

# 異常SMTP訊務與Email Spam 的自動通告

中央大學 電算中心  
楊素秋

Email: [center7@cc.ncu.edu.tw](mailto:center7@cc.ncu.edu.tw)



國立中央大學電子計算機中心  
National Central University, Computer Center  
320-01 桃園縣中壢市中大路300號

# 大 網

- 1. 研究動機
- 2. 異常SMTP訊務的監測
- 3. Spam與異常SMTP訊務的相關
- 4. Spam 事件的自動通告
- 5. 結論



# 1. 研究動機

- 加速 Email Spam 通告
  - IP 管理資訊查詢
    - 區網 Routing Table
    - RWhois查詢服務
  - Spam event 的自動通告
- 異常SMTP訊務的監測
  - Flow count 超量
  - Packet Density
- 分析超量SMTP傳訊主機與通告spam relay/sender 的相關



## 2. SMTP與 Spam傳訊

- SMTP 傳輸

- Client詢問DNS MX list, 建立信件delivery route
  - 紀錄sender與receiver間的多個mail relay/server
  - 將 reverse-path加入mail header
  - 與SMTP relay建立雙向連接, 沿SMTP route傳送信件
- relay收進信件後
  - 與下一relay 建立連接/轉送信件.
- 最後的deliver relay
  - 將信件分送到用戶mailbox.



- Spam
  - UCE (Unsolicited Commercial Mail)
  - spammer利用自動搜尋程式
    - 持續尋找 newsgroup (BBS boards)
    - Join mailing list
    - 網頁的mail addresses
    - 所侵入系統的mail account
    - Regular sequence mail account
  - 重複/密集寄送廣告信件



- Spammer
  - 以最低的成本, 透過全球網路傳送超大量廣告信
- Internet用戶
  - 花費可觀的連線費用, 時間與精力下載/收取/刪除大量spam.
- ISP
  - 耗費更龐大的網路與系統資源重複傳送junk mails
  - 影響mail的正常收送



- 為避免回覆大量的spam complain
  - Spammer藉由自動搜尋程式
    - 尋找未設防的SMTP server 作為spam relay/sender
    - 傳送廣告信件往蒐集的newsgroup/mailing list及mail accounts
  - 甚至透過mail夾檔散播病蟲或攻擊程式
    - 侵入網路主機. 集結更大量的感染主機
    - 寄發/轉送更大量的spam.



- 減緩Spam倍數成長的主要途徑
  - (1)回報/檢舉Spam event
    - 減少一個 spam relay/sender
      - 減少millions of spams
  - (2)監測可能的spammer主機及訊務
    - SMTP訊務量測
    - 篩選異常訊務量





- 回報/檢舉Spam event
  - 連網中心建立abuse Email帳號
    - abuse@domain, spam@domain, security@domain
    - 接受所轄IP主機的Spam/ Junk通告信.
  - 網路用戶
    - 依據spam route, 萃取發送主機與relay servers
      - » “Received:”, “From:” 紀錄項
    - 回應給發信主機與relay server擁有者
  - Report給spam report site
    - EX: spamcop.net



- 偵測可能的spammer主機及訊務
  - 依據Spam 傳訊特徵, 實作異常SMTP訊務的統計
    - *Intensive*
      - » Obviously high SMTP connection count
    - *Iteration*
      - » last for several hours
  - 協助管理者監測異常的mail訊務
    - 據以Check /var/log/maillog
    - 據以Check user mailbox
  - 預先發現感染主機, 通告用戶修補漏洞



- 通告的Email Spam (2003年 7月至 11月)
  - 桃園區網每月處理的Spam mail通告主機總數.
  - 主要的abuse通告信件
    - Spamcop.net 通報
      - 廣告郵件的 relay server/sender
    - myNetWatch 通報
      - CodeRed/Nimda感染主機(80/TCP)
      - SYN Flooding (445/TCP, 17300/TCP, ...)
    - 環球或派拉蒙製片
      - 通告侵犯智財權的eDonkey主機及其影片檔存放
    - Others



