

桃園區網 維運工作報告

中央大學電算中心 楊素秋

2013-10-31



報告大綱

- ❑ 1. PaloAlto 5060 IPS
- ❑ 2. Links 連線狀況偵測
 - Fail Link通告*
- ❑ 3. Cloud-based異常流量偵測
 - TopN 流量, Top UDP流量
 - FDNS異常流量
 - Kscore
- ❑ 4. Asoc資安事件自動轉通告
- ❑ 5. 未來規劃



1. PaloAlto 5060 IPS

□ PaloAlto 5060 IPS

➤ 2012-12 啟用 IPS

➤ 監看 IPS 資源應用比率

- CPU load (mgt processor, data processor)
- Sessions
- **Temperature**

➤ 2013-03 設定超量攻擊 threshold

- **當 Cpu > 70% , 影響網路傳輸狀況**
 - Dns, ssh, MS_rdp (2012-12, 2013-03 調整threshold)
 - MySql, MsSql, Pop3 (2013-03-28)



163.25.251.55/Kscore/Di x

163.25.251.55/Kscore/Demo.zul

應用程式 建議的網站 網管工具箱 網頁快訊圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate jazon.com/histor... Text File to JPG file ... 其他書籤



臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

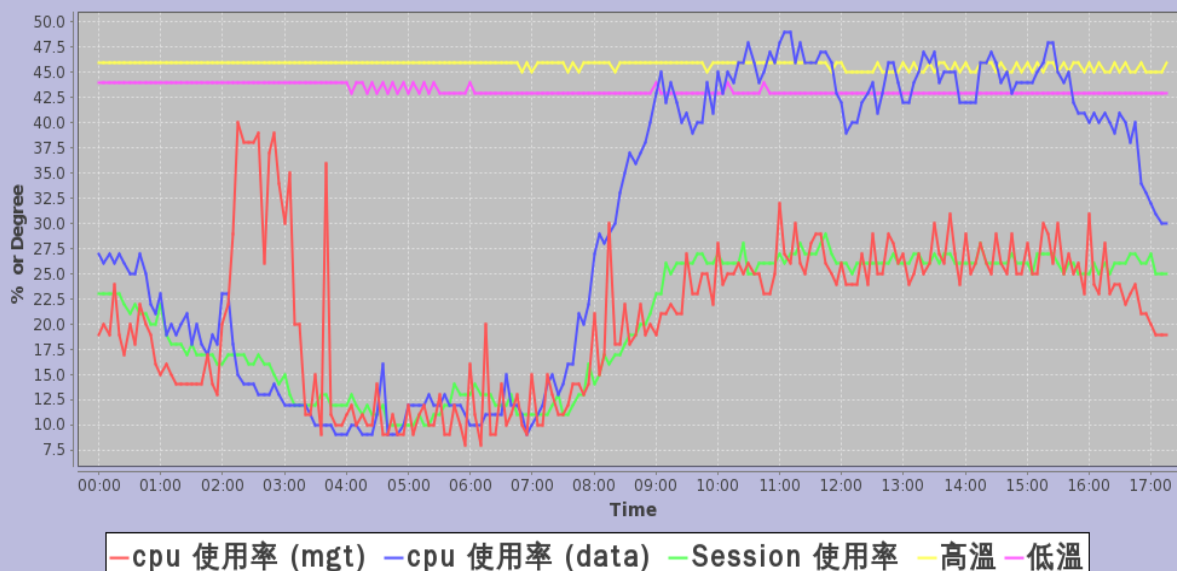
桃園區網 伺服器主機群
中央大學 伺服器主機群

Service Usage Statistics

區網 PaloAlto 5060 IPS

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-25)

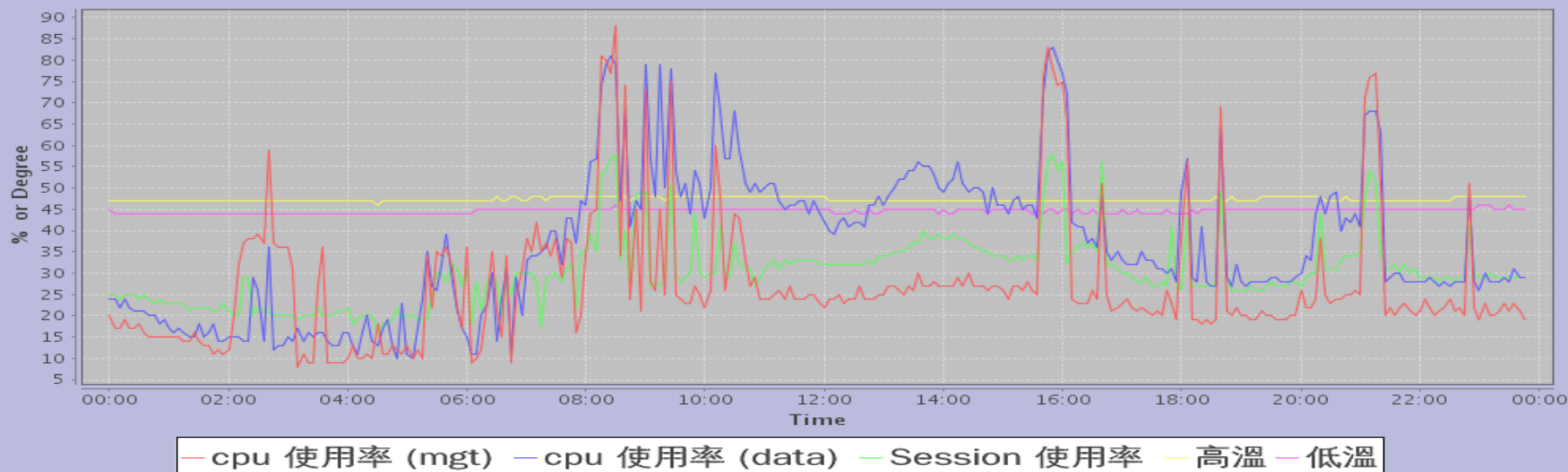
系統運作溫度 不可過高, Session使用率 不可過高



國立中央大學 電算中心

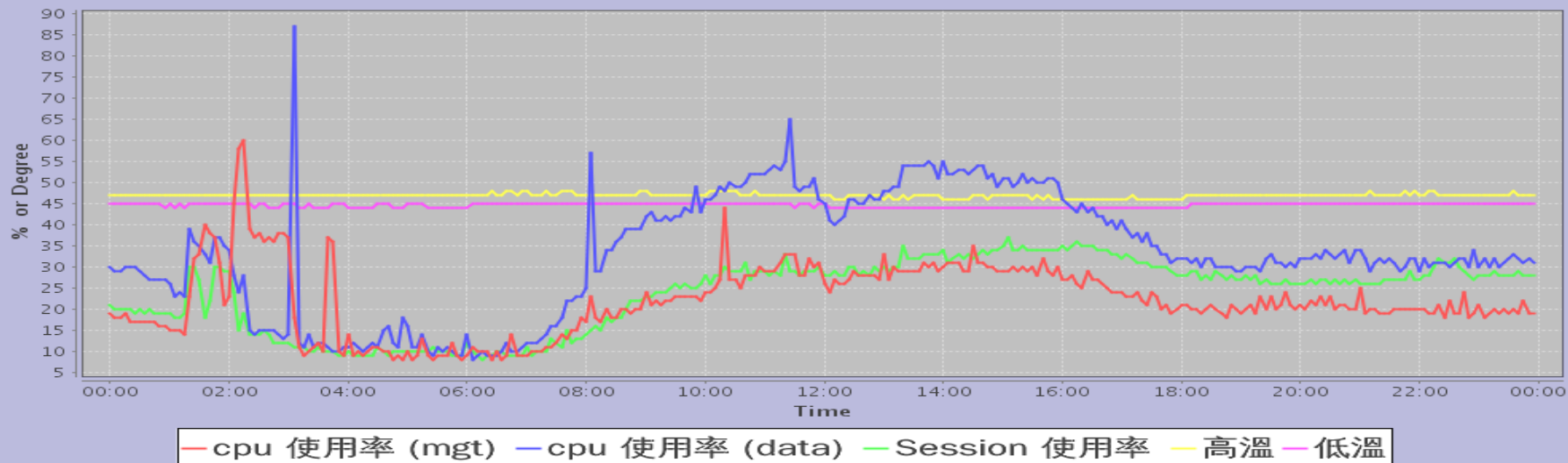
桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-09-23)

系統運作溫度 不可過高, Sesssion使用率 不可過高



桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-22)

系統運作溫度 不可過高, Sesssion使用率 不可過高





1. PaloAlto 5060 IPS 管理(cont.)

➤ 單日 Botnet自動通報 (2013-04)

- <http://links.tyrc.ncu.edu.tw/Links/viewAllBotnets.do>
- <http://kscore.tyc.edu.tw/Kscore>
 - <http://kscore.tyc.edu.tw/Kscore/searchBotnetMvc.zul>

➤ 單日網路應用量分布資訊(2013-04)

- <http://links.tyrc.ncu.edu.tw/viewAllTopApps.do>
- <http://kscore.tyc.edu.tw/Kscore>
 - http://links.tyrc.ncu.edu.tw/Thank_Pie/palo.zul



臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
 PaloAlto 5060 IPS
 區網機房 溫度/濕度

IPS 偵測資料

網路應用分布

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
 連線學校 連線狀態

異常流量監看

桃園區網 異常流量
 中央大學 異常流量

伺服器服務檢查

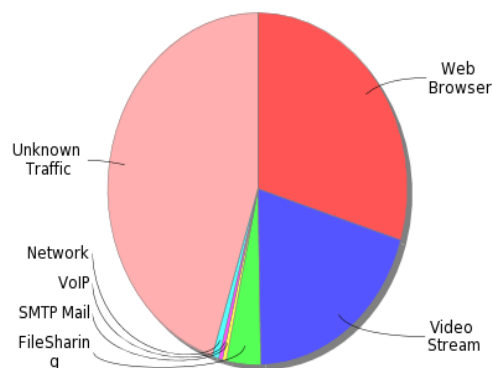
桃園區網 伺服器主機群
 中央大學 伺服器主機群

Service Usage Statistics

桃園區網 網路應用分布圖

桃園區 網路應用分布圖(日)

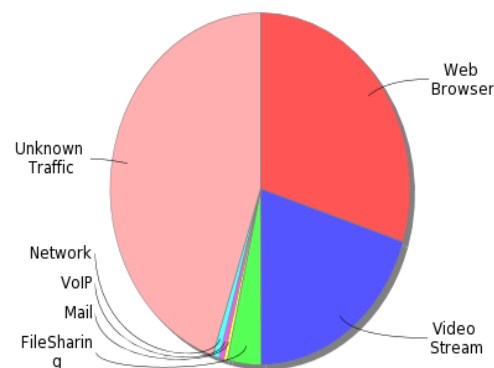
Tyrc Network App. Dist. (20131024)



● Web Browser 27.7 ● Video Stream 18.6 ● FileSharing 3.4
 ● SMTP Mail 0.4 ● VoIP 0.4 ● Network 0.7 ● Unknown Traffic 42

桃園區 網路應用分布圖(月)

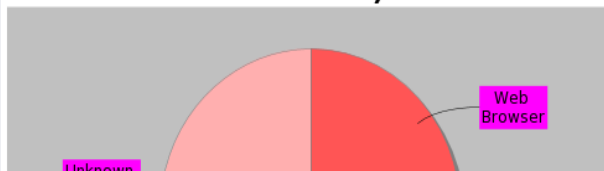
Tyrc Network App. Dist.(201310)



● Web Browser 27.9 ● Video Stream 18.6 ● FileSharing 3.4 ● Mail 0.4
 ● VoIP 0.4 ● Network 0.7 ● Unknown Traffic 41.8

桃園區 網路應用分布圖(週)

Tyrc Network App. Dist.(20131018 ~ 20131024)





臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

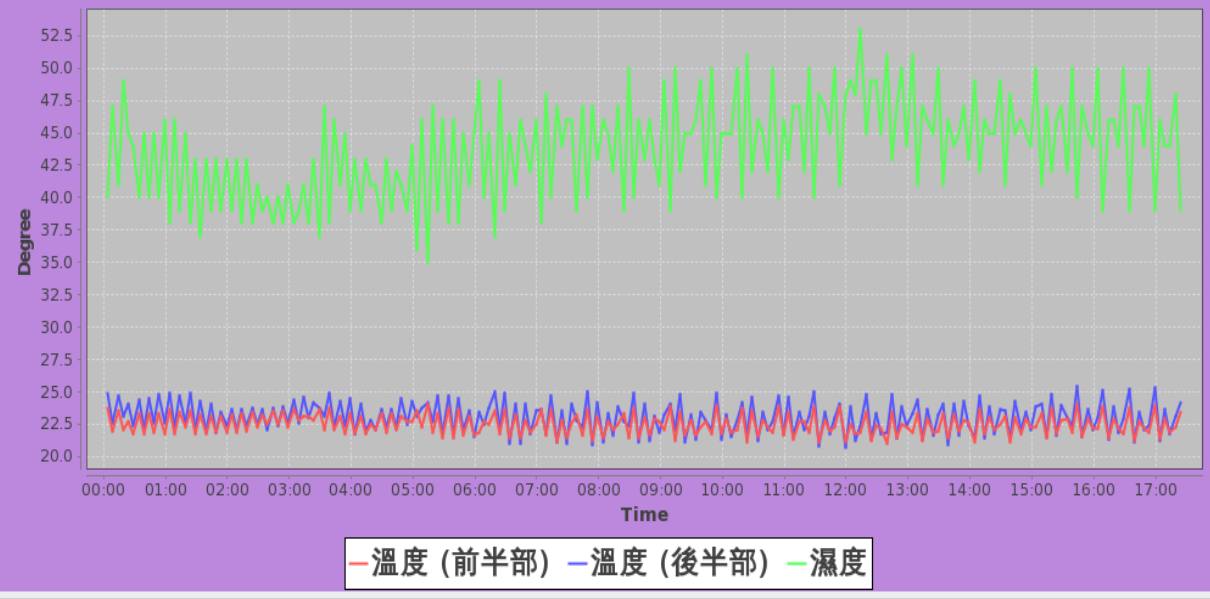
桃園區網 伺服器主機群
中央大學 伺服器主機群

Service Usage Statistics

區網 機房溫度/濕度

桃園區網機房 溫度/濕度 監看 (2013-10-25)

連網機房溫度 不可過高





臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器機群
中央大學 伺服器機群

Service Usage Statistics

區網 Cisco 6509 Router

桃園區網 Router 6509 CPU 使用率 / 溫度監看 (2013-10-25)

系統運作溫度 不可過高, CPU 使用率 不可過高



—cpu 使用率 (1 秒) —cpu 使用率 (1 分) —溫度 (1) —溫度(2)

臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

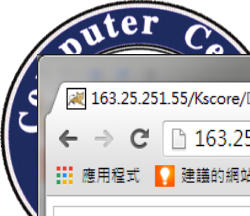
桃園區網 Botnet 通告紀錄查詢

Keyword:

Search

Botnet_信度	Botnet IP	Botnet 判別依據	Botnet 管理者 Email	通告日期
4	140.115.20.48	vsys1 Repeatedly visited (54) the same malicious URL \secure-content-delivery.com\	hsuhm@cc.ncu.edu.tw,wangcy@cc.ncu.edu.tw	2013-10-24 00:00:00
4	140.115.43.92	vsys1 Repeatedly visited (24) the same malicious URL \secure-content-delivery.com\	gracelin@ncu.edu.tw,hhtsai@cc.ncu.edu.tw	2013-10-23 00:00:00
4	140.115.231.108	vsys1 Repeatedly visited (64) the same malicious URL \api.idown.org/api/update_server.php\	center9@cc.ncu.edu.tw	2013-10-23 00:00:00
4	120.124.62.204	vsys1 Repeatedly visited (30) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	tychui@mail.vnu.edu.tw,cysung@mail.vnu.edu.tw	2013-10-23 00:00:00
4	140.115.230.9	vsys1 Repeatedly visited (32) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	center9@cc.ncu.edu.tw	2013-10-23 00:00:00
4	140.115.53.122	vsys1 Repeatedly visited (30) the same malicious URL \server.mobogenie.com/client/pb/drive/device\	jjhuang@cc.ncu.edu.tw,wjwang@csie.ncu.edu.tw	2013-10-22 00:00:00
4	140.115.219.57	vsys1 Repeatedly visited (28) the same malicious URL \api.luckyleap.net\	center9@cc.ncu.edu.tw	2013-10-22 00:00:00
4	140.135.31.2	vsys1 Repeatedly visited (20) the same malicious URL \api.luckyleap.net\	yeh@cycu.edu.tw,wenhan@cycu.edu.tw,anpin	2013-10-22 00:00:00
4	140.115.66.145	vsys1 Repeatedly visited (22) the same malicious URL \api.webconnect.co/rs\	opcwl@ncu.edu.tw,tlyeh@cc.ncu.edu.tw,howa	2013-10-22 00:00:00
4	140.135.26.155	vsys1 Repeatedly visited (33) the same malicious URL \secure-content-delivery.com\	yeh@cycu.edu.tw,wenhan@cycu.edu.tw,anpin	2013-10-21 00:00:00
4	140.138.225.90	vsys1 Repeatedly visited (32) the same malicious URL \www.searchto.kr/ncs/info_nrc.nhn\	joejoe@saturm.yzu.edu.tw,c7ht@saturm.yzu.edu.tw	2013-10-21 00:00:00

國立中央大學 電算中心



臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
PaloAlto 5060 IPS
區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
桃園區網 KSCORE 紀錄查詢
中央大學 異常流量偵測系統

伺服器服務檢查

桃園區網 伺服器主機群
中央大學 伺服器主機群

區網 Asoc Abuse紀錄查詢

Keyword:

Asoc_ID	IP	School	AbuseType	Date
AISAC-28522	192.192.250.155	開南大學資訊科技中心	對外攻擊	2013-10-23 11:16:31
AISAC-28283	140.135.198.35	中原大學電算中心	對外攻擊	2013-10-21 08:56:54
AISAC-28251	210.60.0.2	國立體育大學	殭屍電腦(Bot)	2013-10-21 08:26:22
ASOC-EWA-201310-0645	140.135.25.98	中原大學電算中心	對外攻擊	2013-10-17 16:02:10
AISAC-28124	192.83.181.124	國立體育大學	網頁置換	2013-10-16 22:26:26
AISAC-28110	192.192.250.94	開南大學資訊科技中心	對外攻擊	2013-10-16 17:36:05
AISAC-27968	140.115.71.237	中央大學電機	對外攻擊	2013-10-15 14:27:08
AISAC-27966	140.115.152.210	中央大學通訊	對外攻擊	2013-10-15 14:26:58
AISAC-27875	140.115.5.32	中央大學教職員宿舍	對外攻擊	2013-10-12 22:36:32
AISAC-27855	140.115.65.65	中央大學機械	對外攻擊	2013-10-11 11:56:30
AISAC-27789	140.115.185.82	總務處	對外攻擊	2013-10-08 15:26:05
AISAC-27641	210.60.0.2	國立體育大學	殭屍電腦(Bot)	2013-10-03 14:56:32
AISAC-27470	140.135.24.101	中原大學	對外攻擊	2013-09-28 13:46:17
AISAC-27339	120.124.129.31	健行科技大學	對外攻擊	2013-09-25 08:36:27
AISAC-27294	140.135.50.72	中原大學	殭屍電腦(Bot)	2013-09-24 13:53:05
AISAC-26791	140.135.56.124	中原大學	對外攻擊	2013-09-09 17:48:01
AISAC-26599	140.138.31.199	元智大學	殭屍電腦(Bot)	2013-09-05 10:27:26
AISAC-26458	140.115.65.65	中央大學機械	對外攻擊	2013-09-03 09:28:42
NTUSOC-EWA-201308-0094	120.124.74.210	萬能科技大學	可疑連線	2013-08-30 11:40:55
AISAC-26247	140.115.49.1	中央大學生資	對外攻擊	2013-08-27 15:57:33

國立中央大學 電算中心



臺灣學術網路 桃園區網中心

網路設備運作狀況

Cisco 6509 Router
 PaloAlto 5060 IPS
 區網機房 溫度/濕度

IPS 偵測資料

通告之 Botnet 紀錄查詢
 網路應用分布

Asoc 資安通告事件查詢

Asoc 事件通告紀錄查詢
 Asoc 事件通告紀錄

連網狀況 / 管理資訊

Rwhois IP 資訊查詢
 連線學校 連網狀態

異常流量監看

桃園區網 異常流量偵測系統
 桃園區網 KSCORE 紀錄查詢
 中央大學 異常流量偵測系統

伺服器服務檢查

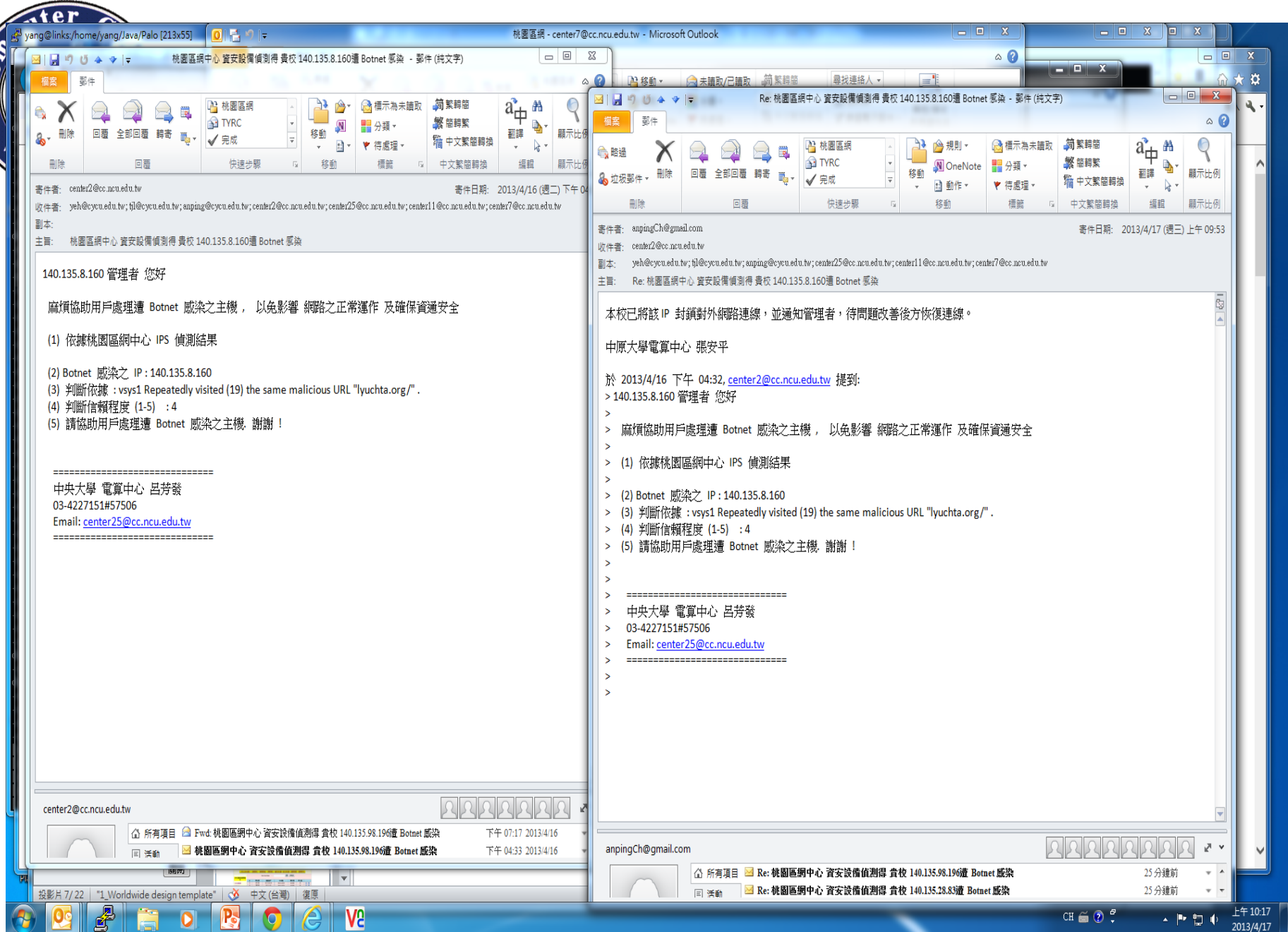
桃園區網 伺服器主機群
 中央大學 伺服器主機群

桃園區網 UDP Flooding 紀錄查詢

Keyword:

