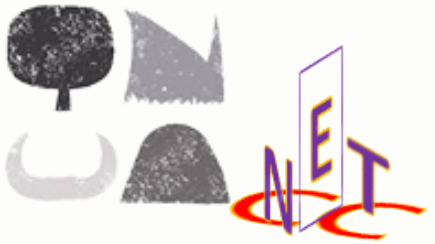
TNUA

疫情期間

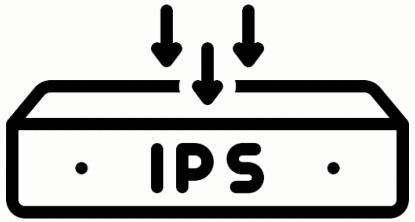
居家辦公VPN 自動化管理
&
電子郵件攻防~實例探討

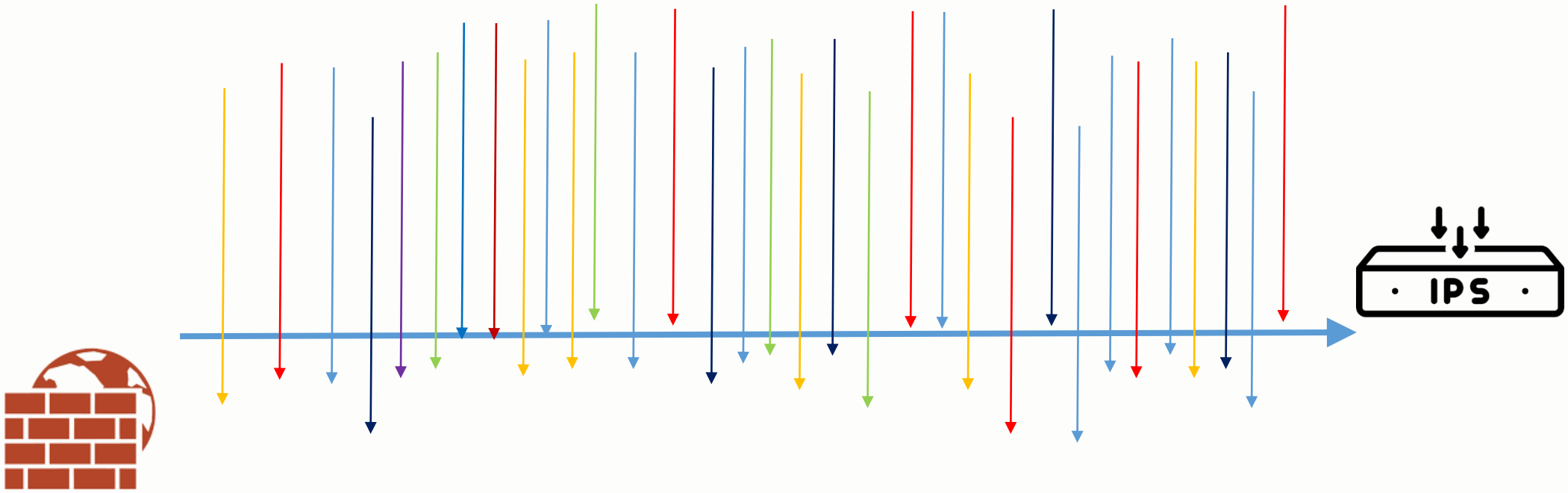
分享人:  許煒城

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

■ 盤點現有設備

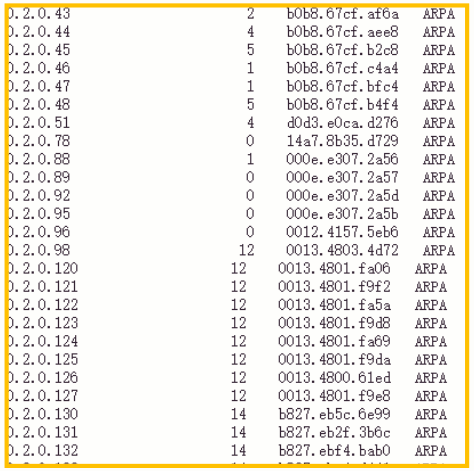




收集IP

教學網頁

ARP TABLE

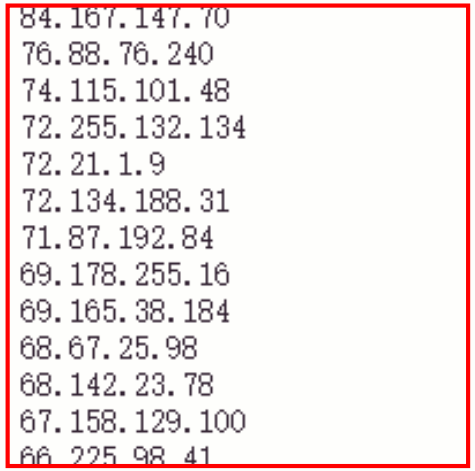


0.2.0.43	2	b0b8.67cf.af6a	ARPA
0.2.0.44	4	b0b8.67cf.aee8	ARPA
0.2.0.45	5	b0b8.67cf.b2c8	ARPA
0.2.0.46	1	b0b8.67cf.c4a4	ARPA
0.2.0.47	1	b0b8.67cf.bfc4	ARPA
0.2.0.48	5	b0b8.67cf.b4f4	ARPA
0.2.0.51	4	d0d3.e0ca.d276	ARPA
0.2.0.78	0	14a7.8b35.d729	ARPA
0.2.0.88	1	000e.e307.2a56	ARPA
0.2.0.89	0	000e.e307.2a57	ARPA
0.2.0.92	0	000e.e307.2a5d	ARPA
0.2.0.95	0	000e.e307.2a5b	ARPA
0.2.0.96	0	0012.4157.5eb6	ARPA
0.2.0.98	12	0013.4803.4d72	ARPA
0.2.0.120	12	0013.4801.fa06	ARPA
0.2.0.121	12	0013.4801.f9f2	ARPA
0.2.0.122	12	0013.4801.fa5a	ARPA
0.2.0.123	12	0013.4801.f9d8	ARPA
0.2.0.124	12	0013.4801.fa69	ARPA
0.2.0.125	12	0013.4801.f9da	ARPA
0.2.0.126	12	0013.4800.61ed	ARPA
0.2.0.127	12	0013.4801.f9e8	ARPA
0.2.0.130	14	b827.eb5c.6e99	ARPA
0.2.0.131	14	b827.eb2f.3b6c	ARPA
0.2.0.132	14	b827.ebf4.bab0	ARPA

