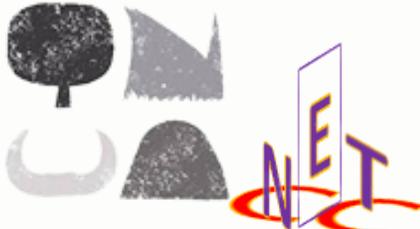




疫情期間

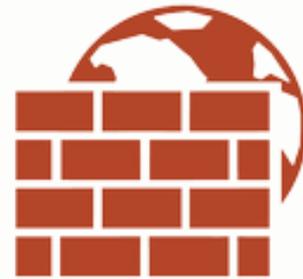
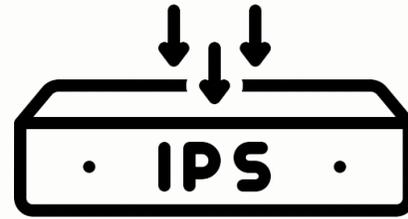
居家辦公VPN 自動化管理
&
電子郵件攻防~實例探討

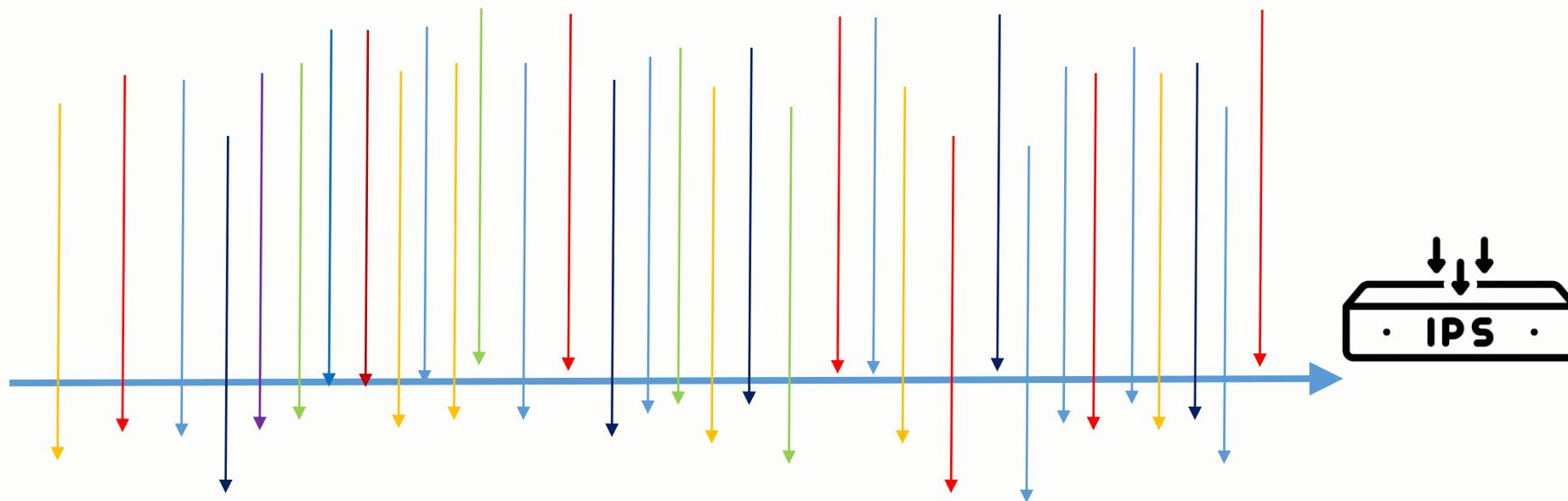
分享人:  許煒城

大綱

- 疫情期間居家辦公VPN自動化管理
 - 盤點現有設備
 - 製作教學網頁
 - 資料庫透過Except 界接Firewall
- 電子郵件攻防
 - Email黑名單、白名單收集
 - Email Reputation 檢查
 - Expect 黑名單上傳 IPS&Firewall
 - SMTP2SMS 預警
 - 電子郵件攻防實戰討論
 - SPAMMER 只有你能打我嗎?
 - 網路攻擊一直都有
 - 被動式防護
 - 結論







收集IP



教學網頁



ARP TABLE

D. 2. 0. 43	2	b0b8.67cf.af0a	ARPA
D. 2. 0. 44	4	b0b8.67cf.aee8	ARPA
D. 2. 0. 45	5	b0b8.67cf.b2c8	ARPA
D. 2. 0. 46	1	b0b8.67cf.c4a4	ARPA
D. 2. 0. 47	1	b0b8.67cf.bfc4	ARPA
D. 2. 0. 48	5	b0b8.67cf.b4f4	ARPA
D. 2. 0. 51	4	d0d3.e0ca.d276	ARPA
D. 2. 0. 78	0	14a7.8b35.d729	ARPA
D. 2. 0. 88	1	000e.e307.2a56	ARPA
D. 2. 0. 89	0	000e.e307.2a57	ARPA
D. 2. 0. 92	0	000e.e307.2a5d	ARPA
D. 2. 0. 95	0	000e.e307.2a5b	ARPA
D. 2. 0. 96	0	0012.4157.5eb6	ARPA
D. 2. 0. 98	12	0013.4803.4d72	ARPA
D. 2. 0. 120	12	0013.4801.f906	ARPA
D. 2. 0. 121	12	0013.4801.f9f2	ARPA
D. 2. 0. 122	12	0013.4801.f95a	ARPA
D. 2. 0. 123	12	0013.4801.f9d8	ARPA
D. 2. 0. 124	12	0013.4801.f969	ARPA
D. 2. 0. 125	12	0013.4801.f9da	ARPA
D. 2. 0. 126	12	0013.4800.61ed	ARPA
D. 2. 0. 127	12	0013.4801.f9e8	ARPA
D. 2. 0. 130	14	b827.eb5c.6e99	ARPA
D. 2. 0. 131	14	b827.eb2f.3b0c	ARPA
D. 2. 0. 132	14	b827.ebf4.bab0	ARPA

教學網頁:

- 1.使用者便於操作
包含投影片、與影片檔
- 2.將VPN連結相關檔案整理

ARP TABLE:

將IP對應 MAC 位置以Mail 方式留存

SPAM國別

```
Canada
CapeVerde
Germany
France
HongKong
KoreaRepublicof
Peru
RussianFederation
Taiwan
Ukraine
UnitedStates
Yemen
```

SPAM IP

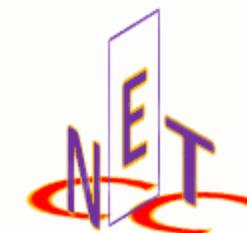
```
84.167.147.70
76.88.76.240
74.115.101.48
72.255.132.134
72.21.1.9
72.134.188.31
71.87.192.84
69.178.255.16
69.165.38.184
68.67.25.98
68.142.23.78
67.158.129.100
66.225.98.41
```

SPAM 國別:

將對應國別以 ip2c 查詢後留存

SPAM IP:

將SPAM IP 寫入資料庫以利統計



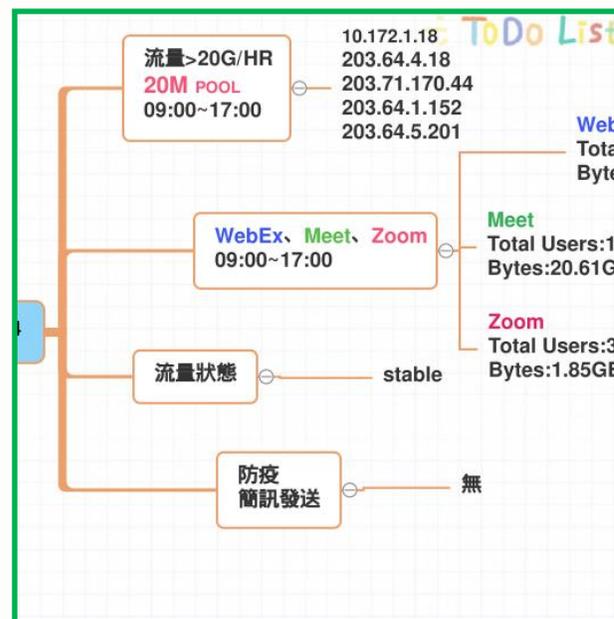
VPN 自動開關(校內)



VPN關、開

依據人事差勤系統，申請居家班公者
08:00~19:00

防疫日誌



防疫日誌

WebEx 維運
依照流量管制辦法，設定QoS 管控，以利教學

視訊流量

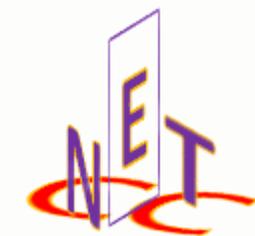


視訊流量

WebEx 維運
做為日後頻寬升級佐證



● 疫情期間居家辦公VPN自動化管理



109年總共被猜中**12**次密碼
比統一發票**開獎**頻率還高

教育平台資安通報

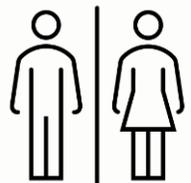
填寫矯正預防單

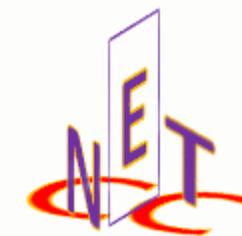
當事人變更強度的密碼

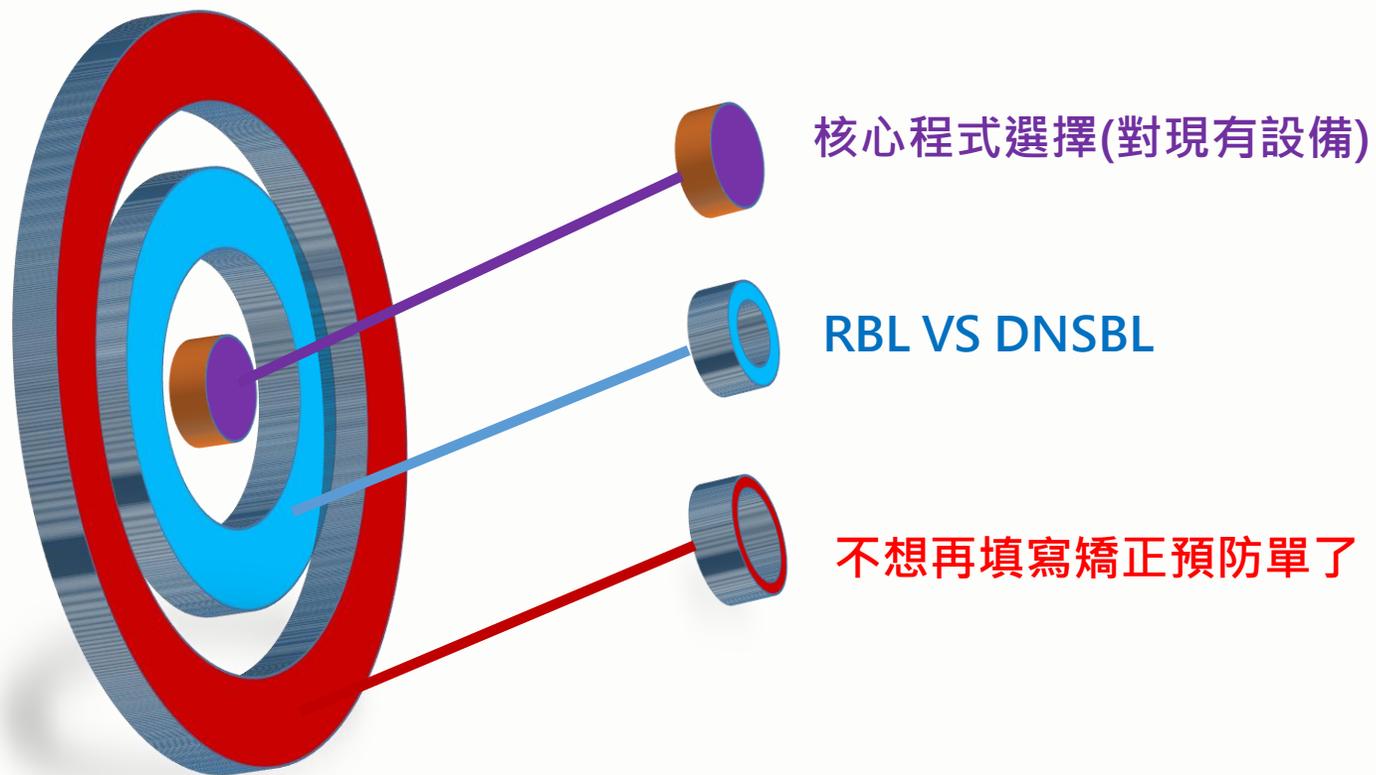
確認Reputation 狀態

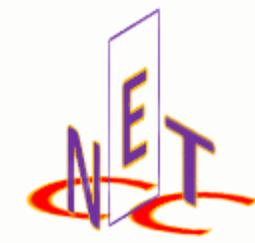
處理Reputation-IP、結案

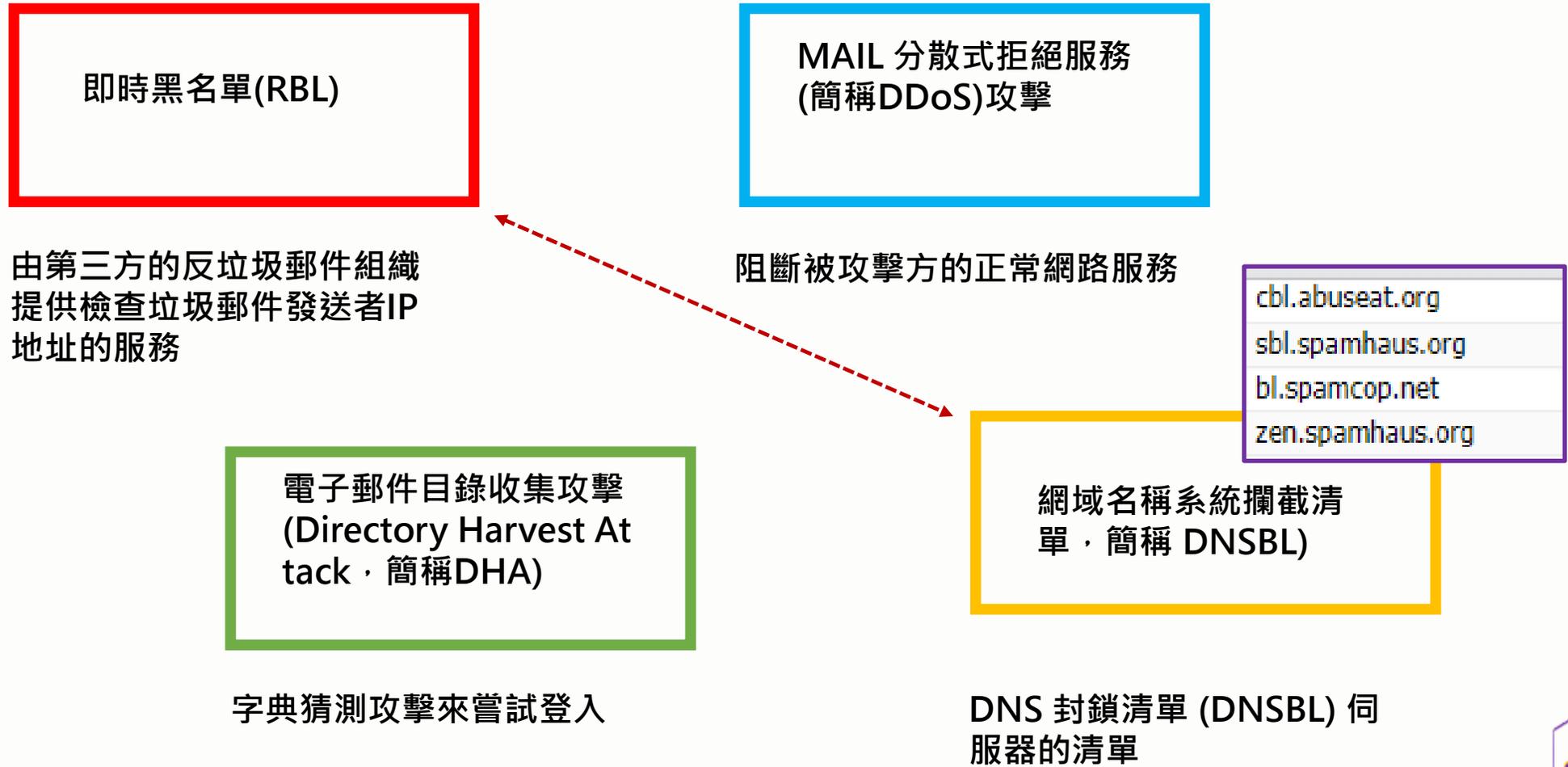


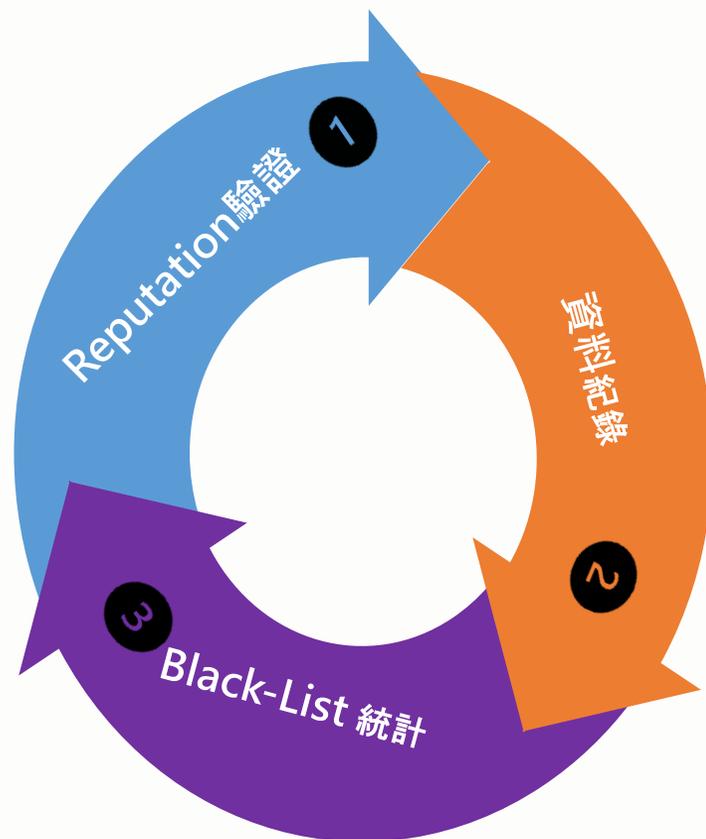












Reputation 驗證

- 1 <https://talosintelligence.com/>
- <https://maltiverse.com/>
- <https://stopforumspm.com>

資料紀錄

- 2 國別
- IP

Black-List 統計

- 3 累計、周、月...
- Expect 可以使用
- IPS Black-List 可使用



Black List IP位址 ▾ 地區 ▾

黑名單

查詢

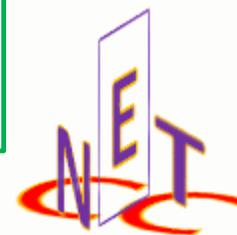
近7天內
近30天內
近60天內
近90天內

共 22254 個IP位址發生過異常活動。

下載

排名	Maltiverse	Stop Forum Spam	IP位址	發生次數
1			121.136.2.87	24
2	⊘		116.86.105.45	23
3			138.75.231.48	23
4			94.244.36.237	23
5	⊘		111.70.0.124	21
6		⊘	185.233.38.71	21
7			59.125.177.173	21
8	⊘	⊘	209.9.37.60	20
9			95.217.223.171	20
10			183.104.14.159	19
11			211.225.232.24	19
			223.171.72.234	19

10.36.3.91/BlackList/IPRanking.aspx?tvpe=twomonth



```
2022-02-23 07:35:22] -2.000,AUTH_POP3,ERR,,160.242.79.138:60265,203.71.17
2022-02-23 07:35:22] -2.000,AUTH_SERVER,ERR,,160.242.79.138:60265,203.71.
2022-02-23 07:35:57] -2.000,AUTH_POP3,ERR,,160.242.73.97:51548,203.71.172
2022-02-23 07:35:57] -2.000,AUTH_SERVER,ERR,,160.242.73.97:51548,203.71.1
2022-02-23 07:43:00] -2.000,AUTH_POP3,ERR,,208.168.230.99:59325,203.71.17
2022-02-23 07:43:00] -2.000,AUTH_SERVER,ERR,,208.168.230.99:59325,203.71.
2022-02-23 07:43:19] -2.000,AUTH
2022-02-23 07:43:19] -2.000,AUTH Content:0,EDM:-25,RT:0,SF:100,FILE:0,RULE:EDM_GE969F\r\n\t26,ACTION:release,TS:57\r\nX-CID-META: VersionHa
ed32786,C\r\n\tOID:17b061e05f4b,Recheck:0,SF:60|28|16|19|48,TC:1,Content:1,EDM:1,IP:nil,U\r\n\tRL:1,File:ni
2022-02-23 07:44:03] -2.000,AUTH 2022-05-18 23:53:57,OUTBOUND|1652889236,ahtbrkmgasrgbtgtgusikgg==_1101599026848_a/bqeehpeeoltnsuupqfdg==@ir
ertFlyers|info@floridaconcertflyers.com|info@floridaconcertflyers.com,wendypiano@gmail.com|,1175949882:5a40
2022-02-23 07:50:18] -2.000,AUTH 11101,0:N/A,Orchestra Miami's Season Finale ~An Evening with Wendy Pedersen
2022-02-23 07:50:18] -2.000,AUTH {}
2022-02-23 07:50:20] -2.000,AUTH 2022-05-18 23:54:41,INBOUND|1652889277,admin@m1.etc-meisai.jp(128.1.40.232)|E T C利用照会サービス|admin@m1
18793701;3665596260b441c19e7c35048fd87c52-20220518,3188,QUARANTINE,11206,0:N/A,etcサービスご利用者様へ大切
2022-02-23 07:50:20] -2.000,AUTH {"X-ANTISPAM-HEADER":"X-CID-RULE: Spam_0895A9A4\r\nX-CID-INFO: VERSION:1.1.5,REQID:e9091f1e-46ca-4535-b1f2-
:60,Content:-20,EDM:-25,RT:0,SF:100,FILE:0,RULE:Spam_0\r\n\tS95A9A4,ACTION:quarantine,TS:137\r\nX-CID-META:
3a34-dfc5f7bb086d,C\r\n\tOID:587d6304d1b8,Recheck:0,SF:61|820|23|16|18|42|801,TC:3,Content:1,EDM:1,\r\n\tE
2022-05-18 23:54:41,INBOUND|1652889277,admin@m1.etc-meisai.jp(128.1.40.232)|E T C利用照会サービス|admin@m1
7045892:a770d5b196b54a4895984b950a982694-20220518,3181,QUARANTINE,11206,0:N/A,etcサービスご利用者様へ大切な
{"X-ANTISPAM-HEADER":"X-CID-RULE: Spam_0895A9A4\r\nX-CID-INFO: VERSION:1.1.5,REQID:e3ab19b3-670c-4e39-bd49-
:60,Content:-20,EDM:-25,RT:0,SF:100,FILE:0,RULE:Spam_0\r\n\tS95A9A4,ACTION:quarantine,TS:137\r\nX-CID-META:
3a34-dfc5f7bb086d,C\r\n\tOID:587d6304d1b8,Recheck:0,SF:61|820|23|16|18|42|801,TC:3,Content:1,EDM:1,\r\n\tE
```