Table 1 通告的區網Abuse主機數分布

	Spam Hosts	SYN Flooding	Infringer Hosts
Jul	5	18	6
Aug	15	22	5
Sep	20	0	9
Oct	11	3	6
Nov	7	1	12



# 3 異常SMTP訊務的監測

- 異常SMTP訊務的監測
  - Spam傳訊特徵
    - Intensive
      - Obviously high frequency of SMTP connections
    - Iteration
      - Last for Many hours
    - Mean Packet size
      - Little than 100 Bytes per Packt
      - More than 100 Bytes per packet



- Transportation Traffic Logs
  - all network operators depend on the quantifiable traffic log data to evaluate the network performance
    - TCPDUMP
    - NetFlow, sFlow
    - Others



## – Tcpdump

- a raw packet capture program.
  - Gather the layer 4 transportation traffic logs through
- The dump transport traffic logs involved the detail fields of each IP packet header
  - source/destination IP addresses,
  - source/destination application ports,
  - protocol identity,
  - number of packets,
  - number of bytes,
  - TCP operators



- Netflow

- router 轉送訊務紀錄

- Flow-based layer 4 transport traffic log

- Source & destination IP address
      - Source & destination application port
      - Source & destination interface#
      - protocol identifier
      - packet count
      - byte count





- 利用Netflow log統計區網的異常SMTP訊務
  - Accumulate SMTP serv\_flow connection counts statistics
    - Netflowlog gathered from router of aggregate network
    - Threshold\_100\_flow
      - » Less than 100 connections: 99.72 %
      - » More than 100 connections: 0.28 %
    - Threshold\_30\_flow
      - » Less than 30 connections: 98.61 %



Table 2. 區網的SMTP Flows 特徵項分布

Smtplib_flow count	Flow #/Ratio	Byte Ratio
1~ 10	<u>136003 (94.78 %)</u>	<u>73.1 %</u>
11 ~ 30	<u>5502 (3.83 %)</u>	<u>12.5 %</u>
31 ~ 70	1370 (0.95 %)	8.1 %
71 ~ 100	231 (0.16 %)	1.1 %
101 ~ 200	226 (0.16 %)	1.2 %
201 ~ 1000	145 (0.10 %)	1.8 %
> 1000	15 (0.01 %)	2.2 %



- SMTP訊務的統計/監測
  - Monitor Abnormal SMTP Traffic of  $\text{smtp\_flow}_i$
- Combine Several NetFlow features
  - SMTP service port & Src\_IP & Dst\_IP
    - $\text{src\_IP} > \text{dst\_IP}. (25)$
    - $\text{src\_IP}. (25) > \text{dst\_IP}$



## - 統計/ 監測異常的 SMTP 訊務

- 累計SMTP 訊務變量

- 透過 IP protocol\_id & application port的比對, 累計

- » flow [smtp\_flow<sub>i</sub>]

- » pkt [smtp\_flow<sub>i</sub>]

- » byte [smtp\_flow<sub>i</sub>]

- 排序/篩選超量的syn\_flows訊務

- Monitoring SMTP Traffic

- » PHP + Apache



http://163.25.255.16/~yang/Moe/index\_mail.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體 信箱 新聞 股市 氣象 拍賣 交友 家族

網址(D) http://163.25.255.16/~yang/Moe/index\_mail.php 移至

Y! 輸入您想搜尋的文字 搜尋 登入

## Top-N Mail Traffic Logs of TYC (TaoYuan Network Center)

10 月 17 日 SUBMIT

日期:0815-- Top-N Mail Traffic Logs時

( 08-15 : 00)

Src_IP>Dst_IP	flows	psize(KB/pkt)	Pkts	Total (MB)
61.59.176.194>140.115.17.129.(25)	250	0.133	20926	2.726
163.25.253.1>211.158.10.89.(25)	7244	0.047	16412	0.756
163.25.253.1>211.158.10.90.(25)	7196	0.047	16411	0.748
140.138.144.220>205.188.158.57.(25)	418	0.152	12713	1.884
140.138.144.220>205.188.158.25.(25)	422	0.157	12220	1.871
140.138.144.220>64.12.136.57.(25)	367	0.154	11975	1.803
140.138.144.220>64.12.137.89.(25)	391	0.165	11778	1.896
140.138.144.220>64.12.137.184.(25)	396	0.161	11554	1.822
140.138.144.220>64.12.137.121.(25)	425	0.170	11229	1.864
163.25.197.1>210.242.132.16.(25)	126	0.880	10896	9.360
140.138.144.220>64.12.137.152.(25)	408	0.171	10782	1.805

