

# 日誌分析介紹

Ivan Hsueh

# 關於我



Ivan Hsueh <[ivan.hsueh@ckmates.com](mailto:ivan.hsueh@ckmates.com)>  
CKmates資深資安顧問

- 過去經歷：
  - 安碁eDC SOC主任工程師  
資安事件分析與監控規則撰寫
  - 安創技術顧問  
資料分析與視覺化

# 什麼是日誌(Log)

- 日誌：泛指資訊系統以文字或檔案所留存的活動紀錄
- 用途
  - 紀錄
  - 稽核
  - 統計
  - 預測
- 日誌最重要的就是timestamp

# 日誌種類

- 資安設備日誌
  - Firewall、IDS/IPS、WAF、DLP、Content filter、AntiVirus、NAC
- 網路設備日誌
  - Switch、Router、Proxy、Network Monitor
- 系統日誌
  - Linux、Windows (Audit Log、System Log、Access Log、Error Log)
- 應用系統日誌
  - Web、DB、AP、FTP、Mail、Printer、DHCP、DNS

# 需求訪談與日誌完整度

- 弄清楚各設備與系統間的關係
- 不同的需求對應不同的日誌
  - 防資訊外洩
  - 防DDoS
  - 防惡意程式
  - 防非法使用

# 日誌分析工具

- Excel
- 特定日誌專屬分析工具
- 資安事件管理平台 (SIEM)
  - HP ArcSight
  - IBM Security QRadar
- 分散式資料分析工具
  - Splunk
  - ELK
  - Hadoop
- 視覺化資料分析工具
  - Qlik Sense
  - Tableau

# 分析方法



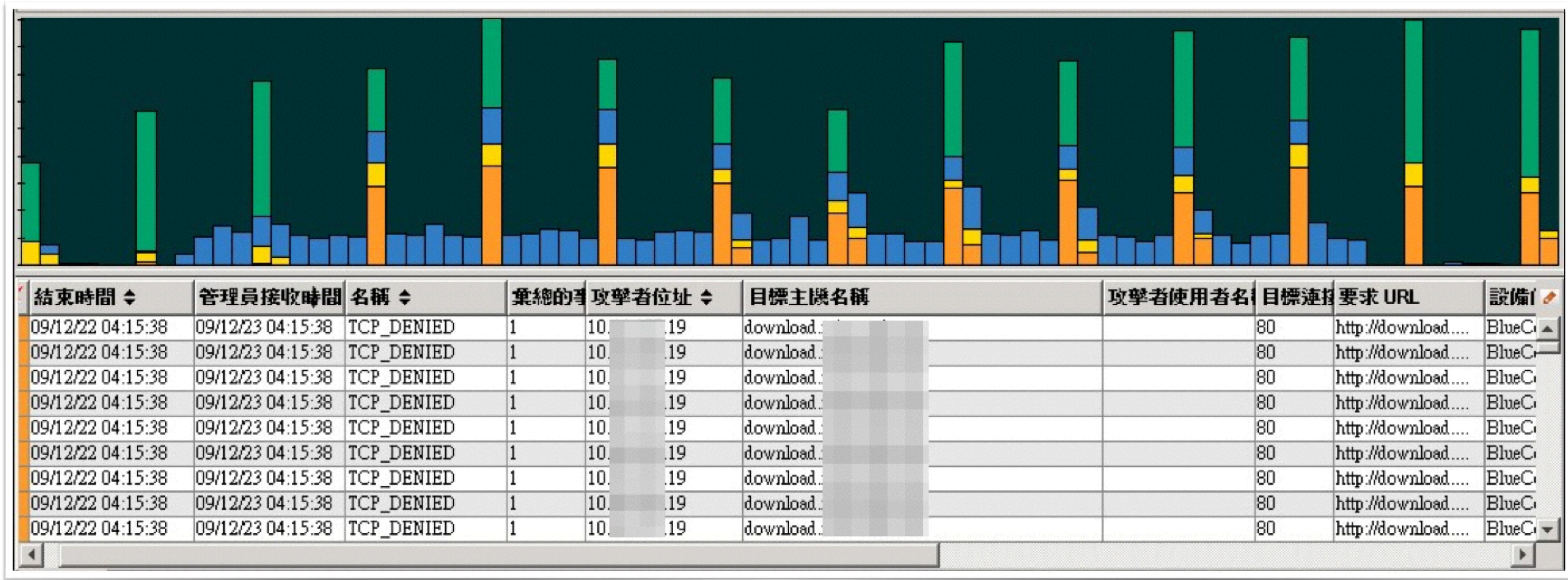
# 多而重複的事件

- 先從事件量大的下手
- 特定頻率的事件
- 一種事件大量發生通常只有兩種可能
  - 極度正常→考慮排除已減少雜訊
  - 極度異常
    - ▶ 問題持續發生
    - ▶ 設定錯誤

