114年度第一次
台北區網(臺大)網管會議
https://reurl.cc/eMnxA7

臺灣大學計資中心
游子興
davisyou@ntu.edu.tw
3366-5008

會議議程

項目	時 間	報告人	報 告 內 容
主席報告	14:00~14:05	謝宏昀教授	
業務報告	14:05~14:20	游子興	區網營運業務報告
	14:20~14:40	史詩妤	資安事件相關說明
	14:40~15:00	李美雯	資安案例分享
專題演講	15:00~15:30	連線單位分享: 空中大學樂可強	本校資通安全與 個資管理推動現況
	15:40~16:10	陳思蘊	IoT 物聯網設備風險現況與防範策略
	16:10~17:00	游子興	DNS Sinkhole & RPZ 運作原理與實際應用
臨時動議		出列席人員2	

臺灣學術網路 400G 專案

- 臺灣學術網路 100G 骨幹網路汰換案已於 113 年 10 月由遠傳電信得標，並已開始進行各區網中心機房及機櫃相關設備的場勘作業。
- 本案預計於 114 年完成建置驗收後，將從原 100G 骨幹網路切換至 400G，以提升網路傳輸能力與效能。

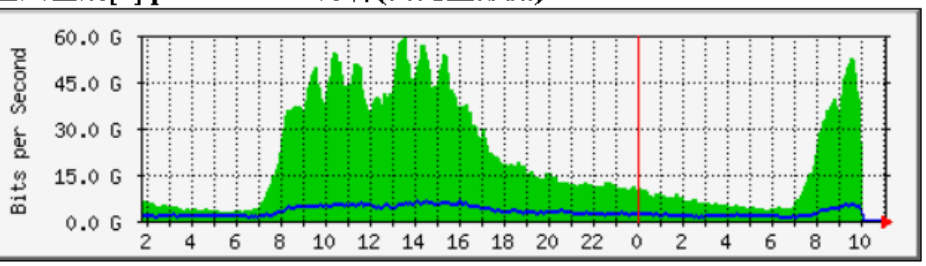
機櫃編號	A12				A11				A10	
U	NTU#01(RDM_R01)	耗電	重量	插頭	U	NTU#02(TAN_R01)	耗電	重量	插頭	U	NTU#03(TWA_R01)
42	既有佔用				42	既有佔用				42	既有佔用
41	既有佔用				41	既有佔用				41	既有佔用
40	既有佔用				40	既有佔用				40	既有佔用
39					39	ODF 48C(LC)				39	ODF 48C(LC)
38					38	ODF 48C(LC)				38	ODF 48C(LC)
37	TT-NTU-NCS2015-01	1101	30	4	37	RJ45 Panel 24P				37	TW-NTU-C93180YC-01
36					36	理線槽				36	理線槽
35					35	TA-NTU-C93180YC-01	375	9.5	2	35	TW-NTU-C93180YC-02
34					34	理線槽				34	理線槽
33			10		33	TA-NTU-C93180YC-02	375	9.5	2	33	TW-NTU-C93180YC-03
32					32	理線槽				32	理線槽
31	TT-NTU-NCS2K-MF-6RU=(背後)				31	TA-NTU-C93180YC-03	375	9.5	2	31	TW-NTU-C93180YC-04
30					30	理線槽				30	理線槽
29					29	TA-NTU-C93180YC-04	375	9.5	2	29	TT-NTU-NPBSW
28					28	理線槽				28	理線槽
27					27	TA-NTU-C8200L	85	4.5	2	27	TT-NTU-NPBNF
26					26	理線槽				26	TT-NTU-NPBVR(R360)
25					25	TA-NTU-MOXA	20	3.6	2	25	TW-NTU-C8200L
24					24	理線槽				24	理線槽
23	托盤				23	TA-NTU-C9200	62	5.2	2	23	TW-NTU-MOXA
22	TT-NTU-NCS2015-02	1516	30	4	22	理線槽				22	理線槽
21					21					21	TW-NTU-C9200-01
20					20					20	理線槽
19					19					19	TW-NTU-C9200-02
18	TT-NTU-15216-EF-40-ODD(背後)		6.6		18					18	理線槽
17					17					17	
16	TT-NTU-15216-EF-40-ODD(背後)		6.6		16	TA-NTU-8608-01	1196	41	4	16	TW-NTU-8608-01
15					15					15	
14	TT-NTU-NCS2K-MF-1RU=(背		4.5		14					14	
13	TT-NTU-NCS2K-MF-1RU=(背		4.5		13					13	
12					12					12	
11					11					11	
10					10					10	
9				2	9					9	
8	托盤			2	8	TA-NTU-8608-02	1196	41	4	8	TW-NTU-8608-02
7				2	7					7	
6	PowerEdge R760	750	36	2	6					6	
5	NTS 他案設備				5					5	
4				2	4					4	
3					3					3	
2				2	2					2	
1			75		1			75		1	
	NTU#01(RDM_R01)	3367	203	20		NTU#02(TAN_R01)	4059	208.3	22		NTU#03(TWA_R01)

