

教育體系資安檢核 網路惡意活動 檢測

臺灣大學計資中心網路組
游子興

davisyou@ntu.edu.tw

02-33665008

網路惡意活動檢測

技服中心每週四公布之
惡意中繼名單

威脅清單下載

* <https://portal.cert.tanet.edu.tw/index.html>

The screenshot shows a web browser window with the URL <https://portal.cert.tanet.edu.tw/reportAll/prog/blackList.php>. The page title is "報表查詢系統 | Developed...". The main content area has a blue header with the text "報表查詢系統" and "Developed By TACERT". Below the header is a navigation menu with several buttons: "OID查詢", "威脅名單", "事件單列表", "EWA列表", "事件類型統計", "轄下單位密碼更動情況", and "DDOS清洗系統". The "威脅名單" button is highlighted with a red border. Below the navigation menu is a search bar with the text "搜尋" and a "Show" button. To the right of the search bar, there are two links: "下載TANET威脅清單" and "下載技服威脅清單". At the bottom of the page, there is a timestamp: "Last modified: 2020/03/18 11:42:53".

資安院(技服) 威脅清單 (實際檢測清單)

* Domain List

1	SN	Domain-List	FirstDate	LastDate					
2	1	opensslv3.csproject.org	2019-08-15	2019-08-15					
3	2	carsails.allowed.org	2019-08-15	2019-08-15					
4	3	ap21.ilvsmail.com	2019-04-25	2019-07-16					
5	4	homepage.neithey.com	2019-04-30	2019-07-16					
6	5	eclient.cybertw.com	2019-04-30	2019-07-01					
7	6	broadweb.cybertw.com	2019-04-30	2019-07-01					
8	7	cloud105.iworksme.com	2019-04-30	2019-06-24					
9	8	tc379.ilvsmail.com	2019-04-25	2019-05-20					
10	9	ad03.eynyforum.com	2019-04-30	2019-05-15					
11	10	update.asuswebstorage.com.ssmailer.com	2019-05-06	2019-05-06					
12	11	www.google.com.dns-report.com	2019-05-06	2019-05-06					
13	12	cksogo.com	2019-05-02	2019-05-02					
14	13	fs53.eynyforum.com	2019-05-02	2019-05-02					
15	14	evnyforum.com	2019-05-02	2019-05-02					

DnList(order_by_Priority)
 DnList(order_by_sn)
 IpList(order_by_Priority)
 IpList(order_by_sn)

* IP List

1	A	B	C	D	E	F	G	H	I	J
1	SN	IP-List	FirstDate	LastDate	Type					
2	1	180.215.218.135	2022-08-04	2022-08-04	Phishing					
3	2	185.207.155.146	2022-07-28	2022-07-28	C2 Server					
4	3	139.59.247.94	2022-07-18	2022-07-18	C2 Server					
5	4	13.229.3.203	2022-08-18	2022-08-18	C2 Server					
6	5	103.179.243.142	2022-09-14	2022-09-14	Phishing					
7	6	110.34.181.166	2022-08-22	2022-08-22	Phishing					
8	7	156.248.153.167	2022-08-05	2022-08-05	Phishing					
9	8	60.205.0.192	2022-08-19	2022-08-19	Phishing					
10	9	156.248.153.181	2022-08-17	2022-08-17	Phishing					
11	10	156.248.153.172	2022-08-11	2022-08-11	Phishing					
12	11	118.107.25.231	2022-08-22	2022-08-22	Phishing					
13	12	14.128.35.26	2022-08-11	2022-08-11	Phishing					
14	13	14.128.35.27	2022-08-11	2022-08-11	Phishing					

DnList(order_by_Priority)
 DnList(order_by_sn)
 IpList(order_by_Priority)
 IpList(order_by_sn)

TANet 威脅清單 (參考用、不檢測)