IP	Rate_in (MB)	Rate_out	Pkz_in (B)	Pkz_out	Flow_in	Flow_out	信賴係數	偵測日期
98.126.161.92	51	241	89	487	72818	81370	4	2013-10-25 04:30:00
98.126.161.92	90	371	90	489	127292	125051	4	2013-10-25 04:20:00
98.126.161.91	27	10	123	287	57482	14195	12	2013-10-25 04:00:00
98.126.161.91	18	0	49	0	85847	0	3	2013-10-25 05:00:00
98.126.161.91	15	0	49	0	72116	0	3	2013-10-25 04:50:00
98.126.161.91	17	0	48	0	83692	0	4	2013-10-25 04:40:00
98.126.161.91	15	0	48	0	77147	0	4	2013-10-25 04:10:00
98.126.161.91	27	10	123	287	57482	14195	4	2013-10-25 04:00:00
98.126.161.91	17	0	49	0	80008	0	5	2013-10-25 06:00:00
98.126.161.91	17	0	48	0	84725	0	6	2013-10-25 05:50:00
98.126.161.91	17	0	50	0	77820	0	6	2013-10-25 05:40:00
98.126.161.91	16	0	50	0	75720	0	6	2013-10-25 05:30:00
98.126.161.91	18	0	50	0	84967	0	7	2013-10-25 05:20:00
98.126.161.91	17	0	49	0	78046	0	7	2013-10-25 05:10:00
98.126.161.91	18	0	49	0	85847	0	8	2013-10-25 05:00:00
98.126.161.91	16	0	49	0	74063	0	2	2013-10-25 07:00:00
98.126.161.91	15	0	48	0	73113	0	2	2013-10-25 06:50:00
98.126.161.91	17	0	49	0	82524	0	3	2013-10-25 06:40:00
98.126.161.91	17	0	49	0	82615	0	4	2013-10-25 06:30:00
98.126.161.91	16	0	50	0	76250	0	4	2013-10-25 06:20:00

國立中央大學 電算中心





2. Links 連線狀況監測

□ 連線學校連線品質

- 連線介面紀錄
- 網管通訊紀錄
- 偵測資料依據 (10-minutes)
 - ping Router IP
 - retrieve www page
- 監看連線狀況
- 連線中斷紀錄
- 連線中斷自動通告*
- 連線 狀況月報表 / 計分月報表

yang@links/home/yang/java/Palo [213x55] 桃園區網 - center7@cc.ncu.edu.tw - Microsoft Outlook

http://140.115.2.27/Links/viewAllInterfaces.do 連網介面資訊 x (5) Facebook

Google 網管通訊錄 * 連線介面 搜尋 更多設定 >>

網頁(P) 安全性(S) 工具(O) ?

桃園區網中心

ASOC_Abuse 通報 區網服務台 區網連線檢查 網管好幫手 區網 TopN 流量 中央 TopN 流量 流量異常偵測 區網網管平台

Enter School Name 搜尋 新增紀錄

Links 連線狀態偵測與通告

Links 偵測首頁

- * 網管通訊錄
- * 連線介面
- * 連線計分
- * 連線狀態 (10-minutes)
- * 連線中斷紀錄
- * 連線中斷處理
- 連線狀況月報表
- 連線計分月報表
- * 單日 Botnet 感染主機
- * 單日網路應用量分布

Id	學校名稱	連網設備 IP	www網址	連線 狀態	URL 狀態	
15	中央大學	203.72.244.236	www.ncu.edu.tw	reachable	OK	修改 刪除
16	元智大學	203.71.2.237	www.yzu.edu.tw	reachable	OK	修改 刪除
17	中原大學	203.71.2.61	www.cycu.edu.tw	reachable	OK	修改 刪除
21	萬能科技大學	203.71.2.209	www.vnu.edu.tw	reachable	OK	修改 刪除
22	健行科技大學	203.71.2.49	www.uch.edu.tw	reachable	OK	修改 刪除
23	開南大學	203.71.2.129	www.knu.edu.tw	reachable	OK	修改 刪除
24	銘傳大學	203.71.2.242	www.mcu.edu.tw	un_reachable	OK	修改 刪除
25	金門縣教育網路中心	192.83.196.180	www.km.edu.tw	reachable	OK	修改 刪除
26	創新技術學院	203.71.2.157	www.tiit.edu.tw	reachable	OK	修改 刪除
28	國防大學理工學院	203.71.2.5	www.ccit.ndu.edu.tw	un_reachable	OK	修改 刪除
29	國防大學	203.71.2.4	www.ndu.edu.tw	reachable	OK	修改 刪除
32	中央警察大學	203.71.2.84	www.cpu.edu.tw	reachable	OK	修改 刪除
33	連江縣教育網路中心	192.83.196.179	www.matsu.edu.tw	reachable	OK	修改 刪除
34	新生醫專	203.71.2.69	www.hsc.edu.tw	reachable	OK	修改 刪除
35	陸軍專科學校	203.71.2.82	www.aaroc.edu.tw	reachable	OK	修改 刪除
36	大華中學	203.71.2.73	www.thsh.tyc.edu.tw	reachable	OK	修改 刪除
37	桃園區網中心	192.192.227.14	163.28.49.4	reachable	OK	修改 刪除
38	桃園縣教育網路中心	192.83.196.181	www.tyc.edu.tw	reachable	OK	修改 刪除
39	體育大學(桃園)	203.71.2.225	www.nts.edu.tw	reachable	OK	修改 刪除
40	核能研究所	203.71.2.41	www.iner.gov.tw	reachable	OK	修改 刪除
41	復旦中學	203.71.2.66	www.ftsh.tyc.edu.tw	reachable	OK	修改 刪除
42	內壢高中	203.71.2.198	www.nlhs.tyc.edu.tw	reachable	OK	修改 刪除

投影片 10/ 22 "1.Worldwide design template" 中文(台灣) 復原 75% 25分鐘前 上午 10:53 2013/4/17

Asoc_Notify - center7@cc.ncu.edu.tw - Microsoft Outlook

http://140.115.2.27/Links/viewAllContacts.do

學校網管資訊 (5) Facebook

Google 搜尋 分享 更多設定 >>

網頁(P) 安全性(S) 工具(O) ?

桃園區網中心

ASOC_Abuse 通報 區網服務台 區網連線檢查 網管好幫手 區網 TopN 流量 中央 TopN 流量 流量異常偵測 區網網管平台

Links 連線狀態偵測與通告

[* Links 偵測首頁](#)

[* 網管通訊錄](#)

[* 連線介面](#)

[* 連線計分](#)

[* 連線狀態 \(10-minutes\)](#)

[* 連線中斷紀錄](#)

[* 連線中斷處理](#)

[連線狀況月報表](#)

[連線計分月報表](#)

[* 單日 Botnet 感染主機](#)

[* 單日網路應用量分布](#)

Enter Contact Name

Id	學校名稱	網館員	Email	聯絡電話	Cell	學校地址	
228	中央大學電算中心(資訊工程)	蘇木春	muchun@csie.ncu.edu.tw	4227151~57500	4252561	桃園縣(320)中壢市中大路300號	Edit Delete
229	中央大學電算中心	王雅慈	center11@cc.ncu.edu.tw	4227151~57514	4252561	桃園縣(320)中壢市中大路300號	Edit Delete
230	中央大學電算中心	劉秋美	center6@cc.ncu.edu.tw	4227151~57501	4252561	桃園縣(320)中壢市中大路300號	Edit Delete
231	中央大學電算中心	楊素秋	center7@cc.ncu.edu.tw	4227151~57505	4252561	桃園縣(320)中壢市中大路300號	Edit Delete
232	中央大學電算中心	呂芳發	center25@cc.ncu.edu.tw	4227151~57506	4252561	桃園縣(320)中壢市中大路300號	Edit Delete
233	中央大學電算中心	周小慧	center15@cc.ncu.edu.tw	4227151~57527	4252561	桃園縣(320)中壢市中大路300號	Edit Delete
234	中原大學電算中心	葉平	yeh@cycu.edu.tw	2652910	2652999	桃園縣(320)中壢市普仁里中北路200號	Edit Delete
235	中原大學電算中心	蔡佳玲	tjl@cycu.edu.tw	2652910	2652999	桃園縣(320)中壢市普仁里中北路200號	Edit Delete
236	元智大學資服處網媒組	鄭建祥	joejoe@saturn.yzu.edu.tw	4638800~2969	4638236	桃園縣(320)中壢市內壢遠東路135號	Edit Delete
237	元智大學資服處網媒組	陳惠慈	c7ht@saturn.yzu.edu.tw	4638800~2961	4638236	桃園縣(320)中壢市內壢遠東路135號	Edit Delete
238	中央警察大學電算中心	溫哲彥	cwen@mail.cpu.edu.tw	3282142	3282321#4481	桃園縣(333)龜山鄉樹人路56號	Edit Delete
239	中央警察大學電算中心	黃嘉宏	ihhuano@mail.cpu.edu.tw	3282142	3282321#4481	桃園縣(333)龜山鄉樹人路56號	Edit Delete

桃園區網中心

ASOC Abuse 通報

區網服務台

區網連線檢查

網管好幫手

區網 TopN 流量

中央 TopN 流量

流量異常偵測

區網網管平台

Links 連線狀態偵測與通告

* Links 偵測首頁

* 網管通訊錄

* 連線介面

* 連線計分

* 連線狀態 (10-minutes)

* 連線中斷紀錄

* 連線中斷處理

連線狀況月報表

連線計分月報表

* 單日 Botnet 感染主機

* 單日網路應用量分布

連線中斷處理

Enter School Name

搜尋

新增紀錄

Id	學校名稱	連網設備 IP	中斷起迄時間	事件原因/處理	紀錄時間	
13	中壢家商	203.71.2.201	2013-03-26 10:50 ~ 11:20 am	該校光纖線路調整造成斷線, 調整後回復正常	2013-03-28 18:11:14.0	修改 刪除
12	武陵高中	203.71.2.79	2013-03-22(Fri) 13:00 ~ 14:30 pm	網路架構調整, 廠商在設定, 有動到部分設定, 造成網路中斷。修正完畢後恢復正常聯外網路	2013-03-22 17:51:08.0	修改 刪除
10	金門縣網中心	192.83.196.180	03-13(三) 08:00 -- 10:30 AM	全島電力中斷造成, 電力恢復後, 連網正常	2013-03-19 16:39:58.0	修改 刪除
11	連江縣網中心	192.83.196.179	03-17(日) 08:20 am -- 23:20 pm	校園工程挖斷線路造成, 施工單位復原後連網正常	2013-03-19 11:40:36.0	修改 刪除
9	新興高中	203.71.2.195	2012-12-20 13:30 PM ~ 14:20 PM	連線異常, 設備重啟	2012-12-26 18:51:46.0	修改 刪除
8	核能研究所	203.71.2.41	(1) 2012-12-13 22:00 PM ~ 2012-12-13 23:30 PM, (2) 2012-12-14 23:30 PM ~ 2012-12-16 15:30 PM	計畫性中斷(機房整線工程)	2012-12-19 11:13:49.0	修改 刪除
5	萬能科技大學	203.71.2.209	2012-11-02 11:40 AM ~ 13:00 PM	IPS 重開後恢復連線	2012-12-06 11:27:25.0	修改 刪除
7	六和高中	203.71.2.72	2012-12-04 21:10 PM ~ 2012-12-05 08:30 AM	12/4 更動防火牆及聯外 router 設備作業, 導致連外節點主連在 12/5 上班後重啟連	2012-12-05 14:47:38.0	修改 刪除

http://140.115.2.27/Links/viewAllFail.do

桃園區網連線狀況月報表 (2012-10)