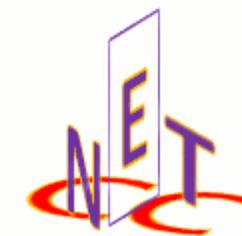
黑名單的收集

有各式各樣的MAIL LOG，
選取有效、可用與安全的紀錄檔案

99.7	100.87	128.1	101.4
99.8	101.157	128.106	101.12
99.9	101.163	133.130	111.240
2.74	104.188	134.119	111.249
2.75	105.140	134.73	111.250
3.157	105.2	136.226	111.254
4.201	108.118	136.228	111.71
5.61	108.166	137.79	111.03
5.78	109.227	138.43	112.78
5.93	109.3	138.68	114.136
6.101	109.242	139.59	114.137
7.176	109.85	140.130	114.198
7.243	109.97	141.36	114.36
7.74	110.0	141.37	114.37
7.89	110.140	141.42	114.42
9.159	110.64	146.0	114.44
9.216	111.01	150.116	1.160
11.254	111.21	157.245	1.161
10.25	111.23	159.65	116.38
10.251	112.38	160.16	1.164
11.216	116.250	162.243	116.08
11.222	118.172	163.13	116.09
11.228	120.128	166.175	1.169
11.230	120.129	167.71	117.111
11.57	120.132	167.99	118.160
11.58	120.136	173.187	118.166
16.159	123.136	175.198	118.168
16.94	123.137	178.128	1.200
19.143	123.138	178.128	121.182
12.102	123.140	178.157	122.116
11.121	123.38	178.62	123.0
11.236	123.39	180.217	123.214
11.137	123.62	180.218	125.135
			125.7

白名單的收集

收集一學期到半年
間正常登入紀錄，
有國內國外，需要
人工再次檢查
Reputation



■ Email黑名單、白名單收集

IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
59.115.249.215	59-115-249-215.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor
59.115.242.160	59-115-242-160.dynamic-ip.hinet.net	Yes	0.0	1.2	1	Poor
59.115.238.135	59-115-238-135.dynamic-ip.hinet.net	Yes	0.0	0.8	1	Poor
59.115.238.53	59-115-238-53.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor
59.115.235.244	59-115-235-244.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor
59.115.235.173	59-115-235-173.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor
59.115.235.37	59-115-235-37.dynamic-ip.hinet.net	Yes	0.0	0.8	1	Poor
59.115.234.225	59-115-234-225.dynamic-ip.hinet.net	Yes	0.0	1.7	1	Poor
59.115.233.46	59-115-233-46.dynamic-ip.hinet.net	Yes	0.0	1.7	1	Poor
59.115.232.182	59-115-232-182.dynamic-ip.hinet.net	Yes	0.0	0.8	2	Poor
59.115.232.158	59-115-232-158.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor
59.115.231.85	59-115-231-85.dynamic-ip.hinet.net	Yes	0.0	0.5	2	Poor
59.115.230.135	59-115-230-135.dynamic-ip.hinet.net	Yes	0.0	1.3	1	Poor
59.115.230.96	59-115-230-96.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor
59.115.228.40	59-115-228-40.dynamic-ip.hinet.net	Yes	0.0	1.3	1	Poor
59.115.227.198	59-115-227-198.dynamic-ip.hinet.net	Yes	0.0	0.5	1	Poor

黑、白名單的收集困難





校內常用外寄外的收集

有利於判斷與上傳防火牆，
作為放行的依據



iCloud

17.58.0.0/16

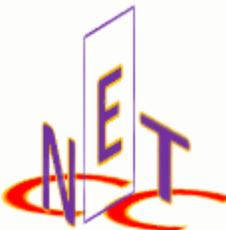


209.85.0.0/16

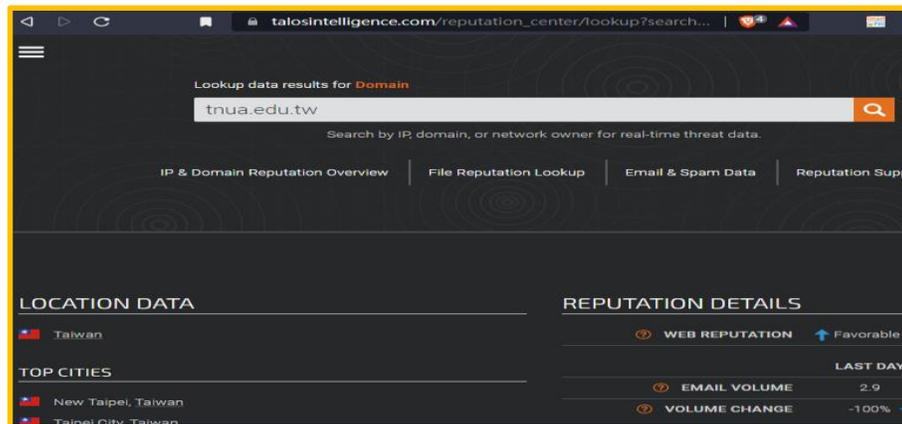
- <https://talosintelligence.com>
- <https://maltiverse.com>
- <https://www.stopforumspam.com>
- <https://mxtoolbox.com/SuperTool.aspx>
- <https://www.blocklist.de>

常用網站

查詢Reputation、
Mail 相關



■ Email Reputation 檢查



Lookup data results for Domain **tnua.edu.tw**

Search by IP, domain, or network owner for real-time threat data.

IP & Domain Reputation Overview | File Reputation Lookup | Email & Spam Data | Reputation Support

LOCATION DATA

- Taiwan

TOP CITIES

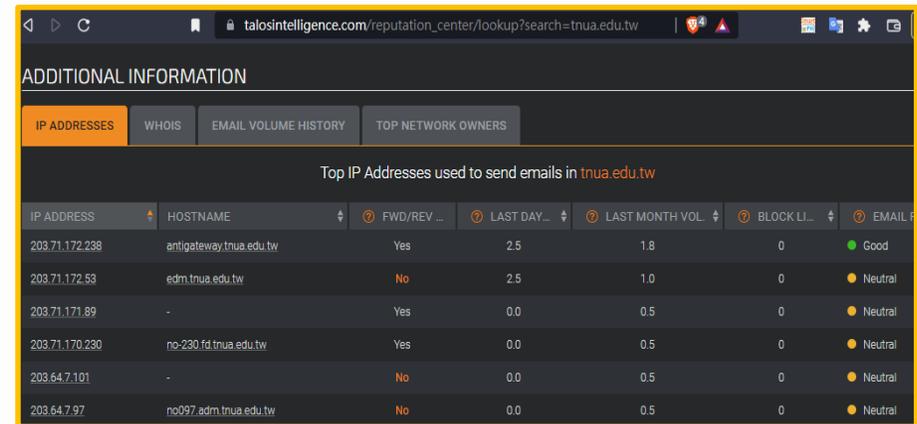
- New Taipei, Taiwan
- Taipei City, Taiwan

REPUTATION DETAILS

- WEB REPUTATION: Favorable
- EMAIL VOLUME: 2.9
- VOLUME CHANGE: -100%

sendbase.com

可以查詢MX相關資訊，
也有暴露網路資訊的疑慮



ADDITIONAL INFORMATION

IP ADDRESSES | WHOIS | EMAIL VOLUME HISTORY | TOP NETWORK OWNERS

Top IP Addresses used to send emails in tnu.edu.tw

IP ADDRESS	HOSTNAME	FWD/REV ...	LAST DAY...	LAST MONTH VOL.	BLOCK LI...	EMAIL F...
203.71.172.238	antigateway.tnu.edu.tw	Yes	2.5	1.8	0	Good
203.71.172.53	edm.tnu.edu.tw	No	2.5	1.0	0	Neutral
203.71.171.89	-	Yes	0.0	0.5	0	Neutral
203.71.170.230	no-230.fid.tnu.edu.tw	Yes	0.0	0.5	0	Neutral
203.64.7.101	-	No	0.0	0.5	0	Neutral
203.64.7.97	no097.adm.tnu.edu.tw	No	0.0	0.5	0	Neutral

Reputation

判斷 Good、
Neutral、Poor

EMAIL REPUTATION

By tracking a broad set of attributes for email, Talos Reputation Center supports very accurate conclusions about a given host. It generates a granular reputation score ranging from -10 to +10. This score is grouped into Good, Neutral and Poor reputation for simplicity reasons. [Read More.](#)



09:28...	do_not_reply@ap...	192.210.172.22	cbl.abuseat.org
08:51...	01010182c82e58c...	54.240.27.74	bl.spamcop.net
08:06...	epaper@books.co...	113.196.241.180	sbl.spamhaus.org
08:05...	bounces+446854...	167.89.42.140	bl.spamcop.net
08:03...	neg25@kcform.co...	59.25.253.56	bl.spamcop.net
08:03...	bounces+446854...	167.89.42.140	bl.spamcop.net
07:47...	crete@dive2gethe...	63.118.59.138	sbl.spamhaus.org
07:42...	gdcjms@mega.nz	103.142.212.133	bl.spamcop.net
07:29...	webmaster@hard...	202.3.164.66	sbl.spamhaus.org
07:10...	fangyin297@gmail...	42.72.15.77	sbl.spamhaus.org
07:03...	namr@mail.saison...	116.80.74.112	bl.spamcop.net
07:02...	zfracpzi@mega.nz	143.92.32.93	cbl.abuseat.org
07:02...	aldo-kemp-b8641...	134.73.202.88	sbl.spamhaus.org
07:00...	bounce_glhmlnk_...	216.24.226.98	bl.spamcop.net
23:52...	neg25@kcform.co...	59.25.253.56	bl.spamcop.net
23:52...	neg25@kcform.co...	59.25.253.56	bl.spamcop.net

Lookup data results for IP Address

63.118.59.138

Search by IP, domain, or network owner

IP & Domain Reputation Overview | File Reputation Lookup

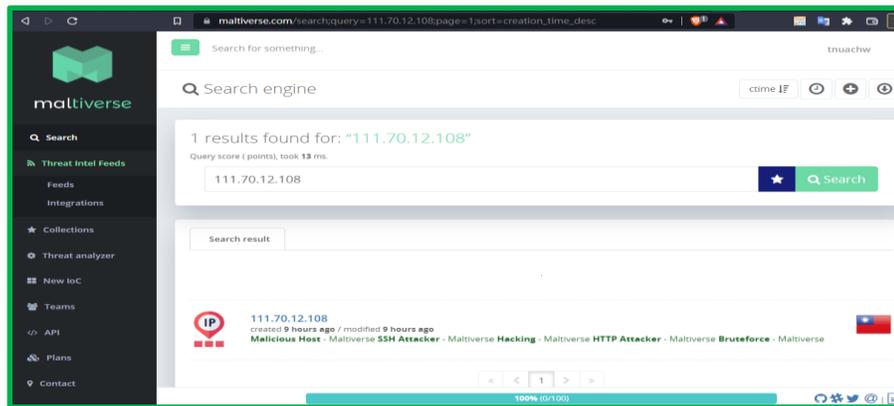
BLOCK LISTS

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	No
-------------------------	----





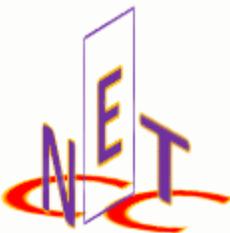
Maltiverse

可以查詢IP reputation相關訊息，
免付費僅提供100個IP



Maltiverse API

校內透過API查詢



■ Email Reputation 檢查

搜尋 : 1.215.191.210

#	時間	備註	寫入時間
1	2022.08.16	系統每日排程	2022-08-17 04:00:23

IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
1.215.191.210	-	No	0.0	1.2	2	Poor

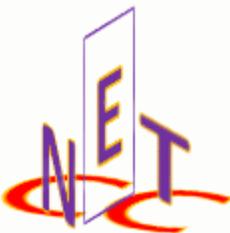
0 results found for: "1.215.191.210"

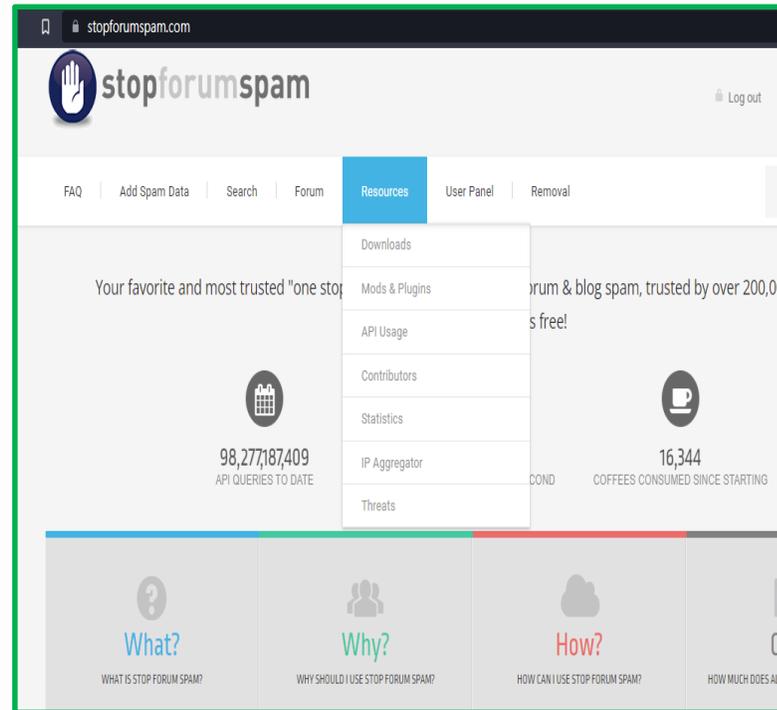
Query score (points), took 9 ms.

1.215.191.210



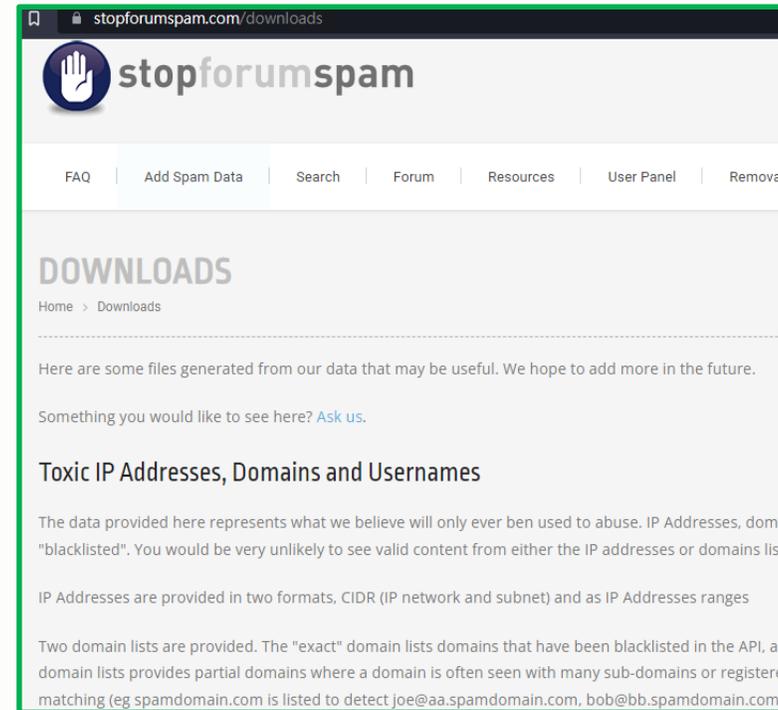
Search





Stopforumspam

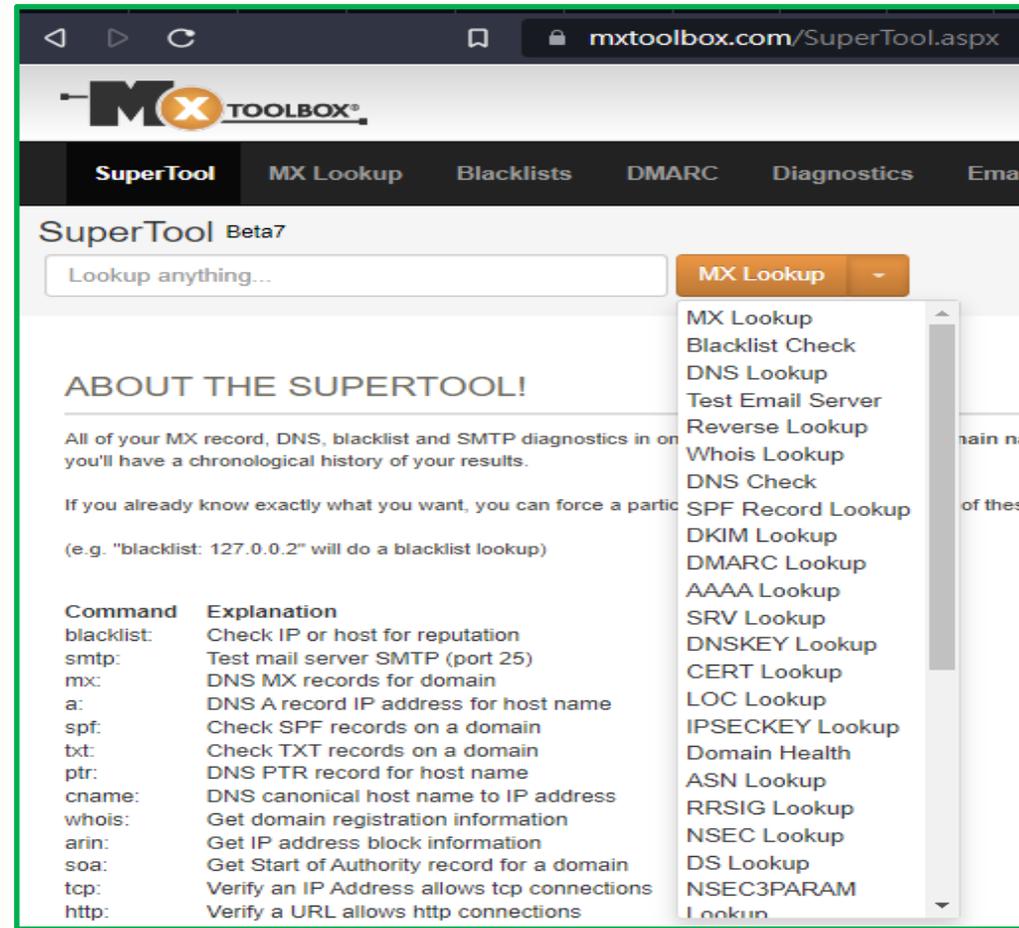
有API 查詢



stopforumspam

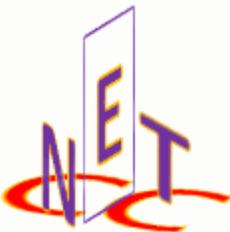
Toxic ip 下載

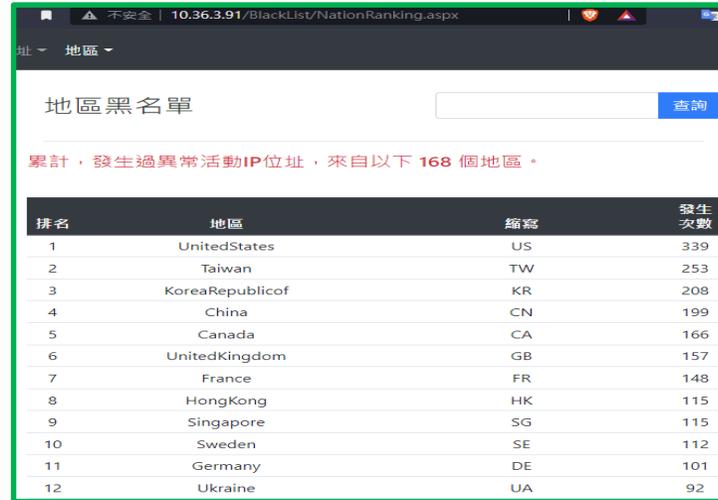




[mxtoolbox](http://mxtoolbox.com)

各式Mail Debug





地區黑名單

查詢

累計，發生過異常活動IP位址，來自以下 168 個地區。

排名	地區	縮寫	發生次數
1	UnitedStates	US	339
2	Taiwan	TW	253
3	KoreaRepublicof	KR	208
4	China	CN	199
5	Canada	CA	166
6	UnitedKingdom	GB	157
7	France	FR	148
8	HongKong	HK	115
9	Singapore	SG	115
10	Sweden	SE	112
11	Germany	DE	101
12	Ukraine	UA	92

地區的收集

有利於判斷與上傳防火牆，
作為阻擋的依據



IP黑名單

查詢

累計，共 22095 個IP位址發生過異常活動。

下載

排名	Maltiverse	Stop Forum Spam	IP位址	發生次數
1			121.136.2.87	24
2	🚫		116.86.105.45	23
3			138.75.231.48	23
4			94.244.36.237	23
5	🚫		111.70.0.124	21
6		🚫	185.233.38.71	21
7			59.125.177.173	21
8	🚫	🚫	209.9.37.60	20
9			95.217.223.171	20
10			183.104.14.159	19
11			211.225.232.24	19