區網對外連線異常

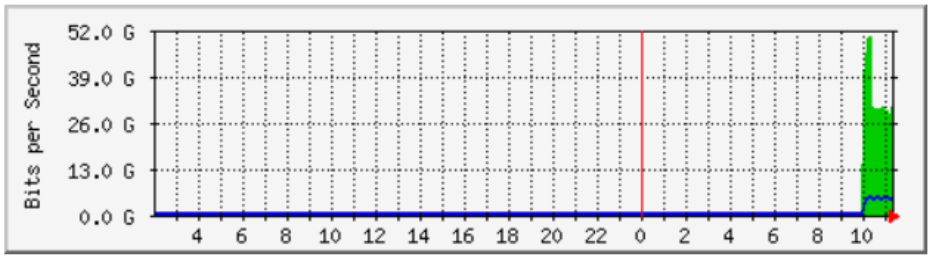
- 2025/05/06 14:30 ~ 14:40
  - 因北區 ASOC IPS FMC 發生異常，將分流器切換成 Bypass 後恢復正常
- 2025/05/10 20:35
  - 將 IPS 切回 Inline

2025/02/25
臺北主節點光纖中斷

臺大區網[1]ipv4 -- TANet骨幹(台北主節點)

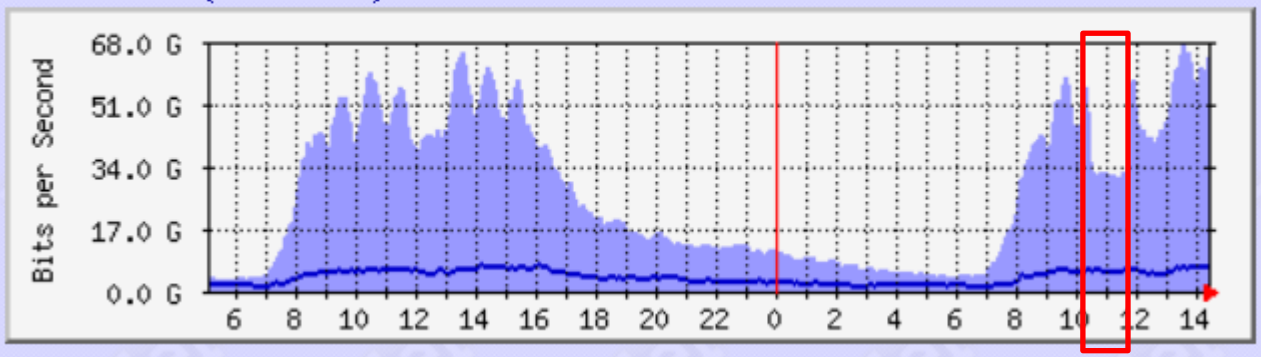


臺大區網[2]ipv4 -- TANet骨幹(新竹主節點)