# 已知的行為模式-1

- 中繼站連線
  - 規律性連線
  - 固定封包傳輸行為
  - 惡意程式最常使用的Protocol為HTTP、IRC、SMTP
  - 惡意程式對外傳送資料常使用FTP、HTTPS
  - 多台主機同時訪問同一個目標主機

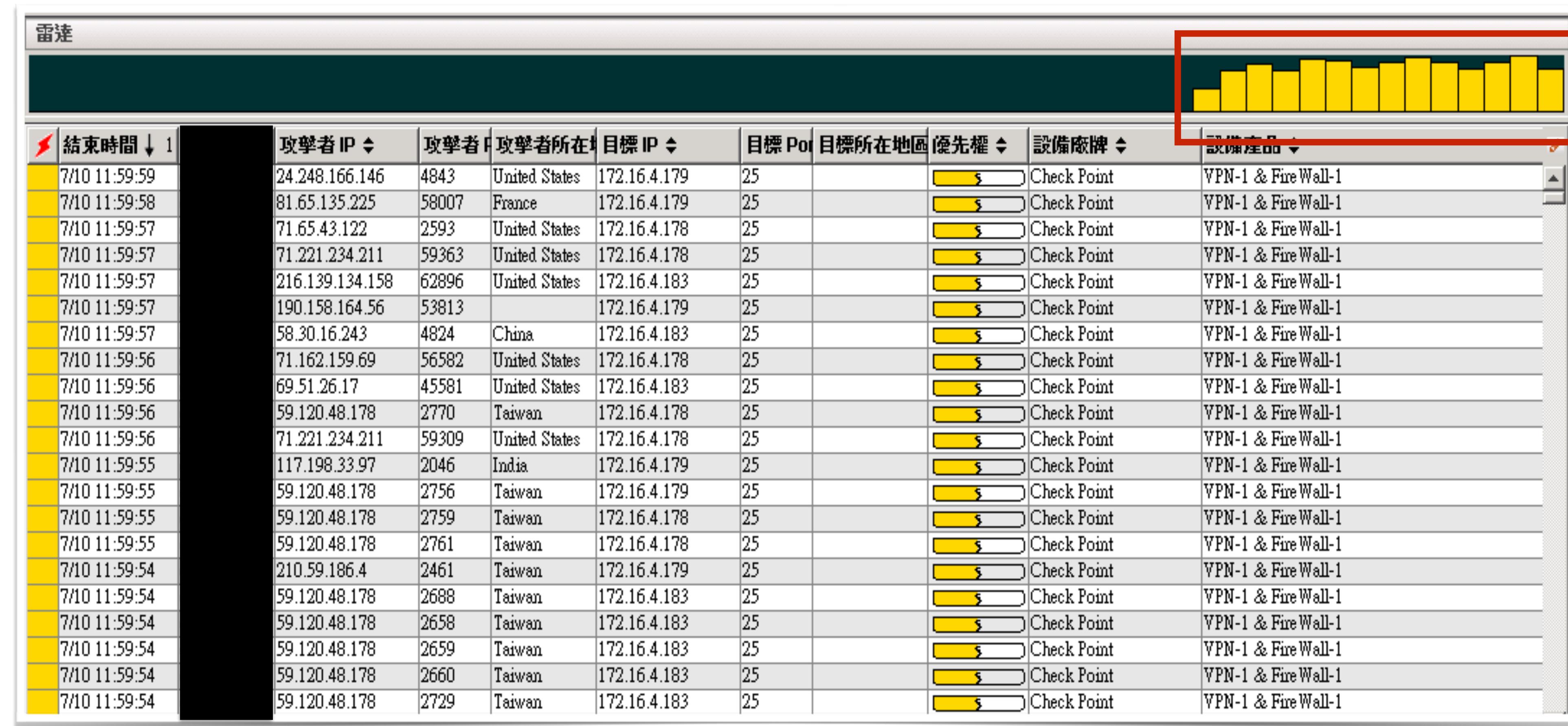
每日凌晨皆發生對外的規律連線，頻率與數量都相同，  
經實際至主機調查確認為惡意程式連往中繼站行為



