

桃園區網工作報告

呂芳發
104年5月



大綱

- ☐ Tanet及TWAREN新骨幹計畫
- ☐ 資安防護



Tanet及TWAREN新骨幹計畫

□ 計畫緣起

- 為提升國家競爭力，強化國內教育學術研究網路服務，提升我國在國際上之網路基礎環境評比，經行政院國科會第198次委員會議於民國101年7月13日決議，請教育部會同中央研究院與國研院國網中心，擬具完整計畫書並推動

□ 計畫目標

- 完成TANet及TWAREN新一代100G全光網路骨幹基礎建設
- 提供教育學術研究網路分流機制及整體頻寬使用分析管理
- 支援教育雲端運算發展及教育部新一代數位學習計畫
- 骨幹頻寬具有高度使用彈性，可提供研究單位或專案使用點對點的專屬頻寬
- 提升多媒體(Multi-Media)與視訊(Video)的廣泛運用
- 支援政府相關網路應用服務
- 利用先進網路技術，配合國內學術研究需求，建立先進研究及創新的網路平臺與國際研究接軌





100G骨幹網路規劃設計考量

□ 規劃設計考量因素

➤ 參考國外先進研網進行規劃設計臺灣學研網路

- 各國研網均具備可以完全由自己支配使用的光設備及Dark Fiber線路

➤ 電信等級之高品質骨幹傳輸網路

- 骨幹網路可用率達99.98%以上、低網路傳輸延遲及低封包遺失率
- 設備備援性(包含卡板、設備備援性)、線路備援性、整體架構設計具備援性



100G骨幹網路規劃設計考量