Mean\_pkt/byte/Flow udp : 50.326 19.463 3.542  
STD\_PKT/BYTE udp : 389.372 254.927 3.542

( 08-15 : 01)

開始 2 Inter... 3 SSH... Windows... Microsoft... abnor\_sm... 異常SM... 下午 08:59



http://163.25.255.16/~yang/Moe/index\_mail.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 · → 下一頁 · 搜尋 我的最愛 媒體

網址(D) http://163.25.255.16/~yang/Moe/index\_mail.php 移至

## Top-N Mail Traffic Logs of TYC (TaoYuan Network Center)

10 月 17 日 SUBMIT

日期:1102-- Top-N Mail Traffic Logs時

( 11-02 : 00)

Src_IP>Dst_IP	flows	psize(KB/pkt)	Pkts	Total (MB)
140.117.198.172.(25)>140.138.140.182	2	1.405	393669	540.038
140.138.140.182>140.117.198.172.(25)	3	0.047	258935	11.939
203.64.191.17.(25)>61.58.77.22	97	0.051	9986	0.497
163.25.154.253>211.20.188.150.(25)	117	1.288	8329	10.478
163.25.154.253>202.1.238.248.(25)	99	1.296	7275	9.209
163.25.233.25>12.161.39.128.(25)	640	0.060	6371	0.375
163.25.154.253>210.59.144.178.(25)	89	1.296	6244	7.902
163.25.154.253>211.76.176.200.(25)	97	1.216	5996	7.122
140.132.3.236>218.32.227.125.(25)	413	0.060	1696	0.099
140.132.20.49>202.1.238.242.(25)	280	0.052	1671	0.086
140.138.148.133>210.200.138.21.(25)	287	0.079	1514	0.117
140.115.113.109>64.12.137.184.(25)	100	0.090	1175	0.103
140.132.3.236.(25)>140.112.193.191	104	0.059	1144	0.066
210.200.138.21.(25)>140.138.148.133	143	0.071	851	0.059
12.161.39.128.(25)>163.25.233.25	130	0.075	846	0.062
163.25.154.253>194.152.243.102.(25)	108	0.055	670	0.036
140.115.155.10>218.32.227.125.(25)	186	0.060	392	0.023

開始 4 L... 6 O... Wind... Strea... 3 S... Micr... 上午 09:39



http://163.25.255.16/~yang/Moe/index\_abnorm\_smtp1.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://163.25.255.16/~yang/Moe/index\_abnorm\_smtp1.php 移至

## Abnormal Mail Relay Logs of TYC (TaoYuan Network Center)

10 月 17 日 SUBMIT

日期:1105-- Abnormal Mail Relay Logs時

( 11-05)

src_IP >dst_IP.(25)	Flow	Packet	Bytes(MB)	Pkt_Sz(B/Pkt)	Ab_Hours
163.25.154.253>211.20.188.150.(25)	4169	320102	405.879	1267.968	14
140.115.113.109>64.12.137.152.(25)	2874	77304	10.063	130.174	13
163.25.154.253>202.1.238.248.(25)	2698	196856	249.685	1268.364	17
140.115.113.109>64.12.137.121.(25)	2490	54355	7.179	132.076	18
140.115.113.109>64.12.138.57.(25)	2331	63118	8.113	128.537	10
140.115.113.109>64.12.138.120.(25)	2163	60331	7.897	130.895	10
140.115.113.109>64.12.136.121.(25)	2033	62346	7.552	121.130	8
140.115.113.109>64.12.137.184.(25)	1980	51212	6.463	126.201	10
140.115.113.109>64.12.138.152.(25)	1721	44754	5.857	130.871	9
140.115.113.109>64.12.138.89.(25)	1555	39570	5.022	126.914	9
140.115.113.109>64.12.137.89.(25)	1548	36107	4.430	122.691	9
163.25.197.1>210.242.132.16.(25)	1435	130430	97.637	748.578	10
163.25.154.253>210.59.144.178.(25)	1349	100214	127.499	1272.267	14
61.58.76.108>203.64.191.17.(25)	1333	109403	110.085	1006.234	24
140.115.112.182>64.12.138.152.(25)	1329	26111	3.405	130.405	2
163.25.154.253>131.107.3.126.(25)	1308	62165	73.186	1177.286	14
140.115.112.182>64.12.138.57.(25)	1244	25517	2.991	117.216	2