* IP List only

惡意威脅來源清單列表

資料來源	通報時間	IP位置	惡意網址	攻擊型態	國家
N-ASOC	2020/3/16	103.27.111.66		SERVER-WEBAPP /etc/passw	Hong Kong
N-ASOC	2020/3/16	137.59.19.212		SERVER-WEBAPP /etc/passw	Hong Kong
N-ASOC	2020/3/16	180.131.52.131		SERVER-OTHER Remote Desl	Korea
N-ASOC	2020/3/16	185.153.199.91	server-185-153-199-91.cloudedic.net	SERVER-OTHER Remote Desl	Russian
N-ASOC	2020/3/16	185.202.2.112		SERVER-OTHER Remote Desl	France
N-ASOC	2020/3/16	185.202.2.137		SERVER-OTHER Remote Desl	France
N-ASOC	2020/3/16	69.10.62.71		MALWARE-CNC User-Agent I	United States
N-ASOC	2020/3/16	93.174.93.216	no-reverse-dns-configured.com	SERVER-WEBAPP MYPower DV	Netherlands
S-ASOC	2020/3/14	103.21.206.230		網路攻擊	Indonesia
S-ASOC	2020/3/14	104.218.50.88		網路攻擊	United States
S-ASOC	2020/3/14	104.244.73.31		網路攻擊	Luxembourg

更新日期：2020年03月18日

情資來源：S-ASOC, N-ASOC, N-ISAC

清單編號：v2020.10

■ 為本次新增之內容

*本清單為機敏文件，限TANet內部人員使用

檢測方法

- * 1. Nmap
- * 2. TraceRoute
 - * PingInfoView
- * 3. 封包側錄

检测方法1

nmap

Nmap IP List Test

- * nmap -sP -iL bad_ip.txt
 - * Nmap scan report for 169.68.10.185.ro.ov0.sc (185.10.68.169)
 - * Host is up (0.32s latency).
 - * Nmap scan report for li1601-50.members.linode.com (139.162.117.50)
 - * Host is up (0.054s latency).
 - * Nmap done: 20 IP addresses (2 hosts up) scanned in 4.98 seconds
- * 參數說明
 - * -sP ping scan

Nmap DNS List Test

- * `nmap -sP -iL bad_dns.txt`
 - * Failed to resolve "mx.msdtc.tw".
 - * Failed to resolve "cnaweb.mrslove.com".
 - * Failed to resolve "infonew.dubya.net".
 - * Nmap scan report for `www.ntu.edu.tw` (140.112.8.116)
 - * Host is up (0.0010s latency).
 - * Nmap done: 1 IP address (1 host up) scanned in 22.47 seconds

Timeout vs. NX Domain

- * Timeout: 權威 DNS 伺服器 無回應

```
> fq.narllab.com
伺服器: dns.google
Address: 8.8.8.8

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
```

- * NX Domain: 權威 DNS 伺服器 回應”無此Doamin”

```
> abcxyz1234.com
伺服器: dns.google
Address: 8.8.8.8

*** dns.google 找不到 abcxyz1234.com: Non-existent domain
```

檢測方法2 TraceRoute (IP 黑名單)

