分散式阻斷服務(Distributed Denial-of-Service)

在九零年代香港黑道片中常見的場景，黑道為了要妨礙店家做生意，就去找一群染著金毛的小弟霸佔住店家營業的店面，讓一般的客人無法也不敢進入，以達到其恐嚇威脅的目的。Denial-of-Service(DoS)是一種類似的網路攻擊的手法，攻擊的目的是要讓被鎖定的目標電腦的網路或是系統資源耗盡，從而中斷或關閉網路或服務，結果是正常的使用者將無法存取目標電腦所提供的服務[1]。為了減少被目標電腦偵測到攻擊及進行相對應的防禦動作，攻擊者會使用多部位於不同空間位置上被其所控制的殭屍電腦，對目標電腦發動 DOS 攻擊。這樣多部電腦同時攻擊的方式被稱為分散式阻斷服務(Distributed Denial-Of-Service, DDoS)攻擊。

攻擊者首先會先透過惡意軟體事先感染網路上的電腦，讓它變成所謂的殭屍電腦做為其攻擊的跳板，在取得這些僵屍電腦遠程控制的權限後，這些電腦構成了一個殭屍網路。透過遠端控制的方法，攻擊者向僵屍電腦發送出攻擊目標電腦的網路位址和攻擊指令，在接收到指令後，殭屍電腦會向目標電腦發送大量正常服務的請求，導致目標電腦超過它所能負擔的服務能力或是超過網路所能承載的容量，這樣會造成正常使用者所提出的服務要求被拒絕。由於提出服務要求的電腦都是合法的設備，因此目標電腦要將攻擊流量與正常流量分開會是很困難的事[2]。

參考資料:

1. Trend Labs 趨勢科技全球技術支援與研發中心., “什麼是分散式阻斷服務 (DDoS) 攻擊?” 資安趨勢部落格.
2. CLOUDFLARE, “What is a DDoS Attack?.” https://www.cloudflare.com/