開始 4 6 W... S... 3 3 v... 卸... 上午 10:06



Nov 3 20:25:58 smtp3 sendmail[7645]: [ID 801593 mail.info] **hA3CPot1007645:**  
from=<[marketing44@disney.biz](mailto:marketing44@disney.biz)>, size=64607, class=0, nrcpts=1,  
msgid=<[200311031225.hA3CPot1007645@smtp3.cc.ncu.edu.tw](mailto:200311031225.hA3CPot1007645@smtp3.cc.ncu.edu.tw)>, proto=SMTP,  
daemon=MTA, relay=[163.25.154.253]

Nov 3 20:25:58 smtp3 sendmail[7645]: [ID 801593 mail.info] hA3CPot1007645:  
to=<[u9043700@cc.ncu.edu.tw](mailto:u9043700@cc.ncu.edu.tw)>, delay=00:00:06, mailer=relay, pri=30258,  
stat=queued

Nov 3 20:26:45 smtp3 mailscanner[3948]: >>> **Virus 'W32/Yaha-P'** found in  
file ./hA3CPot1007645/disney.zip/DOCUME~1\Dennis\LOCALS~1\Temp\setup.exe

Nov 3 20:26:51 smtp3 sendmail[7958]: [ID 801593 mail.info] hA3CPot1007645:  
to=<[u9043700@cc.ncu.edu.tw](mailto:u9043700@cc.ncu.edu.tw)>, delay=00:00:59, xdelay=00:00:00, mailer=relay,  
pri=120258, relay=[140.115.17.89] [140.115.17.89], dsn=2.0.0, stat=Sent  
(hA3CP8k1016181 Message accepted for delivery)

Nov 3 20:27:00 smtp3 mailscanner[3948]: >>> **Virus 'W32/Yaha-P'** found in  
file ./hA3CPot1007645/disney.zip/DOCUME~1\Dennis\LOCALS~1\Temp\setup.exe





http://163.25.255.16/~yang/Moe/index\_abnormSMTP.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

網址(D) http://163.25.255.16/~yang/Moe/index\_abnormSMTP.php

## Abnormal Mail Relay Logs of TYC (TaoYuan Network Center)

10 月 17 日 SUBMIT

日期:0815-- Abnormal Mail Relay Logs時

( 08-15)

src_IP >dst_IP.(25)	Flow	Packet	Bytes(MB)	Pkt_Sz(B/Pkt)	Ab_Hours
61.59.176.194>140.115.17.129.(25)	2602	283996	35.744	125.861	5
140.138.144.220>205.188.158.25.(25)	2379	72073	16.126	223.745	5
140.138.144.220>64.12.137.89.(25)	2050	57375	10.458	182.275	5
140.138.144.220>205.188.158.57.(25)	1940	59964	13.355	222.717	4
140.138.144.220>64.12.137.121.(25)	941	23517	3.906	166.093	2
140.138.144.220>64.12.137.152.(25)	873	23148	3.910	168.913	2
140.138.144.220>64.12.137.184.(25)	864	24850	3.960	159.356	2
61.30.69.216>163.25.86.174.(25)	299	38374	30.516	795.226	3
163.25.25.226>202.1.236.157.(25)	294	92603	12.220	131.961	2
163.25.197.1>210.242.132.16.(25)	269	23400	19.849	848.248	2

