

## 【燕巢IPS 106-05月份報表】

### 威脅數量(前三名)：

vulnerability: 11.73M (11,733,454)

flood: 2.48M (2,477,511)

spyware: 160 (160)

## 威脅活動 Report

### Time

05/01 00:00:00-05/31 23:59:59

### Virtual System

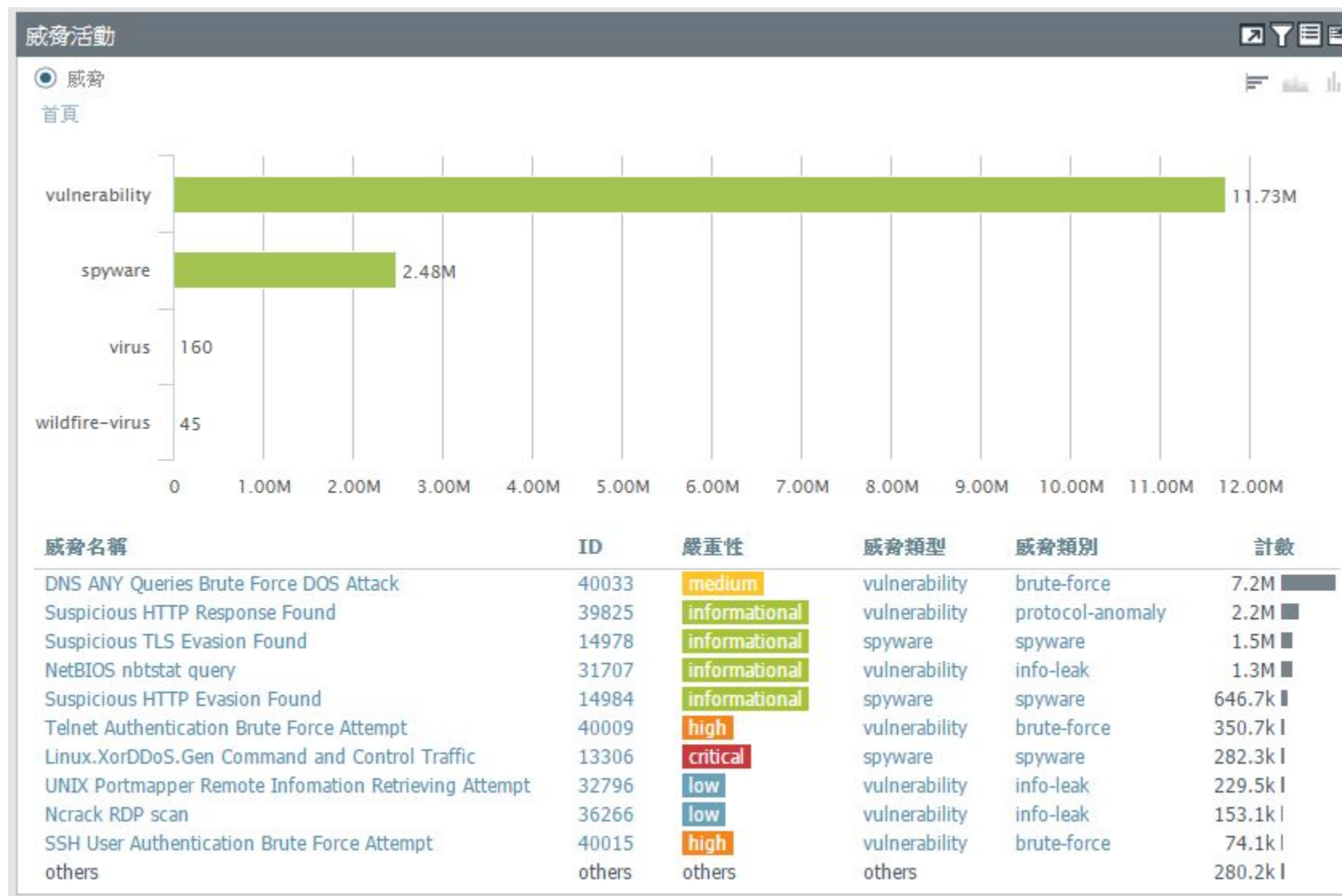
vsys1

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

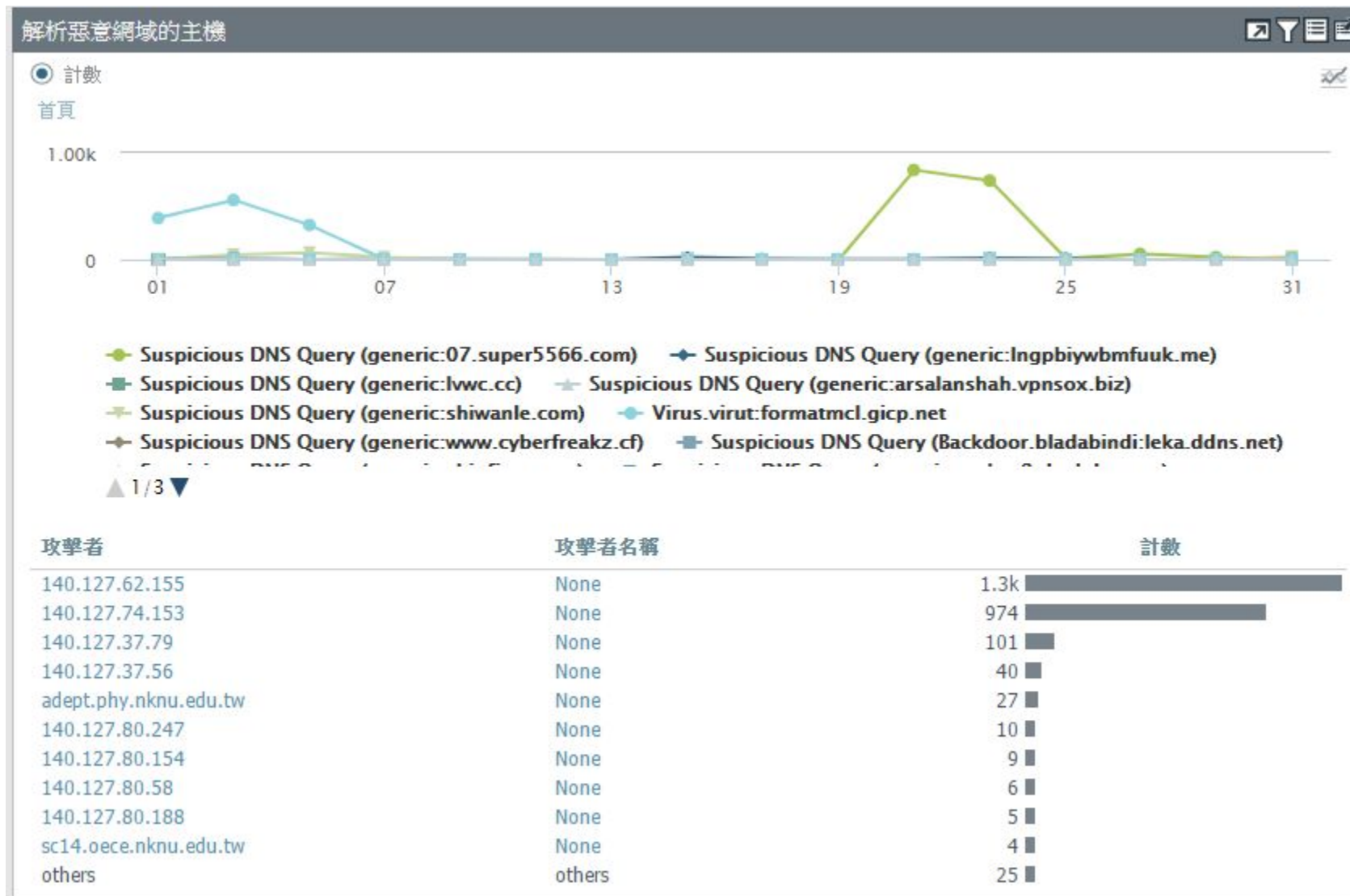
- 漏洞(Vulnerability)
- 間諜軟體(Spyware)
- 漫布型式(Flood)
- 病毒(Virus)，等

