【燕巢IPS 106年06月份報表】

威脅數量(前三名)：
vulnerability: 281.68M (281,681,219)
spyware: 1.94M (1,940,996)
virus: 365 (365)

威脅活動 Report

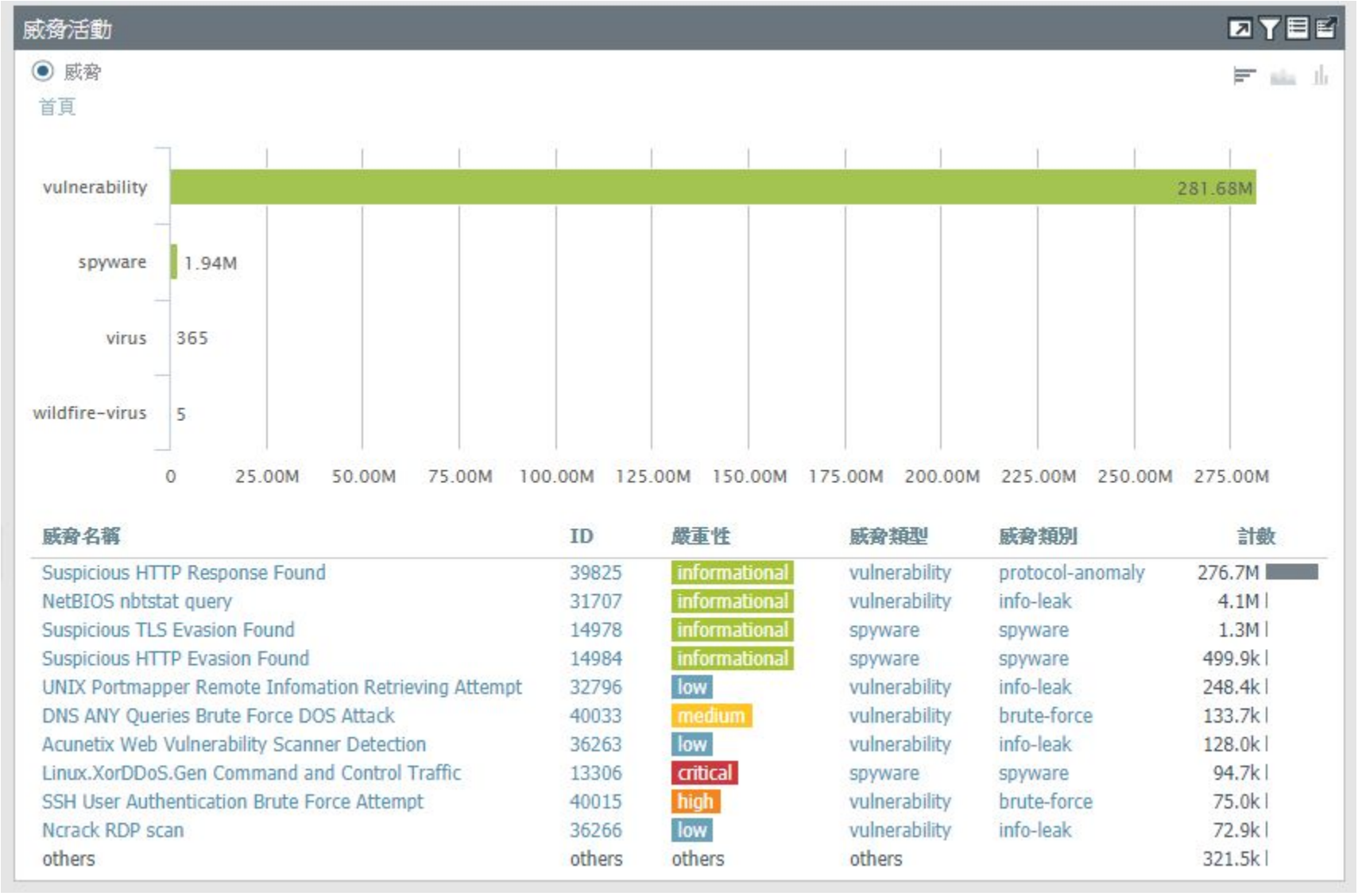
Time
06/01 00:00:00-06/30 23:59:59

Virtual System
vsys1

網路發展正面臨威脅甚加繁多，這些網路威脅可透過各種動態切換通訊埠的應用程式傳送，使用非標準通訊埠，在其他應用程式中建立通道，或隱藏在代理服務、SSL 或其他類型的加密應用中。藉由IPS防火牆可查看應用程式、攻擊軟體漏洞的程式碼、惡意程式、URL、異常的網路行為及針對性惡意程式之間的關係，依據自訂的安全性規則，自動比對出符合威脅特徵的封包，進一步Drop或拒絕並同時記錄日誌，來達到基本網路威脅的防範。
威脅分類可分為