使用 Ping 偵測缺點

- * 偵測方法

- * 未回應 Ping 即假設已順利阻擋。

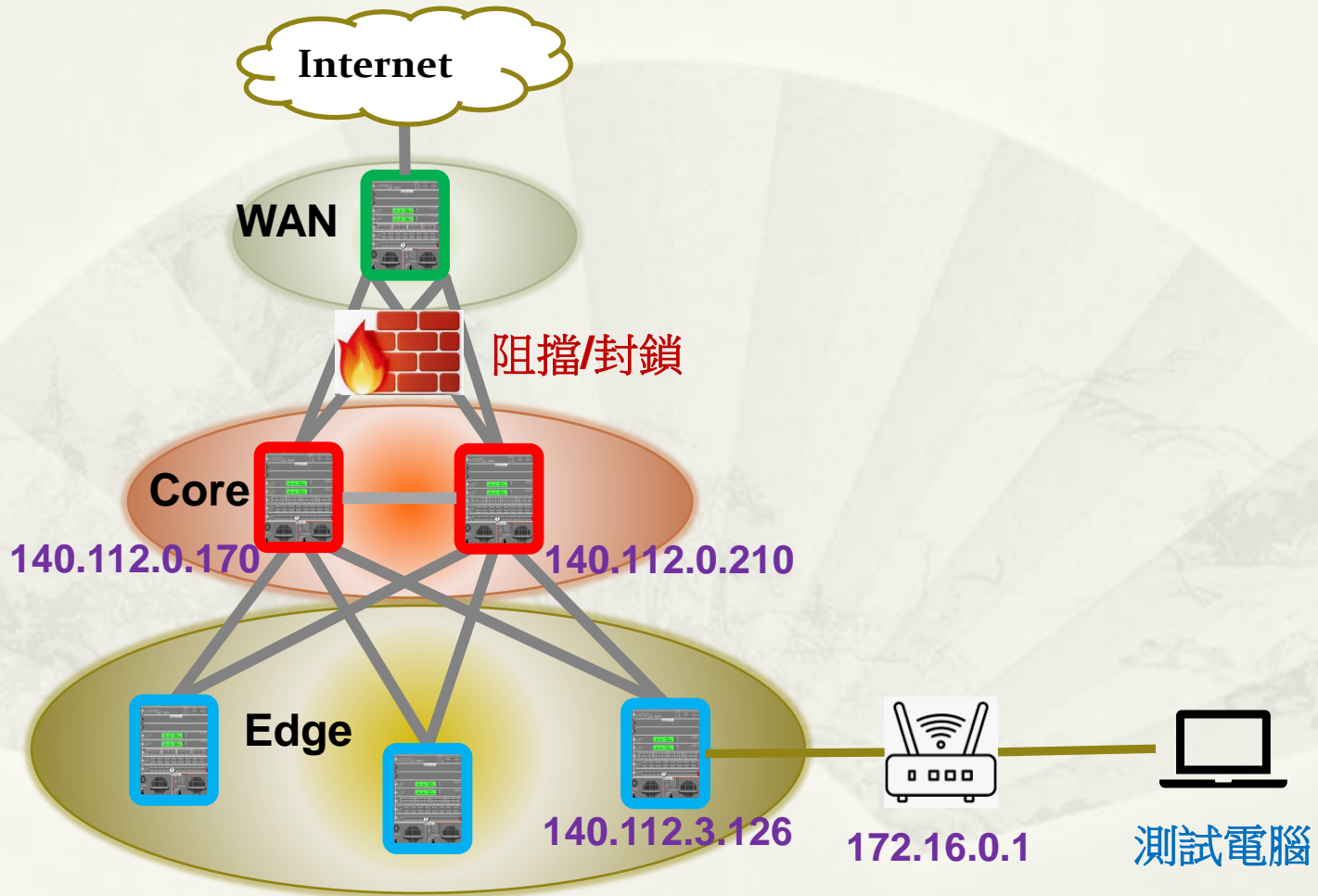
- * 誤判

- * 可能該黑名單 IP 不回應 ping 或 暫時離線關機，而非被資安設備阻擋。

- * 解決方法

- * 使用 TraceRoute 判斷封包丟棄節點

網路架構



利用 TraceRoute 偵測

黑名單 IP: 141.98.212.30

- * 進行封鎖之資安設備位於 Core to WAN 之間
- * Node 3 ~ 4

```
C:\Users\user>tracert -d 141.98.212.30
在上限 30 個躍點上追蹤 141.98.212.30 的路由

 1  <1 ms    <1 ms    <1 ms    172.16.0.1
 2  <1 ms    <1 ms    <1 ms    140.112.3.126
 3  <1 ms    <1 ms    <1 ms    140.112.0.210
 4  *        *        *        要求等候逾時。
 5  *        *        *        要求等候逾時。
 6  *        *        *        要求等候逾時。
 7  AC
```

非黑名單 IP: 141.98.212.31

- * 可順利通過 Node 4 以上

```
C:\Users\user>tracert -d 141.98.212.31
在上限 30 個躍點上追蹤 141.98.212.31 的路由

 1  <1 ms    <1 ms    <1 ms    172.16.0.1
 2  <1 ms    <1 ms    <1 ms    140.112.3.126
 3  <1 ms    <1 ms    <1 ms    140.112.0.170
 4  1 ms     1 ms     1 ms     140.112.0.206
 5  3 ms     1 ms     1 ms     203.160.226.133
 6  9 ms     9 ms     7 ms     203.78.181.217
 7  32 ms    33 ms    32 ms    175.41.60.90
 8  24 ms    24 ms    24 ms    203.160.225.106
 9  38 ms    40 ms    34 ms    63.218.204.62
10  *        *        *        要求等候逾時。
```

