NEITHNET

剖析內網異常橫向流動行為
以藍隊思維角度及早發現駭客蹤跡

ART

騰 曜 網 路 科 技

橫向移動監控的重要

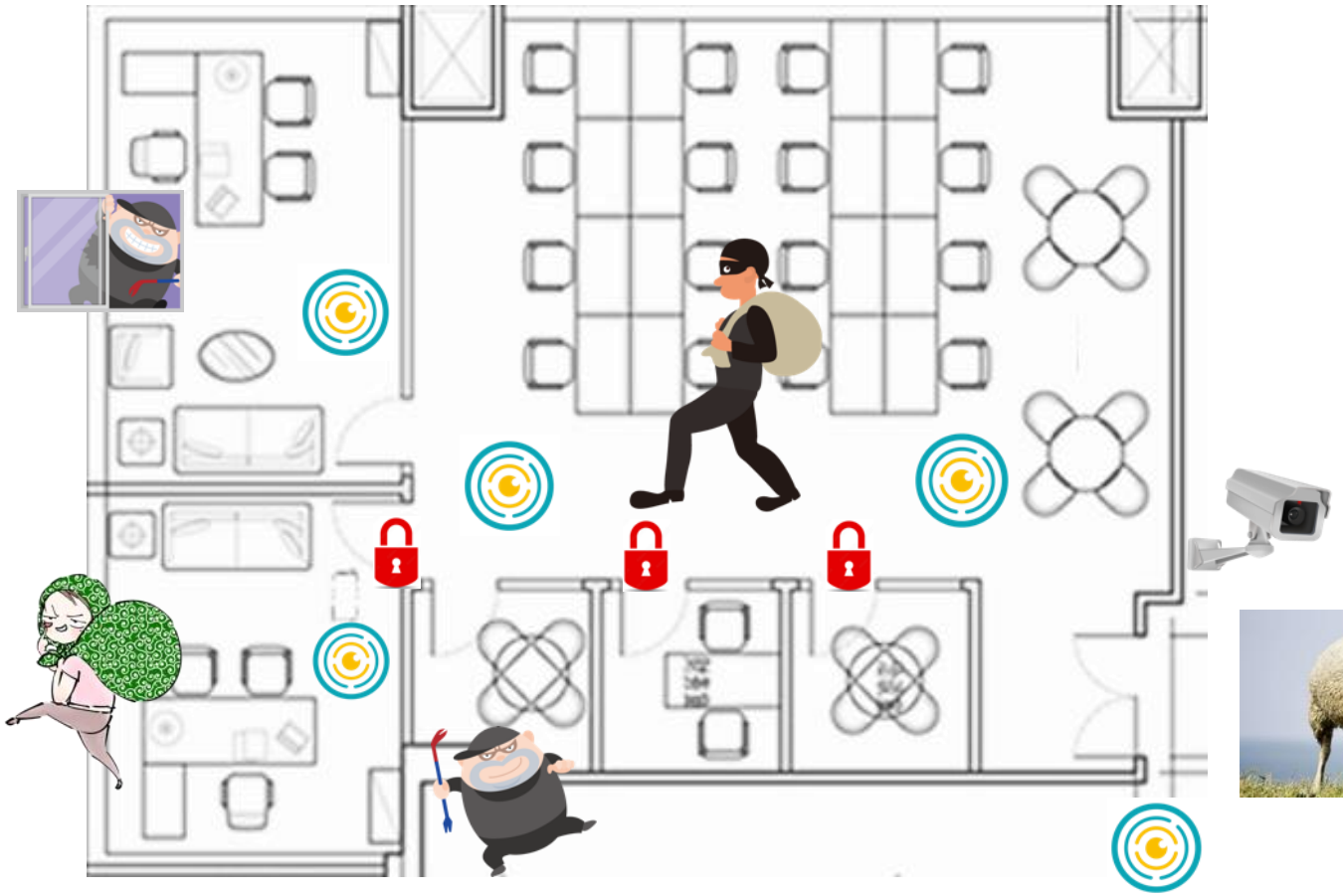
南北向監控遇到的問題

- 加密流量
- 目標發散
- 行為發散

橫向監控的好處

- 異常行為容易定義
- 容易發現駭客行為
- 可提早預防

網路資安 有如辦公室保全



1.端點防護無法完善

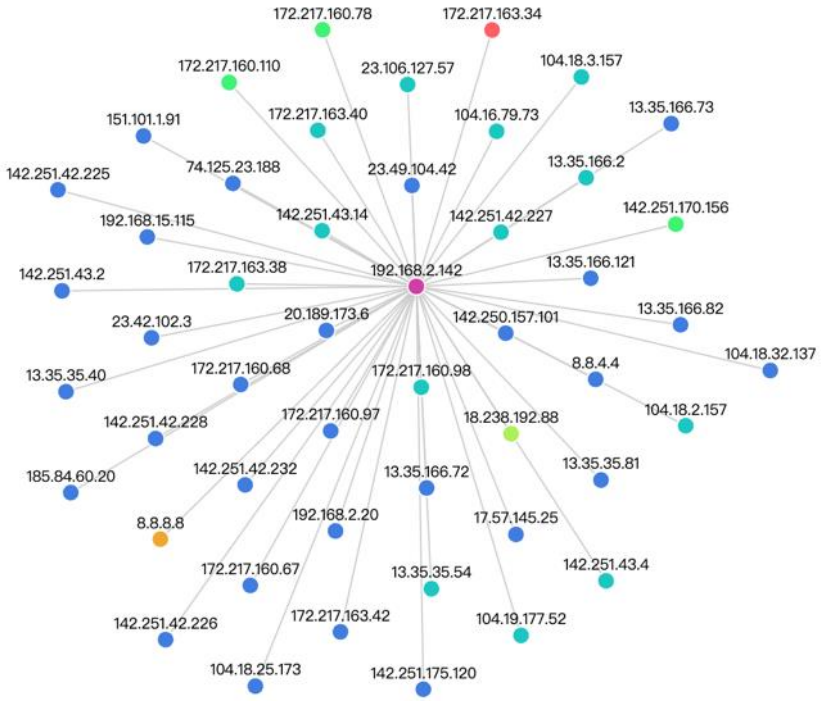
