達到整體提昇網路安全的目的。

Keywords: 網路主機管理、網路安全、稽核分析、資訊安全素養、Code Red.

1. 前言

Code Red 及其變種在今年 8 月陸續在台灣引爆，使得台灣在 Code Red 傷害下成為全球排名第四的嚴重受害地區，僅次於美國、韓國與中國大陸[1]。攻擊的對象不單是台灣學術網路也包含了台灣整個基礎網路環境。就以筆者 HiNet ADSL 固定 IP 網路為例，在 8 月 6 日至 8 月 7 日 AM8:00 經防火牆相關機制攔截下的封包高達 70 多萬次而且以 http port 80 的封包佔絕大多數。攻擊來源遍及民間 ISP 以及部分國外主機。經過反向追蹤以及 OS 和服務辨識，Win 2k 與 WinNT 的 IIS 為攻擊環境，而且快速的蔓延，並可以從相關稽核紀錄檔，明顯發現每部主機會多次發動搜尋與入侵程序，甚至部分主機遭到駭客入侵更改網頁渾然不知。沒有被入侵並不代表就不受到傷害，從流量紀錄發現 512K 的 ADSL 迅速降至 100 多 K 有時更低至 50k。經過反映似乎 ISP 業者也束手無策。反觀台灣學術網路，也嘗受到 Code Red 的苦果，而各校部分 Router CPU 也都滿載到 100% ，不堪負荷的 Router 終以當機回應，變相佔用絕大多數網路系統資源，在 8 月份教育部電算中心不得不對相關學術網路節點提出警告並行文各校公佈有問題的主機，但 Code Red 迅速蔓延最終還是癱瘓部分學術網路節點。其實在問題發生後，網路上已經有相關技術報告與修補工具的提供下載[2]，以技術來處理 Code Red 的問題，但是並不代表問題全面性的解決，所以本篇文獻將不去深究技術方面的資料，而以行政管理的角度去分析。但是還是要基本分析一下 Code Red[3]的技術環境，才能去說明解釋所提出的觀點。本文分為：第一、將粗略描述 Code Red 入侵與追蹤。第二、分析 Code Red 所造成的新的風險與擔憂，以及對校園網路建置的挑戰。第三、再以校園網路為核心，指出目前校園網路的幾項網路管理問題，希望提供網路管理單位或各院系所管理電腦網路時的參考。

2. Code Red 的入侵與追蹤分析

2.1 入侵與攻擊方式

Code Red 是一種自我繁殖的惡意程式碼，可以從 Code Red 的 Code Red Disassembly 技術文件發現。最新變種的 Code Red 可以附掛上相關駭客後門或病毒，包含三部分：感染、繁殖、安裝木馬三個程序，依照 CERT 安全通報 CA-2001-13 原型是透過 Buffer Overflow In IIS Indexing Service DLL 方式進行[4]，但是新變種 Code Red C 也從感染的主機先取得轉址函數，繁殖在子網域中透過隨機不斷嘗試送出測試封包，經由 TCP PORT 80 來尋找 WIN 2K 或是 WINNT4 的 IIS5 環境，入侵後植入後門，檢查"Code Red II" atom 是否已置入，來確定此主機不會被重複感染，接著進入休眠狀態，非中文系統，Code Red II 休眠 1 天；如果是中文系統，Code Red II 休眠 2 天，重新啟動留下後門。並設入 IP_STORAGE 變數，Code Red II 會檢查當前時間是不是小於 2002 年或小於 10 月。若超出前述條件，則重啟系統，使 Code Red II 的活動不會超過 10 月 1 日，Code Red II 選擇下一個要連接的主機 IP 的方

[1] 廖敏如，聯合報：紅色警戒二號發威台灣受災全球第四，2001/08/11：http://udnnews.com/NEWS/INFOTECH/INTERNET/412489.shtml

[2] 微軟公司所提供的修補軟體。http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

[3] 文中所提的 Code Red 包含原型以及其最新變種 Code Red C 都通稱 Code Red

[4] TW-CA-2001-101-[CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL：http://www.cert.org.tw/advisory/200107/TW-CA-2001-101.txt