  

src_IP >dst_IP.(25)	Flow	Packet	Bytes(MB)	Pkt_Sz(B/Pkt)	Ab_Hour
163.25.253.1>211.158.10.89.(25)	81821	180724	8.301	45.932	12
163.25.253.1>211.158.10.90.(25)	81689	182880	8.412	45.997	12
140.115.110.38>210.175.123.23.(25)	17565	52070	2.836	54.465	5

開始 4 I... 收... 2 M... 3 S... Wi... rea... Mi... 下午 05:29



http://163.25.255.16/~yang/Moe/index\_mail\_80.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://163.25.255.16/~yang/Moe/index\_mail\_80.php 移至

Y! 輸入您想搜尋的文字 搜尋 登入 信箱 新聞 股市 氣象 拍賣 交友 家族

```

216.22.24.45>140.138.36.14.(25)      24    0.210    146    0.030
209.198.87.173>140.115.83.240.(25)    26    0.135    112    0.015
65.24.7.38>140.115.83.240.(25)      28    0.258    100    0.025
Mean_pkt/byte/Flow udp : 26.106  11.352  2.144
STD_PKT/BYTE udp : 193.486  162.003  2.144

( 10-27 : 06)
=====
Src_IP>Dst_IP      flows  psize(KB/pkt)  Pkts  Total (MB)
211.78.213.17>140.115.70.28.(25)      28    1.089    1478    1.572
210.60.160.252>210.60.221.40.(25)     134    0.224    1293    0.283
192.83.181.17.(25)>203.221.219.65      93    0.102    1054    0.105
216.93.171.18>140.115.17.129.(25)     56    0.398    800    0.311
210.60.221.40.(25)>210.60.160.252      58    0.196    689    0.132
140.138.148.133>168.95.5.48.(25)     125    0.142    612    0.085
140.138.148.133>168.95.5.49.(25)     118    0.143    607    0.085
163.25.233.1>64.12.137.184.(25)       21    0.160    551    0.086
216.22.24.33>140.115.17.129.(25)      55    0.267    452    0.118
216.22.24.35>140.115.17.129.(25)      49    0.270    379    0.100
216.22.24.36>140.115.17.129.(25)      50    0.280    375    0.103
216.22.24.31>140.115.17.129.(25)      49    0.251    362    0.089
216.22.24.30>140.115.17.129.(25)      47    0.278    362    0.098
216.22.24.32>140.115.17.129.(25)      45    0.274    358    0.096
216.22.24.34>140.115.17.129.(25)      46    0.261    357    0.091
Mean_pkt/byte/Flow udp : 22.106   7.611   2.176
STD_PKT/BYTE udp : 149.955   94.949   2.176

( 10-27 : 07)
=====

```

開始 3 S... Windo... 2 M... 2 M... Telnet... http://... spam\_... 下午 07:04



syslog:Oct 26 08:24:25 smtp3 sendmail[13433]: [ID 801593 mail.info]  
h9Q0ON2a013433: from=<**ur@miltyblinks.net**>, size=6998, class=0, nrcpts=1,  
sgid=<200310260024.h9Q0ON2a013433@smtp3.cc.ncu.edu.tw>, proto=SMTP,  
daemon=MTA, relay=mgexchgr81.malupid.net [216.22.24.81] (may be forged)  
syslog:Oct 26 08:24:25 smtp3 sendmail[13425]: [ID 801593 mail.info]  
h9Q0ON2a013425: from=<**pg@miltyblinks.net**>, size=6994, class=0, nrcpts=1,  
sgid=<200310260024.h9Q0ON2a013425@smtp3.cc.ncu.edu.tw>, proto=SMTP,  
daemon=MTA, relay=mgexchgr85.malupid.net [216.22.24.85] (may be forged)  
syslog:Oct 26 08:24:25 smtp3 sendmail[13435]: [ID 801593 mail.info]  
h9Q0ON2a013435: from=<**eh@miltyblinks.net**>, size=6971, class=0, nrcpts=1,  
sgid=<200310260024.h9Q0ON2a013435@smtp3.cc.ncu.edu.tw>, proto=SMTP,  
daemon=MTA, relay=mgexchgr81.malupid.net [216.22.24.81] (may be forged)  
syslog:Oct 26 08:24:25 smtp3 sendmail[13432]: [ID 801593 mail.info]  
h9Q0ON2a013432: from=<**wc@miltyblinks.net**>, size=6995, class=0, nrcpts=1,  
sgid=<200310260024.h9Q0ON2a013432@smtp3.cc.ncu.edu.tw>, proto=SMTP,  
daemon=MTA, relay=mgexchgr84.malupid.net [216.22.24.84] (may be forged)  
syslog:Oct 26 08:24:25 smtp3 sendmail[13434]: [ID 801593 mail.info]  
h9Q0ON2a013434: from=<**jo@miltyblinks.net**>, size=6965, class=0, nrcpts=1,  
...