2.惡意活動及早發現

3.凡走過必留痕跡

NEITHViewer 網路監視器

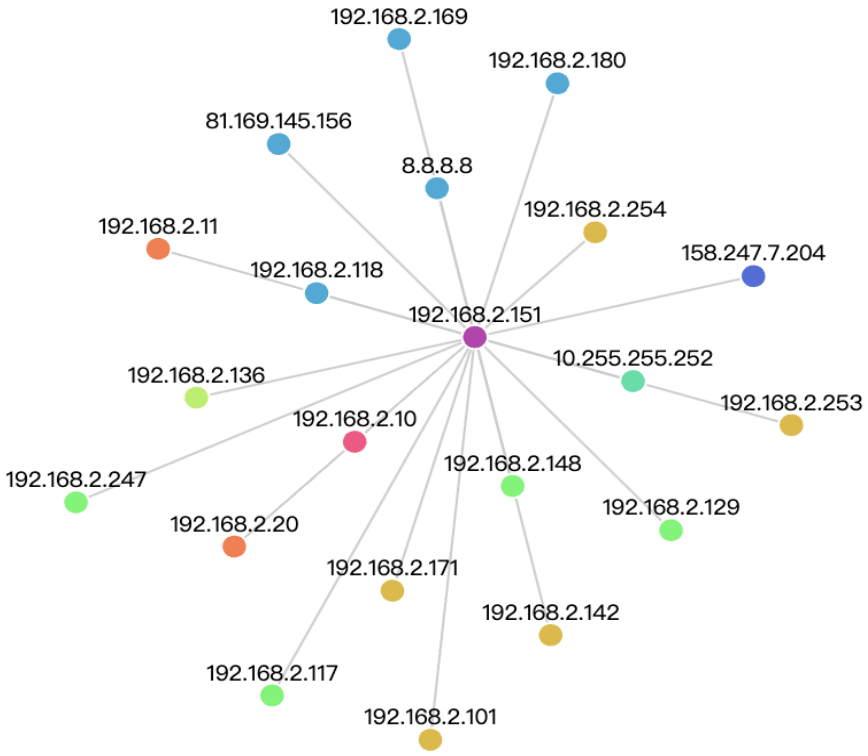
- 重要場所、資產 → 安裝感應器 (EDR/MDR)
- 一般環境 → 監視器監控 (NEITHViewer 網路監視器)
  - 行為異常，通報確認有無問題 (監控告警)
  - 流量異常 (監控告警)
  - 快速發現駭客蹤跡，即時封鎖，避免災害發生

