

# 區網中心網路安全工作報告

中央大學 楊素秋

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

# 報 告 大 綱

- 1. 網路安全工作重點
- 2. Flooding 訊務偵測
  - PortScan, Spam, Packet flooding
- 3. 網路安全概念的宣導
  - 文件整理 & 討論群
- 4. TANet 連線學校資通安全管理規範
- 5. 總結

# 1. 網路安全工作重點

- Key to putting an end to the dark side of network
  - Increase awareness
    - Education users
  - Implement organization policies
  - Use Technology to protect against these threats
    - Flooding Detection system

# 1. 網路安全工作重點(cont.)

- Flooding 訊務偵測
- 網路安全概念宣導工作
  - 相關網站與文件的整理
  - 網路安全資訊的溝通
- TAnet 連線學校資通安全管理規範
  - 參考依據：BS7799 & ISO17799
  - 預計推動時程
- Copyright infringement

## 2. Flooding 訊務偵測

- Flooding 異常訊務量測首頁
  - Abuse complain log
    - [abuse@ncu.edu.tw](mailto:abuse@ncu.edu.tw) 接受abuse通知
    - 自動轉寄管理人員
  - FDS (Flooding Detection System)
    - 實做 Flooding 訊務量測
    - 異常訊務量監測
    - 偵測得異常 flooding sources
    - 自動將訊務數據轉寄管理人員

## 桃園區網中心-- Flooding 異常訊務量測

[ 桃園區網中心首頁 ] [ 教育部 Abuse 列表 ] [ 桃園區網 Abuse 列表 ] [ 異常訊務數據 (舊網頁) ]

[ TANet資通安全管理規範文件 ] [ 智慧財產權教戰手冊 (New) ] [

首頁

異常訊務查詢

區網 IP 配置

Rwhois IP 查詢

網路安全留言

區網連線架構

IPv6 測試網站

TWAREN 訊務監測

連線學校訊務

Top-N 訊務排行

TANet SPAM 防治

桃園縣政府教育局

金門縣網中心

馬祖 連江縣網中心

### Flooding 異常監測網頁

- [SMTP Flooding 訊務監測 \(Spam\)](#)
- [PortScan 異常訊務監測](#)
- [SSH 異常訊務監測 \(密碼猜測\)](#)
- [UDP Packet Flooding 訊務監測](#)
- [監看詳細的 Flooding 異常訊務](#)

### 網路安全由個人做起

一部未安裝防毒 (anti-virus) 軟體, 不及時更新微視窗系統 (Windows Updates), 甚至選用過於簡單的密碼的連網主機, 都有非常高的機率為 hacker 所吸納並用來掩護其發動網路攻擊, 唯有網路用戶能善用 anti-virus/firewall 等工具, 扎實地做好網路防護措施, 並維持良好的網路使用習慣, 才能根本地阻截網路駭客與犯罪組織的橫行. [詳全文](#)

### PortScan 異常訊務偵測

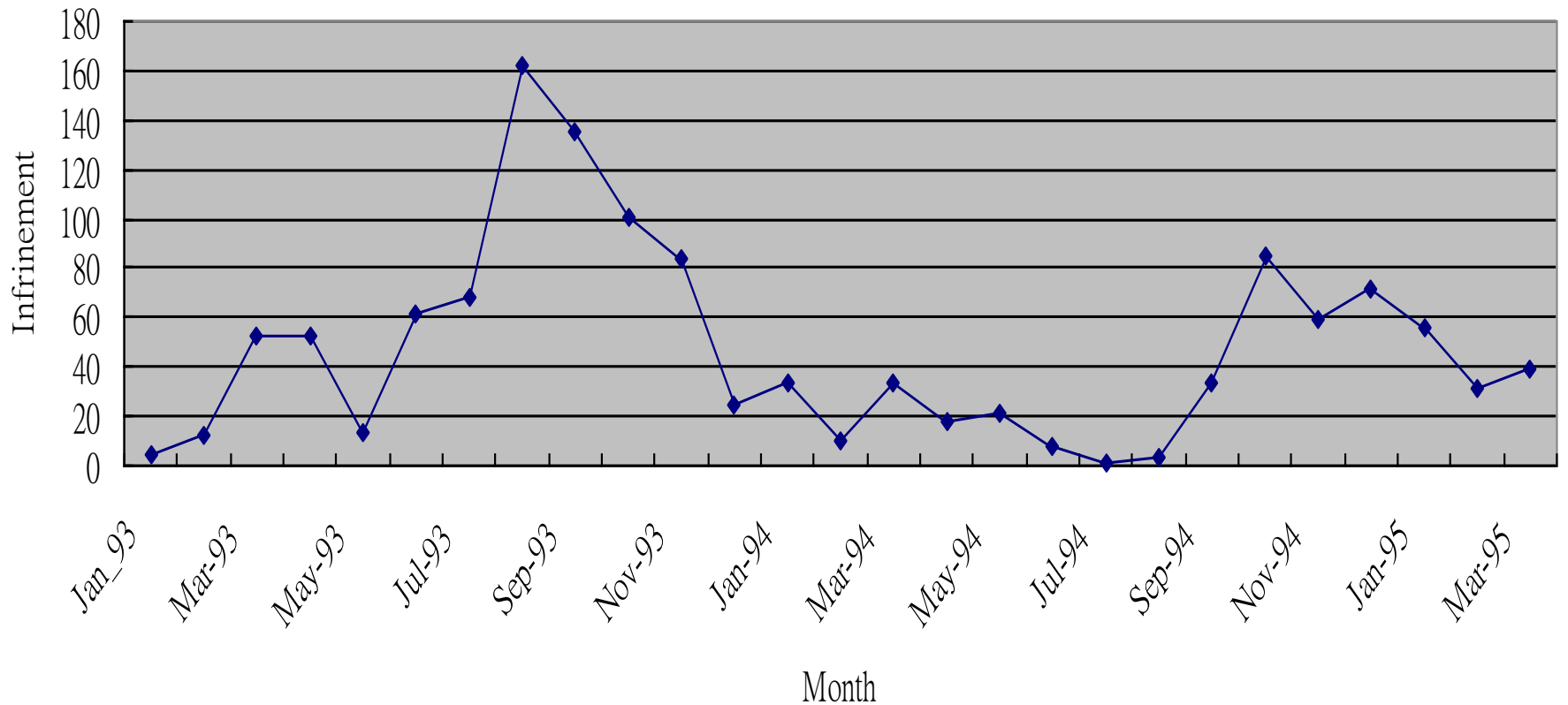
入侵偵測系統 (Intrusion detection system, IDS) 常被安置於校園企業網路主幹, 或 server farm 節點, 協助管理人員處理入侵事件, 而我們所做的工作: 於上游骨幹網路 routing 網路, 增加一層明顯 Flooding 異常訊務偵測系統. 以下為相關說明 [\(詳全文\)](#)

### SMTP 異常訊務偵測

區網節點阻截 Spam 的利器 SMTP Flooding 異常訊務偵測系統以下為相關說明 [\(詳全文\)](#)

