※資訊安全宣導

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~

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

趨勢資訊，主要以分散式阻斷服務攻擊的類型為主，並且提供歷史的資訊方便查詢，也可以針對特定的區域或國家進行長時間統計資料的呈現；再者也能利用播放的功能，縮時呈現當時網路攻擊發生的期間，在全球網路流量的變化，這對於資安研究人員追蹤此類攻擊對網路世界造成的影響，有相當的助益。由前述所提供之資訊不難發現，當進行大規模的分散式阻斷服務攻擊時，幾乎所有的攻擊者都會假冒來源IP位址，除可隱匿本身來源的位址之外，也可造成混沌的效果，讓資安的研究人員難以從當下的網路流量中，判斷真正的攻擊來源為何，加上目前許多的網路攻擊都是利用受駭的電腦所組成的殭屍網路（Botnet）發動，因此在資安的分析上更顯困難。

ALTAS為全球性針對分散式阻斷服務攻擊進行情資發布的研究單位之一，由其商業營運公司在全球超過九成以上的電信客戶，構成完整的情資蒐集來源；利用此種先天上的優勢及其廣大的涵蓋範圍，在所提供的資訊上能具備更趨近於真實的網路。運用網站上的查詢界面，可容易地掌握當下網路攻擊的趨勢地圖，對網管人員或資訊安全研究人員而言，即可利用所蒐集的資料，佐以該網站發布的情資，在進行資訊安全事件的應變與處理時，更精確地進行事件的分析並掌握攻擊者相關的行為特徵。

分散式阻斷服務的攻擊技術若配合關鍵網路服務將形成更大的威脅，目前發現已遭利用的關鍵網路服務包括：DNS名稱解析服務、DHCP位址服務、NTP網路校時服務、Syslog日誌服務、NAC網路存取控管服務、IPAM網路位址管理、Radius身分識別認證管理。這些原本存在網站上的關鍵服務，用以提供使用者接取網路或是網路組態設定上的便利性，惟此長期留存的系統安全與應用服務的弱點，至今已成為攻擊者手上的籌碼，利用「放大攻擊」與其他手法，假冒這些關鍵

服務的通訊行為，讓遭受攻擊的目標無法應變，進而影響真正有需要的

使用者，或是造成下一波的資訊安全威脅，例如：網路釣魚、殭屍電腦等。由去（2014）年發生的大規模資安事件來看，其中以DNS名稱解析服務、NTP網路校時服務最常被拿來利用，配合殭屍網路發起攻擊，假冒來源的IP位址為預計攻擊目標的IP位址，一個簡單的攻擊手法，就能造成大量網路服務查詢所回傳的封包，直接影響遭受攻擊的目標。

分散式阻斷服務攻擊目前已成為亟需建立防禦機制的資安威脅，在國內資通訊環境及網路頻寬不斷擴增之時，針對此類具嚴重威脅卻尚未建立有效防禦機制的情況下，其所造成的威脅將會與日俱增，亟需各網管單位與資安維運中心正視其所造成的嚴重影響，輕則單純影響目標的系統，重則可能影響整個網路環境的穩定。

（作者蔡一郎為雲端安全聯盟臺灣協會理事長、國家實驗研究院國家高速網路與計算機中心主任室研究員）