南北向一般上網行為 圖表解說最直接



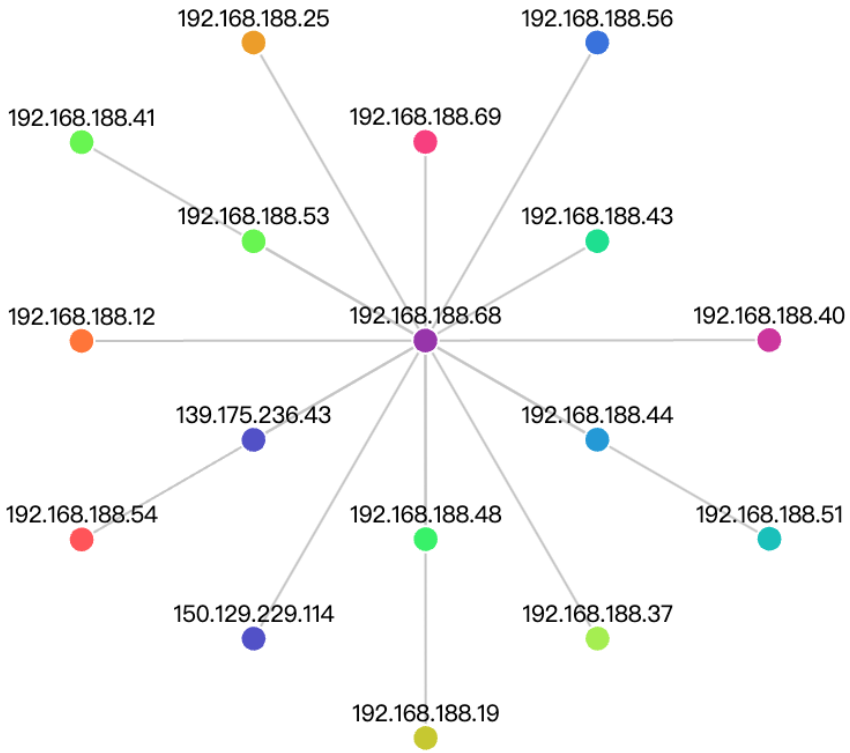
Source IP	Source Hostname	Destination IP	Destination Hostname
192.168.2.142		172.217.163.34	tsa01s13-in-f2.1e100.net
192.168.2.142		8.8.8.8	dns.google
192.168.2.142		18.238.192.88	server-18-238-192-88.sfo53.r.cloudfront.net
192.168.2.142		172.217.160.110	tsa03s06-in-f14.1e100.net
192.168.2.142		172.217.160.78	tsa01s09-in-f14.1e100.net
192.168.2.142		142.251.170.156	tc-in-f156.1e100.net
192.168.2.142		104.16.79.73	
192.168.2.142		23.106.127.57	
192.168.2.142		13.35.166.2	server-13-35-166-2.tpe50.r.cloudfront.net
192.168.2.142		13.35.35.54	server-13-35-35-54.tpe51.r.cloudfront.net