# Mail Relay Testing

- mrt

- <ftp://ftp.monkeys.com/pub/mail-tools/perl/mrt>

- mrt

- test.patterns

- Test.message

- ./mrt -v test.patterns test.message host\_ip\_add



**ann# ./mrt -v ./test.patterns ./test.message 163.25.121.245**

mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused  
mrt: 163.25.121.245: Error connecting: Connection refused



**ann# ./mrt -v ./test.patterns ./test.message 163.25.70.1**

mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: SMTP error (553) reading MAIL response  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: Message accepted  
mrt: 163.25.70.1: SMTP error (553) reading MAIL response



**ann# ./mrt -v ./test.patterns ./test.message 140.115.17.128**

mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (553) reading RCPT response  
mrt: 140.115.17.128: SMTP error (553) reading RCPT response  
mrt: 140.115.17.128: SMTP error (553) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response  
mrt: 140.115.17.128: SMTP error (550) reading RCPT response



# 數據分析

- 60 % 通告spam relay/sender可由統計的異常SMTP主機佇列中篩選得
  - 7月份的60%
  - 8月份的60%
  - 9月份的60%
  - 10月份的100%
  - 11月份的100%
- 異常SMTP/SYN Flooding訊務監測
  - 發現Spam & 網路侵擾訊務





Table 2 區網Abuse host分布(2003年)

	Abnormal SMTP Traffic	Abnormal www /SYN Flooding
Jul	60 %	43 %
Aug	60 %	48 %
Sep	60 %	—
Oct	55 %	100 %
Nov	100 %	100 %



# 4 Spam 事件的自動通告

- Spam/攻擊訊務通告事件
  - 倍數成長的spam 通告
  - 超量的異常 SMTP Traffic
- 網路管理者
  - 非常依賴IP管理資訊查詢系統
    - 通告感染主機用戶與管理者, 修補系統
    - 自動阻斷攻擊訊務, 防堵攻擊訊務的持續擴散



- spam mail的自動通告系統
  - 自動Query IP管理資訊, Email通告
    - 藉由SNMP pulling router ipRoute MIB,
      - 快速萃取連網的龐大 routing資訊
    - 建立IP管理資訊查詢服務
      - 依據 NextHop integrate
        - » The extracted Routing Table
        - » 連線單位通訊資訊檔
        - » RWhois IP管理資料庫



- ipRoute SNMP MIB
  - 儲存連網單位的routing 資訊
    - Network address
    - NetMask辨識號 .1.3.6.1.4.21.2.1.11
    - NextHop 辨識號 .1.3.6.1.4.21.2.1.7
  - Mansfield G. 曾藉由ipRoute MIB
    - 重複搜尋各層routers ipRoute MIB
    - 自動構建區域網路拓樸



- 重複萃取網段IP位址與對應的
  - NetMask/ NextHop位址
  - 分別以IP網段位址index, 儲存
    - NetMask List
    - NextHop List.
- 結合NetMask , NextHop 與Segment佇列
  - 快速重建龐大的區網ip\_routing 紀錄存檔



