殭屍網路與進階持續性滲透攻擊趨勢

◎蔡一郎

資訊安全的發展歷程中，網路攻擊的手法目前已朝向組織化、精緻化發展，大規模的攻擊行為已不多見，取而代之的是經過精心設計的網路攻擊，其中利用各種惡意程式感染受害者為當下最常見的手法之一；而殭屍網路（Botnet）是目前最嚴重的資訊安全威脅之一；進階持續性滲透攻擊（APT, Advanced Persistent Threat）則為近來最熱門的資安議題。在針對性的攻擊行動中，常可見到透過殭屍網路進行資訊的竊取或是大規模的攻擊活動，當攻擊者選定攻擊的對象或目標後，將會採用多種不同的攻擊手法，針對特定目標進行長期且持續性的攻擊，不擇手段以達成攻擊的目的。許多受駭的電腦在不自覺的情況下，參與了駭客所發起的攻擊行動，而殭屍網路所使用的惡意程式，大多針對該目標被發掘的弱點進行客製化的開發；此「特殊」用途的惡意程式，在潛伏與感染的階段很難被發現，除非掌握其行為模式，否則也不容易由特徵比對的方式進行偵測，再加上惡意程式的變種速度快，系統一旦被感染，防毒軟體恐不易偵測與清除。

殭屍電腦為了能穿透防火牆等資訊安全設備的防禦，大多採用一些在防火牆上允許通過的協定與通訊埠，也改變了傳統的資訊安全防護機制。以往大多將內部的網路視為安全等級較高的區域，而外部的網路則是安全等級較低的區域，在存取的管制上，較高安全等級的區域預設就能夠連線到較低安全等級的區域，因此許多受到惡意程式感染的殭屍電腦，能夠自由地進出防火牆等資安設備，而不會受到阻擋，這也是造成殭屍網路大規模擴散與感染大量電腦主機的原因之一。目前殭屍網路經常使用的通訊協定，包括 http、ftp、tftp、irc 等，而這些通訊協定廣泛地使用在許多的應用程式上，因此當殭屍網路透過這些常見的通訊協定進行通訊時，網管單位或是遭到惡意程式感染的系統，往往很難察覺這些通訊行為的存在；尤其當殭屍網路仍在潛伏期，除了與中繼站或駭客的控制平台保持微量的通訊外，在傳統網路流量的統計方式上，並無法有效掌握這些微量的通訊行為。

殭屍網路與傳統電腦病毒、木馬程式或是網路蠕蟲最大的差別在於前者除了對我們的系統造成影響之外，也配合中繼站或是中央控制站角色，提供了殭屍網路更有效的管理方式，受害的殭屍電腦會主動與這些中繼站或中央控制站進行連線，並隨時等待來自攻擊者所下達的指令，一旦接獲攻擊的指令，便能在最短的時間內依據指令的內容進行惡意攻擊，改變傳統攻擊者必須自行下達指令予分散各地的受駭主機模式，除了更有效率的管理外，也能在較短的時間內進行針對式的攻擊活動。

目前地下的經濟活動，大多配合殭屍網路進行相關的非法活動，例如：個人機敏資料的竊取，及網站帳號密碼、鍵盤或系統畫面的側錄等，或是參與殭屍網路所進行的惡意攻擊行為，這些都是造成資訊安全事件的主要

原因。加上惡意程式的變形工具或是原始碼在網路上流傳，更造成惡意程式偵測上的困難。如今資訊匯流及數位經濟的發展，促使資訊安全應用遍及各個領域，而雲端應用技術及行動商務模式的興起，更讓資訊安全防護有更多的考量。在新環境、新技術的考驗下，行動及寬頻終端、網路、服務、應用平台、資料中心、犯罪調查、國家安全各領域，亦需面對功力高深的駭客攻擊、惡意程式植入等相關挑戰。

2012 年可稱得上是進階持續性滲透攻擊（APT）相當活躍的一年，多起資訊安全事件都與此種攻擊的手法有關。APT 不是一種新的攻擊，而是同時採用多種不同類型的攻擊手法，使用多種不同類型的攻擊方式以因應攻擊目標的環境。整個攻擊的流程可分為多個不同的階段，包括資料的收集與分析、系統與應用程式弱點的掃瞄、Rootkit 的使用、針對 Web Application 的安全弱點運用等。除了知名的 RSA、HBGary 等以資安設備或服務為主的公司皆遭到此類型的攻擊，後續衍生出其客戶的資安風險，或是由於所使用的資安設備或服務遭到破解造成的資訊安全事件，皆造成不小的影響；這類型的攻擊同樣發生在 Sony 的遊戲社群平台、花旗銀行、Google、VISA 信用卡國際組織等，這些針對特定目標與目的所進行的多起攻擊事件仍時有所聞。由此攻擊趨勢觀察，駭客的攻擊對象，除了由一般使用者的電腦竊取資料之外，也對重要且有指標性的目標逐漸感到興趣，且有長時間準備發動攻擊行為的規劃，透過社交工程、網路探勘與偵測等細緻的攻擊手法，針對特定的目標與目的，客製成為獨特的攻擊手法，以達到目的為最終的目標，未達成目的前決不輕言放棄；此類型的攻擊行為，往往長達數個月或一年以上。攻擊者經常使用或發送一些看似正常的網路服務或是文件，透過其中夾帶惡意程式發動零時差的攻擊，並針對尚未發布的系統或應用程式的弱點進行攻擊。至於遭受攻擊的目標，往往受駭者並不會察覺，當殭屍網路與持續進階滲透的攻擊相互結合時，攻擊者能有效地運用龐大的殭屍網路做為幫手，針對該目標進行多類型的攻擊，並利用多種管道將惡意程式植入特定目標的系統中，以達成攻擊者的目的。

目前我們正處在一個不斷演變的網路環境，對於結合多種攻擊手法，運用殭屍網路進行資訊的蒐集或是攻擊的活動，每隔一段時間就有新的技術問世。而在資訊安全的趨勢分析上，往往會因不同的應用而有新的風險產生，因此隨時掌握資訊安全的發展趨勢以及相關攻擊手法的演變，為當下至為重要的課題。唯有掌握最新的資訊安全趨勢，了解常見的攻擊手法，並對本身系統或應用程式的保護，避免風險的發生以及曝露在不安全的環境中，才是提升本身安全性的不二法門。

（文摘自法務部調查局-清流月刊 102 年 3 月號）

嘉義區監理所 關心您