佛大新聞網
佛光大學
Fo Guang University

公告

網內搜尋 GO

公告

- 佛光大學率先實施新生「收費公立化」措施
- 【人間心燈】林谷芳、羅逸東、林大森-婆娑世界的教育行者
- 「竹板王子」林文彬 漫談說唱藝術
- 淺談「殭屍網路」病毒 (BotNet)
- 學數系資訊志工熱心參與
- 人文學院李紀祥院長致力推動「國際釋奠學會」
- 3D動畫軟體趕熱潮
- 產品與媒體設計系學生自己動手做「公仔」
- 產品與媒體設計學系「設計教學成果展」圓滿落幕
- 天使心．資訊情3

分享朋友

淺談「殭屍網路」病毒 (BotNet)

暫時停止呼吸！！

--淺談「殭屍網路」病毒 (BotNet)

理工學院顏雲生、林昭名／撰稿

危機四伏的網路世界

近年來，隨著網際網路的蓬勃發展，各種相關應用也呈爆炸性的擴張，從

- 標題頁

網頁瀏覽，到電子郵件、檔案下載、網路購物、網路銀行...等，已然成為日常生活的一環。

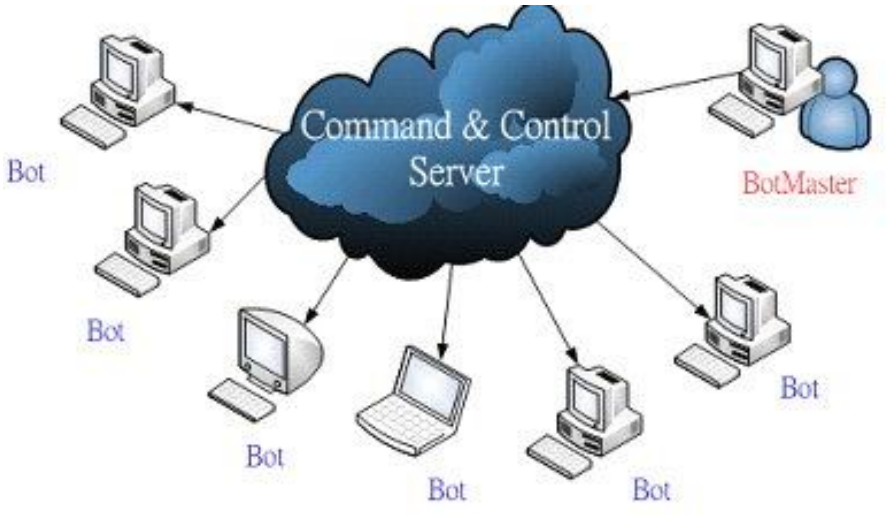
網路強大而多元的功能，為我們的生活帶來極度的便捷，但卻也隱藏了難以預料的危險，有心人士正虎視眈眈，想竊取您的個人資料、信用卡卡號、網路銀行帳號密碼...等資料，以便從其中獲取更大的經濟利益。

什麼是殭屍網路？

「殭屍網路」 (Botnet)，顧名思義就是由許多殭屍電腦所形成的網路。殭屍電腦的來源，大多是因為感染電腦病毒，或是被植入後門，以及隨著即時通訊軟體、電子郵件或電腦系統漏洞的方式，侵入到使用者的電腦，再藏身於任何一個程式裡，伺時展開攻擊、侵害；而使用者卻渾然不知，自己已然成為殭屍網路的一員。

這時「殭屍控制者」 (Botmaster)就可以透過網路，用遠端的方式來遙控這些電腦的行為，進行濫發垃圾郵件/廣告信件(SPAM)、發動分散式阻斷服務攻擊(DDoS)、散播病毒/蠕蟲、竊取個人私密資料等，殭屍網路通常具有主

動攻擊或散播、自我複製，和難以察覺的特性。由於受感染者不易發覺，最近駭客製造出各種變種的殭屍網路病毒，防毒軟體更不易偵測，形成目前網際網路極大的安全威脅，或引起大規模的災情。



「殭屍網路」(Botnet)示意圖

(圖片來源:資訊學系無線網路技術實驗室)

看不見的超級殺手

「殭屍」 (Bot)指的就是被殭屍控制者所控制的電腦，也有人稱為「肉雞」，網路上甚至還出現殭屍電腦的拍賣市場，依殭屍電腦的狀況待價而沽，整個市場頗為活絡。

「殭屍」(Bot)電腦

(圖片來源：http://www.freerepublic.com/focus/f-chat/2230288/posts)

