郵件病毒與廣告信防治實作

黃國鈞 劉立美
苗栗縣教育網路中心 台中縣新社鄉協成國小
panda@mlc.edu.w ohaha@pchome.com.tw

摘要

網際網路的蓬勃發展，帶來了無限的商機，也衍生出了無窮境的病毒及非授權商業信件(UCM)的困擾。要防治未授權商業廣告信件或郵件病毒有不少商業化的軟硬體，但所費不貲，不是一般學校所負擔得起。

本篇文章提供了免費且有效的解決方案，透過 MailScanner[1]搭配 ClamAV[2] 、SpamAssassin[3]，有效解決困擾使用者多年的郵件病毒及廣告郵件的嚴重問題。

關鍵詞：spam、virus、MailScanner、ClamAV、SpamAssassin

1. 前言

年前苗栗縣建立網擎(openfind)mail2000 郵件系統[4]提供網頁式收發信件及防毒功能的信箱，頗受好評，是各校限於經費考量，並沒有多餘的費用能夠購買防毒模組，只建立有基本的郵件收發功能郵件伺服器，沒有防毒功能，更不用說防治廣告信件了，只能透過不停的教育宣導讓中毒機率降低，但成效有限，病毒信件及網告信件仍是讓各校困擾不已的嚴重問題。

2. TANet 現行郵件系統比較

將 TANet 各連線單位現行且常用的郵件系統條列進行分析比較，如下表 1

這些在 TANet 連線單位常見到的郵件系統種類，依照難度及優缺點分析縣市網路中心使用網擎商業版(苗栗縣網、台北市網、宜蘭縣網等。)和搭配 procmail[5]的進階郵件郵件系統(雲林縣網、苗栗縣網、台南縣網等。)，中小學則限於經費或網管教師技術問題，多使用網擎教育版系統[6]或是 OpenWebmail 系統[7]，部分單位仍維持最基本的郵件系統。

但不論是 OpenWebmail 或是網擎商業版本都不是我們最好的考量。站在節省國家經費及網管維護人力考量，建議的解決方案為 MailScanner 搭配 ClamAV 及 Spamassassin：

2.1 Mailscanner + ClamAV + Spamassassin 系統

此系統可以將郵件內容含附加檔案進行分析掃描，判斷出是否屬於已知病毒感染或是廣告郵件，並針對信件屬性進行不同處理(包含郵件主旨標示或刪除) ，信件誤刪率為 0。

3. 系統運作原理與架構

sendmail 程式負責送信，收到郵件遞送要求時，會豪不猶豫地把郵件透過已身子程序遞送給本機或遠端使用者，只有在遞送失敗狀況下，才會暫存郵件，等待再次遞送。圖 1 為一般郵件系統收發郵件過程示意圖。

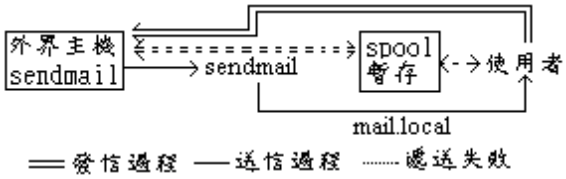


圖 1　一般郵件系統收發郵件過程示意

表 1　TANet 現行郵件系統比較

郵件系統名稱	基本郵件系統 (sendmail)	網擎 mail2000 教育版(v2。75)	網擎 mail2000 商業版(v3。00)	OpenWebmail (sendmail)	進階郵件系統 (procmail) (sendmail)	MailScanner ClamAV Spamassassin
廣告信防治	△	△	△	△	△	○
病毒信防治	╳	╳	△	△	△	○
廣告信學習	╳	╳	╳	╳	╳	○
病毒碼更新	╳	╳	○	╳	╳	○
自由軟體	○	○	╳	○	○	○
安裝難易度	易	易	易	普通	普通	普通
統計圖表	╳	△	△	╳	╳	○

因為 sendmail 的及知及行送信特性，所以在郵件處理過程中，找不到讓其他掃描程式插手郵件遞送工作。

所以 MailScanner 系統透過把原有的 sendmail 遞送程式停止，只啟動 sendmail 的 mta 子程序，讓原先 sendmail 收信後馬上遞送的方式變更為將所收到的郵件先暫存在另外一個資料夾(mqueue。in)，等到 ClamAV 及 SpamAssassin 進行完成病毒及廣告信件檢查後，將檢查結果回報給 MailScanner 進行郵件後續加工動作(如將郵件主旨增加{spam}或{virus}樣式，亦可直接刪除該郵件)，最後將處理過的郵件檔案放回至原先 sendmail 遞送失敗時存放郵件的暫存資料夾，此時 MailScanner 功成身退把遞送功能交還給 sendmail，回到最初 sendmail 程式處理程序完成郵件送收。圖 2 為 MailSacnner 系統郵件處理過程示意圖。