- 漏洞(Valnerability)
- 間諜軟體(Spyware)
- 漫布型式(Floor)
- 病毒(Virus)，等

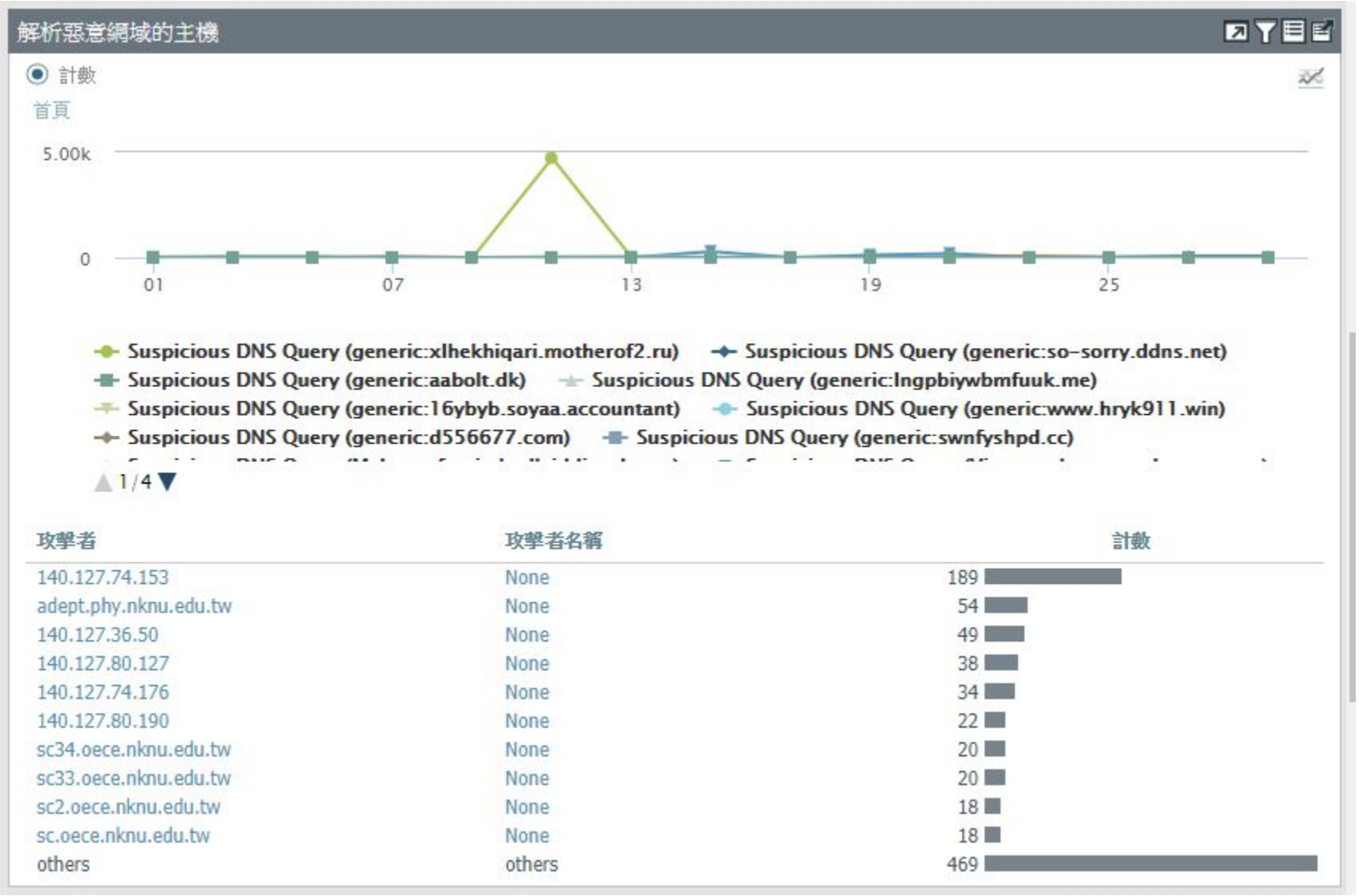
威脅分類分佈圖



威脅名稱	ID	嚴重性	威脅類型	威脅類別	計數
Suspicious HTTP Response Found	39825	informational	vulnerability	protocol-anomaly	276.7M
NetBIOS nbtstat query	31707	informational	vulnerability	info-leak	4.1M
Suspicious TLS Evasion Found	14978	informational	spyware	spyware	1.3M
Suspicious HTTP Evasion Found	14984	informational	spyware	spyware	499.9k
UNIX Portmapper Remote Infomation Retrieving Attempt	32796	low	vulnerability	info-leak	248.4k
DNS ANY Queries Brute Force DOS Attack	40033	medium	vulnerability	brute-force	133.7k
Acunetix Web Vulnerability Scanner Detection	36263	low	vulnerability	info-leak	128.0k
Linux.XorDDoS.Gen Command and Control Traffic	13306	critical	spyware	spyware	94.7k
SSH User Authentication Brute Force Attempt	40015	high	vulnerability	brute-force	75.0k
Ncrack RDP scan	36266	low	vulnerability	info-leak	72.9k
others	others	others	others		321.5k

說明：**漏洞威脅**發生頻率最高，多數為**暴力攻擊(Brute-Force)**，無論是內部網路對，校內使用者可能因網路瀏覽網頁習慣、開啟釣魚信件/信件連結，可能不經意下載木馬程式。該系統會於(開機)背景執行狀態，人員未操作電腦狀態下，自動對外以高頻率次數進行嘗試登入(Telnet)外部系統；反之，外部網路對內部重要資訊系統，亦會進行暴力攻擊；前述兩者，當成功被登入後，該主機則會被利用來作其他惡意用途。諸如此類，透過防火牆特徵比對，可防範基本的網路漏洞。

