解析DDoS攻擊的

楊榮富／大同大學資訊經營學系　　陳志誠／大同大學資訊經營學系

摘要

分散式阻斷服務攻擊一直是網路通訊的重大威脅，也是電腦犯罪專章規範的違法行為。有一些不法者會先組織一個龐大的機器人網路去連結多達百萬台的電腦或設備，並發動兆位元級的大流量攻擊，造成企業或組織的網路服務中斷。因此了解這種分散式阻斷服務攻擊，是電腦犯罪偵查和資訊安全的一個重要研究課題 。本文藉由實驗詳細敘述機器人網路的結構及運作手法，剖析不法者如何連結百萬台的設備，以發動大流量的攻擊。本文的分析有助於犯罪偵查人員處理此類犯罪行為，同時也為網路管理人員提出防禦建議，以強化資訊安全。

關鍵詞 DDoS、氾濫攻擊、分散式阻斷服務攻擊、資訊安全

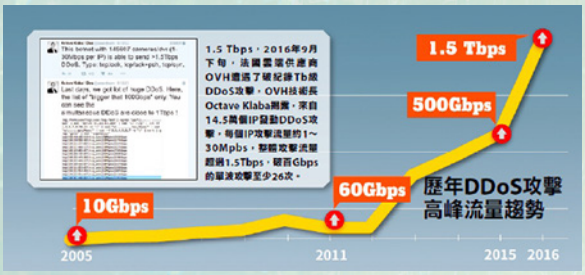
一、引言

在近十幾年來「分散式阻斷服務攻擊」（Distributed Denial of Service, DDoS）不停地出現在每個產業領域的資安攻擊事件中，成為資訊界重要關注的焦點。DDoS是利用網路上已被攻陷的電腦或設備（稱之為「殭屍（Zombie）」作為攻擊者，向某一特定目標電腦（往往是組織或企業的網路伺服器）發動大量的、密集式的「服務」請求（例如Ping連結），藉此耗盡目標電腦的網路資源，使它無法向其他正常使用者提供服務。駭客透過將多個「殭屍」組成的機器人網絡（又稱殭屍網路），就可以發動大規模的DDoS氾洪攻擊（ Flooding Attack）。 另外，他們也可以利用機器人網絡進行增加網站流量以獲取收益、寄送圾垃郵件，癱瘓目標網站，出租網路大軍、甚至於攻擊競爭對手等商業活動。

自從網際網路開放給民用之後，人與人的溝通交流就不再需要親自的面對面才能完成。為了人們之間的連繫更能快速更方便，1988年時，芬蘭的歐蘆大學Jarkko Oikarinen在實驗室裡

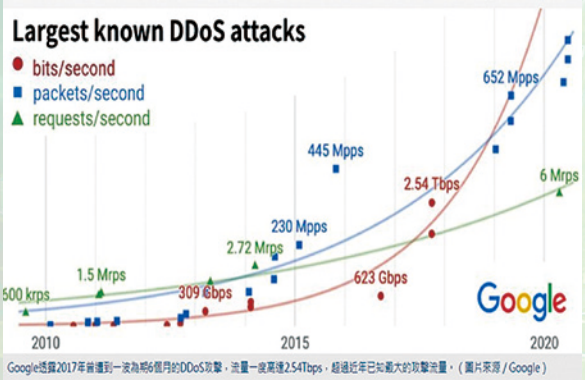
犯罪手法

開發了一套名叫網路交談系統（Internet relay chat , IRC）（Zang et al.,2011）。之後Greg Lindahl在此架構上開發了一款叫做遊戲管理者（Game Manager） 的軟體去自動管理網路電腦遊戲，這一種使用自動化的指令碼高效率完成人類短時間內難以完成任務的軟體，是最早的IRC機器人網路。安裝有這種代理人程式的電腦稱之為Bot；由Bot組成的網路是為「機器人網路（Botnet）」。這種機器人網路有其正面用途: 它被搜尋引擎廣泛使用，收集資料，以回應使用者的服務請求。近年來全球商業在不斷競爭下，機器人網路早已被拿來當作有效服務工具（稱之為網路爬蟲Crawler），支援各種網路商業行為，並且快速持續的擴張。可惜，也有不法者利用它來進行「阻斷服務攻擊」的犯罪。