# 已知的行為模式-2

- DDoS攻擊
  - 大量外部連線，且外部IP不固定
  - 超大流量塞爆頻寬
  - 不間斷的連線癱瘓設備
  - 過量的正常請求影響網站服務

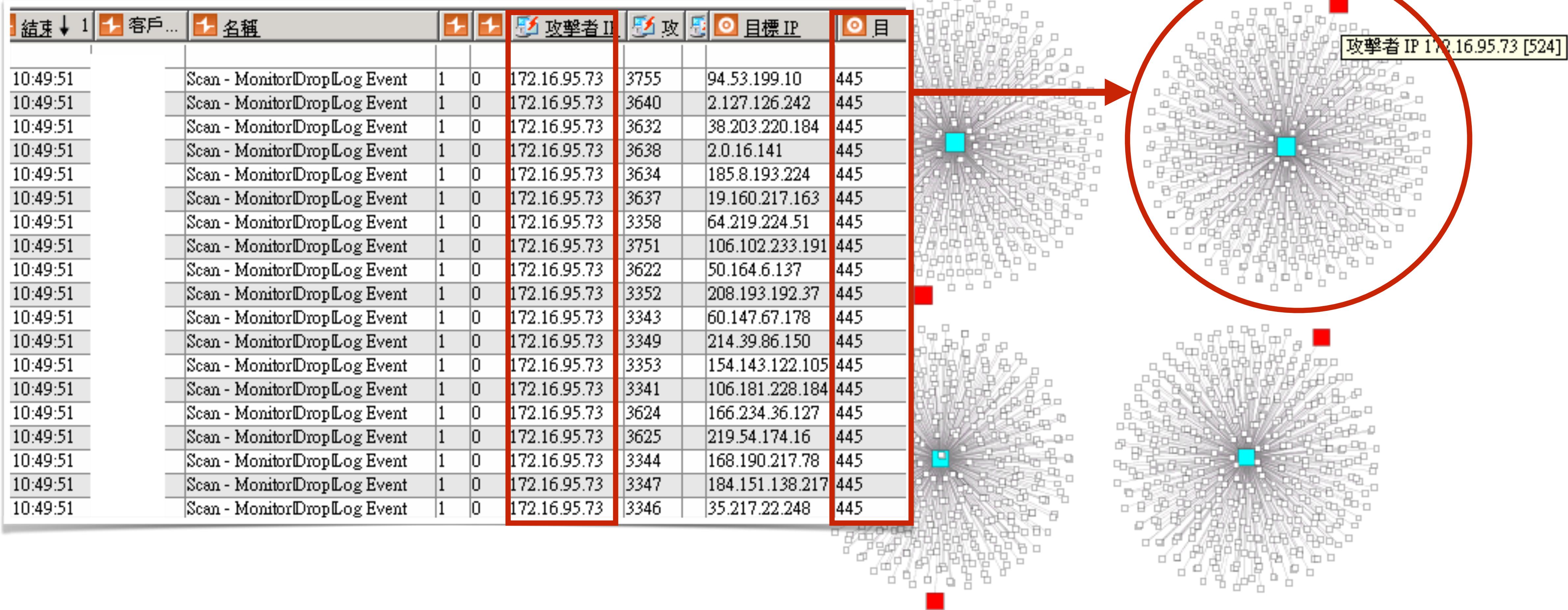
接近中午突然發生大量外部主機對正常服務Port的連線，  
數量是平時的100倍以上，已對正常服務造成影響