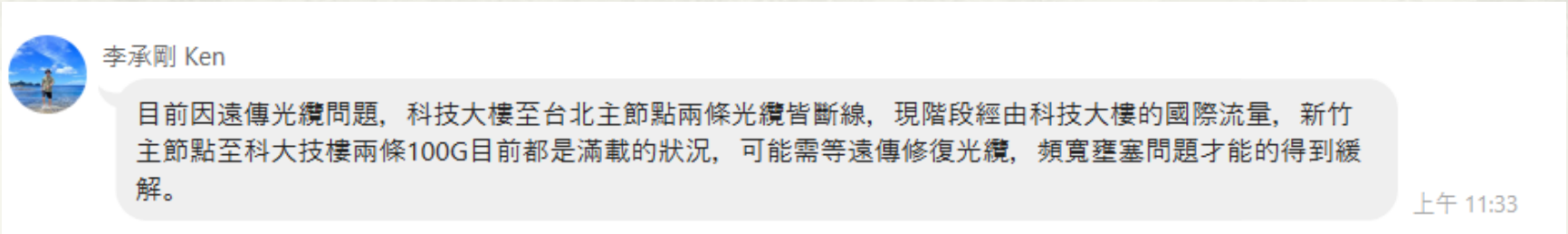
	Max	Average	Current
新竹主節點 => 北區區網	50.4 Gb/s (50.4%)	1388.8 Mb/s (1.4%)	30.5 Gb/s (30.5%)
北區區網 => 新竹主節點	5123.9 Mb/s (5.1%)	192.1 Mb/s (0.2%)	4744.0 Mb/s (4.7%)

台北區網 I (台灣大學) --- 主節點



2025/02/25
臺北主節點光纖中斷

* 因遠傳光纜問題，科技大樓至台北主節點兩條光纜皆斷線
* 現階段經由科技大樓的國際流量，新竹主節點至科大技樓兩條100G目前都是滿載的狀況，可能需等遠傳修復光纜，頻寬壅塞問題才能的得到緩解。



.ORG 權威伺服器 IP 被區網 IPS 封鎖

挖礦礦池 黑名單

2025/02/03 北科大反應

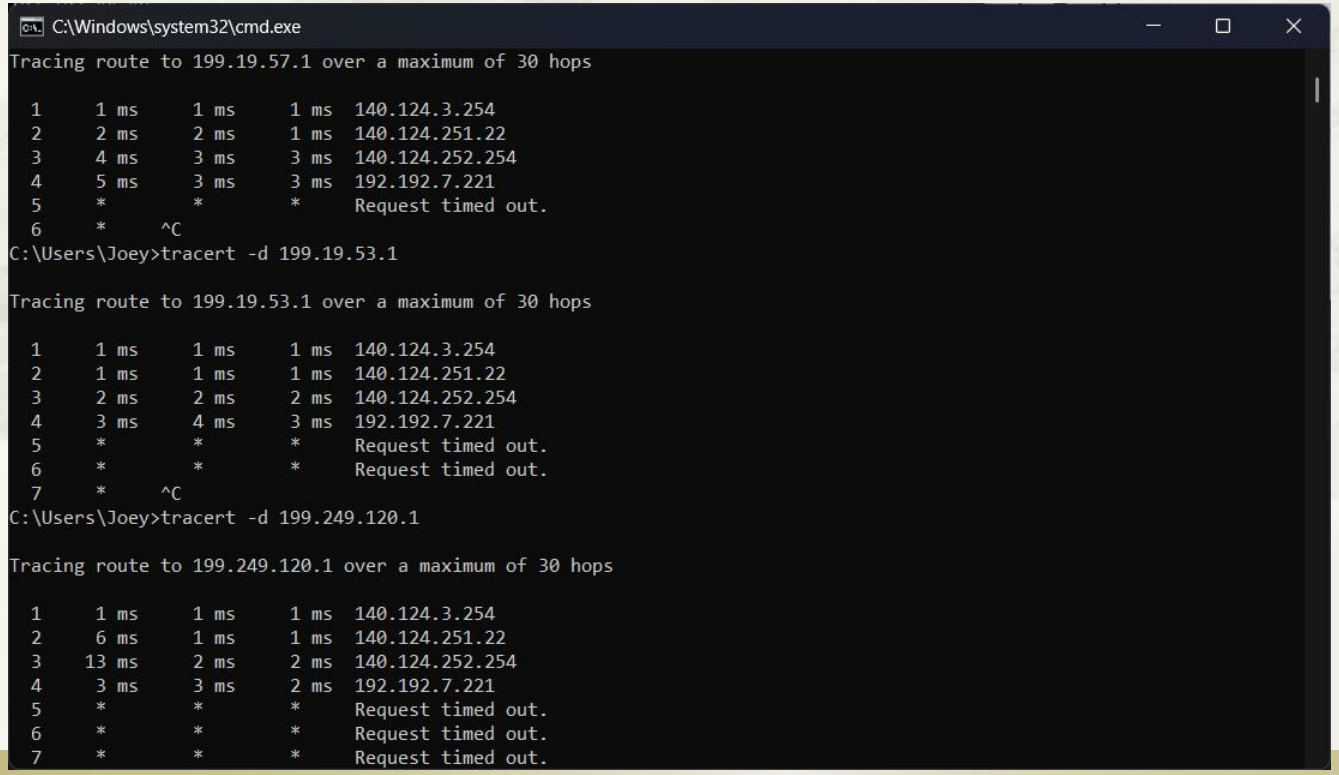
2月3日(一)