### ***ipRouteMask OID***

*ip.ipRouteTable.ipRouteEntry.ipRouteMask.192.192.40.0 = IpAddress: 255.255.252.0*  
*ip.ipRouteTable.ipRouteEntry.ipRouteMask.192.192.44.0 = IpAddress: 255.255.255.0*  
*ip.ipRouteTable.ipRouteEntry.ipRouteMask.192.192.45.0 = IpAddress: 255.255.255.0*  
*ip.ipRouteTable.ipRouteEntry.ipRouteMask.192.192.46.0 = IpAddress: 255.255.255.0*

### ***ipRouteNextHop OID***

*ip.ipRouteTable.ipRouteEntry.ipRouteNextHop.192.192.40.0 = IpAddress: 203.71.2.72*  
*ip.ipRouteTable.ipRouteEntry.ipRouteNextHop.192.192.44.0 = IpAddress: 192.83.175.111*  
*ip.ipRouteTable.ipRouteEntry.ipRouteNextHop.192.192.45.0 = IpAddress: 192.83.175.116*  
*ip.ipRouteTable.ipRouteEntry.ipRouteNextHop.192.192.46.0 = IpAddress: 192.83.175.111*



NextHop	Dest.	Netmask	Seg
=====			
203.72.244.226,	140.115.0.0,	255.255.0.0,	256
203.71.2.5,	140.132.0.0,	255.255.0.0,	256
203.71.2.61,	140.135.0.0,	255.255.0.0,	256
203.71.2.237,	140.138.0.0,	255.255.0.0,	256
203.71.2.209,	192.192.40.0,	255.255.252.0,	4
203.71.2.209,	203.68.52.0,	255.255.252.0,	4...



- IP邏輯位址不包含任何管理資訊
  - Router藉由routing table的查詢
  - 依據 NextHop 紀錄 switch packet
    - Switch 往正確的 routing interface





- RWhois分享軟體

- 利用Mark Kusters' DataBase (MKDB) 支援資料的管理與查詢.
- 資料庫查詢伺服器程式rwhoisd
- 資料庫建置程式rwhoisd\_indexer



- RWhois Server

- 藉由IP管理資料庫伺服系統的建置, 作為自動通告Spam 的基礎.

- 讀取routing紀錄, 依據Nexthop 紀錄比對/ 萃取對應的管理聯絡資訊檔
    - 構建RWhois network schema關聯紀錄檔
    - 建立資料庫indexing, 提供管理資訊 query網頁.



– 選取的Network schema特徵

- IP-Network(網段位址)
- Admin-Contact (管理人員)
- Address(街道地址)
- Tel(聯絡電話)
- Updated-By(資料建立者)
- Updated (資料建立日期)



http://163.25.255.10/~yang/rwhois.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體 信箱 新聞 股市 氣象 拍賣 交友

網址(D) http://163.25.255.10/~yang/rwhois.php 移至

輸入您想搜尋的文字 搜尋 登入

Type the Query IP address Here:  SUBMIT

Responsible for 163.25.5.1 is :  
 : 黃嘉宏 [jhhuang@sun4.cpu.edu.tw](mailto:jhhuang@sun4.cpu.edu.tw)  
[abuse@sun4.cpu.edu.tw](mailto:abuse@sun4.cpu.edu.tw) [security@sun4.cpu.edu.tw](mailto:security@sun4.cpu.edu.tw)

003fff	00 susan.tyc.edu.tw (by Network Solutions, Inc. V-1.5.7.3)
Auth-Area	163.25.0.0/16
Class-Name	network
Network-Name	TANet-TYC-桃園區網 中央警察大學
IP-Network	163.25.5.0/24
Admin-Contact;I	黃嘉宏
Address	桃園縣(333)龜山鄉樹人路56號
Tel	3282142
Updated-By	<a href="mailto:jhhuang@sun4.cpu.edu.tw">jhhuang@sun4.cpu.edu.tw</a>
Updated	200306131802

開始 4 SS... 2 Out... 2 Mi... 2 Inte... Windo... icmp\_st... 下午 07:41



http://163.25.255.10/~yang/rwhois.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 輸入您想搜尋的文字 搜尋 登入 信箱 新聞 股市 氣象 拍賣 交友