法。它首先在 1 到 254 的範圍內隨機生成 4 節避開 IP 地址為一個 0 或 255。[5]接著則是將後門載入所入侵的主機，當取得 SYSTEM 系統目錄 C:\WINNT\SYSTEM32 後，便把 cmd.exe（命令提示字元）複製以及更名到 WIN2K 或 WINNT 的 C:\INETPUB\SCRIPTS\ROOT.EXE 中（圖 1）

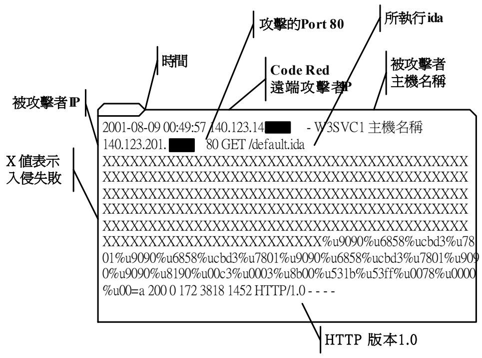
圖 1、Code Red II Disassembly Code

```
seg000:00000831  E8 1C 00 00 00        call   CREATESCRIPTSROOT ; pointer to this inetpubscript string
seg000:00000831                        ; [illegible]?
seg000:00000836  64 3A 5C 69 6E 65+aDInetpubScript db 'd:\inetpub\scripts\root.exe',0
seg000:00000852                        ; [illegible]?
seg000:00000852
seg000:00000852                 CREATESCRIPTSROOT:                ; CODE XREF: sub_1C4+66D   p
seg000:00000852  8B 0C 24          mov    ecx, [esp+44h+HMODULE_WS2_32]      ; pointer to this inetpubscript  string
seg000:00000855  88 19                 mov    [ecx], bl  ; set   first char to letter
seg000:00000857  8D 85 5C FE FF FF     lea    eax, [ebp+HOST_BUF] ;   Load Effective Address
seg000:0000085D  50                    push   eax
seg000:0000085E  FF 55 DC              call   [ebp+CopyFileA] ; copy cmd.exe to [ckl]:\inetpub\scripts\root.exe
```

（資料來源：eEye Digital Security 所公佈 Code Red II Disassembly 技術文件）

將 cmd.exe 複製更名到 C:\PROGRA~1\COMMON~1\SYSTEM\MSADC\ROOT.EXE 就可以執行 Unicode 入侵指令。接著建立 Explorer.Exe，為了是想利用微軟所公佈的另一個安全漏洞 MS00-052(http://www.microsoft.com/technet/security/bulletin/MS00-052.asp) 來進行入侵。[6]而請清除或修補完相關升級程式後，還是需要觀察是否真的完全修護或者只是休眠，另外後門是否被開啟或植入更多新的後門，簡單的說當 root.exe 被植入後，駭客可植入其他的後門作備用，實在防不勝防。況且但是這樣的攻擊不侷限於 WIN IIS5 凡是開放 PORT 80 的 WWW 伺服器都會留下相關干擾紀錄（圖 2）。

圖 2、Code Red 干擾紀錄



（資料來源：國立中正大學電訊傳播所網站 http://140.123.201.2，2001）

對於英文版的 WIN 2K 或 WINNT4 系統則會竄改網頁成為 HELLO! Welcome to http://www.worm.com! Hacked By Chinese! 的內容，以及留下入侵紀錄。而且網頁內容是被寫入在記憶體中，無法在硬碟找出相關文件，所以在.ida 可以在 memory 找到相關紀錄（圖 3）。[7]

圖 3、Memory Record

```
Code Red memory
<MORE 4E 00>
4E 00 4E 00 4E 00 4E 00
4E 00 4E 00 4E 00 4E 00
4E 00 4E 00 4E 00 4E 00
92 90 58 68 4E 00 4E 00
4E 00 4E 00 4E 00 4E 00
FA 00 00 00 90 90 58 68
D3 CB 01 78 90 90 58 68
D3 CB 01 78 90 90 58 68
D3 CB 01 78 90 90 90 90
90 81 C3 00 03 00 00 8B
1B 53 FF 53 78
```

（資料來源：eEye Digital Security）

Code Red 入侵時也會取得 Local System security context 的權限，進而控管主機。對某些區域網路 Router CPU 會產生高負載，而易造成類似 DDOS 的阻斷服務。使得進行網頁瀏覽速度變慢，或無法連結其他網站的現象，可以從封包輸出輸入的流量紀錄察覺出來。