Joey Chen

@游子興 子興老師新年快樂，打擾您
https://www.iana.org/domains/root/db/org.html
中org的root server 我們這邊都問不到，traceroute的結果如下，發現過了到台大的PEER IP以後就不回應了，想請問可能的原因，感謝

> **.org Domain Delegation Data**
> Delegation Record for .ORG (Generic top-level domain) Sponsoring Organisation Public Interest Registry (PIR) 11911 Freedom Drive, 10th Floor, Suite 1000 Reston VA 20190 United States of America (the) Administrative Contact Director of Operations, Compliance and Customer Support Public Interest Regis...

下午 2:06



.ORG 權威伺服器 IP

* https://www.iana.org/domains/root/db/org.html

Name Servers

HOST NAME	IP ADDRESS(ES)
a0.org.afilias-nst.info	199.19.56.1 2001:500:e:0:0:0:0:1
a2.org.afilias-nst.info	199.249.112.1 2001:500:40:0:0:0:0:1
b0.org.afilias-nst.org	199.19.54.1 2001:500:c:0:0:0:0:1
b2.org.afilias-nst.org	199.249.120.1 2001:500:48:0:0:0:0:1
c0.org.afilias-nst.info	199.19.53.1 2001:500:b:0:0:0:0:1
d0.org.afilias-nst.org	199.19.57.1 2001:500:f:0:0:0:0:1

.ORG 權威伺服器 IP

```
root@ubuntu24:/tmp# dig +trace mozilla.org

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> +trace mozilla.org
;; global options: +cmd
.                       87203   IN      NS      i.root-servers.net.
.                       87203   IN      NS      j.root-servers.net.
.                       87203   IN      NS      l.root-servers.net.
.                       87203   IN      NS      b.root-servers.net.
.                       87203   IN      NS      d.root-servers.net.
.                       87203   IN      NS      e.root-servers.net.
.                       87203   IN      NS      k.root-servers.net.
.                       87203   IN      NS      h.root-servers.net.
.                       87203   IN      NS      m.root-servers.net.
.                       87203   IN      NS      f.root-servers.net.
.                       87203   IN      NS      g.root-servers.net.
.                       87203   IN      NS      c.root-servers.net.
.                       87203   IN      NS      a.root-servers.net.
;; Received 239 bytes from 127.0.0.53#53(127.0.0.53) in 7 ms

org.                    172800  IN      NS      b0.org.afilias-nst.org.
org.                    172800  IN      NS      a2.org.afilias-nst.info.
org.                    172800  IN      NS      c0.org.afilias-nst.info.
org.                    172800  IN      NS      d0.org.afilias-nst.org.
org.                    172800  IN      NS      a0.org.afilias-nst.info.
org.                    172800  IN      NS      b2.org.afilias-nst.org.
org.                    86400   IN      DS      26974 8 2 4FEDE294C53F438A
org.                    86400   IN      RRSIG   DS 8 1 86400 20250216220000
kUYEJInxE7UPjR1NwAvtDthsnzmQkVm56p7T2KIbkxnhAuQMHsTfef 4Pz2C3avVjpRut3HsX7
lmsUDNsc5E jNrr0JjWtrQ9UTFwurLmHTutEKKJjFy52zCnPpiKtoIBcA15DAM5YKGm L6aW5/
;; Received 808 bytes from 192.33.4.12#53(c.root-servers.net) in 62 ms

; communications error to 199.19.54.1#53: timed out
; communications error to 199.19.54.1#53: timed out
; communications error to 199.19.54.1#53: timed out
```