### 網路安全相關網站

## 智財權抱怨信頻次分布 (2004-2006)



保護智慧財產權相關資訊 - 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

網址(D) http://lisa.tyc.edu.tw/Copyright/index.html 移至 連結 >>

Google 智慧財產 網路 搜索 38 個已拦截 拼写检查 选项 智慧財產 網路

## 保護智慧財產權相關資訊

[經濟部智慧財產局](#) | 1

### 智慧財產相關網頁 (摘自經濟部智慧財產局)

- [「權利管理電子資訊」之說明](#)

著作權的「權利管理資訊」就是指有關著作權利狀態的訊息，諸如著作名稱是什麼？著作人是誰？著作財產權係由何人享有？由何人行使？受保護的期間到什麼時候？有意侵權著作財產權的人，應與何人聯繫洽商？欲利用著作的人，應向什麼人徵求授權？授權條件，例如金額、範圍等，又是如何？凡此種種與著作權管理相關的訊息，稱之為權利管理資訊。
- [網路行為適法性之探討](#)

一般民眾往往只著重於網路上資訊流通之便利性，卻忽略了這些網路行為法律的適法性與否。本文僅針對一般民眾利用網路從事檔案交換行為之適法性作初淺的探討。
- [校園著作權利用之相關問題](#)

從網頁上將他人電腦軟體、歌曲、圖片或文章下載回自己的電腦，或將自己手頭上的電腦軟體、歌曲、圖片或文章上載到學校的FTP站上，都是一種重製行為。除非有可以主張合理使用的情形，否則應經各類著作之著作財產權人同意或授權，才不致構成著作權侵害。
- [利用BT、Emule等P2P（點對點）傳輸軟體下載及上傳他人著作之法律責任](#)

民眾利用BT軟體，任意自網路下載圖片或影片等著作，如權利人依法告訴，該多數人均有共同負擔法律責任之可能性。仍會造成侵害著作權人重製權及公開傳輸權。

完成 網路網路

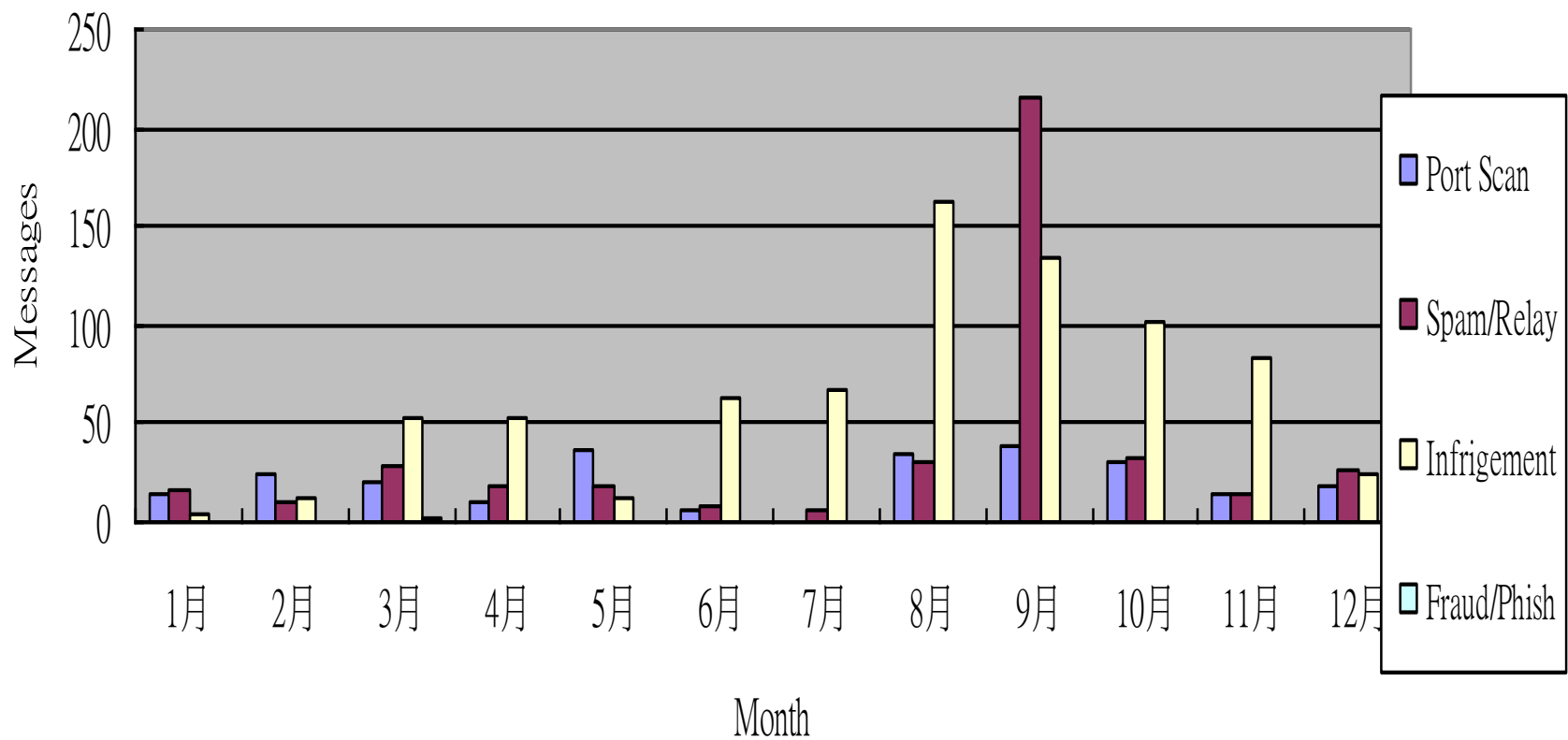
開始 5 Internet ... 4 Outlook ... 2 SSH Secu... 33次區網會... Microsoft Pow... Adobe Photos... 命令提示字元 下午 03:13



