網路頻寬與資訊安全

【研究紀要】

【文／教育資源及出版中心副研究員　朱麒華】

最近美國一家內容傳遞網路（Content Delivery Network CDN）公司 Akamai，發表了 2013 年第一季全球網際網路現況報告（The State of the Internet）。由於 Akamai 是全球最大的內容傳遞網路公司，藉由其業務特性，能夠搜集大量網際網路資訊內容，對外公告其研究報告。此報告主要區分成資訊安全（Security）、網際網路與寬頻的使用（Internet and Broadband Adoption）及移動網路覆蓋率（Mobile Connectivity）三大部份。關於臺灣與其他國家/地區的比較與探討，我們可以發現：臺灣的網路連線速度並不快，但資訊安全卻有待加強。從網路攻擊來源位址統計，臺灣排名第七，2.5%的網路攻擊來源位址源自臺灣；但網路速度，無論是寬頻，還是平均連線速度的排名都遠遠落在三十名之外。

表：臺灣與鄰近區域的比較

國家/地區	攻擊來源比率		平均連線速度		高速寬頻使用率	
	排名	百分比	排名	Mbps	排名	百分比
臺灣	7	2.5%	47	4.3	37	4.5%
香港	10	1.6%	3	10.9	3	34%
日本	14	0.9%	2	11.7	2	43%
南韓	11	1.4%	1	14.2	1	50%
新加坡	35	0.1%	21	6.9	18	16%
中國大陸	1	34%	98	1.7	50	0.2%

整理自 Akamai 2013，The State of the Internet, 1st Quarter, 2013 Report。

依據中國大陸的《2012 年中國互聯網網路安全報告》，2012 年中國大陸境內有 1419.7 萬餘台主機受到境外木馬或殭屍網路控制，較 2011 年增長 59.6%。其中被來自美國網路位址的木馬或殭屍網路控制的伺服器和主機數量，佔全部的 17.6%和 74%，均名列第一。如果從中國大陸境內伺服器被控制的比例來看，來自日本和臺灣的網路位址緊隨美國之後，分列第二、三位，分別佔 9.6%和 7.6%；從控制的境內主機數量來看，來自韓國和德國的網路位址分列第二、三位，分別控制 78.5 萬和 77.8 萬台主機（北京新浪網 8/5/2013）。這種利用分散式阻斷服務攻擊（Distributed Denial of Service: DDoS）來癱瘓網路服務是國際上常常發生的資安事件。南韓【東亞日報】在七用卅一日報導了北韓在南韓境內設置了十萬台殭屍電腦，將發動史上最大的分散式阻斷服務攻擊。在過去 2009 年及 2011 年就已經對南韓的網路發動了分散式阻斷服務攻擊。

許多電腦被植入病毒或木馬程式，受到遠方主機的控制。一旦駭客發起攻擊，這些受駭的電腦就會收到指令，對相同的網路主機發動一連串的攻擊，造成網路塞車或是主機永遠忙線中，阻斷了正常的服務。這些受駭的電腦稱之為殭屍電腦（Zombie Computer），通常殭屍電腦的使用者不易查覺自己是受害者，反而容易被別人誤認為是加害者。因此統計網路攻擊來源位址，並不能真正顯示幕後發起攻擊的位置，但可以反應出資訊安全管理上的漏洞。電腦被植入病毒或有害程式，通常起因於使用者管理的怠惰。系統沒有修補、病毒碼沒有即時更新常常是駭客覬覦覦的對象。

從以上的新聞及研究報告中可以看出，網路速度的提升並不會危害資訊安全。在提升網路服務的同時，依然可以擁有安全的資訊環境。金錢可以汰換網路設備，但資訊安全卻有賴使用者的認知，每一個使用者都應該對擁有的電腦善盡保管責任。