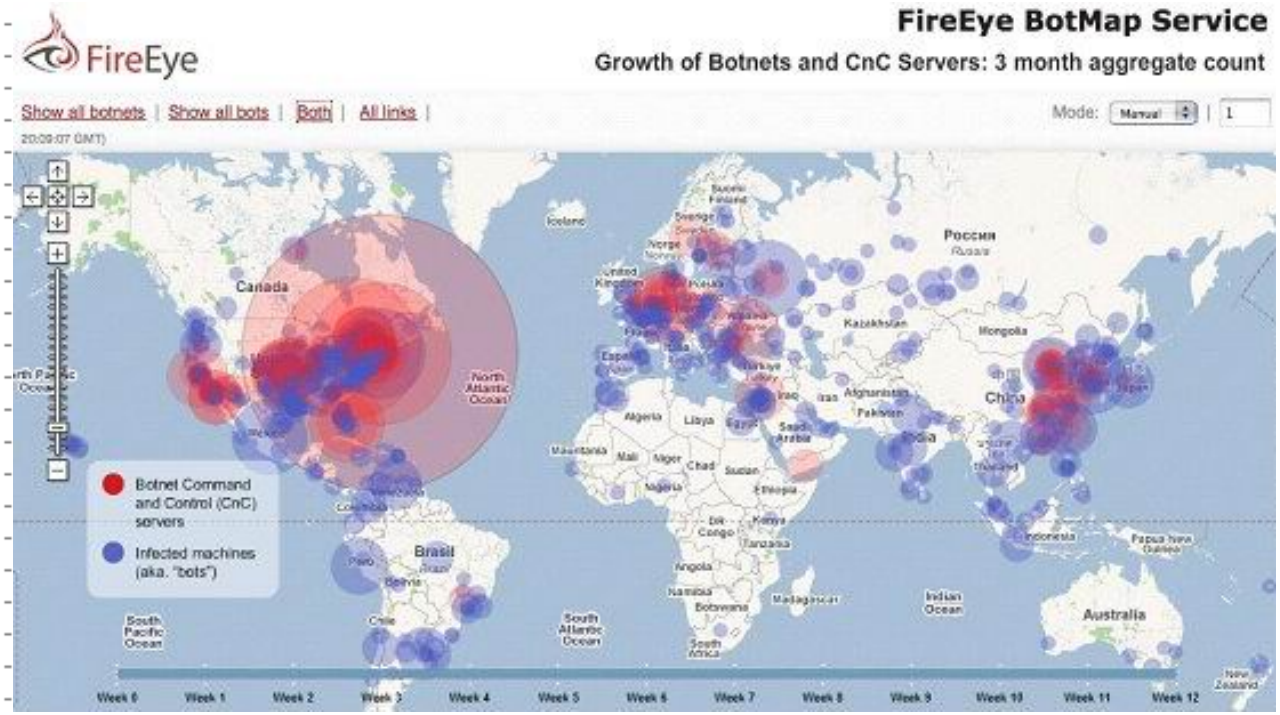
這些電腦為什麼會被稱為「殭屍電腦」呢？主要原因是，一旦遭到Bot感染，就彷彿是殭屍(或傀儡)一樣，任由殭屍控制者來控制；而且，感染Bot的電腦，症狀並不會過於明顯，系統執行的速度也不會受到太多影響，使用者察覺不出很大的差別，所以毫不知情，直到被網路管理者通知自己的電腦正在攻擊別人，成為攻擊的跳板，或是正在散播病毒/垃圾電子郵件時，才會驚覺事情的嚴重性。

台灣蟲害．名列前茅

根據2006年的統計，台灣 Botnet感染的主機大約有八萬八千台，在亞洲僅次於南韓，全世界排名第六名。2008年刑事局偵九隊統計，全台大約有三分之一的電腦遭到植入惡意程式。

紐約電腦安全公司 MessageLabs 的年度報告指出，現在有超過80%垃圾郵件來自殭屍網路。殭屍網路成長的速度非常驚人，根據統計，目前全球將近有七億台電腦連上網際網路，其中大約有百分之十都被植入殭屍程式，也就是十台連上網路的電腦之中就可能有一台是殭屍電腦，比率之高，令人戰慄。

通常殭屍病毒的感染來源，主要是駭客(Hacker)為了欺騙受害者上當，會利用大量垃圾信件，配上最熱門的關鍵字吸引使用者點閱；或是利用社交工程偽裝成親朋好友，降低使用者的戒心；或是先攻陷有弱點的網頁伺服器，在網頁中掛馬攻擊，讓網頁中隱含著惡意程式，一旦使用者點閱電子郵件或瀏覽網頁後，就會立即感染病毒或被植入後門，不知不覺就成為「殭屍網路」的一員。



「殭屍網路」(Botnet)分佈圖

(圖片來源：http://www.fireeye.com/other/botmap/growth/FireEye_BotMap_Accumulate.html)

同時，駭客還可以利用被感染的電腦繼續去感染其他的電腦，來組成「殭屍網路大軍」。例如當一個擁有數萬、數十萬甚至數百萬台電腦組成的殭屍網路大軍，駭客就可以招攬垃圾郵件生意，在適當的時機，透過其所控制的伺服器，一聲令下讓所有殭屍電腦向郵件伺服器發送垃圾郵件。

有些人會認為自己的電腦有安裝防毒軟體，可以高枕無憂；但實際上，現在的殭屍病毒會不斷的變種，而且要產生新的殭屍病毒，對於駭客來說門檻不高，防殭屍病毒軟體實難抵擋這類電腦病毒的入侵，而且常有很多病毒是防毒軟體掃描不到的，使用者幾乎完全暴露在危險當中。

謹慎防範，安全有保障

為了保護自己的資訊安全，避免成為殭屍電腦的受害者，除了電腦要安裝防毒或是防火牆軟體，也要時常更新病毒碼，作業系統部分也要隨時安裝最新的修正程式，並提高使用網路的危機意識，除了不要隨便瀏覽可疑網站，任意閱讀有附件的電子郵件，安裝不明或非法軟體，在網路上也不隨便輸入個人真實資料。

此外，定時備份重要資料，這樣才能快樂的在網路世界馳騁，不會成為駭客眼中的「肉雞」。