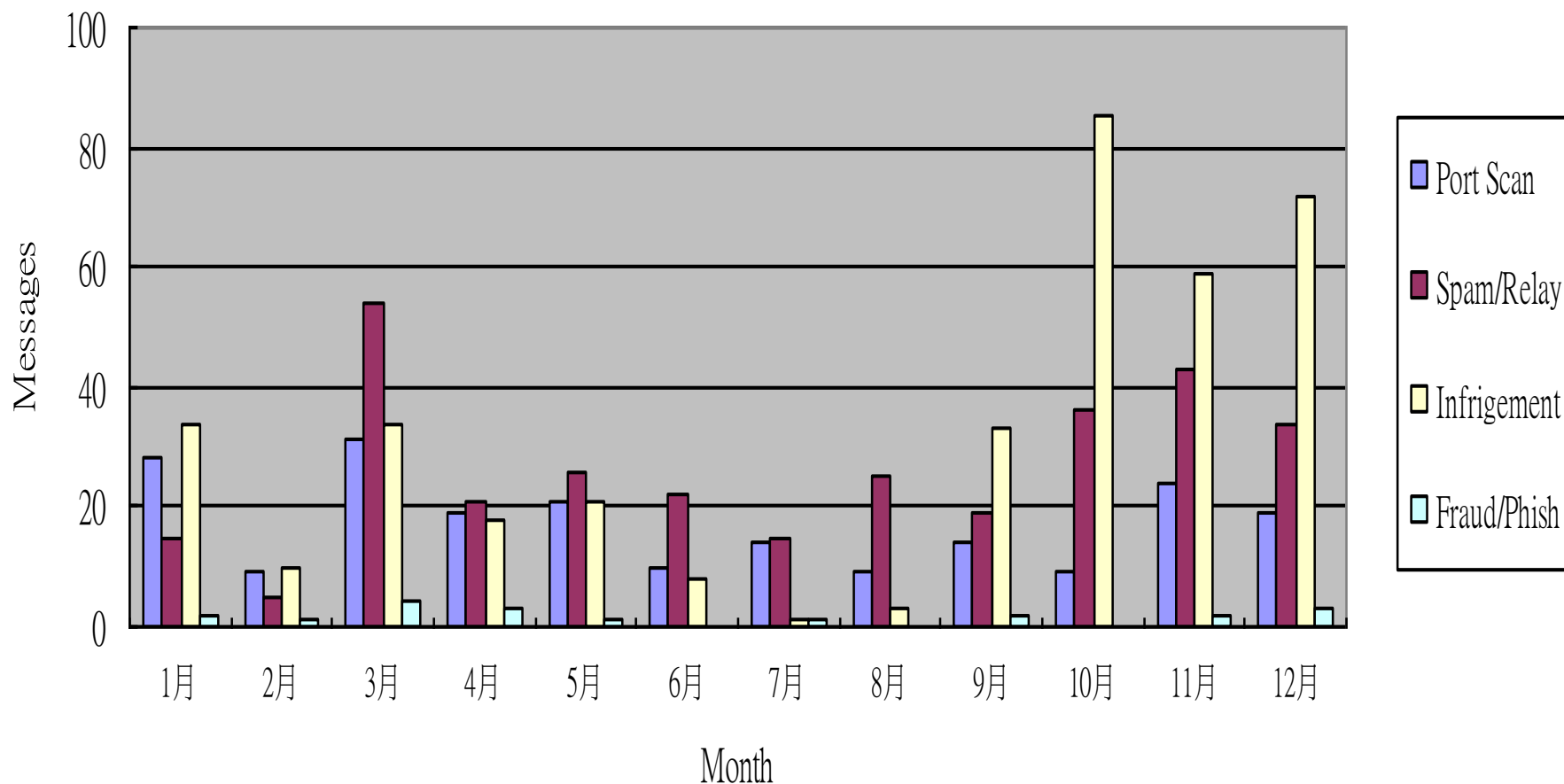
## 2. Flooding 訊務偵測(cont.)

- Abuse complain的處理
  - [http://ayang.tyc.edu.tw/~yang/Moe/index\\_spam.php](http://ayang.tyc.edu.tw/~yang/Moe/index_spam.php)
  - PortScan/Password crack
  - Spam (廣告/色情)
  - Infringement (侵犯智慧財產權)
  - Phishing (Fraud)

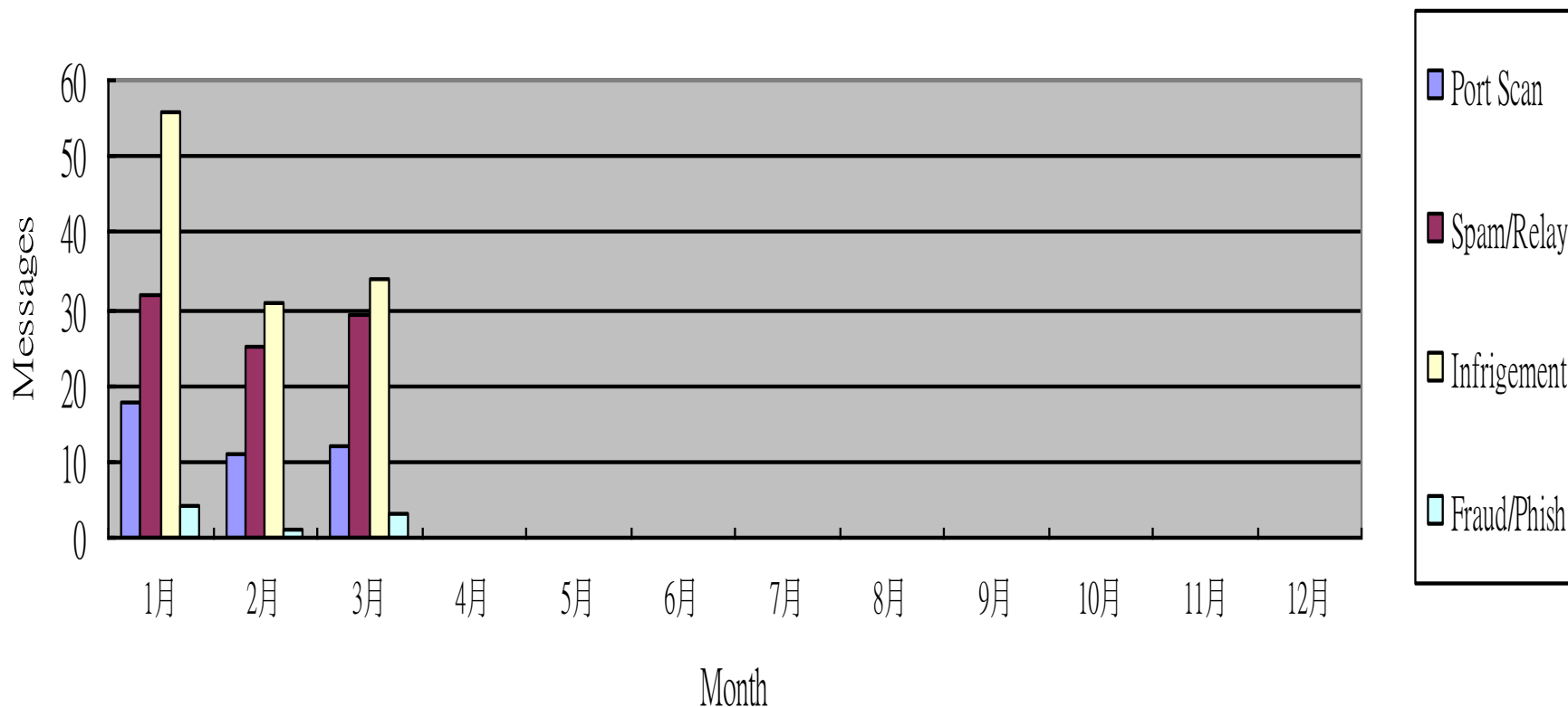
## 桃園區網Abuse 檢舉信件分布圖(year-2004)



