網路日誌行為分析

指導教授：林柏青 老師
專題學生：傅皓群、張伍賢

一. 簡介

現今網路極為普遍，也深深地體會到網路的便利，各大企業、組織皆佈署網路對外提供服務，也讓內部人員可以存取廣大的網路資源、和外界進行訊息交換。但是，在豐富的資訊洪流裡面可能潛藏惡意活動，正在進行DNS折射攻擊、嘗試登入遠端未授權的主機等，或是組織內的主機已被入侵，被當成跳板在攻擊其它主機。這些攻擊將不時地變化，並用更好方式來隱藏自己，企業面對這樣的危險，需採取適當措施來防禦自己。

因此，我們將以程式分析封包的方式來偵測異常、惡意行為，提供分析結果給網管，讓網管可盡早做適當的防護措施，把正在攻擊的內部主機進行斷網，降低危害、資訊損失的嚴重程度。另一方面，每天的流量極大，以人工去檢視將耗時又耗力，自動化偵測將帶來便利性。

二. 系統架構

錄製封包的架構圖如圖1所示，校內封包要從路由器進到Internet前，都會被複製一份傳給我們的伺服器，伺服器是以10 Gigabit的網路介面卡來接收資料，再透過Bro把所有封包記錄下來，並自動分類成各種不同的資料類型。

封包錄好後，執行各種偵測不同特徵的程式來分析並輸出結果，再利用工具、Google搜尋鑑識，判斷是不是惡意活動的紀錄，流程如圖2。

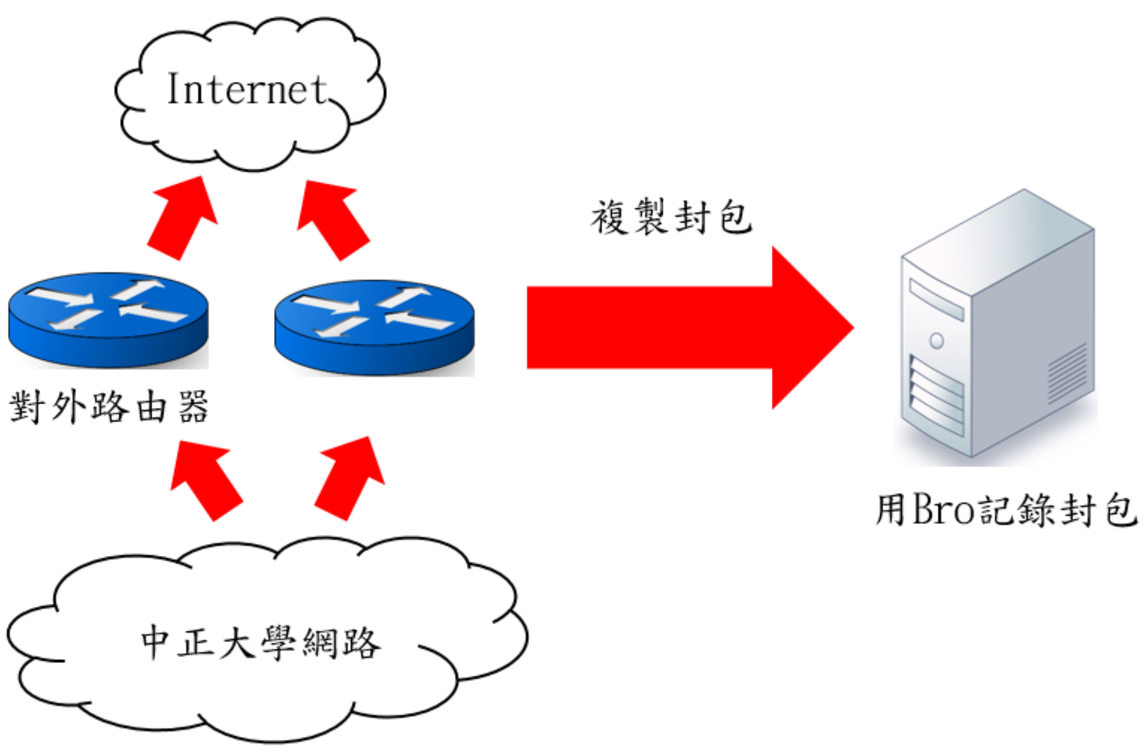
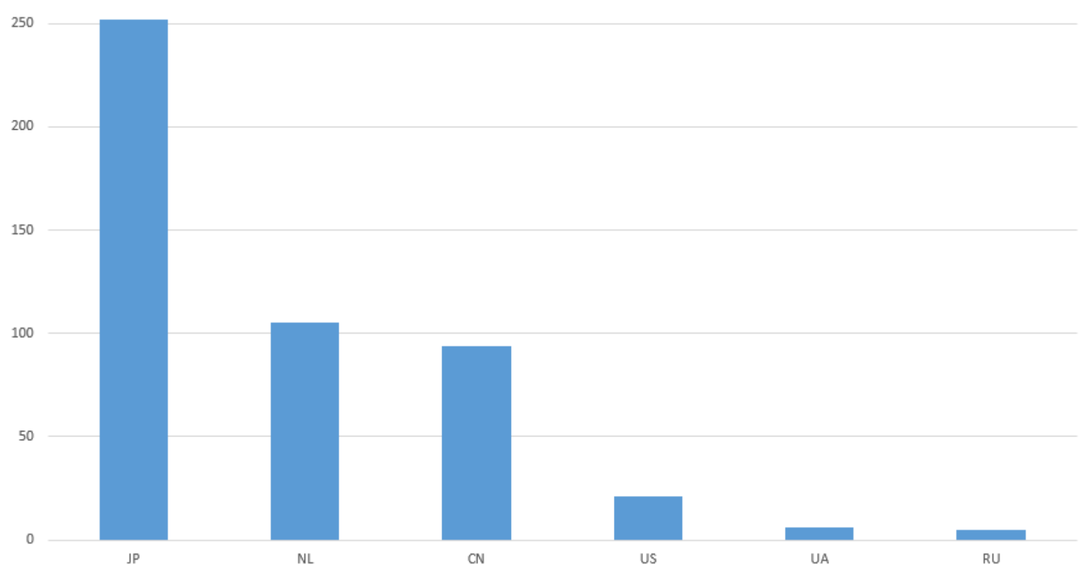