橫向監控 圖表解說最直接



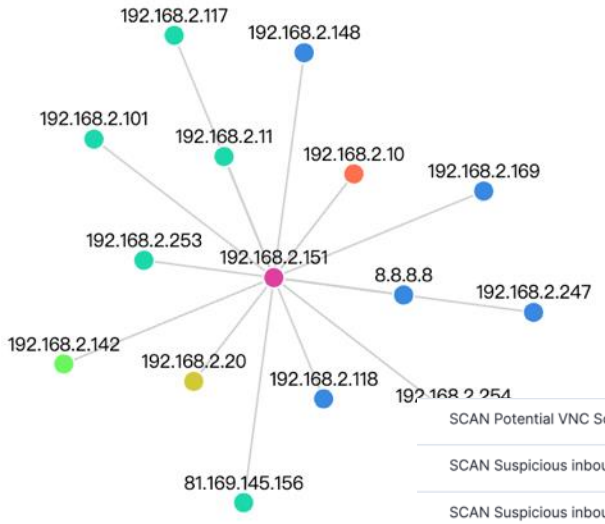
Source IP	Source Hostname	Destination IP	Destination Hostname	Count
192.168.2.151		192.168.2.10		13
192.168.2.151		192.168.2.20		12
192.168.2.151		192.168.2.11		12
192.168.2.151		192.168.2.254		9
192.168.2.151		192.168.2.253		9
192.168.2.151		192.168.2.171		9
192.168.2.151		192.168.2.142		9
192.168.2.151		192.168.2.101		9
192.168.2.151		192.168.2.136	CHT	8
192.168.2.151		192.168.2.117		6

Server 連線型態



signature	source.ip	source.port	destination.ip	destination.p
:Y Windows Update P2P Activit	192.168.188.41	53,677	192.168.188.68	7,680
:Y Windows Update P2P A	192.168.188.41	53,677	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.41	53,672	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.41	53,672	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.53	64,128	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.53	64,128	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.54	52,153	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.54	52,153	192.168.188.68	7,680
:Y Windows Update P2P Activit	192.168.188.69	61,928	192.168.188.68	7,680