# 桃園區網Abuse 檢舉信件分布圖(year-2005)

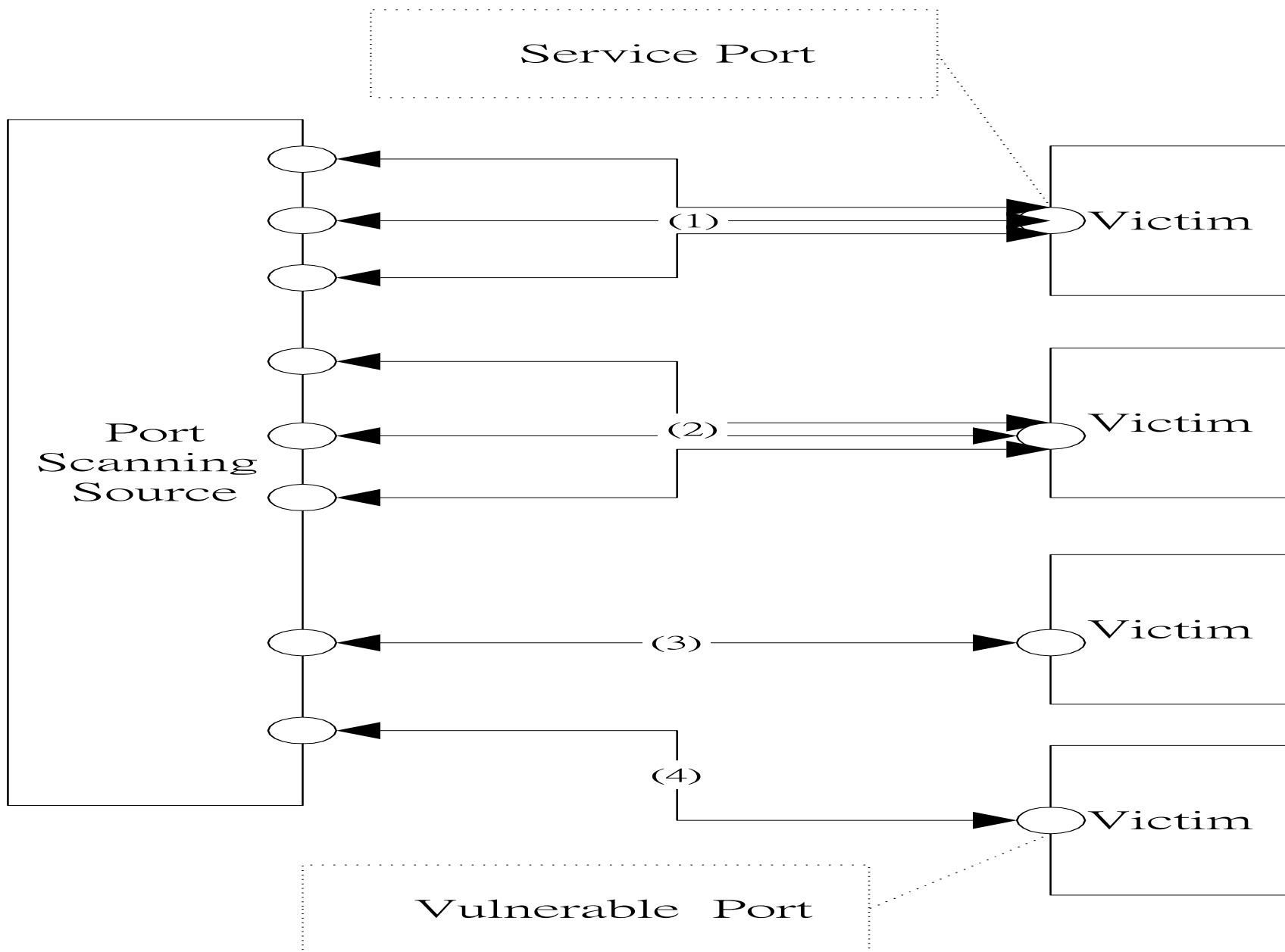


## 桃園區網Abuse 檢舉信件分布圖(year-2006)



## 2. Flooding 訊務偵測(cont. )

- FDS uses technology to protect against abuse threats
  - PortScan, Spam and Packet flooding sources
    - Share a crucial common feature
    - Send out excessive probes/messages to a huge amount of destination systems



## 2. Flooding 訊務偵測(cont. )

- FDS offers a cheap accessible way for detecting the extremely flooding anomalies
  - Gathering the NetFlow data
  - Constructing feature of the anomaly
  - Aggregating and sort out the top-N source systems
  - Detecting the anomaly through comparing the multiple measured traffic variables

## 2. Flooding 訊務偵測(cont.)

- FDS (Flooding Detection System)
  - Flooding 異常訊務監測網頁
    - <http://lisa.tyc.edu.tw>
  - (a) PortScan anomaly
  - (b) SMTP flooding
  - (c) UDP packet flooding



# SMTP Flooding 訊務監測網頁(一) : Hourly Anomalies

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

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 信箱 新聞 股市 氣象 拍賣 交友 家族

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

12 月 02 日 SUBMIT

日期:1202-- Top-N Mail Traffic Logs

( 12-02 : 00)

Src_IP>Dst_IP	flows	psize(KB/pkt)	Pkts	Total (MB)
163.25.154.253>202.1.238.248.(25)	387	1.298	27320	34.643
163.25.154.253>211.20.188.150.(25)	196	1.272	12533	15.571
163.25.154.253>202.1.238.251.(25)	140	1.300	9249	11.739
163.25.154.253>202.1.234.240.(25)	113	1.306	8893	11.339
163.25.154.253>210.200.181.220.(25)	95	1.302	7639	9.711
192.192.21.1.(25)>210.85.244.225	288	0.063	3520	0.218
202.1.238.248.(25)>163.25.154.253	92	0.051	2994	0.149
209.228.32.181>140.115.83.240.(25)	99	0.984	1633	1.569
210.85.244.225>192.192.21.1.(25)	124	0.206	1545	0.311
163.25.233.10.(25)>163.24.7.245	131	0.184	1326	0.238
209.228.32.171>140.115.83.240.(25)	83	0.987	1325	1.278
61.131.4.142.(25)>203.68.77.5	103	0.054	1164	0.062
163.25.154.253>194.152.243.102.(25)	189	0.054	918	0.049
140.115.112.147>218.32.227.125.(25)	193	0.046	837	0.038
163.25.237.2.(25)>163.24.156.4	91	0.380	714	0.265
140.132.3.236>218.32.227.125.(25)	179	0.060	697	0.041
202.248.37.147>140.138.2.235.(25)	278	0.047	684	0.032

20 開始 3 Inte... 2 SS... 2 Outl... Window... abnor\_s... 上午 10:29 7

# SMTP Flooding 訊務監測網頁(二): Detected anomalies

http://163.25.255.16/~yang/Moe/index\_ab\_spamsrc.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\_ab\_spamsrc.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