黑名單的收集

有利於判斷與上傳防火牆，
作為阻擋的依據





Expect是Unix系統中用來進行自動化控制和測試的軟體工具，由Don Libes製作，作為Tcl腳本語言的一個擴展，應用在交互式軟體中如telnet，ftp，Passwd，fsck，rlogin，tip，ssh等等。該工具利用Unix偽終端包裝其子進程，允許任意程序通過終端接入進行自動化控制；也可利用Tk工具，將交互程序包裝在X11的圖形用戶界面中。

```
#!/usr/bin/expect
set home "/home/anonymous/expect-ip"
set tool "/usr/bin/expect"
set host "202.44.2.222"
set password "anonymous"
spawn telnet $host $password
expect "password:"
send "anonymous\r"
expect " * *"
send "reading mode\r"
expect " * *"
send "quit mode\r"
expect " * *"
send "reading mode address\r"
expect " * *"
set ip [lindex [lsort -b -t /etc/passwd/iptof.txt r] 0]
while {[gets $tofofd "\n"] == 0} {
    set ip [lindex [lsort -b -t /etc/passwd/iptof.txt r] 0]
    send "quit mode\r"
    expect " * *"
    send "quit mode ip $ip\r"
    send "quit mode\r"
}
close $tofofd
send "quit mode\r"
sleep 3
spawn $tool $host $password $home/0.txt
#!/usr/bin/expect
add foreignbits address-group
sleep 5
set home "/home/anonymous/expect-ip"
set tool "/usr/bin/expect"
set host "202.44.2.222"
set password "anonymous"
spawn telnet $host $password
expect "password:"
send "anonymous\r"
expect " * *"
send "reading mode\r"
expect " * *"
send "quit mode\r"
expect " * *"
send "reading mode address\r"
expect " * *"
send "quit mode ip $ip\r"
expect " * *"
set ip [lindex [lsort -b -t /etc/passwd/iptof.txt r] 0]
while {[gets $tofofd "\n"] == 0} {
    set ip [lindex [lsort -b -t /etc/passwd/iptof.txt r] 0]
    send "quit mode ip $ip\r"
    send "quit mode\r"
}
```

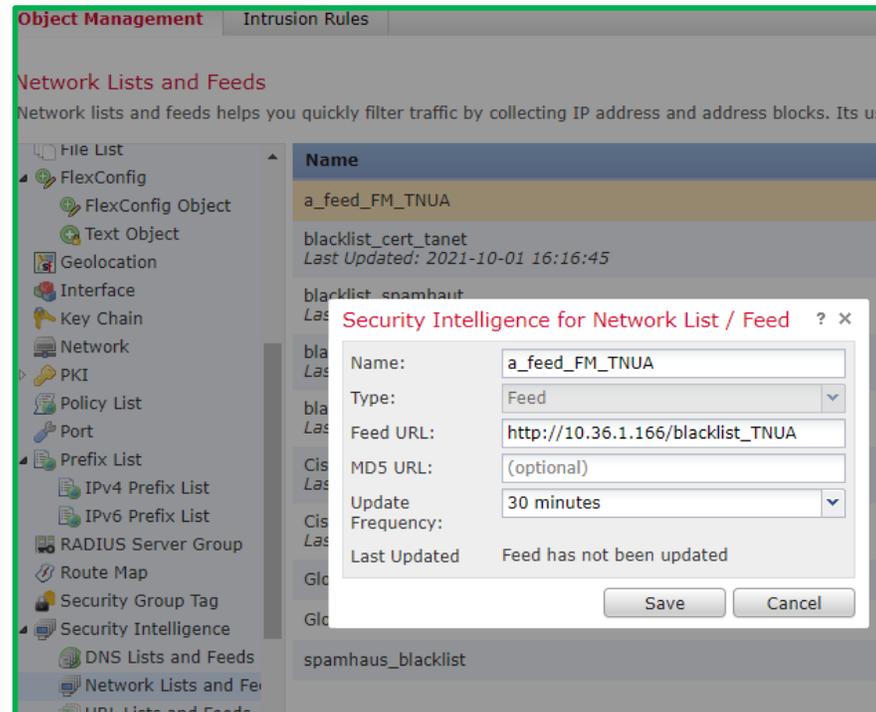


Expect 黑名單上傳 IPS&Firewall

```
59.14.152.204
59.13.81.175
59.13.37.131
59.127.36.212
59.127.213.192
59.127.18.204
59.126.50.25
59.126.45.26
59.126.214.54
59.126.171.175
59.126.139.208
59.126.129.234
59.125.98.83
59.125.78.83
59.125.74.249
59.125.247.249
59.125.210.231
59.125.2.63
59.125.177.173
59.125.122.90
59.125.120.183
59.125.101.97
59.125.101.188
59.125.101.187
59.125.101.167
59.124.81.19
59.124.71.192
59.124.227.41
[root@166 html]# wc blacklist_TNUA
19089 19089 272251 blacklist_TNUA
```

IP的收集

黑名單提供IPS，
作為阻擋的依據



IP的讀取

可以透過 FEED
URL方式



Expect 黑名單上傳 IPS&Firewall

Black List IP位址 ▾ 地區 ▾

地區黑名單 查詢

累計，發生過異常活動IP位址，來自以下 168 個地區。

排名	地區	縮寫	發生次數
1	UnitedStates	US	337
2	Taiwan	TW	252
3	KoreaRepublicof	KR	207
4	China	CN	199
5	Canada	CA	166
6	UnitedKingdom	GB	157
7	France	FR	147
8	HongKong	HK	115
9	Singapore	SG	115
10	Sweden	SE	111
11	Germany	DE	101
12	Ukraine	UA	92
13	Sudan	SD	72
14	Austria	AT	65
15	Japan	JP	63
16	Switzerland	CH	59
17	Australia	AU	57
18	Denmark	DK	55
19	RussianFederation	RU	55

P位址 ▾ 地區 ▾

IP黑名單 查詢

搜尋：99.197.236.168

#	時間	備註	寫入時間
1	2022.04.13	系統每日排程	2022-04-14 04:00:03

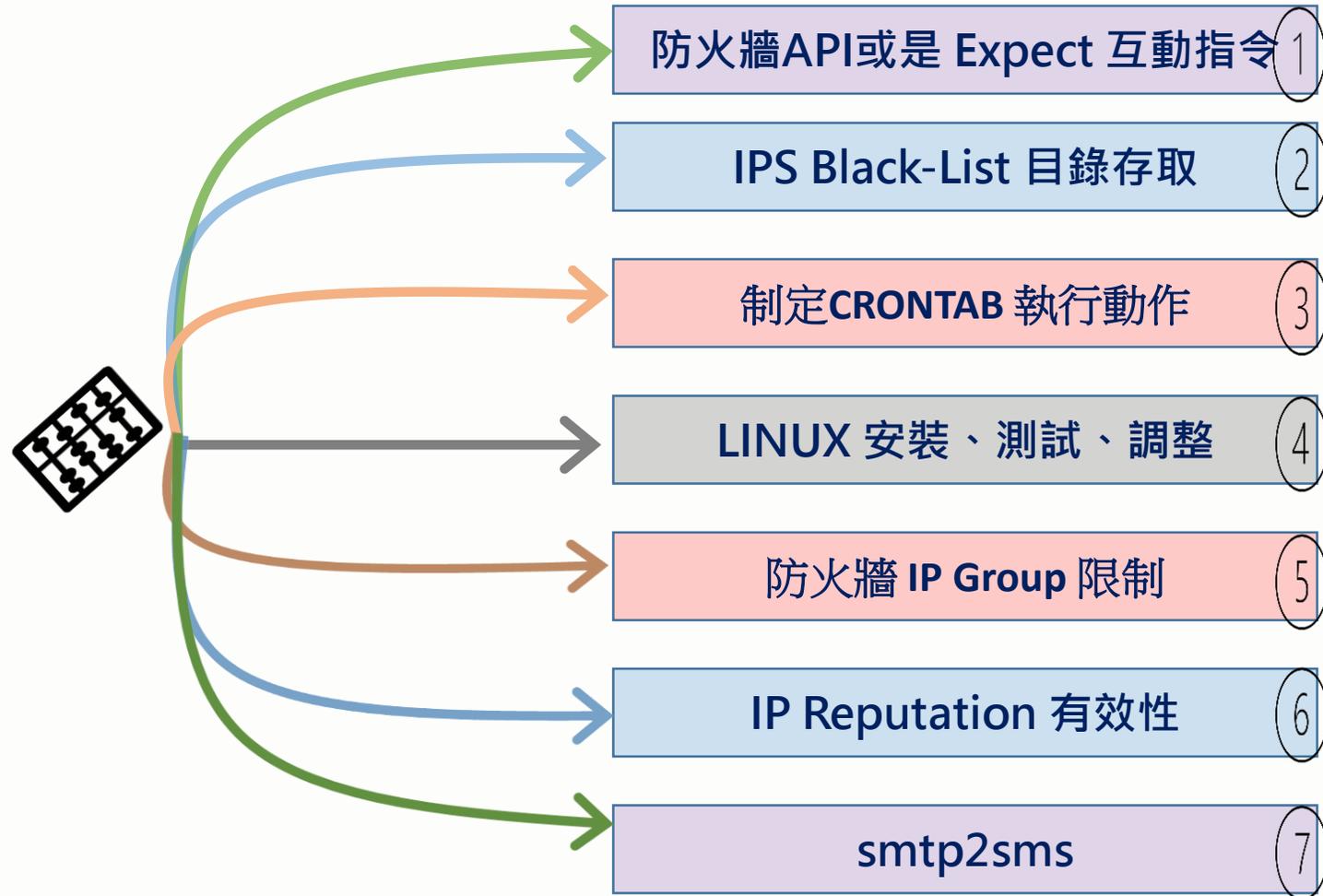
```
[root@166 data]# dig www.pku.edu.cn +short
www.lb.pku.edu.cn.
162.105.131.160
[root@166 data]# GET http://ip2c.org/162.105.131.160
1;CN;CHN;China[root@166 data]#
```

轉換

<http://ip2c.org>



■ Expect 黑名單上傳 IPS&Firewall



```
[crontest@166 data]$ more smscheck.sh
```

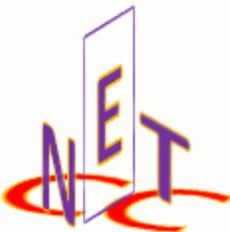
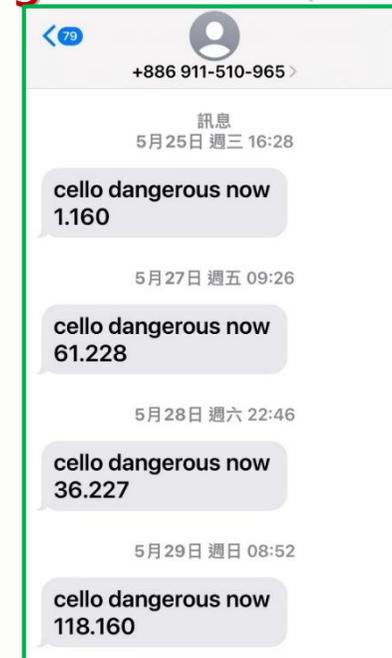
```
.  
.
```

```
while read IP  
do
```

```
    $tools/cat -v $home/mail2sms.txt | $tools/mail -s "cello dangerous now $IP"  
    mail2sms@mail.twsms.com
```

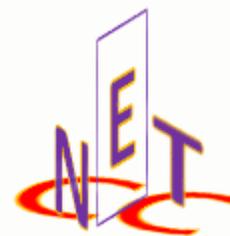
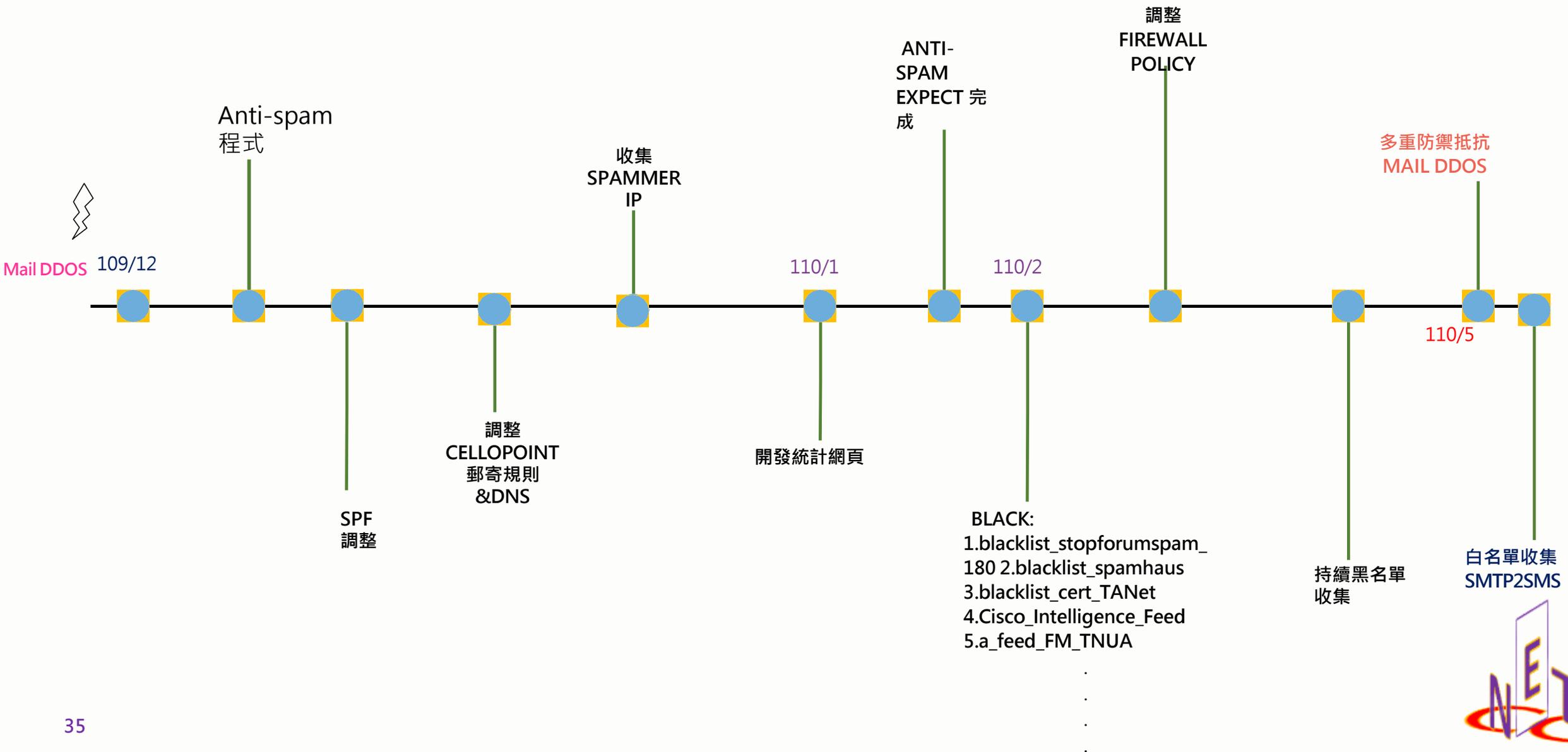
```
.  
.
```

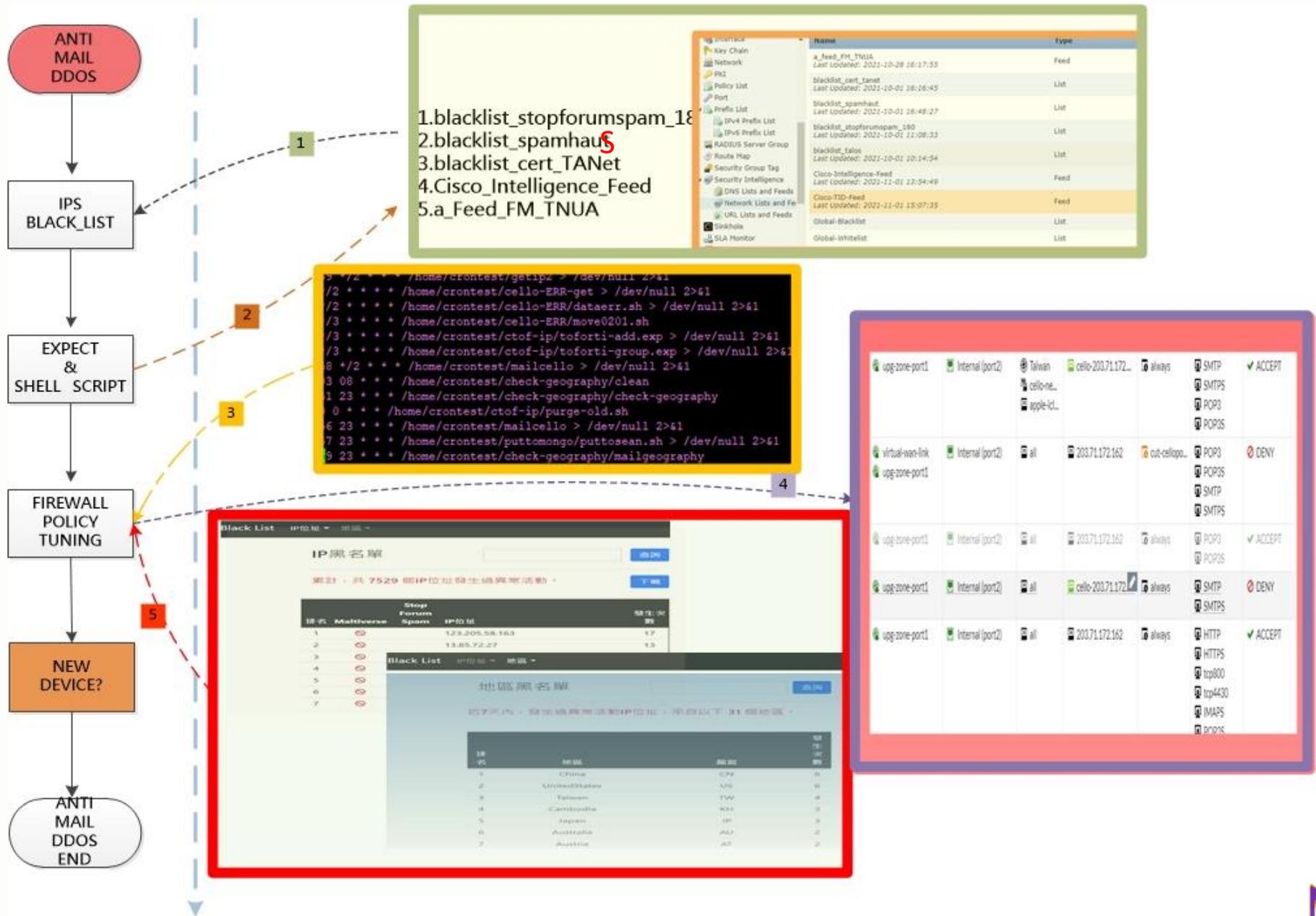
```
[crontest@166 data]$ more mail2sms.txt  
user:HELLO0000L  
pw>HelloWorld  
mobile:XXXXXXXXXX
```

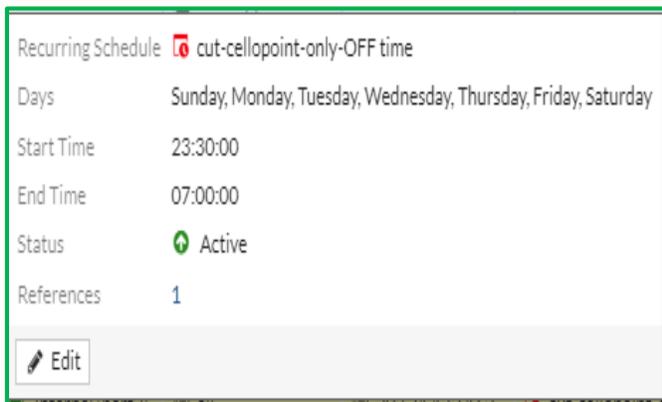


■ 電子郵件攻防實戰討論

電子郵件攻防實戰討論







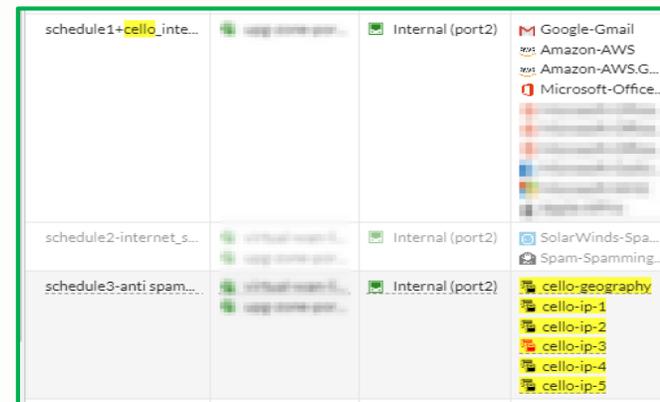
防火牆調整

每天晚上23:30~
隔天07:00



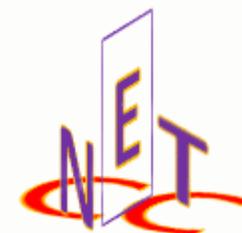
IP黑名單

會將放行設定的較為
嚴苛



防火牆調整

僅允許部分IP或網站
Relay



收集的黑名單IP(a_feed_FM_TNUA)匯入 ，可以快速阻擋於內網外

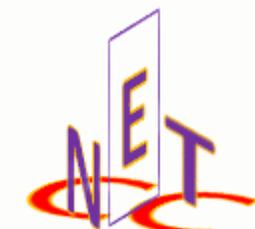
Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	IP Block	96.42.45.206	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	54704 / tcp	465 (smtps) / tcp
Block	IP Block	121.141.69.61	KOR	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	40628 / tcp	465 (smtps) / tcp
Block	IP Block	121.146.134.92	KOR	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	49622 / tcp	25 (smtp) / tcp
Block	IP Block	103.104.170.61	HKG	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	43002 / tcp	465 (smtps) / tcp
Block	IP Block	98.148.3.61	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	35963 / tcp	465 (smtps) / tcp
Block	IP Block	206.74.113.143	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	35882 / tcp	465 (smtps) / tcp
Block	IP Block	210.17.16.248	TWN	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	43953 / tcp	465 (smtps) / tcp
Block	IP Block	71.1.125.205	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	55000 / tcp	465 (smtps) / tcp
Block	IP Block	58.74.229.133	KOR	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	60550 / tcp	465 (smtps) / tcp
Block	IP Block	104.174.13.215	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	54594 / tcp	465 (smtps) / tcp
Block	IP Block	196.1.198.173	SDH	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	43006 / tcp	465 (smtps) / tcp
Block	IP Block	59.6.251.187	KOR	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	53733 / tcp	465 (smtps) / tcp
Block	IP Block	121.147.186.173	KOR	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	43404 / tcp	465 (smtps) / tcp
Block	IP Block	90.160.139.163	ESP	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	59792 / tcp	465 (smtps) / tcp
Block	IP Block	170.205.161.87	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	44549 / tcp	465 (smtps) / tcp
Block	IP Block	111.67.50.227	TWN	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	51121 / tcp	465 (smtps) / tcp
Block	IP Block	175.206.113.93	KOR	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	51050 / tcp	465 (smtps) / tcp
Block	IP Block	24.182.52.19	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	58246 / tcp	465 (smtps) / tcp
Block	IP Block	176.129.155.76	ERA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	58960 / tcp	465 (smtps) / tcp
Block	IP Block	195.178.184.196	SWE	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	60985 / tcp	465 (smtps) / tcp
Block	IP Block	67.244.101.31	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	52392 / tcp	465 (smtps) / tcp
Block	IP Block	41.209.87.186	SDH	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	43802 / tcp	465 (smtps) / tcp
Block	IP Block	209.85.222.51	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	39653 / tcp	25 (smtp) / tcp
Block	IP Block	31.208.250.206	SWE	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	47150 / tcp	465 (smtps) / tcp
Block	IP Block	69.196.152.139	CAN	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	37075 / tcp	465 (smtps) / tcp