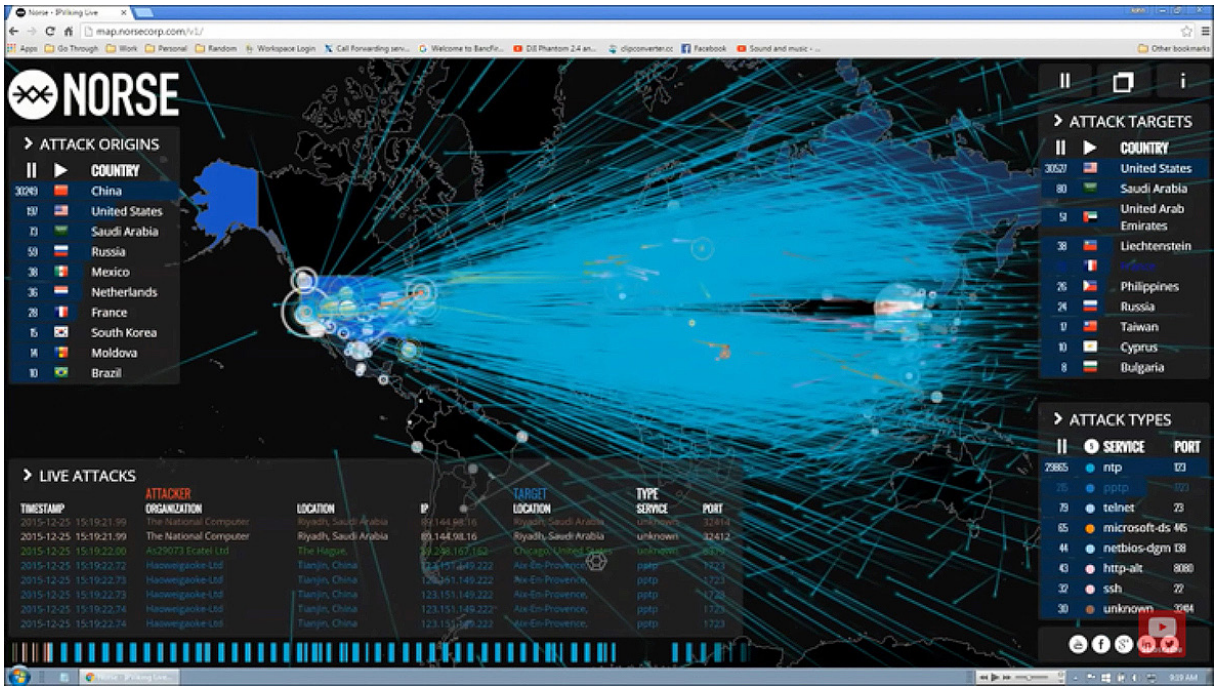
圖一、DDoS攻擊流量呈指數增長的發展勢
資料來源：https://www.ithome.com.tw/news/110135

阻斷服務攻擊可以具體分成三種形式：頻寬消耗型、資源消耗型和漏洞觸發型。前兩者都是透過大量合法或偽造的請求占用大量網路以及器材資源，以達到癱瘓網路以及系統的目的。而漏洞觸發型，則是觸發漏洞導致系統崩潰癱瘓服務；三者的共同特徵都是產生巨大流量（DoS wiki （2023））。例如在法國的網站代管服務供應商 OVH 曾經遭受了流量高達每秒一兆位元（1Tbps）的DDoS 攻擊（IThome,2016）。圖一和圖二中的曲線顯示近年來DDoS攻擊流量呈指數增長的發展趨勢。迄今最大規模的 DDoS 攻擊發生於 2017 年 9 月，該攻擊的目標是 Google 服務，規模達到 2.54 Tbps（DoS wiki, 2023）。



圖二、已知最大的DDoS的攻擊流量
資料來源： https://anquan.baidu.com/article/1447

DDoS攻擊的激烈情形可以由圖三所顯示的看出：這是2015/12/25 Lizard Squad/Phantom Squad – 機器人網絡 / DDoS 攻擊 - 北歐實況錄像，在聖誕節擷取的。 Lizard Squad/Phantom Squad 駭客組織聯手發動DDoS攻擊關閉了 Playstation 和 Xbox 網絡；主要攻擊來自中國，多點對多點發動；攻擊目標在美國，但也在多點多國受影響。Lizard Squad和Phantom Squad是兩個國際駭客組織，主要是為了破壞與遊戲相關的服務為目標，以其聲稱的分散式阻斷服務攻擊（DDoS）而聞名。

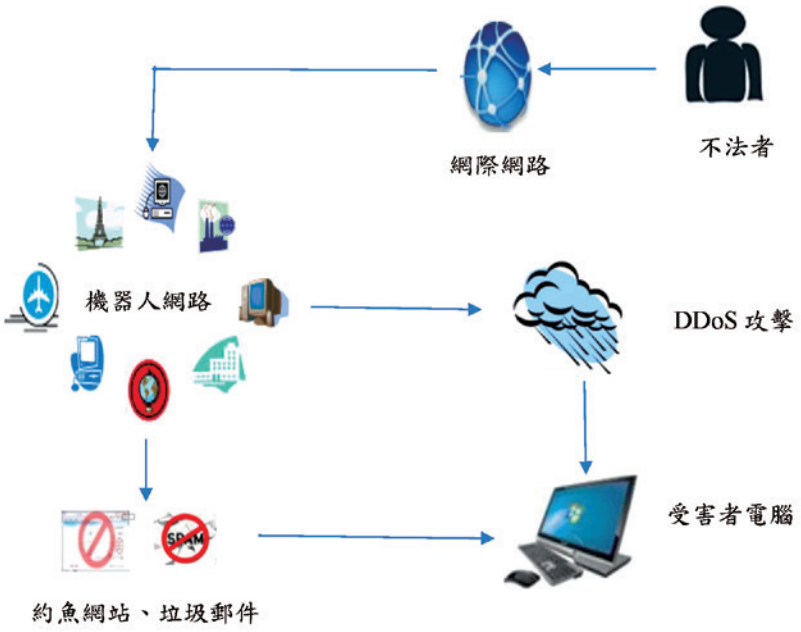


圖三、DDoS 攻擊實況錄像
資料來源: https://www.youtube.com/watch?v=1wq6LIjPHkk

由於組建機器人網路和實施阻斷服務攻擊都是違法行為， 因此本研究將僅藉實驗來模擬不法者的攻擊手法，以獲取必要的數據與知識，用來了解不法者的行為及其危害，並提供資訊安全人員做防護參考。在此，我們首先簡單介紹機器路的架構。