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

12 月 02 日 SUBMIT

日期:1202-- Abnormal Mail Relay Hosts

( 12-02 )

src_IP >#. #. #. #. (25)	Flow	Packet	MBytes	Pkt_Sz(B/Pkt)	Hr_Flws	School_Name
163.25.154.253>#. #. #. #. (25)	12764	970353	1233.2	1270.9	73	桃園區網 陸軍高級中學
163.25.206.1>#. #. #. #. (25)	5143	390459	391.5	1002.8	23	TANet-桃園縣教育局-內定國小
163.25.54.97>#. #. #. #. (25)	4819	413314	389.0	941.2	56	TANet-桃園縣教育局-同安國小
140.138.137.54>#. #. #. #. (25)	3551	64901	12.9	198.4	66	桃園區網元智大學
163.25.50.104>#. #. #. #. (25)	3360	306326	114.6	374.0	13	TANet-桃園縣教育局-南門國小
163.25.187.129>#. #. #. #. (25)	3277	40552	13.1	324.1	54	TANet-桃園縣教育局-石門國中
140.115.236.47>#. #. #. #. (25)	2222	220516	250.3	1135.2	20	中央大學資策會
203.71.101.1>#. #. #. #. (25)	2173	183882	171.7	933.9	42	桃園區網 治平中學
163.25.233.25>#. #. #. #. (25)	1521	25179	5.0	197.1	11	TANet-桃園縣教育局-武漢國小

src_IP >#. #. #. #. (25)	Flow	Packet	Bytes(MB)	Pkt_Sz(B/Pkt)	Ab_Hr_Flws
163.25.187.129>#. #. #. #. (25)	11705	45934	2.29	49.83	139(11705)
163.25.233.25>#. #. #. #. (25)	8453	39552	2.13	53.80	125(8453)
140.115.112.147>#. #. #. #. (25)	6911	29460	1.32	44.84	27(6911)
218.150.79.141>#. #. #. #. (25)	5139	14464	0.90	62.29	46(5139)

開始 3 Inte... 2 SS... 2 Outl... Window... mail\_att... 上午 10:28

# SMTP Flooding 訊務監測介面 (三): 通告信內容

The screenshot shows a Microsoft PowerPoint window titled 'Microsoft PowerPoint - IPDS 簡報 2004\_10131'. The slide content is an email titled 'The suspicious Spamming Host 163.25.50.105 in Your Camplus'. The email header shows it was sent from center7@cc.ncu.edu.tw on 2004年10月12日 下午 10:38 to center7@cc.ncu.edu.tw; mis@host3.nmes.tyc.edu.tw; and eric@mail.tyc.edu.tw. The subject is 'The suspicious Spamming Host 163.25.50.105 in Your Camplus'.

The email body contains the following text:

Please help the owner of the machine  
to check and fix its Open Mail Relay Problem or Patch  
Please refer the detail traffic log on

[http://163.25.255.16/~yang/Moe/index\\_ab\\_spamsrc.php](http://163.25.255.16/~yang/Moe/index_ab_spamsrc.php)  
Many Thanks !  
From : susna yang

=====

SRC_IP>#.#.#.#.(Serv_port)	Flows	pk_size(KB)	Pkts	Total(MB)
163.25.50.105>203.65.76.252.(25)	803	0.528	30374	15656
163.25.50.105>163.17.200.129.(25)	465	0.513	18146	9083
163.25.50.105>210.241.85.53.(25)	460	0.538	17128	8999
163.25.50.105>80.88.36.130.(25)	610	0.059	4694	0.271
163.25.50.105>61.107.31.33.(25)	517	0.056	3443	0.190

The slide is part of a presentation titled 'IPDS 簡報 2004\_10131'. The taskbar at the bottom shows the Windows XP interface with the Start button, taskbar, and system tray. The system clock shows 上午 11:20.



# Port Scan訊務監測介面 (一) : Hourly Anomalies

http://163.25.255.16/~yang/Moe/index\_tcp.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\_tcp.php 移至 連結 >>

## Hourly Security Probe/SYN Flooding Traffic of TYC

05 月 17 日

日期:0312-- Hourly Security Probe Traffic時

03-12 :: 00

SRC_IP>serv_port	Flows	pk_size(KB)	Pkts	Total(MB)
163.25.148.155>#.###.(20168)	109613	0.048	167730	8.051
140.115.206.22>#.###.(17300)	100082	0.048	161347	7.745
140.115.81.24>#.###.(17300)	84463	0.048	133474	6.407
140.115.135.179>#.###.(4899)	81208	0.048	92166	4.424
140.115.227.220>#.###.(17300)	77745	0.048	123765	5.941
140.138.145.12>#.###.(1433)	52503	0.048	79547	3.818
163.25.131.240>#.###.(20168)	47352	0.048	94258	4.524
140.115.230.216>#.###.(6667)	46153	0.048	95040	4.560
140.115.123.82>#.###.(17300)	40152	0.048	65388	3.139
203.68.82.203>#.###.(6129)	28538	0.048	99155	4.759
203.68.82.203>#.###.(135)	28330	0.048	29738	1.427
163.25.196.1>#.###.(135)	24616	0.048	24616	1.182
203.68.82.203>#.###.(445)	23538	0.048	24349	1.169
203.68.41.7>#.###.(135)	22591	0.048	67458	3.238
140.115.81.13>#.###.(445)	22092	0.048	22287	1.070
140.138.168.16>#.###.(135)	21414	0.048	24425	1.172
203.68.87.150>#.###.(135)	19273	0.048	21572	1.035
203.68.87.150>#.###.(445)	18683	0.048	20944	1.005

開始 3S 31 收... De... Re... Mi... 未... 下午 08:10

# Port Scan 訊務監測介面 (二): Detected anomalies

http://163.25.255.16/~yang/Moe/index\_abuse\_port.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 83 blocked AutoFill Options

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

Google Search Web

[IP Prefix 小範圍查詢](#) [Scanning 歷史紀錄查詢](#)