2.2 追蹤分析與補救措施

從相關稽核紀錄資料去分析，可以發現相關干擾源絕大多數來自同區域的 B Class 佔其多數，所以排除 B Class 同區域的 Code Red 是維繫該區域網路與對外網路順暢的重要手段，在網路上 www.eeye.com 目前提供了 Code Red Scanner 作為追蹤工具[8]（圖 5）。

圖 5、Code Red Scanner

No.	Server	Banner	Result
1	211.75.241.37	Apache/1.3.12 (Unix) (Red Hat/Linu...	Not tested.
2	211.75.241.41	Apache/1.3.19 (Unix) (Red-Hat/Linu...	Not tested.
3	211.75.241.56	Apache/1.3.14 (Win32)	Not tested.
4	211.75.241.58	Microsoft-IIS/5.0	Not vulnerable!
5	211.75.241.47	Microsoft-IIS/5.0 感染 Code Red →	VULNERABLE!
6	211.75.241.69	Microsoft-IIS/4.0	Not vulnerable!
7	211.75.241.85	ZOT-828/2.01	Not tested.
8	211.75.241.60	Microsoft-IIS/5.0 感染 Code Red →	VULNERABLE!
9	211.75.241.46	Microsoft-IIS/5.0	Not vulnerable!
10	211.75.241.171	Apache/1.3.12 (Unix) (Red Hat/Linu...	Not tested.
11	211.75.241.65	Microsoft-IIS/5.0 感染 Code Red →	VULNERABLE!
12	211.75.241.185	Apache/1.2b7	Not tested.

（資料來源：www.eeye.com Code Red Scanner testing）

可以發現都是針對微軟 IIS5.0 版本的服務漏洞所造成。接著必須先將 WIN 2K 或 WINNT 4.X 主機先安裝 Service Pack 才能安裝修補 Code Red 的程式碼；或是使用微軟公司也提供了 Code Red Cleanup，但是微軟的 tool 僅將 IIS5.0 的 WWW 服務關閉而已，是一種治標不治本的做法。單是這樣是不夠的，因為新型的 Code Red 變種，可以順便植入相關駭客後門，例如：搭配 Unicode 使用的 cmd.exe 轉換 root.exe 等命令提示指定於開放的攻擊位置或載入 Explorer.Exe，透過將 cmd.exe 改名存放於 Inetpub / Scripts 目錄之下。所必需要再仔細的檢測自身的主機的安全漏洞的修補才能有效抑制駭客後門。再這裡提供一個一般網路主機管理的

[5] Code Red II 分析報告 http://www.eeye.com/html/advisories/coderedII.zip

[6] 可以參考 www.eeye.com 所公佈的 Explorer.exe Disassembly

[7] http://www.eeye.com/html/Research/Advisories/AL20010717.html

[8] Code Red Scanner from eEye Digital Security：http://www.eeye.com/html/Research/Tools/codered.html

的有效工具 twwwscan[9]它可以檢測出相關系統的安全漏洞並產生紀錄當作為修補漏洞所使用（圖 6），唯一可惜的是對 FrontPage Extension 漏洞無法做檢測，更建議不應該用在駭客攻擊使用上。

圖 6、 twwwscan 所產生的 log 檢測紀錄

（資料來源：search.iland.co.kr/twwwscan 的檢測紀錄）

再透過手動的步驟來刪除後門:

1) 必需刪除 C:\exploer.exe 和 D:\exploer.exe。而這兩個程式都被改成隱藏和唯讀屬性。先要將所有文件設定為"顯示所有文件"才能看見。

2) 刪除 \inetpub\scripts\root.exe 和 \program files\common files\system\MSADC\root.exe 在【執行】命令區執行 regedit，尋找 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots 將"/C"和"/D"的項刪除，並將"/scripts"和"/MSADC"項中",,217"改成",,201"

3）HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WinLogon 的 0FFFFFF9D 值改回 0。