網址(D) http://163.25.255.10/~yang/rwhois.php 移至

Type the Query IP address Here:  SUBMIT

Responsible for 140.115.202.35 is :

: 張維巖 center9@cc.ncu.edu.tw  
 abuse@cc.ncu.edu.tw security@cc.ncu.edu.tw

003fff	00 susan.tyc.edu.tw (by Network Solutions, Inc. V-1.5.7.3)
Auth-Area	163.25.0.0/16
Class-Name	network
Network-Name	TANet-TYC-中央宿網cc.ncu.edu.tw
IP-Network	140.115.202.35/32
Admin-Contact;I	u1401001@cc.ncu.edu.tw
Address	D2-202宿網用戶
Updated-By	u1401001@cc.ncu.edu.tw
Created	200306200804
Auth-Area	163.25.0.0/16
Class-Name	network
Network-Name	TANet-TYC-桃園區網中央大學(1)
IP-Network	140.115.192.0/18
Admin-Contact;I	張維巖

開始 4 SS... 2 Out... 2 Mi... 2 Inte... Windo... tyc\_rw... 下午 07:42



- Sendmail

- 最普遍使用的電子郵件傳送程式

- Mail server 藉由sendmail daemon 接受 mail client連接要求
    - 輾轉發送mail到 destination mail server
    - 接收送達的user mail, 並轉存到user mail-box
      - 存成 /var/mail/user\_name檔.



- 自動化的Spam通告程序
  - 讀取 /var/mail/abuse buffer 檔
    - 依據 “From ” 萃取各單封的mail存檔.
  - parsing信件內容, 萃取攻擊IP位址.
  - 自動連線RWhois server, 查詢IP管理資訊.
  - 依據IP管理資訊, 將萃取的信件內容檔轉送給管理員/用戶mail



http://163.25.255.16/~yang/Moe/index\_spam.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 · → · × · ↻ · 搜尋 · 我的最愛 · 媒體 · 信箱 · 新聞 · 股市 · 氣象 · 拍賣 · 交友 · 家族 · 移至

網址(Q) http://163.25.255.16/~yang/Moe/index\_spam.php

Y! 輸入您想搜尋的文字 搜尋 登入 信箱 新聞 股市 氣象 拍賣 交友 家族 >>

## Spam Mail Logs of TYC (TaoYuan Network Center)

11 月份 SUBMIT

### 09 月份 Spam Notice Logs

Spam Mail[09-02]

=====

0 140.115.5.47 (Virus Mail)

Spam Mail[09-04]

=====

0 140.115.5.47 (Virus Mail)  
11 163.25.148.67 (Infringers IP Address)  
12 163.25.148.39 (Infringers IP Address)  
19 203.72.100.9(Mail Relay & Mail From)

Spam Mail[09-05]

=====

20 140.138.144.220(Mail Relay)  
22 140.138.36.188(Mail Relay )

Spam Mail[09-08]

=====

1 140.138.144.220(Mail Relay)





# 攻擊訊務的自動阻絕與通告

- 周期地篩選超量攻擊訊務，萃取攻擊主機IP
- 依據主機IP, 自動連線RWhois server, 查詢管理資訊.
- 依據管理資訊, 遠端設定區網 router
  - 限制攻擊主機傳訊, 防止超量攻擊訊務的擴散
- 連接RWhois 查詢伺服主機, 查詢管理資訊
  - 自動發信通知管理人員/用戶
  - 協助修補感染的系統, 排除攻擊訊務起源.



## 5. 結語

- 實作IP管理資訊查詢系統
  - 為Spam/網路攻擊訊務的自動通告基礎
- Spam/攻擊事件自動通告機制
  - 提升spam的通告效率
  - 減輕網路管理者處理大量抱怨信的負荷



- 異常 SMTP/www DoS 訊務的統計
  - 檢測感染主機及 Spam senders
  - 主動遏止 SMTP 干擾訊務.
- 教育網路用戶
  - 提升 mail server 被冒用的警覺性
  - 加強異常網路訊務的監測
    - PING Storm, SYN Flooding, Spam relay
  - 分享網路攻擊模式與防堵經驗

