分散式阻斷服務攻擊是近來主要的網路安全威脅之一，
各網管單位與資安維運中心需正視其造成的嚴重影響。

新世代的DDoS威脅

◎蔡一郎

隨著資訊技術的進步，現今社群網路成為人們社交的主要管道，透過網路的連結提供需求雙方資訊的交換，終端裝置的多樣化，提供即時的資訊；而人是物聯網主要的使用者，運用各種行動裝置加以緊密結合。逐漸成熟的數位化智慧城市時代已經來臨，IDC（國際數位公司）預計全球資料量將急速攀升，從2013年至2020年將成長10倍的資料量，資料總量將從4.4ZB（ZB為電腦儲存單位，1ZB相當於270 bytes）增加至44ZB，其中有三分之二的資料量是由個人所產生，約為2.9ZB；而2013年全球有60%的資料來自於成熟市場，也就是已開發國家，包含美、加、紐、澳、日、西歐，僅約30%的資料來自於新興市場，包含中國大陸、巴西、印度、俄國和墨西哥；然而到2020年，情況則將逆轉，60%的資料來自於新興市場，而成熟市場的資料量則降至40%。

在各種不同的網路安全威脅之後，其中分散式阻斷服務攻擊（DDoS, Distribution Deny of Service）已成為近來主要的網路安全威脅之一。此類型的攻擊，大多非直接入侵，而是透過耗盡網路資源、計算資源等方式，降低服務主機本身的系統效能，以達成影響受害者系統的目的，因此當遭遇此類網路攻擊時，受害者往往在短時間內就會直接影響原本的服務。近年透過關鍵網路之服務弱點，進行網路放大攻擊，可避免因連外網路頻寬不足而無法執行大規模的攻擊。

分散式阻斷服務攻擊，具備以下幾項特性：有目標、有理想的攻擊；來源分散、不容易阻擋；當成為目標時最有感覺；對企業影響範圍大；網路的連結，讓攻擊者無所不在。目前針對分散式阻斷服務攻擊，尚無直接有效的防禦方式，主要在於目前的攻擊技術，也隨著網路服務的多樣化而轉變得更不容易防禦，因此大多數面對此類網路攻擊時，採取的策略都以降低其所造成的影響為主；一旦網路服務遭受攻擊，可供我們進行應變的時間往往相當有限，因此從攻擊手法的行為偵測到應用資安設備進行防禦，都需要配合進行調整。為此在近幾年網路化與雲端化的趨勢下，出現了許多針對此類網路攻擊提供「流量清洗」的服務，即利用前端網路流量特徵的偵測，蒐集來自網路設備的資訊，例如：路由器所提供的Netflow資料，經過網路行為特徵的分析，找到當時攻擊者所使用的攻擊手法，再將該連線的行為轉移到「清洗中心」進行過濾；而「清洗中心」針對網路的流量進行比對，當確認網路流量中的異常行為時，則將該網路封包丟棄，最後再將經過純淨處理後的流量導回原本的網路設備，讓已過濾完成的網路流量可以到達目的地。利用「清洗中心」進行異常網路流量的清除，可以減輕被攻擊之目標承受來自分散式阻斷服務攻擊的影響，但因攻擊的手法極有可能多樣化，或是當攻擊者發現所使用的攻擊方法無法達成預期的目標時，皆有可能轉換成其他的攻擊手法。因此從資安防禦的角度而言，建立預警的偵測機制，也成為相當重要的一環，配合前端的資料蒐集與預警，可方便後續進行的應變與處置。

Google是目前全球最大的雲端服務業者，也有自己的國際線路，而今每天使用Google雲端服務的使用者相當多，從本身所管理的網路環境中進行分散式阻斷服務的偵測，對於網路安全趨勢的觀測而言，有相當程度的參考價值。目前在Google所開發的「Digital Attack Map」網站中，提供了接近即時的網路安全