# 已知的行為模式-3

- 病毒擴散
  - 多台主機中相同病毒
  - 多台主機產生相似的異常連線
  - 異常的內網存取
  - 不合理的對外連線

# 對外大量主機的445 port進行連線 經查該來源主機感染勒索病毒



# 已知的行為模式-4

- 資訊外洩
  - 非法實體設備存取
  - 特定關鍵字偵測
  - 異常檔案傳輸
  - 規避管理的連線行為
  - 帳號盜用

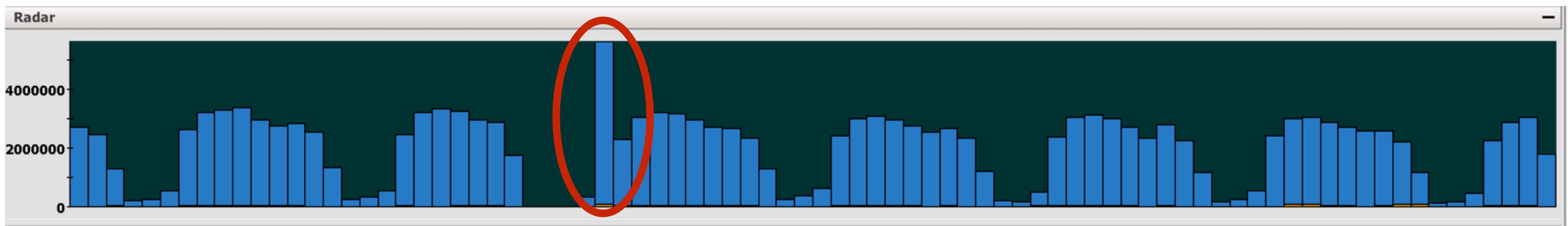
藉由排序與統計使用者的傳輸量，找出對外異常大檔傳輸

時間戳記	↑ 傳送位元組	接收位元組	要求 URL 連接埠	攻擊者使用者...	攻擊者主機名稱	攻擊者位址	目標主機名稱	要求方法	要求用戶端應用程式
26 九月 2010 02:00:00 CST	7594845	4913	80	[REDACTED]		10.60.129.22	sn134w.snt134.mail.live.com	POST	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
26 九月 2010 02:00:00 CST	2120596	5006	80	[REDACTED]		10.60.129.22	sn134w.snt134.mail.live.com	POST	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
26 九月 2010 02:00:00 CST	1193808	5029	80	[REDACTED]		10.60.129.22	sn134w.snt134.mail.live.com	POST	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
26 九月 2010 02:00:00 CST	947243	4946	80	[REDACTED]		10.60.129.22	sn134w.snt134.mail.live.com	POST	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)

# 比對法

- 固定特定參數，比對不同區間的行為差異
  - 固定時間與IP，比對不同日期的連線行為
  - 固定帳號與FTP存取路徑，比對不同時間的存取行為
  - 固定主機網段與時間，比對不同使用者的登入行為