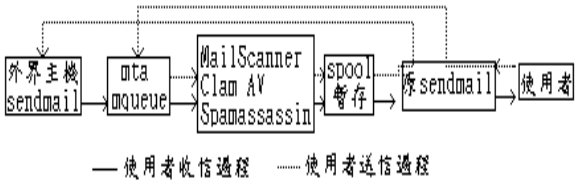


圖 2　MailSacnner 系統郵件處理過程示意圖

4.平台與程式安裝

4.1 平台建議:

強烈建議採用 FreeBSD[8]系統。CPU 及 RAM 是郵件處理量而定。基本上當然是越大越好。

苗栗縣網建置的 MailScanner 系統是一台舊 PC，配備為 PentiumII-350 的 CPU，128MB 的 RAM，realtek 晶片網卡，作業系統使用 FreeBSD 4。7-RELEASE。

4.2 程式安裝:

透過 FreeBSD 的 ports tree 軟體安裝。只要單純的切換到程式路徑輸入 make install 即可完成安裝。

ClamAV 安裝路徑：
/usr/ports/mail/p5-Mail-ClamAV/

SpamAssassin 安裝路徑：
/usr/ports/mail/p5-Mail-SpamAssassin/

MailScanner 安裝路徑：
/usr/ports/mail/MailScanner/
MailScanner 除了透過 make install 安裝之外,還要透過 make init

MailScanner-mrtg 安裝路徑：
/usr/ports/MailScanner-mrtg/

4.3 程式修改:

MailScanner 設定檔修改前:
Virus Scanner= none
Use SpamAssassin= no

MailScanner 設定檔修改後：
Virus Scanner= none
Use SpamAssassin= no

mta.sh 執行檔修改前：
mta=exim

mta.sh 執行檔修改後：
mta=sendmail

/etc/rc.conf 啟動檔新增：
clamav_freshclam_enable=”YES”
sendmail_enable=”NONE”

新增郵件暫存資料夾：
/var/spool/下，新增 MailScanner 及 mqueue.in 資料夾存放相關郵件。

在/var/spool/MailScanner/下，新增 incoming 及 quarantine 資料夾，存放 MailScanner 運作用資料。

所有資料夾權限皆為 755。使用者及群組分別為 root 及 daemon。

新增 MailScanner 規則用空檔案：
/usr/local/etc/MailScanner/rules/bounce.rules

4.4 程式啟動:

停止現有 sendmail 執行：
kilall sendmail

啟動 mta 收信程式：
/usr/local/etc/rc.d/mta.sh start

啟動 MailScanner 程式：
/usr/local/etc/rc.d/mailscanner.sh start

啟動 ClamAV 更新病毒碼程式：
/usr/local/etc/rc.d/clamav-freshclamav.sh
其餘兩個 ClamAV 程式不用執行。

mailscanner-mrtg 只要透過 crontab 每隔 5 分鐘執行一次即可，與一般普通的 mrtg 相同。

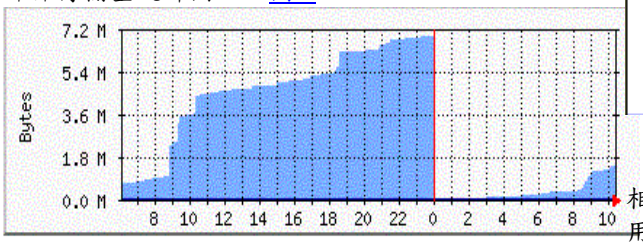
執行測試時，請注意/var/mail/mail.log 紀錄，可以透過此紀錄檢查您的設定是否正確。

若您想要改回原先的 sendmail 程式，可以直接把 MailScanner 和 mta 停掉，重新啟動原先的 sendmail 程式，並且把 mqueue.in 資料夾中的所有檔案搬移回 mqueue 即可。