PingPlotter

商用軟體

* <https://www.pingplotter.com/>

黑名單 IP 皆停在 4 Hops

Status	Count	IP	Name	Setting	Avg	Min	Cur	PL%	Hops	Latency
	10	180.215.218.135	180.215.218.135	Default Settings	*			100.0	4	
	10	185.207.155.146	185.207.155.146.static.xtom.c	Default Settings	*			100.0	4	
	10	139.59.247.94	139.59.247.94	Default Settings	*			100.0	4	
	10	13.229.3.203	ec2-13-229-3-203.ap-southe	Default Settings	*			100.0	4	
	10	103.179.243.142	103.179.243.142	Default Settings	*			100.0	4	
	11	110.34.181.166	110.34.181.166.STATIC.KRYPT	Default Settings	*			100.0	4	
	10	156.248.153.167	156.248.153.167	Default Settings	*			100.0	4	
	11	60.205.0.192	60.205.0.192	Default Settings	*			100.0	4	
	11	156.248.153.181	156.248.153.181	Default Settings	*			100.0	4	
	10	156.248.153.172	156.248.153.172	Default Settings	*			100.0	4	
	10	118.107.25.231	118.107.25.231	Default Settings	*			100.0	4	
	10	14.128.35.26	14.128.35.26	Default Settings	*			100.0	4	
	10	14.128.35.23	14.128.35.23	Default Settings	*			100.0	4	
	10	14.128.35.19	14.128.35.19	Default Settings	*			100.0	4	
	10	118.107.45.189	118.107.45.189	Default Settings	*			100.0	4	
	10	118.107.45.186	118.107.45.186	Default Settings	*			100.0	4	
	10	156.248.153.173	156.248.153.173	Default Settings	*			100.0	4	
	10	38.54.23.18	38.54.23.18	Default Settings	*			100.0	4	
	10	14.128.35.29	14.128.35.29	Default Settings	*			100.0	4	
	10	156.248.153.176	156.248.153.176	Default Settings	*			100.0	4	
	10	14.128.35.28	14.128.35.28	Default Settings	*			100.0	4	
	10	156.248.153.178	156.248.153.178	Default Settings	*			100.0	4	
	10	103.159.132.238	103.159.132.238	Default Settings	*			100.0	4	
	10	103.199.17.184	103.199.17.184	Default Settings	*			100.0	4	
	10	64.176.50.176	64.176.50.176.vultruserconter	Default Settings	*			100.0	4	
	10	101.34.59.52	101.34.59.52	Default Settings	*			100.0	4	

利用 TraceRoute 偵測

黑名單 IP: 141.98.212.30

- * TTL = 3 (Core)

```
C:\Users\user>ping -i 3 141.98.212.30

Ping 141.98.212.30 (使用 32 位元組的資料):
回覆自 140.112.0.210: TTL 在傳輸時到期。
回覆自 140.112.0.210: TTL 在傳輸時到期。
回覆自 140.112.0.210: TTL 在傳輸時到期。
回覆自 140.112.0.210: TTL 在傳輸時到期。
```

- * TTL = 4 (WAN) 無法到達

```
C:\Users\user>ping -i 4 141.98.212.30

Ping 141.98.212.30 (使用 32 位元組的資料):
要求等候逾時。
要求等候逾時。
要求等候逾時。
要求等候逾時。
```

- * TTL = 5 (Internet) 無法到達

```
C:\Users\user>ping -i 5 141.98.212.30

Ping 141.98.212.30 (使用 32 位元組的資料):
要求等候逾時。
要求等候逾時。
要求等候逾時。
要求等候逾時。
```

非黑名單 IP: 141.98.212.31

- * TTL = 3 (Core)

```
C:\Users\user>ping -i 3 141.98.212.31

Ping 141.98.212.31 (使用 32 位元組的資料):
回覆自 140.112.0.170: TTL 在傳輸時到期。
回覆自 140.112.0.170: TTL 在傳輸時到期。
回覆自 140.112.0.170: TTL 在傳輸時到期。
回覆自 140.112.0.170: TTL 在傳輸時到期。
```