□ 規劃設計考量因素

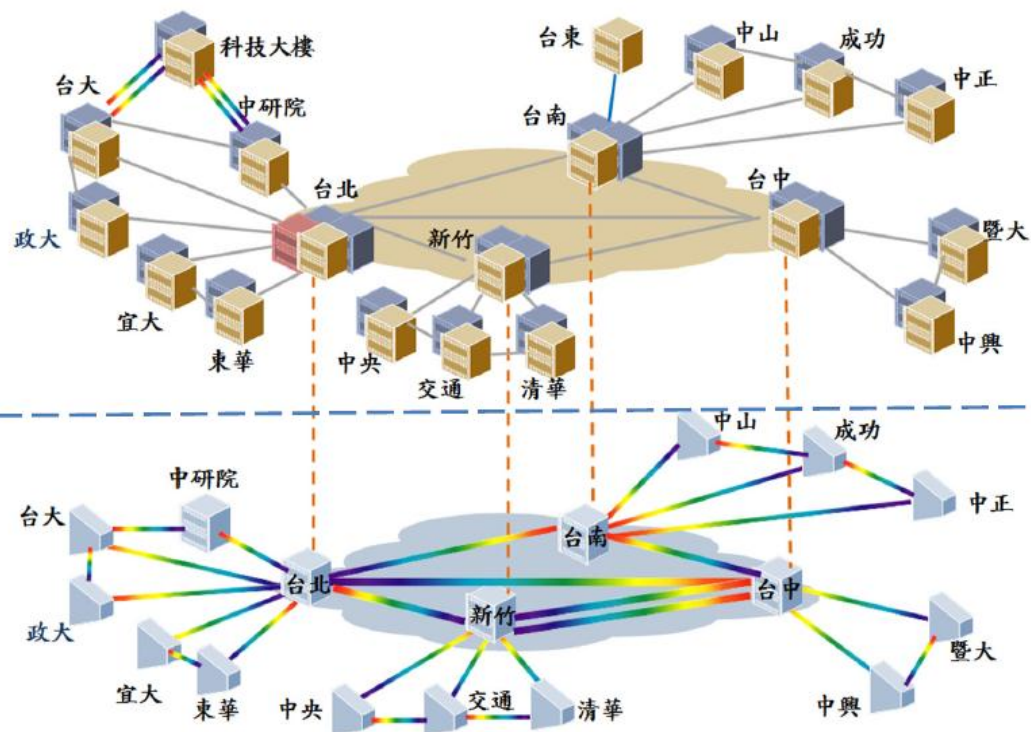
➤ 頻寬彈性調度及未來擴充性

- 僅需採購擴充設備卡板即可達到頻寬擴充
- TANet及TWAREN頻寬可視實際使用需求調度頻寬互相支援

➤ 提供多層次(Multi-Layer)網路服務

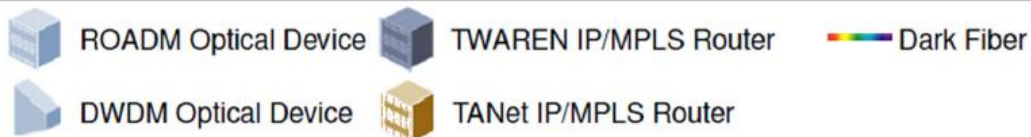
- 提供Layer 0&1點對點專屬大頻寬服務
- 提供Layer2 Multi-point to Multi-point VPN服務、Layer 3 VPN服務
- 提供Layer3 IPv4/IPv6 Internet及Internet2研網路由轉訊(transit)服務
- 新一代骨幹網路完成後能搭配SDN(Software Defined Network)技術與全球學研網路合作，讓國內研究學者能運用100G骨幹參與國際研究計畫

100G網路服務分層示意圖



IP/MPLS骨幹路由交換設備提供
Layer2&Layer3 VPN專屬網路服務)
及IPv4/IPv6 Layer3 Internet及國際
研網路由transit服務

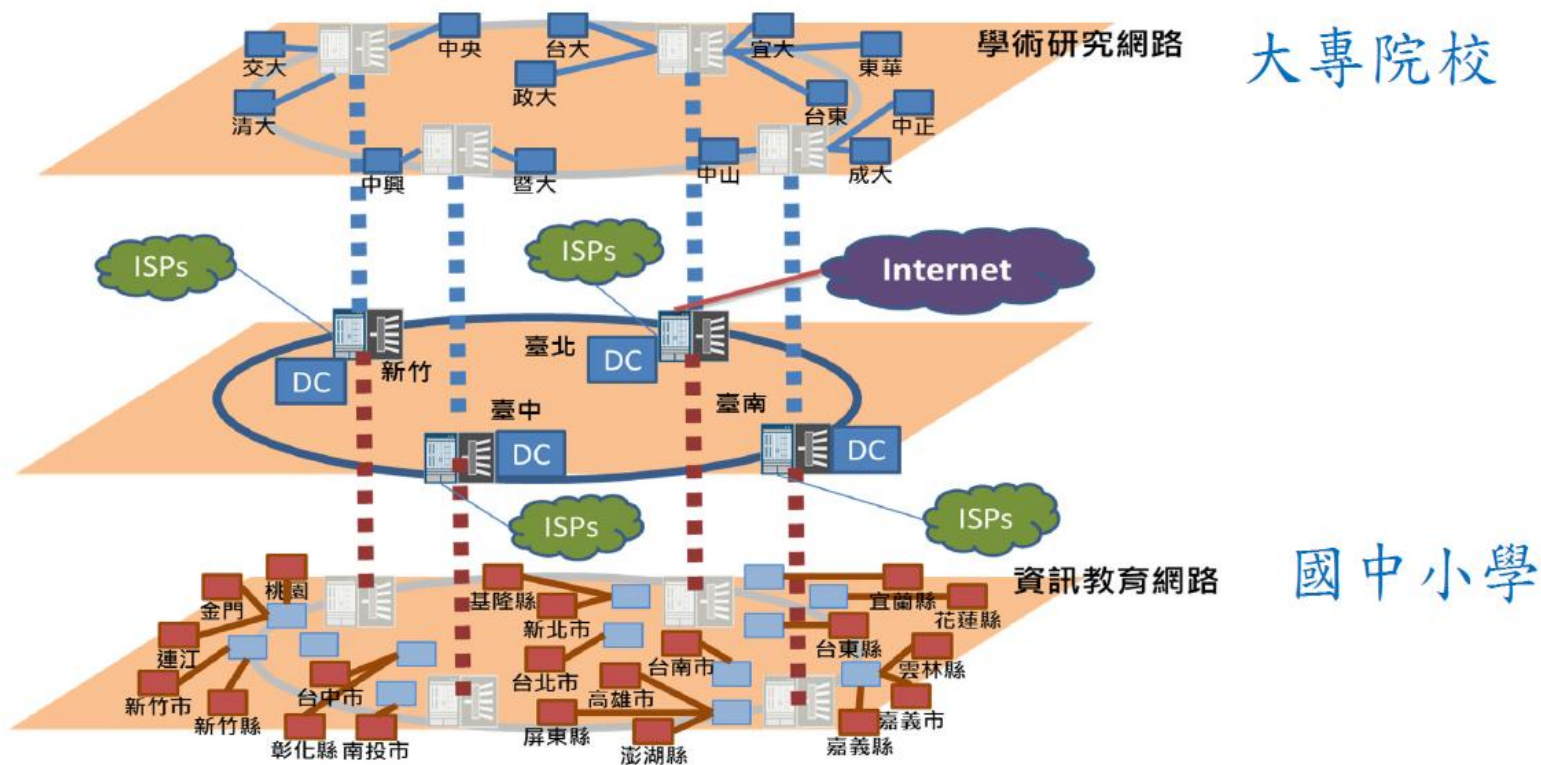
光網路設備透過ROADM(主節點之
間)與DWDM(主節點到GigaPOP)
技術提供專屬 λ 線路服務、點對點
專屬保證頻寬服務