平日上班時間網路流量都很固定，  
但某一天突然爆大量，高出標準值許多



- 都找不到問題怎麼辦？
  - 資料數量太多，不易找
  - 沒有太特別或高風險的事件

# 刪去法

- 換個角度思考
  - 先把正常的連線挑出來
  - 排除正常連線後，分析剩下的事件
  - 再與正常連線進行關聯分析
  - 正常連線可建立baseline

# 視覺化

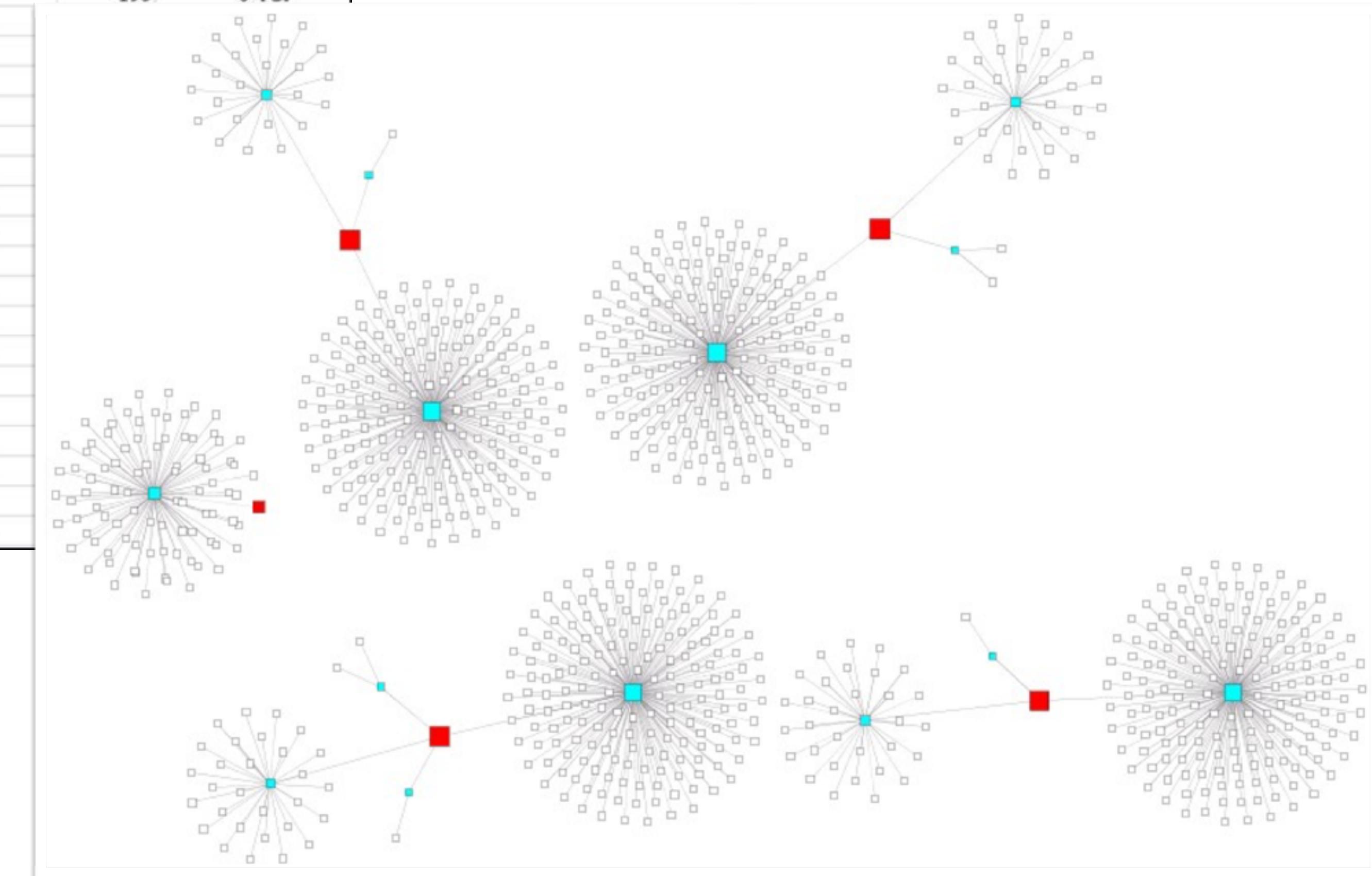
- 使用視覺化工具將資料進行統計與分類

- 較容易找到切入點
- 可分析趨勢行為



客戶反應網路速度低落，經查詢Firewall log發現有部份主機大量對外連線行為

2010/12/7	13:42:10	Permit	192.168.33.195:36909	192.168.243.239:512	:33743	59 sec	64	0 ICMP
2010/12/7	13:42:18	Permit	192.168.33.195:36911	10.222.177.51:512	:39229	60 sec	64	0 ICMP
2010/12/7	13:42:14	Permit	192.168.33.195:3714	27.38.42.150:4899	:54902	20 sec	132	0 TCP
2010/12/7	13:42:16	Permit	192.168.33.195:3716	71.255.106.58:4899	:22405	20 sec	198	0 TCP
2010/12/7	13:42:08	Permit	192.168.33.195:37164	75.23.161.193:512	:52326	60 sec		
2010/12/7	13:42:14	Permit	192.168.33.195:37166	61.161.89.26:512	:37944	59 sec		
2010/12/7	13:42:18	Permit	192.168.33.195:37167	172.26.135.169:512	:45245	60 sec		
2010/12/7	13:42:20	Permit	192.168.33.195:3720	60.189.218.209:4899	:21055	19 sec		
2010/12/7	13:42:12	Permit	192.168.33.195:3721	98.164.150.92:4899	:5046	8 sec		
2010/12/7	13:42:14	Permit	192.168.33.195:3723	174.174.10.53:4899	:57169	3 sec		
2010/12/7	13:42:08	Permit	192.168.33.195:3724	114.102.52.122:4899	:40093	2 sec		
2010/12/7	13:42:14	Permit	192.168.33.195:3728	139.102.87.56:4899	:9918	2 sec		
2010/12/7	13:42:18	Permit	192.168.33.195:3731	85.1.255.14:4899	:29108	5 sec		
2010/12/7	13:42:08	Permit	192.168.33.195:37420	188.242.128.53:512	:42435	60 sec		
2010/12/7	13:42:10	Permit	192.168.33.195:37421	208.171.176.178:512	:39238	59 sec		
2010/12/7	13:42:18	Permit	192.168.33.195:37423	54.42.45.70:512	:35160	60 sec		
2010/12/7	13:42:08	Permit	192.168.33.195:37676	206.29.122.84:512	:49222	60 sec		
2010/12/7	13:42:08	Permit	192.168.33.195:37932	145.194.35.80:512	:15534	60 sec		
2010/12/7	13:42:10	Permit	192.168.33.195:37933	158.100.131.179:512	:41202	59 sec		
2010/12/7	13:42:14	Permit	192.168.33.195:37934	119.136.68.238:512	:15416	59 sec		
2010/12/7	13:42:18	Permit	192.168.33.195:37935	192.168.168.51:512	:24170	60 sec		
2010/12/7	13:42:08	Permit	192.168.33.195:38188	31.43.15.249:512	:36519	60 sec		



# 小結

- 日誌完整度決定你能找到的東西
- 注意整體網路環境與配置
- 在有限的時間內完成明確的目標
- 分析方法
  - 可優先找量大的
  - 以行為來找事件特徵
  - 比對異常與正常的情況
  - 排除雜訊縮小範圍
  - 資料視覺化

*Q & A*