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
```

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

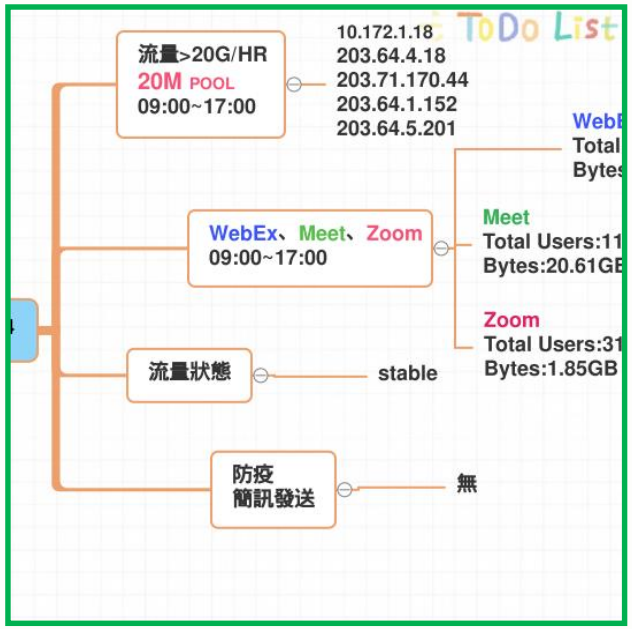
SPAM 國別:
將對應國別以 ip2c 查詢後留存

SPAM IP:
將SPAM IP 寫入資料庫以利統計

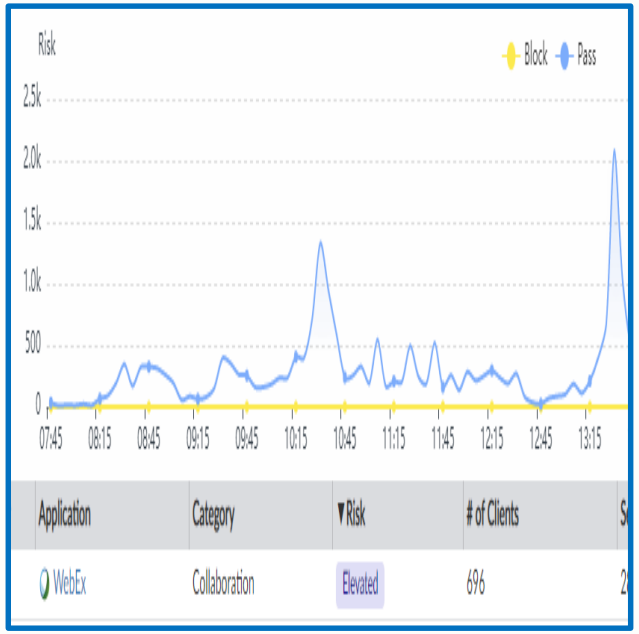
■ 資料庫透過Except界接Firewall

VPN 自動開關(校內)

防疫日誌



視訊流量



VPN關、開

依據人事差勤系統，申請
居家班公者
08:00~19:00

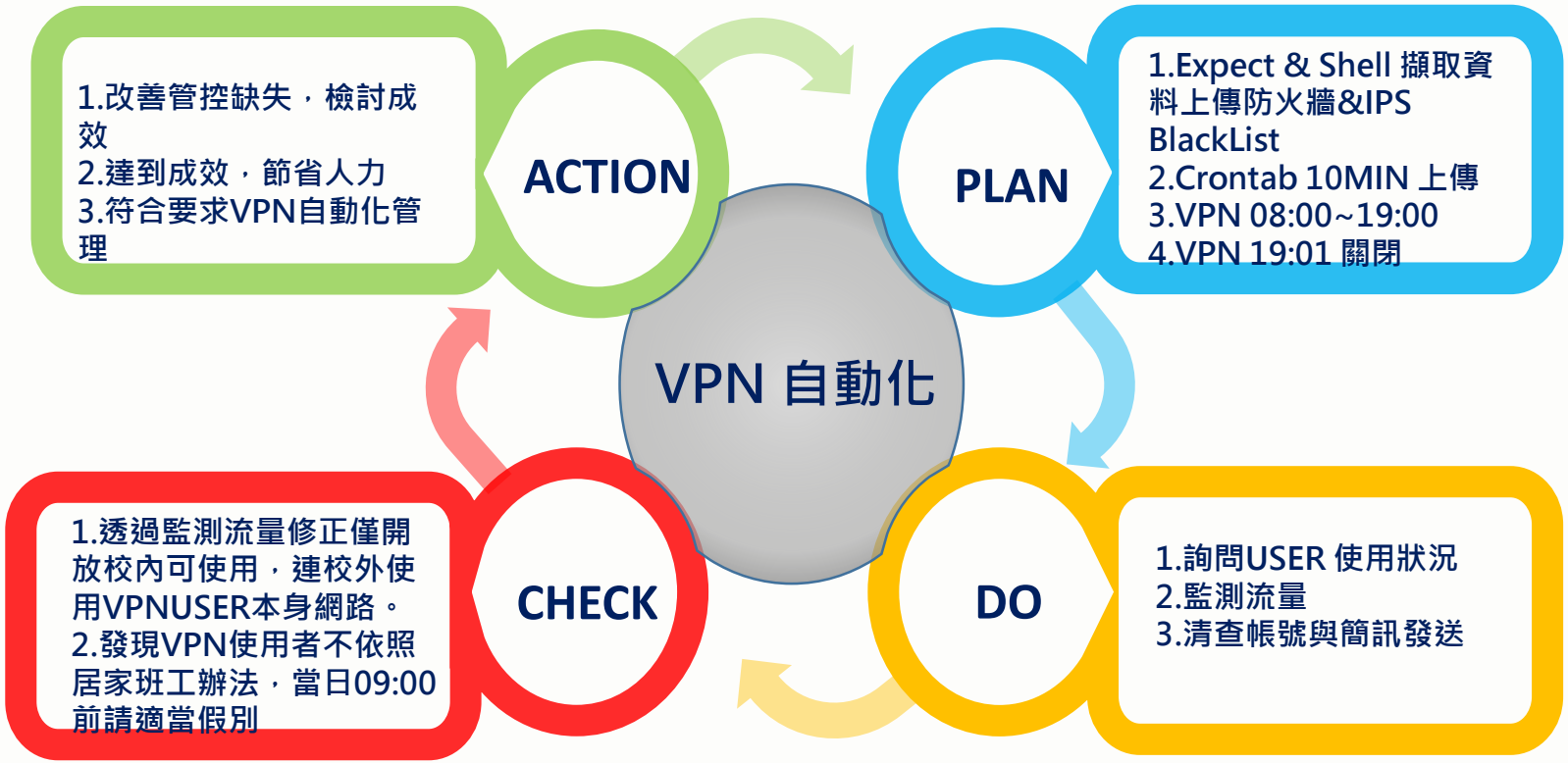
防疫日誌

WebEx 維運
依照流量管制辦法，設
定QoS 管控，以利教學

視訊流量

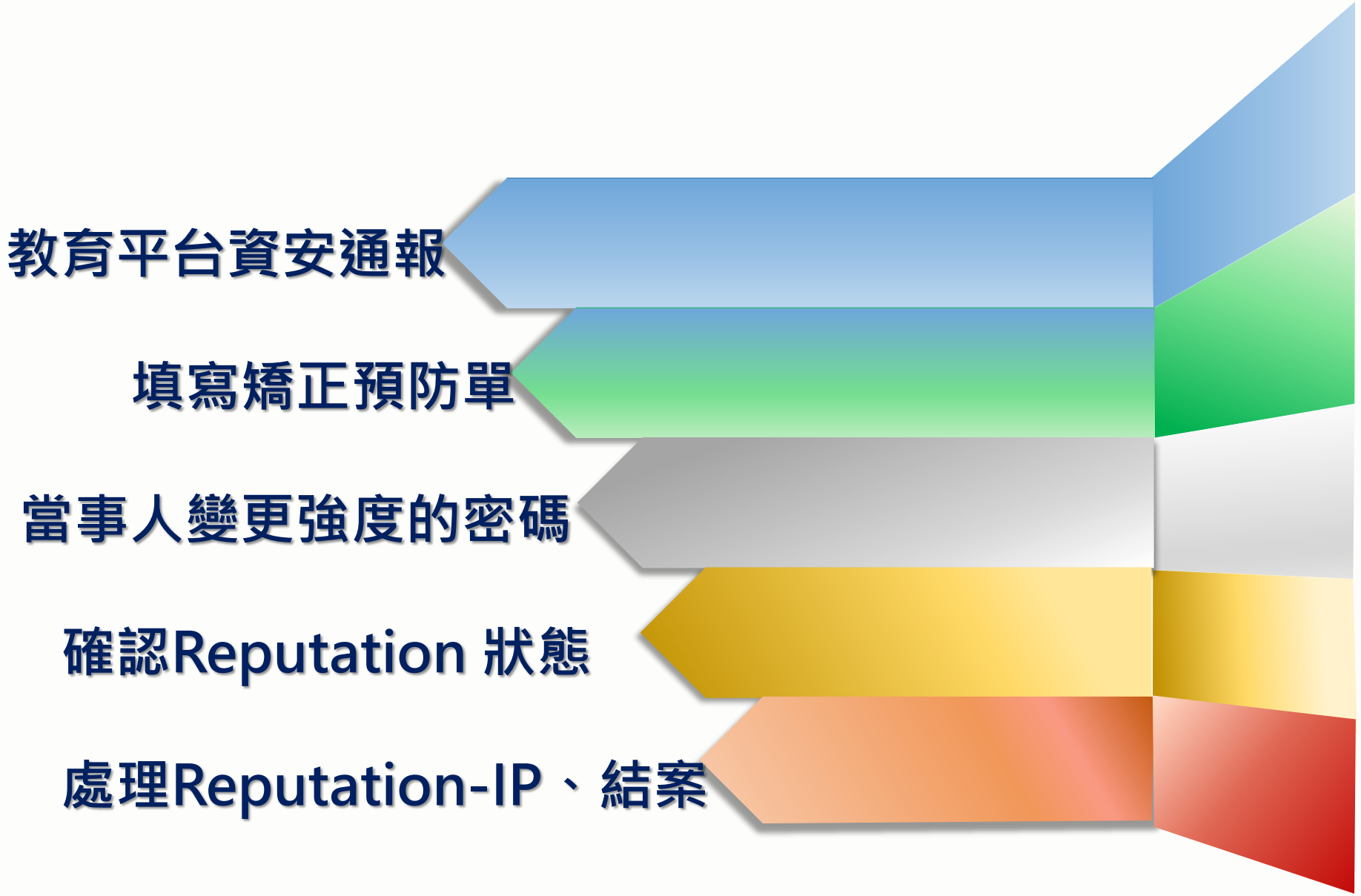
WebEx 維運
做為日後頻寬升級佐證

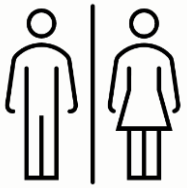
疫情期間居家辦公VPN自動化管理



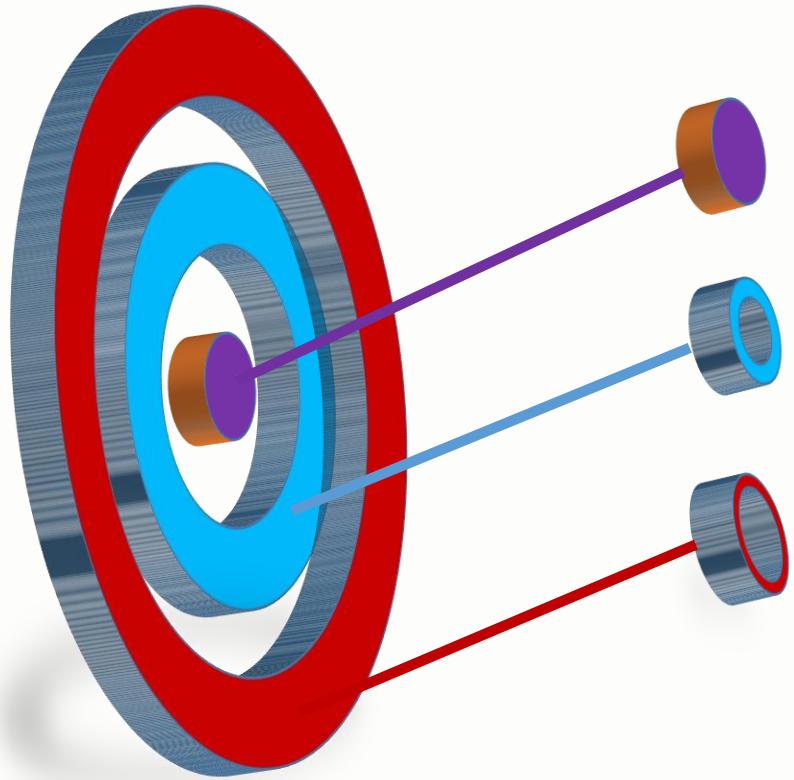
109年總共被猜中12次密碼

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




1.網路組能開發相關網管程式、安裝相關套件，加強網路管理
2.對於網路設備熟捻，可加強整合效能
S
W
T
O
無經費購置相關設備或是訂閱制的資料庫比對、防護
1.新型態網路攻擊，以加密方式規避防火牆相關設備解析，需設備支援
2.資安法要求人員、經費超過學校預期支付能力
1.因為程式開發過程，強化系統、網路程式經驗
2.孰悉Anitgateway防護



核心程式選擇(對現有設備)

RBL VS DNSBL

不想再填寫矯正預防單了


VISION
變成罐頭
MISSION
知彼知己
百戰不殆
、
知天知地
勝乃可全
STRATEGY
黑名單
、
白名單
、
smtp2sms
GOAL
SPAM 搬家

即時黑名單(RBL)

由第三方的反垃圾郵件組織提供檢查垃圾郵件發送者IP地址的服務

MAIL 分散式拒絕服務(簡稱DDoS)攻擊

阻斷被攻擊方的正常網路服務

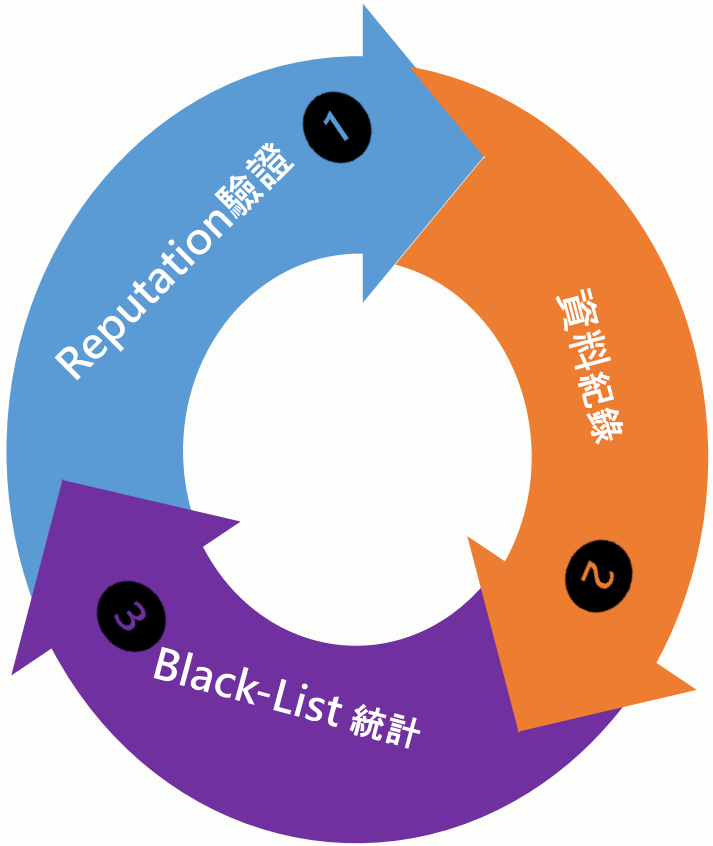
電子郵件目錄收集攻擊(Directory Harvest Attack，簡稱DHA)

字典猜測攻擊來嘗試登入

網域名稱系統攔截清單，簡稱 DNSBL)

cbl.abuseat.org
sbl.spamhaus.org
bl.spamcop.net
zen.spamhaus.org

DNS 封鎖清單 (DNSBL) 伺服器的清單



Reputation驗證

1. https://talosintelligence.com/
2. https://maltiverse.com/
3. https://stopforumspm.com

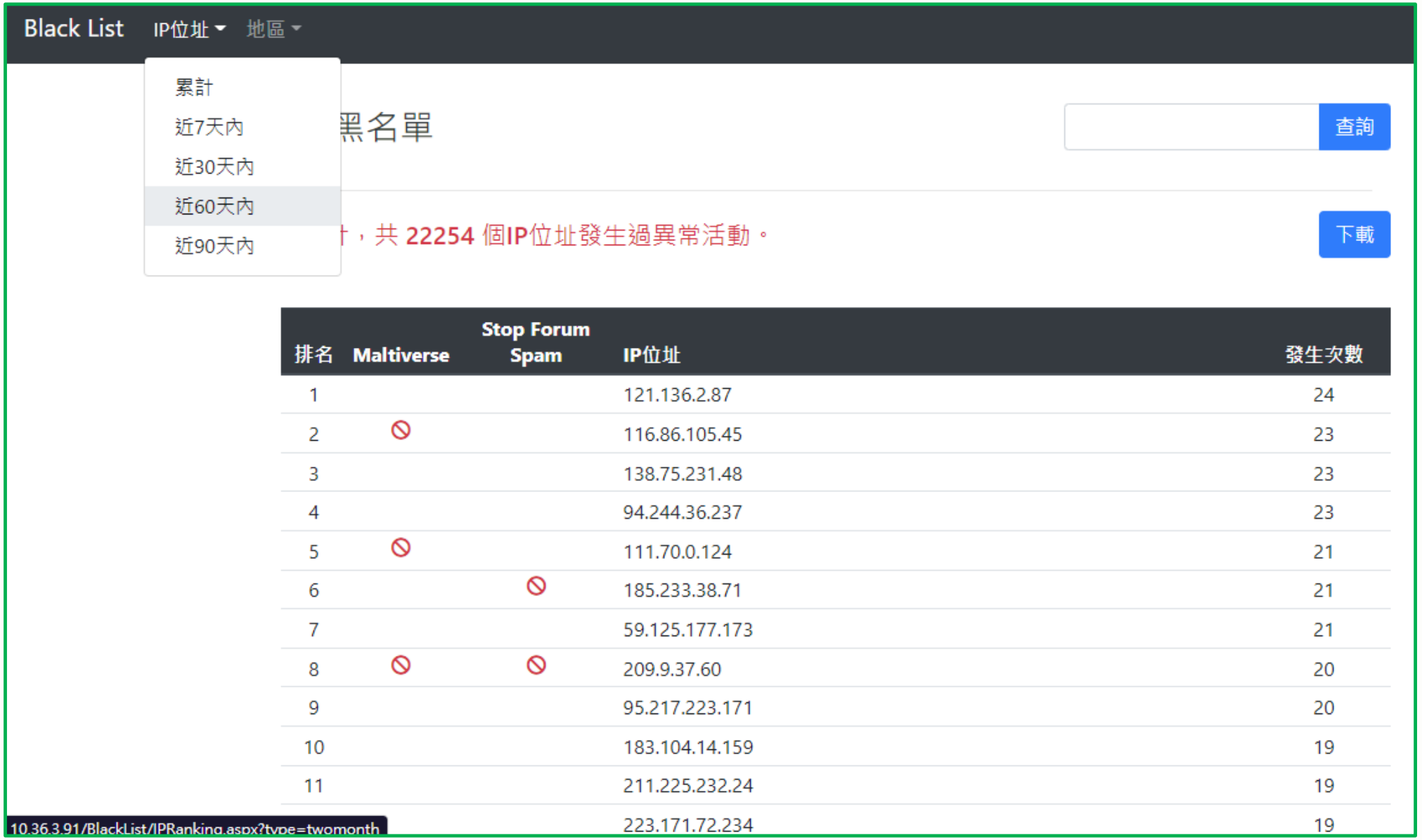
資料紀錄

2. 國別
3. IP

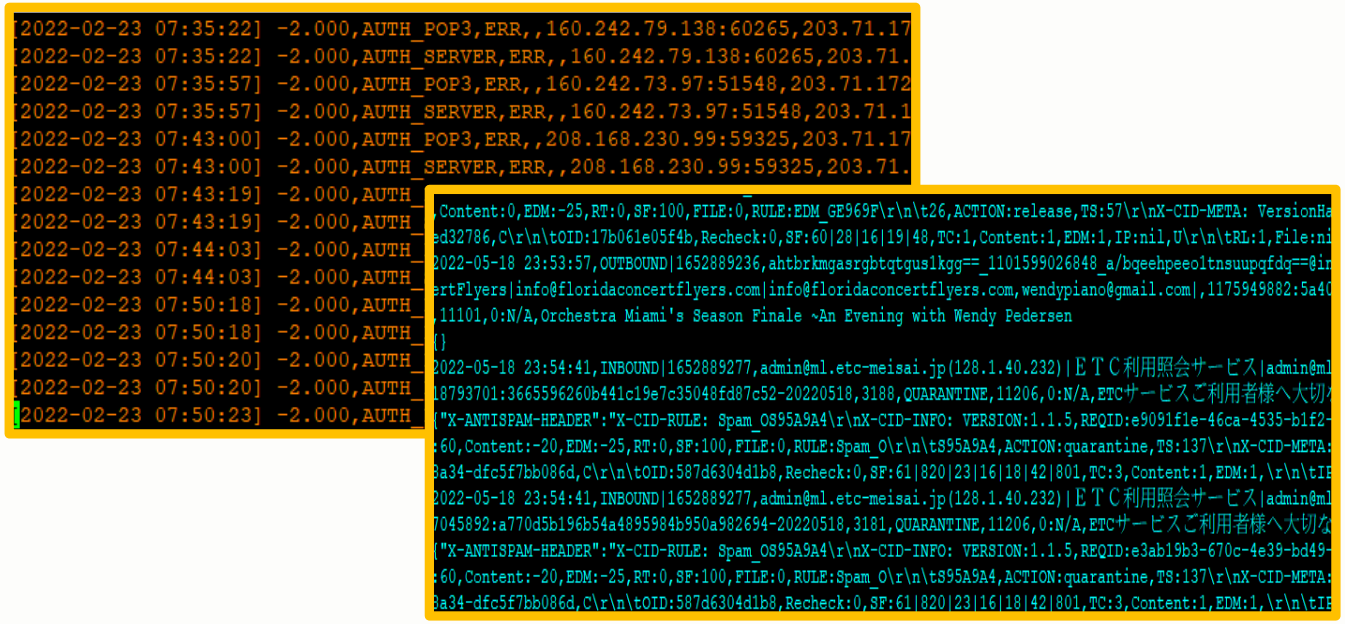
Black-List 統計

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

- Black-List 統計

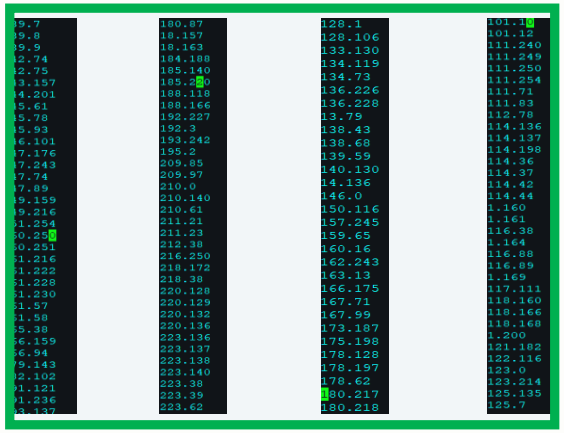


Email黑名單、白名單收集



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



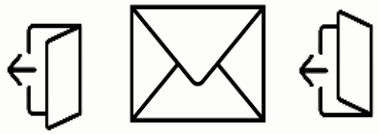
白名單的收集

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	59-115-238-135.dynamic-ip.hinet.net	0.0	0.8	1	Poor
59.115.238.53	59-115-238-53.dynamic-ip.hinet.net	59-115-238-53.dynamic-ip.hinet.net	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

Gmail

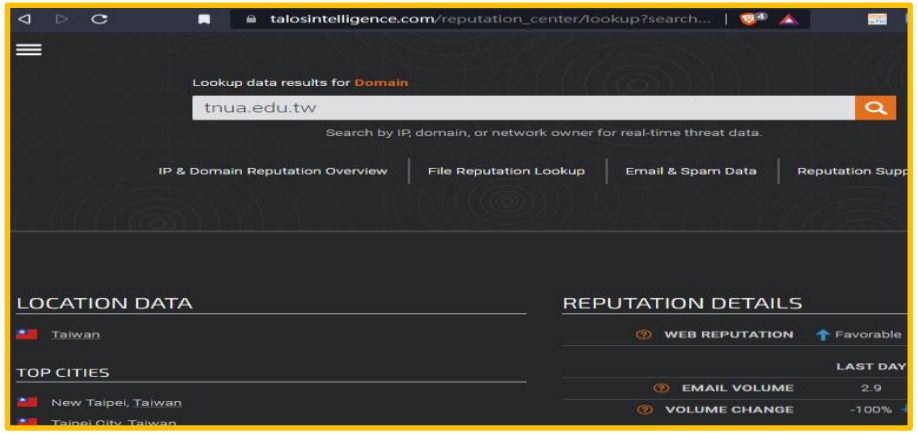
209.85.0.0/16

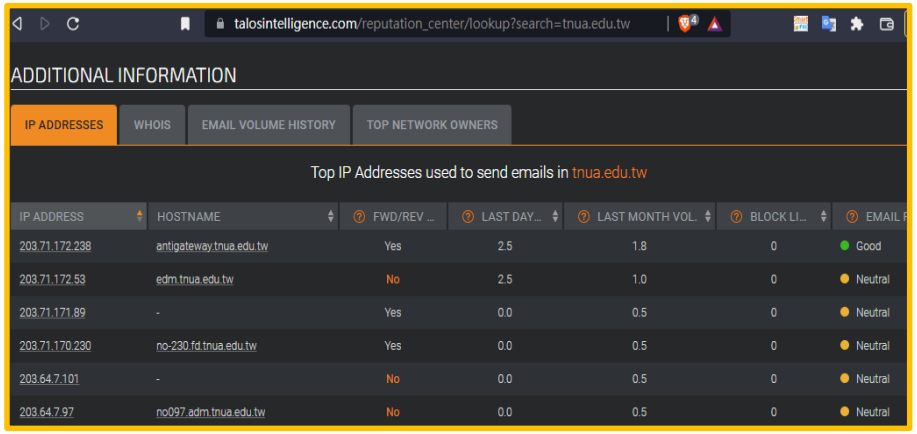
- https://talosintelligence.com
- https://maltiverse.com
- https://www.stopforumspam.com
- https://mxtoolbox.com/SuperTool.aspx
- https://www.blocklist.de

常用網站

查詢Reputation、
Mail 相關

Email Reputation 檢查



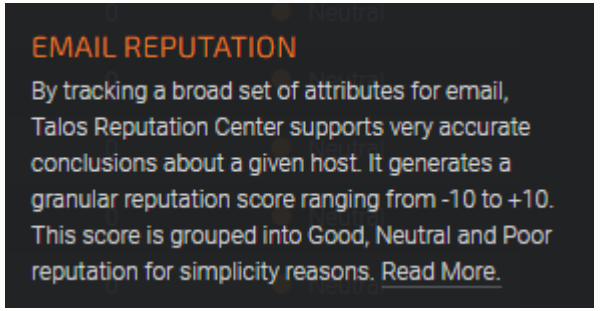


sendbase.com

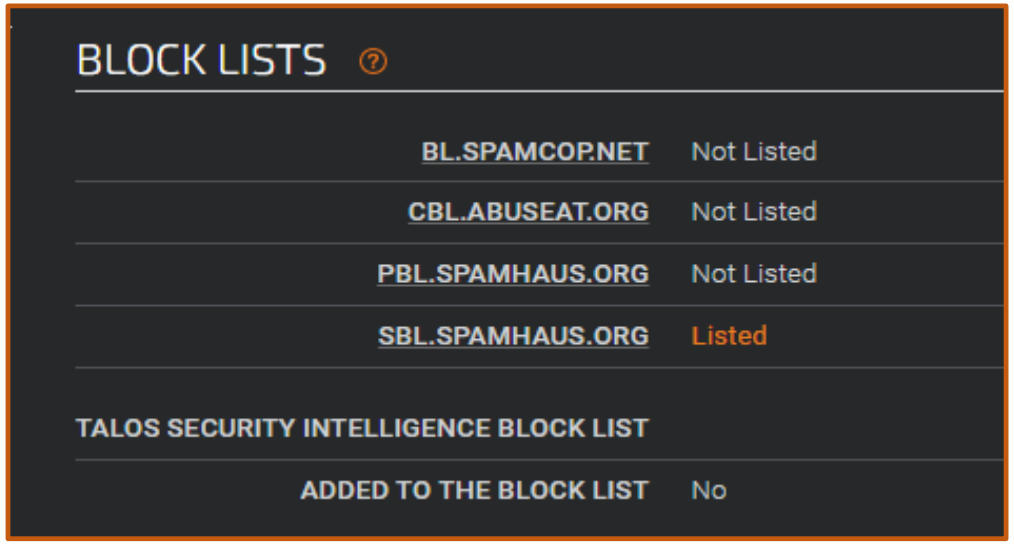
可以查詢MX相關資訊，
也有暴露網路資訊的疑慮

Reputation

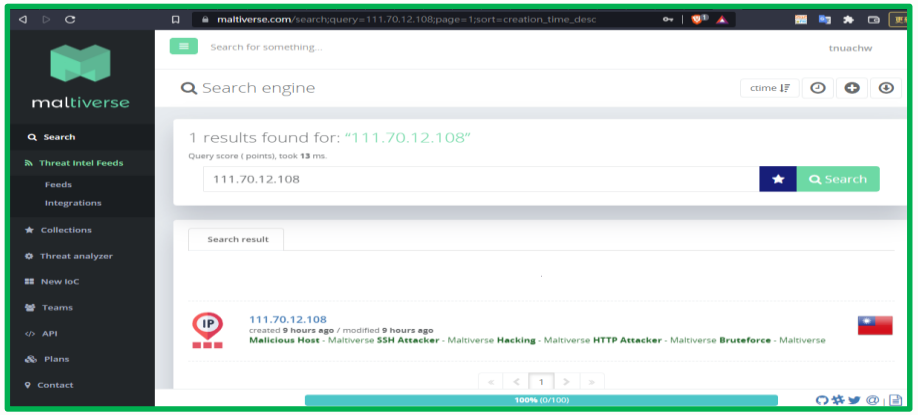
判斷Good、
Neutral、Poor



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...	gdcmjs@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...	zfrafpzii@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

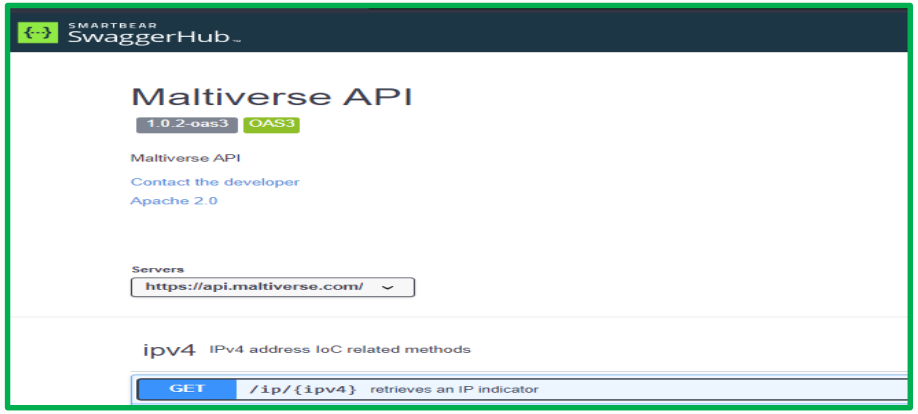


Email Reputation 檢查



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

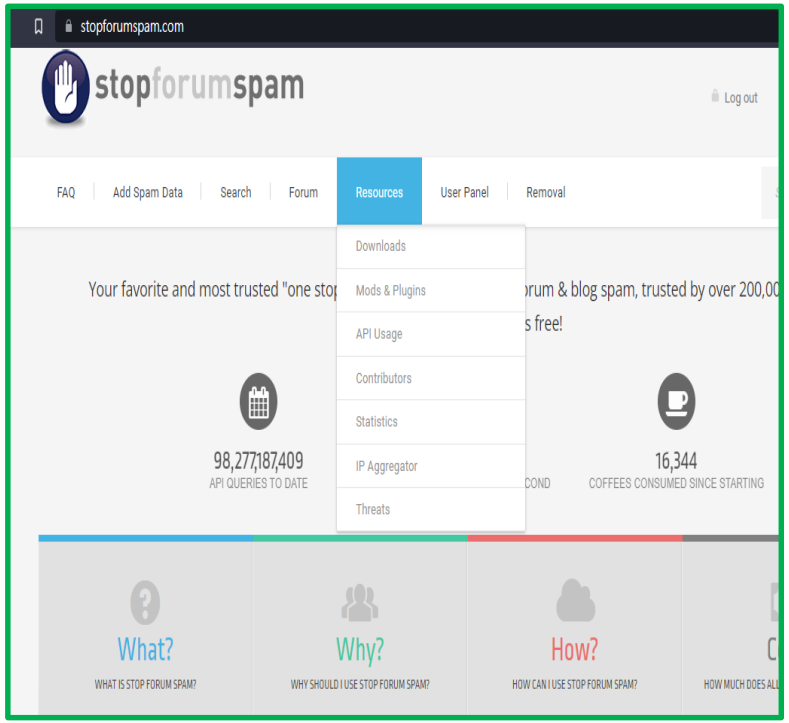
IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
1.215.191.210	-	No	0.0	1.2	2	Poor

0 results found for: "1.215.191.210"

Query score (points), took **9** ms.

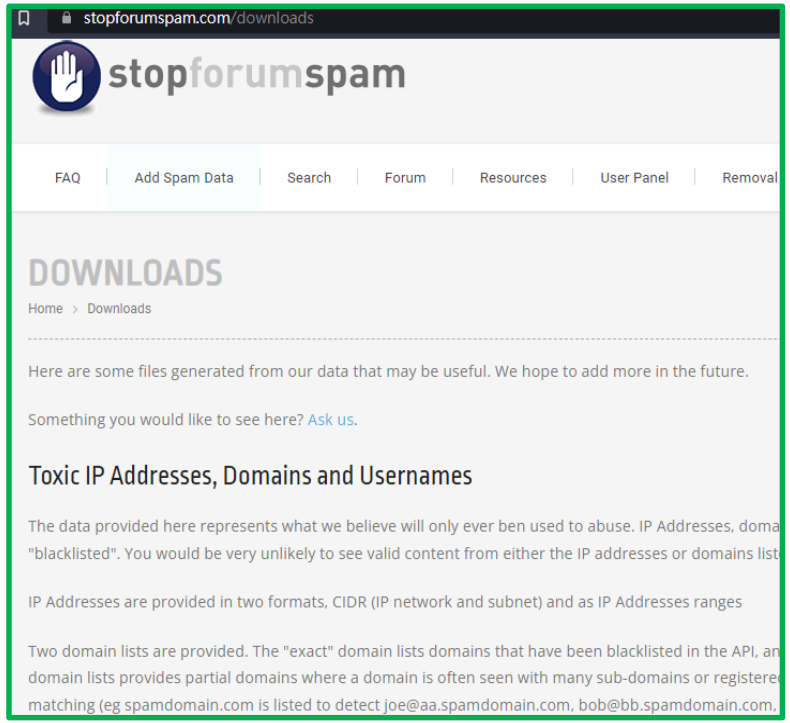
1.215.191.210 ★ Search

Email Reputation 檢查



Stopforumspam

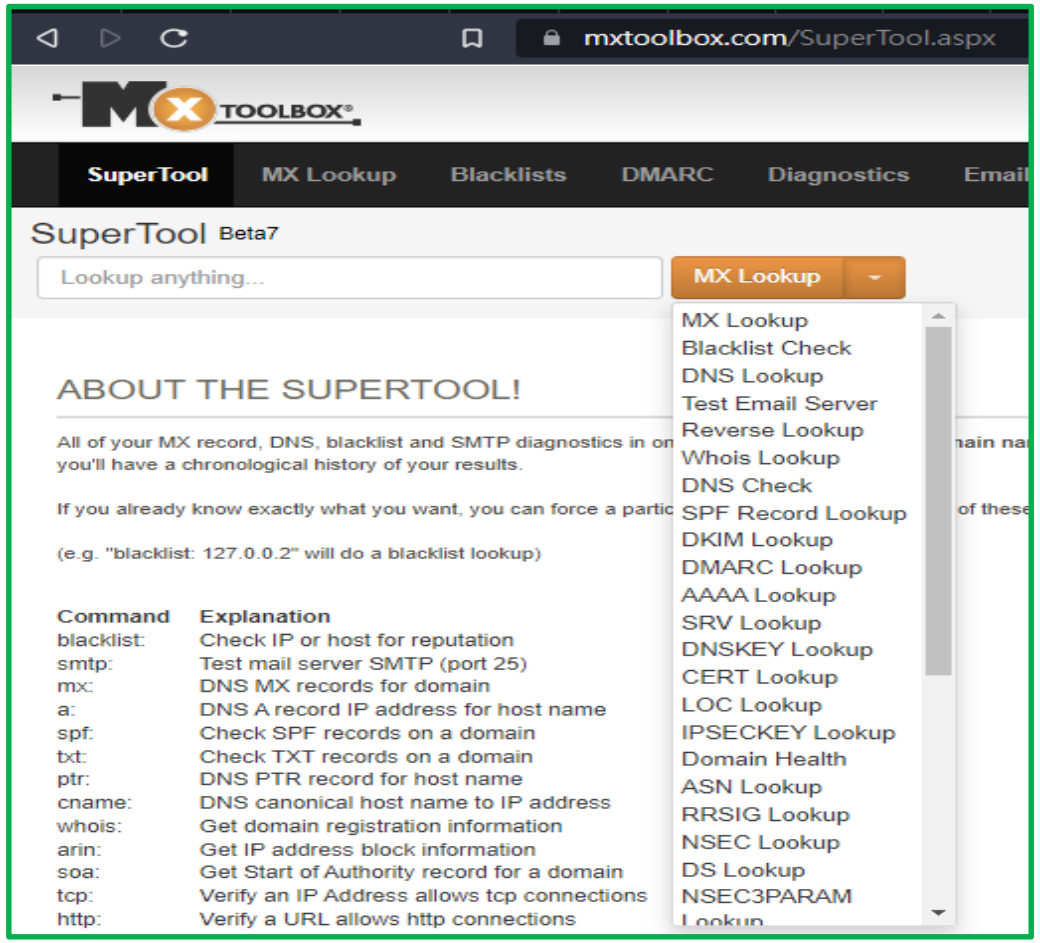
有API 查詢



stopforumspam

Toxic ip 下載

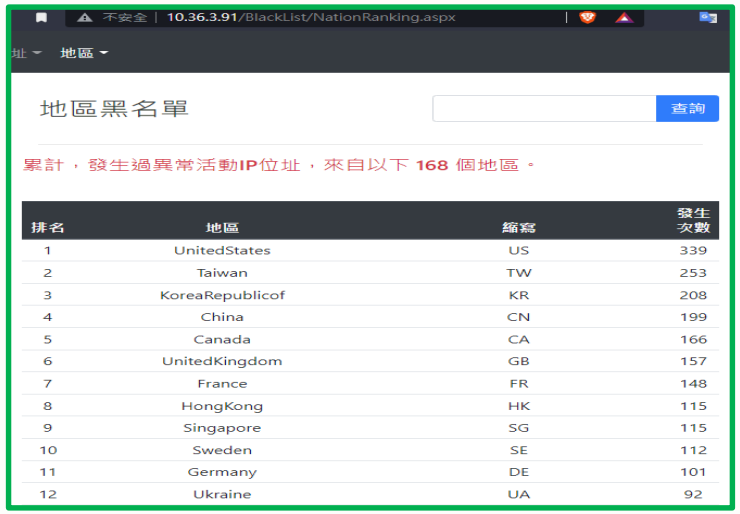
Email Reputation 檢查



[mxtoolbox]

各式Mail Debug

■ Email黑名單、白名單收集



地區的收集

有利於判斷與上傳防火牆，
作為阻擋的依據

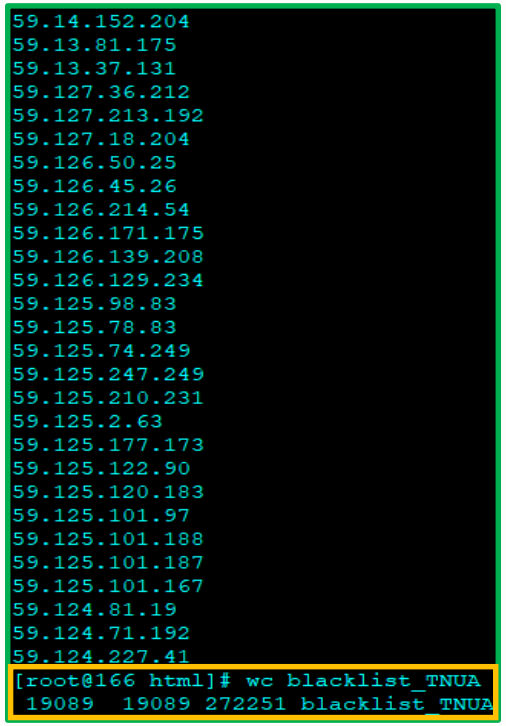
黑名單的收集

有利於判斷與上傳防火牆，
作為阻擋的依據

■ Expect 黑名單上傳 IPS&Firewall

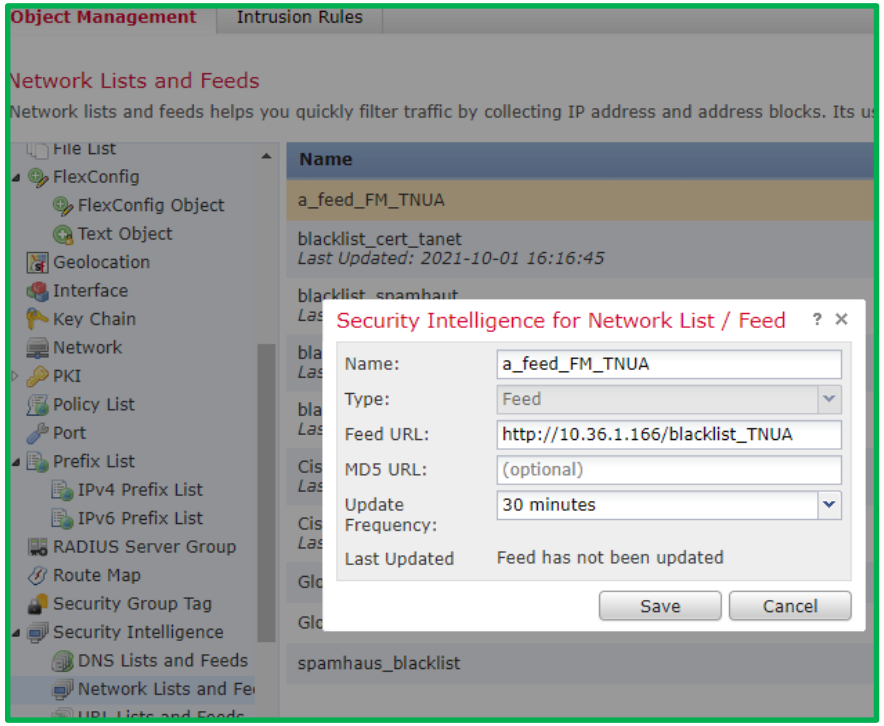
Expect是Unix系統中用來進行自動化控制和測試的軟體工具，由Don Libes製作，作為Tcl腳本語言的一個擴展，應用在交互式軟體中如telnet，ftp，Passwd，fsck，rlogin，tip，ssh等等。該工具利用Unix偽終端包裝其子進程，允許任意程序通過終端接入進行自動化控制；也可利用Tk工具，將交互程序包裝在X11的圖形用戶界面中。

Expect 黑名單上傳 IPS&Firewall



IP的收集

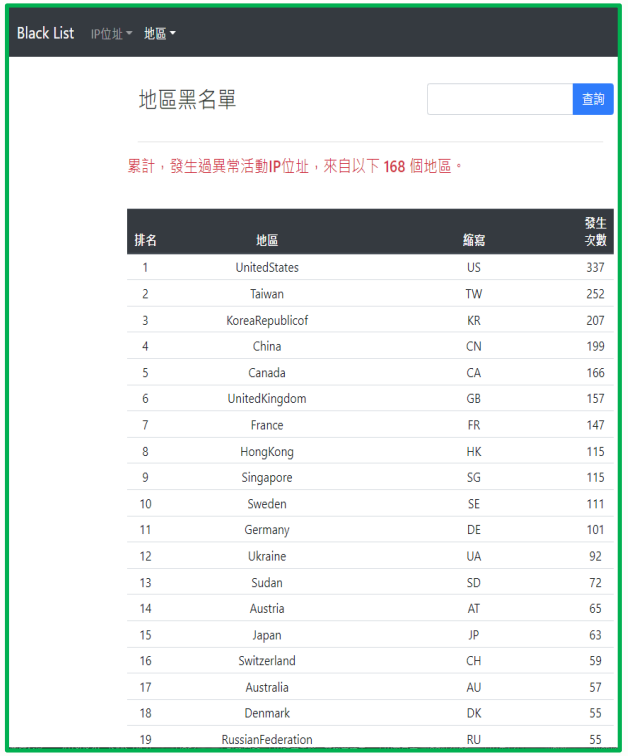
黑名單提供IPS，
作為阻擋的依據



IP的讀取

可以透過 FEED
URL方式

Expect 黑名單上傳 IPS&Firewall



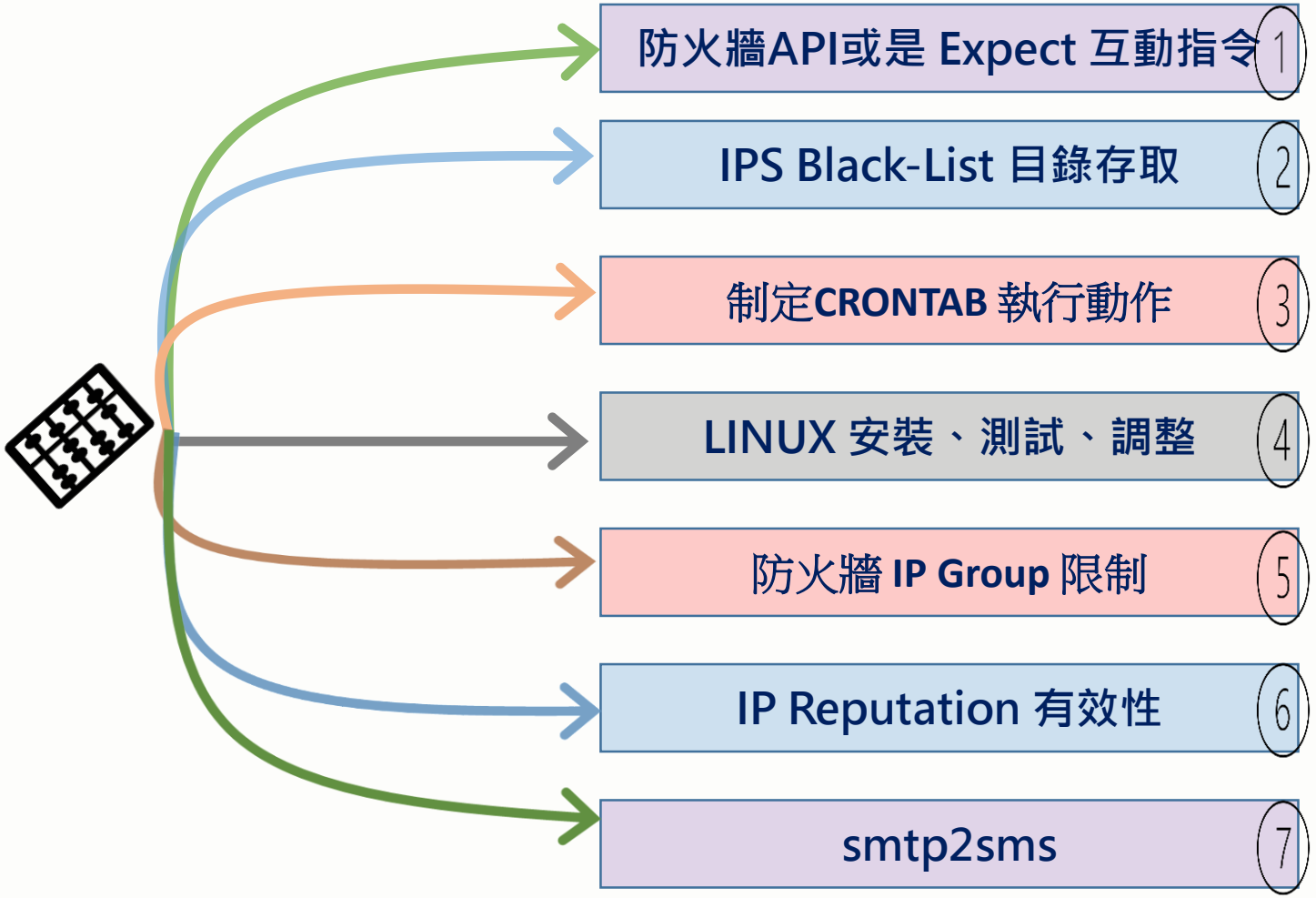
排名	地區	縮寫	發生次數
1	UnitedStates	US	337
2	Taiwan	TW	252
3	KoreaRepublicof	KR	207
4	China	CN	199
5	Canada	CA	166
6	UnitedKingdom	GB	157
7	France	FR	147
8	HongKong	HK	115
9	Singapore	SG	115
10	Sweden	SE	111
11	Germany	DE	101
12	Ukraine	UA	92
13	Sudan	SD	72
14	Austria	AT	65
15	Japan	JP	63
16	Switzerland	CH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