二、機器人網路的架構

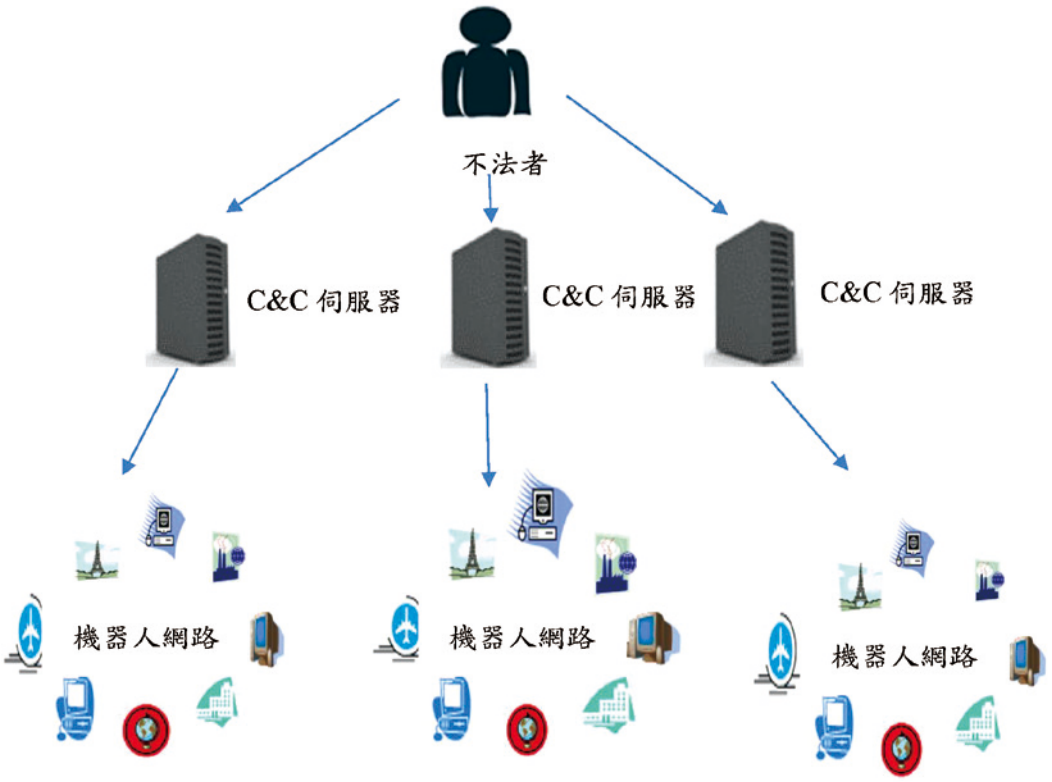
機器人網路是目前最主要的資安威脅來源之一，其運作結構如圖四所示，係由一群被不法者植入病毒的網路設備所構成，不法者可透過這些機器人網路將病毒傳播出去，以感染更多的設備。最後，不法者可以透過操控機器人網路進行一些不法的行為，如惡意的DDoS攻擊、竊取公司內的重要個人資料與機密文件、惡意的散播含有病毒的垃圾或釣魚郵件等（Schaffer, 2006）。



圖四、機器人網路運作結構圖

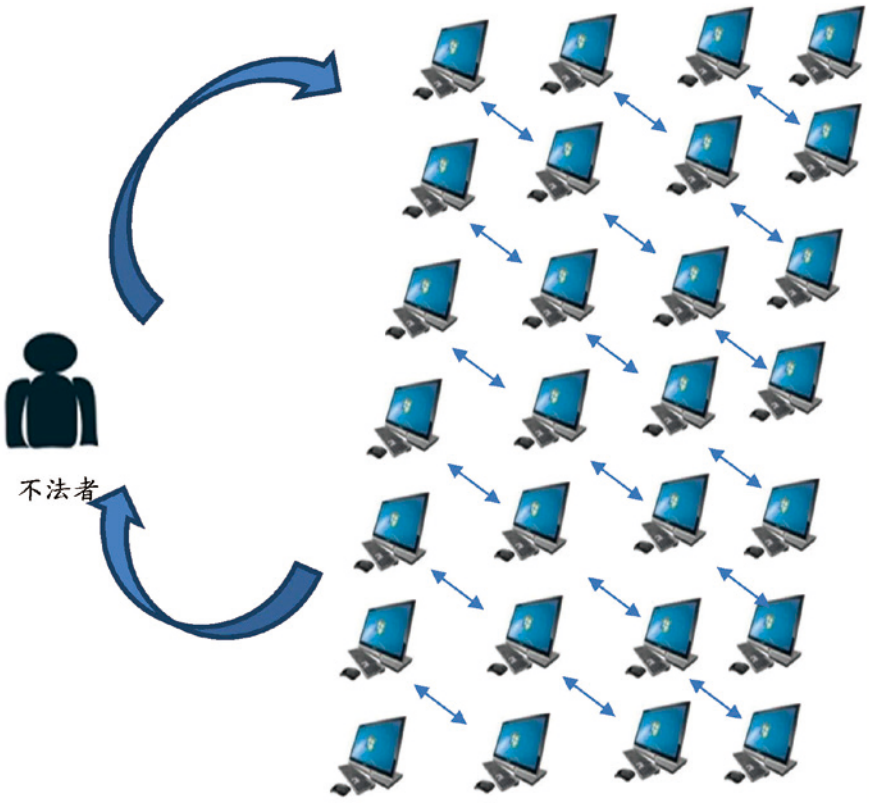
當然，機器人網路不是臨時組成的，而是平時不斷組建而成。提早發現機器人網路的識別，以防範DDoS攻擊已成為一個非常具有挑戰性的話題，特別是因為它們可以被惡意網路攻擊者隨時改變其攻擊策略，大多數的檢測技術仍然無法在早期找到最新的機器人網路。追根究柢其主要原因是它的整體的攻擊方式不斷在蛻變，但原則上仍基於命令和控制的結構基礎。Behal and Kumar（2009）根據文獻研究指出，機器人網路的基本架構可分為有集中式機器人網路（Centralized Botnet）和P2P機器人網路（Peer-to-Peer Botnet）兩種，當然也有混合式P2P機器人網路（Hybrid Peer-to-Peer Botnet）：