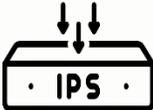
透過FEED URL

a_feed_FM_TNUA
較為快速阻擋在IPS

SMTP

阻擋SMTP、SMTPS



收集的黑名單IP(a_feed_FM_TNUA)匯入 ，亦可阻擋部分攻擊

Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	IP Block	66.68.83.241	USA	203.71.174.9	TWN	a_feed_FM_TNUA	External	Internal	7753 / tcp	22 (ssh) / tcp
Block	IP Block	221.146.237.156	KOR	203.71.174.218	TWN	a_feed_FM_TNUA	External	Internal	19473 / tcp	23 (telnet) / tcp
Block	IP Block	213.21.123.171	SWE	203.71.173.101	TWN	a_feed_FM_TNUA	External	Internal	39523 / tcp	23 (telnet) / tcp
Block	IP Block	95.108.30.198	POL	203.64.7.43	TWN	a_feed_FM_TNUA	External	Internal	22482 / tcp	22 (ssh) / tcp
Block	IP Block	64.127.146.51	USA	192.192.16.46	TWN	a_feed_FM_TNUA	External	Internal	44115 / tcp	23 (telnet) / tcp
Block	IP Block	213.21.123.171	SWE	203.64.0.22	TWN	a_feed_FM_TNUA	External	Internal	47052 / tcp	22 (ssh) / tcp
Block	IP Block	198.105.80.94	USA	192.192.97.189	TWN	a_feed_FM_TNUA	External	Internal	1311 / tcp	22 (ssh) / tcp
Block	IP Block	66.68.83.241	USA	203.71.173.140	TWN	a_feed_FM_TNUA	External	Internal	7753 / tcp	22 (ssh) / tcp
Block	IP Block	218.146.49.72	KOR	192.192.11.60	TWN	a_feed_FM_TNUA	External	Internal	34399 / tcp	23 (telnet) / tcp
Block	IP Block	1.253.174.206	KOR	192.192.16.89	TWN	a_feed_FM_TNUA	External	Internal	8882 / tcp	22 (ssh) / tcp
Block	IP Block	87.96.182.178	SWE	203.64.3.5	TWN	a_feed_FM_TNUA	External	Internal	24166 / tcp	22 (ssh) / tcp
Block	IP Block	209.85.214.169	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	37645 / tcp	25 (smtp) / tcp
Block	IP Block	47.24.76.147	USA	192.192.10.172	TWN	a_feed_FM_TNUA	External	Internal	49856 / tcp	22 (ssh) / tcp
Block	IP Block	87.96.182.178	SWE	203.64.3.25	TWN	a_feed_FM_TNUA	External	Internal	24166 / tcp	22 (ssh) / tcp
Block	IP Block	213.21.123.171	SWE	203.64.0.190	TWN	a_feed_FM_TNUA	External	Internal	47052 / tcp	22 (ssh) / tcp
Block	IP Block	65.115.13.41	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	4759 / tcp	465 (smtps) / tcp
Block	IP Block	125.227.144.49	TWN	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	36431 / tcp	465 (smtps) / tcp
Block	IP Block	198.105.80.94	USA	203.64.4.61	TWN	a_feed_FM_TNUA	External	Internal	1311 / tcp	22 (ssh) / tcp
Block	IP Block	80.68.125.160	SWE	192.192.11.29	TWN	a_feed_FM_TNUA	External	Internal	45960 / tcp	22 (ssh) / tcp
Block	IP Block	47.24.76.147	USA	192.192.10.196	TWN	a_feed_FM_TNUA	External	Internal	49856 / tcp	22 (ssh) / tcp
Block	IP Block	66.68.83.241	USA	192.192.10.243	TWN	a_feed_FM_TNUA	External	Internal	7753 / tcp	22 (ssh) / tcp
Block	IP Block	69.55.18.163	USA	192.192.97.224	TWN	a_feed_FM_TNUA	External	Internal	58746 / tcp	22 (ssh) / tcp
Block	IP Block	213.21.123.171	SWE	192.192.99.72	TWN	a_feed_FM_TNUA	External	Internal	47052 / tcp	22 (ssh) / tcp
Block	IP Block	28.146.70.22	USA	203.71.173.238	TWN	a_feed_FM_TNUA	External	Internal	28726 / tcp	23 (telnet) / tcp

有效

阻擋部分
攻擊



Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	IP Block	192.241.215.188	USA	203.64.5.20	TWN	blacklist_cert_tanet	External	Internal	47211 / udo	137 (netbios-ns) / udo
Block	IP Block	192.241.215.188	USA	203.71.170.243	TWN	blacklist_cert_tanet	External	Internal	46104 / udo	137 (netbios-ns) / udo
Block	IP Block	64.62.197.105	USA	192.192.17.124	TWN	blacklist_cert_tanet	External	Internal	32926 / tcp	8443 / tcp
Block	IP Block	193.201.9.229	RUS	203.64.3.238	TWN	CnC	External	Internal	59033 / tcp	77 (netrjs) / tcp
Block	IP Block	192.241.215.188	USA	203.71.170.31	TWN	blacklist_cert_tanet	External	Internal	42253 / udo	137 (netbios-ns) / udo
Block	IP Block	193.201.9.229	RUS	203.64.3.141	TWN	CnC	External	Internal	59033 / tcp	555 (df) / tcp
Block	IP Block	64.62.197.107	USA	192.192.99.187	TWN	blacklist_cert_tanet	External	Internal	30494 / udo	10074 / udo
Block	IP Block	192.241.215.188	USA	203.64.0.33	TWN	blacklist_cert_tanet	External	Internal	45704 / udo	137 (netbios-ns) / udo
Block	IP Block	64.62.197.228	USA	203.64.4.180	TWN	blacklist_cert_tanet	External	Internal	60103 / tcp	8443 / tcp
Block	IP Block	193.201.9.229	RUS	192.192.97.135	TWN	CnC	External	Internal	48719 / tcp	2321 / tcp
Block	IP Block	65.49.20.87	USA	192.192.95.219	TWN	blacklist_cert_tanet	External	Internal	56067 / tcp	8443 / tcp
Block	IP Block	192.241.215.188	USA	203.64.5.70	TWN	blacklist_cert_tanet	External	Internal	54829 / udo	137 (netbios-ns) / udo
Block	IP Block	192.241.215.188	USA	203.64.1.94	TWN	blacklist_cert_tanet	External	Internal	56825 / udo	137 (netbios-ns) / udo
Block	IP Block	193.201.9.229	RUS	203.71.174.191	TWN	CnC	External	Internal	48719 / tcp	2305 / tcp
Block	IP Block	192.241.215.188	USA	203.64.4.23	TWN	blacklist_cert_tanet	External	Internal	56042 / udo	137 (netbios-ns) / udo
Block	IP Block	193.201.9.229	RUS	203.64.1.100	TWN	CnC	External	Internal	48719 / tcp	2260 / tcp
Block	IP Block	216.218.206.84	USA	203.64.3.247	TWN	blacklist_cert_tanet	External	Internal	38696 / udo	161 (snmp) / udo
Block	IP Block	192.241.215.188	USA	203.64.0.221	TWN	blacklist_cert_tanet	External	Internal	55325 / udo	137 (netbios-ns) / udo
Block	IP Block	216.218.206.80	USA	192.192.10.101	TWN	blacklist_cert_tanet	External	Internal	44097 / udo	161 (snmp) / udo
Block	IP Block	192.241.215.188	USA	203.71.171.174	TWN	blacklist_cert_tanet	External	Internal	35458 / udo	137 (netbios-ns) / udo
Block	IP Block	65.49.20.66	USA	203.71.171.68	TWN	blacklist_cert_tanet	External	Internal	45120 / tcp	8443 / tcp

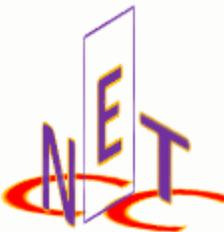
Block	IP Block	93.90.72.181	ZAF	192.192.98.109	TWN	forti-anomaly-0811	External	Internal	58556 / tcp	1009 / tcp
Block	IP Block	45.127.98.36	CHN	203.64.6.252	TWN	forti-anomaly-0811	External	Internal	49518 / tcp	11967 / tcp
Block	IP Block	185.156.74.58	NLD	192.192.98.210	TWN	forti-ios-0812	External	Internal	45626 / tcp	12566 / tcp
Block	IP Block	211.103.227.254	CHN	192.192.97.243	TWN	forti-anomaly-0811	External	Internal	8 (Echo Request) / icmp	0 (No Code) / icmp
Block	IP Block	64.227.115.244	DEU	192.192.17.241	TWN	forti-anomaly-0811	External	Internal	40451 / tcp	2375 / tcp
Block	IP Block	211.103.227.254	CHN	192.192.97.157	TWN	forti-anomaly-0811	External	Internal	8 (Echo Request) / icmp	0 (No Code) / icmp
Block	IP Block	211.103.227.254	CHN	192.192.11.187	TWN	forti-anomaly-0811	External	Internal	8 (Echo Request) / icmp	0 (No Code) / icmp
Block	IP Block	45.81.34.70	GBR	192.192.95.250	TWN	forti-anomaly-0811	External	Internal	56795 / tcp	8998 / tcp
Block	IP Block	103.118.253.197	CHN	203.71.173.210	TWN	forti-anomaly-0811	External	Internal	37256 / udo	9100 / udo
Block	IP Block	185.156.74.58	NLD	192.192.99.95	TWN	forti-ios-0812	External	Internal	45626 / tcp	12566 / tcp
Block	IP Block	45.81.34.197	GBR	192.192.16.153	TWN	forti-anomaly-0811	External	Internal	33320 / tcp	20221 / tcp
Block	IP Block	211.103.227.254	CHN	192.192.95.250	TWN	forti-anomaly-0811	External	Internal	8 (Echo Request) / icmp	0 (No Code) / icmp
Block	IP Block	103.118.253.201	CHN	192.192.95.219	TWN	forti-anomaly-0811	External	Internal	34628 / tcp	2222 / tcp
Block	IP Block	85.192.63.5	RUS	192.192.99.200	TWN	blacklist.de-0815	External	Internal	32221 / tcp	23 (telnet) / tcp
Block	IP Block	45.127.98.52	CHN	203.64.4.144	TWN	forti-anomaly-0811	External	Internal	55916 / tcp	3171 / tcp
Block	IP Block	94.102.56.15	NLD	203.71.172.35	TWN	forti-anomaly-0811	External	Internal	42126 / tcp	65120 / tcp
Block	IP Block	45.127.98.52	CHN	203.64.6.248	TWN	forti-anomaly-0811	External	Internal	58134 / tcp	3171 / tcp
Block	IP Block	85.208.214.66	JPN	203.64.7.1	TWN	forti-anomaly-0811	External	Internal	36814 / tcp	61616 / tcp

Block	IP Block	185.196.220.70	DEU	203.71.170.156	TWN	cert_from NTU_0810	External	Internal	50936 / udo	3283 / udo
Block	IP Block	146.88.240.248	USA	203.64.7.82	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	192.192.96.52	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	192.192.20.198	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	192.192.16.69	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	192.192.99.165	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.71.170.93	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.71.171.140	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.71.172.115	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.64.6.204	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	185.196.220.70	DEU	192.192.97.94	TWN	cert_from NTU_0810	External	Internal	52704 / udo	3283 / udo
Block	IP Block	185.196.220.70	DEU	192.192.98.2	TWN	cert_from NTU_0810	External	Internal	47891 / udo	3283 / udo
Block	IP Block	146.88.240.248	USA	203.71.170.194	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.64.6.220	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.64.7.76	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.64.4.55	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	146.88.240.248	USA	203.64.6.156	TWN	cert_from NTU_0810	External	Internal	1701 / udo	1701 / udo
Block	IP Block	185.196.220.70	DEU	203.64.7.78	TWN	cert_from NTU_0810	External	Internal	55650 / udo	3283 / udo

Block	IP Block	68.183.188.159	SGP	192.192.95.36	TWN	blacklist.de-0815	External	Internal	42442 / tcp	509
Block	IP Block	142.93.112.39	USA	192.192.95.199	TWN	blacklist.de-0815	External	Internal	45781 / tcp	372
Block	IP Block	206.189.198.55	USA	203.64.3.220	TWN	blacklist.de-0815	External	Internal	49673 / tcp	141
Block	IP Block	183.107.205.177	KOR	203.71.173.68	TWN	blacklist.de-0815	External	Internal	50300 / tcp	22
Block	IP Block	177.184.133.130	BRA	192.192.17.188	TWN	blacklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	164.90.194.36	NLD	203.64.0.43	TWN	blacklist.de-0815	External	Internal	54681 / tcp	323
Block	IP Block	177.184.133.130	BRA	192.192.17.82	TWN	blacklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	177.184.133.130	BRA	192.192.16.244	TWN	blacklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	45.61.188.170	USA	203.64.2.221	TWN	blacklist.de-0815	External	Internal	38815 / tcp	22
Block	IP Block	134.209.150.200	IND	203.64.0.203	TWN	blacklist.de-0815	External	Internal	47201 / tcp	258
Block	IP Block	45.61.188.170	USA	192.192.95.210	TWN	blacklist.de-0815	External	Internal	41614 / tcp	22
Block	IP Block	163.123.143.78	USA	203.64.1.90	TWN	blacklist.de-0815	External	Internal	44586 / tcp	111
Block	IP Block	42.201.63.247	CHN	192.192.10.199	TWN	blacklist.de-0815	External	Internal	55930 / tcp	22
Block	IP Block	141.98.11.92	LTU	203.71.170.218	TWN	blacklist.de-0815	External	Internal	45585 / tcp	80
Block	IP Block	177.184.133.130	BRA	203.64.6.153	TWN	blacklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	163.123.143.78	USA	192.192.20.111	TWN	blacklist.de-0815	External	Internal	34970 / tcp	111
Block	IP Block	163.123.143.78	USA	203.64.0.206	TWN	blacklist.de-0815	External	Internal	60005 / tcp	111
Block	IP Block	116.7.245.26	CHN	203.64.1.219	TWN	blacklist.de-0815	External	Internal	56863 / tcp	22
Block	IP Block	159.89.205.91	SGP	192.192.17.34	TWN	blacklist.de-0815	External	Internal	47884 / tcp	527
Block	IP Block	141.98.11.92	LTU	203.64.3.79	TWN	blacklist.de-0815	External	Internal	47606 / tcp	80

透過FEED

收集各式的blacklist



寄件者: "行政院國家資通安全會報技術服務中心"
<contactus@nccst.nat.gov.tw>
收件者: "chw" <chw@tnua.edu.tw>
寄件備份: 2021 10 月 1 星期五 下午 1:37:04
主旨: 回覆：主旨：請問如何申請 ip reputation 下載

感謝您的來信，有關「申請ip reputation下載」，說明如下：

1.本中心目前未針對Spammer DDoS攻擊提供IP黑名單資訊。
2.若貴單位有黑名單相關需求，可參考TACERT教育機構資安通報平台與教育學術資訊分享與分析中心(A-ISAC)威脅清單資訊，取得方式請參考以下網址：

(1)教育機構資安通報平台

(<https://info.cert.tanet.edu.tw/prog/index.php>)。

(2)威脅清單資訊取得資訊說明頁面

(<https://cert.tanet.edu.tw/pdf/threatdoc.pdf>)。

3.另提供國外資安組織提供之SPAM阻擋黑名單資訊，取得方式請參考網址(<https://www.spamhaus.org/drop/drop.txt>)。

4.若有其他問題，歡迎您透過服務信箱

(<https://www.nccst.nat.gov.tw/MailToCenter?lang=zh>)再次來信與本中心聯繫，謝謝。

技服回應快速

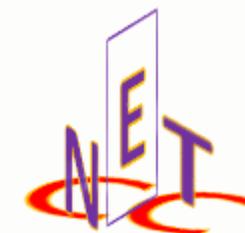
有求必應

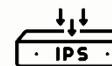


IP Block	🚫 192.241.220.4	USA	192.192.16.231	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.10.58	TWN	blacklist cert tanet	
IP Block	🚫 64.62.197.9	USA	203.64.4.162	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.95.186	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.96.214	TWN	blacklist cert tanet	
IP Block	🚫 64.62.197.239	USA	192.192.20.209	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.10.118	TWN	blacklist cert tanet	
IP Block	🚫 74.82.47.61	USA	203.71.174.222	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.11.250	TWN	blacklist cert tanet	
IP Block	🚫 64.62.197.9	USA	192.192.98.74	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.96.124	TWN	blacklist cert tanet	
IP Block	🚫 113.140.39.178	CHN	203.71.171.34	TWN	blacklist stopforumspam 180	
IP Block	🚫 192.241.220.4	USA	192.192.99.175	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.11.175	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.98.255	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.16.200	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.17.116	TWN	blacklist cert tanet	
IP Block	🚫 64.62.197.239	USA	203.71.173.49	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.95.114	TWN	blacklist cert tanet	
IP Block	🚫 64.62.197.106	USA	203.71.174.91	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.17.32	TWN	blacklist cert tanet	
IP Block	🚫 192.241.220.4	USA	192.192.98.240	TWN	blacklist cert tanet	

FEED LIST

可以在IPS阻擋





38 seconds ago	██████	120.77.40.56	6
38 seconds ago	██████	120.77.40.56	6
4 minutes ago	██████	52.91.230.28	1
5 minutes ago	██████	3.82.122.207	1
7 minutes ago	██████	3.94.173.19	1
7 minutes ago	██████	43.138.54.100	6
12 minutes ago	██████	45.164.20.107	17
12 minutes ago	██████	45.164.20.107	17
22 minutes ago	██████	20.163.80.27	6
23 minutes ago	██████	20.163.80.27	6
26 minutes ago	██████	43.226.152.7	6
26 minutes ago	██████	43.226.152.7	6
27 minutes ago	██████	103.78.35.229	6
27 minutes ago	██████	45.164.20.107	17
27 minutes ago	██████	103.78.35.2	6
27 minutes ago	██████	103.78.35.229	6
32 minutes ago	██████	85.17.90.246	6
38 minutes ago	██████	103.109.3.229	6
39 minutes ago	██████	20.163.80.27	6
40 minutes ago	██████	210.57.214.46	6
40 minutes ago	██████	185.40.4.199	6

Context Explorer Connections Security Intelligence Events Intrusions Files Hosts Users Correlation Advanced Search

Security Intelligence Events [\(switch workflow\)](#)

Security Intelligence with Application Details > Table View of Security Intelligence Events

No Search Constraints [\(Edit Search\)](#)

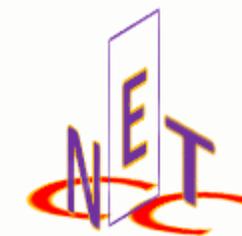
Jump to...