```
[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]#
```

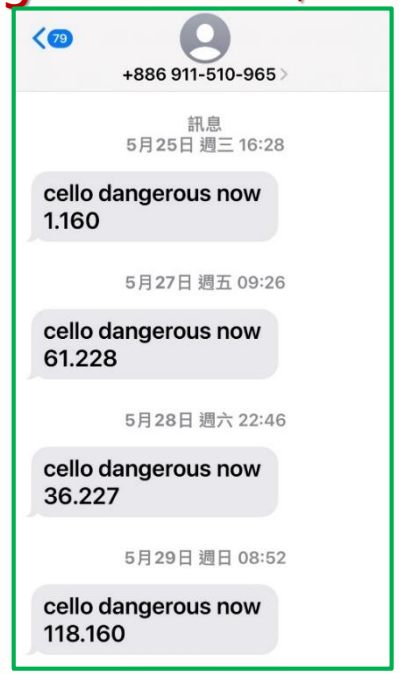
轉換

http://Ip2c.org

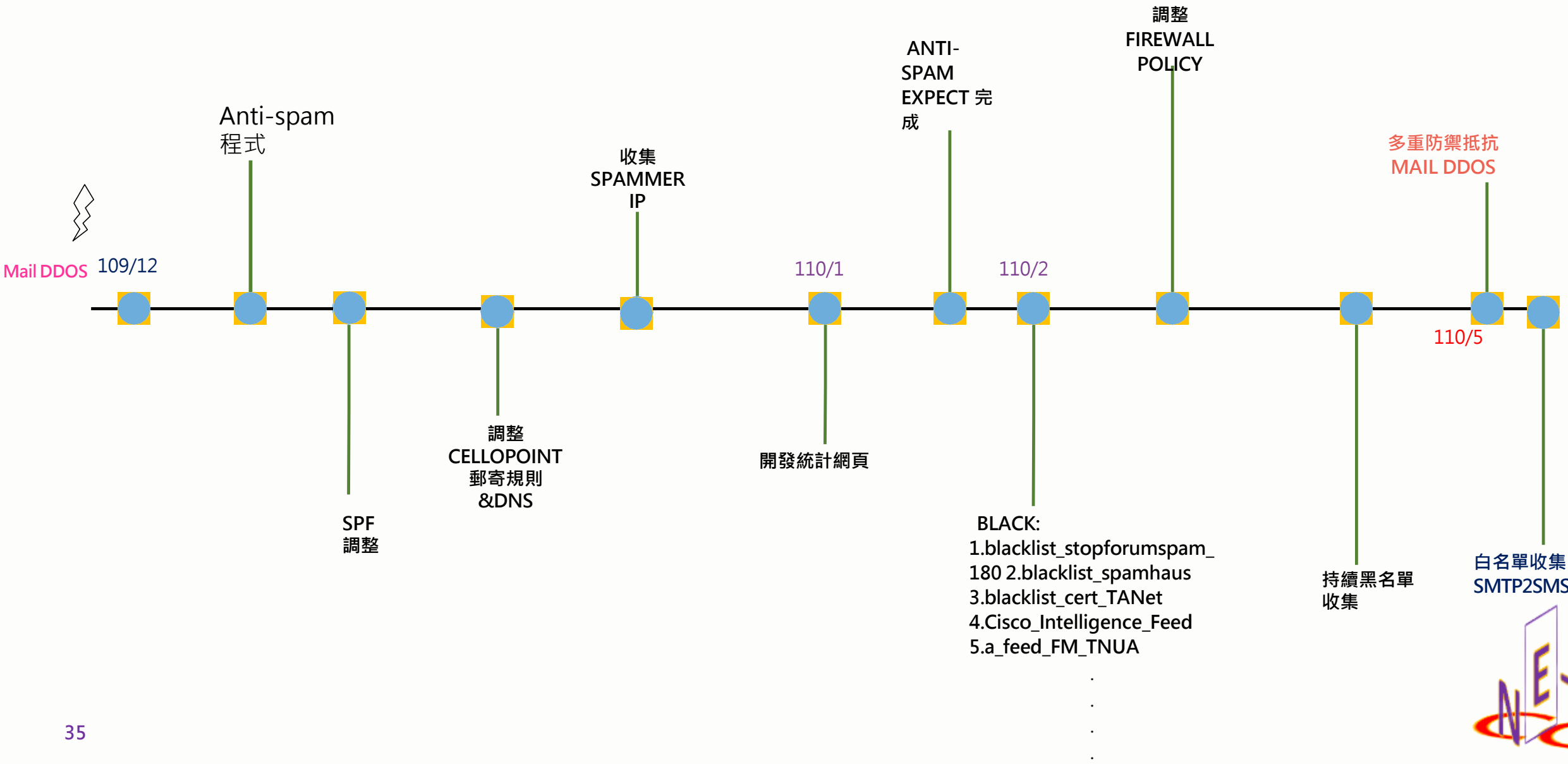
■ Expect 黑名單上傳 IPS&Firewall

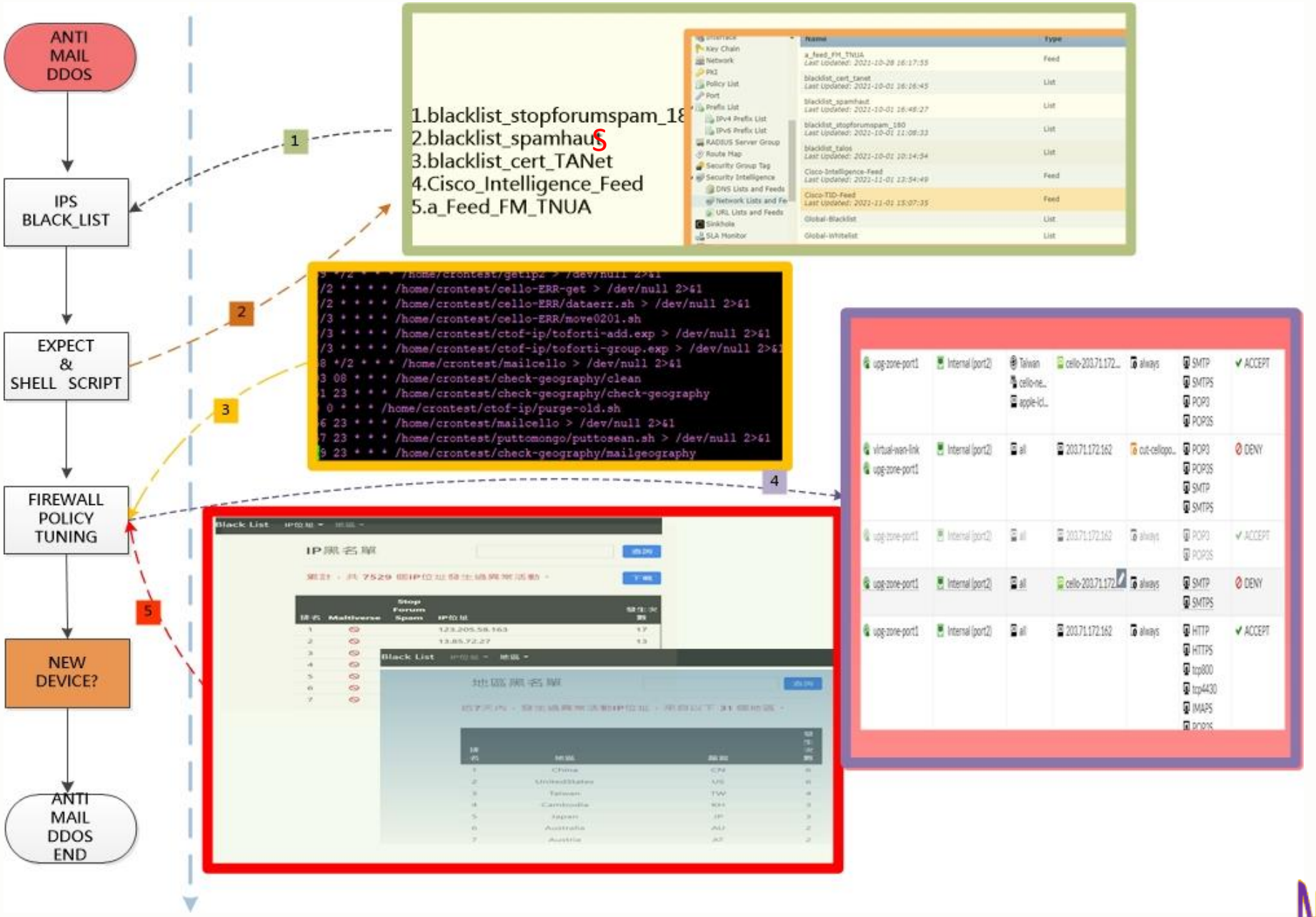


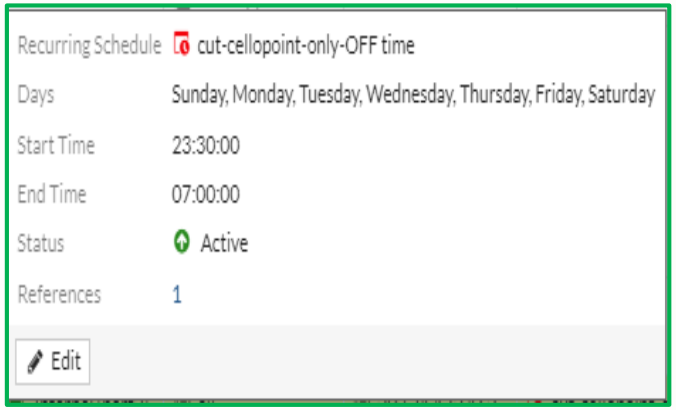
```
[crontest@166 data]$ more smscheck.sh
.
.
while read IP
        do
                $tools/cat -v $home/mail2sms.txt | $tools/mail -s "cello dangerous now $IP"
mail2sms@mail.twsms.com
.
.