（1）中控式機器人網路：中控式機器人網路（Centralized Botnet）是目前使用最為廣泛的一種機器人網路，也是機器人網路發展初期時最常見的架構。如圖五所示，中控式的機器人網路是由主控者藉由將指令發布到中央控管伺服器中，機器人再從中央控管伺服器取得指令來管理整個機器人網路。最常見的溝通模式可根據通訊協定分為Internet Relay Chat（IRC）與Hypertext Transfer Protocol（HTTP）機器人網路。（王欣怡，2011）



圖五、中控式機器人網路架構

（2）P2P機器人網路：在點對點機器人網路（Peer-to-Peer Botnet）中，沒有固定的中央控管伺服器，所有的機器人都有可能是中央控管伺服器。不法主控者可以用隨機的方式向任何一部機器人網路發布指令。機器人也會定期向自己的鄰近節點（Peer）通訊取得最新消息，大家都有機會扮演伺服器的角色負責傳遞指令的工作，如圖六所示（陳天豪，2009）。在P2P機器人網路中，不法主控者不會與固定的中央控管伺服器通訊，機器人間相互通訊是依靠鄰近節點清單（Peer List）維繫，Peer List即為每個機器人所擁有的鄰近節點名單，由於每個機器人擁有大量的鄰近節點，因此機器人網路不會因為部分的機器人被破壞而中斷聯繫，有更高隱蔽性與存活性（Kaur and Behal, 2014）。因為不法主控者與機器人沒有直接的聯繫，網路安全人員無法針對異常流量分析，而追蹤到不法主控者的位址。



圖六、中控式機器人網路架構

Datadrome（2021）目前對機器人網路攻擊的偵測與防範，可以歸納為下列幾種：

（1）即時更新端點防護軟體，以偵查並移除惡意病毒。

（2）收集網路封包流量分析，可事先察覺機器人網路移動之軌跡。

（3）詳細記錄主機log軌跡檔，包括syslog, netlog, dblog等，以作細部比對分析。

（4）導入最新的網路攻擊偵測與防衛工具提高資安防護強度。

為了提升機器人網路的存活率與網路資料傳遞效能更有人發展出Fast-flux技術（曾仲強，2009；蔡秉澂，2015）。大部份不法者會選擇管制較鬆散的區域性的網域註冊公司來設定 Fast-flux，以規避嚴謹法令與實際作業的審核。使用Fast-flux 技術的機器人網路運作方式如下 :

（1）惡意者將單一個特定的域名（Flux.合法註冊.com）對應至多個 IP 位址，平時這些網路機器人（10.0.2.1/24）對應的IP皆為一般安全的服務主機不會被察覺。

（2）一旦網域擁有者計畫要進行惡意行為的時候，就會事先更換網域的連結至惡意的單一組IP來傳送訊息資料。

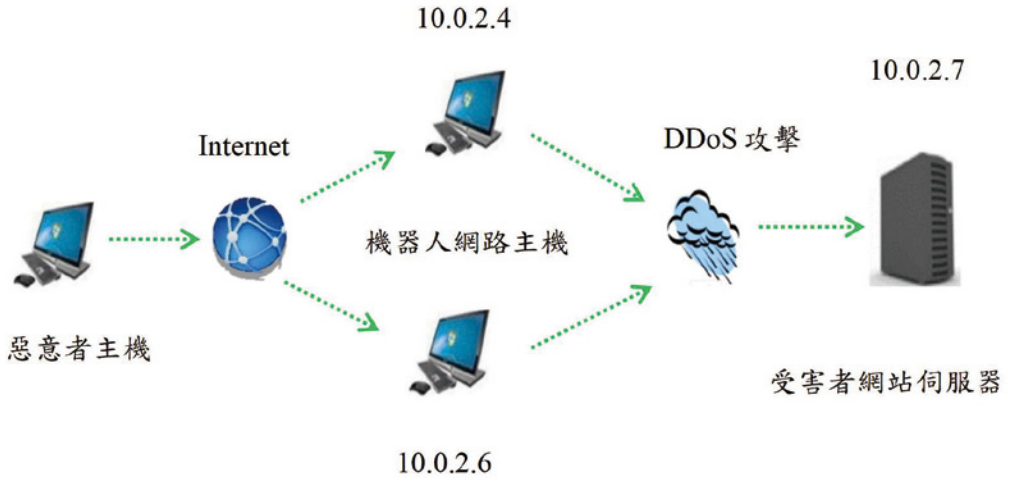
（3）在這種架構裡，當惡意者對受害者主機短時間下達指令的操作過程中比較隱密，惡意的IP因為只有短暫的出現就比較不容易被偵測發現，而招至瓦解失聯。

組建Botnet和進行DDoS攻擊，在網路上都有可資利用的資源（表一）。為進一步了解機器人網路的組建和分散是阻斷服務攻擊，我們將藉由實驗，以獲得必要的數據和知識。本研究所使用的程式則由Python語言撰寫而成，整合惡意攻擊工具brutespray及goldeneye，最後使用nginx架設簡易網站模擬受害者，並用iptop流量監控工具來顯示受害者主機在受到DDoS攻擊時當下的網路流量。

表一、組建Botnet和進行DDoS攻擊的工具設備

名稱	功能
Ubuntu OS	Linux 作業系統
brutespray	Python惡意腳本工具
goldeneye	持續性與目標建立連線工具
multiconn-client	點對點連線監控工具
nginx	簡易網站架設軟體
iptop	主機型網路流量監控工具