## 威脅分類分佈圖



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



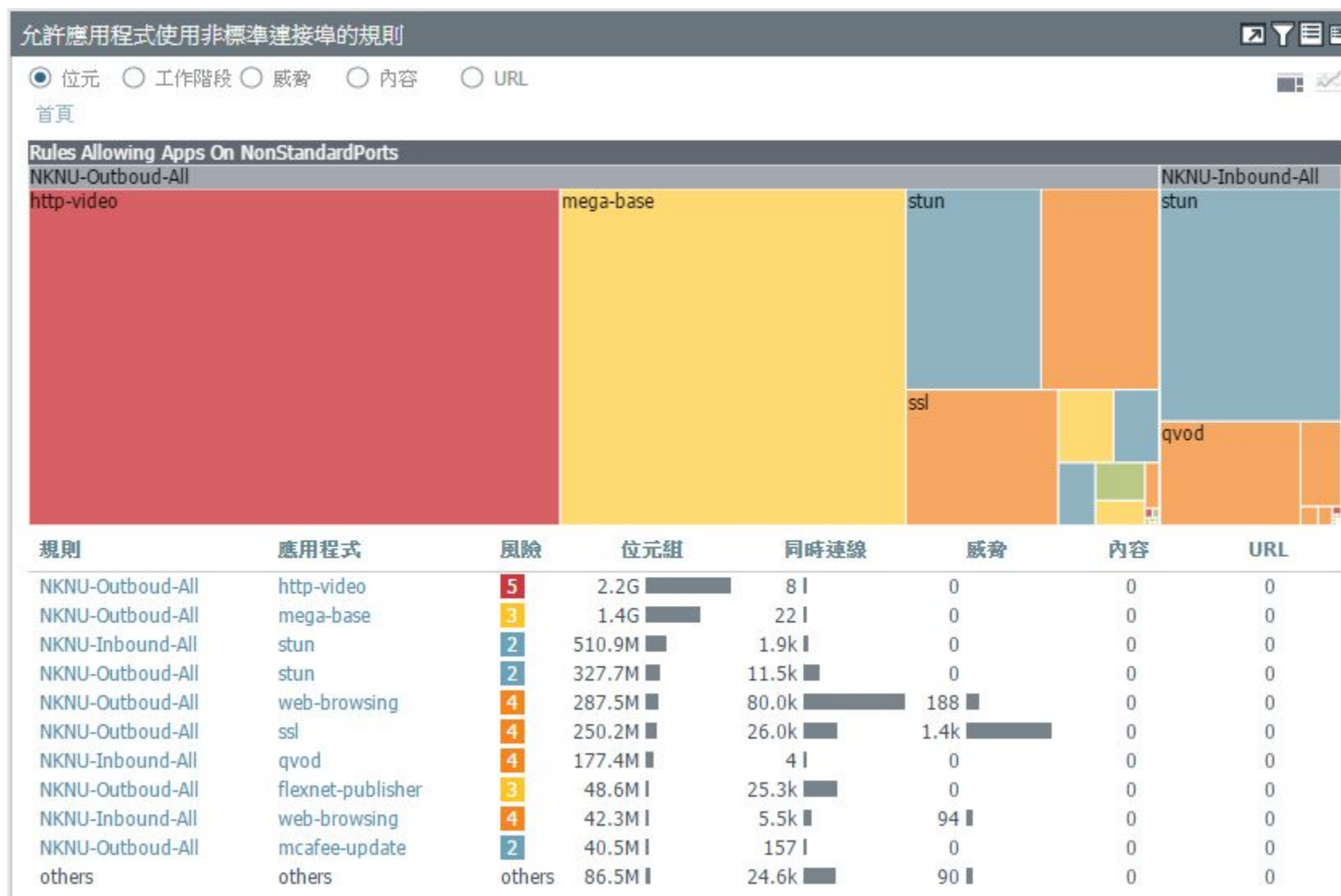
說明：140.127.40.3為本校Domain Name Server，故累計次數較高；次高，140.127.41.248-250則為本校無線網路設備使用。