Summarizing SYN Floodinf /Port Scan over TaoYuan Network Center

03 月 17 日 SUBMIT

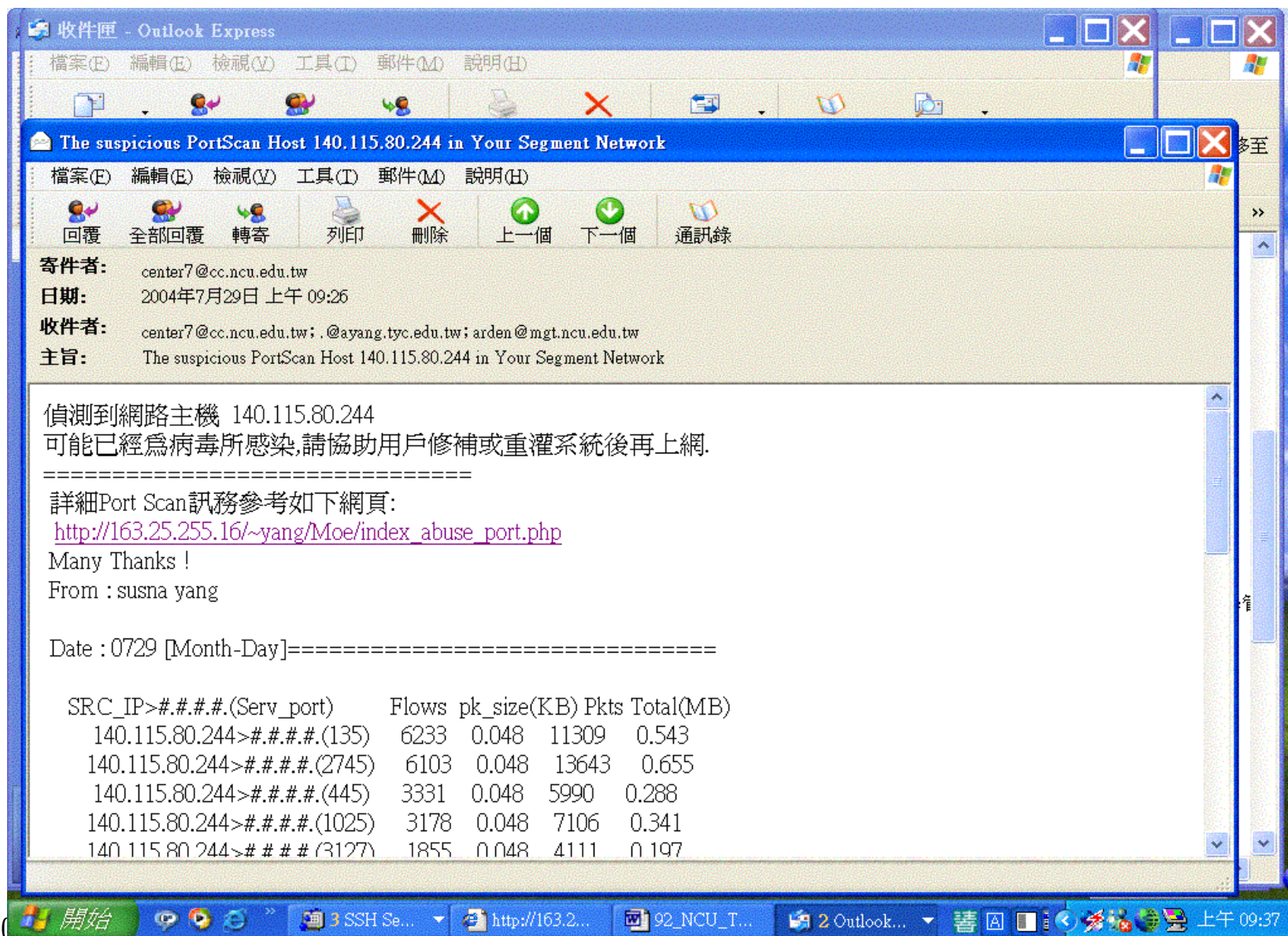
日期:0312

src_IP >#.##.##	DST_P1/Flows	DST_P2/Flows	DST_P3/Flows	DST_P4/Flows	(FwRate *Hour)[Shool]
140.115.135.179>#.##.##	4899/2432201	I@ 101341 * 24[中央大學網學]			
140.115.227.220>#.##.##	17300/1794435	I@ 112152 * 16[中央大學宿舍網路(1)]			
203.68.82.203>#.##.##	6129/227067	135/253755	445/220525	I@ 58445 * 12[萬能技術學院]	
203.68.90.153>#.##.##	6129/185040	135/182901	445/165136	139/160647	I@ 86715 * 8[萬能技術學院]
203.68.54.4>#.##.##	6129/151357	135/261833	445/172077	I@ 25446 * 23[萬能技術學院]	
140.138.168.16>#.##.##	135/574736	I@ 23947 * 24[元智大學]			
203.68.76.209>#.##.##	6129/211998	135/170416	445/138586	139/484	I@ 57942 * 9[萬能技術學院]
203.68.87.207>#.##.##	6129/179134	135/202293	445/134379	I@ 30341 * 17[萬能技術學院]	
140.115.98.250>#.##.##	17300/446721	445/5254	I@ 45197 * 10[中央大學藝術]		
140.115.130.72>#.##.##	6129/58208	135/51296	445/52328	80/57822	I@ 31917 * 14[中央大學圖書館]
203.68.41.7>#.##.##	135/259125	80/90049	I@ 19398 * 18[南亞技術學院]		
140.115.206.22>#.##.##	17300/325342	445/11079	I@ 67284 * 5[中央大學宿舍網路(1)]		
140.138.246.132>#.##.##	135/228051	445/90104	I@ 13256 * 24[元智大學]		
203.68.82.83>#.##.##	135/212375	445/51442	139/16666	I@ 11686 * 24[萬能技術學院]	
210.240.213.238>#.##.##	135/114080	445/141187	80/10653	139/9496	I@ 11475 * 24[體育學院]
140.138.40.208>#.##.##	135/137269	445/124015	139/3441	I@ 11030 * 24[元智大學]	
140.138.145.12>#.##.##	1433/250853	I@ 50170 * 5[元智大學]			
140.138.248.82>#.##.##	135/155278	445/81977	I@ 9885 * 24[元智大學]		

開始 3 S... 3 O... Deg... 2 I... Win... icm... 上午 10:46



## Port Scan訊務監測介面 (三): 通告信內容



# UDP Packet Flooding監測介面 (一) : Hourly Anomalies

http://163.25.255.16/~yang/Moe/index\_evil.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( ) http://163.25.255.16/~yang/Moe/index\_evil.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

## UDP Attack Traffic Statistic of Taoyuan Network Center

03 月 17 日 SUBMIT

日期:0209-- UDP Attack Logs時

We should investigate the Traffic Pairs and Association  
IF the Pair\_Packet counter > 10,000,000  
OR the Pair\_Total counter > 10,000 MB

SRC_IP > DST_IP	Flows	pk_size(KB)	Pkts	Total(MB)
UDP 02-09 :: 00				
140.115.155.8>62.219.113.127	1255006	0.046	62816008	2821.693
140.115.160.47>217.132.237.9	1249653	0.046	30281724	1360.232
140.117.205.162>203.72.244.6	2	1.449	500211	707.821
140.113.138.4>192.192.42.194	3	0.072	162805	11.378
202.202.106.16>140.125.07.55	2	0.065	156720	0.071

開始 4 S... Real... 4 L... Degr... 命令... 3 O... 下午 05:22



## UDP Packet Flooding監測介面 (二) : Detected Anomalies

http://163.25.255.16/~yang/Moe/index\_udp\_flood.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 83 blocked AutoFill Options