至於實驗的模擬環境則是封閉的實驗室，與外界無網路連結。我們在實驗環境裡指定一台不法者的Linux 控制主機，二台為一般不知情的Linux受害者主機組織成機器人網路，另外設定一台為正常提供網路服務的Linux網站主機為DDos攻擊受害者目標如圖七所示：左方是惡意攻擊者的電腦（Botmaster），右方（IP：10.0.2.7）是攻擊目標，中間兩個設備構成一個簡單的機器人網路。



圖七、實驗網路架構示意圖（攻擊目標為10.0.2.7）

三、 機器人網路的組建

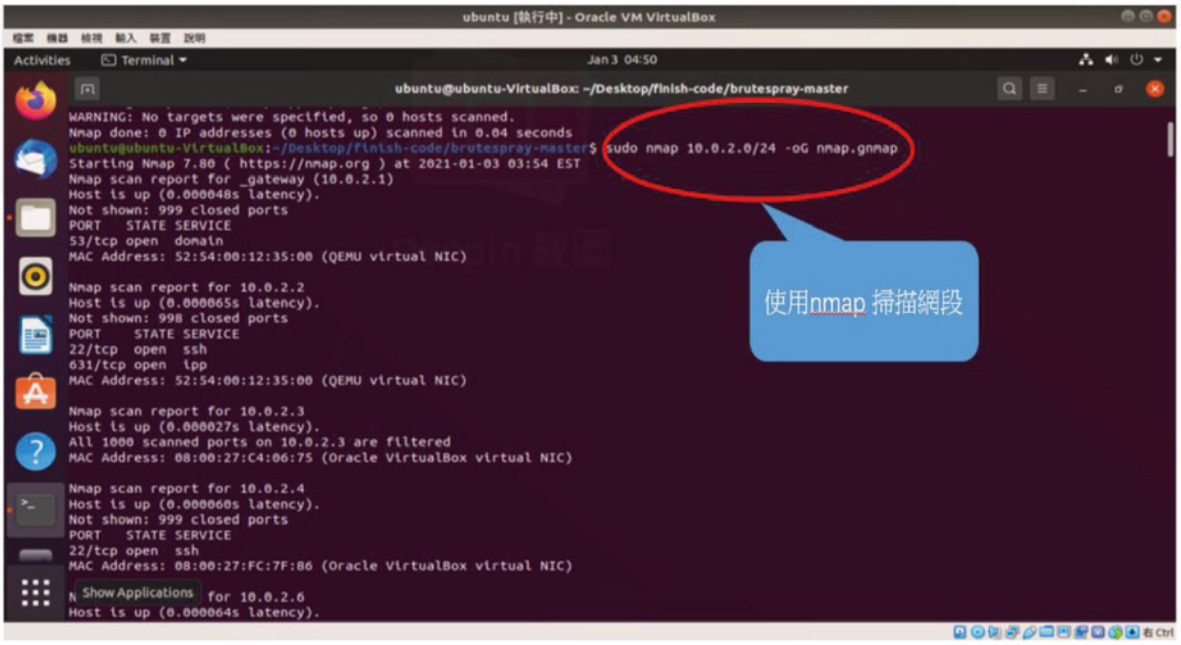
無論多麼龐大的系統，都是由一個個具體的元素組成的，機器人網路也是一樣。我們在討論系統的組建時，一般會討論兩個方面：「組成系統的元素是什麼?」以及「這些元素是如何相互聯繫起來的?」。對於機器人網路來說，就是分別對應到機器人網路的節點和控制方式。機器人網路由大量功能節點共同組成，這些節點可能是普通PC、伺服器或移動設備（手機及平板電腦）。通常將一個普通的節點變成機器人網路的主機，一般要經歷三個過程，即感染中毒、接入機器人網路以及命令執行。

在感染中毒的步驟裡惡意者使用的手法我們可分為主動式攻擊及被動式攻擊兩種方式。被動式攻擊手法如使用社交工程（如寄送惡意垃圾信件、架設惡意網站），惡意者在大量的寄送垃圾郵件上夾帶惡意附件或架設惡意網站上佈署惡意病毒，這些具有惡意危害系統的行為如蠕蟲、木馬、後門等。這種手法必須等待不知情的受害者點擊開啟動作後，攻擊才能成功。隨著物聯網（Internet of Things,IoT）技術的發展，駭客的攻擊目標不再局限於電腦或手機設備。而我們周遭的各種事物也隨處可見與IoT結合的場域，無論是工作環境、校園、企業、交通工具、家具甚至醫療設備等，都與網路息息相關。在資安思慮方面，IoT設備相較於電腦，缺乏完善的防護機制，只要設備上出現安全弱點，駭客便可輕易地藉由漏洞植入惡意軟體，將其納為麾下進行惡意行為。其中最常被利用的安全漏洞是IoT設備的出場預設密碼往往很簡單，例如「0000」或「1234」，很容易被入侵而受控制。2016年，有攻擊者把對攻擊對象轉移到了大量出現的 IoT設備，Mirai 惡意程式就是其中之一。它被人研究出並被人利用取得大量監控攝影設備並發動了 DDoS攻擊。

至於主動式攻擊的方式是採取暴力破解密碼的手段入侵電腦及設備；龔恩緯（2011）對此有較詳細的介紹。這種攻擊手法的好處是惡意者能立刻得到攻擊是否成功的答案，可以完全掌握時間。一旦受害者主密碼破解成功立即上傳安裝好受害者主機上的後門監控軟體，便通過解析內置的域名及通訊埠進行聯絡，構建網路通道加入機器人網路，這些都是透過網段掃描工具收集整理而來可攻擊的系統資訊。在受害者的設備成功加入機器人網路後，不法者利用每台回傳的系統權限帳密資料，整理歸類成Peer List 檔案，並不定時確認這些受害的機器人網路系統狀態，等待後續發動DDoS攻擊指令。