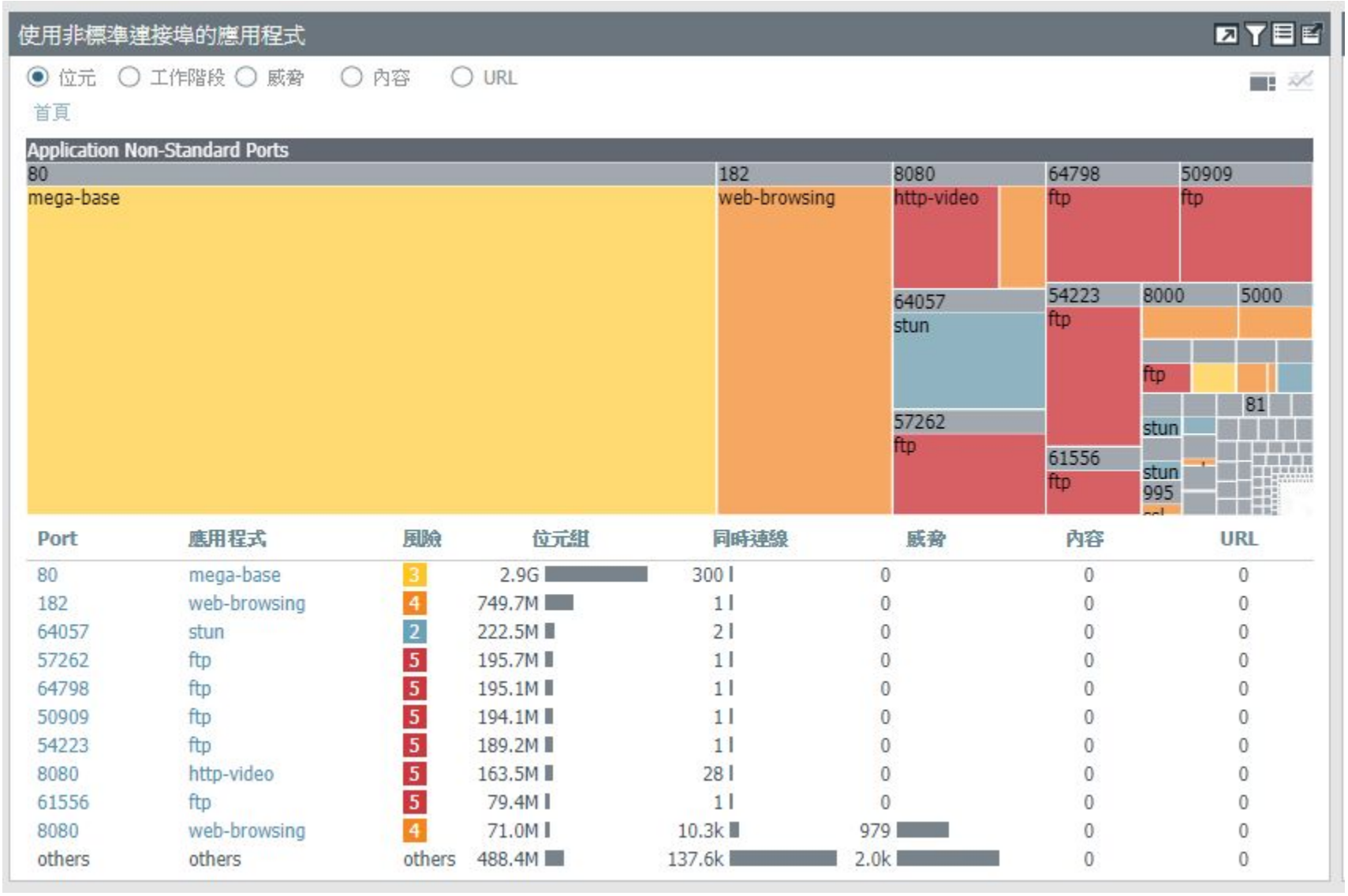
主機查詢惡意網域名稱頻率次數圖



攻擊者	攻擊者名稱	計數
140.127.74.153	None	189
adept.phy.nknu.edu.tw	None	54
140.127.36.50	None	49
140.127.80.127	None	38
140.127.74.176	None	34
140.127.80.190	None	22
sc34.oece.nknu.edu.tw	None	20
sc33.oece.nknu.edu.tw	None	20
sc2.oece.nknu.edu.tw	None	18
sc.oece.nknu.edu.tw	None	18
others	others	469

說明：**140.127.40.3為本校Domain Name Server**，故累計次數較高；次高，140.127.41.248-250則為本校無線網路設備使用。

未使用標準port之Apps流量分佈圖



說明：網路協定中有針對不同服務給定特定port，例如：**網頁瀏覽(Web-browsing)**為HTTP或HTTPS，標準埠號分別為80及443，觀察上述有使用81、8080、10050。另外，埠號80主要為HTTP服務，**但mega-base網頁行檔案分享服務，反而利用埠號80為傳輸埠號**；透過此資訊可進一步分析研究。