詳細操作步驟及畫面由於本篇文章篇幅關係，請參閱筆者的網站[9]資料。

5.成果展示

郵件傳輸量統計圖。如圖 3



最大 : 7120.0 k bytes　平均 : 3149.0 k bytes　目前 : 1548.0 k bytes

圖 3 每 5 分鐘郵件傳輸量圖表

判斷為廣告信的數量統計圖。如圖 4

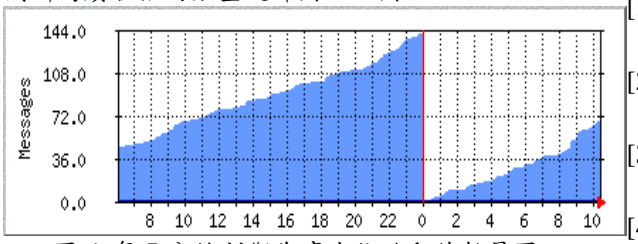
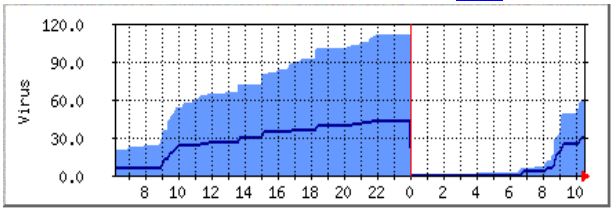


圖 4 每 5 分鐘判斷為廣告信的郵件數量圖

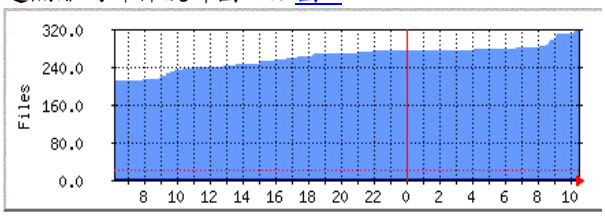
判斷為郵件病毒的郵件數量統計圖。如圖 5



最大 Infected Mail 112.0　平均 Infected Mail 51.0　目前 Infected Mail 61.0
最大 Viruses Detected 44.0　平均 Viruses Detected 21.0　目前 Viruses Detected 31.0

圖 5 每 5 分鐘判斷為病毒感染的郵件數量圖

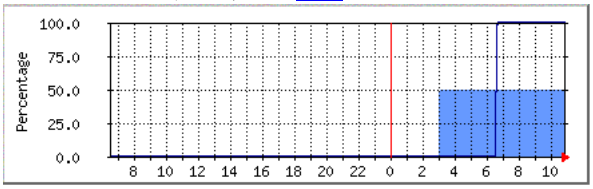
遭隔離的郵件統計圖。如圖 6



最大 : 317.0 Files　平均 : 263.0 Files　目前 : 318.0 Files

圖 6 每 5 分鐘遭隔離的郵件數量圖

病毒信件的比率統計。如圖 7



最大 Blocked郵件: 50.0 %　平均 Blocked郵件: 50.0 %　目前 Blocked郵件: 50.0 %
最大 病毒郵件: 100.0 %　平均 病毒郵件: 55.0 %　目前 病毒郵件: 100.0 %

圖 7 病毒信件比率統計圖

outlook express 收信時的狀況。如圖 8

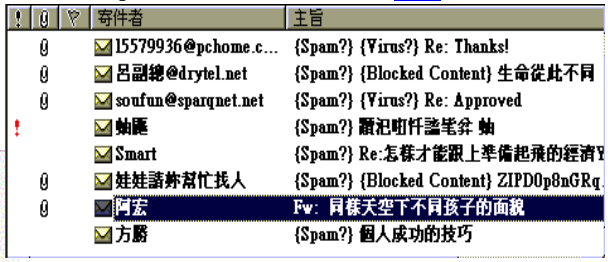


圖 8 outlook express 實際收信狀況圖

相關圖表還有廣告信件比率、伺服器負載、CPU 使用狀況及 RAM 使用狀況圖表[10]。

參考文獻

[1] MailScanner 官方網站
http://www.sng.ecs.soton.ac.uk/mailscanner/

[2] ClamAV 官方網站
http://www.clamav.net/

[3] SpamAssassin 官方網站
http://www.spamassassin.org/

[4] 苗栗縣網 mail2000 系統
http://webmail.mlc.edu.tw/

[5] procmail 官方網站
http://www.procmail.org/

[6] 網擎 mail2000 教育版代表客戶
http://edu.openfind.com.tw/customer.htm

[7] Open Webmail Project 官方網站
http://openwebmail.org/

[8] The FreeBSD Project 官方網站
http://www.freebsd.org/

[9] 黃國鈞。劉立美 OhaHa's 學習心得
http://ohaha.ks.edu.tw/

[10] 苗栗縣網 MailScanner-mrtg 圖表
http://mail.mlc.edu.tw/