<input type="checkbox"/>	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category
↓	2022-08-11 15:29:50		Block	IP Block	198.199.92.190	USA	203.71.170.72	TWN	blacklist_storforums0am_0810
↓	2022-08-11 15:29:50		Block	IP Block	198.199.92.190	USA	203.64.0.182	TWN	blacklist_storforums0am_0810
↓	2022-08-11 15:29:50		Block	IP Block	45.143.200.102	BGR	192.192.10.54	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	185.156.73.67	RUS	192.192.11.208	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	185.156.73.67	RUS	192.192.95.41	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	103.118.253.195	CHN	203.64.1.56	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	192.241.236.109	USA	192.192.11.56	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	185.156.73.100	RUS	192.192.16.61	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	150.129.81.243	HKG	192.192.17.31	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	103.118.253.243	CHN	203.64.5.78	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	81.240.118.75	HKG	203.64.5.240	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	103.118.253.201	CHN	192.192.98.51	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	45.143.203.15	RUS	192.192.11.5	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	103.118.253.196	CHN	203.71.174.214	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	185.156.73.100	RUS	192.192.11.119	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	150.129.81.243	HKG	203.71.173.96	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	45.81.24.68	GBR	192.192.99.172	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	45.127.98.37	CHN	203.64.2.49	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	45.127.98.23	CHN	203.64.3.113	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	185.156.73.100	RUS	203.71.174.110	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	45.127.98.39	CHN	203.71.174.240	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	45.127.98.36	CHN	192.192.97.67	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	167.71.237.196	IND	203.71.172.109	TWN	blacklist_storforums0am_0810
↓	2022-08-11 15:29:50		Block	IP Block	47.96.178.225	CHN	203.64.7.10	TWN	forti-anomaly-0811
↓	2022-08-11 15:29:50		Block	IP Block	185.156.73.63	RUS	203.64.5.99	TWN	forti-anomaly-0811

Page 1 of 59795 | Displaying rows 1-25 of 1494864 rows

FEED LIST

從防火牆擷取IP，
餵給IPS



Block	IP Block	92.63.197.100	RUS	192.192.16.184	TWN	forti-anomaly-0811
Block	IP Block	185.156.73.57	RUS	192.192.16.161	TWN	forti-anomaly-0811
Block	IP Block	185.156.73.100	RUS	203.64.5.83	TWN	forti-anomaly-0811
Block	IP Block	92.63.197.100	RUS	192.192.16.83	TWN	forti-anomaly-0811
Block	IP Block	92.63.197.100	RUS	203.64.1.94	TWN	forti-anomaly-0811
Block	IP Block	92.63.197.100	RUS	203.64.1.244	TWN	forti-anomaly-0811
Block	IP Block	185.156.73.100	RUS	203.64.3.192	TWN	forti-anomaly-0811

ws 1-25 of 143621 rows

Block	IP Block	45.127.98.57	CHN	203.71.171.105	TWN	forti-anomaly-0811
Block	IP Block	211.103.227.254	CHN	192.192.16.167	TWN	forti-anomaly-0811
Block	IP Block	219.141.207.253	CHN	192.192.16.165	TWN	forti-anomaly-0811
Block	IP Block	219.141.207.253	CHN	192.192.16.175	TWN	forti-anomaly-0811
Block	IP Block	211.103.227.254	CHN	192.192.17.25	TWN	forti-anomaly-0811
Block	IP Block	211.103.227.254	CHN	192.192.17.135	TWN	forti-anomaly-0811
Block	IP Block	211.103.227.254	CHN	192.192.16.108	TWN	forti-anomaly-0811
Block	IP Block	211.103.227.254	CHN	192.192.17.141	TWN	forti-anomaly-0811

ws 1-25 of 256127 rows

Block	IP Block	45.81.34.68	GBR	192.192.98.49	TWN	forti-anomaly-0811
Block	IP Block	45.81.34.68	GBR	192.192.16.242	TWN	forti-anomaly-0811
Block	IP Block	45.81.34.70	GBR	192.192.99.160	TWN	forti-anomaly-0811
Block	IP Block	45.81.34.68	GBR	192.192.17.193	TWN	forti-anomaly-0811
Block	IP Block	45.81.34.67	GBR	203.71.171.123	TWN	forti-anomaly-0811
Block	IP Block	45.81.34.68	GBR	192.192.98.132	TWN	forti-anomaly-0811
Block	IP Block	45.81.34.67	GBR	203.64.4.17	TWN	forti-anomaly-0811

ws 1-25 of 75569 rows

Block	IP Block	94.102.56.15	NLD	203.71.172.36	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.117	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.181	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.252	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.204	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.64	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.215	TWN	forti-anomaly-0811
Block	IP Block	94.102.56.15	NLD	203.71.172.123	TWN	forti-anomaly-0811

ws 1-25 of 122503 rows

Block	IP Block	93.90.72.215	ZAF	192.192.17.114	TWN	forti-anomaly-0811
Block	IP Block	93.90.72.181	ZAF	203.71.171.168	TWN	forti-anomaly-0811
Block	IP Block	93.90.72.164	ZAF	203.71.174.198	TWN	forti-anomaly-0811
Block	IP Block	93.90.72.168	ZAF	203.71.170.109	TWN	forti-anomaly-0811
Block	IP Block	93.90.72.210	ZAF	203.71.174.149	TWN	forti-anomaly-0811
Block	IP Block	93.90.72.210	ZAF	203.64.1.130	TWN	forti-anomaly-0811
Block	IP Block	93.90.72.164	ZAF	203.71.171.105	TWN	forti-anomaly-0811

ws 1-25 of 46338 rows

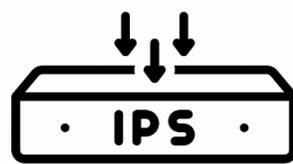
Block	IP Block	185.165.190.17	USA	192.192.11.2	TWN	forti-ips-0812
Block	IP Block	65.49.20.81	USA	192.192.95.84	TWN	blacklist cert tanet
Block	IP Block	64.62.197.58	USA	203.71.174.54	TWN	blacklist cert tanet
Block	IP Block	64.62.197.97	USA	192.192.16.177	TWN	blacklist cert tanet
Block	IP Block	64.62.197.215	USA	192.192.98.115	TWN	blacklist cert tanet
Block	IP Block	64.62.197.56	USA	192.192.95.110	TWN	blacklist cert tanet
Block	IP Block	128.14.134.134	USA	192.192.17.19	TWN	blacklist cert tanet

ws 1-25 of 108361 rows

Block	IP Block	150.129.81.228	HKG	203.64.0.184	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.5.219	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.6.138	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.5.33	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.4.180	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.213	HKG	203.71.172.92	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.226	HKG	192.192.99.77	TWN	forti-anomaly-0811

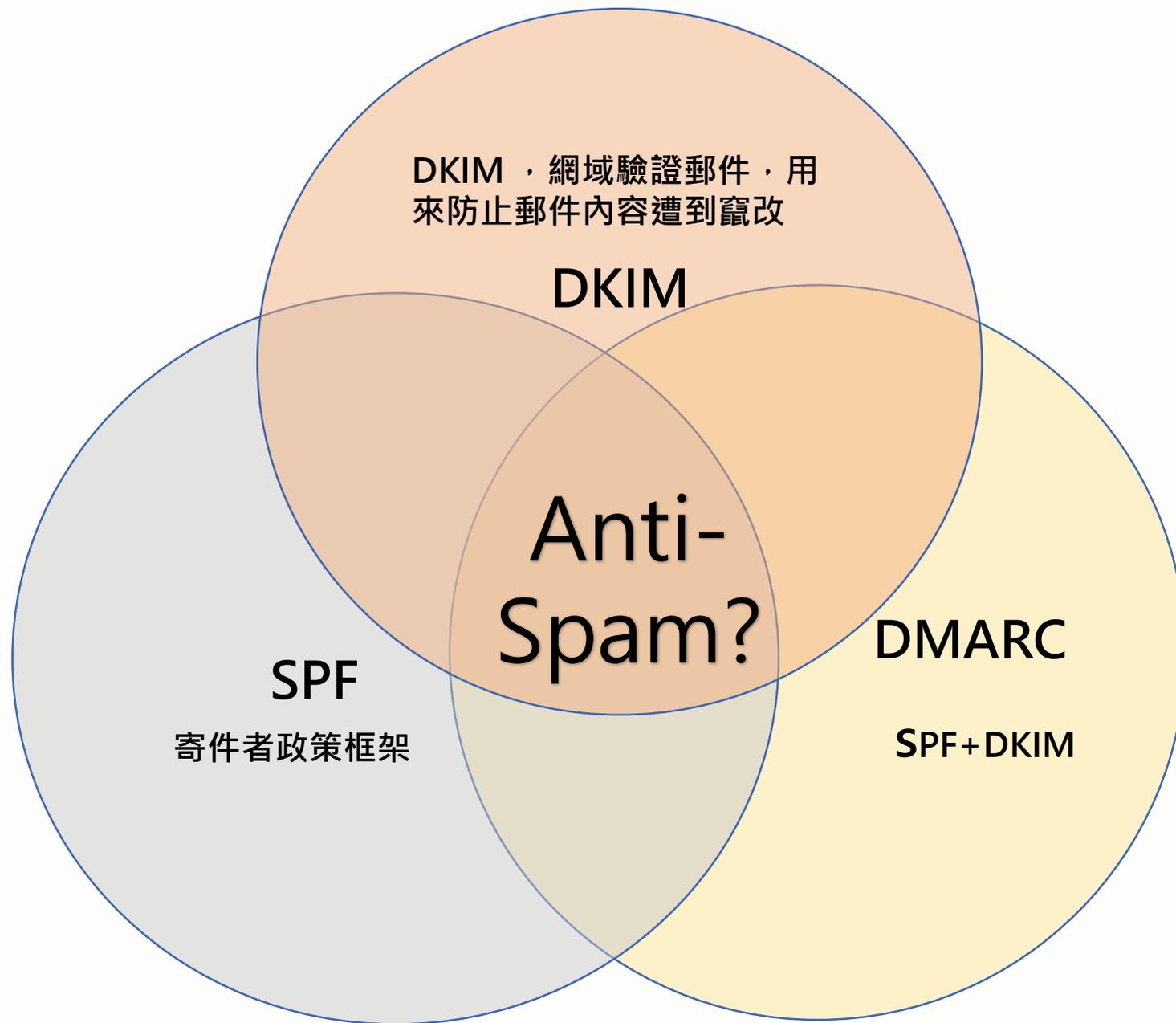
ws 1-25 of 105737 rows

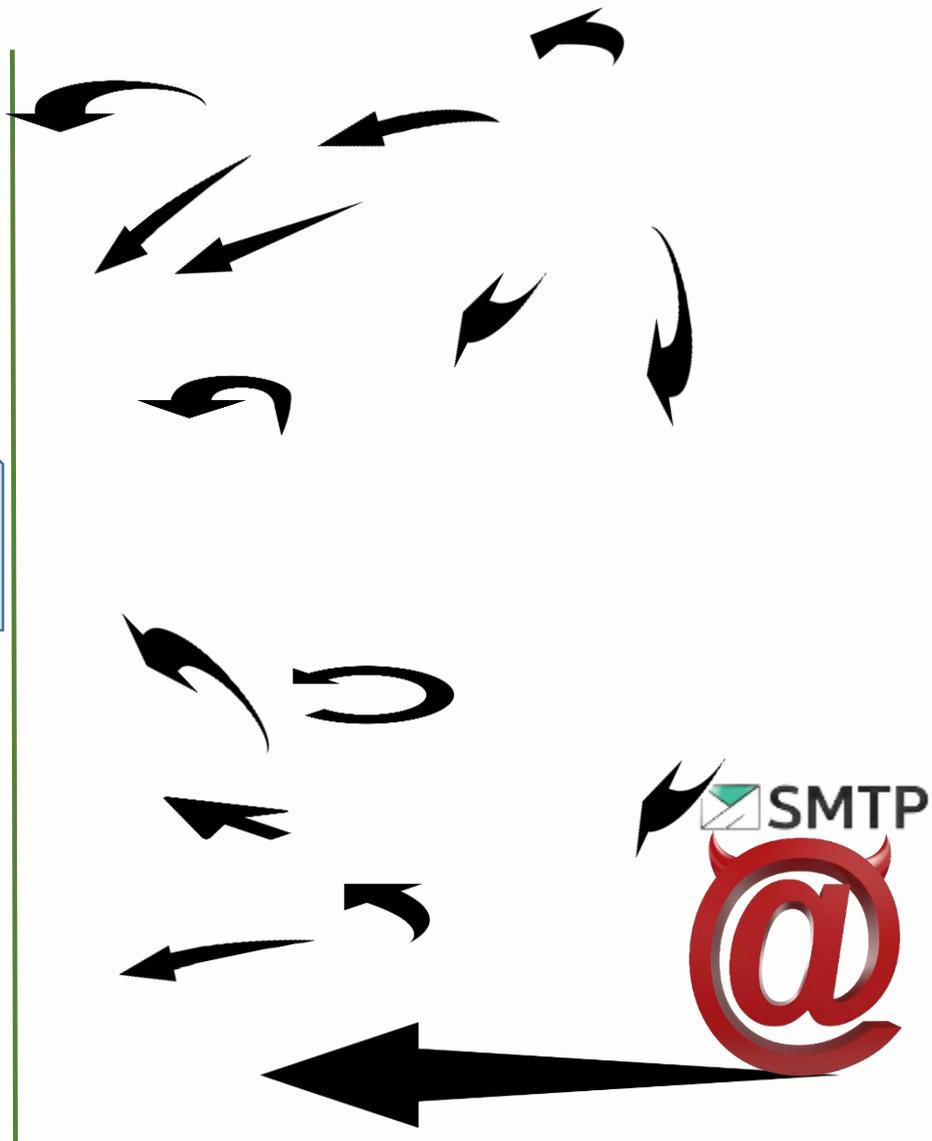


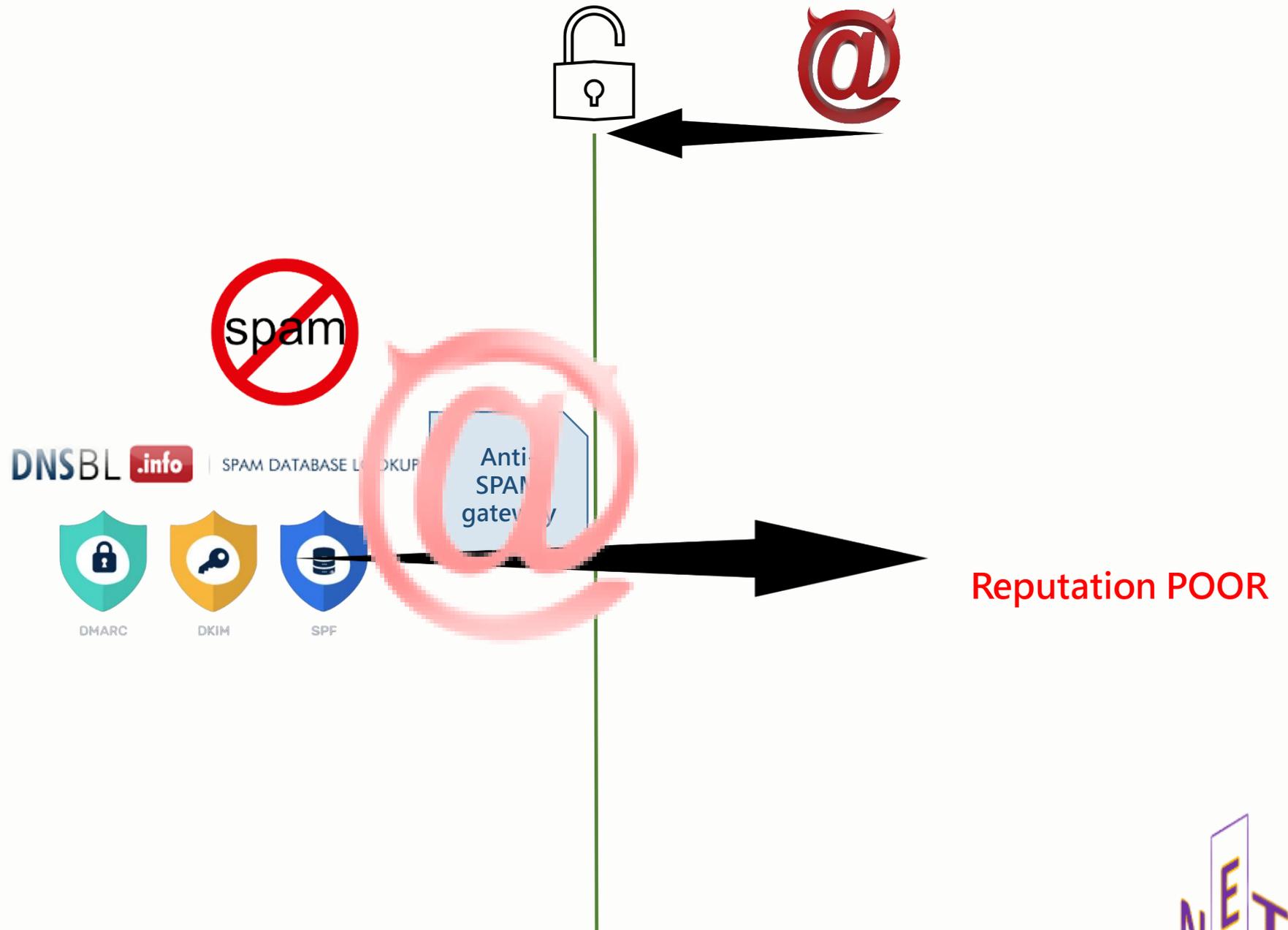


a_feed_FM_TNUA	 Feed	 
blacklist_cert_tanet <i>Last Updated: 2021-10-01 16:16:45</i>	List	 
blacklist_spamhaut <i>Last Updated: 2021-10-01 16:48:27</i>	List	 
blacklist_stopforumspam_0810 <i>Last Updated: 2022-08-10 15:22:55</i>	List	 
blacklist_stopforumspam_180 <i>Last Updated: 2022-08-12 17:16:40</i>	List	 
blacklist_talos <i>Last Updated: 2021-10-01 10:14:54</i>	List	 
blocklist.de-0815 <i>Last Updated: 2022-08-15 18:02:08</i>	List	 
cert_from_NTU_0810 <i>Last Updated: 2022-08-10 15:58:33</i>	List	 
Cisco-Intelligence-Feed <i>Last Updated: 2022-03-06 22:42:31</i>	Feed	 
Cisco-TID-Feed <i>Last Updated: 2022-08-17 15:33:09</i>	Feed	 
 forti-anomaly-0811 <i>Last Updated: 2022-08-11 13:14:14</i>	List ✓	 
 forti-ips-0812 <i>Last Updated: 2022-08-12 09:00:18</i>	List ✓	 
Global-Blacklist	List	 
Global-Whitelist	List	 
spamhaus_blacklist	Feed	 







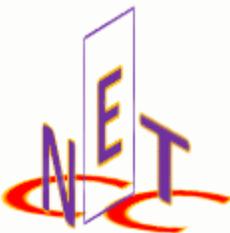




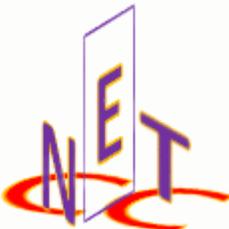
MOE Gateway

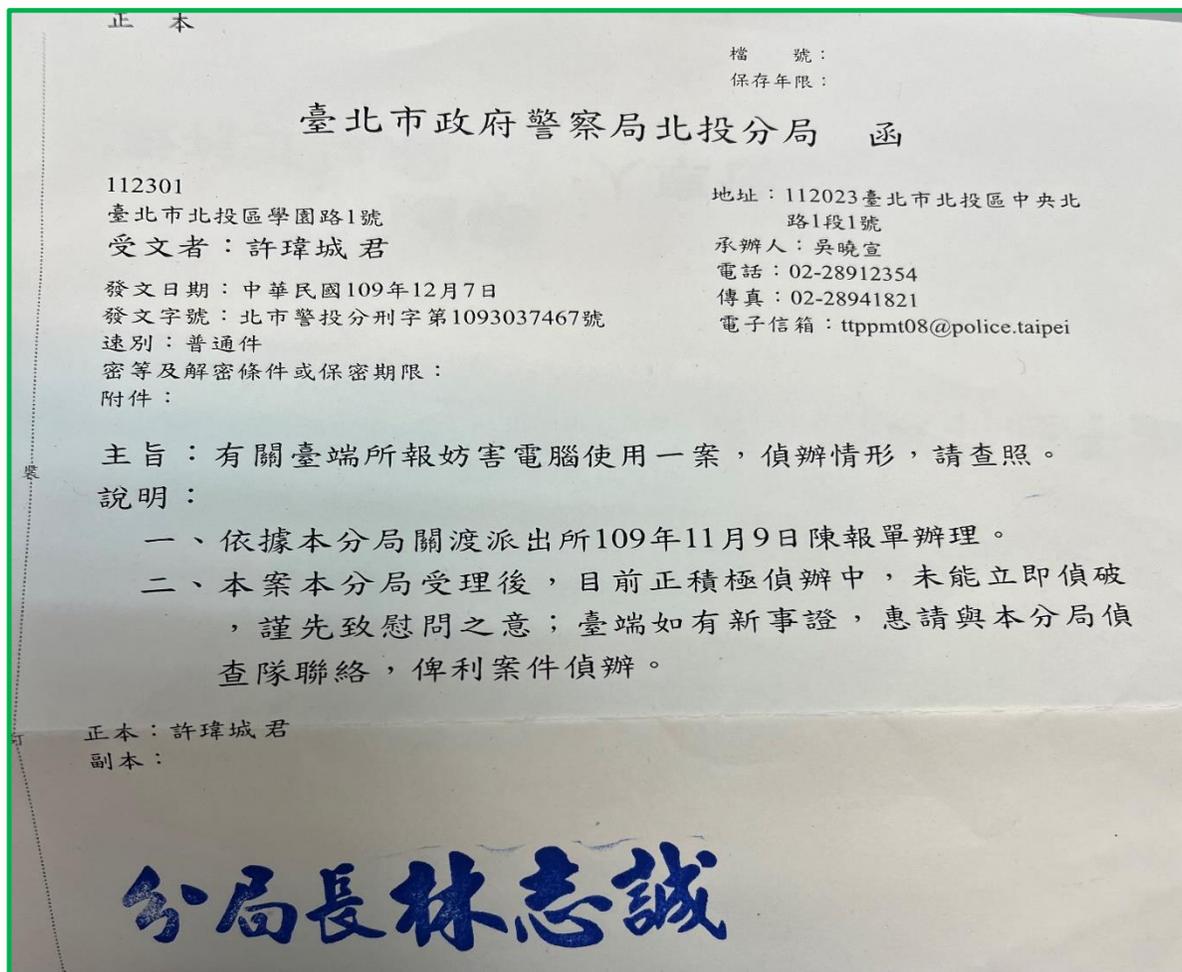


TNUA Gateway



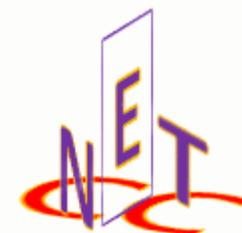
11/06 校內郵件伺服器主機遭受攻擊 處理時間說明 (109)