未使用標準port之應用服務流量分佈圖

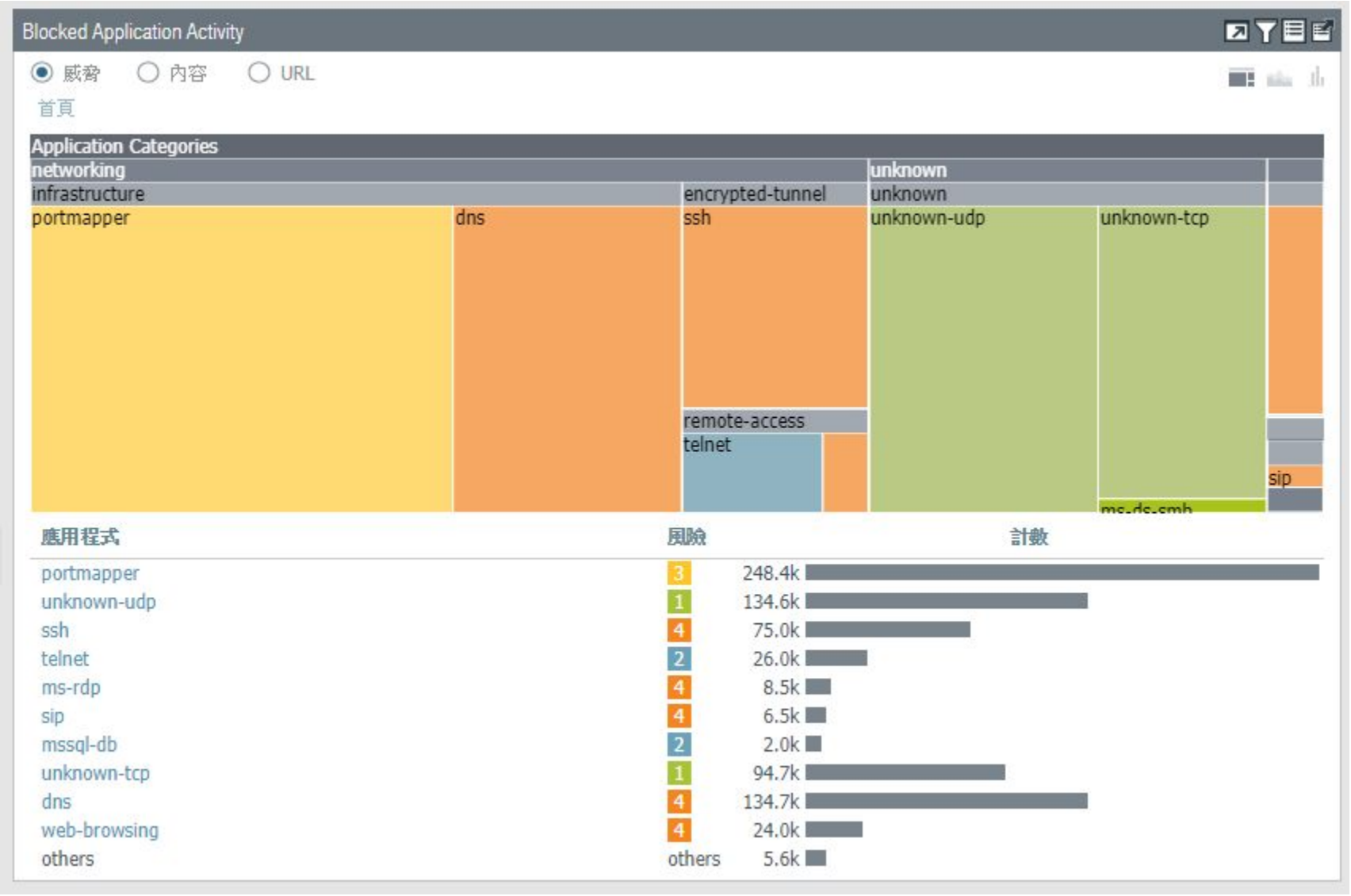
規則	應用程式	風險	位元組	同時連線	威脅	內容	URL
NKNU-Outboud-All	mega-base	3	2.9G	300	0	0	0
NKNU-Outboud-All	web-browsing	4	914.4M	90.4k	113	0	0
NKNU-Inbound-All	ftp	5	897.9M	37	2	0	0
NKNU-Inbound-All	stun	2	336.5M	53	0	0	0
NKNU-Outboud-All	http-video	5	163.5M	28	0	0	0
NKNU-Inbound-All	web-browsing	4	67.0M	7.8k	1.0k	0	0
NKNU-Outboud-All	flexnet-publisher	3	53.7M	24.0k	0	0	0
NKNU-Outboud-All	ssl	4	46.2M	6.5k	1.8k	0	0
NKNU-Outboud-All	stun	2	27.3M	450	0	0	0
NKNU-Outboud-All	upnp	2	16.5M	12.3k	0	0	0
others	others	others	25.7M	6.4k	20	0	0