在組建Botnet之時，首先是網路掃描尋找入侵對象，不法者可以利用PortSacn掃描公共IP網段的主機上開放可運作的網路服務埠: 用brutespray工具下達指令搜索鎖定網域的範圍，尋找有開放埠 22 （SSH通訊埠）的主機。不法者下達“sudo nmap <<網段>> -oG nmap.gnmp”的指令掃描該網段設備，掃描結束後會回報易受攻擊的設備或服務系統，並產生一個nmap.gnmap的結果檔，以此確認可攻擊的主機（圖八）。此階段是網絡攻擊者利用該服務已知的漏洞探測

目標主機。



圖八、掃描網段的設備（實驗案例中的網段是: 10.0.2.0/24）

接下來是對鎖定的目標對象進行密碼破解，以便進行控制。不法者可能使用brutespray python腳本，進行通訊埠掃描和針對掃描服務的自動暴力攻擊。使用nmap進行掃描後，再用GNMAP / XM輸出文件圖九所示，以暴力破解帳密攻擊的方式來強行使用nmap掃描後可用的通訊埠服務主機。不法者可以下達“python3 brutespray.py --file 22.xml --threads 5 --hosts 5”指令，逐一對名單內的IP主機的暴力破解程序。完成後，會在程序目錄/brutespray-output/的目錄下生成ssh-success.txt檔案，再使用“cat ssh-success.txt”命令查看破解成功的結果。

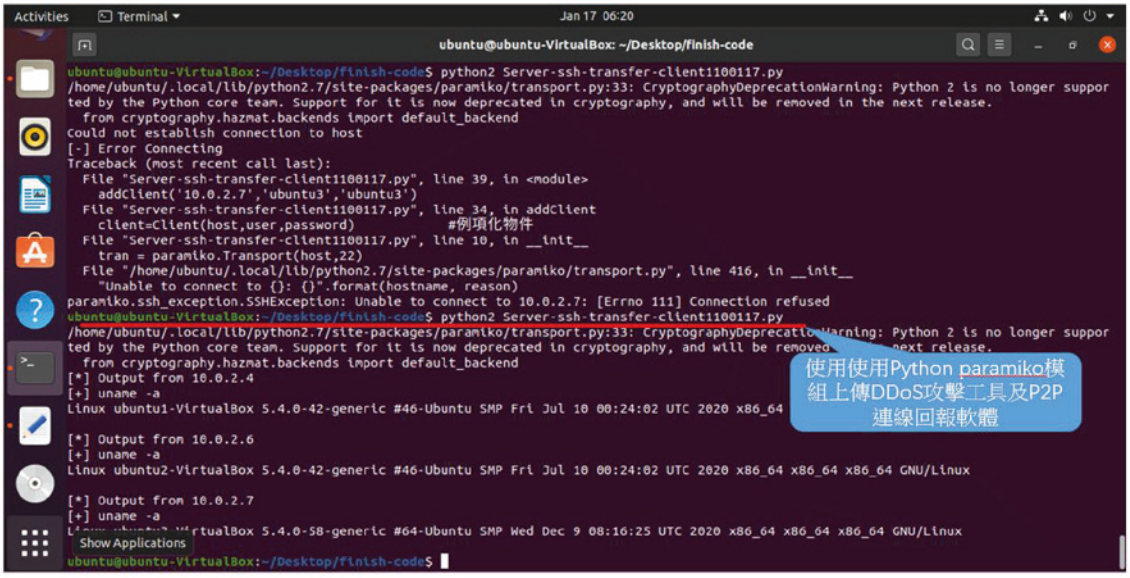
圖九、GNMAP / XML輸出檔案

五、 機器人網路的DDoS攻擊

機器人網路是聯合眾多有連網能力的計算機所組成的一個攻擊平台，不法者利用自已可操控的機器人網路可以發動各式各類客製化的系統攻擊，可以導致整個硬體基礎系統架構或軟體重要服務系統癱瘓，或造成擴大電腦病毒感染的範圍從事螢幕背後的一些惡意計劃。

不法者利用以取得掌控權成功組建機器人網路之後，並安裝好DDoS工具在每台「殭屍」上，確認好目標服務網站，即可從中控主機集團下達同步DDoS攻擊指令給機器人網路群組，接受到攻擊指令的機器人立即從本身的主機持續不斷產生大量網路流量封包，湧進目標系統服務網站以造成網路擁塞，使得一般正常用戶端訪客無法連線，網站無法再提供服務。