學校名稱	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. 中央大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	98	100	100	100	100	100	100	100									
2. 元智大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	97	100	100	100	100	100	100	100									
3. 中原大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	98	100	100	100	100	100	100	100									
4. 萬能科技大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	98	100	100	100	100	100	100	100									
5. 健行科技大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	98	100	100	100	100	100	100	100									
6. 開南大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
7. 銘傳大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
8. 金門縣網中心	100	100	100	99	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
9. 創新技術學院	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
10. 國防大學理工學院	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
11. 國防大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
12. 中央警察大學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
13. 連江縣網中心	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	94	100	100	100	97	98	100									
14. 新生醫專	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
15. 陸軍專科學校	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	99	98	100									
16. 大華中學	100	100	100	100	100	100	100	100	100	100	99	100	100	100	100	100	100	100	100	100	100	100									
17. 桃園區網中心	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	99	100	100									
18. 桃園縣網中心	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	99	99	100									
19. 體育大學(桃園)	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
20. 核能研究所	100	100	99	100	96	0	26	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
21. 復旦中學	100	100	100	100	100	100	100	100	100	76	100	100	100	100	100	100	100	100	100	100	100	100									
22. 內壢高中	100	100	100	100	100	100	100	100	100	97	100	98	100	100	100	100	100	100	100	99	100	100									
23. 桃園農工	100	100	100	99	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
24. 新興高中	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
25. 治平中學	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
26. 圓光佛學研究所	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
27. 育達高中	100	100	100	95	99	100	100	100	100	100	100	98	100	100	100	100	100	100	100	99	97	100									
28. 至善高中	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100									
29. 楊梅高中	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	99	100									



3. 資安事件自動轉通告

□ Asoc 資安事件自動轉通告與管理系統

➤ 包含 Asoc 資安通報種類

- AISAC-20607
- NTUSOC-EWA-201210-0015
- ASOC-EWA-201210-0610
- NTHU-EWA-201210-0086

➤ 桃園區網 ASOC ABUSE轉通報系統

<http://ncusvr.ncu.edu.tw>

http://ncusvr.ncu.edu.tw/Contact_Tiles

<http://kscore.tyc.edu.tw/Kscore/searchAsocMvc.zul>

Computer Center

http://tyc.ncu.edu.tw/Contact_Tiles/abuse_tyc.html

Asoc ABUSE_TYC

Google 搜尋 分享 更多設定

登入

桃園區網中心

[Asoc_Abuse](#)
[區網連線檢查](#)
[網管好幫手](#)
[中央 FDNS/TopN 流量](#)
[區網 FDNS/TopN 流量](#)
[流量異常偵測 \(圖\)](#)
[區網網管平台](#)

ASOC ABUSE通報

[中央大學 Abuse](#)
[桃園區網 Abuse](#)

Asoc ABUSE_TYC List

通告編號	主機 IP	所屬學校	網管人員	事件類型	通告日期
AISAC-13522	192.192.250.192	開南大學	吳世彥	殭屍電腦(Bot)	2012-10-19 11:35:57.0
AISAC-13507	140.115.219.120	中央大學	戴元任	對外攻擊	2012-10-19 07:35:56.0
AISAC-13502	203.68.248.248	新興高中	林燦堂	殭屍電腦(Bot)	2012-10-19 07:15:56.0
AISAC-13415	140.132.27.183	中正理工學院	張凱威	殭屍電腦(Bot)	2012-10-16 14:15:53.0
AISAC-13413	120.125.84.170	銘傳大學	游象勇	殭屍電腦(Bot)	2012-10-16 12:55:53.0
AISAC-13363	203.68.248.248	新興高中	林燦堂	殭屍電腦(Bot)	2012-10-16 07:15:53.0
NTUSOC-EWA-201210-0015	210.60.239.13	青輔會青年職訓中心	蔡宏松	疑發起對外攻擊	2012-10-16 07:04:28.0
AISAC-13353	140.115.113.150	軟體中心	王躍強	殭屍電腦(Bot)	2012-10-15 13:45:53.0
AISAC-13351	120.124.199.253	清雲科技大學	林大為	殭屍電腦(Bot)	2012-10-15 13:25:53.0
AISAC-13339	210.59.41.252	啟英高中	宋清風	垃圾郵件(Spam)	2012-10-15 09:46:00.0
AISAC-13332	140.115.14.178	電算中心	戴元任	對外攻擊	2012-10-15 09:05:53.0
AISAC-13327	140.115.120.128	太空	呂凌霄	對外攻擊	2012-10-15 08:35:53.0

http://tyc.ncu.edu.tw/Contact_Tiles/abuse_tyc.html

CH 上午 10:38 2012/10/22

Asoc_Notify - center7@cc.ncu.edu.tw - Microsoft Outlook

我的最愛

- 收件匣 (1)
- 郵件備份
- 刪除的郵件 (153)
- ADuse_mail (25)
- ASOC (4)
- Asoc_Notify (6)
- FDNS
- NCUCC (21)
- ISMS (14)
- TWNIC
- 工讀生進度
- 曾黎明老師
- 劉進光/柏安
- OR
- SA
- Statistics (1)
- 學校通知 (24)
- RSS 摘要
- TANET (17)
- Spring
- 桃園區網 (23)
- AppFuse
- BW_Mgt (3)
- SVRCHK (57)
- TV/AREN
- 網路維護 (6)
- Botnet 計畫
- 垃圾郵件 (4)
- 朋友們 (6)
- Han_Doc (1)
- Rita (1)
- 郵件
- 行事曆
- 連絡人

項目: 18 未讀取: 6

搜尋 Asoc_Notify (Ctrl+E)

重要性: 普通 (18 個項目, 6 個未讀取)	發件者	主題	收到日期
	@ center2@cc...	教育機構資安通報 140.115.77.46 - AISAC-21654 請儘速回報電算中心	2013/4/8 (週一) 下午 12:51
	@ center2@cc...	教育機構資安通報 140.115.107.17 - AISAC-21599 請儘速回報電算中心	2013/4/8 (週一) 上午 9:40
	service	資安預警通報(駭客掃描ASOC-EWA-201304-0060)	2013/4/1 (週一) 下午 2:10
	@ yang@ncusv...	教育機構資安通報 140.115.155.199 - AISAC-21451 請儘速回報電算中心	2013/4/1 (週一) 上午 11:11
	@ yang@ncusv...	教育機構資安通報 140.115.216.28 - ASOC-EWA-201303-1389 請儘速回報電算中心	2013/3/29 (週五) 上午 9:40
	@ yang@ncusv...	教育機構資安通報 140.115.77.46 - AISAC-21335 請儘速回報電算中心	2013/3/29 (週五) 上午 8:40
	hsuht@csie.n...	Re: 教育機構資安通報 140.115.53.27 - AISAC-20686 請儘速回報電算中心	2013/3/19 (週二) 下午 1:11
	Xaver Y.R. Ch...	Re: 教育機構資安通報 140.115.53.27 - AISAC-20686 請儘速回報電算中心	2013/3/19 (週二) 下午 1:11
	@ yang@ncusv...	教育機構資安通報 140.115.53.27 - AISAC-20686 請儘速回報電算中心	2013/3/19 (週二) 上午 8:40
	@ yang@ncusv...	教育機構資安通報 140.115.65.235 - AISAC-20687 請儘速回報電算中心	2013/3/19 (週二) 上午 8:40
	service	(事件單編號:AISAC-20686)(告知通報)入侵事件警訊	2013/3/19 (週二) 上午 8:40
	service	(事件單編號:AISAC-20687)(告知通報)入侵事件警訊	2013/3/19 (週二) 上午 8:40
	@ yang@ncusv...	教育機構資安通報 140.115.82.191 - AISAC-20685 請儘速回報電算中心	2013/3/19 (週二) 上午 8:40
	service	(事件單編號:AISAC-20685)(告知通報)入侵事件警訊	2013/3/19 (週二) 上午 8:40
	service	(事件單編號:AISAC-20683)(告知通報)入侵事件警訊	2013/3/19 (週二) 上午 8:40
	service	(事件單編號:AISAC-20682)(告知通報)入侵事件警訊	2013/3/19 (週二) 上午 8:40
	@ 劉進光center...	Fwd: Fw: 教育機構資安通報 140.115.216.180 - AISAC-20588 請儘速回報電算中心	2013/3/18 (週一) 下午 1:11
	service	(事件單編號:AISAC-20607)(告知通報)入侵事件警訊	2013/3/18 (週一) 上午 9:40

教育機構資安通報 140.115.77.46 - AISAC-21654 請儘速回報電算中心 - 郵件 (純文字)

發件者: center2@cc.ncu.edu.tw 寄件日期: 2013/4/8 (週一) 下午 12:51

收件者: arden@cc.ncu.edu.tw; cychen@mgt.ncu.edu.tw; clement10601@hotmail.com; 994003063@cc.ncu.edu.tw; 994003067@cc.ncu.edu.tw; 994003528@cc.ncu.edu.tw; 984003534@cc.ncu.edu.tw; 100403062@cc.ncu.edu.tw; 984003531@cc.ncu.edu.tw; 100403532@cc.ncu.edu.tw; 994003042@cc.ncu.edu.tw; 100403017@cc.ncu.edu.tw; center2@cc.ncu.edu.tw; center25@cc.ncu.edu.tw; center11@cc.ncu.edu.tw; center7@cc.ncu.edu.tw

副本:

主旨: 教育機構資安通報 140.115.77.46 - AISAC-21654 請儘速回報電算中心

訊息: _home_yang_java_Asoc_EWA_Attach_AISAC-21654.html (2 KB)

140.115.77.46 管理者 您好

麻煩處理, 並請 24hr. 內 提供以下相關資訊, 以便通告 教育機構資安通報平台

- (1)機器型號
- (2)作業系統
- (3)保管人
- (4)作何用途
- (5)是否有防火牆或其他防護功能
- (6)如何處理, 謝謝!

請將上述資訊回覆電算中心, 聯絡人資料如下

=====

中央大學 電算中心 劉進光
03-4227151#57508
Email: center2@cc.ncu.edu.tw
Email: center25@cc.ncu.edu.tw

=====

center2@cc.ncu.edu.tw

所有項目 Fwd: 桃園區網中心 資安設備偵測得 貴校 140.135.98.196遭 Botnet 感染 下午 07:17 2013/4/16
同 活動 桃園區網中心 資安設備偵測得 貴校 140.135.98.196遭 Botnet 感染 下午 04:33 2013/4/16

2013/10/31

©2012 Computer Center, National Central University.

22

Asoc_Notify - center7@cc.ncu.edu.tw - Microsoft Outlook

教育機構資安通報 140.115.107.17 :: AISAC-21599 請速回報電算中心 - 郵件 (純文字)

刪除 回復 全部回復 轉寄 快速步驟 移動 標籤 中文繁體轉換 編輯 顯示比例

附件: center2@cc.ncu.edu.tw 郵件日期: 2013/4/8 (週一) 上午 11:20

收件者: cake@cc.ncu.edu.tw; wronglin@cc.ncu.edu.tw; cassie@cc.ncu.edu.tw; wible45@yahoo.com; solars@cc.ncu.edu.tw; 965002017@cc.ncu.edu.tw; center2@cc.ncu.edu.tw; center25@cc.ncu.edu.tw; center11@cc.ncu.edu.tw; center7@cc.ncu.edu.tw

副本:

主旨: 教育機構資安通報 140.115.107.17 :: AISAC-21599 請速回報電算中心

訊息 | _home_yang_Java_Asoc_EWA_Attach_AISAC-21599.html (3 KB)

140.115.107.17 管理者 您好

麻煩處理, 並請 24hr. 內 提供以下相關資訊, 以便通告 教育機構資安通報平台

- (1)機器型號
- (2)作業系統
- (3)保管人
- (4)作何用途
- (5)是否有防火牆或其他防護功能
- (6)如何處理, 謝謝!