封鎖的活動 Report

Time
06/01 00:00:00-06/30 23:59:59

Virtual System
vsys1

已封鎖不良意圖之應用服務分佈圖

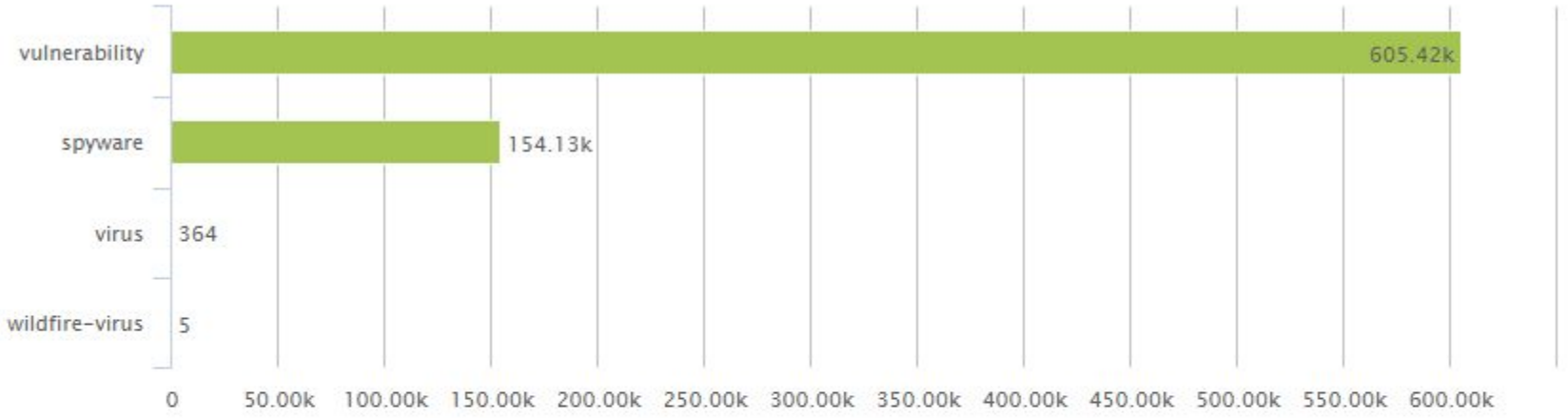


已封鎖威脅類型次數分佈圖

封鎖的威脅

威脅

首頁



威脅名稱	ID	威脅類型	威脅類別	嚴重性	計數
UNIX Portmapper Remote Infomation Retrieving Attempt	32796	vulnerability	info-leak	low	248.4k
DNS ANY Queries Brute Force DOS Attack	40033	vulnerability	brute-force	medium	133.7k
Linux.XorDDoS.Gen Command and Control Traffic	13306	spyware	spyware	critical	94.7k
SSH User Authentication Brute Force Attempt	40015	vulnerability	brute-force	high	75.0k
Netis/Netcore Router Default Credential Remote Code Execution Vulnerability	39587	vulnerability	code-execution	high	69.7k
ZeroAccess.Gen Command and Control Traffic	13235	spyware	botnet	critical	28.4k
ASUS/Netcore Router Default Credential Remote Code Execution Vulnerability	39438	vulnerability	code-execution	medium	25.1k
Telnet Authentication Brute Force Attempt	40009	vulnerability	brute-force	high	22.3k
HTTP SQL Injection Attempt	30514	vulnerability	sql-injection	medium	11.9k
Win32.Conficker.C p2p	12544	spyware	adware	critical	11.2k
others	others	others	others		39.6k

已封鎖使用者活動 - 安全性規則之類型次數分佈圖