4）如果自己也沒把握是否還有其他後門，重新建立新的 OS 環境以及修補相關漏洞是最安全做法。

3. Code Red 所造成的的風險與擔憂

3.1 新型態的整合攻擊模式

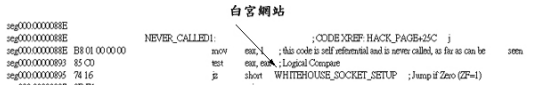
Code Red 的誕生，代表了一個全新的網路風險時代的開始，在駭客的攻擊行為，多半先探測主機系統的基本環境與試探漏洞，或以此漏洞進行 DDOS 阻斷服務來進行駭客手法；而病毒多半是使用者被執行或載入而發生傷害，可是這次的 Code Red 卻是結合了病毒的活動方式、駭客的後門植入、以及 DDOS 阻斷服務的綜合體方式來運作，更將作業系統與網路服務漏洞徹底的結合，是值得擔憂的問題。Code Red 的自我偵測自我複製的機制，將嚴重干擾到資訊網路服務的運作[10]，而且在往後也可能發展到其他作業系統。需要國內外資訊網路安全專家特別注意，當服務被阻斷、主機被入侵、或像病毒般的蔓延，這樣的損失將非常慘重。更麻煩的是，傳統駭客可以被相關防火牆作適度嚇阻，但是由軟體自身產生的攻擊入侵行為將難以追查，因為很難找出源頭，除非入侵的紀錄被 trace 否則對目前消極資訊犯罪防範機制將是一種挑戰。就以這次 Code Red 事件為例子，進行攻擊的遠端主機本身可能也是受害者，所以去反追蹤駭客攻擊的源頭就很困難，不像是單一駭客入侵，偏偏 Code Red 變種卻可以提供駭客後門，實在防不勝防。更嚴重的是當我們將 TCP Port 80 停用，相對的我們也宣告我們網站服務停擺，即使透過 DNS 來限定特定 PORT 作為 WWW 服務使用，也將有礙資訊服務的流通。另一方面 Code Red 所進犯的系統漏洞還在，無疑更加深主機服務的風險，況且主機的漏洞何只一處，如果都以 Code Red 方式進行，對網路服務是一個很大的危機。

3.2 網路服務的全面性癱瘓新社會問題

在 3.1 已經描述了 Code Red 所帶來的風險，若將這樣的風險轉換到下列層面。

3.2.1 國家安全的問題：已經可以達到資訊戰癱瘓網路的功能，與原先網際網路建立時的繞址或難以毀滅有著很大的差異。就以學術網路的癱瘓來看，其實已經干擾到相關研究計劃的進行以及資訊的流通。以 Code Red 原型為例子，就被設定攻擊癱瘓特定網站[11]（圖 7），若 Code Red 被輕易修改攻擊目標，就可以達到完全癱瘓的目的。

圖 7、Code Red 原型攻擊特定網站



（資料來源：eEye Digital Security 所公佈 Code Red Disassembly 技術文件）

3.2.2 商業資訊科技發展的危害：e 化的政府或商業活動已經成為國內重要的改革，許多企業多半使用 ITC 作為營運的核心，當資訊科技反成為入侵、竊取資料、癱瘓運作的武器時，商業上所蒙受的損失將難以估計，而檢視電信網路基礎建設的產業，大量負載的頻寬，除了降低客戶的信任外，本身因租用線路的成本也相對增加，所以網路 ISP 或電信業者必須有管制能力來解決這類的問題

3.2.3 網路秩序的混亂：拿 8 月份 Code Red 蔓延的窘境，讓相關網路管理單位呈

[9] http://search.iland.co.kr/twwwscan/

[10] 台灣賽門鐵克電腦病蟲通報紅色警戒變種病蟲 CodeRed.v3 (CodeRed.C)：http://www.symantec.com/region/tw/avcenter/vinfo/codered.v3.html

[11] 被設定攻擊白宮 http://www.eeye.com/html/Research/Advisories/AL20010717.html

現混亂的狀況，各大區網中心單位不分國內外都貼出公告，即使對岸中國大陸也不例外[12]，向瘟疫般一發不可收拾，這樣的態勢對於國內資訊技術轉型的發展上規劃必須加以修定。只會使用或半調子的主機架站者，是目前網路混亂的根源，全面性提昇資訊安全的素養，將和提昇資訊素養一樣重要。所以這類管裡者兼具「權利意識薄弱群」「受害意識薄弱群」的特質，[13]也是造成網路安全更混亂重要因素。

