利用 Google Analytics 分析網站惡意攻擊之研究

系所／資訊工程學系
指導老師／蘇民揚
組員／劉星宇、茅恩澤、談哲明、邱育謙

如今在電腦網路系統中，惡意的篡改、破壞行爲越來越多。而且這樣的威脅種類隨著時代的進步變得越來越複雜。常見的網路攻擊有垃圾流量、篡改消息等等，網路安全更顯重要。Google Analytics 可以收集和匯總網路流量，包括有關網路訪問者的位置，訪問日期和時間，訪問過的網頁和搜索關鍵字的資訊，進行分析，建立分析後的資料表，和已知模擬過網路攻擊後收集的數據進行對比分析，這樣可以找出相似點以推測網路攻擊的種類幷且封鎖危險 IP 以確保 Web Server 的安全。所以我們可以利用 Google Analytics 來收集大數據以進行網路攻擊的預防和偵測。

本專題目的即是進行流量分析的比較，我們將進行攻擊模擬，幷紀錄被攻擊時的流量分析，幷借助網路上有公信網站所提供的流量數據，進行兩相對比，建立資料庫，通過數據分析、篩選，運用我們自己的算法挑選出特殊網絡攻擊，來顯示出攻擊者的一些蛛絲馬迹，從而助于網絡安全的維護。

目前專題成果如圖 1 到圖 3 所示。圖 1 為本系統的登入畫面，輸入 View ID、起始日期和結束日期即可利用 API 將對應日期內 Google Analytics 中相關資料以 Excel 檔的格式保存在對應文件夾中。

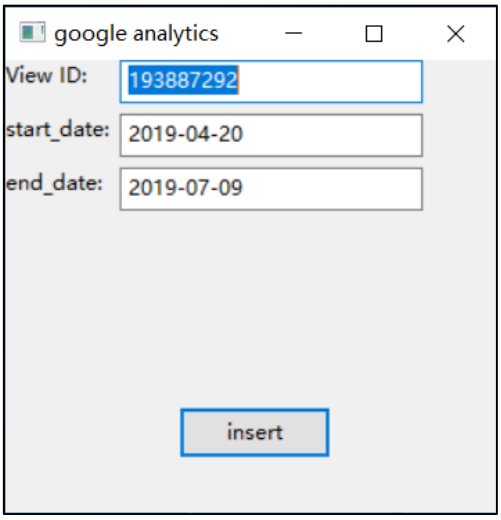

圖 1：網站安全分析系統登入畫面

圖 2 顯示的為我們收集到的部分資料，以 Excel 檔呈現。

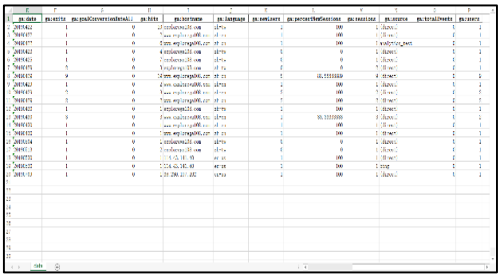

圖 2：利用 API 收集到的部分資料

之後我們將收集到的數據進行分析，運用我們自己的相關算法，挑選出幾個可能會是惡意網站攻擊的資料，將信息傳給網站管理者，圖 3 呈現的是產生垃圾流量的網路 bot 攻擊。

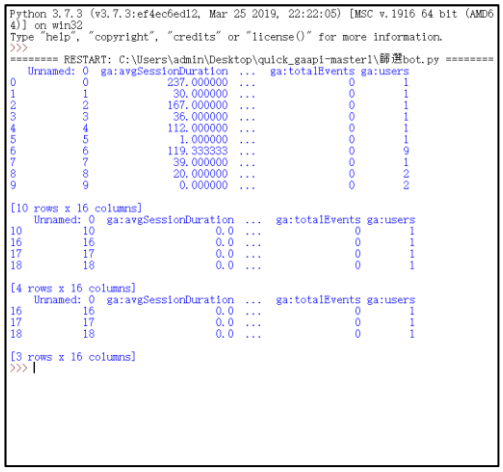

圖 3：產生垃圾流量的網路 bot 攻擊