2025/02/03 IPS 新增黑名單

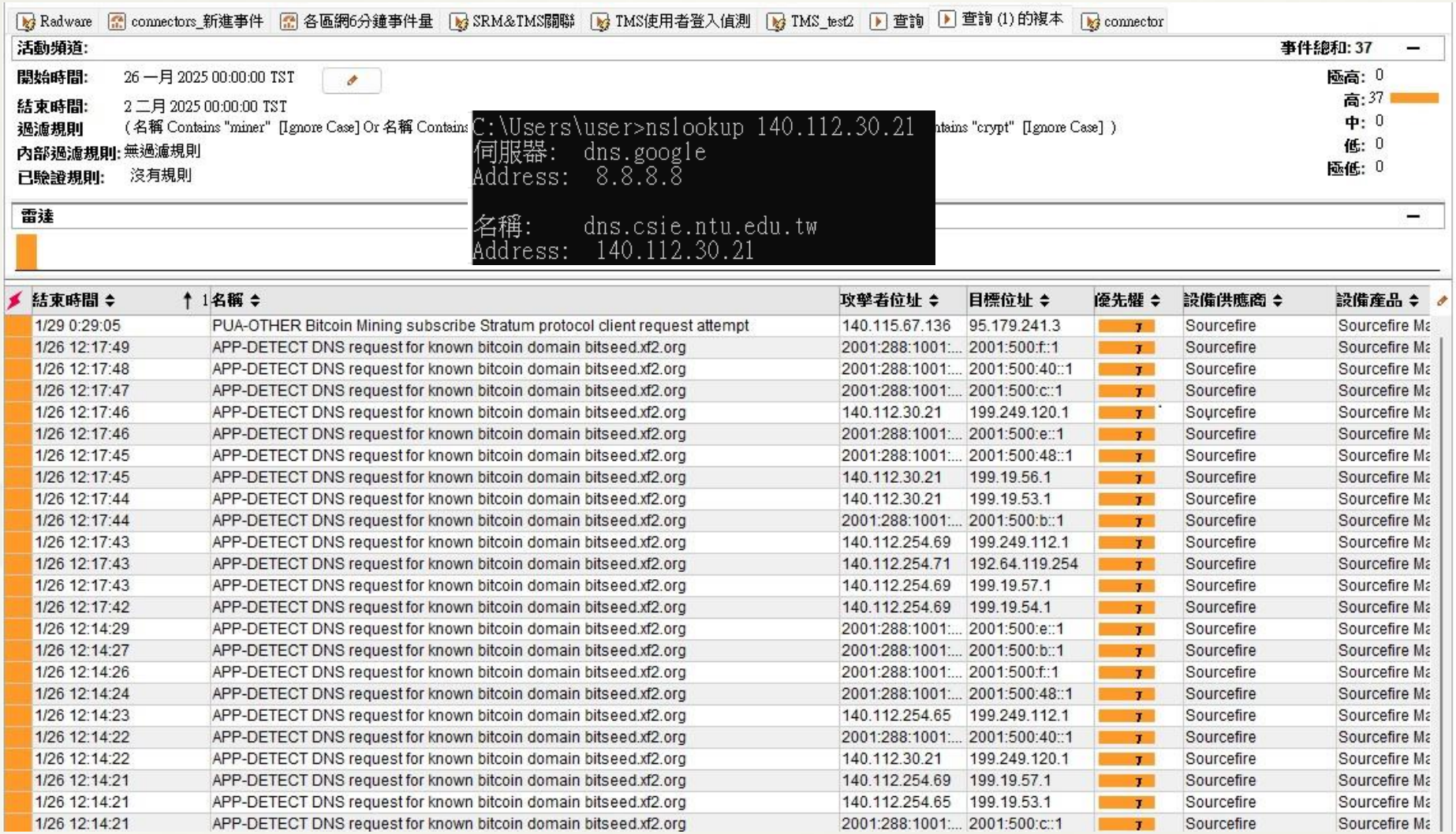
```
#20250203 update
199.249.120.1
199.249.112.1
199.19.56.1
199.19.53.1
199.19.54.1
199.19.57.1
192.64.119.254
95.179.241.3
```