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



■電子郵件攻防實戰討論


Anti-spam
程式
收集
SPAMMER
IP
ANTI-
SPAM
EXPECT 完
成
調整
FIREWALL
POLICY
多重防禦抵抗
MAIL DDOS
Mail DDOS
109/12
110/1
110/2
110/5
SPF
調整
調整
CELLOPOINT
郵寄規則
&DNS
開發統計網頁
BLACK:
1.blacklist_stopforumspam_
180 2.blacklist_spamhaus
3.blacklist_cert_TANet
4.Cisco_Intelligence_Feed
5.a_feed_FM_TNUA
持續黑名單
收集
白名單收集
SMTP2SMS


ANTI MAIL DDOS
IPS BLACK_LIST
EXPECT & SHELL SCRIPT
FIREWALL POLICY TUNING
NEW DEVICE?
ANTI MAIL DDOS END
1
2
3
4
5
1.blacklist_stopforumspam_18
2.blacklist_spamhaus
3.blacklist_cert_TANet
4.Cisco_Intelligence_Feed
5.a_Feed_FM_TNUA
/2 * * * * /home/crontest/cello-ERR-get > /dev/null 2>&1
/2 * * * * /home/crontest/cello-ERR/dataerr.sh > /dev/null 2>&1
/3 * * * * /home/crontest/cello-ERR/move0201.sh
/3 * * * * /home/crontest/ctof-ip/toforti-add.exp > /dev/null 2>&1
/3 * * * * /home/crontest/ctof-ip/toforti-group.exp > /dev/null 2>&1
*/2 * * * /home/crontest/mailcello > /dev/null 2>&1
08 * * * /home/crontest/check-geography/clean
23 * * * /home/crontest/check-geography/check-geography
0 * * * /home/crontest/ctof-ip/purge-old.sh
23 * * * /home/crontest/mailcello > /dev/null 2>&1
23 * * * /home/crontest/puttomongo/puttosean.sh > /dev/null 2>&1
23 * * * /home/crontest/check-geography/mailgeography
Black List
IP黑名單

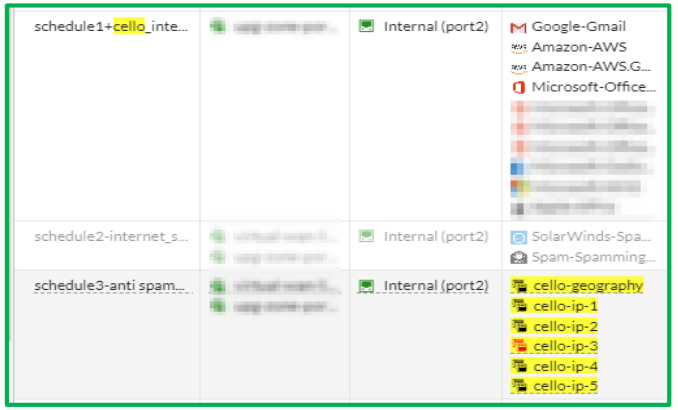


防火牆調整

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 IPS，可以快速阻擋於內網外

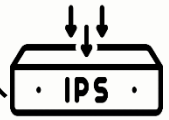
Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	IP Block	96.42.45.206	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	54704 / tcp	465 (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	SDN	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	FRA	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	SDN	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

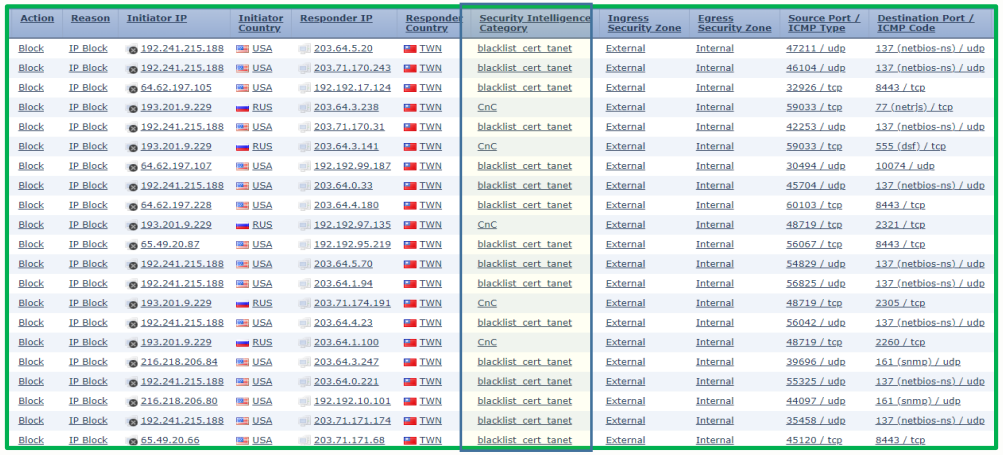
收集的黑名單IP(a_feed_FM_TNUA)匯入 

，亦可阻擋部分攻擊

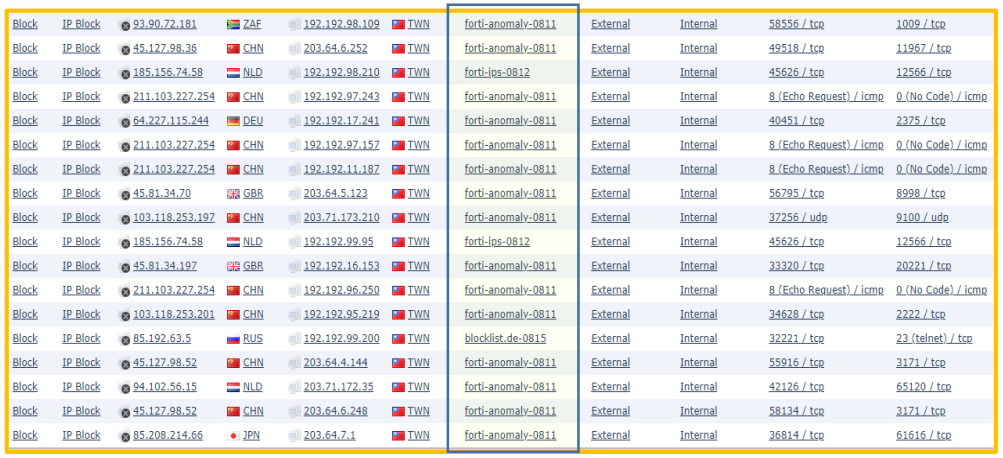
Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
Block	IP Block	66.68.83.241	USA	203.71.174.9	TWN	a_feed_FM_TNUA	External	Internal	7753 / tcp	22 (ssh) / 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	38.146.70.32	USA	203.71.172.238	TWN	a_feed_FM_TNUA	External	Internal	28736 / 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 / udp	137 (netbios-ns) / udp
Block	IP Block	192.241.215.188	USA	203.71.170.243	TWN	blacklist_cert_tanet	External	Internal	46104 / udp	137 (netbios-ns) / udp
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 / udp	137 (netbios-ns) / udp
Block	IP Block	193.201.9.229	RUS	203.64.3.141	TWN	CnC	External	Internal	59033 / tcp	555 (dsf) / tcp
Block	IP Block	64.62.197.107	USA	192.192.99.187	TWN	blacklist_cert_tanet	External	Internal	30494 / udp	10074 / udp
Block	IP Block	192.241.215.188	USA	203.64.0.33	TWN	blacklist_cert_tanet	External	Internal	45704 / udp	137 (netbios-ns) / udp
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 / udp	137 (netbios-ns) / udp
Block	IP Block	192.241.215.188	USA	203.64.1.94	TWN	blacklist_cert_tanet	External	Internal	56825 / udp	137 (netbios-ns) / udp
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 / udp	137 (netbios-ns) / udp
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	39696 / udp	161 (snmp) / udp
Block	IP Block	192.241.215.188	USA	203.64.0.221	TWN	blacklist_cert_tanet	External	Internal	55325 / udp	137 (netbios-ns) / udp
Block	IP Block	216.218.206.80	USA	192.192.10.101	TWN	blacklist_cert_tanet	External	Internal	44097 / udp	161 (snmp) / udp
Block	IP Block	192.241.215.188	USA	203.71.171.174	TWN	blacklist_cert_tanet	External	Internal	35458 / udp	137 (netbios-ns) / udp
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-ips-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	203.64.5.123	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 / udp	9100 / udp
Block	IP Block	185.156.74.58	NLD	192.192.99.95	TWN	forti-ips-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	192.192.96.250	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	blocklist.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 / udp	3283 / udp
Block	IP Block	146.88.240.248	USA	203.64.7.82	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	192.192.96.52	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	192.192.20.198	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	192.192.16.69	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	192.192.99.165	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.71.170.93	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.71.171.140	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.71.172.115	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.64.6.204	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	185.196.220.70	DEU	192.192.97.94	TWN	cert_from_NTU_0810	External	Internal	52704 / udp	3283 / udp
Block	IP Block	185.196.220.70	DEU	192.192.98.2	TWN	cert_from_NTU_0810	External	Internal	47891 / udp	3283 / udp
Block	IP Block	146.88.240.248	USA	203.71.170.194	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.64.6.220	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.64.7.76	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.64.4.55	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	146.88.240.248	USA	203.64.6.156	TWN	cert_from_NTU_0810	External	Internal	1701 / udp	1701 / udp
Block	IP Block	185.196.220.70	DEU	203.64.7.78	TWN	cert_from_NTU_0810	External	Internal	55650 / udp	3283 / udp

Block	IP Block	68.183.188.159	SGP	192.192.95.36	TWN	blocklist.de-0815	External	Internal	42442 / tcp	509
Block	IP Block	142.93.112.39	USA	192.192.95.199	TWN	blocklist.de-0815	External	Internal	45781 / tcp	372
Block	IP Block	206.189.198.55	USA	203.64.3.220	TWN	blocklist.de-0815	External	Internal	49673 / tcp	141
Block	IP Block	183.107.205.177	KOR	203.71.173.68	TWN	blocklist.de-0815	External	Internal	50300 / tcp	22
Block	IP Block	177.184.133.130	BRA	192.192.17.188	TWN	blocklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	164.90.194.36	NLD	203.64.0.43	TWN	blocklist.de-0815	External	Internal	54681 / tcp	323
Block	IP Block	177.184.133.130	BRA	192.192.17.82	TWN	blocklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	177.184.133.130	BRA	192.192.16.244	TWN	blocklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	45.61.188.170	USA	203.64.2.221	TWN	blocklist.de-0815	External	Internal	38815 / tcp	22
Block	IP Block	134.209.150.200	IND	203.64.0.203	TWN	blocklist.de-0815	External	Internal	47201 / tcp	258
Block	IP Block	45.61.188.170	USA	192.192.96.210	TWN	blocklist.de-0815	External	Internal	41614 / tcp	22
Block	IP Block	163.123.143.78	USA	203.64.1.90	TWN	blocklist.de-0815	External	Internal	44586 / tcp	111
Block	IP Block	42.201.63.247	CHN	192.192.10.199	TWN	blocklist.de-0815	External	Internal	55930 / tcp	22
Block	IP Block	141.98.11.92	LTU	203.71.170.218	TWN	blocklist.de-0815	External	Internal	45585 / tcp	80
Block	IP Block	177.184.133.130	BRA	203.64.6.153	TWN	blocklist.de-0815	External	Internal	51801 / tcp	235
Block	IP Block	163.123.143.78	USA	192.192.20.111	TWN	blocklist.de-0815	External	Internal	34970 / tcp	111
Block	IP Block	163.123.143.78	USA	203.64.0.206	TWN	blocklist.de-0815	External	Internal	60005 / tcp	111
Block	IP Block	116.7.245.26	CHN	203.64.1.219	TWN	blocklist.de-0815	External	Internal	56863 / tcp	22
Block	IP Block	159.89.205.91	SGP	192.192.17.34	TWN	blocklist.de-0815	External	Internal	47884 / tcp	527
Block	IP Block	141.98.11.92	LTU	203.64.3.79	TWN	blocklist.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。