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



# 封鎖的活動 Report

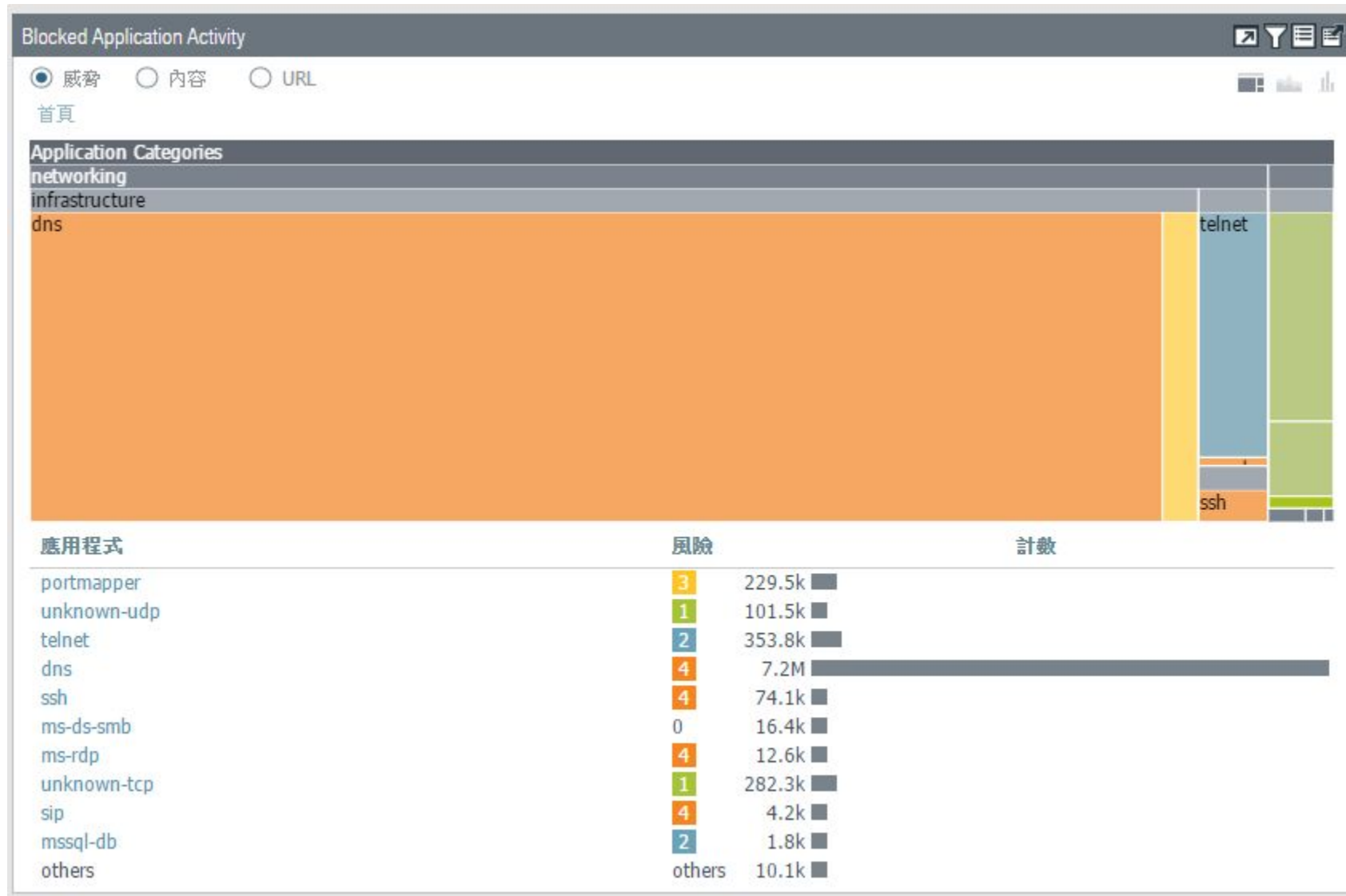
## Time

05/01 00:00:00-05/31 23:59:59