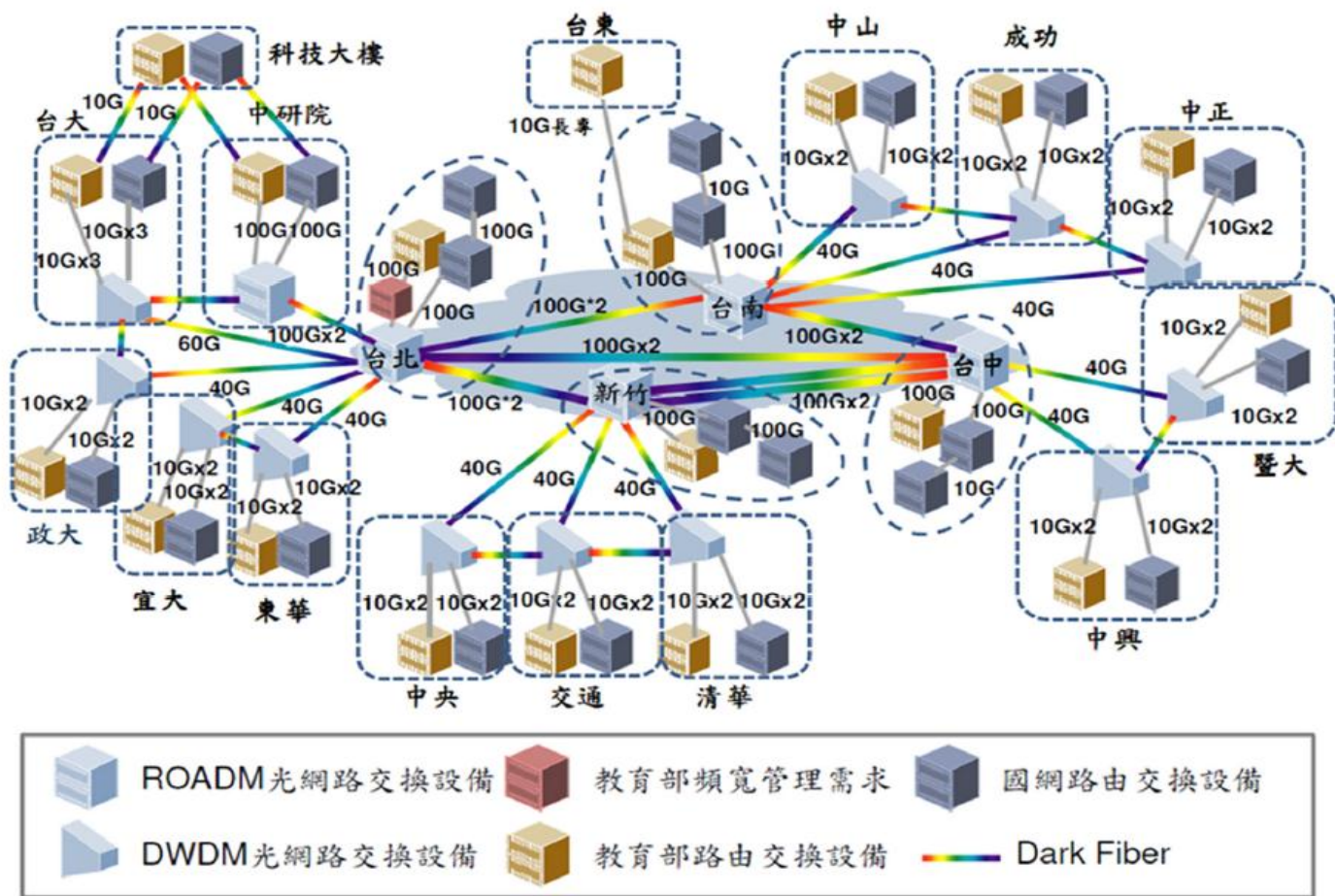


TANet新一代網路管理分流機制

1. 劃分大專院校及國中小學使用網路
2. 彈性使用國中小學離峰時間可規劃提供民眾使用



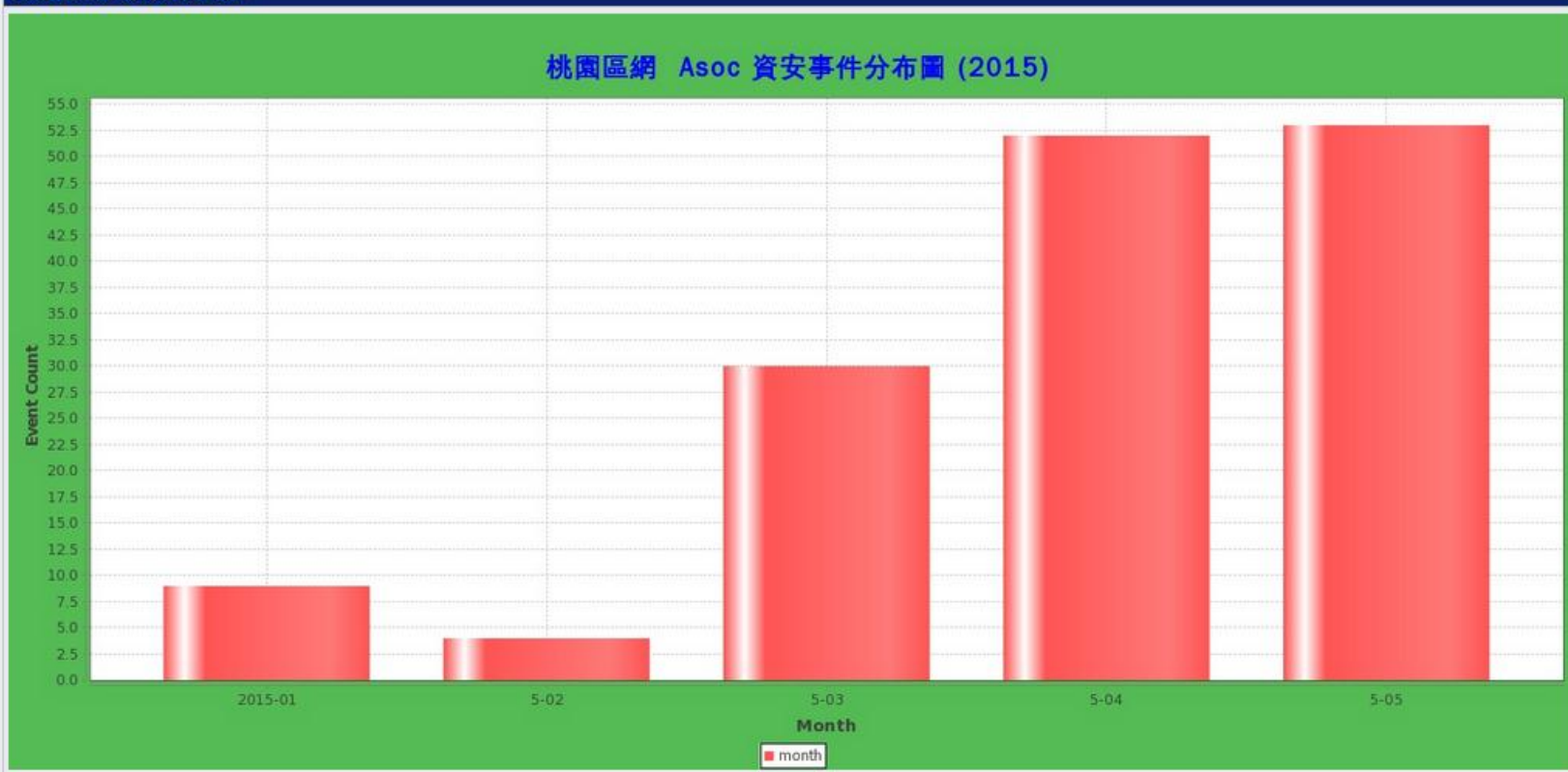