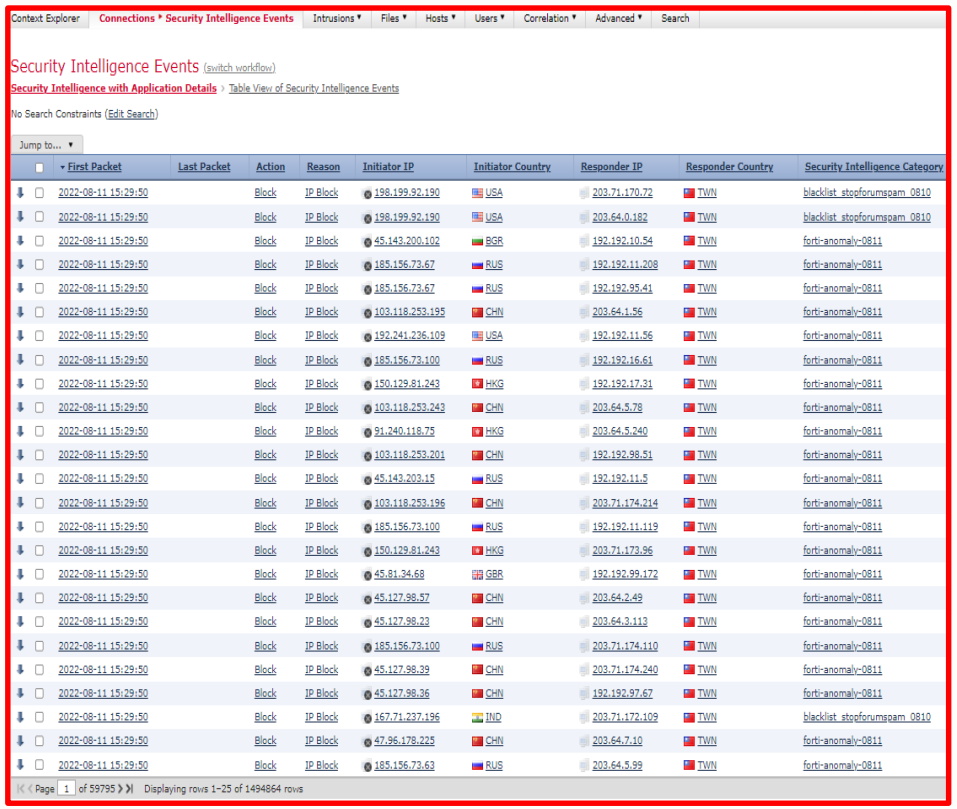
技服回應快速

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

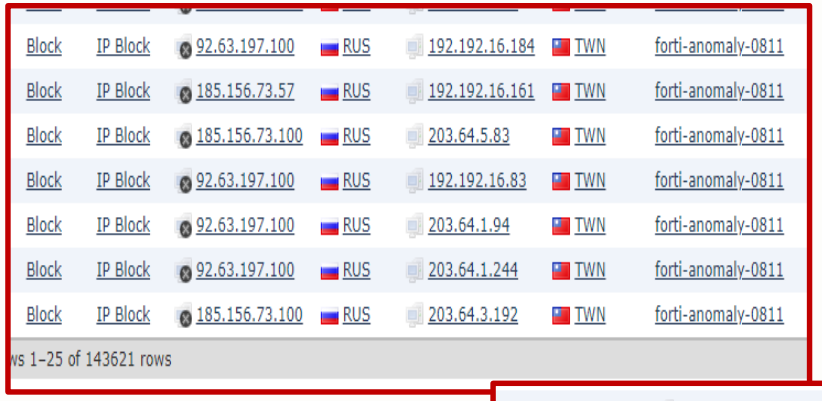
可以在IPS阻擋

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



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

s 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

s 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

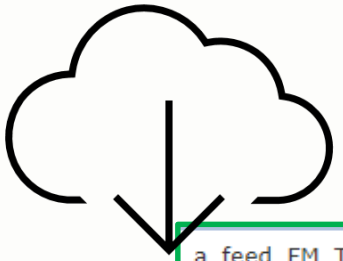
s 1-25 of 46338 rows

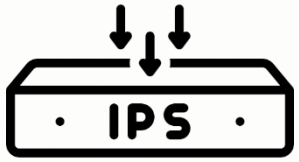
Block	IP Block	185.165.190.17	USA	192.192.11.2	TWN	forti-ips-0812
Block	IP Block	65.49.20.81	USA	192.192.95.84	TWN	blacklist_cert_tanet
Block	IP Block	64.62.197.58	USA	203.71.174.54	TWN	blacklist_cert_tanet
Block	IP Block	64.62.197.97	USA	192.192.16.177	TWN	blacklist_cert_tanet
Block	IP Block	64.62.197.215	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

s 1-25 of 108361 rows

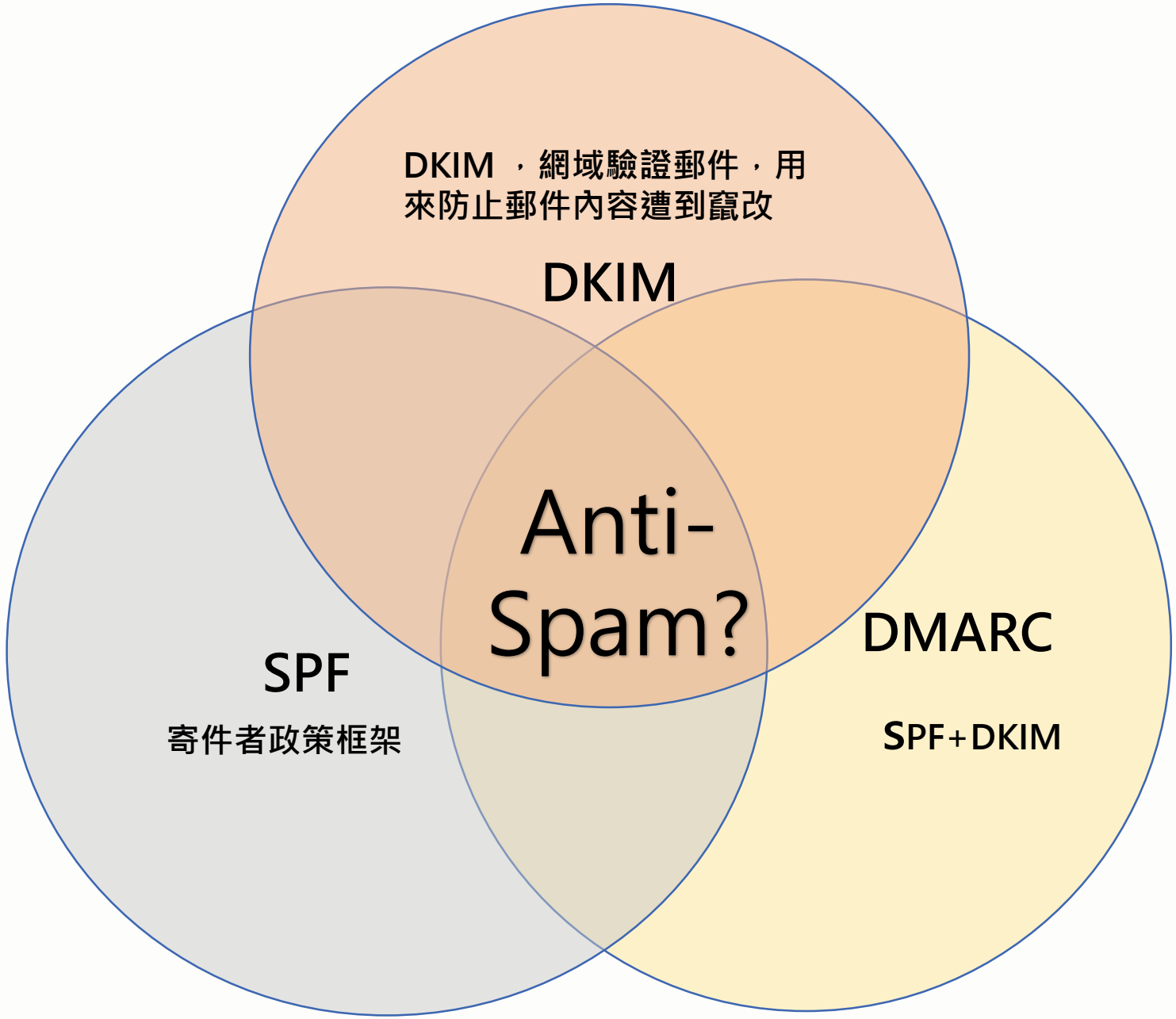
Block	IP Block	150.129.81.228	HKG	203.64.0.184	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.5.219	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.6.138	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	HKG	203.64.5.33	TWN	forti-anomaly-0811
Block	IP Block	150.129.81.210	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

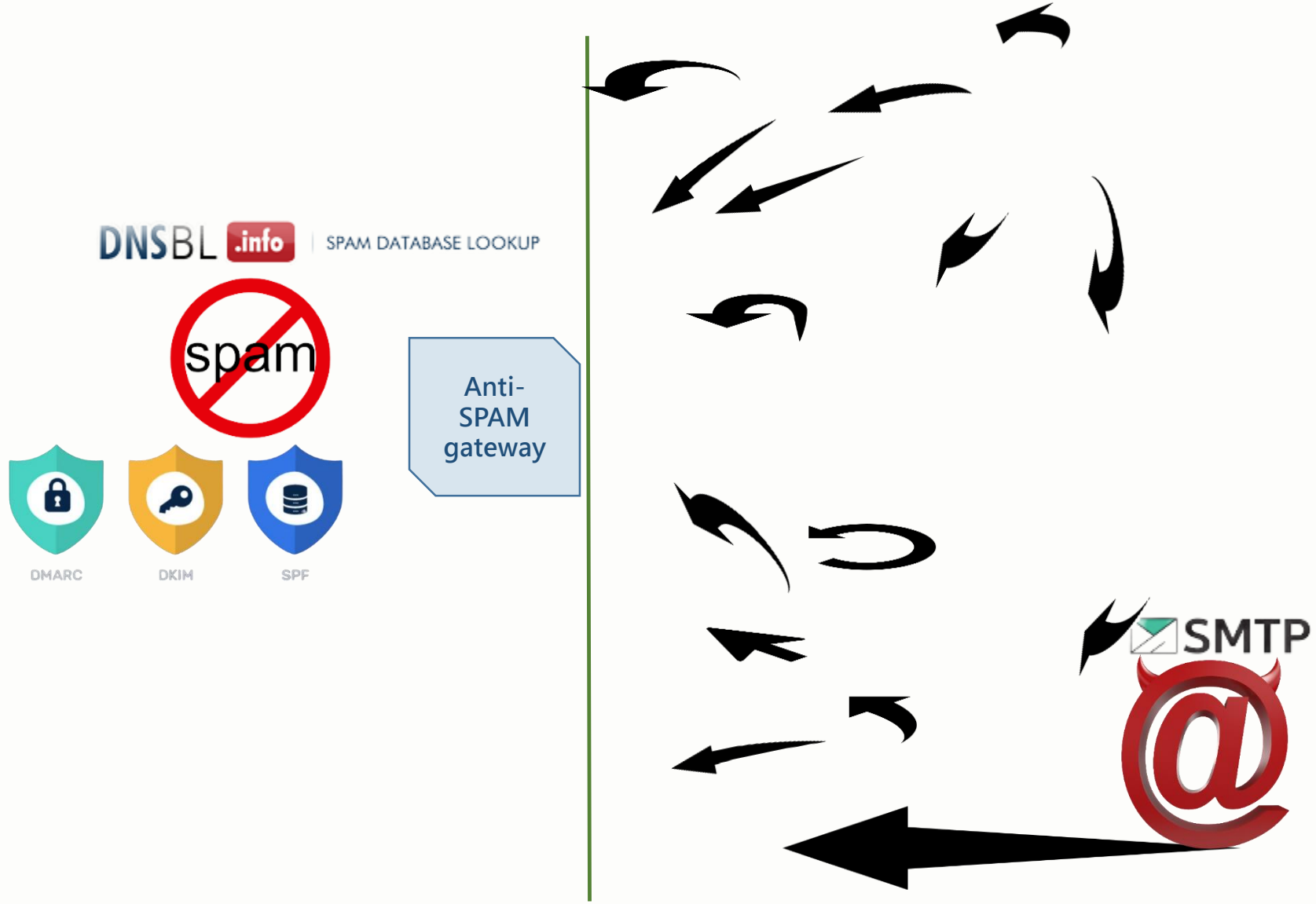
s 1-25 of 105737 rows

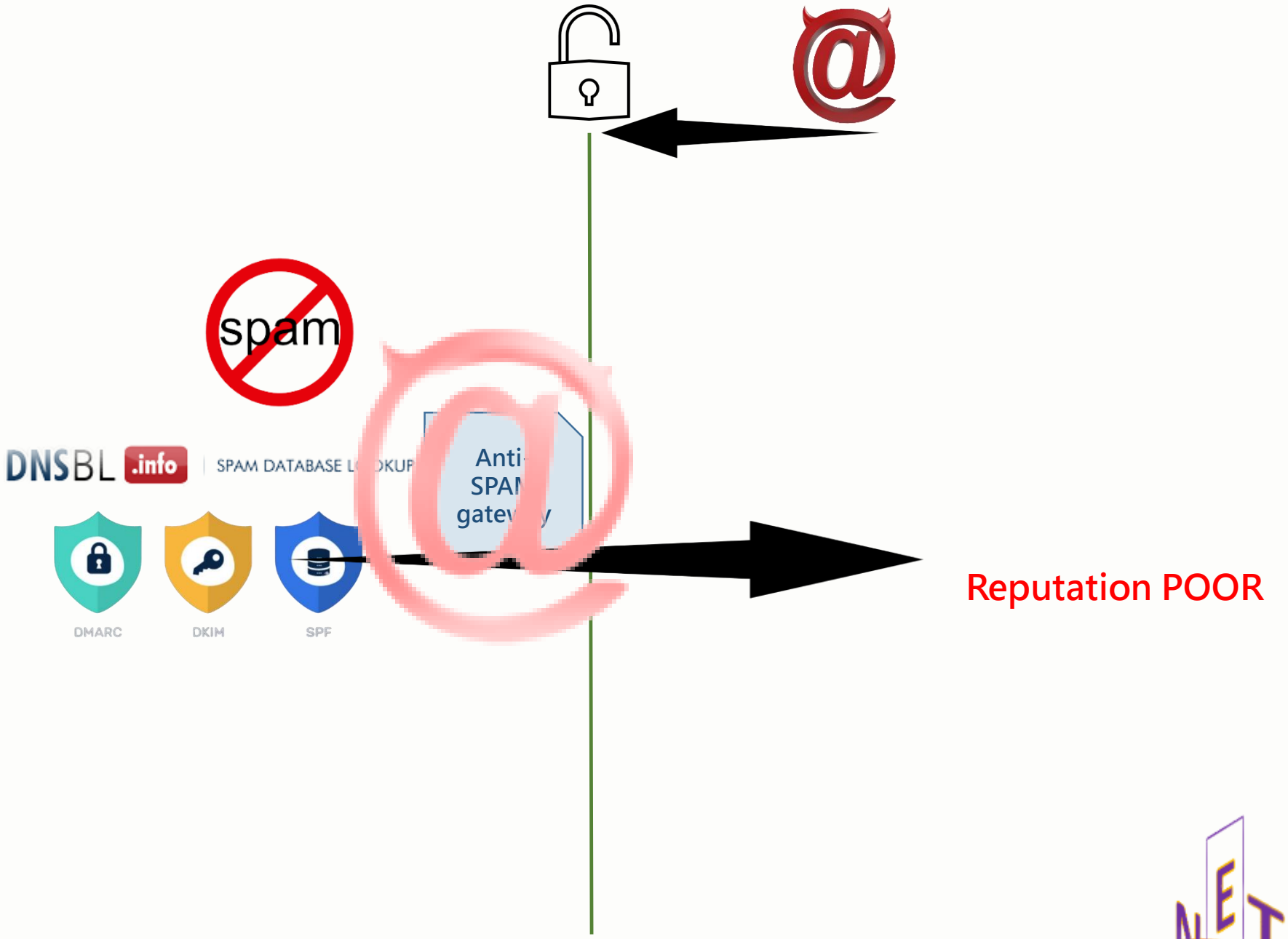




a_feed_FM_TNUA	Feed		
blacklist_cert_tanet *Last Updated: 2021-10-01 16:16:45*	List		
blacklist_spamhaut *Last Updated: 2021-10-01 16:48:27*	List		
blacklist_stopforumspam_0810 *Last Updated: 2022-08-10 15:22:55*	List		
blacklist_stopforumspam_180 *Last Updated: 2022-08-12 17:16:40*	List		
blacklist_talos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


DKIM ，網域驗證郵件，用來防止郵件內容遭到竄改
DKIM
Anti-Spam?
SPF
寄件者政策框架
DMARC
SPF+DKIM

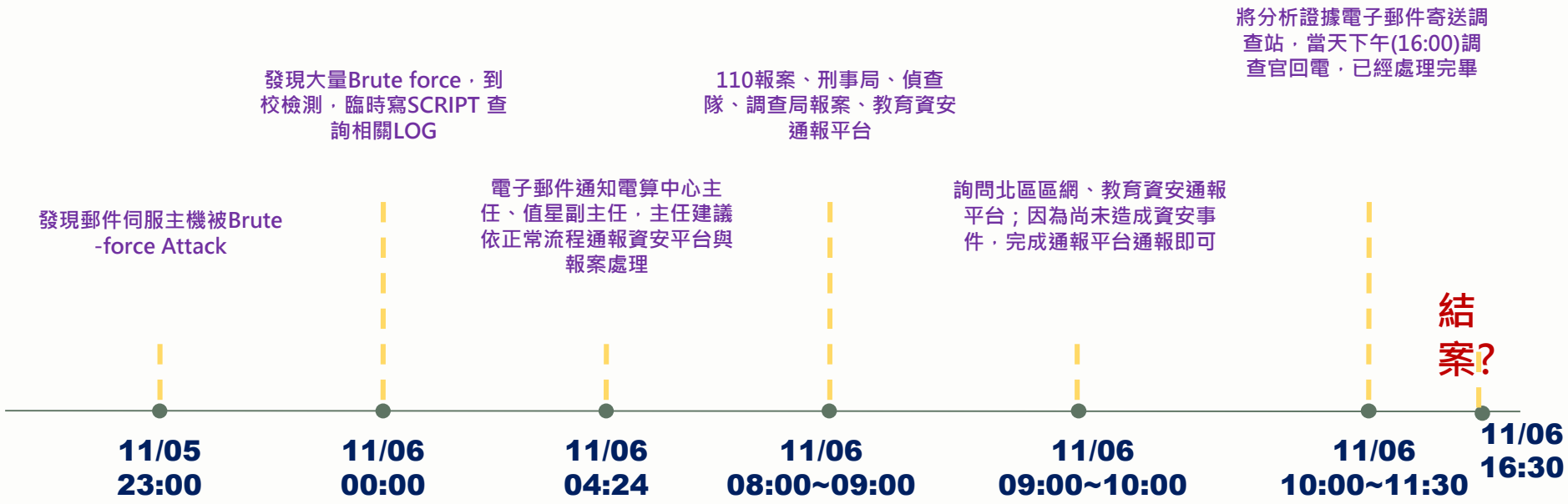

DNSBL .info
SPAM DATABASE LOOKUP
spam
DMARC
DKIM
SPF
Anti-
SPAM
gateway
SMTP

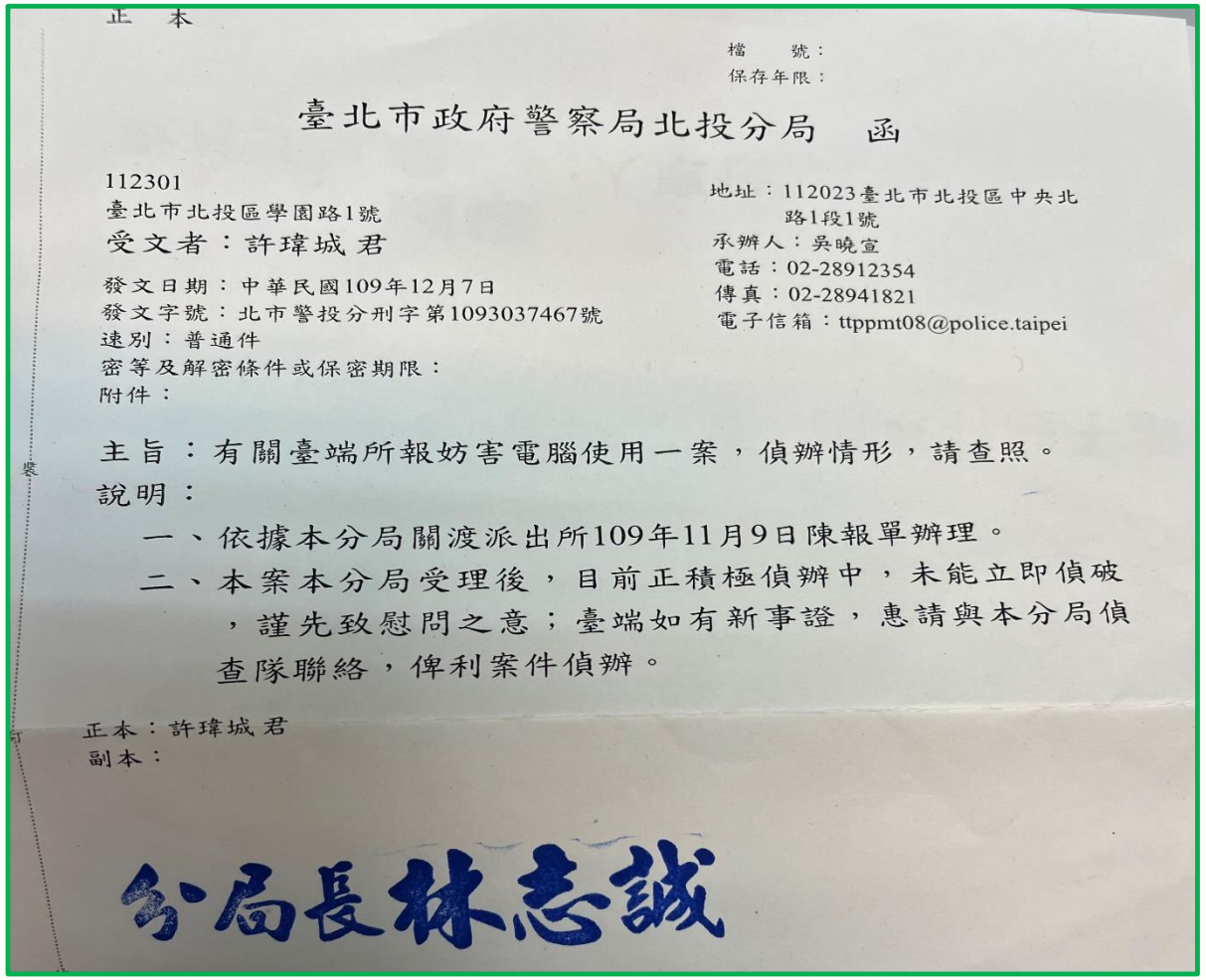

spam
DNSBL .info
SPAM DATABASE L OKUP
Anti-
SPAM
gate y
DMARC
DKIM
SPF
Reputation POOR