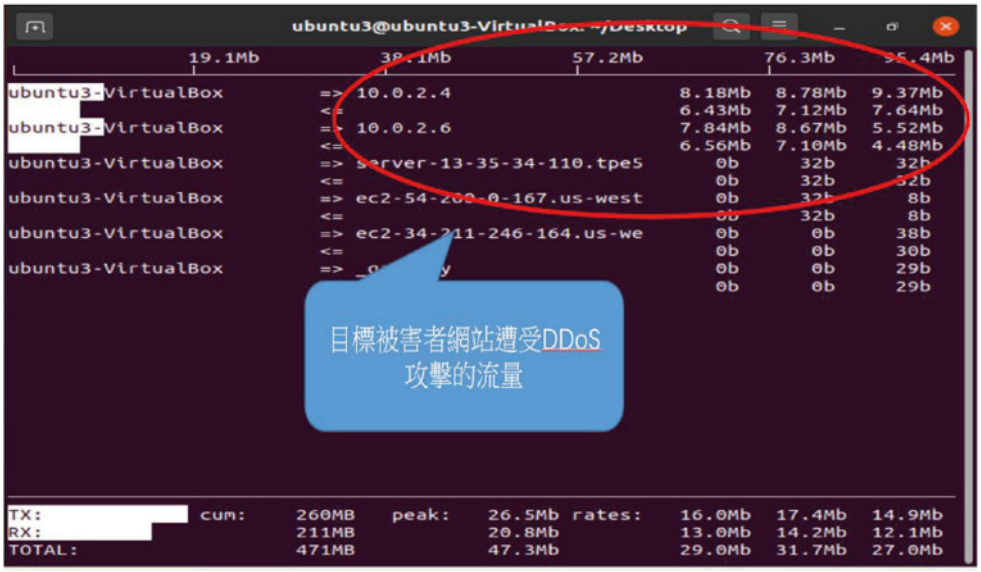
以下以一個具體的手法，說明駭客如何進行DDoS攻擊。首先是建立駭客主機和機器人網路之間的連結，這個連結往往會有數條，不只是一條線，以防單線被切斷而失去對他們對整個網路大軍的控制。 它們可以利用paramiko P2P SSH v2 加密協定的第三方模組，進行與多台機器人網路主機進行遠端連線（如圖十所示）: 在駭客主控主機下達“python2 Server-ssh-transfer-client1100117.py”指令，並上傳DDoS攻擊工具goldeneye，且植入P2P連線監控軟體multiconn-client到這些機器人網路主機。



圖十、駭客與（兩台）機器人網路主機的遠端連線示例

在不法者的主控主機取的與機器人的網路取得聯繫之後，不法者就可以利用goldeneye工具，遠端同時下達DDos攻擊指令。攻擊者利用 “python2.7 /home/ubuntu/goldeneye.py http://<<受控主機位址:通訊埠>>/ -s 5 -m random”指令，讓受控主機發動DDoS攻擊。同時，不法者可利用iptop網路監控流量工具看到受控「殭屍」湧入攻擊目標的網路流量，平均每台約發

送大約8Mbps的攻擊流量，造成目標主機的對外服務受影響如圖十一。



圖十一、受害者主機大量的網路流量湧入

DDS攻擊的模擬數據分析

在以上的模擬實驗中，我們得到了一些參數如表2；其中我們特別感興趣的是

暴力破解一台設備所需時間約為21.15小時；

上傳DDoS攻擊指令所需時間約為5秒；

一個受控機器人可能產生的攻擊資料流量大約為8Mbps。

表2、DDoS實驗相關參數（僅供參考，環境及設備不同，參數亦將不同）

預設破解使用的帳號	50組
預設使用的破解密碼數量	250組
掃描網段<<30台設備>>的時間	11.03秒（不考慮機器效能及外在因素）
破解程式猜測驗證一個密碼的時間	6秒（不考慮機器效能及外在因素）
單台機器人網路主機帳號設定在50組內及密碼設定在250組內被破解時間	約21.15小時（不考慮機器效能及外在因素）
機器人網路暴力破解成功總花費時間	約43.45小時（不考慮機器效能及外在因素）
單台機器人網路產生的網路流量	8Mbps
機器人網路接受DDos攻擊指令的時間	約為5秒（同一個網域內）（不考慮機器效能及外在因素）

如果我們擴大模擬機器人網路規模，進行DDoS攻擊，在理想的情況下，只要約需集結超過100萬台受控設備，即可所產生出來大約1 Tbps級別的最大攻擊流量。 而目前所知，最大的機器人網路如所使用最大機器人的數量根據資料顯示: Kido駭客組織的機器人網路就集結了10,500,000台；Oficla駭客組織的機器人網路更多達 30,000,000台 （Botnet wiki， 2023）。可見駭客要組建一個百萬大軍的殭屍網路並不困難。另外，請注意: 這裡所說的理想情況主要是指防禦方的網路管理人員未採取限制流量措施，以及機器人網路的所有攻擊節點未被破壞。

在2021年Journal of Cyber Security的一篇研究表示影響機器人網路水平的好壞另一個技術因素是不良的網路衛生環境（Cyber Hygiene）或一個國家是否可被利用來放大DDoS攻擊的潛在漏洞的數量。機器人網路可以通過一種稱為「反射的技術」來放大DDoS攻擊的影響。不法者使用他們被感染的「殭屍」發送數以千計小量假的請求，用以開放的雲端伺服器，欺騙自己的IP地址，使其看起來像攻擊的目標是一個發送請求數據的索引擎。這種技術允許較小型的機器人網路產生巨大影響，使攻擊的強度可以提高到多達179倍。這意味著，如果一個機器人網路若控制了100,000台設備，可以利用此漏洞擴大其攻擊能力，從而產生1790萬台規模的大型殭屍網路的影響能力；所有DDoS攻擊中約80–90%使用此技術。（Haner and Knake, 2021）

六、資安防護問題討論與結論

利用破解密碼入侵他人電腦/設備，建立殭屍網路，將觸犯刑法第358條「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者」的罪責。如果進一步發動惡意的DDos攻擊，可能會觸犯刑法電腦犯罪專章的360條「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於

公眾或他人者」的罪責；兩者均可判處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

本文中我們敘述了不法者如何組建機器人網路，並如何發動DDoS攻擊。然而根據實驗數據顯示，破譯密碼所需的時間很長，建構一個機器人網路大軍需要的時間更長，所以資安防護人員平素就應提高警覺，發現是否有電腦設備被入侵，及時排除，瓦解整個機器人網路。