100G教育學術研究網路頻寬需求架構圖



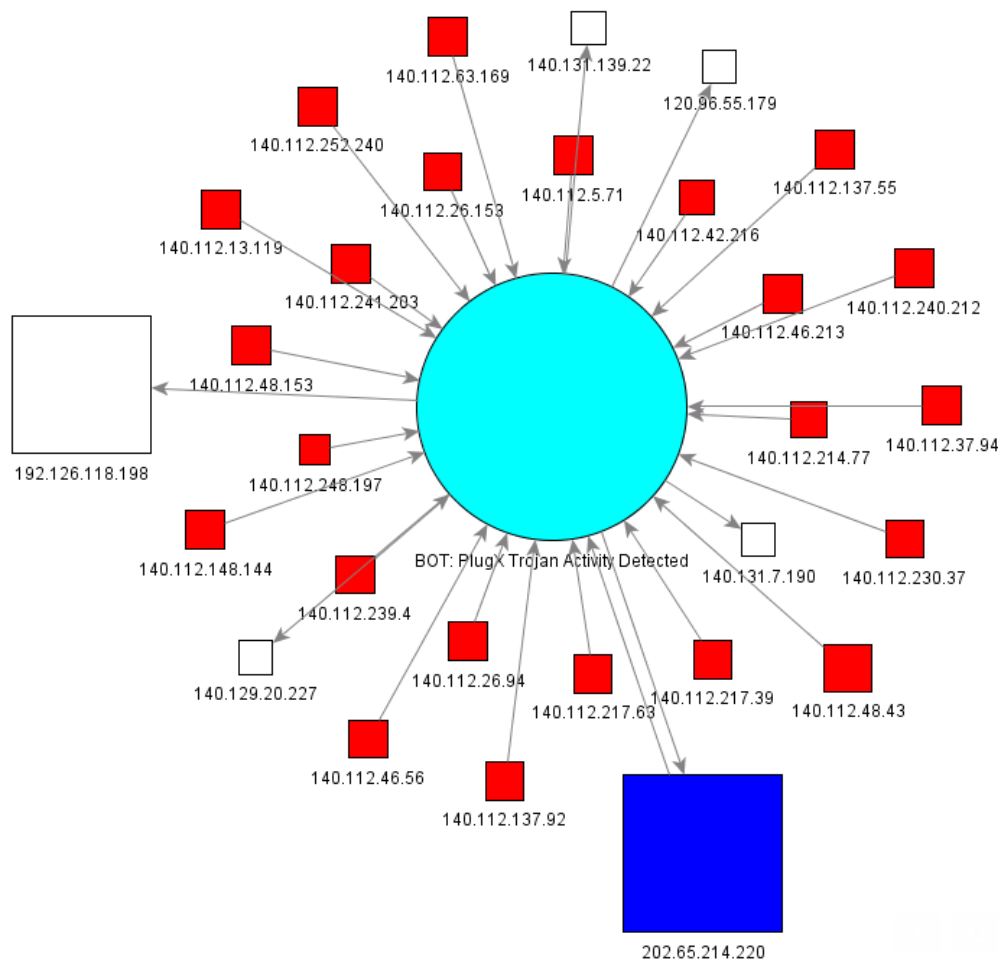


資安通報統計

區網 Asoc 資安事件分布圖



PlugX 木馬程式



✓ 事件偵測說明

- 遠端存取木馬PlugX變種，為103年11月份台北區網最多的資安事件
- 疑似大規模感染
- 北區ASOC針對此惡意程式進行深入分析，透過封包及Sandbox分析，了解此惡意程式感染路徑及影響範圍



PlugX 木馬程式 分析報告 (1/2)