110報案過程

109/11/06報案，關渡派出所109/11/09送達
北投分局，北投分局 109/12/07 回函





中和某影城

案發事主，使用NVR系統

兩部 NVR 廠牌的DVR, IP是 118.111.111.17&118.111.111.18



中和某影城

109/11/06凌晨看到的
DVR畫面



```

2021-10-26 21:20:23 -2.000,AUTH_POP3_ERR,,117.68.147.178:58200,203.71.172.162:995,l1chen,123456l1chen,SSL,INBOUND
2021-10-26 21:20:23 -2.000,AUTH_SERVER_ERR,,117.68.147.178:58200,203.71.172.238:25,l1chen,123456l1chen,SSL,INBOUND
2021-10-26 21:20:42 -2.000,AUTH_POP3_ERR,,117.68.147.178:59024,203.71.172.162:995,l1chen,123l1chen,SSL,INBOUND
2021-10-26 21:20:42 -2.000,AUTH_SERVER_ERR,,117.68.147.178:59024,203.71.172.238:25,l1chen,123l1chen,SSL,INBOUND
2021-10-26 21:20:59 -2.000,AUTH_POP3_ERR,,117.68.147.178:59863,203.71.172.162:995,l1chen,mail11chen,SSL,INBOUND
2021-10-26 21:20:59 -2.000,AUTH_SERVER_ERR,,117.68.147.178:59863,203.71.172.238:25,l1chen,mail11chen,SSL,INBOUND
2021-10-26 21:21:00 -2.000,AUTH_POP3_ERR,,147.182.250.180:43160,203.71.172.162:995,m10162021@newmedia.tnuu.edu.tw,sss100421,NOSSL,INBOUND
2021-10-26 21:21:00 -2.000,AUTH_SERVER_ERR,,147.182.250.180:43160,203.71.172.238:25,m10162021@newmedia.tnuu.edu.tw,sss100421,NOSSL,INBOUND
2021-10-26 21:21:13 -2.000,AUTH_POP3_ERR,,69.89.126.130:38993,203.71.172.162:995,lanwu@www.tnuu.edu.tw,lanwu2221,SSL,INBOUND
2021-10-26 21:21:13 -2.000,AUTH_SERVER_ERR,,69.89.126.130:38993,203.71.172.238:465,lanwu@www.tnuu.edu.tw,lanwu2221,SSL,INBOUND
2021-10-26 21:21:15 -2.000,AUTH_POP3_ERR,,117.68.147.178:61063,203.71.172.162:995,l1chen,l1chen@theatre,SSL,INBOUND
2021-10-26 21:21:15 -2.000,AUTH_SERVER_ERR,,117.68.147.178:61063,203.71.172.238:25,l1chen,l1chen@theatre,SSL,INBOUND
2021-10-26 21:22:02 -2.000,AUTH_POP3_ERR,,123.186.228.118:62581,203.71.172.162:995,l1chen,theatre123456,SSL,INBOUND
2021-10-26 21:22:02 -2.000,AUTH_SERVER_ERR,,123.186.228.118:62581,203.71.172.238:25,l1chen,theatre123456,SSL,INBOUND
2021-10-26 21:22:15 -2.000,AUTH_POP3_ERR,,166.155.95.83:18373,203.71.172.162:995,lanwu@www.tnuu.edu.tw,lanwu22421,SSL,INBOUND
2021-10-26 21:22:15 -2.000,AUTH_SERVER_ERR,,166.155.95.83:18373,203.71.172.238:465,lanwu@www.tnuu.edu.tw,lanwu22421,SSL,INBOUND
2021-10-26 21:22:20 -2.000,AUTH_POP3_ERR,,123.186.228.118:63703,203.71.172.162:995,l1chen,theatre54321,SSL,INBOUND
2021-10-26 21:22:20 -2.000,AUTH_SERVER_ERR,,123.186.228.118:63703,203.71.172.238:25,l1chen,theatre54321,SSL,INBOUND
2021-10-26 21:22:40 -2.000,AUTH_POP3_ERR,,123.186.228.118:64832,203.71.172.162:995,l1chen,theatre111,SSL,INBOUND
2021-10-26 21:22:40 -2.000,AUTH_SERVER_ERR,,123.186.228.118:64832,203.71.172.238:25,l1chen,theatre111,SSL,INBOUND
2021-10-26 21:23:09 -2.000,AUTH_POP3_ERR,,123.186.228.118:49729,203.71.172.162:995,l1chen,theatre666,SSL,INBOUND
2021-10-26 21:23:09 -2.000,AUTH_SERVER_ERR,,123.186.228.118:49729,203.71.172.238:25,l1chen,theatre666,SSL,INBOUND
2021-10-26 21:23:26 -2.000,AUTH_POP3_ERR,,123.186.228.118:51562,203.71.172.162:995,l1chen,theatre888,SSL,INBOUND
2021-10-26 21:23:26 -2.000,AUTH_SERVER_ERR,,123.186.228.118:51562,203.71.172.238:25,l1chen,theatre888,SSL,INBOUND
2021-10-26 21:23:43 -2.000,AUTH_POP3_ERR,,123.186.228.118:52544,203.71.172.162:995,l1chen,theatre999,SSL,INBOUND
2021-10-26 21:23:43 -2.000,AUTH_SERVER_ERR,,123.186.228.118:52544,203.71.172.238:25,l1chen,theatre999,SSL,INBOUND
2021-10-26 21:24:00 -2.000,AUTH_POP3_ERR,,123.186.228.118:53458,203.71.172.162:995,l1chen,theatre,SSL,INBOUND
2021-10-26 21:24:00 -2.000,AUTH_SERVER_ERR,,123.186.228.118:53458,203.71.172.238:25,l1chen,theatre,SSL,INBOUND
2021-10-26 21:24:18 -2.000,AUTH_POP3_ERR,,123.186.228.118:54371,203.71.172.162:995,l1chen,theatre123,SSL,INBOUND
2021-10-26 21:24:18 -2.000,AUTH_SERVER_ERR,,123.186.228.118:54371,203.71.172.238:25,l1chen,theatre123,SSL,INBOUND
2021-10-26 21:24:36 -2.000,AUTH_POP3_ERR,,192.181.170.32:48885,203.71.172.162:995,edison@www.tnuu.edu.tw,god46534821,SSL,INBOUND
2021-10-26 21:24:36 -2.000,AUTH_SERVER_ERR,,192.181.170.32:48885,203.71.172.238:465,edison@www.tnuu.edu.tw,god46534821,SSL,INBOUND
2021-10-26 21:24:43 -2.000,AUTH_POP3_ERR,,123.186.228.118:55228,203.71.172.162:995,l1chen,theatre2012,SSL,INBOUND
2021-10-26 21:24:43 -2.000,AUTH_SERVER_ERR,,123.186.228.118:55228,203.71.172.238:25,l1chen,theatre2012,SSL,INBOUND
2021-10-26 21:25:00 -2.000,AUTH_POP3_ERR,,123.186.228.118:56540,203.71.172.162:995,l1chen,theatre2013,SSL,INBOUND
2021-10-26 21:25:00 -2.000,AUTH_SERVER_ERR,,123.186.228.118:56540,203.71.172.238:25,l1chen,theatre2013,SSL,INBOUND
2021-10-26 21:54:58 -2.000,AUTH_POP3_ERR,,122.116.120.46:44829,203.71.172.162:995,m9414001@music.tnuu.edu.tw,Zusmonique17701,SSL,INBOUND
2021-10-26 21:54:58 -2.000,AUTH_SERVER_ERR,,122.116.120.46:44829,203.71.172.238:465,m9414001@music.tnuu.edu.tw,Zusmonique17701,SSL,INBOUND
2021-10-26 21:55:04 -2.000,AUTH_POP3_ERR,,111.240.211.62:56157,203.71.172.162:995,m10162021@newmedia.tnuu.edu.tw,sss100401,NOSSL,INBOUND
2021-10-26 21:55:04 -2.000,AUTH_SERVER_ERR,,111.240.211.62:56157,203.71.172.238:25,m10162021@newmedia.tnuu.edu.tw,sss100401,NOSSL,INBOUND
2021-10-26 21:55:34 -2.000,AUTH_POP3_ERR,,122.116.120.46:45182,203.71.172.162:995,lanwu@www.tnuu.edu.tw,lanwu22401,SSL,INBOUND
2021-10-26 21:55:34 -2.000,AUTH_SERVER_ERR,,122.116.120.46:45182,203.71.172.238:465,lanwu@www.tnuu.edu.tw,lanwu22401,SSL,INBOUND

```

持續猜密碼

晨昏定省

```

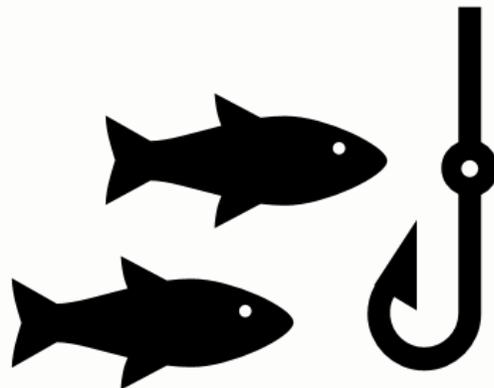
2022-06-14 10:50:08 -2.000,AUTH_SERVER_ERR,,172.90.21.238:45092,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:06:51 -2.000,AUTH_POP3_ERR,,199.77.205.160:49904,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:06:51 -2.000,AUTH_SERVER_ERR,,199.77.205.160:49904,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:07:22 -2.000,AUTH_POP3_ERR,,194.230.103.103:56549,203.71.172.162:995,shichang@newmedia.tnuu.edu.tw,shichang2008,
2022-06-14 11:07:22 -2.000,AUTH_SERVER_ERR,,194.230.103.103:56549,203.71.172.162:995,shichang@newmedia.tnuu.edu.tw,shichang2008
2022-06-14 11:24:31 -2.000,AUTH_POP3_ERR,,217.9.101.34:34142,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:24:31 -2.000,AUTH_SERVER_ERR,,217.9.101.34:34142,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:26:52 -2.000,AUTH_POP3_ERR,,63.41.161.202:54191,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:26:52 -2.000,AUTH_SERVER_ERR,,63.41.161.202:54191,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:27:55 -2.000,AUTH_POP3_ERR,,38.89.156.44:60017,203.71.172.162:995,school@fmaul@maul.tnuu.edu.tw,gle3r4,SSL
2022-06-14 11:27:55 -2.000,AUTH_SERVER_ERR,,38.89.156.44:60017,203.71.172.162:995,school@fmaul@maul.tnuu.edu.tw,gle3r4,SSL
2022-06-14 11:32:20 -2.000,AUTH_POP3_ERR,,216.49.232.146:39940,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:32:20 -2.000,AUTH_SERVER_ERR,,216.49.232.146:39940,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:32:54 -2.000,AUTH_POP3_ERR,,194.158.241.155:52487,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:32:54 -2.000,AUTH_SERVER_ERR,,194.158.241.155:52487,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:45:06 -2.000,AUTH_POP3_ERR,,209.173.162.231:60493,203.71.172.162:995,school@fmaul@maul.tnuu.edu.tw,schoolofm
2022-06-14 11:45:06 -2.000,AUTH_SERVER_ERR,,209.173.162.231:60493,203.71.172.162:995,school@fmaul@maul.tnuu.edu.tw,schoolofm
2022-06-14 11:51:36 -2.000,AUTH_POP3_ERR,,46.165.180.97:50447,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:51:36 -2.000,AUTH_SERVER_ERR,,46.165.180.97:50447,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 11:57:00 -2.000,AUTH_POP3_ERR,,209.188.65.59:55980,203.71.172.162:995,tellin@maul.tnuu.edu.tw,tellin2012,SSL,INB
2022-06-14 11:57:00 -2.000,AUTH_SERVER_ERR,,209.188.65.59:55980,203.71.172.162:995,tellin@maul.tnuu.edu.tw,tellin2012,SSL,INB
2022-06-14 12:00:28 -2.000,AUTH_POP3_ERR,,43.135.156.107:55104,203.71.172.162:995,master@lance.tnuu.edu.tw,88888888,SSL,IN
2022-06-14 12:00:28 -2.000,AUTH_SERVER_ERR,,43.135.156.107:55104,203.71.172.162:995,master@lance.tnuu.edu.tw,88888888,SSL,INB
2022-06-14 12:10:04 -2.000,AUTH_POP3_ERR,,211.39.130.134:1377,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:10:04 -2.000,AUTH_SERVER_ERR,,211.39.130.134:1377,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:11:59 -2.000,AUTH_POP3_ERR,,101.98.52.66:45218,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:11:59 -2.000,AUTH_SERVER_ERR,,101.98.52.66:45218,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:15:06 -2.000,AUTH_POP3_ERR,,217.91.16.45:39994,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:15:06 -2.000,AUTH_SERVER_ERR,,217.91.16.45:39994,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:19:51 -2.000,AUTH_POP3_ERR,,84.241.80.93:58202,203.71.172.162:995,master@lance.tnuu.edu.tw,123456,SSL,INBOUND
2022-06-14 12:19:51 -2.000,AUTH_SERVER_ERR,,84.241.80.93:58202,203.71.172.162:995,master@lance.tnuu.edu.tw,123456,SSL,INBOUND
2022-06-14 12:20:04 -2.000,AUTH_POP3_ERR,,207.190.110.158:48198,203.71.172.162:995,master@lance.tnuu.edu.tw,123456,SSL,INB
2022-06-14 12:20:04 -2.000,AUTH_SERVER_ERR,,207.190.110.158:48198,203.71.172.162:995,master@lance.tnuu.edu.tw,123456,SSL,INB
2022-06-14 12:28:54 -2.000,AUTH_POP3_ERR,,212.101.17.133:41401,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:28:54 -2.000,AUTH_SERVER_ERR,,212.101.17.133:41401,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:34:00 -2.000,AUTH_POP3_ERR,,64.203.198.219:59948,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2
2022-06-14 12:34:00 -2.000,AUTH_SERVER_ERR,,64.203.198.219:59948,203.71.172.162:995,shilaupeng@lincarta.tnuu.edu.tw,shilaupeng2

```

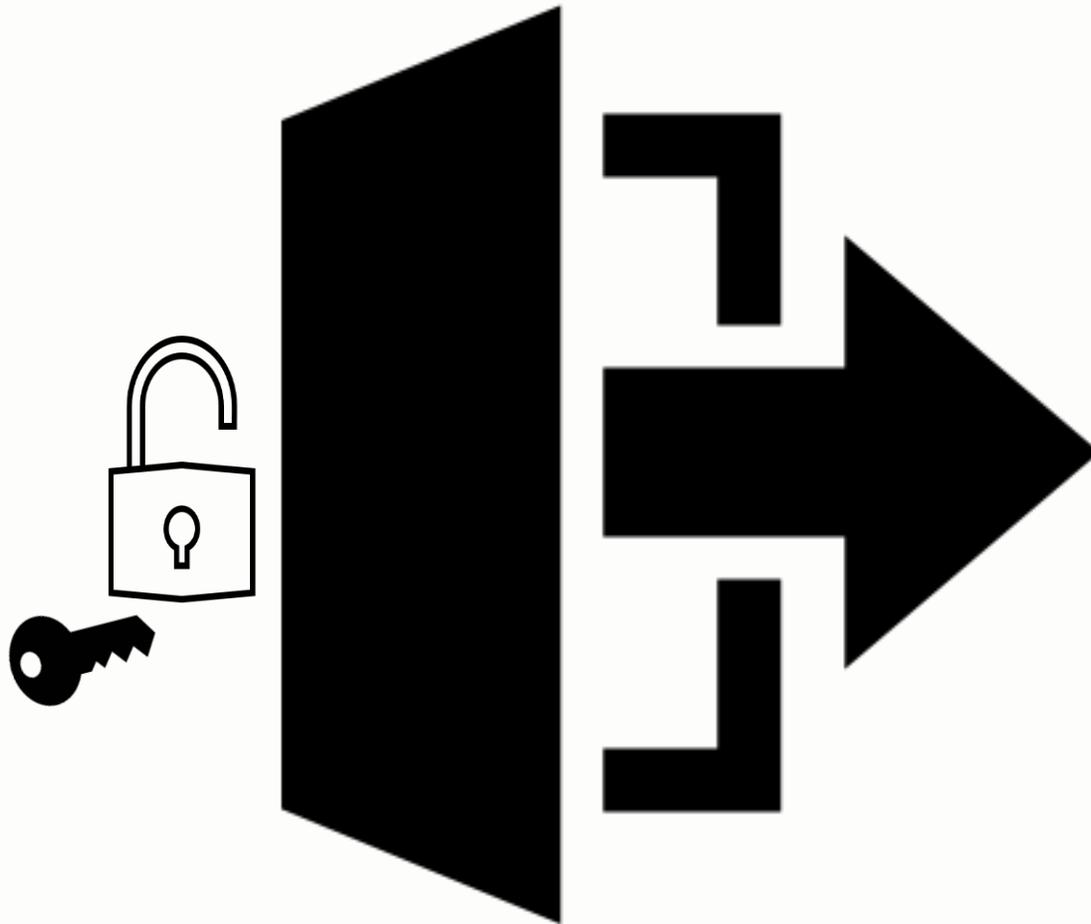
持續猜密碼

照三餐問候





釣魚是一種娛樂
尤其是釣黑魚



◆ 用於驗證，並非是攻擊手法或是網路攻擊示範，僅用於研討會實例說明。

◆ 部分圖示節錄於網路，僅供研討會使用

162.105.240.2	-	No	0.0	0.5	1	Poor
162.105.109.222	-	No	0.0	0.5	1	Poor
162.105.98.229	-	No	0.0	0.5	1	Poor
162.105.78.230	-	No	1.9	0.5	1	Poor
162.105.78.182	-	No	0.0	0.5	1	Poor
162.105.78.72	-	No	1.9	0.5	1	Poor
162.105.65.182	-	No	0.0	0.5	1	Poor
162.105.60.11	-	No	0.0	0.5	1	Poor
162.105.59.113	-	No	0.0	0.8	1	Poor
162.105.54.3	-	No	0.0	1.4	1	Poor
162.105.52.86	-	No	0.0	0.5	1	Poor
162.105.49.198	-	No	0.0	0.5	1	Poor
162.105.48.194	-	No	0.0	0.8	1	Poor
162.105.41.41	-	No	0.0	0.5	1	Poor
162.105.35.123	-	No	0.0	0.5	1	Poor
162.105.35.75	-	No	0.0	0.5	1	Poor
162.105.33.30	-	No	0.0	0.5	1	Poor
osa-3281.health.cmu.edu	Yes	0.0	0.8	1	Poor	
osa-3005.health.cmu.edu	Yes	0.0	0.5	1	Poor	
osa-dock-3254.studentaffairs.cmu.edu	Yes	0.0	1.3	1	Poor	
osa-3265.health.cmu.edu	Yes	0.0	0.5	1	Poor	
storaiviv-d.health.cmu.edu	Yes	0.0	0.5	1	Poor	
osa-2919.health.cmu.edu	Yes	0.0	0.5	1	Poor	
th-lie-12.health.cmu.edu	Yes	0.0	0.5	1	Poor	
stroom212-d.studentaffairs.cmu.edu	Yes	0.0	1.0	1	Poor	
st-image-d.health.cmu.edu	Yes	0.0	0.5	1	Poor	
th-lab03-d.health.cmu.edu	Yes	0.0	0.5	1	Poor	
osa-1990.health.cmu.edu	Yes	0.0	1.0	1	Poor	
osa-2938.health.cmu.edu	Yes	0.0	0.5	1	Poor	
st-mieffer-d.health.cmu.edu	Yes	0.0	0.5	1	Poor	
th-piemison-h.campus-services.cmu.edu	Yes	3.2	3.2	1	Poor	
st-oncall-i.health.cmu.edu	Yes	0.0	0.5	1	Poor	
osa-3272.health.cmu.edu	Yes	0.0	0.8	1	Poor	

透過sendbase

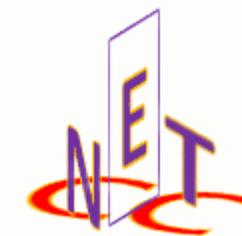
是否可以找到pku, cmu Reputation 相關?

```
227 Entering Passive Mode (140.110.10.231,218,192)
150 Opening BINARY mode data connection for 'file list'.
dr-xr-xr-x  1 james  users           16 Oct 23  2018 CLUSE
dr-xr-xr-x  1 shangyu users          128 Sep 16  2018 CNN-DailyMail
-r-xr-xr-x  1 shangyu users       254487464 Jun 01  2020 12kd_data.zip
dr-xr-xr-x  1 james  users           16 Dec 10  2018 rationale_data
226 Transfer complete.
```

```
[root@166 ~]# nmap -Pn 140.110.10.231
Starting Nmap 7.70 ( https://nmap.org ) at 2022-08-10 10:03:33 CST
Nmap scan report for srlab.140.110.10.231.tw (140.110.10.231)
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   filtered netbios-ssn
389/tcp   filtered ldap
443/tcp   open  https
445/tcp   filtered microsoft-ds
548/tcp   open  afp
636/tcp   filtered ldapssl
873/tcp   open  rsync
2000/tcp  open  cisco-sccp
2049/tcp  open  nfs
3261/tcp  open  winshadow
5000/tcp  open  upnp
5001/tcp  open  complex-link
5060/tcp  open  sip
6666/tcp  filtered irc
6667/tcp  filtered irc
6668/tcp  filtered irc
6669/tcp  filtered irc
8008/tcp  open  http
```

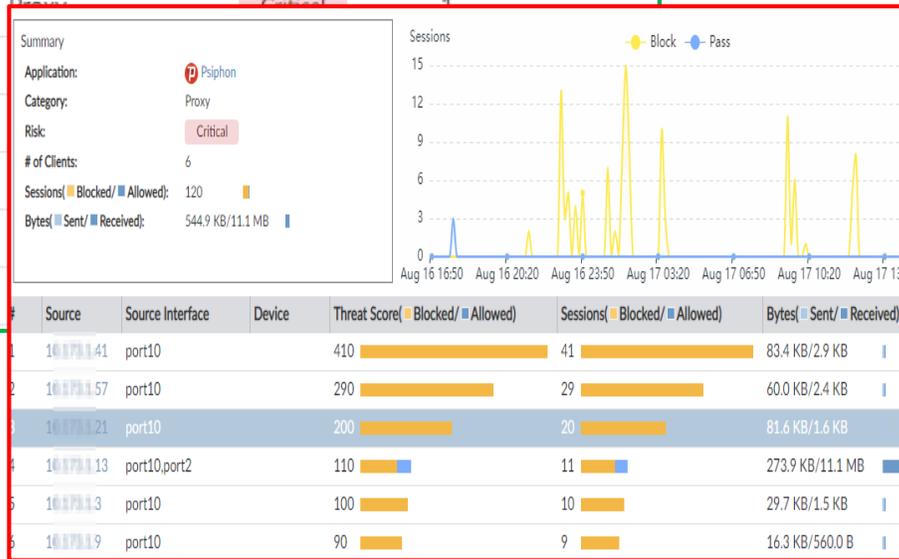
TANet 掃描PORT

找到NAS, 如何找使用者名稱?

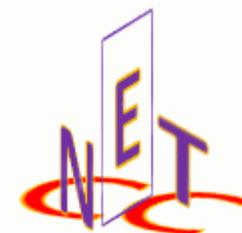


SPAMMER 只有你能打我嗎?

#	Application	Category	▼ Risk	# of Clients
1	Proxy.HTTP	Proxy	Critical	98
2	Surfshark.VPN	Proxy	Critical	3
3	Psiphon	Proxy	Critical	6
4	Cloudflare.1.1.1.1.VP Proxy	Proxy	Critical	3
5	Hola.Unblocker	Proxy	Critical	1
6	Hotspot.Shield	Proxy	Critical	1
7	Ultrasurf	Proxy	Critical	1
8	Hamachi	Proxy	Critical	1
9	SOCKS4	Proxy	Critical	1
10	SOCKS5	Proxy	Critical	1



VPN	Best Price
+ NordVPN	\$ 3.99 /月
+ Surfshark	\$ 2.30 /月
+ ExpressVPN	\$ 8.32 /月
+ IPVanish	\$ 3.25 /月
+ TorGuard	\$ 4.99 /月
+ FastestVPN	\$ 2.49 /月
+ PIA	\$ 2.42 /月
+ 熱點S.	\$ 7.99 /月
+ PureVPN	\$ 3.33 /月
+ 的VyprVPN	\$ 2.50 /月



SPAMMER 只有你能打我嗎?