MOE Gateway

TNUA Gateway

11/06 校內郵件伺服主機遭受攻擊 處理時間說明 (109)





正　本

檔　　號：
保存年限：

臺北市政府警察局北投分局　函

112301
臺北市北投區學園路1號
受文者：許瑋城 君

發文日期：中華民國109年12月7日
發文字號：北市警投分刑字第1093037467號
速別：普通件
密等及解密條件或保密期限：
附件：

地址：112023臺北市北投區中央北路1段1號
承辦人：吳曉宣
電話：02-28912354
傳真：02-28941821
電子信箱：ttppmt08@police.taipei

主旨：有關臺端所報妨害電腦使用一案，偵辦情形，請查照。
說明：
一、依據本分局關渡派出所109年11月9日陳報單辦理。
二、本案本分局受理後，目前正積極偵辦中，未能立即偵破，謹先致慰問之意；臺端如有新事證，惠請與本分局偵查隊聯絡，俾利案件偵辦。

正本：許瑋城 君
副本：

分局長林志誠

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.[redacted]7&118.[redacted]8

中和某影城

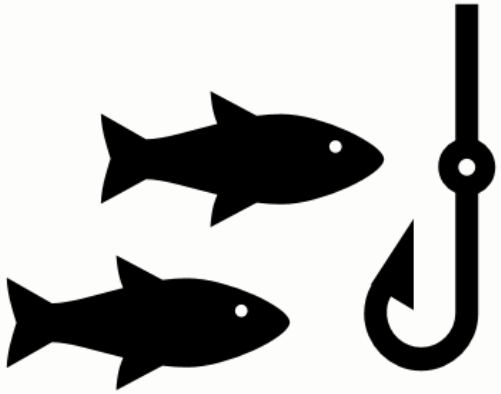
109/11/06凌晨看到的
DVR畫面

持續猜密碼

晨昏定省

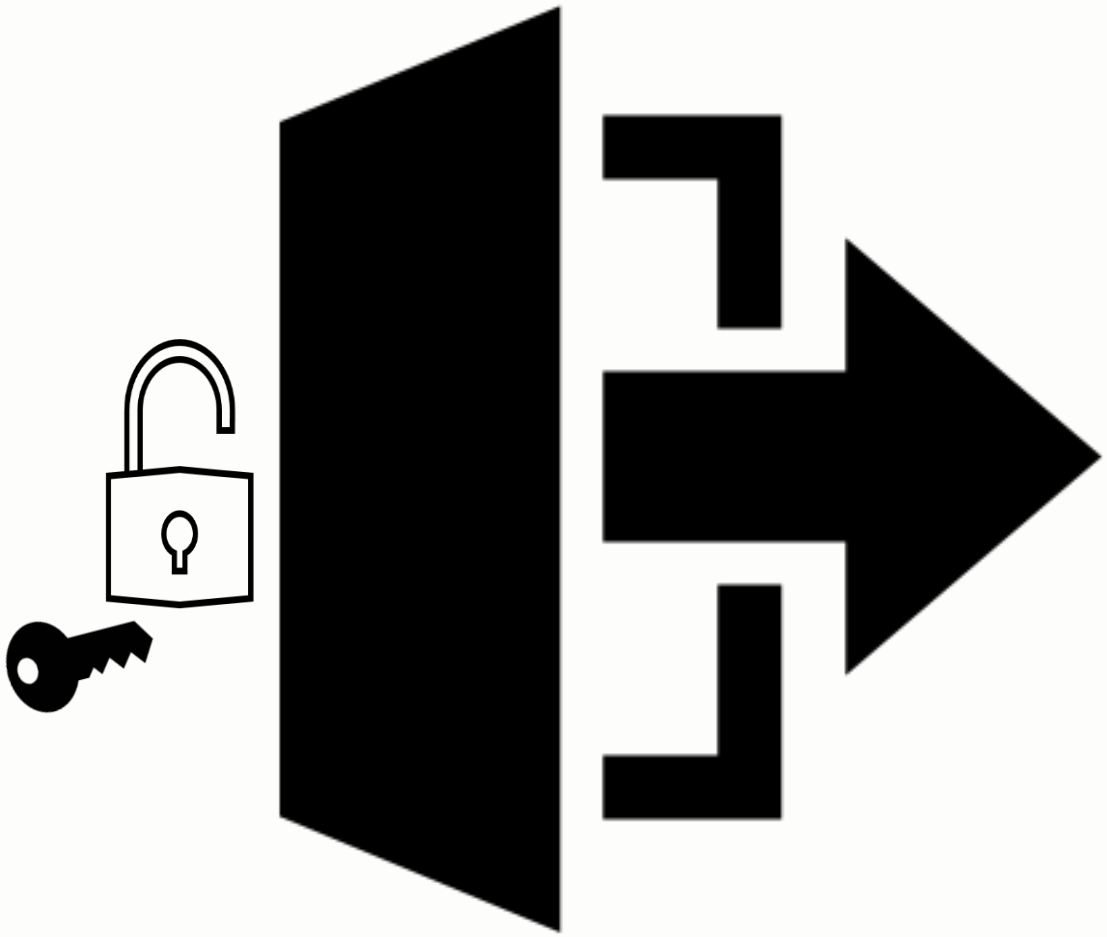
持續猜密碼

照三餐問候



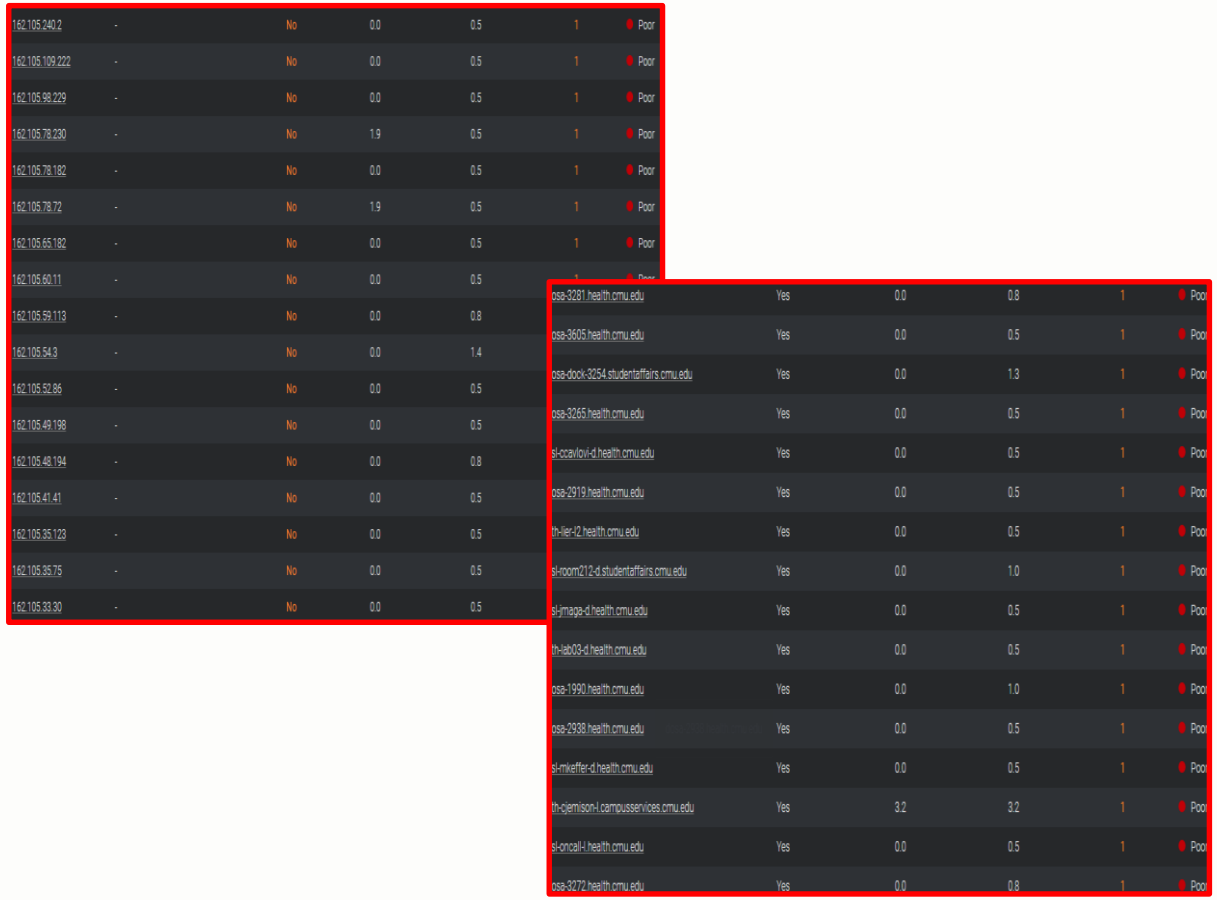
釣魚是一種娛樂

尤其是釣黑魚



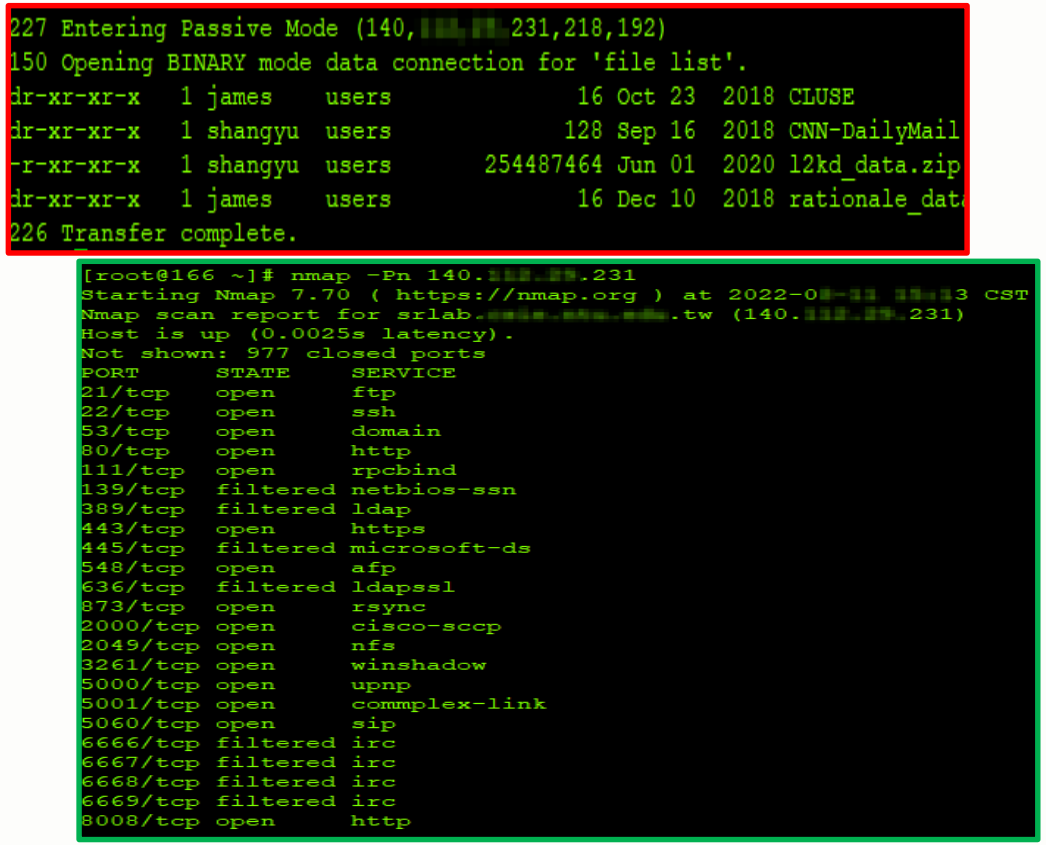
◆ 用於驗證，並非是攻擊手法或是網路攻擊示範，僅用於研討會實例說明。

◆ 部分圖示節錄於網路，僅供研討會使用



透過sendbase

是否可以找到pku，cmu
Reputation 相關?

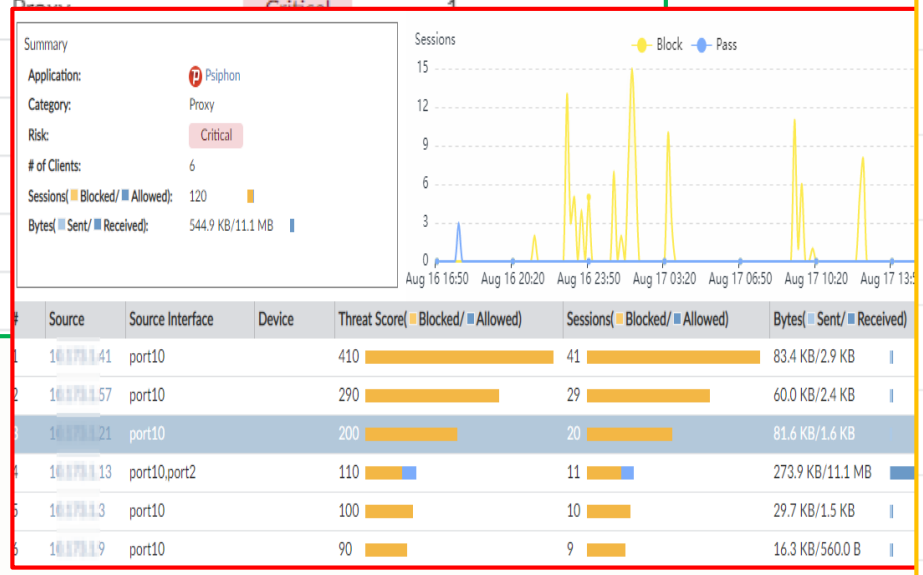


TANet 掃描PORT

找到NAS，如何找
使用者名稱?

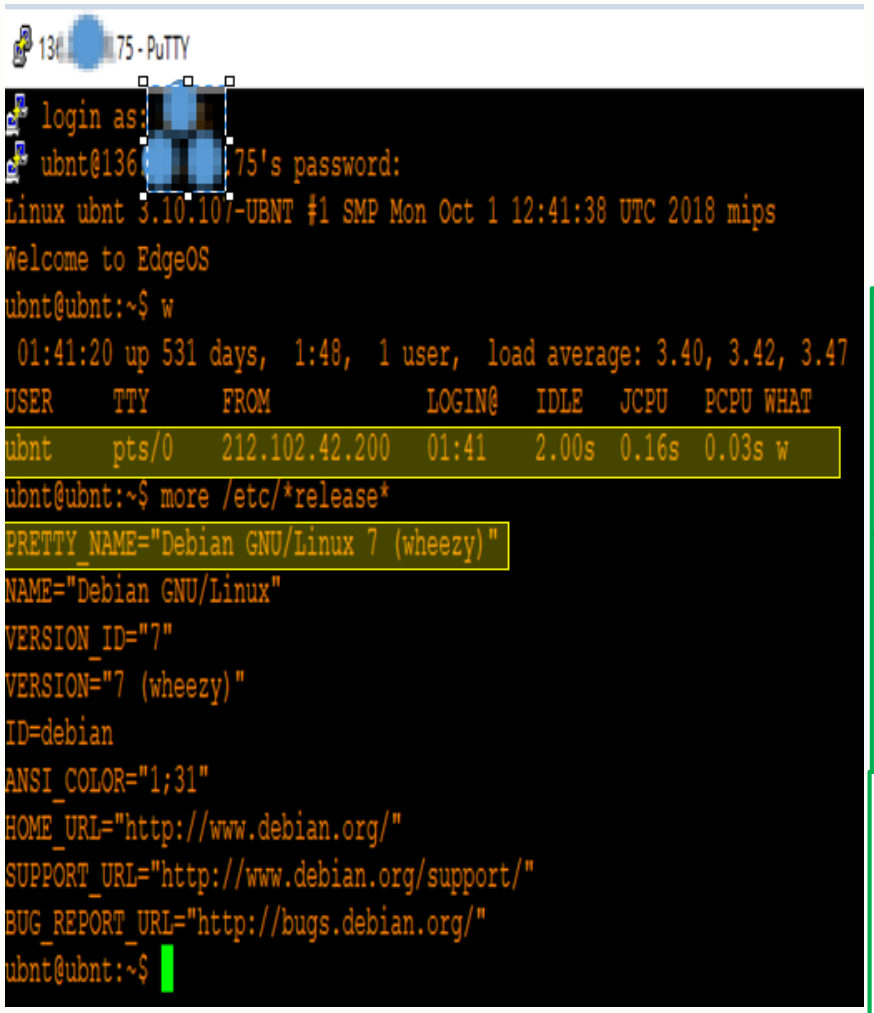
SPAMMER 只有你能打我嗎?

#	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	Critical	3
5	Hola.Unblocker			
6	Hotspot.Shield			
7	Ultrasurf			
8	Hamachi			
9	SOCKS4			
10	SOCKS5			

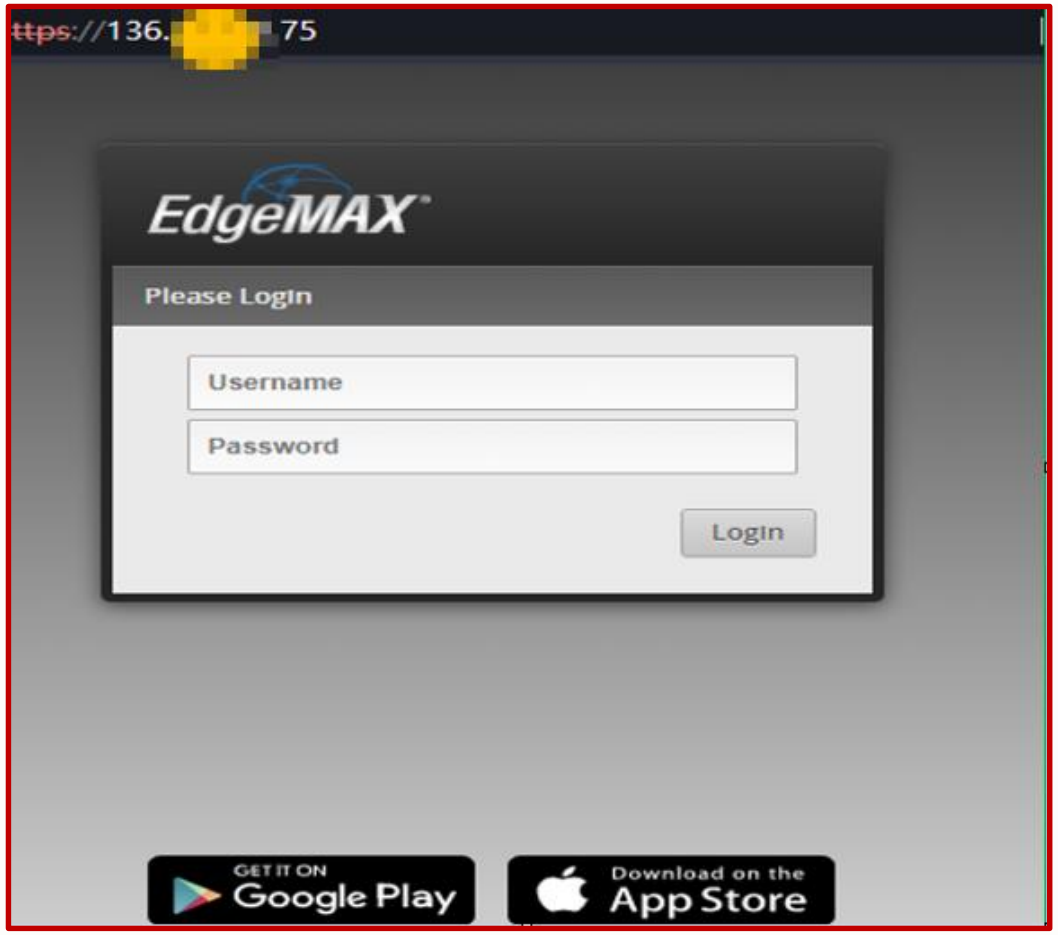


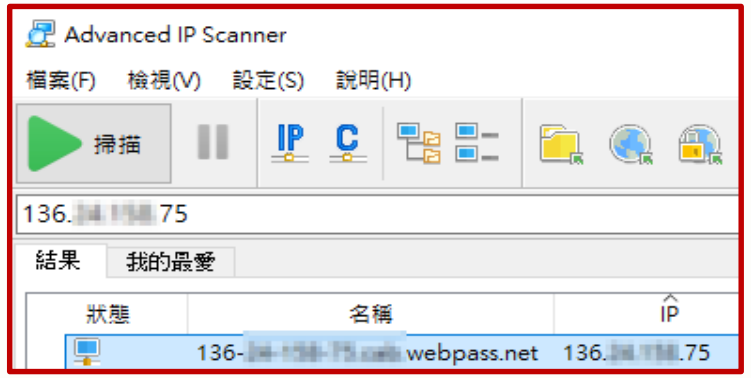
VPN	Best Price
NordVPN	$ 3.99 /月
Surfshark	$ 2.30 /月
ExpressVPN	$ 8.32 /月
IPVanish	$ 3.25 /月
TorGuard	$ 4.99 /月
FastestVPN	$ 2.49 /月
PIA	$ 2.42 /月
熱點S.	$ 7.99 /月
PureVPN	$ 3.33 /月
的VyprVPN	$ 2.50 /月

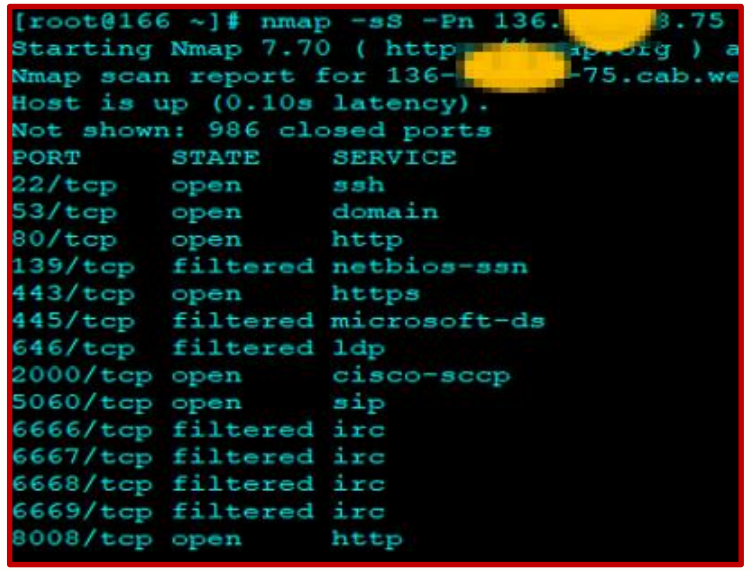
SPAMMER 只有你能打我嗎?