Whois & Quick Stats

Email	sexndomain@gmail.com is associated with ~4 domains	→
Registrant Org	Google Inc. is associated with ~15,607 other domains	→
Dates	Created on 2014-06-05 - Expires on 2015-06-05	→
IP Address	202.65.214.220 - 1 other site is hosted on this server	→
IP Location	🇭🇰 - Hong Kong (sar) - Hong Kong - Diyixian.com Limited	→
ASN	AS9584 GENESIS-AP Diyixian.com Limited,HK (registered Jul 27, 1999)	→
Whois History	6 records have been archived since 2014-08-08	→
Whois Server	whois.twnic.net.tw	

Website

Website Title	None given.	→
---------------	-------------	---

Whois Record (last updated on 2014-12-02)

Domain Name:	playdr2.tw
Registrant:	
	Google Inc.
DNS Admin	sexndomain@gmail.com
	+65.6506234000
	+1.6506188571
	1600 Amphitheatre Parkway Mountain View CA 94043 US
	Kuala Lumpur, Kuala Lumpur
	SG
Administrative Contact:	
DNS Admin	sexndomain@gmail.com
	+65.6506234000
	+1.6506188571

✓ 問題主機之中繼站

- 分析結果顯示，多數感染 PlugX Trojan 主機，皆連向同一 IP 位址 202.65.214.220 傳送特定格式代碼
- 進一步查詢該 IP 註冊區域為香港，並假造 Whois Record 資料，顯示該 IP 為 Google 公司所有

✓ 問題主機連線遊戲公司

- 北區 ASOC 經交叉比對確認感染主機連線之目的 IP 與某網路遊戲公司 IP 相同



PlugX 木馬程式 分析報告 (2/2)

SHA256: 0b41a1bc8d3b6e90c7d62b82b0bf5a496d34292f4d44ad7d1d4e1ceb3ccb46ee

File name: POETWLauncher.exe

Detection ratio: 13 / 55

Analysis date: 2014-12-02 18:38:59 UTC (11 hours, 9 minutes ago)

HKKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\IHM
HKKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKKEY_CURRENT_USER\SOFTWARE\Microsoft\CTF
HKKEY_LOCAL_MACHINE\Software\Microsoft\CTF\SystemShared
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\tmp1.tmp
HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{20D04FE0-3AEA-1069-A2D8-08002B309D}\InProcServer32
HKKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B309D}\InProcServer32
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{475c7950-e3d2-11e0-8d7a-806d6172696f}\
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{475c7952-e3d2-11e0-8d7a-806d6172696f}\
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{475c7952-e3d2-11e0-8d7a-806d6172696f}\
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{475c7950-e3d2-11e0-8d7a-806d6172696f}\
HKKEY_CLASSES_ROOT\Directory
HKKEY_CLASSES_ROOT\Directory\CurVer
HKKEY_CLASSES_ROOT\Directory\CurVer
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKKEY_CLASSES_ROOT\Directory\ShellEx\IconHandler
HKKEY_CLASSES_ROOT\Directory\ShellEx\IconHandler
HKKEY_CLASSES_ROOT\Directory\ShellEx\IconHandler
HKKEY_CLASSES_ROOT\Folder
HKKEY_CLASSES_ROOT\Folder\Clsid
HKKEY_CURRENT_USER\Keyboard Layout\Toggle
HKKEY_CURRENT_USER\SOFTWARE\Microsoft\CTF\LangBarAddIn\
HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\LangBarAddIn\
HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName
ActiveComputerName
HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Parameters
HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKKEY_LOCAL_MACHINE\System\WPA\Starter

✓ VirusTotal分析

- 透過Virustotal方式分析遊戲程式執行檔，確認共有13家掃毒引擎判定異常，具有高度風險

✓ Sandbox分析

- Sandbox分析結果顯示，該遊戲執行程式在系統註冊表中建立多種高度可疑的服務，同時修改系統安全性相關登錄檔，主機系統暴露於高度風險中

✓ 緊急處理

- 北區A-SOC通知遊戲公司檢測，於各維運點阻擋連往惡意IP網路流量，並提供遭感染主機回復處理流程SOP，防止感染情況擴大



參考資料

- ❑ 國網中心張聖翊:教育學術研究骨幹網路頻寬效能提升計畫—100G骨幹網路建置規劃說明
- ❑ 臺灣大學計資中心李美雯:北區A-SOC資訊安全維運中心資安案例分享報告



Computer Center, National Central University.



Thank You!