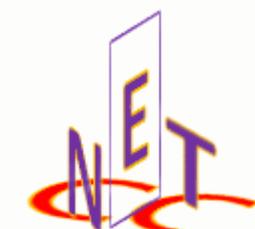
```
136 75 - PuTTY
login as:
ubnt@136:75's password:
Linux ubnt 3.10.107-UBNT #1 SMP Mon Oct 1 12:41:38 UTC 2018 mips
Welcome to EdgeOS
ubnt@ubnt:~$ w
 01:41:20 up 531 days, 1:48, 1 user, load average: 3.40, 3.42, 3.47
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
ubnt     pts/0    212.102.42.200  01:41    2.00s  0.16s  0.03s w
ubnt@ubnt:~$ more /etc/*release*
PRETTY_NAME="Debian GNU/Linux 7 (wheezy)"
NAME="Debian GNU/Linux"
VERSION_ID="7"
VERSION="7 (wheezy)"
ID=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support/"
BUG_REPORT_URL="http://bugs.debian.org/"
ubnt@ubnt:~$
```

IP 位址查詢

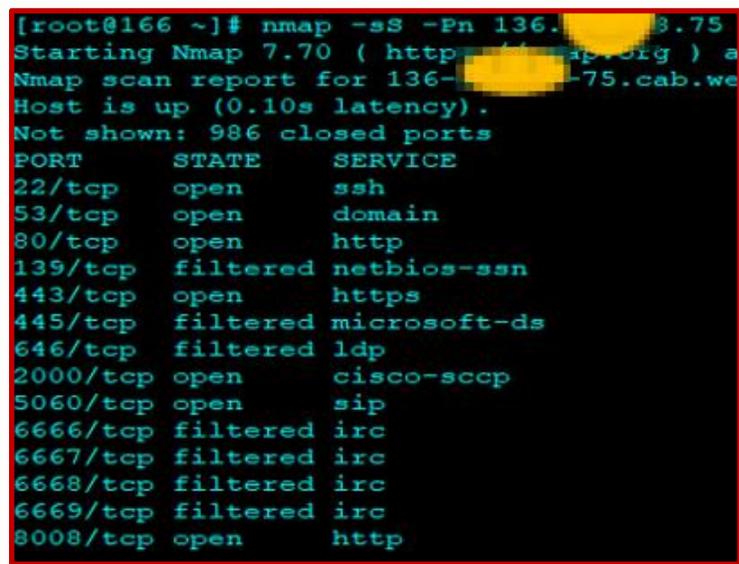
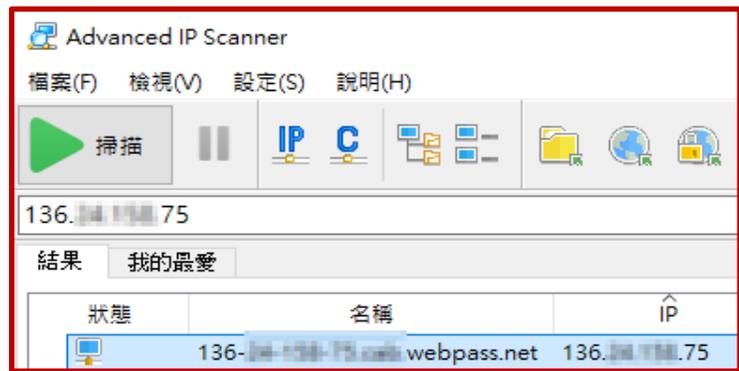
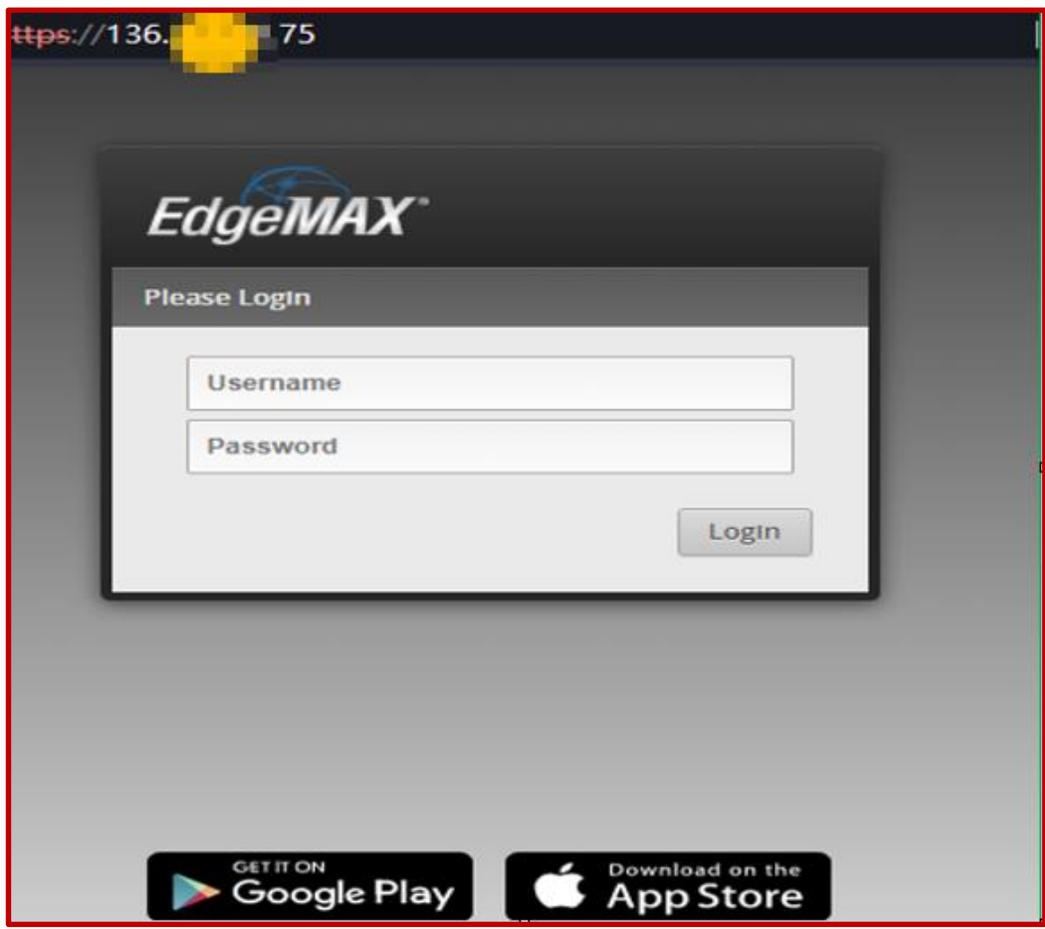
請輸入您想查詢的 IP 位址:

免費 IP 查詢 地圖資料 ©2022 提供協助 區域地圖服務

提供詳細的 IP 位址資訊	查詢名稱
Datacamp Limited	cdn77.com
國家	地區 / 州
Hong Kong, Central and Western District, Central	Central and Western District
城市	區域
Central	Unknown



■ SPAMMER 只有你能打我嗎?



■ SPAMMER 只有你能打我嗎?

IP黑名單

16[REDACTED].199 查詢

搜尋 : 16[REDACTED].199

#	時間	備註	寫入時間
1	2022.06.23	系統每日排程	2022-06-24 04:00:02

16[REDACTED].199/default.asp

DIGI TRANSPORT WR44V2 (SN: 538243) CONFIGURATION A

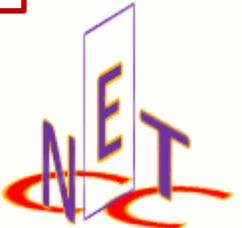
User : username

- Home
- Wizards
- Configuration
 - Network
 - Alarms
 - System
 - Remote Management
 - Security
 - Telemetry
- Applications
 - Basic
 - Python
- Management
 - Network Status
 - Connections
 - Telemetry
 - Event Log
 - Analyser
 - Top Talkers
- Administration
 - System Information
 - File Management
 - X.509 Certificate Management

Management - Event Log

```
18:34:33, 04 Aug 2022, GP socket connect
18:34:33, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:29, 04 Aug 2022, GP socket connect
18:34:29, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:26, 04 Aug 2022, GP socket connect
18:34:25, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:20, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:20, 04 Aug 2022, TCP Req Fail: 166
18:34:19, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:17, 04 Aug 2022, GP socket connect
18:34:17, 04 Aug 2022, TCP Req Fail: 166
18:34:17, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:17, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:10, 04 Aug 2022, GP socket connect
18:34:10, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:08, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:07, 04 Aug 2022, GP socket connect
18:34:06, 04 Aug 2022, TCP Req: 0.0.0.0:
18:34:00, 04 Aug 2022, TCP Req: 0.0.0.0:
18:33:59, 04 Aug 2022, TCP Req: 0.0.0.0:
18:33:59, 04 Aug 2022, GP socket connect
18:33:59, 04 Aug 2022, TCP Req: 0.0.0.0:
18:33:57, 04 Aug 2022, GP socket connect
18:33:57, 04 Aug 2022, TCP Req: 0.0.0.0:
18:33:56, 04 Aug 2022, GP socket connect
```

Refresh Clear Log Open in New Window



■ SPAMMER 只有你能打我嗎?

IP黑名單

147.███.███.11 查詢

搜尋：147.███.███.11

#	時間	備註	寫入時間
1	2022.07.09	系統每日排程	2022-07-10 04:00:01

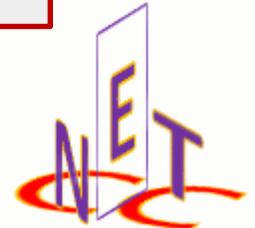
IgniteNet GLINQ IgniteNet

DASHBOARD NETWORK WIRELESS SYSTEM

System Settings Maintenance User Accounts Services Diagnostics

System Actions

View Log	View system log
Troubleshooting Log	Download this device's troubleshooting log
Reboot	Reboot your device
Reset	Reset to factory default settings
Backup	Download this device's configuration settings
Restore	Restore the configuration settings of this device



■ SPAMMER 只有你能打我嗎?

```
20220623.log:[19:37:14] [67.225.189.124:57732] [P] connect to 203.71.173.162 port 995
20220623.log:[19:37:14] [67.225.189.124:57732] [P] USER jim@lamesa.tnua.edu.tw
20220623.log:[19:37:14] [67.225.189.124:57732] [P] PASS XXXXXXXX
20220623.log:[19:37:24] [67.225.189.124:57732] [P] PASS failed: -ERR LOGIN failed
20220623.log:[19:37:24] [67.225.189.124:57732] [S] 535 Authentication failed
20220623.log:[19:37:24] [67.225.189.124:57732] smtp_fsm: peer_closed
```

TANKS										
Image	Manifold ID	Tank ID	Name	Product	Alarms	Level	Gross Volume	Net Volume	Ullage	Water Level
		1	Unlead	Unlead	🕒	61.92	3,165.69	3,112.79	639.95	0.03
		2	Diesel	Diesel	🕒	33.20	1,472.83	1,457.75	2,332.83	0.02
		3	Dyed Diesel	Dyed Diesel	🕒	52.23	2,617.32	2,588.85	1,188.37	0.01



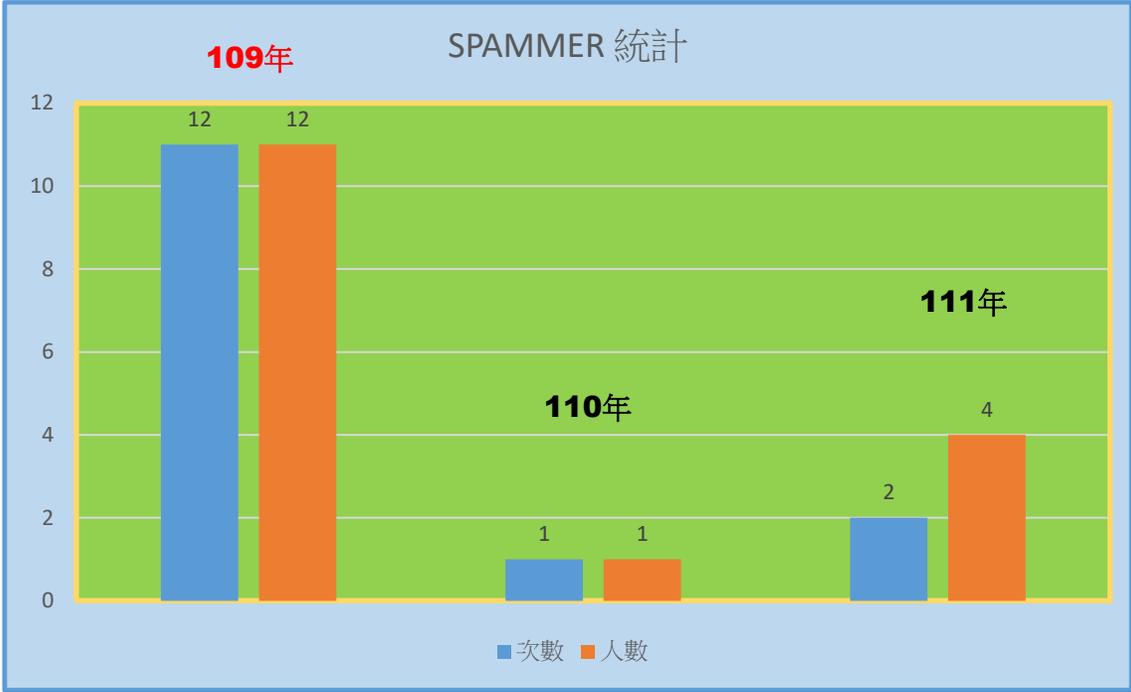
SPAMMER 只有你能打我嗎?

The screenshot shows a network monitoring dashboard with a table of scan results and a terminal window displaying an nmap scan output.

Time	Host	Method	Level	Port
2021/04/21-11:52:38	...	偵測:手動	AL1	i184
2021/04/21-11:52:38	...	偵測:手動	AL1	i188
2021/06/16-10:31:35
2021/10/25-14:26:37
2021/11/01-19:47:45
2022/01/13-16:14:06
2022/01/13-16:14:19
2022/03/18-15:16:17
2022/04/13-10:24:39
2022/05/27-10:46:01
2022/06/16-15:40:39
2022/07/20-00:50:10
2022/07/21-13:36:35
2022/07/21-13:36:35
2022/07/21-13:36:35
2022/07/30-21:42:35
2022/08/17-00:13:16
2022/08/18-08:14:29
2022/08/18-08:15:27

```
[root@166 ~]# nmap -O 220.128.143.73
Starting Nmap 7.70 ( https://nmap.org ) at 2022-08-18 11:58:08
Nmap scan report for 220.128.143.73
Host is up (0.044s latency).
Not shown: 983 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
53/tcp    open      domain
80/tcp    open      http
111/tcp   open      rpcbind
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
2000/tcp  open      cisco-sccp
3306/tcp  open      mysql
5060/tcp  open      sip
6666/tcp  filtered  irc
6667/tcp  filtered  irc
6668/tcp  filtered  irc
6669/tcp  filtered  irc
8008/tcp  open      http
8080/tcp  open      http-proxy
8888/tcp  open      sun-answerbook
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.39
Network Distance: 8 hops
```







發送時間：	2022-07-23 15:04:06
簡訊內容：	cello dangerous now 216.52
簡訊長度：	26 字
發送統計：	成功：2 筆, 失敗：0 筆, 尚未回覆狀態：0 筆

姓名	扣除通數	手機號碼	發送狀態
1		0921615281	已送達, 手機接收時間: 2022/07/23 15:04:06

發送時間：	2022-07-29 15:24:03
簡訊內容：	cello dangerous now 107.174
簡訊長度：	27 字
發送統計：	成功：2 筆, 失敗：0 筆, 尚未回覆狀態：0 筆

發送時間：	2022-07-30 15:56:07
簡訊內容：	cello dangerous now 104.168
簡訊長度：	27 字
發送統計：	成功：2 筆, 失敗：0 筆, 尚未回覆狀態：0 筆

姓名	扣除通數	手機號碼	發送狀態
1		0921615281	已送達, 手機接收時間: 2022/07/30 15:56:11

主旨: Re: EmailToSMS狀況回報

附加 提示: 從桌面上拖放檔案, 以將附件附加到此郵件。

寄件者: "台灣簡訊" <mailer@gw.twsms.com>
 收件者: "chw" <chw@tnua.edu.tw>
 寄件備份: 2022 7 月 29 星期五 下午 3:24:03
 主旨: EmailToSMS狀況回報

EMailToSMS 狀況回報.

時間: 2022-07-29 15:24:03

原因: 發送完成!

內容: cello dangerous now 107.174

星期五 15:24

cello dangerous now 107.174

前天 15:56

cello dangerous now 104.168



TNUA

2022-07-30 15:53:01	b109	被害OR加害	104.168.34.187	ollegas2021@gmail.c...	antigateway.tnua.edu.tw 465 b109
2022-07-30 15:52:52	b109		104.168.34.187	ollegas2021@gmail.c...	antigateway.tnua.edu.tw 465 b109
2022-07-29 15:50:25	b109		107.174.142.103	ollegas2021@gmail.c...	534330
2022-07-29 15:21:07	b109		107.174.142.103	ollegas2021@gmail.c...	4731
2022-07-23 15:01:32	b107		216.52.48.138	ollegas2021@gmail.c...	antigateway.tnua.edu.tw 465 b107

107.174.142.103 mail-mail-f187.looppose.com No 4.0 3.8 1 Poor

IP address details
107.174.142.103

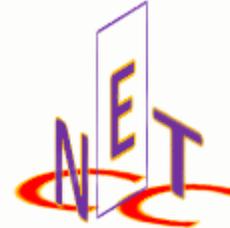
Los Angeles, CA

IP address details
216.52.48.138

Boston, Massachusetts, United States

IP address details
104.168.34.187
Washington, Washington, D.C., United States

104.168.34.187 104-168-34-187-host.colocrossing.com No 4.5 3.9 2 Poor



TNUA

帳號密碼查詢

請輸入以下資料做為身分驗證

身分資料(英文字母大寫)

身分證、居留證號、護照、入台證、大陸身分證(擇一)

生日

範例格式: 19860112

圖片驗證碼
12090

圖片驗證碼

(1) 密碼不能和前2次的一樣。

(2) 密碼一定要有8碼以上的英文與數字組合。

(3) [REDACTED]

(4) 密碼不可以有您的生日數字的組合，舉例：假設生日是1960.04.28，不可以有19600428(年月日)、1960(年)、0428(月日)、04(月)、28(日)的數字。

(5) 密碼不可以有您的EMAIL帳號，舉例：假設EMAIL是 usertnua@tnua.edu.tw，不可以有 usertnua文字。

(6) 教職員密碼不可以有您的學校分機號碼。

(7) [REDACTED]

新密碼

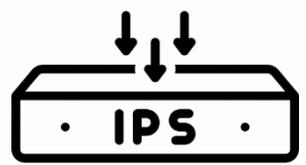
再次輸入新密碼

圖片驗證碼
80976

密碼設定

強度夠的密碼搭配好的MX政策
可以讓駭客猜到天荒地老





Initiator Country	Total Connections
CHN (China)	10,618,571
TWN (Taiwan Republic Of China)	8,821,824
USA (United States)	4,116,723
NLD (Netherlands)	2,224,845
HKG (Hong Kong)	1,673,311
GBR (United Kingdom)	1,506,558
DEU (Germany)	635,271
ZAF (South Africa)	587,047
RUS (Russian Federation)	536,929
IND (India)	394,730

阻擋的地區

凌晨阻擋七小福

IP Security Intelligence Category	Total Connections
forti-anomaly-0811	10,331,407
blocklist.de-0815	1,074,775
blacklist cert tanet	798,085
cert from NTU 0810	618,175
forti-ips-0812	387,958
Malware	191,360
blacklist stopforumspam 180	182,497
blacklist spamhaut	161,776
CnC	2,404
a feed FM TNUA	1,792

BLACK(BLOCK) IP



Block	IP Block	103.118.253.197	CHN	192.192.98.220	TWN	forti-anomaly-0811	External	Internal	60782 / tcp
Block	IP Block	185.90.169.230	LBN	192.192.98.50	TWN	forti-anomaly-0811	External	Internal	4247 / tcp
Block	IP Block	45.127.98.24	CHN	192.192.98.233	TWN	forti-anomaly-0811	External	Internal	37061 / tcp
Block	IP Block	45.127.98.24	CHN	192.192.98.202	TWN	forti-anomaly-0811	External	Internal	37173 / tcp
Block	IP Block	198.98.61.9	USA	192.192.98.231	TWN	blocklist.de-0815	External	Internal	55344 / tcp
Block	IP Block	185.90.169.230	LBN	192.192.98.34	TWN	forti-anomaly-0811	External	Internal	62751 / tcp
Block	IP Block	185.90.169.230	LBN	192.192.98.42	TWN	forti-anomaly-0811	External	Internal	17427 / tcp
Block	IP Block	93.90.72.183	ZAF	192.192.98.103	TWN	forti-anomaly-0811	External	Internal	49586 / tcp
Block	IP Block	185.90.169.230	LBN	192.192.98.37	TWN	forti-anomaly-0811	External	Internal	62659 / tcp
Block	IP Block	185.90.169.230	LBN	192.192.98.29	TWN	forti-anomaly-0811	External	Internal	62667 / tcp
Block	IP Block	45.95.55.24	DEU	192.192.98.204	TWN	forti-anomaly-0811	External	Internal	10704 / tcp
Block	IP Block	218.210.37.124	TWN	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	47427 / tcp
Block	IP Block	89.248.165.52	NLD	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	40587 / tcp
Block	IP Block	120.25.147.48	CHN	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	6000 (x11) /
Block	IP Block	139.59.14.1	IND	192.192.17.252	TWN	blocklist.de-0815	External	Internal	44544 / tcp
Block	IP Block	64.62.197.116	USA	192.192.17.252	TWN	blacklist_cert_tanet	External	Internal	51841 / tcp
Block	IP Block	167.248.133.137	USA	192.192.17.252	TWN	Malware	External	Internal	4483 / tcp
Block	IP Block	150.129.81.246	HKG	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	54240 / tcp
Block	IP Block	211.103.227.254	CHN	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	8 (Echo Requ
Block	IP Block	45.143.200.102	BGR	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	40028 / tcp
Block	IP Block	5.180.99.245	GBR	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	44523 / tcp
Block	IP Block	45.93.16.115	USA	192.192.17.252	TWN	forti-anomaly-0811	External	Internal	5077 / udp

新申請IP

網頁沒有暴露相關訊息，
但是持續有相關掃描

zh-hant.ipshu.com/ip_d_list/192.192.99

IP / 域名 / 關鍵字 搜尋 我的IP 路由器 Whois

第一個IP地址示例

192.192.99.1 Taiwan (TW)

Region: Taiwan
Area: Taipei
City: Taipei
ISP: MOEC

Usage Type: EDU
University/College/School

Net Speed: COMP

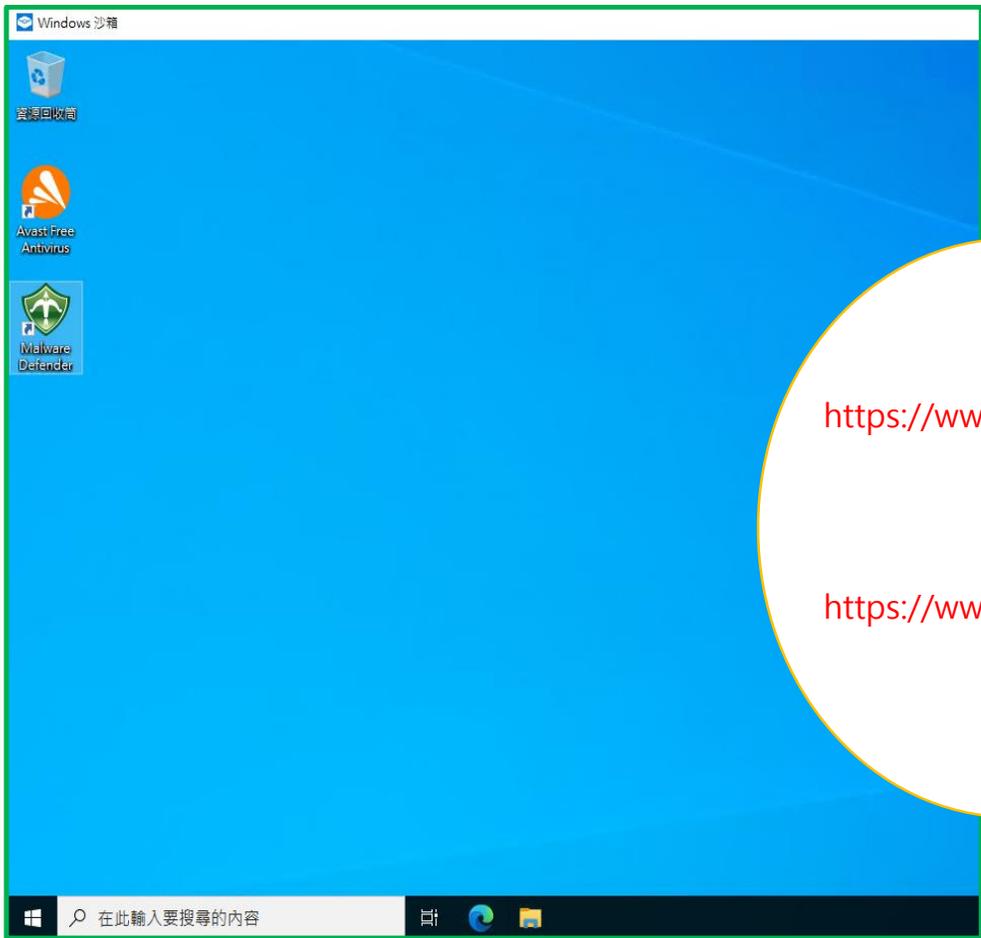
#截止2022-08-21, 台湾IP地址共计587条记录, IP地址总数35695616.