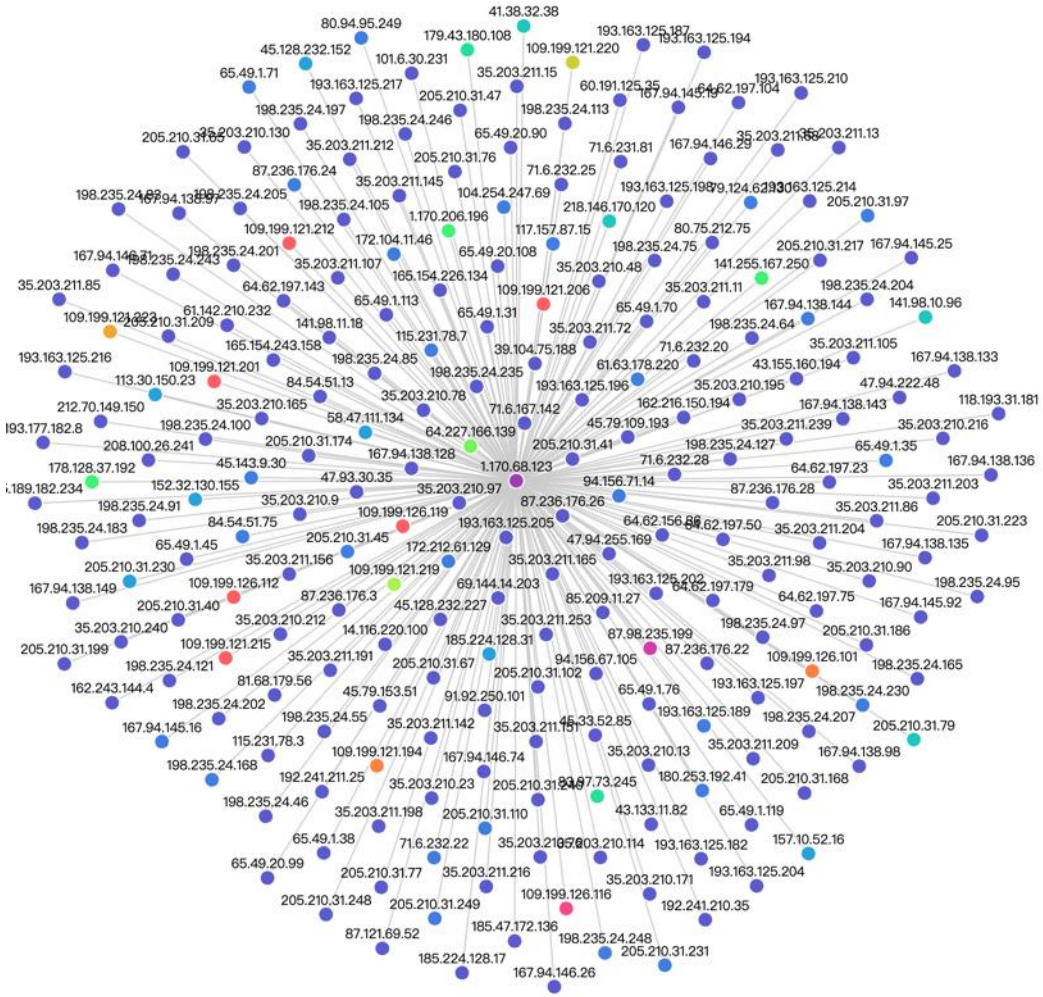
找尋攻擊目標



192.168.2.151	192.168.2.10		7
192.168.2.151	192.168.2.20		4
192.168.2.151	192.168.2.254		3
192.168.2.151	192.168.2.142		3
192.168.2.151	192.168.2.253		2
192.168.2.151	192.168.2.117		2
192.168.2.151	192.168.2.101		2
192.168.2.151	192.168.2.11		2
192.168.2.151	81.169.145.156	w9c.rzone.de	2
192.168.2.151	8.8.8.8	dns.google	1

SCAN Potential VNC Scan 5800-5820	192.168.2.151	49,364	192.168.2.10		5,800
SCAN Suspicious inbound to mySQL port 3306	192.168.2.151	49,336	192.168.2.20		3,306
SCAN Suspicious inbound to MSSQL port 1433	192.168.2.151	49,335	192.168.2.20		1,433
SCAN Suspicious inbound to mySQL port 3306	192.168.2.151	49,336	192.168.2.20		3,306
SCAN Suspicious inbound to MSSQL port 1433	192.168.2.151	49,335	192.168.2.20		1,433
USER_AGENTS Suspicious User Agent (Autoupdate)	192.168.2.151	49,283	81.169.145.156	w9c.rzone.de	80
ADWARE_PUP PUP TheSZ AutoUpdate CnC Beacon	192.168.2.151	49,283	81.169.145.156	w9c.rzone.de	80
INFO Observed Google DNS over HTTPS Domain (dns .google in TLS SNI)	192.168.2.151	49,174	8.8.8.8	dns.google	443
INFO RDP - Response To External Host	192.168.2.151	3,389	192.168.2.142		50,298
INFO RDP - Response To External Host	192.168.2.151	3,389	192.168.2.142		50,298