SPAMMER 只有你能打我嗎?







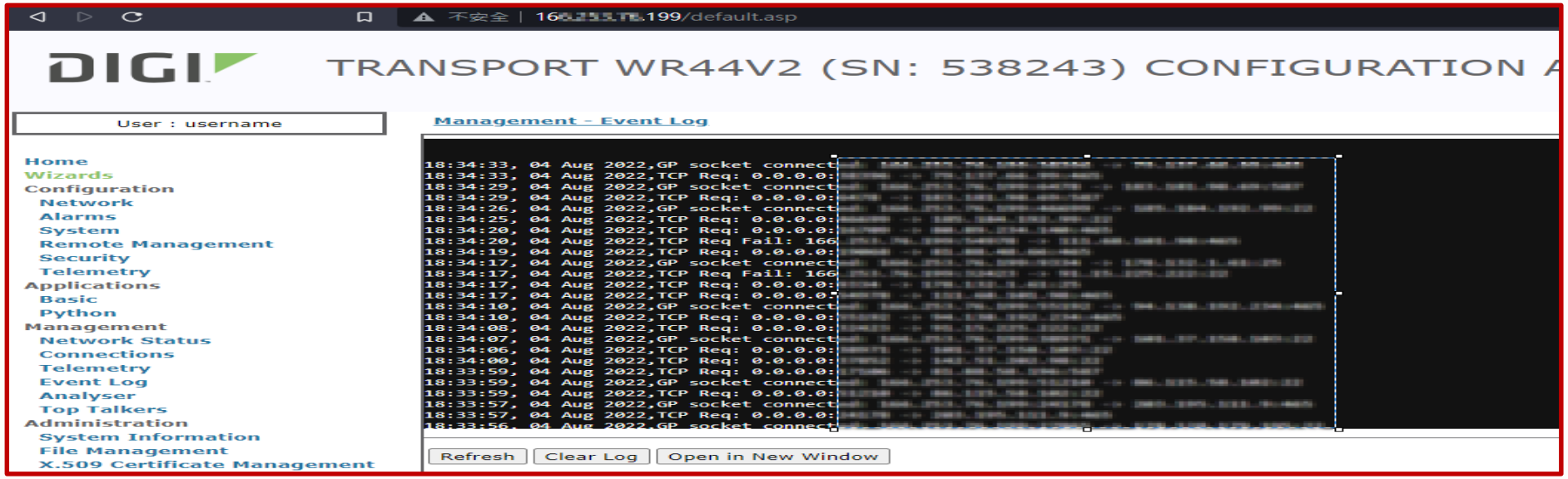
SPAMMER 只有你能打我嗎?

IP黑名單

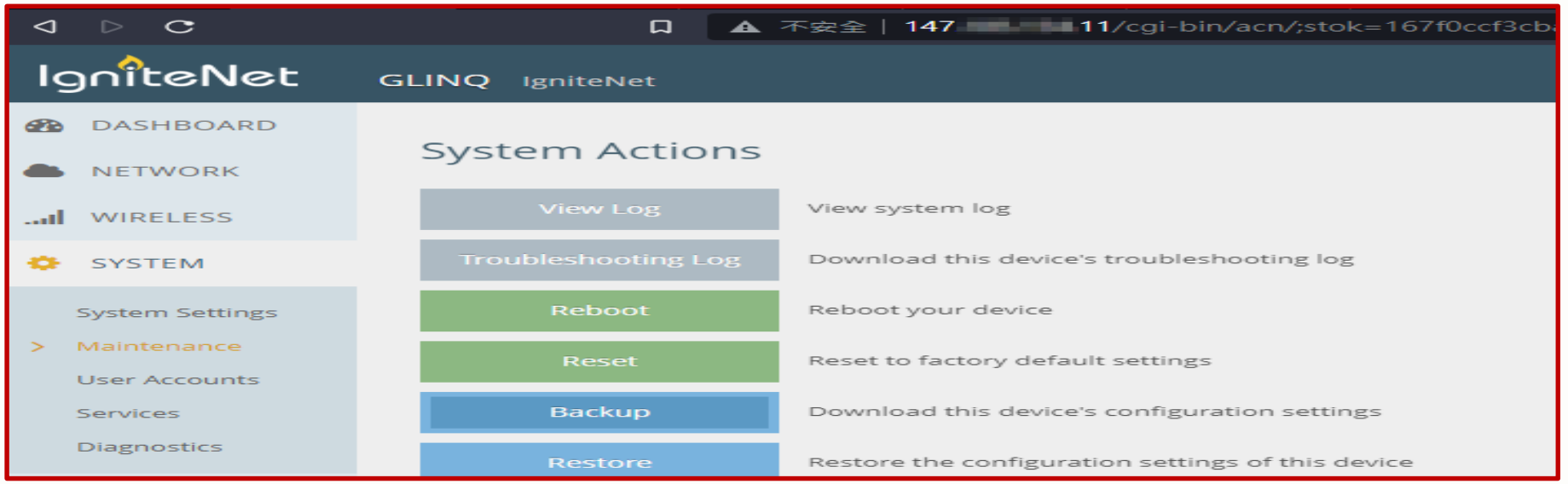
16[redacted]199 查詢

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



SPAMMER 只有你能打我嗎?



SPAMMER 只有你能打我嗎?

```
20220623.log:[19:37:14] [67.[redacted].124:57732] [P] connect to 203.[redacted]62 port 995
20220623.log:[19:37:14] [67.[redacted].124:57732] [P] USER jim[redacted].tnua.edu.tw
20220623.log:[19:37:14] [67.[redacted].124:57732] [P] PASS XXXXXXXX
20220623.log:[19:37:24] [67.[redacted].124:57732] [P] PASS failed: -ERR LOGIN failed
20220623.log:[19:37:24] [67.[redacted].124:57732] [S] 535 Authentication failed
20220623.log:[19:37:24] [67.[redacted].124:57732] smtp_fsm: peer_closed
```

不安全 | 67.[redacted]124/22518948/tank_status.html

Lamesa Butane - Guest access level

Franklin Fueling Systems

Tank Status

System FMS Setup

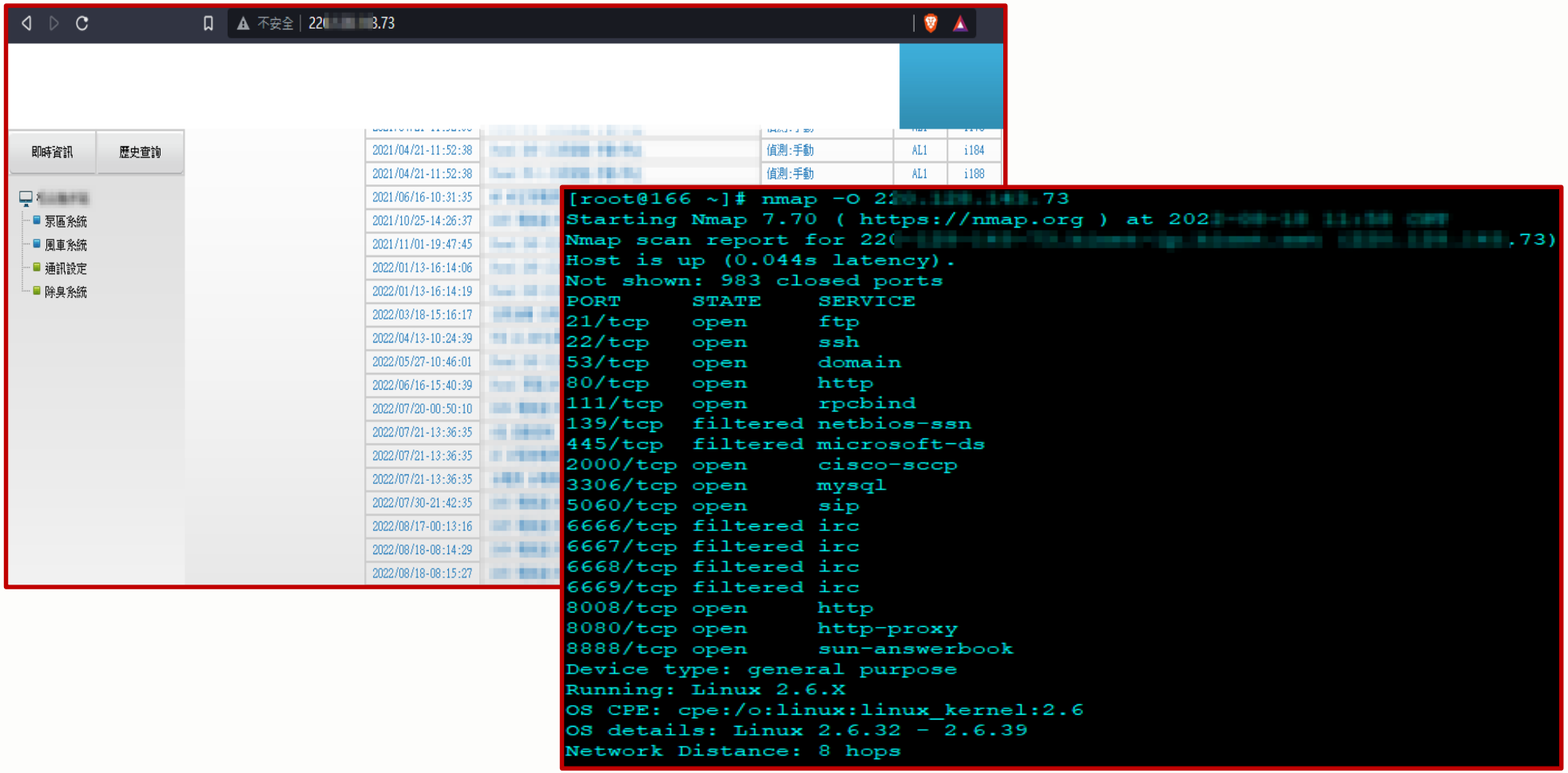
Status Alarms Control Compliance Reports Data Logging

Tanks

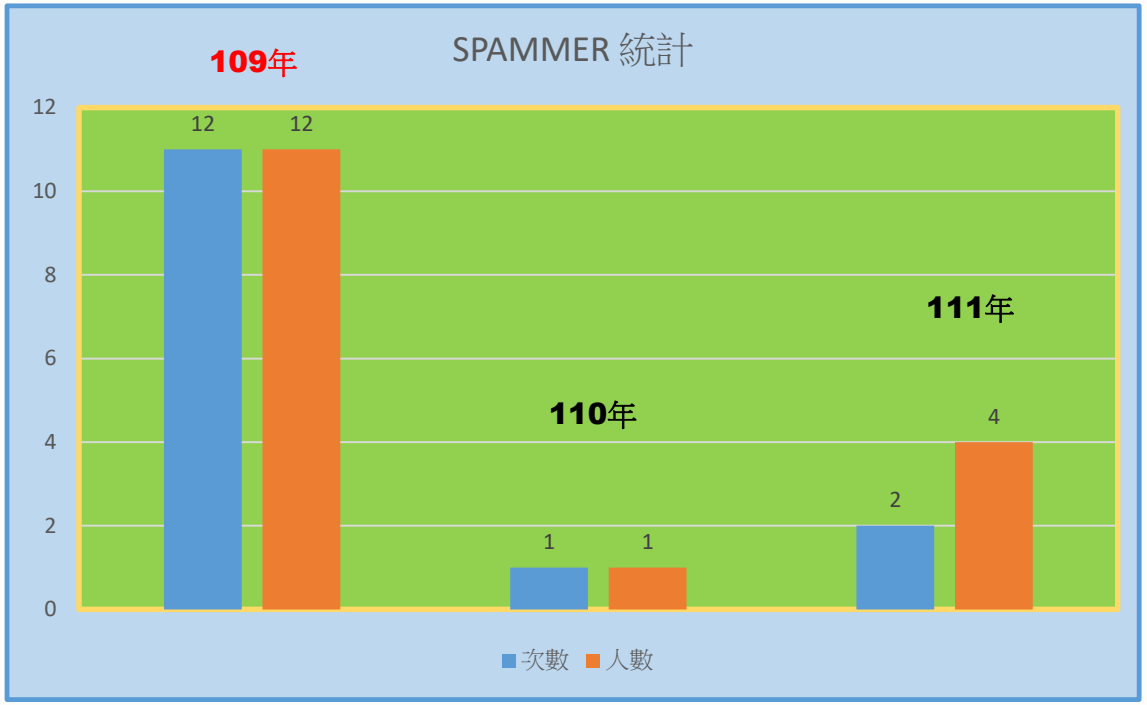
TANKS

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?



■ 網路攻擊一直都有




1.改善黑、白名單誤判，以及回寫系統封鎖，檢討成效
2.能更有效達成校內電子郵件防護
ACTION
PLAN
PPT P28
電子郵件攻防
1.透過監測流量修正policy僅開放白名單可使用(深夜)。
2.修正與確認收集黑、白名單有效性
CHECK
DO
1.查詢程式使用狀況
2.監測LOG流量
3.清查帳號與簡訊發送

■ 網路攻擊一直都有

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

姓名

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: 2022/0

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。

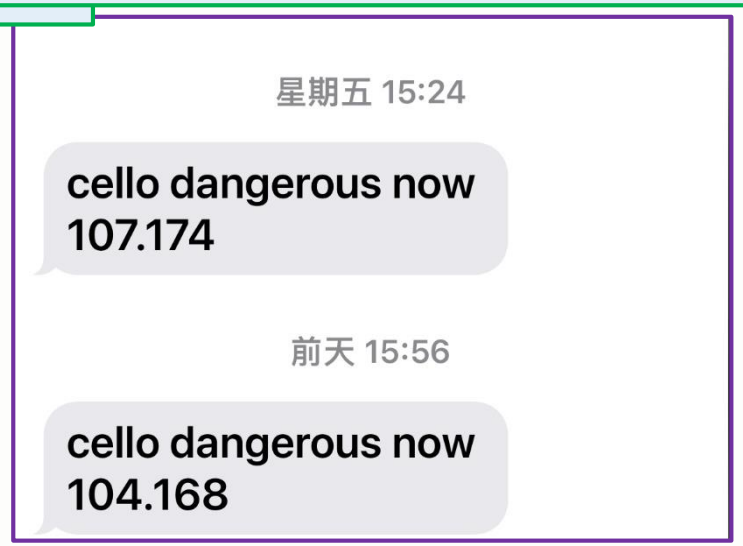
寄件者: "台灣簡訊" <mailer@gw.twsms.com>
收件者: "chw" <chw@tnua.edu.tw>
寄件備份: 2022 7 月 29 星期五 下午 3:24:03
主旨: EmailToSMS狀況回報

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



■ 網路攻擊一直都有

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, C

IP address details

216.52.48.138

Boston, Massachusetts, United States

IP address details

104.168.34.187

Washington, Washington, D.C., United States

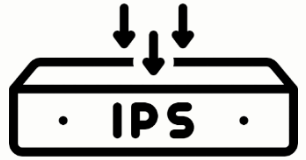
104.168.34.187	104-168-34-187-host.colocrossing.com	No	4.5	3.9	2	Poor

TNUA

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

■ 網路攻擊一直都有



Connections by Source Country

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

Connections by Network SI Categories

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

■ 網路攻擊一直都有

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								
Block	IP Block								
Block	IP Block								
Block	IP Block								
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

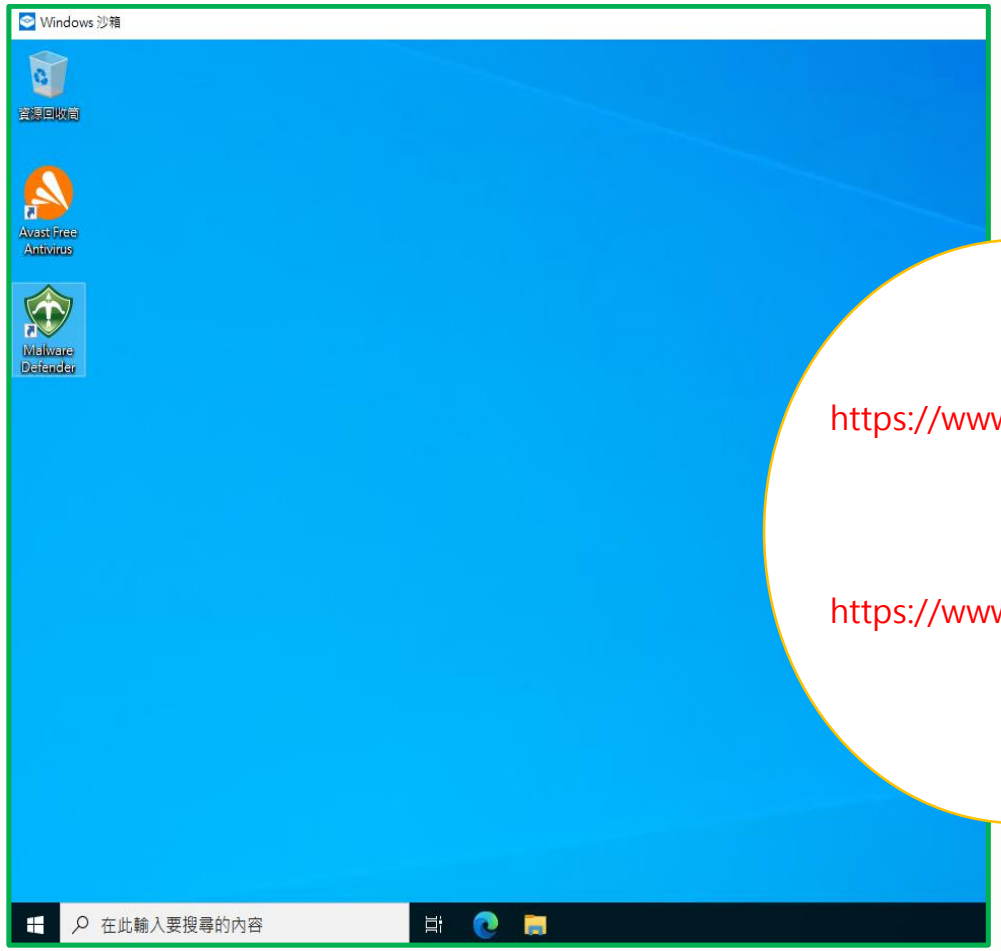
■ 網路攻擊一直都有

#截止2022-08-21，[redacted]台湾IP地址共计587条记录，IP地址总数35695616。
#查看 [redacted]台湾[redacted]