#查看 台湾

#IP起始	结束	数量
1.34.0.0	1.35.255.255	131072
1.160.0.0	1.175.255.255	1048576
1.200.0.0	1.200.255.255	65536
2.58.240.0	2.58.243.255	1024
27.0.152.0	27.0.155.255	1024
27.51.0.0	27.53.255.255	196608
27.96.224.0	27.96.255.255	8192
27.100.64.0	27.100.127.255	16384
27.105.0.0	27.105.255.255	65536
27.147.0.0	27.147.63.255	16384
27.240.0.0	27.247.255.255	524288
36.224.0.0	36.239.255.255	1048576
39.1.0.0	39.1.255.255	65536
39.8.0.0	39.15.255.255	524288
42.0.64.0	42.0.127.255	16384
42.64.0.0	42.79.255.255	1048576
43.224.20.0	43.224.23.255	1024
43.224.248.0	43.224.249.255	512
43.226.232.0	43.226.235.255	1024
43.227.24.0	43.227.27.255	1024
43.240.24.0	43.240.27.255	1024
43.240.44.0	43.240.47.255	1024
43.240.104.0	43.240.111.255	2048
43.240.152.0	43.240.155.255	1024
43.241.32.0	43.241.35.255	1024
43.241.160.0	43.241.163.255	1024
43.243.252.0	43.243.255.255	1024
43.246.188.0	43.246.191.255	1024
43.246.216.0	43.246.219.255	1024

IP資訊





<https://www.zoomeye.org/>
<https://www.shodan.io/host>

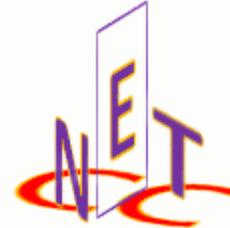


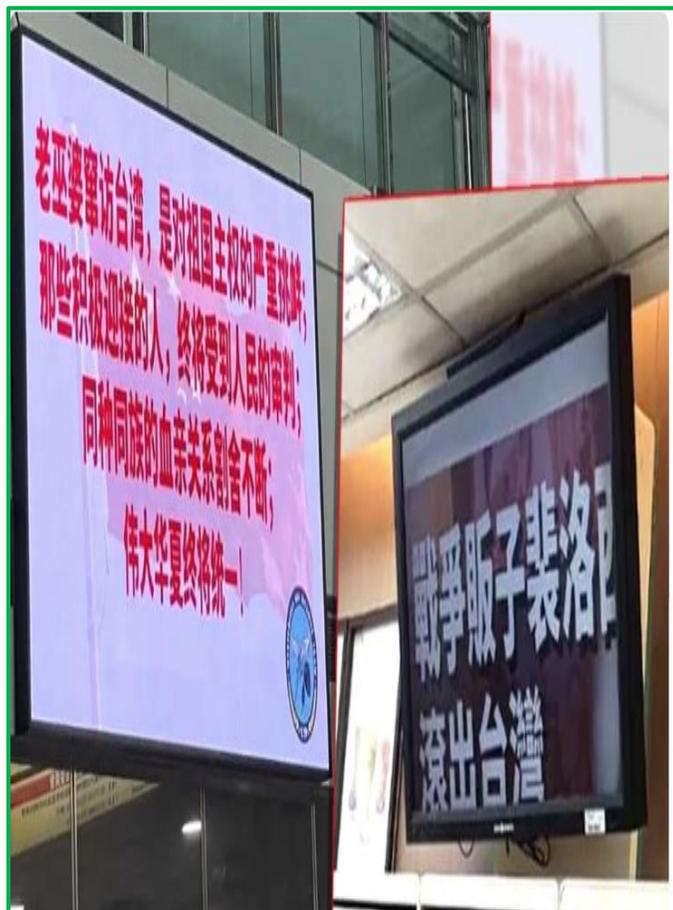
建議使用 虛擬機、windows 沙箱

來路不明軟體、或是測試
關機後 沙箱會清除

網路使用疏忽會有資安疑慮

手機熱點分享筆電使用後，筆電內有明碼紀錄





成立資安專案，爰請各校協助辦理以下事項：

一、請密切注意貴校首頁內容是否有遭惡意竄改、插旗等行為，至8月8日中午12時止請24小時定期檢視，並於校安系統回報狀況。

二、若遭竄改，除依通報流程儘速通報外，也請緊急將網頁下架，減輕傷害。

三、假日期間若行政單位或系所網站無服務之必要，建議關機或限制連線，降低風險。

四、大專校院校安中心配合事項：

網路攻擊

推播系統

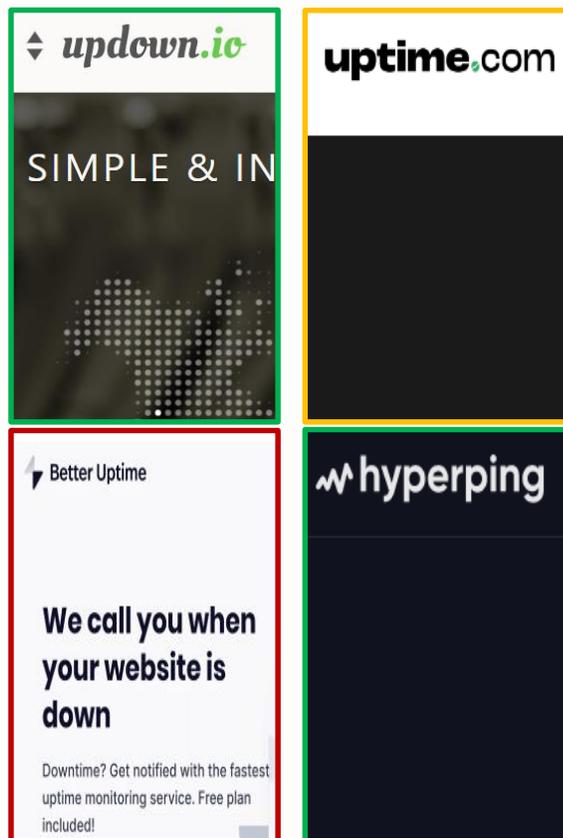
校安通知

檢測首頁



UptimeRobot

50個網站監測



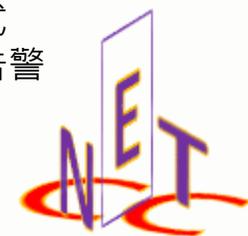
網站監測服務

有付費與免付費

```
[root@166 html]# md5sum 08-16 > h1
[root@166 html]# more h1
56d57306b6d6ef13cb35e1fbf177fcf3 08-16
[root@166 html]# vi 08-16
[root@166 html]# md5sum 08-16 > h2
[root@166 html]# more h2
8a05b1c29cae3eb26ccf8db309d26f1a 08-16
[root@166 html]# diff h1 h2
1c1
< 56d57306b6d6ef13cb35e1fbf177fcf3 08-16
---
> 8a05b1c29cae3eb26ccf8db309d26f1a 08-16
```

簡易還原

定時網站內檢測首頁檔案雜湊函式，或是檔案大小，發現有異，發出告警



資料夾HASH值比對&寄送通知

SourceFolderHash.py

計算資料夾的HASH，HASH值為檔名

```

1 import hashlib,time
2 from pathlib import Path
3
4 #=====計算整個資料夾HASH=====
5 while 10==10:
6     def md5_update_from_file(filename, hash):
7         assert Path(filename).is_file()
8         with open(str(filename), "rb") as f:
9             for chunk in iter(lambda: f.read(4096), b""):
10                hash.update(chunk)
11            return hash
12
13     def md5_file(filename):
14         return md5_update_from_file(filename, hashlib.md5()).hexdigest()
15
16     def md5_update_from_dir(directory, hash):
17         assert Path(directory).is_dir()
18         for path in sorted(Path(directory).itenddir()):
19             hash.update(path.name.encode())
20             if path.is_file():
21                 hash = md5_update_from_file(path, hash)
22             elif path.is_dir():
23                 hash = md5_update_from_dir(path, hash)
24         return hash

```

計算HASH

CheckFileCount.py

計算HASH資料夾裡的檔案數
如果檔案數量有變動，代表HASH值有改變，就發通知

```

1 #算資料夾內的資料夾及檔案總數
2
3 import time,smtplib,os,urllib.request
4 from email.mime.text import MIMEText
5
6 #判斷Source_HASH裡的檔案總數，若不同就發信、發簡訊通知
7 #EMAIL函數
8 def sendmail():
9     msg = MIMEText(Now_Time + " 偵測到資料夾HASH值有異動，請檢查CCNET ", "plain")
10    msg["Subject"] = "Check CCNET"
11    msg["From"] = "寄件人信箱"
12    msg["To"] = "收件人信箱1;收件人信箱2"
13    smtp = smtplib.SMTP("smtp.gmail.com", 587)
14    smtp.ehlo()
15    smtp.starttls()
16    smtp.login("寄件人帳號", "寄件人密碼")
17    smtp.send_message(msg)
18 #簡訊函數
19 def sendSMS(tel):
20     username = "TWSMS帳號"
21     password = "TWSMS密碼"
22     mobile = tel
23     message = "CCNET_HASH_Change!"
24
25     msg = 'username='+username+'&password='+password+'&mobile='+mobile+'&message='+message
26     url = 'http://api.twsms.com/json/sms_send.php?'+msg
27

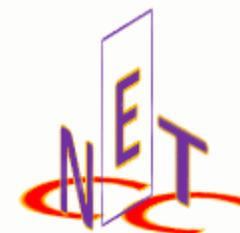
```

寄發郵件、簡訊

<https://youtu.be/gWsS8ZVKXVQ>



郵件、簡訊

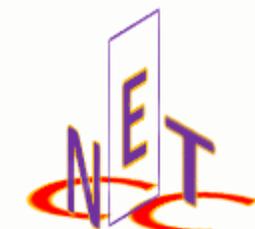


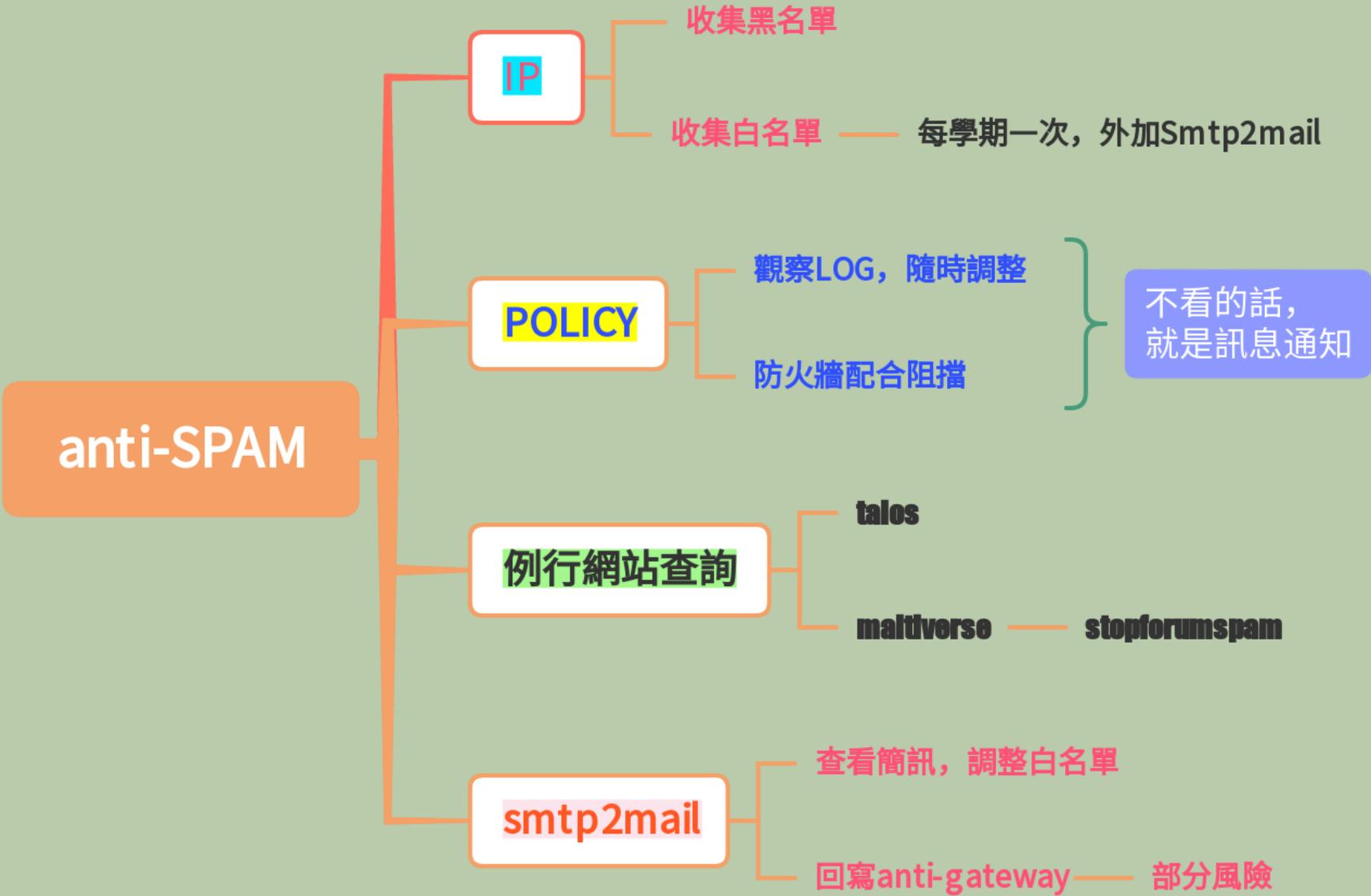
	IP	FLOW'S	OCTETS	PACKETS
1	203.64.3.198	587842	21.66GB	44105437
2	203.64.3.177	296090	56.14MB	417307
3	10.171.0.60	149070	582.99MB	1714216
4	10.171.1.24	123652	576.46MB	2006369
5	10.170.1.77	123301	71.7MB	373958
6	10.170.1.37	121141	9.48GB	14373249
7	10.171.0.126	92141	1.08GB	3894883
8	203.71.172.4	76757	1.64GB	1539748
9	203.64.3.250	57636	1.12GB	2233219
10	10.170.1.157	54067	2.84GB	6568547
11	10.171.1.14	30947	56.22MB	853974
12	10.171.0.147	29963	106.47MB	363903
13	203.71.172.22	29782	6.41MB	76240
14	203.64.7.10	26124	499.48MB	880574
15	10.170.0.218	22434	385.76MB	610241
16	10.170.0.112	21806	2.04GB	4073044
17	203.64.3.251	21669	1.71GB	1416198
18	203.64.3.230	20676	395.21MB	2521847
19	10.171.0.209	19080	1.37GB	5659440
20	203.71.172.209	18949	1.81GB	1529416
21	10.171.0.81	16397	339.72MB	3118173
22	10.170.0.16	16106	0.78 GB	3373603

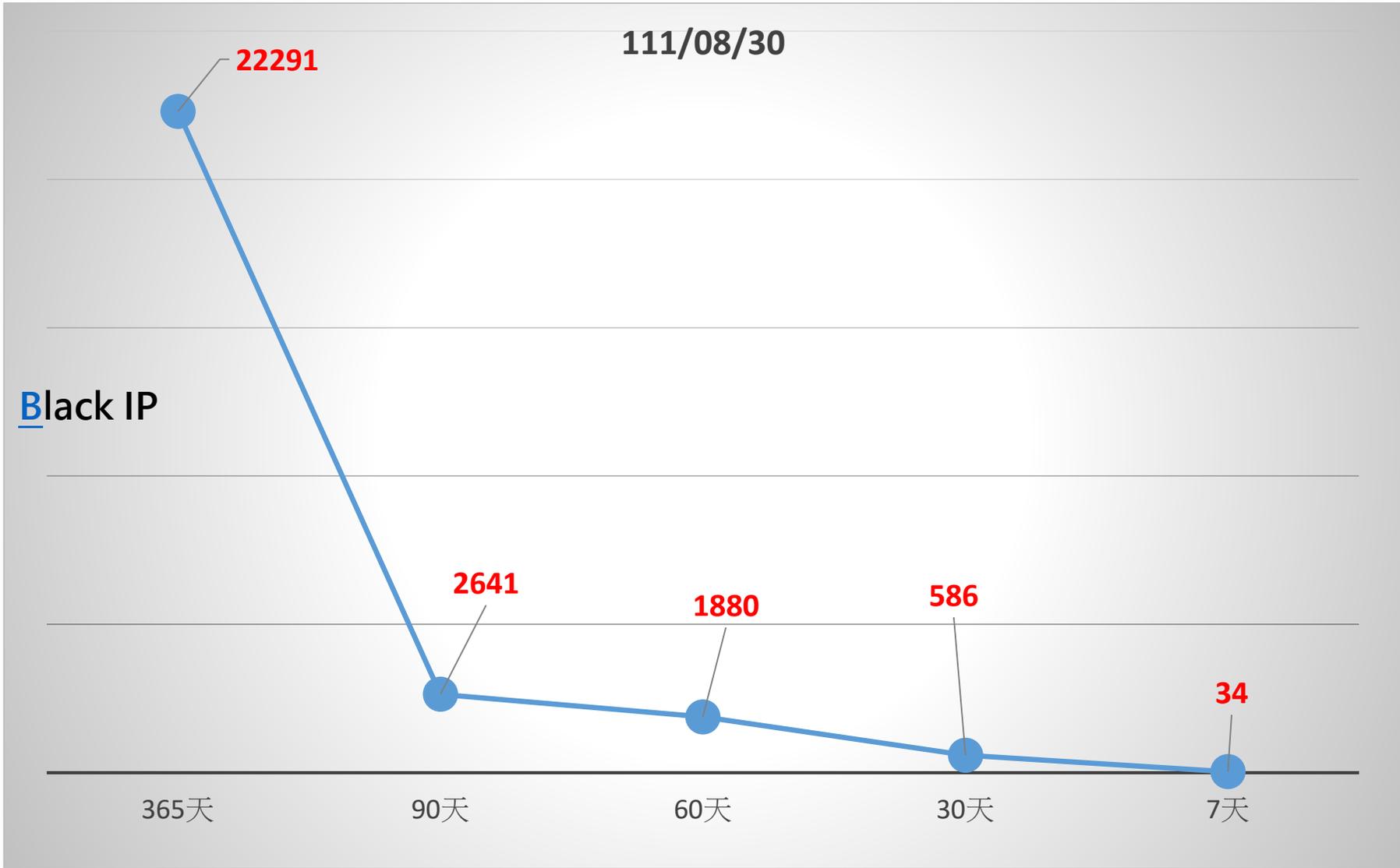


主辦單位：教育部 Ministry of Education

承辦單位：國立台灣科技大學







◆ BLOCK(BLACK) LIST名單



◆ 有效的白名單



◆ 高強度密碼規則



防火牆

防火牆建議:

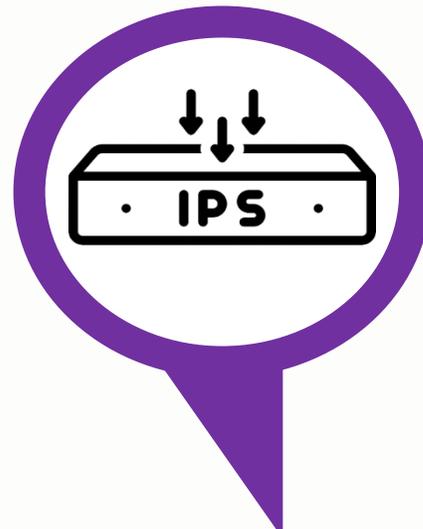
- ◆ 可以適度地打開防護DoS功能阻擋TCP、UDP掃描，收集IP
- ◆ 也可以觀察內對外已遭入侵主機異常行為(相對應功能)



黑白名單

黑白名單建議:

- ◆ 各種黑白名單收集強化過濾功能，阻擋進入校內
- ◆ 需要定時的更新與蒐集有效的黑白名單



入侵防護

IPS建議:

- ◆ 可以觀察分析地區國別分類，用以因應網路攻擊
- ◆ 需要定時的更新與蒐集有效的黑白名單



合作

合作建議:

- ◆ LINE平台，是否可供上傳黑名單供各校參考
- ◆ 當然上級機關的支援也很重要

● Q&A