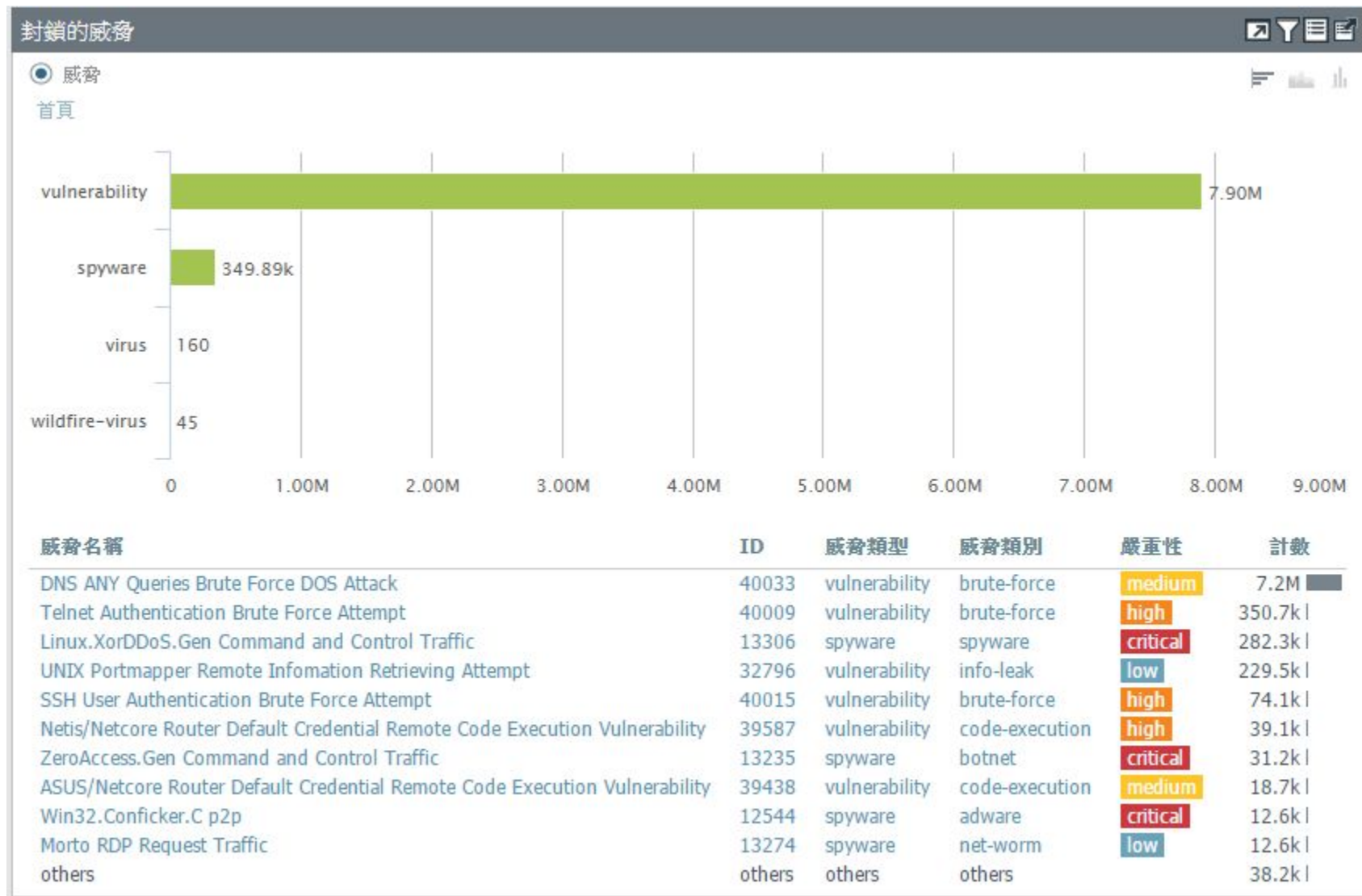
## Virtual System

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





## 已封鎖安全性規則之類型次數分佈圖