請將上述資訊回覆電算中心, 聯絡人資料如下

=====

中央大學 電算中心 劉道光
03-4227151#57508
Email: center2@cc.ncu.edu.tw
Email: center25@cc.ncu.edu.tw

=====

center2@cc.ncu.edu.tw

所有項目 | Fwd: 桃園區網中心 資安設備偵測得 貴校 140.135.98.196遭 Botnet 感染 下午 07:17 2013/4/16

同 活動 | 桃園區網中心 資安設備偵測得 貴校 140.135.98.196遭 Botnet 感染 下午 04:33 2013/4/16

教育機構資安通報 140.115.77.46 :: AISAC-21654 請速回報電算中心 - 郵件 (純文字)

刪除 回復 全部回復 轉寄 快速步驟 移動 標籤 中文繁體轉換 編輯 顯示比例

附件工具

刪除 快速列印 另存新檔 儲存所有附件 移除附件 全選 複製 中文繁體轉換 顯示郵件

動作 選取項目 中文繁體轉換 郵件

檔案名稱: _home_yang_Java_Asoc_EWA_Attach_AISAC-21654.html
大小: 2 KB

訊息 | _home_yang_Java_Asoc_EWA_Attach_AISAC-21654.html (2 KB)

教育機構資安通報平台

事件類型: 入侵事件警訊

事件單編號 AISAC-21654

原發布編號	NTUSOC-INT-201304-0311	原發布時間	2013-04-08 12:37:37
事件類型	對外攻擊	原發現時間	2013-04-08 11:16:00
事件主旨	教育部資安事件通告—國立中央大學[140.115.77.46]主機嘗試Host掃描攻擊警訊通知		
事件描述	弱點掃描攻擊內容包含檢測重要網頁或內部主機系統弱點的各類攻擊封包, 會造成目標主機服務運作異常或網路阻塞等問題, 一旦目標主機被攻擊成功, 來源主機將可取得目標系統控制權並執行任意程式, 或成為攻擊跳板, 擴大攻擊事件範圍。入侵偵測防禦系統偵測到來源IP (140.115.77.46) 發送針對性類型的攻擊封包, 短時間內針對大量目標IP進行弱點掃描攻擊。		
手法研判	無		
建議措施	經確認後, 若發現未經授權的內部主機對內部主機進行弱點掃描, 則可利用防火牆ACL阻擋該外部IP連線, 並持續監控後續活動及採取適當防禦措施, 降低內部主機被入侵的機率。		
此事件需要進行通報, 請貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議, 歡迎與我們連絡。			

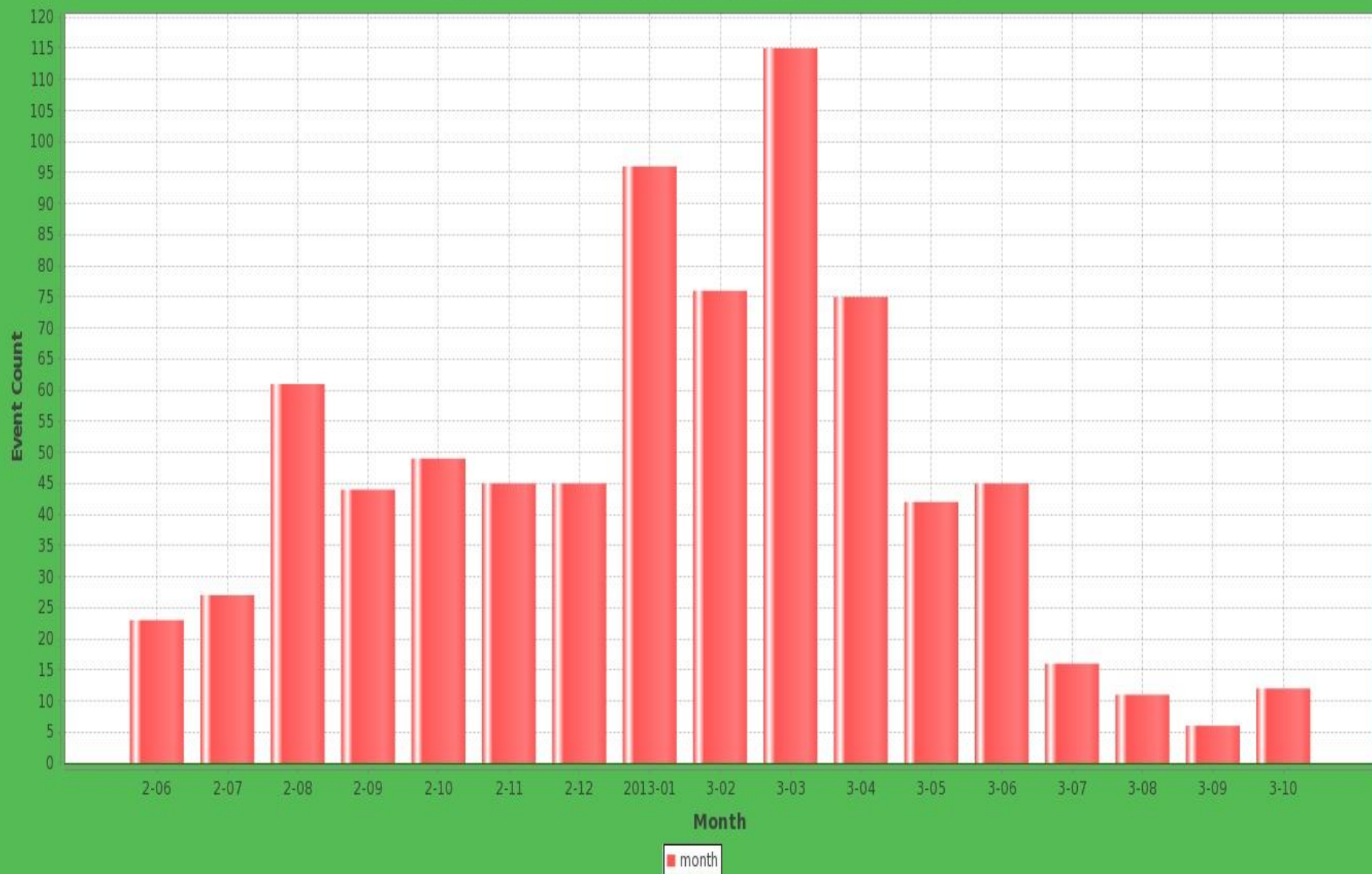
教育機構資安通報應變小組
網址: <https://info.cert.tanet.edu.tw/>
專線電話: 07-5250211
網路電話: 98400000
E-Mail: service@cert.tanet.edu.tw

center2@cc.ncu.edu.tw

所有項目 | Fwd: 桃園區網中心 資安設備偵測得 貴校 140.135.98.196遭 Botnet 感染 下午 07:17 2013/4/16

同 活動 | 桃園區網中心 資安設備偵測得 貴校 140.135.98.196遭 Botnet 感染 下午 04:33 2013/4/16

桃園區網 Asoc 資安事件分布圖 (2012-2013)





3. 資安事件自動轉通告(cont.)

□ 區網中心的應變措施

- **Botnet 自動通告** (2013-04-16)
- AppServ套件的phpmyadmin含漏洞(2013-05)
 - <http://cert.tanet.edu.tw/prog/shownews.php?id=671>
- **Udp Flooding Traffic Detection** (2013-06)
 - IP spoofing問題 (**Unicast Reverse Path Forwarding**)
 - **ip verify unicast source reachable-via rx**
- **圖形化 PaloAlto 5060指標參數監看介面** (2013-09)
- **請協助處理 140.xxx.yy.zz 主機遭感染** (2013-10)

桃園區網中心

ASOC_Abuse 通報

服務台

連線檢查

網管好幫手

區網異常連結

流量異常偵測

網管平台

FDNS 異常流量監測

* FDNS 首頁

* FDNS 異常監看

* TopN 流量排行

* TopN 連結排行

* 連線單位 單日流量

* 網路應用 單日流量

* 連線單位流量分布

* 網路應用流量分布

* TopN Udp 流量排行

* 單日 UDP Flood Traffic

* 單時 UDP Flood Traffic

* 詳細 UDP Flood Traffic

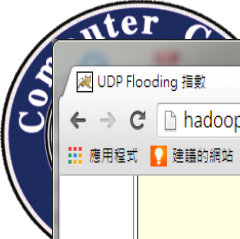
* UDP Traffic 指數

UDP Kscore

Enter IP Address

搜尋

Id	主機 IP	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	flow_in	flow_out	Kscore	紀錄時間
72551	94.125.182.255	1024	0	1379	0	37954	0	21	2013-10-28 07:30:00.0
72445	94.125.182.255	13431	0	1383	0	216583	0	16	2013-10-28 05:50:00.0
72773	93.115.210.72	644	0	653	0	562474	0	14	2013-10-28 10:10:00.0
72550	91.236.182.1	9190	0	1382	0	222346	0	21	2013-10-28 07:30:00.0
72766	89.43.74.6	30	0	49	0	599493	0	8	2013-10-28 11:00:00.0
72767	89.43.74.6	27	0	49	0	548980	0	9	2013-10-28 10:50:00.0
72768	89.43.74.6	30	0	49	0	599893	0	10	2013-10-28 10:40:00.0
72769	89.43.74.6	28	0	49	0	566037	0	11	2013-10-28 10:30:00.0
72770	89.43.74.6	28	0	48	0	576577	0	12	2013-10-28 10:20:00.0
72771	89.43.74.6	33	0	49	0	665774	0	13	2013-10-28 10:10:00.0
72772	89.43.74.6	35	0	49	0	699709	0	14	2013-10-28 10:00:00.0



UDP Flooding 指數									
hadoop5.tyc.edu.tw/Tops/viewAllKscores.do									
應用程式 建議的網站 網管工具箱									
72512	163.30.68.10	0	1262	0	1366	0	15054	14	2013-10-28 07:40:00.0
72513	163.30.68.10	0	2992	0	1357	0	44483	14	2013-10-28 07:30:00.0
72514	163.30.68.10	0	978	0	1320	0	34948	14	2013-10-28 07:20:00.0
72509	163.30.45.16	0	3968	0	1385	0	43867	14	2013-10-28 07:30:00.0
72510	163.30.45.16	0	1985	0	1385	0	22838	14	2013-10-28 07:20:00.0
72433	163.30.45.16	0	2028	0	1386	0	15364	9	2013-10-28 05:50:00.0
72595	163.30.40.224	0	1910	0	1371	0	7487	9	2013-10-28 08:30:00.0
72596	163.30.40.224	0	263	0	1497	0	16105	10	2013-10-28 08:20:00.0
72507	163.30.40.224	0	3789	0	1386	0	48052	13	2013-10-28 07:30:00.0
72508	163.30.40.224	0	2011	0	1385	0	21888	13	2013-10-28 07:20:00.0
72432	163.30.28.220	0	1099	0	1386	0	15340	9	2013-10-28 05:50:00.0
72734	163.30.201.135	0	570	0	1317	0	55693	7	2013-10-28 11:00:00.0
72735	163.30.201.135	0	1043	0	1321	0	68834	7	2013-10-28 10:50:00.0
72736	163.30.201.135	0	1738	0	956	0	656679	7	2013-10-28 10:10:00.0
72660	163.30.201.135	0	1101	0	1322	0	77692	8	2013-10-28 09:40:00.0
72661	163.30.201.135	0	1150	0	1341	0	110557	8	2013-10-28 09:30:00.0
72662	163.30.201.135	0	1127	0	1336	0	85642	8	2013-10-28 09:20:00.0
72592	163.30.201.135	0	557	0	1334	0	39205	9	2013-10-28 09:00:00.0



UDP Flooding 指數										
hadoop5.tyc.edu.tw/Tops/viewAllKscores.do										
應用程式 建議的網站 網管工具箱 網頁快訊圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate jazon.com/histor... Text File to JPG file ... gotoalberto/mong...										
72580	140.138.152.6	0	1912	0	1371	0	8871	9	2013-10-28	08:30:00.0
72430	140.138.152.6	0	2016	0	1377	0	15143	9	2013-10-28	05:50:00.0
72578	140.138.152.1	0	2940	0	1370	0	11430	9	2013-10-28	08:30:00.0
72579	140.138.152.1	0	2498	0	1379	2	23615	9	2013-10-28	08:20:00.0
72429	140.138.146.167	0	2412	0	1377	0	18859	9	2013-10-28	05:50:00.0
72326	140.135.32.189	1652	30	1283	71	1566	682	7	2013-10-28	01:40:00.0
72327	140.135.32.189	214	12	1217	68	1040	479	7	2013-10-28	01:30:00.0
72491	140.135.10.82	0	4151	0	1372	0	24694	12	2013-10-28	07:30:00.0
72492	140.135.10.82	0	2044	0	1367	0	5863	12	2013-10-28	07:20:00.0
72428	140.135.10.82	0	2137	0	1375	0	17381	9	2013-10-28	05:50:00.0
72574	140.115.156.73	0	3584	0	1193	0	399374	8	2013-10-28	09:00:00.0
72651	140.115.156.73	0	3584	0	1193	0	399374	8	2013-10-28	09:00:00.0
72575	140.115.156.73	0	3721	0	1109	0	664901	9	2013-10-28	08:50:00.0
72576	140.115.156.73	0	1851	0	1285	0	98861	9	2013-10-28	08:40:00.0
72577	140.115.156.73	0	516	0	1361	0	4135	9	2013-10-28	08:30:00.0
72485	140.115.156.73	0	3361	0	1039	0	839962	7	2013-10-28	07:50:00.0
72486	140.115.156.73	0	3814	0	1042	0	908869	8	2013-10-28	07:40:00.0
72487	140.115.156.73	0	4294	0	1166	0	574874	9	2013-10-28	07:30:00.0