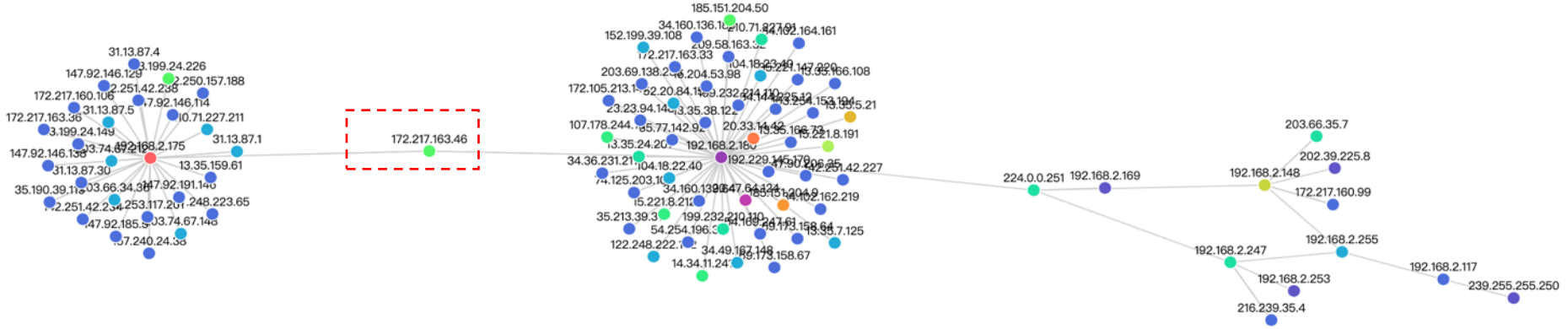
外網攻擊



Source IP	Source Hostname	Destination IP	Destination Hostname	Count
87.98.235.199	ip199.ip-87-98-235.eu	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	232
109.199.126.116	vmi1828531.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	118
109.199.126.119	vmi1828532.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	115
109.199.126.112	vmi1828530.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	115
109.199.121.215	vmi1827542.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	115
109.199.121.212	vmi1827541.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	115
109.199.121.206	vmi1827540.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	115
109.199.121.201	vmi1827539.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	115
109.199.126.101	vmi1828529.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	114
109.199.121.194	vmi1827538.contaboserver.net	1.170.68.123	1-170-68-123.dynamic-ip.hinet.net	114

找出共同點

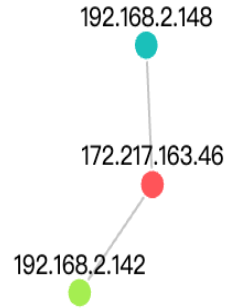
1



2

source.ip	source.hostname	source.port	destination.ip	destination.hostname	destination.por
192.168.2.148		49,414	172.217.163.46	maa05s01-in-f14.1e100.net	443
192.168.2.148		57,522	172.217.163.46	maa05s01-in-f14.1e100.net	443
192.168.2.142		50,165	172.217.163.46	maa05s01-in-f14.1e100.net	80
192.168.2.142		50,165	172.217.163.46	maa05s01-in-f14.1e100.net	80
192.168.2.142		50,166	172.217.163.46	maa05s01-in-f14.1e100.net	443
192.168.2.142		50,166	172.217.163.46	maa05s01-in-f14.1e100.net	443
192.168.2.142		50,164	172.217.163.46	maa05s01-in-f14.1e100.net	80
192.168.2.142		50,164	172.217.163.46	maa05s01-in-f14.1e100.net	80
192.168.2.142		54,804	172.217.163.46	maa05s01-in-f14.1e100.net	443
192.168.2.142		54,804	172.217.163.46	maa05s01-in-f14.1e100.net	443

3



網路偵查的重要 (NEITHViewer)

偵測網路異常行為

- 攻擊 前 的偵測 →不要被駭客攻打進去機器才偵測
- 攻擊 中 的偵測 →當駭客正在攻擊，快速指出根源
- 攻擊 後 的偵測 →檢查是否還有未清除的惡意機器

IT 的困境

老闆要您有紅軍的思維、藍軍的技術

您需要的是

- 藍軍的基本技巧 → 而不是專研
- 有好的工具 → 協助您找出問題
- 強有力的資安顧問 → 作為後盾

資安人員的欠缺 讓專業的來協助您

➢別忘了您原來的工作是什麼 ？

打卡系統有問題、Mail 能不能使用、ERP 系統很慢、網路電話不通、VPN 不能用、網頁打不開、官網打不開、電腦很慢、螢幕打不開、程式不能裝 ……

➢讓專業的來！

資安團隊 → 各種領域怪才

有經驗 → 每天與駭客對抗，研究新的攻擊手法

即時訊息 → 每天來自全世界重要情資資訊，比您更早知道

NEITHNET

感謝聆聽

Thank You for Your Time

騰 曜 網 路 科 技

【填問卷】拿精美好禮

FB

快來社群媒體追蹤我們！

IG