網址(1) http://163.25.255.16/~yang/Moe/index\_udp\_flood.php 移至

### Flood Traffic of UDP Procols (TaoYuan Network Center)

02 月 09 日 SUBMIT

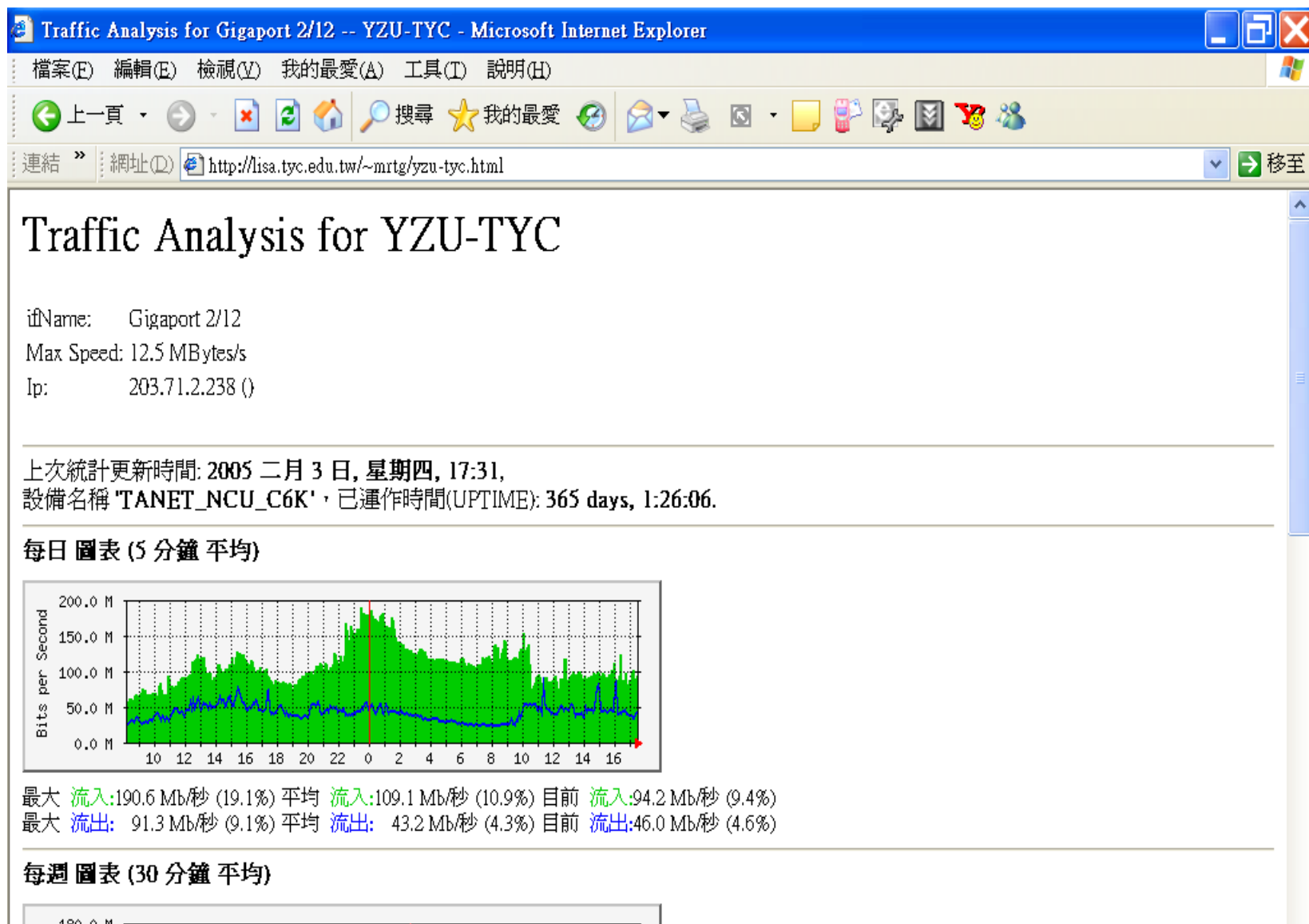
日期:0209-- Packet Flood Traffic of UDP Protocols

src_IP >dst_IP	Flows	Pkts	Bytes	Pkt_SZ	(Pkt_Rate *Hour)[Shool]
140.115.156.35>66.252.7.97	9407947	695989846	31263	45	100 63271804 * 11 [中央大學通訊中心]
140.115.160.47>217.132.123.5	31530818	220673767	9912	45	100 11614408 * 19 [中央大學管理學院]
140.115.160.47>80.179.228.107	26202356	205142857	9214	45	100 11396825 * 18 [中央大學管理學院]
140.115.155.8>62.219.113.127	8824966	189336844	8504	45	100 17212440 * 11 [中央大學通訊中心]
140.115.155.8>66.252.7.97	6678552	86177637	3870	45	100 7834330 * 11 [中央大學通訊中心]
140.115.160.47>217.132.237.9	2277925	55490076	2492	45	100 27745038 * 2 [中央大學管理學院]

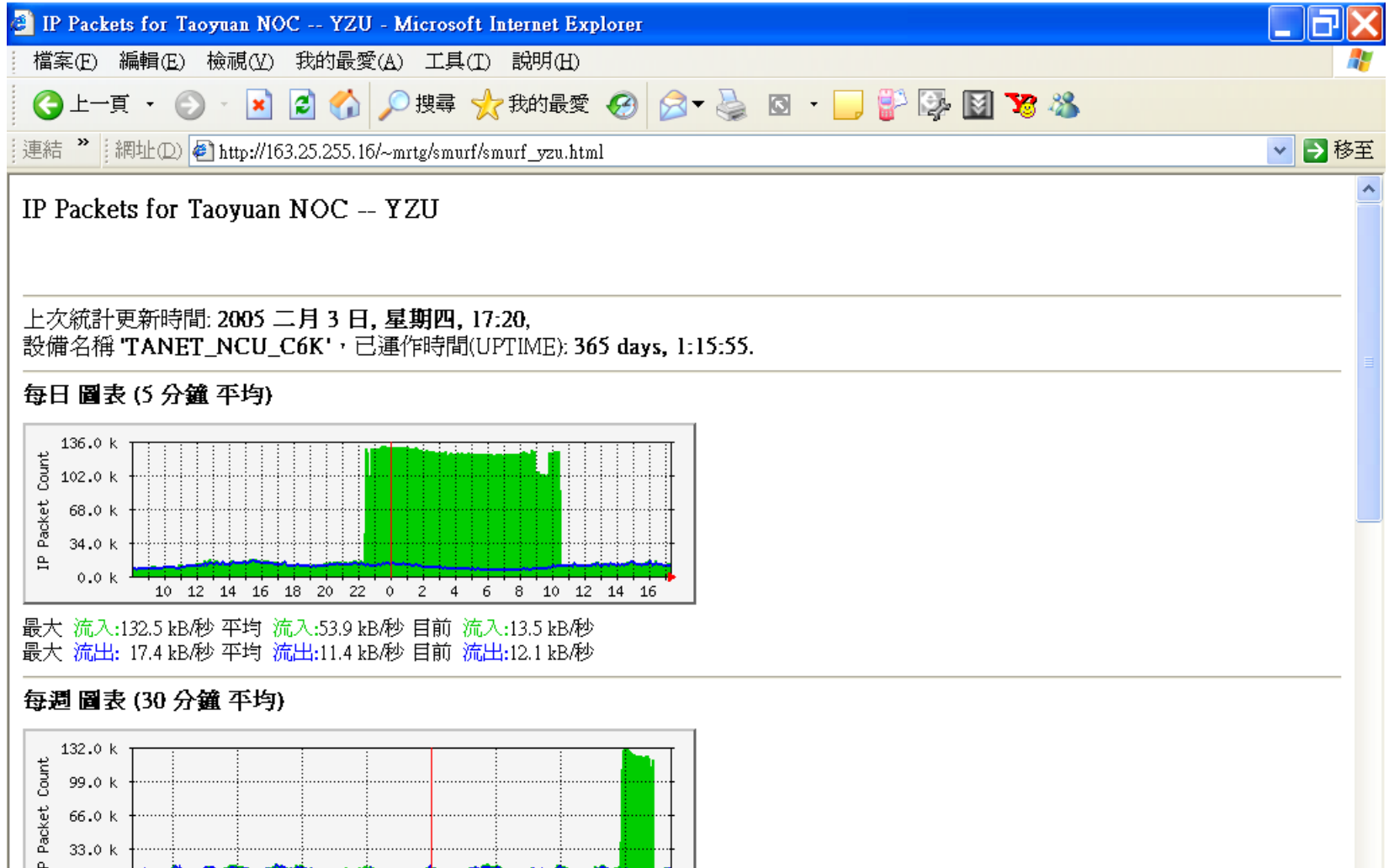
開始 2 SS... 4 Int... Windo... NCU ... Degree... 上午 08:52