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-28)

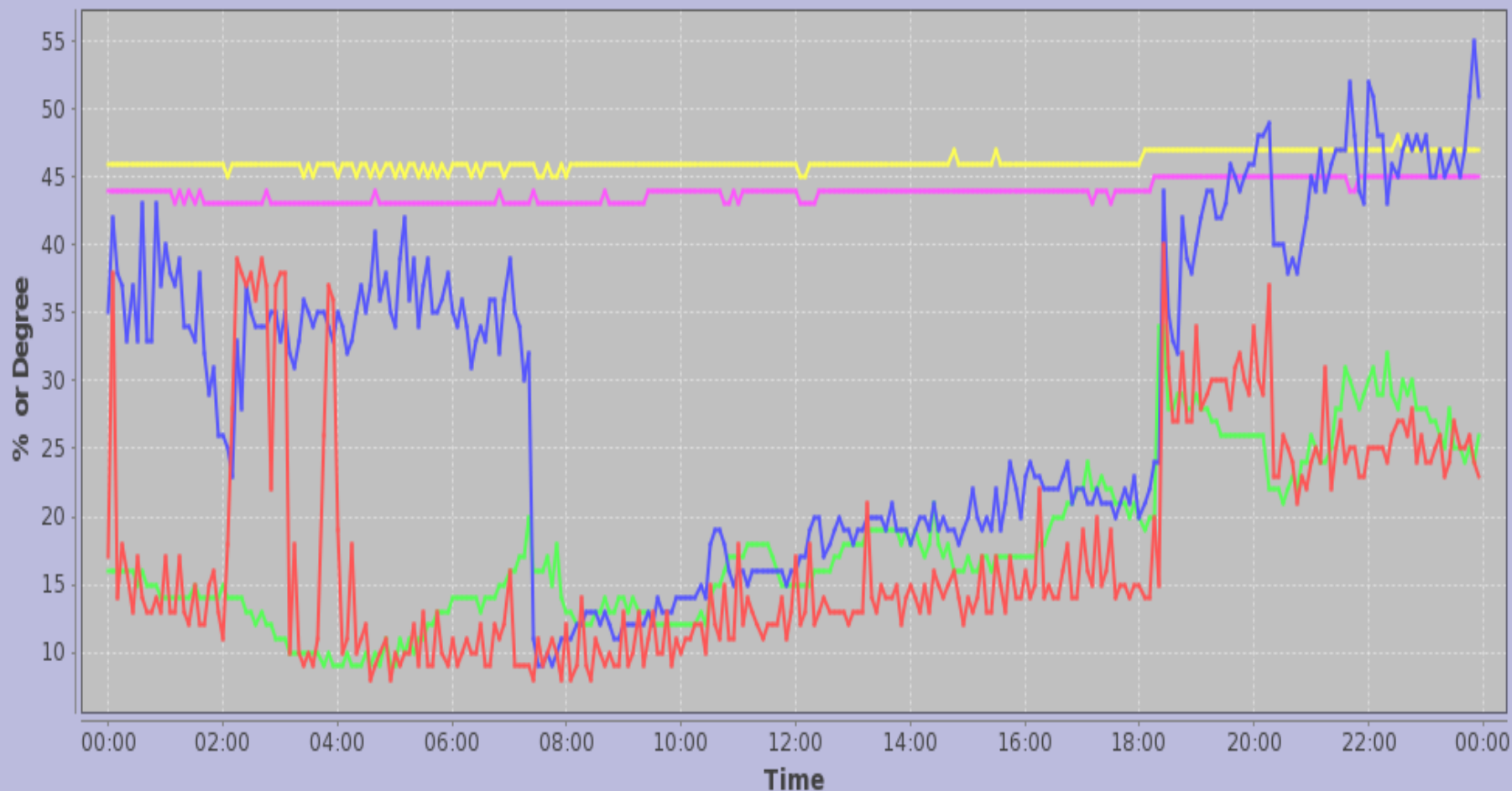
系統運作溫度 不可過高, Sesstion使用率 不可過高



—cpu 使用率 (mgt) —cpu 使用率 (data) —Session 使用率 —高溫 —低溫

桃園區網 PaloAlto 5060 資源使用率 / 溫度監看 (2013-10-27)

系統運作溫度 不可過高, Sesssion使用率 不可過高



—cpu 使用率 (mgt) —cpu 使用率 (data) —Session 使用率 —高溫 —低溫

寄件者: Susan Yang <center7@cc.ncu.edu.tw>

寄件日期: 2013/10/6 (週日) 上午 10:28

收件者: 'richardw@cc.ncu.edu.tw'; 'spchen@cc.ncu.edu.tw'; 'yjchang@dop.ncu.edu.tw'; '982006011@cc.ncu.edu.tw'; '101226031@cc.ncu.edu.tw'

副本: center6@cc.ncu.edu.tw; center25@cc.ncu.edu.tw; Tai Yuan-Runn; 'cc_王組長' (center11@cc.ncu.edu.tw)

主旨: 請協助處理 140.115.49.6 140.115.41.199 兩主機是否遭感染

依據近日幾天的觀察

140.115.49.6 140.115.41.199 有相當異常的傳送紀錄

1. 傳送超大量的Packet size 小 (< 60 Byte /pkt) 的封包
2. 建立超大量的socket connections (> 70000 connection /10-minute)

兩主機有可能遭感染, 請協助處理

Thanks!

UDP Kscore

表單的頂端

Enter IP Address

表單的底部

Id	主機 IP	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	flow_in	flow_out	Kscore	紀錄時間
72607	140.115.49.6	11	4	53	49	72633	73802	2	2013-10-05 23:10:00.0
72608	140.115.49.6	14	4	55	47	88632	76509	4	2013-10-05 23:00:00.0
72591	140.115.49.6	11	4	55	47	71673	76889	2	2013-10-05 22:50:00.0
72592	140.115.49.6	12	4	54	49	77875	73300	4	2013-10-05 22:40:00.0
72593	140.115.49.6	12	4	56	48	77408	74789	6	2013-10-05 22:30:00.0
72594	140.115.49.6	12	4	56	47	74666	76236	8	2013-10-05 22:20:00.0

Susan Yang

所有項目 RE: 桃園區網IPS流量

DE: 請協助處理 140.115.156.73 140.115.152.142 兩主機是否遭感染

下午 12:21 2013/10/27

下午 03:32 2013/10/26





4. Cloud-based之異常流量偵測

□ Cloud-based異常流量偵測系統

➤ 桃園區網TopN 流量排行

- <http://hadoop5.tyc.edu.tw/Tops>
- TopN 流量/連結 排行
- TopN Flooding排行
- 連線學校 網路量排行
- 國中小/高中職/大學 網路量 分布

➤ 中央大學 TopN 流量排行

<http://140.115.2.23/Tops>

- 中央大學 Top UDP 流量排行
- 中央大學 TopN Flooding排行

Flood 異常監視 x

hadoop5.tyc.edu.tw/Tops/viewAllFdns.do

應用程式 建議的網站 網管工具箱 網頁快訊圖庫 Map Reduce Seco... download Invoice - Sample In... (Part 1) Configurin... Spring Hibernate jazon.com/histor... Text File to JPG file ... gotoalberto/mong...

其他書籤

桃園區網中心

ASOC_Abuse 通報 服務台 連線檢查 網管好幫手 區網異常連結 流量異常偵測 網管平台

FDNS 異常流量監測

- * FDNS 首頁
- * FDNS 異常監看
- * TopN 流量排行
- * TopN 連結排行
- * 連線單位 單日流量
- * 網路應用 單日流量
- * 連線單位流量分布
- * 網路應用流量分布
- * TopN Udp 流量排行
- * 單日 UDP Flood Traffic
- * 單時 UDP Flood Traffic
- * 詳細 UDP Flood Traffic
- * UDP Traffic 指數

Year (4-digit): 2013 Month: 10 Day: 14 Submit: Display

桃園區網 異常流量監測 (2013-10-14)

id	IP	連結總量	輸入	輸出	總流量 (MB)	PktSize
1	192.83.181.136@25	8952413	4288800	4663613	4721	86
2	140.135.112.22@25	5035581	2290030	2745551	2791	81
3	100.125.11.230@443	3216545	1448836	1867708	18770	506
4	91.226.177.72@19	3243834	2233435	1010399	3060	935
5	108.170.31.115@19	3225677	2242283	983394	3181	946
6	120.125.11.230@80	3061391	1391692	1669699	189484	1025
7	163.30.198.58@80	2730393	79086	2651307	1847	110
8	210.60.0.2@443	2407437	1272921	1134516	38039	750
9	210.60.0.2@80	2359895	1256680	1103215	270683	1113
10	163.30.82.222@80	2011169	801016	1210153	1016	103
11	70.185.249.253@19	1937417	1431581	505836	1995	1002
12	163.25.34.254@80	1906163	736450	1169713	120281	893
13	210.71.44.7@80	1754708	601810	1152898	1248	142
14	84.173.58.64@19	1687475	1181745	505730	1629	953
15	163.25.34.254@443	1624897	636957	987940	19010	607
16	71.204.91.107@19	1369521	959215	410306	1314	951
17	140.135.112.22@80	1320222	543706	776516	26937	807
18	173.2.104.147@19	1125819	759304	366515	1047	919
19	68.39.141.59@19	1090946	789478	301468	1073	981
20	72.208.222.67@19	1087461	787350	300111	1071	982

桃園區網中心

ASOC_Abuse 通報 服務台 連線檢查 網管好幫手 區網異常連結 流量異常偵測 網管平台

FDNS 異常流量監測

* [FDNS 首頁](#)

* [FDNS 異常監看](#)

* [TopN 流量排行](#)

* [TopN 連結排行](#)

* [連線單位 單日流量](#)

* [網路應用 單日流量](#)

* [連線單位流量分布](#)

* [網路應用流量分布](#)

* [TopN Udp 流量排行](#)

* [單日 UDP Flood Traffic](#)

* [單時 UDP Flood Traffic](#)

* [詳細 UDP Flood Traffic](#)

* [UDP Traffic 指數](#)

Year (4-digit): 2013 Month: 10 Day: 28 Submit:

中央大學 TopN Connection (2013-10-28)

id	IP	連結總量	輸入	輸出	總流量 (MB)	PktSize
1	120.124.18.19	10379145	2	10379143	6944	465
2	74.91.112.214	6083863	6083863	0	13559	878
3	140.115.156.73	5296233	0	5296233	33837	1140
4	210.60.0.2	4757787	2441127	2316660	212397	479
5	163.30.201.135	3249987	95	3249892	16342	1175
6	163.25.34.254	1765878	743657	1022221	58048	843
7	31.13.68.16	1662176	1155732	506444	21506	559
8	120.124.84.213	1622759	3957	1618802	6226	1092
9	37.187.53.64	1519537	1519537	0	13858	1210
10	120.125.11.230	1345785	639509	706276	56217	882
11	163.28.5.24	1315758	642790	672968	61716	949
12	163.28.5.16	1074556	531285	543271	39358	954
13	163.28.5.27	1070249	492087	578162	65984	973
14	163.28.5.17	1028231	516118	512113	64493	976
15	119.160.254.215	987491	460898	526593	20183	813
16	119.160.254.197	963934	450291	513643	20155	817
	203.72.116.27	905740	407799	497941	11372	705