4. 目前校園網路的幾項網路管理問題與建議

網路的管理在各區網管理結構大環境下，有著不一樣的成效，而且不同的網路服務目的，也有著不一樣處理態度，就以民間 ISP 業者與學術網路相比就有各自處理網路危機的問題，所以選擇將這樣的危機限制在學術網路下校園網路內來看管理問題，並提出建議。其理由有以下各點：1、有完整的通報追蹤管制體系。2、學術網路各大節點有較完備的設備與技術人力。3、相關紀錄與追蹤環境較民間 ISP 完善。4、學術網路相關技術升級規範能力較優於民間 ISP，且具備獨立管理能力。所以以此為核心提出建議並去分析校園網路內的主機管理或網路建置的環境。

4.1 目前校園網路主機管理的問題

4.1.1 校園 IP 與主機架設管制鬆散：

在學術網路的架構下，各校都有自身的規範與管理模式，通常主幹或重要 SUB-NET 由資訊中心所掌控，而分配給各系所單位的次 CLASS 則由各系所單位所控管。這次 Code Red 蔓延控制不佳的關鍵，就是在於所下放的 IP 分配管理上，各系所無法掌握所擁有主機數量與類型，而無法有效抑制阻絕 Code Red 的蔓延，其隱藏其中的問題包含了架站軟體或技術取得容易，不需經過通報管制，讓相關資訊中心疲於奔命。各系所自身建置的電腦教室或機房，專責管理人員缺乏，更加深學術網路的 Code Red 至今無法有效控管。而這類私設的站台，排除學術用途，多少因藏著許多問題。如：地下 FTP 站台、非法商業性網站…等。

4.1.2 Router 對於策略性管制機制建立不足

當前一小節的先天失調的大環境下，還有的機會補強的方式，就是對 Router 做更嚴格的規劃與管理，雖然 Router 若搭配相關管理介面的設備十分昂貴，但是透過 Router 管制搭配相關防火牆機制，可以暫時阻絕有問題主機的流動，或面對校外大量封包湧入時，為維繫服務，可以限定進出的管制策略，來分攤學術網路處理問題的時效。換言之，可以先將 Code Red 所進犯的 Port 80 先阻決於外，在逐步清除校園內受到入侵的主機。可惜的是目前鮮少看到校園對於 Router 作最佳化的利用，或建立 Router 管制策略[14]。這是最可惜的地方。

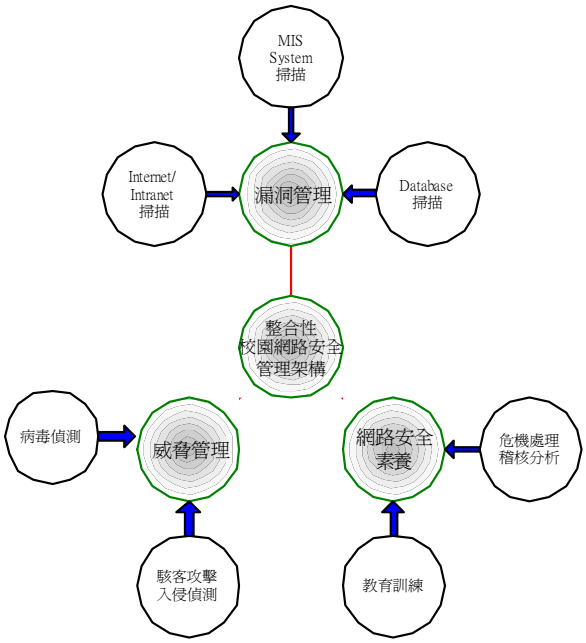
4.1.3 防火牆與校園稽核體系無統籌規劃

雖然防火牆無法絕對的杜絕所有網路安全問題，卻能達到一定的阻絕功效，但是一套兼具防毒防火牆實在非一般系所單位所能承擔，可是主管校園資訊網路安全單位是責無旁貸的責任。到底目前學術網路類的整合性防或牆機制多少已經建立，是一個問題。但是都不建立，端靠主機管理者的防範是在危險，由校方統籌管理將比起零散建立相關機制更為有效。另外校園稽核紀錄的分析管理也是一個關鍵，雖然學術自由與隱私權問題不絕於耳，但是相關損失的輕重必須要有所權衡，不妨建立分析管制的機制與原則，加以利用稽核紀錄可以有效了解相關網路問題的來源或提供管理結構上的調整。