Root Cause

- https://snort.org/rule_docs/1-30853
- alert udp $HOME_NET any -> any 53 (msg:"APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org"; flow:to_server; byte_test:1,!&,0xF8,2; content:"|07|bitseed|03|xf2|03|org|00|"; fast_pattern:only; metadata:service dns; classtype:policy-violation; sid:30853; rev:3; gid:1;)

- 所有挖礦事件之 Dest IP 皆列為黑名單
- Case1: Client -> DNS Resolver
  - 168.95.1.1
  - 8.8.8.8
- Case2: DNS Resolver -> Authoritative DNS
  - .org Authoritative DNS server IP 會被列入黑名單
  - .xf2.org Authoritative DNS server IP 會被列入黑名單

Root Cause



結束時間	名稱	攻擊者位址	目標位址	優先權	設備供應商	設備產品
1/29 0:29:05	PUA-OTHER Bitcoin Mining subscribe Stratum protocol client request attempt	140.115.67.136	95.179.241.3	7	Sourcefire	Sourcefire Ma
1/26 12:17:49	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:f::1	7	Sourcefire	Sourcefire Ma
1/26 12:17:48	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:40::1	7	Sourcefire	Sourcefire Ma
1/26 12:17:47	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:c::1	7	Sourcefire	Sourcefire Ma
1/26 12:17:46	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.30.21	199.249.120.1	7	Sourcefire	Sourcefire Ma
1/26 12:17:46	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:e::1	7	Sourcefire	Sourcefire Ma
1/26 12:17:45	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:48::1	7	Sourcefire	Sourcefire Ma
1/26 12:17:45	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.30.21	199.19.56.1	7	Sourcefire	Sourcefire Ma
1/26 12:17:44	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.30.21	199.19.53.1	7	Sourcefire	Sourcefire Ma
1/26 12:17:44	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:b::1	7	Sourcefire	Sourcefire Ma
1/26 12:17:43	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.69	199.249.112.1	7	Sourcefire	Sourcefire Ma
1/26 12:17:43	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.71	192.64.119.254	7	Sourcefire	Sourcefire Ma
1/26 12:17:43	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.69	199.19.57.1	7	Sourcefire	Sourcefire Ma
1/26 12:17:42	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.69	199.19.54.1	7	Sourcefire	Sourcefire Ma
1/26 12:14:29	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:e::1	7	Sourcefire	Sourcefire Ma
1/26 12:14:27	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:b::1	7	Sourcefire	Sourcefire Ma
1/26 12:14:26	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:f::1	7	Sourcefire	Sourcefire Ma
1/26 12:14:24	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:48::1	7	Sourcefire	Sourcefire Ma
1/26 12:14:23	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.65	199.249.112.1	7	Sourcefire	Sourcefire Ma
1/26 12:14:22	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:40::1	7	Sourcefire	Sourcefire Ma
1/26 12:14:22	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.30.21	199.249.120.1	7	Sourcefire	Sourcefire Ma
1/26 12:14:21	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.69	199.19.57.1	7	Sourcefire	Sourcefire Ma
1/26 12:14:21	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	140.112.254.65	199.19.53.1	7	Sourcefire	Sourcefire Ma
1/26 12:14:21	APP-DETECT DNS request for known bitcoin domain bitseed.xf2.org	2001:288:1001:...	2001:500:c::1	7	Sourcefire	Sourcefire Ma