- * TTL = 4 (WAN) 順利到達

```
C:\Users\user>ping -i 4 141.98.212.31

Ping 141.98.212.31 (使用 32 位元組的資料):
回覆自 140.112.0.206: TTL 在傳輸時到期。
回覆自 140.112.0.206: TTL 在傳輸時到期。
回覆自 140.112.0.206: TTL 在傳輸時到期。
回覆自 140.112.0.206: TTL 在傳輸時到期。
```

- * TTL = 5 (Internet) 順利到達

```
C:\Users\user>ping -i 5 141.98.212.31

Ping 141.98.212.31 (使用 32 位元組的資料):
回覆自 203.160.226.133: TTL 在傳輸時到期。
回覆自 203.160.226.133: TTL 在傳輸時到期。
回覆自 203.160.226.133: TTL 在傳輸時到期。
回覆自 203.160.226.133: TTL 在傳輸時到期。
```




PINGINFOVIEW

免費軟體

IP 黑名單

File -> Ping Options

Ping Options

Addresses list to ping:

- 180.215.218.135
- 185.207.155.146
- 139.59.247.94
- 8.8.8.8

IP 黑名單

也可直接編輯檔案 PingInfoView_hosts.txt

Ping Timeout (in ms): 1000 Ping Size (in bytes): 32

Ping again every... 30 seconds

Remember addresses list

Use IP-Host Description format

Start pinging immediately without displaying this dialog-box

Resolve host name to IP address on every ping

Use IP Options: Time To Live: 4 Don't Fragment

大於 4 ~ TAnet 內部最遠節點 皆可

結果

* 正常阻擋

* Reply IP Address: 空

* Last Ping Status: Request Timeout

* 未被阻擋

* Reply IP Address: 非空

* Last Ping Status: TTL Expired In Transit

Host Name	IP Address	Reply IP Address	Succeed Co...	Failed Count	Consecutive F...	Max Consec...	Max Consecuti...	% Failed	Total Sent Pin...	Last Ping Status
140.82.23.214	140.82.23.214		0	1	1	1	2023/12/15 下...	100.00%	1	Request Timeout
64.64.234.24	64.64.234.24		0	1	1	1	2023/12/15 下...	100.00%	1	Request Timeout
66.98.126.203	66.98.126.203		0	1	1	1	2023/12/15 下...	100.00%	1	Request Timeout
67.198.130.66	67.198.130.66		0	1	1	1	2023/12/15 下...	100.00%	1	Request Timeout
8.8.8.8	8.8.8.8	140.112.0.206	0	1	1	1	2023/12/15 下...	100.00%	1	TTL Expired In Transit

PINGINFOVIEW

DNS 黑名單

File -> Ping Options

Ping Options

Addresses list to ping:

```
ivibers.com  
drive.zolik.com  
acc.microsoftonetravel.com  
online.msdnupdate.com  
www.ntu.edu.tw  
www.buda.idv.tw|
```

DNS 黑名單

也可直接編輯檔案 `PingInfoView_hosts.txt`

結果

* 正常阻擋

- * IP Address: 空

- * Last Ping Status: Bad Host name

* 未被阻擋

- * IP Address: 非空 (順利解出 IP)

Host Name	IP Address	Reply IP Address	Succeed Co...	Failed Count	Consecutive F...	Max Consec...	Max Consecuti...	% Failed	Total Sent Pin...	Last Ping Status
acc.microsoftonetravel.com			0	1	1	1	2023/12/15 下...	100.00%	1	Bad Host Name
drive.zolik.com			0	1	1	1	2023/12/15 下...	100.00%	1	Bad Host Name
ivibers.com			0	1	1	1	2023/12/15 下...	100.00%	1	Bad Host Name
online.msdnupdate.com			0	1	1	1	2023/12/15 下...	100.00%	1	Bad Host Name
www.buda.idv.tw	125.229.210.102		0	1	1	1	2023/12/15 下...	100.00%	1	Request Timeout
www.ntu.edu.tw	140.112.8.116	140.112.8.116	1	0				0%	1	Succeeded

解析出 內網/虛擬 IP 網段?