桃園區網中心

ASOC_Abuse 通報 服務台 連線檢查 網管好幫手 區網異常連結 流量異常偵測 網管平台

FDNS 異常流量監測

- * [FDNS 首頁](#)
- * [FDNS 異常監看](#)
- * [TopN 流量排行](#)
- * [TopN 連結排行](#)
- * [連線單位 單日流量](#)
- * [網路應用 單日流量](#)
- * [連線單位流量分布](#)
- * [網路應用流量分布](#)
- * [TopN Udp 流量排行](#)
- * [單日 UDP Flood Traffic](#)
- * [單時 UDP Flood Traffic](#)
- * [詳細 UDP Flood Traffic](#)
- * [UDP Traffic 指數](#)

Year (4-digit): 2013 Month: 10 Day: 28 Submit: Display

中央大學 TopN Traffic (2013-10-28)

id	IP	HostName	總量 (MB)	輸入	輸出	FlowCnt	PktSize	傳輸期間
1	210.60.0.2@17	210.60.0.2	47016	44757	2258	465814	176	66
2	140.115.156.73@17	widm73.csie.ncu.edu.tw	33837	0	33837	5296233	1140	12
3	203.64.11.36@17	203.64.11.36	33457	25269	8187	15440	715	15
4	210.64.136.148@17	210.64.136.148	28029	232	27797	49225	172	62
5	120.124.10.115@17	120-124-10-115.IP.vnu.edu.tw	20216	1320	18896	71280	560	66
6	112.120.86.169@17	n11212086169.netvigator.com	19023	18713	310	12818	1114	65
7	163.25.122.249@17	163.25.122.249	17675	14	17661	2147	1453	51
8	140.115.152.135@17	140.115.152.135	16811	176	16635	38450	1044	50
9	163.30.201.135@17	163.30.201.135	16338	0	16338	3249823	1175	14
10	120.124.128.5@17	yuhualee.csie.uch.edu.tw	15432	12	15420	1582	1464	42
11	94.125.182.255@17	ircu.atw.hu	14456	14456	0	254537	1382	2
12	163.30.197.163@17	163.30.197.163	14410	12586	1823	46274	758	13
13	37.187.53.64@17	cloud-l-fr64.castmess.it	13858	13858	0	1519537	1210	10
14	74.91.112.214@17	74.91.112.214	13559	13559	0	6083863	878	9
15	195.60.214.23@17	195.60.214.23	12037	12037	0	105331	1378	2
16	101.133.173.201@17	undmnet.renchenmosing.net	11070	11070	0	227701	1501	2
17	120.125.94.225@17	ip-120-125-94-225.mcu.edu.tw	11030	9167	1862	233394	628	66
18	49.01.146@17	undmnet.renchenmosing.net	10018	10018	0	250180	1201	2



4. Cloud-based之異常流量偵測 (cont.)

Id	主機 IP	sum_in (MB)	sum_out	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	Duration (10-minutes)	flow_in	flow_out	紀錄時間
12120	140.115.126.180	0	34	0	34	0	58	1	1	577852	2013-05-22 08:00:00.0
12109	140.115.126.180	0	36	0	36	0	58	1	1	610785	2013-05-22 07:50:00.0
12033	140.115.126.180	0	50	0	50	0	59	1	0	838475	2013-05-22 06:30:00.0
12019	140.115.126.180	0	101	0	101	0	113	1	1	888568	2013-05-22 06:20:00.0
12006	140.115.126.180	0	1316	0	1316	0	1051	1	0	1250280	2013-05-22 06:10:00.0
11986	140.115.126.180	0	35	0	35	0	59	1	1	583344	2013-05-22 05:50:00.0
11962	140.115.126.180	0	62	0	62	0	59	1	1	1033436	2013-05-22 05:30:00.0
11948	140.115.126.180	0	107	0	107	0	59	1	2	1797380	2013-05-22 05:20:00.0
11937	140.115.126.180	0	78	0	78	0	59	1	1	1312964	2013-05-22 05:10:00.0
11907	140.115.126.180	0	102	0	102	0	59	1	3	1712362	2013-05-22 04:50:00.0
11894	140.115.126.180	0	130	0	130	0	59	1	0	2162525	2013-05-22 04:40:00.0
11879	140.115.126.180	0	181	0	181	0	75	1	3	2369188	2013-05-22 04:30:00.0



4. Cloud-based之異常流量偵測 (cont.)

Id	主機 IP	sum_in (MB)	sum_out	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	Duration (10-minutes)	flow_in	flow_out	紀錄時間
47 72	140.115.65.235	0	12127	0	6063	0	1348	2	0	380364	2013-05-21 06:00:00.0
47 51	140.115.65.235	0	11243	0	3747	0	1349	3	0	412958	2013-05-21 05:00:00.0
47 35	140.115.65.235	0	24190	0	4838	0	1351	5	0	1098029	2013-05-21 04:00:00.0
47 12	140.115.65.235	0	25393	0	5078	0	1350	5	0	1019859	2013-05-21 03:00:00.0
46 83	140.115.65.235	0	23846	0	4769	0	1349	5	0	881038	2013-05-21 02:00:00.0
46 48	140.115.65.235	0	15231	0	3046	0	1292	5	0	1013157	2013-05-21 01:00:00.0
45 66	140.115.65.235	0	15266	0	3053	0	1325	5	0	402953	2013-05-20 22:00:00.0
45 30	140.115.65.235	0	6180	0	2060	0	1289	3	0	302215	2013-05-20 21:00:00.0
40 37	140.115.65.235	0	9141	0	4570	0	1320	2	0	77897	2013-05-20 06:00:00.0
40 03	140.115.65.235	0	18274	0	3654	0	1321	5	0	223395	2013-05-20 05:00:00.0
39 65	140.115.65.235	0	66	0	33	0	49	2	0	1331874	2013-05-20 04:00:00.0
39 18	140.115.65.235	0	56	0	28	0	49	2	0	1129277	2013-05-20 03:00:00.0
38 87	140.115.65.235	0	13896	0	3474	0	1334	4	0	878366	2013-05-20 02:00:00.0



4. Cloud-based之異常流量偵測 (cont.)

Id	主機 IP	sum_in (MB)	sum_out	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	Duration (10-minutes)	flow_in	flow_out	紀錄時間
846	140.115.161.32	0	213	0	53	0	45	4	12	4547014	2013-05-20 16:00:00.0
847	140.115.8.45	0	139	0	34	1289	45	4	0	2985596	2013-05-20 16:00:00.0
845	140.115.66.203	0	127	0	31	1177	101	4	1	1228376	2013-05-20 16:00:00.0
842	140.115.49.6	173	126	43	31	130	148	4	359910	346309	2013-05-20 16:00:00.0
849	60.208.78.233	0	124	0	31	78	72	4	0	480157	2013-05-20 16:00:00.0
839	140.115.30.225	1307	42	653	21	1430	112	2	1055	2836	2013-05-20 16:00:00.0
837	140.115.186.11	0	67	0	16	0	45	4	862	1449162	2013-05-20 16:00:00.0
833	140.115.155.208	3021	7	755	1	1027	45	4	299138	3349	2013-05-20 16:00:00.0
834	140.115.155.54	11	0	11	0	45	739	1	212521	0	2013-05-20 16:00:00.0
850	89.137.189.9	575	0	143	0	52	1481	4	10707968	0	2013-05-20 16:00:00.0

UDP Flooding 指數
hadoop5.tyc.edu.tw/Tops/viewAllKscores.do
您希望 Google Chrome 儲存密碼嗎? 儲存密碼

ASOC_Abuse 通報 服務台 連線檢查 網管好幫手 區網異常連結 流量異常偵測 網管平台

桃園區網中心

UDP Kscore

Enter IP Address

Id	主機 IP	rate_in (MB)	rate_out	pkz_in(B)	pkz_out	flow_in	flow_out	Kscore	紀錄時間
66609	94.23.71.149	365	0	1027	0	354850	0	2	2013-10-12 06:50:00.0
66610	94.23.71.149	469	0	1027	0	455949	0	2	2013-10-12 06:40:00.0
66611	94.23.71.149	660	0	1027	0	641043	0	2	2013-10-12 06:30:00.0
66612	94.23.71.149	927	0	1027	0	900952	0	2	2013-10-12 06:20:00.0
66613	94.23.71.149	875	0	1027	0	849885	0	2	2013-10-12 06:10:00.0
66614	94.23.71.149	945	0	1027	0	917807	0	2	2013-10-12 06:00:00.0
66537	94.23.71.149	1565	0	1027	0	1519196	0	2	2013-10-12 03:50:00.0
66538	94.23.71.149	1391	0	1027	0	1351248	0	2	2013-10-12 03:40:00.0
66539	94.23.71.149	1449	0	1027	0	1407345	0	2	2013-10-12 03:30:00.0
66540	94.23.71.149	1410	0	1027	0	1369465	0	2	2013-10-12 03:20:00.0
66541	94.23.71.149	1412	0	1027	0	1371275	0	2	2013-10-12 03:10:00.0
66542	94.23.71.149	1265	0	1027	0	1228360	0	2	2013-10-12 03:00:00.0
66450	94.23.71.149	627	0	1027	0	609230	0	1	2013-10-12 02:50:00.0

FDNS 異常流量監測

- * [FDNS 首頁](#)
- * [FDNS 異常監看](#)
- * [TopN 流量排行](#)
- * [TopN 連結排行](#)
- * [連線單位 單日流量](#)
- * [網路應用 單日流量](#)
- * [連線單位流量分布](#)
- * [網路應用流量分布](#)
- * [TopN Udp 流量排行](#)
- * [單日 UDP Flood Traffic](#)
- * [單時 UDP Flood Traffic](#)
- * [詳細 UDP Flood Traffic](#)
- * [UDP Traffic 指數](#)

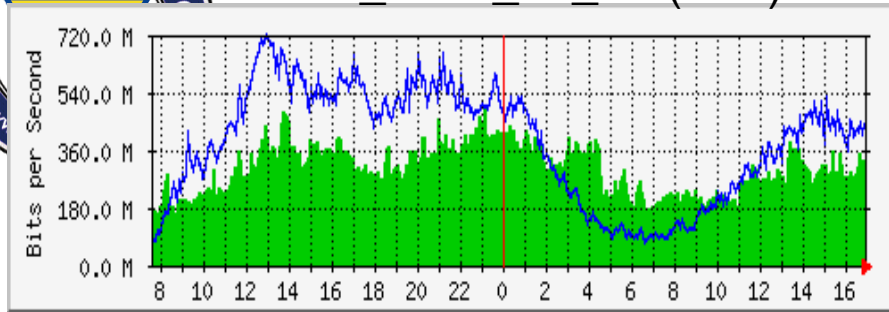


UDP Flooding 指數										
hadoop5.tyc.edu.tw/Tops/viewAllKscores.do										
您希望 Google Chrome 儲存密碼嗎？ 儲存密碼										
66617	140.115.49.230	166	92	1048	259	3294	53980	1	13:00:00.0	2013-10-12 09:50:00.0
66618	140.115.49.230	166	90	1057	282	3127	53352	1	13:00:00.0	2013-10-12 09:30:00.0
66680	140.115.42.164	47	3834	55	1462	355	1689	1	14:10:00.0	2013-10-12 14:10:00.0
66681	140.115.42.164	1282	4161	390	1328	309	1332	2	14:00:00.0	2013-10-12 14:00:00.0
66643	140.115.42.164	80	5052	70	1462	417	1466	1	13:40:00.0	2013-10-12 13:40:00.0
66644	140.115.42.164	1348	2264	591	1215	401	1797	1	13:30:00.0	2013-10-12 13:30:00.0
66645	140.115.42.164	44	1151	66	1450	448	2106	1	13:20:00.0	2013-10-12 13:20:00.0
66646	140.115.42.164	27	523	77	1448	448	1475	1	13:10:00.0	2013-10-12 13:10:00.0
66647	140.115.42.164	34	724	173	1416	387	1889	1	13:00:00.0	2013-10-12 13:00:00.0
66615	140.115.42.164	1158	3866	414	1303	293	1468	1	09:10:00.0	2013-10-12 09:10:00.0
66616	140.115.42.164	179	1339	848	1387	280	1299	1	09:00:00.0	2013-10-12 09:00:00.0
66471	140.115.217.9	0	279	0	1026	0	270862	1	03:50:00.0	2013-10-12 03:50:00.0
66472	140.115.217.9	0	495	0	1026	0	481117	1	03:20:00.0	2013-10-12 03:20:00.0
66473	140.115.217.9	0	505	0	1026	0	490798	1	03:10:00.0	2013-10-12 03:10:00.0
66474	140.115.217.9	0	430	0	1026	0	417960	1	03:00:00.0	2013-10-12 03:00:00.0
66384	140.115.217.9	0	163	0	1024	0	158726	1	02:50:00.0	2013-10-12 02:50:00.0
66550	140.115.205.194	0	98	0	1027	0	95250	1	06:30:00.0	2013-10-12 06:30:00.0
66551	140.115.205.194	0	407	0	1026	0	396195	1	06:20:00.0	2013-10-12 06:20:00.0
66552	140.115.205.194	0	372	0	1026	0	361916	1	06:10:00.0	2013-10-12 06:10:00.0
66553	140.115.205.194	0	417	0	1027	0	405301	1	06:00:00.0	2013-10-12 06:00:00.0