如何避免誤判 1

- Hit 次數統計
  - 若真的是惡意 IP，連線次數應不會很高
  - 若過高表示很多人在連線，可能是誤判

如何避免誤判 2

- https://www.shodan.io/host/199.19.56.1
- IP 反解名稱
  - Google Search
  - VirusTotal
    - https://www.virustotal.com/gui/domain/c0.org.afilias-nst.org
  - .org 的 name server


```
S:\>nslookup
預設伺服器:  dns.google
Address:  8.8.8.8

> set type=ns
> org
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
org     nameserver = b0.org.afilias-nst.org
org     nameserver = d0.org.afilias-nst.org
org     nameserver = a2.org.afilias-nst.info
org     nameserver = a0.org.afilias-nst.info
org     nameserver = c0.org.afilias-nst.info
org     nameserver = b2.org.afilias-nst.org
```

```
S:\>nslookup 199.19.53.1
伺服器:  dns.google
Address:  8.8.8.8

名稱:    c0.org.afilias-nst.org
Address:  199.19.53.1


S:\>nslookup 199.19.54.1
伺服器:  dns.google
Address:  8.8.8.8

名稱:    b0.org.afilias-nst.org
Address:  199.19.54.1


S:\>nslookup 199.249.120.1
伺服器:  dns.google
Address:  8.8.8.8

名稱:    b2.org.afilias-nst.org
Address:  199.249.120.1


S:\>nslookup 199.249.112.1
伺服器:  dns.google
```

區網暑期課程

* https://my.ntu.edu.tw/actregister/sessionList.aspx?actID=20252204_06

分類	課程	教室	講題	講者
資安	7/17 14:00~17:00	R106	教育體系滲透測試常見問題與防護	正修科大 洪瑞展兼任講師
AI	7/22 14:00~17:00	R106	AI多代理協作自動會議與安全漏洞掃描	劉得民老師
網路	7/25 14:00~17:00	R106	解碼網路宇宙：網管必備知識與網路異常排除方法	史詩妤、游子興
資安	7/30 14:00~17:00	R212	找出OWASP Juice Shop的漏洞練習	中央大學 許時準組長
資安	8/5 14:00~17:00	R106	網站安全重點防禦 1.網站常見漏洞與案例分享 2.細說 Cookie 之運作原理	陳思蘊、游子興
雲端	8/11 14:00~16:00	R106	Kubernetes 私有雲實作指南：企業 IT 現代化的第一步 **(Free)**	鋐迪資訊 鍾迪資深技術顧問
法規	8/13 14:00~16:00	R106	政府機關導入零信任架構初探 **(Free)**	資誠聯合會計師事務所 黃承漢經理
法規	8/20 14:00~17:00	R106	智慧財產權發展之新趨勢—以校園網路著作權保護與合理使用為中心	陳匡正教授
資安	8/29 14:00~17:00	R106	惡意程式攻防與數位鑑識分析	許晉銘

區網會議主題分享

- 每學期區網會議
- 時間: 0.5 HR (講師費 $1000)
- 可分享主題
  - 資安防護、網路、機房基礎建設、跨校區網路規劃
  - 基礎資料更新現況 - 臺灣學術網路管理規範
- 至連線單位舉行區網會議
  - 交通方便:
    - 捷運可抵達
    - 停車方便
  - 可進行視訊會議
  - 餐點、飲料代訂

區網會議主題分享順序
(每次兩個大學單位)

* 國防大學（復興崗校區）
* 空中大學
* 國防醫學院
* 臺北護理健康大學
* 臺灣藝術大學
* 臺北商業大學
* 銘傳大學
* 實踐大學
* 真理大學
* 大同大學
* 龍華科技大學
* 宏國德霖科技大學
* 亞東科技大學
* 致理科技大學
* 黎明技術學院
* 康寧大學
* 華夏科技大學
* 私立明志科技大學
* 德明財經科技大學
* 法鼓文理學院
* 臺北市立大學
* 臺北基督學院
* 臺灣科技大學
* 東吳大學
* 淡江大學
* 臺北大學
* 臺灣大學醫學院附設醫院
* 臺灣師範大學
* 臺北藝術大學
* 臺北醫學大學
* 台北海洋科技大學
* 臺北科技大學
* 中華科技大學

簡報完畢
謝謝