4.2 對管理制度上的建議

歸納上述相關問題整理出下列建議事項，作為管理制度調整上的參考，如下：（圖 8）

圖 8、整合性管理制度



（資料來源：研究整理）

4.2.1 建立整合性校園網路安全管理架構：

包含三個部分：1、威脅管理。2、漏洞管理。3、網路安全素養。相關資訊設備採購或是防火牆防毒系統引進都只是片斷分散的考慮。必須從相關危機經驗中建立符合自身校

[12] 北京大學公告，關於防範 IIS 紅色蠕蟲病毒 Code Red II 的緊急通知：http://www.pku.edu.cn/~zhp/codered/codered.html

[13] 宋振華、楊子翔、樊國楨，資訊系統入侵與偵防技術簡介。TANET2000：成功大學。2000

[14] 詹嘉隆（2000）：《網際網路接取路由器之差別化服務之實現》。國立中正大學電機工程研究所碩士論文。

園需要的資訊網路安全管理流程。例如：當危機發生時，如何從資訊流、設備運作和人員調度的面向妥善操作。簡單的說，就是將相關 ITC 的硬體設備，人員運作置於最適合的位置。例如：Router 的策略性管制技術的建立、建立全校性規劃責任在校園資訊中心，但是系所單位都需要全力配合。此外，平時就針對相關網路安全漏動作掃描與修補，以及對病毒或駭客異常活動進行追蹤通報，對於防火牆與防毒系統作定期的更新與升級。再配合相關資訊素養的提昇，最少可以降低其風險。

4.2.2 建立分工的網路主機架站通報機制，便於聯繫、訓練、維護管理

這一點才是 Code Red 危機中需要大幅改善的問題，校院校系所都需要全面性檢討 IP 與主機架設的設計與規劃，因為有完整的紀錄，才能讓相關資訊管理者在最快的時間內完成修護與阻絕，總比現在在 BBS 板上大聲疾呼哪一個 IP 被入侵或攻擊其他主機來的有效。[15]雖然這次受害的主機為 WIN 2K 以及 WINNT IIS5.0 但是不論所架設主機為何種類型，都必須定期要求相關主機負責人接受教育訓練課程，或建立獎懲制度來抑制不安全的網路主機的存在。其次建立學院或系所需要建立自身的管理模式，例如：建立專責的技術管理人員。再去搭配全校的網路安全架構才能有效降低網路安全風險的辦法。至於是否嚴格管制 IP 則端賴各院系所管理機制來訂立，但是通報網路主機架設狀況是維繫網路安全管理必要處理的過程。

4.3 對於校園內主機架設者的建議

這樣的建議，其實是老生常談了，但是還是要一再的叮嚀，在校園網路安全整體制度面還未建立時，主機管理者的警覺性與責任心，是面對管理制度未迨時刻的保全手段，不只是過渡時期的參考，更是要持之以恆的管理原則，每次筆者在掃描區域網路時，總會發現久未升級修補的主機，這類主機將是網路安全的不定時炸彈，許多研究計劃結束了，而主機閒置在哪，還不如選擇關站或固定修補，一來不會成為攻擊的跳板；二來不會成為被入侵的對象。有哪些面向需要注意呢？列舉如下：

4.3.1 注意電腦網路安全通報與漏洞修補

網路主機管理者要隨時注意相關安全漏洞與病毒通知，依自身主機系統類型去修補，國內可以到台灣電腦網路危機處理中心 http://www.cert.org.tw/，或國外主要安全通報機構 http://www.cert.org 注意安全通告，以及到各作業系統公司，如：微軟的 http://www.microsoft.com/technet/ 。小動作卻能確保主機安全。