圖1 系統架構

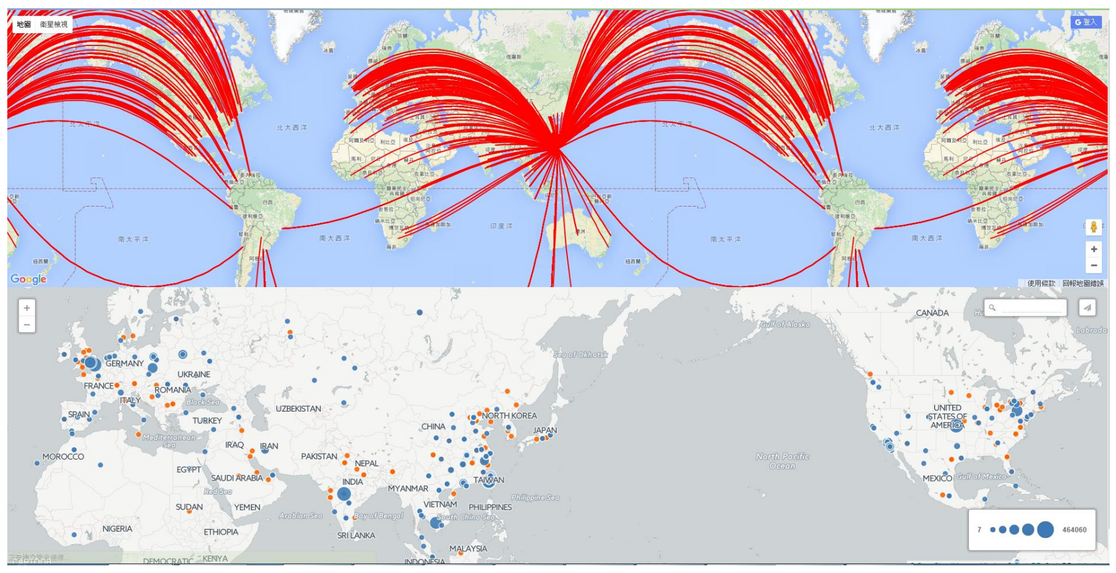
圖2 執行流程

三. 分析項目

- 嘗試登入 port 3389
- CGI scan
- Domain對應目的地IP
- 重導
- 黑名單domain、IP比對
- 應警覺的副檔名
- 來源IP為廣播IP
- 查詢domain長度過長
- Mail server IP無法反解
- Port scan, Port sweep偵查
- SMTP, FTP, SSH連線數量異常
- 網頁連結點擊判定



圖三 7、9、10月CGI scan analysis



圖四 攻擊路徑示意圖