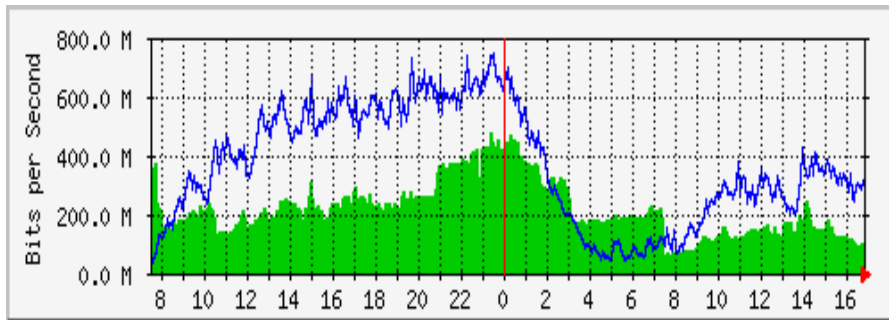


UDP Flooding 指數										
hadoop5.tyc.edu.tw/Tops/viewAllKscores.do										
您希望 Google Chrome 儲存密碼嗎? <input type="checkbox"/> 儲存密碼										
66570	140.135.112.141	0	313	0	1026	1	304056	1	2013-10-12 06:20:00.0	
66571	140.135.112.141	0	327	0	1025	0	318161	1	2013-10-12 06:10:00.0	
66486	140.135.112.141	0	248	0	1025	0	241222	1	2013-10-12 03:50:00.0	
66487	140.135.112.141	0	272	0	1026	0	264213	1	2013-10-12 03:40:00.0	
66488	140.135.112.141	0	299	0	1025	0	290871	1	2013-10-12 03:30:00.0	
66489	140.135.112.141	0	276	0	1025	0	268474	1	2013-10-12 03:20:00.0	
66490	140.135.112.141	0	278	0	1025	0	270418	1	2013-10-12 03:10:00.0	
66491	140.135.112.141	0	244	0	1027	0	236981	1	2013-10-12 03:00:00.0	
66397	140.135.112.141	0	221	0	1025	0	215107	1	2013-10-12 02:50:00.0	
66398	140.135.112.141	0	273	0	1027	0	265193	1	2013-10-12 02:40:00.0	
66399	140.135.112.141	0	280	0	1025	0	272648	1	2013-10-12 02:30:00.0	
66400	140.135.112.141	0	271	0	1027	0	263341	1	2013-10-12 02:20:00.0	
66401	140.135.112.141	0	268	0	1024	0	261074	1	2013-10-12 02:10:00.0	
66402	140.135.112.141	0	286	0	1025	0	278149	1	2013-10-12 02:00:00.0	
66560	140.135.11.158	0	1033	0	1027	75	993126	1	2013-10-12 06:50:00.0	
66561	140.135.11.158	1	1052	57	1035	34	979476	1	2013-10-12 06:40:00.0	
66562	140.135.11.158	0	1001	0	1027	34	966329	1	2013-10-12 06:30:00.0	
66563	140.135.11.158	0	904	0	1027	36	871042	1	2013-10-12 06:20:00.0	
66564	140.135.11.158	1	920	70	1039	34	837295	1	2013-10-12 06:10:00.0	
66565	140.135.11.158	0	898	0	1025	36	872679	1	2013-10-12 06:00:00.0	

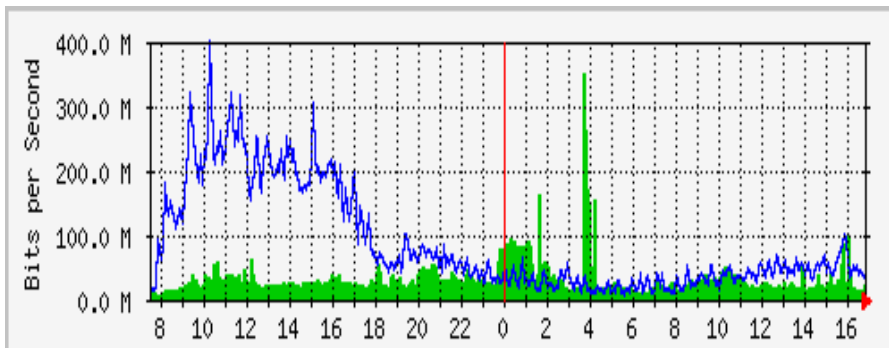
ncu_2013_10_12 (Sat.)



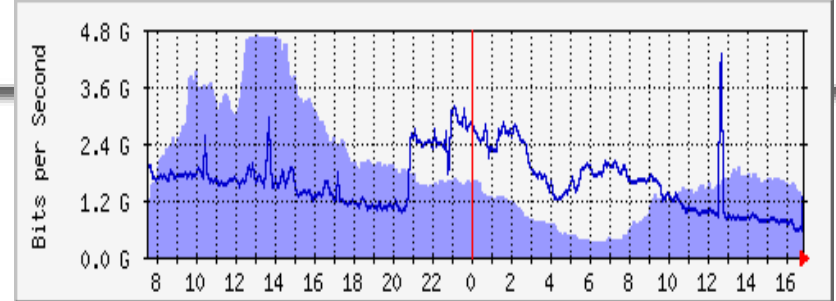
cycu_2013_10_12



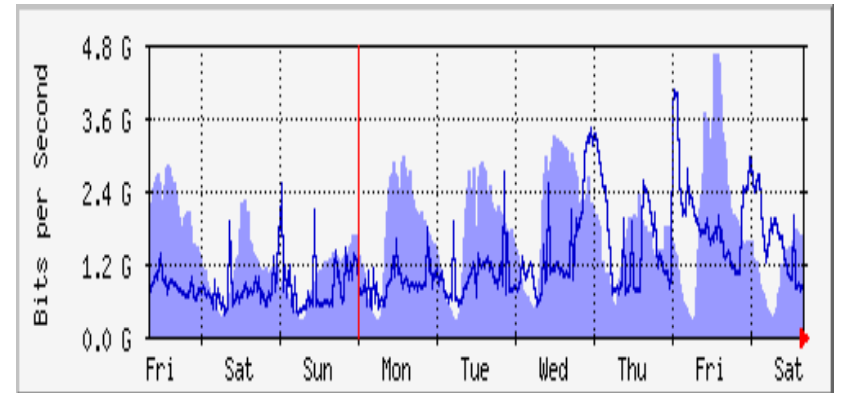
mcu_2013_10_12



Moe-internet_2013_10_12



Moe-internet_2013_10





4. Cloud-based之異常流量偵測 (cont.)

❑ Target UDP Flooding

❑ 篩選規則 (per 10-minute)

- rule_1 : bw_flooding
if (volume > 3 GB)
- rule_2 : portscan / DDoS attack
if ((pkz_out < 60 && pkz_in < 60) && (cnt_out > 80000 || cnt_in > 80000))
- rule_3 : udp_flooding
if (pkz_out >= 1000 && cnt_out > 1000000)
- rule_4 : php_vulnerable
if (pkz_out >= 1495 && cnt_out > 10000)
- rule_5 : packet_flooding
if (pkt_out >= 20000000) // 20M packets per 10-min
- rule_6 : flow_flooding
if (flow_out >= 5000000) // 5M connections per 10-min



Target UDP Flooding (cont.)

- Anomalies Notification
 - grade labeling
 - Traffic detail
- Automatically Blocking
 - Black hole routing
 - Shell script
 - Routing attack source traffic to null0



5. 規劃工作項

□ 桃園區網服務台

<http://140.115.2.26/SvcDesk>

- 研習課程維護
- 網管意見箱*
- 相關活動公告*
- MongoDB 相關應用
 - 網管經驗分享, log 蒐集/查詢
- ZK + MongoDB 相關應用
 - 網路設備資源應用狀態監看



中央大學服務台

[Home](#)

[中心通訊表](#)

[瀏覽研討資訊](#)

[活動展示](#)

[藝文活動](#)

[新增課程](#)

[新增群組](#)

[新增通訊紀錄](#)

登出

中央大學 電算中心

[流量異常偵測](#) [區網網管平台](#) [區網連線檢查](#) [網管好幫手](#) [TopN 流量排行](#) [TopN 連結量排行](#) [FDNS 連結量排行](#)

電算中心通訊表

Name	Phone	Email	Departments
戴元任*	57504	center24@cc.ncu.edu.tw	網路系統組
吳素芬	57502	center12@cc.ncu.edu.tw	網路系統組
張慈敏	57509	center23@cc.ncu.edu.tw	網路系統組
包元輝	57538	center21@cc.ncu.edu.tw	網路系統組
張維巖	57539	center9@cc.ncu.edu.tw	網路系統組
莊宜諺	57543	center31@cc.ncu.edu.tw	網路系統組
吳鏐美	57522	center18@cc.ncu.edu.tw	網路系統組
陳慶彥*	57530	center22@cc.ncu.edu.tw	校務資訊組
王文秀	57513	center13@cc.ncu.edu.tw	校務資訊組
許時準	57507	center20@cc.ncu.edu.tw	校務資訊組
蔡嘉安	57540	center40@cc.ncu.edu.tw	校務資訊組
李浩帆	57519	center19@cc.ncu.edu.tw	校務資訊組
楊豐瑜	57533	center37@cc.ncu.edu.tw	校務資訊組
張仕昌	57517	center51@cc.ncu.edu.tw	校務資訊組
劉秋美*	57512	center6@cc.ncu.edu.tw	技術研發組
劉劍青	57503	center5@cc.ncu.edu.tw	技術研發組
劉道光	57508	center2@cc.ncu.edu.tw	技術研發組
謝棋安	57526	center17@cc.ncu.edu.tw	技術研發組
李宛芸	57545	center45@cc.ncu.edu.tw	技術研發組
王雅慈*	57514	center11@cc.ncu.edu.tw	資源管理組



Computer Center

CH

上午 10:57
2012/10/22

http://140.115.2.26/SvcDesk/manageCourses.html

manageCourses

Google

搜尋

分享

更多設定 >>

網頁(P)

安全性(S)

工具(O)

登入

中央大學 電算中心

[流量異常偵測](#)[區網網管平台](#)[區網連線檢查](#)[網管好幫手](#)[TopN 流量排行](#)[TopN 連結量排行](#)[FDNS 連結量排行](#)

中央大學服務台

[Home](#)
[中心通訊表](#)
[瀏覽研討資訊](#)
[活動展示](#)
[藝文活動](#)
[新增課程](#)
[新增群組](#)
[新增通訊紀錄](#)
[登出](#)

新增研討課程

課程編號	主題	主講員	時間	地點	主辦單位	修改課程資訊
0cf382983a02b7d7013a02b898dd0002	網路攻防戰之木馬入侵大揭秘	呂守箴先生	2012-09-27 14:00~16:00	中央大學志希館 I-210	桃園區網中心(中央大學)	Edit Delete
0cf382983a05c7c4013a05cbdf30002	防毒軟體與防間碟軟體的應用	呂守箴先生	2012-10-04 14:00~16:00	中央大學志希館 I-210會議室	桃園區網中心(中央大學)	Edit Delete

[Add new course](#)
[Home](#)

© NCU Computer Center



Computer Center, National Central University.



Thank You!