* Why 解析出

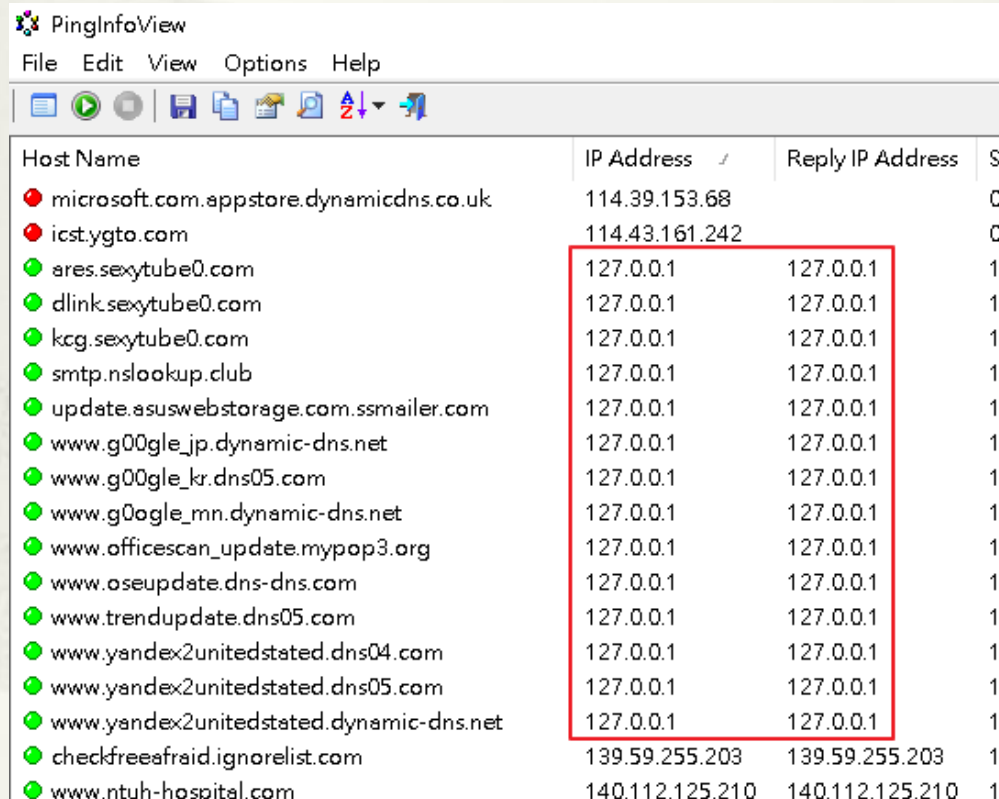
* 127.0.0.1

* 192.168.x.x

* 172.16.x.x

* 原因

* 駭客為避免暴露伺服器 IP 位址，暫時使用特殊用途網段



Host Name	IP Address	Reply IP Address
microsoft.com.appstore.dynamicdns.co.uk	114.39.153.68	
icst.ygto.com	114.43.161.242	
ares.sexytube0.com	127.0.0.1	127.0.0.1
dlink.sexytube0.com	127.0.0.1	127.0.0.1
kcg.sexytube0.com	127.0.0.1	127.0.0.1
smtp.nsllookup.club	127.0.0.1	127.0.0.1
update.asuswebstorage.com.ssmailer.com	127.0.0.1	127.0.0.1
www.google.jp.dynamic-dns.net	127.0.0.1	127.0.0.1
www.google.kr.dns05.com	127.0.0.1	127.0.0.1
www.google.mn.dynamic-dns.net	127.0.0.1	127.0.0.1
www.officescan_update.mypop3.org	127.0.0.1	127.0.0.1
www.oseupdate.dns-dns.com	127.0.0.1	127.0.0.1
www.trendupdate.dns05.com	127.0.0.1	127.0.0.1
www.yandex2unitedstated.dns04.com	127.0.0.1	127.0.0.1
www.yandex2unitedstated.dns05.com	127.0.0.1	127.0.0.1
www.yandex2unitedstated.dynamic-dns.net	127.0.0.1	127.0.0.1
checkfreeafraid.ignorelist.com	139.59.255.203	139.59.255.203
www.ntuh-hospital.com	140.112.125.210	140.112.125.210

簡報完畢
謝謝