# Transportation Byte/Octet MRTG 監測介面



# Transportation Packet MRTG 監測介面



# 3. 網路安全概念的宣導

- 相關網站與文件的整理
  - 文件
    - SMTP Flooding Detection
    - PortScan Detection
    - Others
  - 網站
    - SANS (SysAdmin, Audit, Network, Security)
    - 國家資通安全通報中心及技術中心
    - CERT/TWCERT, MicroSoft, Trend
  - 網路安全資訊的溝通
    - 網路安全留言板



# 4. TANet 連線學校資通安全管理規範

- 緣由

- 資安事件的層出不窮，指出了資訊相關單位在事件防範能力上的不足，多數單位對於建置資通安全系統的需求。
- 政府制定的「行政院及所屬各機關資訊安全管理規範」，無法適用於TANet 連線學校(學術單位與政府機關的屬性不同)，有必要研擬一套專屬的資通安全管理規範。

- 執行單位

- 成功大學
- NII 產業發展協進會

# TANet 連線學校資通安全 管理規範（草案）

## • 任務

- 擬定並維護TANet 連縣學校之ISMS 建置相關標準、規範、流程、須知，以及訓練教材等文件。
- 辦理TANet 連線學校資通安全推廣相關研討會、講習會，以及師資培訓課程活動。
- 接受教育部或其他機構委託規劃及辦理TANet 連線學校資通安全推廣活動。
- 稽核檢驗TANet 連線學校ISMS 之推行結果。
- 出版TANet 連線學校資通安全相關之刊物。
- 連繫學校、政府機構、企業及學術界，促進TANet 連線學校資通安全相關議題之交流與討論。
- 確保TANet 連線學校資通安全標準與教材內涵發展符合網路與電腦資訊技術發展情形。
- 推動TANet 聯線學校之ISMS 建置之落實。
- 辦理其他為達成本小組宗旨之必要事項。

# TANet 連線學校資通安全管理規範（cont.）

- 參考規範
  - 以 ISO 27001:2005(E)、ISO17799:2005 規範為主要參考依據
  - 考量各連線單位之規模及需求，進行內容調整
  - 以行政院及所屬各機關資訊安全管理規範為主要的稽核點內容
  - 依據配合各規範之條款，進行各項目之調整。

# TANet 連線學校資通安全 管理規範（cont.）

- 適用範圍

- 本標準適用於教育部電算中心、部屬館所、縣市網中心、大專院校以及高中職資訊管理單位等資訊業務相關單位。
- 由於上述之單位，無論是層級、位置、規模有著不小的差異，為避免施行單位面對部分規範窒礙難行的問題，本標準將適用單位分為三群。
- 主要目標以「學術網路系統」與「校務資訊系統」為範疇，配合上述三群分屬，制定出適宜該施行單位所需之條款。



# TANet 連線學校資通安全管理規範 (cont.)

- 第一群

- 本群適用單位以教育部電算中心、部屬館所、縣市網中心、大專院校執行區網功能之學校等為主，適用之規範須遵從較高的嚴謹度，並且不得轉換至其他二群(除了原屬其他二群之單位外)。。

- 第二群

- 本群適用單位以公私立大專院校計中(不包含區網中心之學校)為主，適用規範之嚴謹度較低於第一群單位，若原屬本群之單位根據自身的需求，可轉往適用第一群或是第三群之準則。。

- 第三群

- 本群適用單位以公私立高中職學校資訊管理單位為主要對象；適用規範之嚴謹度為三群中最為寬鬆者，乃為配合此群中所屬單位之規模與經費之故，但亦可根據自身的需求，轉往依循另兩群之準則。

# TANet 連線學校資通安全管理規範 (cont.)

- 試作點導入

- 成大計網中心導入ISMS 之範圍

- 網路應用服務-以網路作業組所之作業流程及所提供之網路應用服務為主
    - 行政資訊應用-以校務資訊組之[校務行政電腦化]之系統開發, 維護及應用為主.

- 成大計網中心配合本計劃之考量點.

- 在政策, 安全組織尚未明確之情況下
    - 時間因素, 經費考量, 人力考量
    - 現有管理措施之改變, 環境架構之改變

# TANet 連線學校資通安全 管理規範（cont.）

- 成大計網中心配合本計劃之措施
  - 訂定資安政策, 呈請上級支持此政策並成立[資安會報]組織
  - 就目前現有安控管理措施進行文件化
    - 政策文件, 網路運作緊急應變計劃
    - 帳號密碼管理原則, 病毒防範機制, 備份作業, 主機伺服器管理, 機房門禁管理, 弱點掃描
    - 資安檢視, 資安事件處理, 資安事件通報機制, 機房設備建置, 機房安全緊急處理程序, 宿網管理辦法, 個人電腦使用規範
  - 教育訓練實施計劃
  - 永續經營計劃
  - 異地備援

# TANet 連線學校資通安全 管理規範（cont.）

- 持續調整「資通安全推動小組」架構以及相關任務分屬。
  - 調整規範內容，確認各分群之適用性。
  - 邀集各群組單位之代表，進行規範的檢視，了解實際狀況與需求。
  - 積極進行試作點的建置，務求各方面的完善。
  - 設計規範說明會以及教育訓練之文件，提供予相關單位代表，作為所屬單位之參考。
  - 製作ISMS 建置教學影片，作為日後各單位導入資安防護時的依歸。
  - 協助各連線單位建置ISMS ，以最低成本形成一有效之安全環境。

# TANet 連線學校資通安全 管理規範 (cont.)

- ISMS 推動時程
  - 準備階段(2006年)
    - 制定全責組織/任務草案
    - 訂定規範及相關參考文件
      - ISMS (Information Security management Standard)
    - 規範宣導/教育訓練/試作點建立
  - 執行階段(2007年)
    - 落實於 TANet連線學校之資安稽核服務

# 5. 總結

- 日趨完整的網路安全防禦
  - Technique
    - 區網
    - 校園網
    - 使用者端
  - Education end user
  - Security policy

## 5. 總結(cont.)

- 進行中的工作
  - 網路安全文件的彙整與分享
  - 網路管理工具與說明文件的彙整
  - Content-based 網路入侵偵測系統
    - Mining
    - Detection