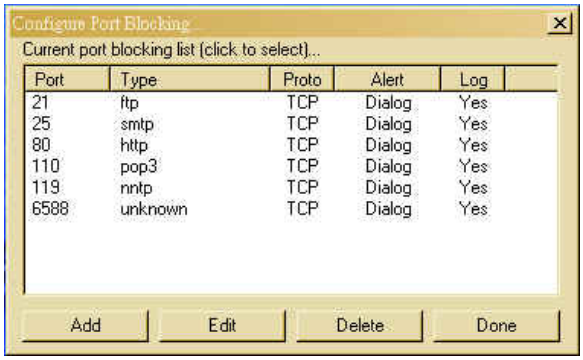
4.3.2 管理者必須熟捻網路相關技術規範，便於手動調整

這是一個關於資訊安全素養的重要問題，主機管理者往往無法面面兼顧，使得整體的技術無法提昇，例如再發生危機時，若有充分的網路或系統技術，就可以適度以手動方式提昇主機的基本防禦能力，諸如熟悉 TCP/IP 的相關協定與架構、系統的設定值、或相關網路服務設定的修改…等。

4.3.3 架設自身安全機制，阻絕、關閉不需要的服務

透過修改系統設定值或使用相關工具軟體，關閉不必要的服務與通訊埠（圖 9）或對特定網域服務作限制，例如：限制可以 ACCESS 的遠端 IP，這是另一種維繫主機安全的方式。

圖 9、關閉阻絕不必要的通訊埠



（資料來源：Port Blocker：http://www.analogx.com）

4.3.4 隨時注意稽核紀錄的狀態與追蹤回應

這是一個比較消極處理方式，也是確保祝基安全的重要紀錄，話說回來高階的駭客或許可以清除相關的稽核紀錄，但是管理若能有效的調整或加設相關稽核機制，也不失一種回溯追蹤的方式，雖然有些技術可以匿名攻擊，但是面對這類的目前問題總是少數，透過稽核紀錄（Access Log）[16]才有助於主機管理者作調整，或通報校園資訊中心做出處置。對其他單位的主機也是一種保障。

5. 結論

在這次 Code Red 癱瘓校園學術網路的事件中發現，沒有建立一套分工的網路主機架站通報機制，是目前最嚴重的缺失，也讓目前 Code Red 延續至今遲遲未消退主因，問題不外乎遍尋不到主機的位置與管理者，只能在 BBS 上通報，或通知系所單位時，總問該如何處理的窘境，更突顯出校園網路安全機制的不健全，使得處理 Code Red 問題呈現混亂的場面。反觀民間 ISP 相比發現，相關網路安全技術人員更是極度缺乏，多半集中在重要機房，使得區域機房無法解決，都是急待改善的問題。希望經歷過近一週的混亂場面，可以讓相關校園資訊部門有所思考，適度的管制將有助於問題的解決，也是公平維繫學術網路多數一般使用者的權益，不讓少數不良的主機管理阻斷多數使用者的權利，更可以降低事後處理的困擾。

[15] telnet://bbs.ccu.edu.tw 電算中心版

[16] David Hughes，Have I Been Hacked?：Sys Admin. Auguest 2001, v10, no:8

6. 參考文獻

[1]、廖敏如，聯合報：紅色警戒二號發威台灣受災全球第四，2001/08/11

[2]、微軟公司的修補報告。
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

[3]、TW-CA-2001-101-[CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL：
http://www.cert.org.tw/advisory/200107/TW-CA-2001-101.txt

[4]、Code Red II 分析報告
http://www.eeye.com/html/advisories/coderedII.zip

[5]、台灣賽門鐵克電腦病蟲通報紅色警戒變種病蟲 CodeRed.v3,http://www.symantec.com/region/tw/avcenter/vinfo/codered.v3.html

[6]、北京大學公告，關於防範 IIS 紅色蠕蟲病毒 Code Red II 的緊急通知：
http://www.pku.edu.cn/~zhp/codered/codered.html

[7]、宋振華、楊子翔、樊國楨，資訊系統入侵與偵防技術簡介。TANET2000：成功大學。2000。

[8]、詹嘉隆（2000）：《網際網路接取路由器之差別化服務之實現》。國立中正大學電機工程研究所碩士論文。

[9]、http://www.analogx.com

[10]、http://www.cert.org

[11]、telnet://bbs.ccu.edu.tw

[12]、David Hughes，Have I Been Hacked?：Sys Admin. Auguest 2001, v10, no:8