#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

■ 網路攻擊一直都有



https://www.zoomeye.org/

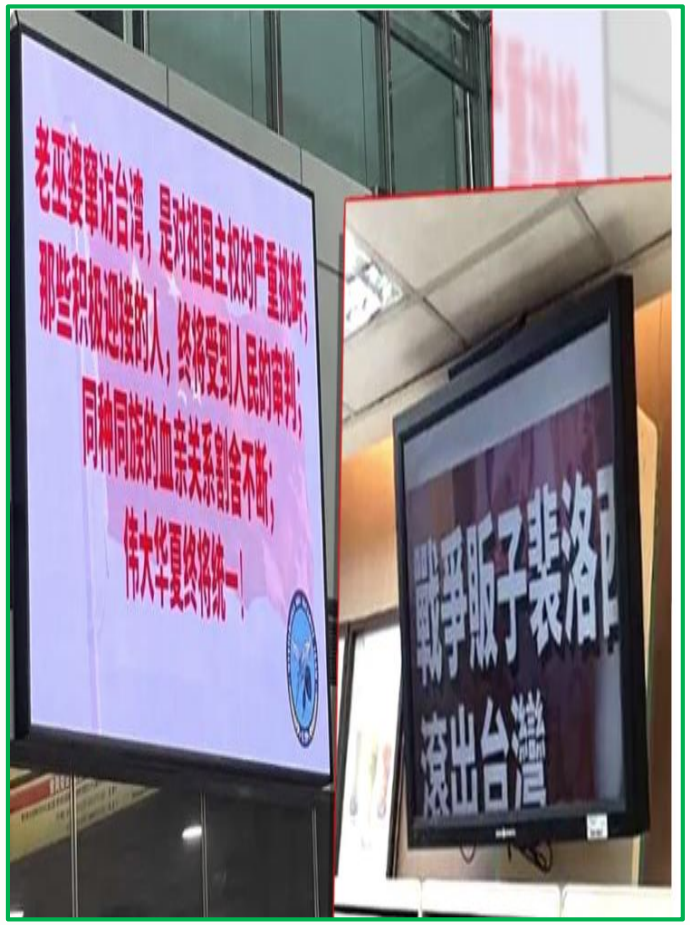
https://www.shodan.io/host

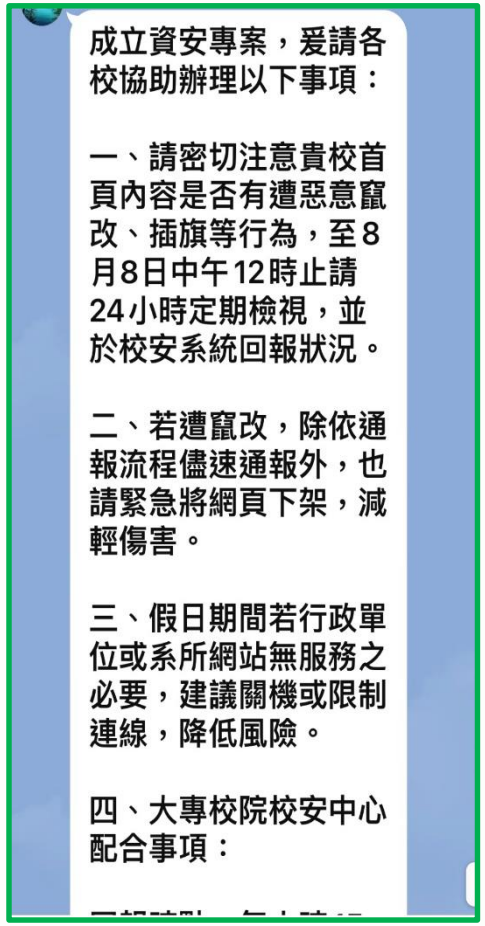
建議使用 虛擬機、windows 沙箱

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



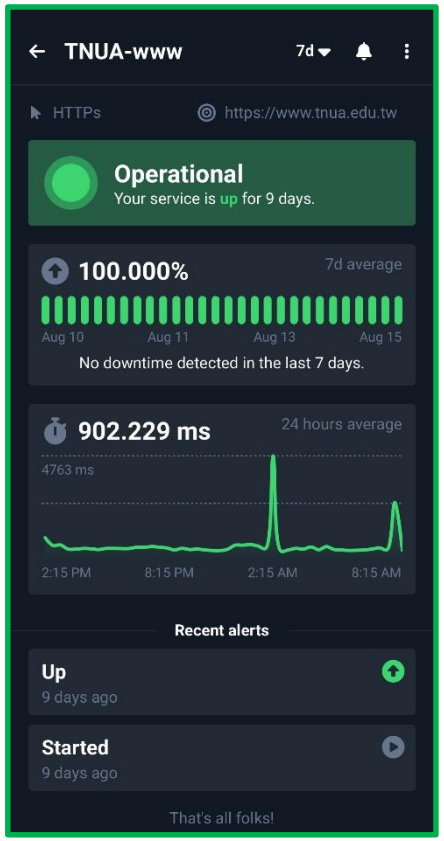


網路攻擊

推播系統

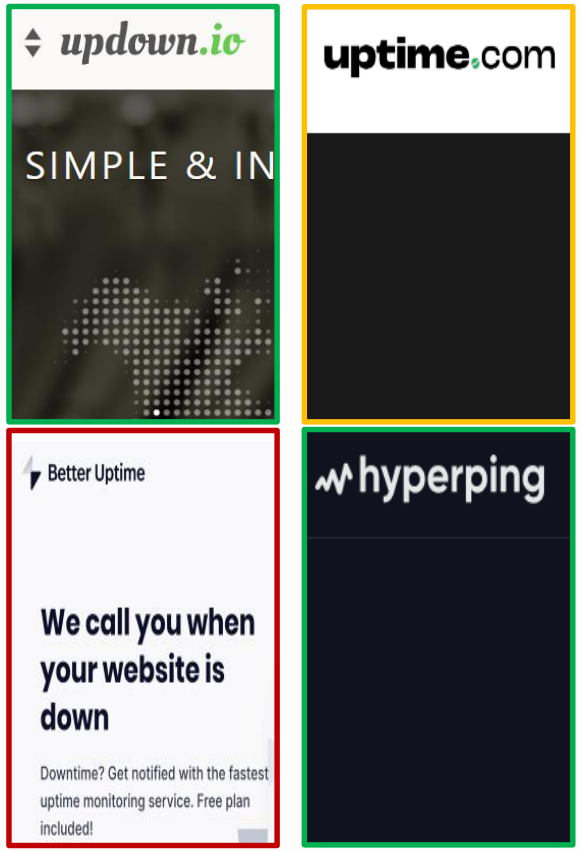
校安通知

檢測首頁



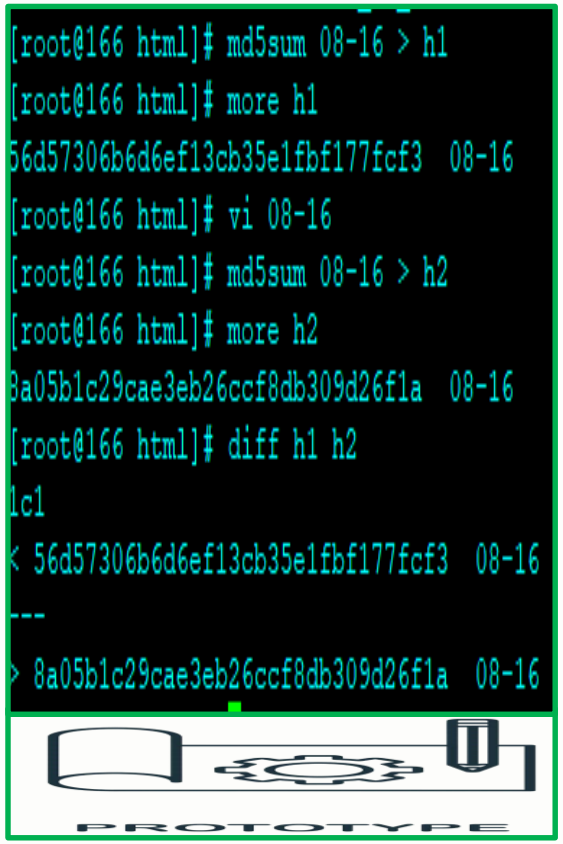
UptimeRobot

50個網站監測



網站監測服務

有付費與免付費



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

算資料夾的HASH，HASH值為檔名

```python
import hashlib,time
from pathlib import Path

#=========計算整個資料夾HASH=========
while 10==10:
    def md5_update_from_file(filename, hash):
        assert Path(filename).is_file()
        with open(str(filename), "rb") as f:
            for chunk in iter(lambda: f.read(4096), b""):
                hash.update(chunk)
        return hash

    def md5_file(filename):
        return md5_update_from_file(filename, hashlib.md5()).he

    def md5_update_from_dir(directory, hash):
        assert Path(directory).is_dir()
        for path in sorted(Path(directory).iterdir()):
            hash.update(path.name.encode())
            if path.is_file():
                hash = md5_update_from_file(path, hash)
            elif path.is_dir():
                hash = md5_update_from_dir(path, hash)
        return 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

```python
#算資料夾內的資料夾及檔案總數

import time,smtplib,os,urllib.request
from email.mime.text import MIMEText

#判斷Source_HASH裡的檔案總數，若不同就發信、發簡訊通知
#EMAIL函數
def sendmail():
    msg = MIMEText(Now_Time + " 偵測到資料夾HASH值有異動，請檢查CCNET ", "plain
    msg["Subject"] = "Check CCNET"
    msg["From"] = "寄件人信箱"
    msg["To"] = "收件人信箱1;收件人信箱2"
    smtp = smtplib.SMTP("smtp.gmail.com", 587)
    smtp.ehlo()
    smtp.starttls()
    smtp.login("寄件人帳號","寄件人密碼")
    smtp.send_message(msg)
#簡訊函數
def sendSMS(tel):
    username = "TWSMS帳號"
    password = "TWSMS密碼"
    mobile = tel
    message = "CCNET_HASH_Change!"

    msg = 'username='+username+'&password='+password+'&mobile='+mobile+'&mes
    url = 'http://api.twsms.com/json/sms_send.php?'+msg
```

https://youtu.be/gWsS8ZVKXVQ

計算HASH

寄發郵件、簡訊

郵件、簡訊

結論

TNUA Network 首頁 -> NetFlow

類別 : report 日期 : 2009 06 16 時間 : 23:55 [IN / OUT] | [遞減 / 遞增]

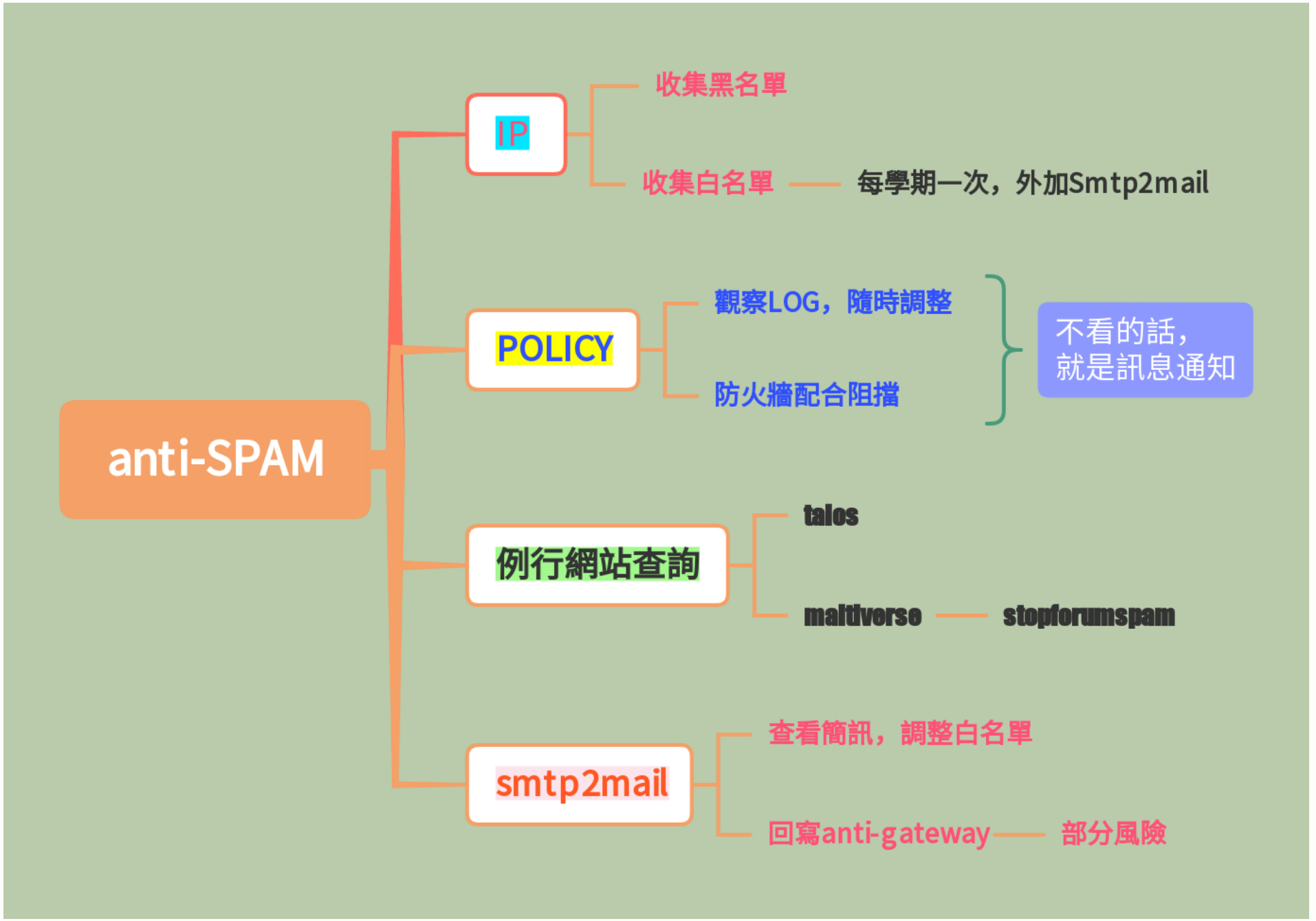
本日 本周(2009-06-09 至 2009-06-16) 本月

	IP	FLOWS	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

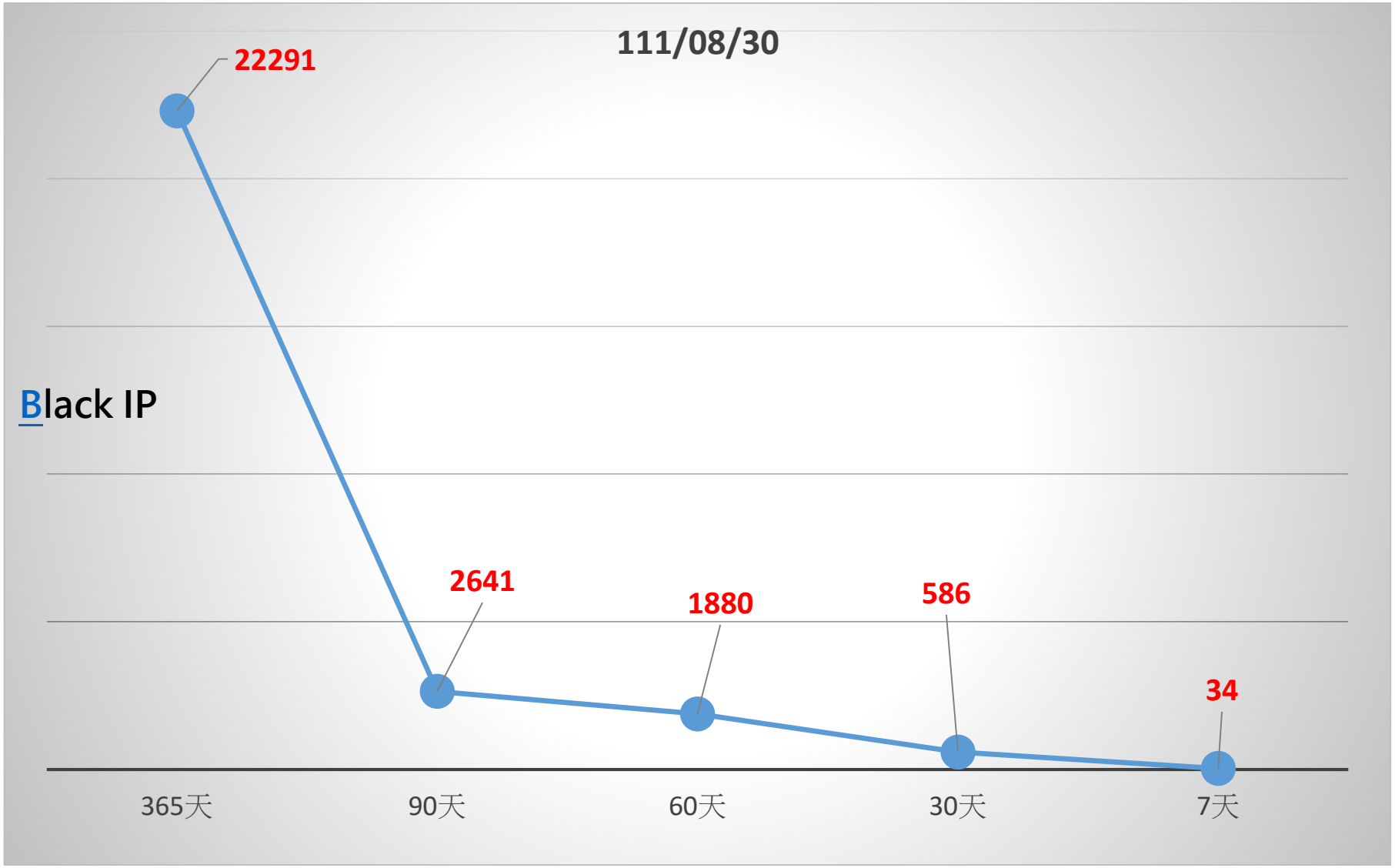
主辦單位：教育部 Ministry

承辦單位：國立台灣科技大

- 結論


anti-SPAM
IP
收集黑名單
收集白名單
每學期一次，外加Smtp2mail
POLICY
觀察LOG，隨時調整
防火牆配合阻擋
不看的話，
就是訊息通知
例行網站查詢
talos
maltiverse
stopforumspam
smtp2mail
查看簡訊，調整白名單
回寫anti-gateway
部分風險

- 結論



◆BLOCK(BLACK) LIST名單

◆有效的白名單

◆高強度密碼規則

防火牆

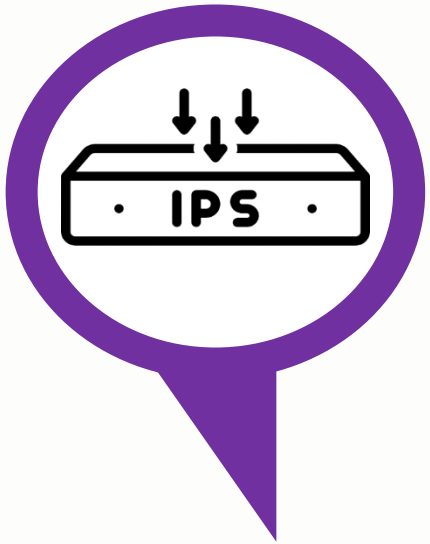
防火牆建議:

- 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