其次，不法者可能會利用通訊埠掃描（Port Scan），得悉哪些設備的Telnet （Port 23），FTP （Port 21），HTTP（Port 80） 是可以利用的，以建立一個龐大的機器人列表。 因此，網路管理人員必須加強對這些通訊埠的管理。

最後，不法者可能利用社交工程手法，例如利用釣魚郵件詐騙收件人，或崁入式惡意的點擊連結，來組建殭屍網路。甚至於更簡單的利用用戶懶得修改預設密碼的疏忽，以廠商預設帳號密碼來控制IoT設備。這些安全管理鬆散的設備很容易讓不法者得手。

在了解機器人網路的攻擊方式後，我們就可以對DDoS攻擊採取防範措施，如何停止和防

止機器人網絡攻擊的具體方法，建議如下:

（1）保持軟件更新: 養成定期更新軟件和操作系統的習慣。就不會因為忽略更新軟件而被惡意軟件或任何其他類型的網路安全威脅感染。（尹碩楷，2014）

（2）密切監控網路: 密切監視網路中是否有異常活動。如果對典型的流量以及一切通常的行為方式有了更好的了解，有利於網路管理。可利用設定排程方式執行檢測異常行為的分析和數據收集解決方案來對網路進行24小時監控。（王品翰，2018）

（3）監視失敗的登錄嘗試: 機器人網路通常會經過測試大量的用戶名和密碼組合破解主機，以便獲得對用戶帳戶的未授權訪問。監視通常的失敗登錄嘗試次數將幫助我們建立基線，以便我們可以設置警報，以通知失敗登錄的任何高峰，這可能是機器人網路攻擊的跡象；尤其在頻繁登錄嘗試時間超過一天以上的情況。

（4）為了避免組織因DDoS攻擊而服務中斷，目前企業多數會加購Bypass模組。雖然設備跳到Bypass模組時，系統一定有警告和Log可查詢，但網路管理人員千萬不能以為攻擊停止而輕忽此潛在威脅的警告。目前駭客可能此假借DDoS攻擊之名，進行嚴重性持續威脅（Acute Persistent Threat, APT）攻擊，這是一種新的危害轉變。不法者可能鎖定政府網站以竊取更多機敏資料，或鎖定電子商務和購物網站以竊取用戶資料。 及另駭客若無法獲得及時財務利益，也可轉賣給詐騙集團。

總上所述，本研究之分析為網路犯罪偵查與鑑識人員提供了對DDoS攻擊行為一個較明顯的輪廓，同時也提供了網路安全管理人員一些防範的建議。為有效縮短威脅偵測時間並縮小攻擊影響範圍，提高網路流量可視性與可管理性，以填補防禦缺口，也是未來研究的重點之一。

FACT

參考文獻

1.王欣怡（2011），殭屍網路之攻防架構與分析研究，逢甲大學資訊傳播工程學系碩士論文，第9-14頁，2011/06。

2.王品翰（2018），一個基於蜜罐日誌序列分群的Modbus TCP協定入侵偵測方法，國立中興大學資訊科學與工程學系碩士論文，第8-14頁，2018/06。

3.尹碩楷（2014），建構雲端運算之殭屍網路型分散式阻斷服務攻擊的有效防禦技術，大葉大學資訊管理學系碩士論文，第12-19頁，2014/07。

4.陳天豪（2009），透過封包分析偵測並瓦解殭屍網路，國立中央大學資訊工程學系碩士論文，第25-29頁，2009/01。

5.蔡秉澂（2015），主動式偵測 DGA Domain-Flux 殭屍網路惡意網域機制之研究，國立屏東科技大學資訊管理學系碩士論文，第8-12頁，2015/12。

6.曾仲強 （2009），DNS舊技術新玩法 - Fast Flux，國家資通安全會報技術服務中心資安文章，https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1131，2009/12。

7.楊榮富（2021），隨機組態機器人網路攻擊之分析研究，大同大學資訊經營系碩士論文，2021/07。

8.龔恩緯（2011），SSH字典攻擊BotNet 聯合入侵模式與攻擊密碼特徵分析之研究，國立高雄大學資訊管理學系碩士論文，第1-12頁，2011/01。

9.Behal, S. and Kumar, K.（2009）. “Classification of C & C based Botnet Architectures,” International Journal of Engineering & Information Technology, ISSN 0975-5292, Vol. 1（2009）, pages 28-32.

10.Behal, S., Kumar, K. and Arora, V.（2008）. “Classification of Flood Based DDoS Attacks,” Proceedings of International Conference on Wireless Networks and Embeeded Systems （WECON）, Pages 521-524, October 18-19, 2008.

11.Botnet, wiki （2023）. https://en.wikipedia.org/wiki/Botnet, 存取日期: 2023/04/28

12.Datadrome （2021）. How to stop and prevent botnet attacks on your website and server? https://datadome.co/bot-detection/how-to-stop-and-prevent-botnet-attacks-on-your-website-and-server/ Accessed on 2021/02/10.

13.DoS, wiki （2023）. https://en.wikipedia.org/wiki/Denial-of-service_attack, 存取日期: 2023/05/05

14.Haner, J. and Knake, R.（2021）.“Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity”, Journal of Cyber Security,https://academic.oup.com/cybersecurity/article/7/1/tyab003/6248895?searchresult=1, 2021/04/24. Accessed on 2021/05/19.

15.Kaur, N. and Behal, S.（2014）. P2P-BDS: Peer-2-Peer Botnet Detection System, IOSR Journal of Computer Engineering （IOSR-JCE） e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. V （Sep – Oct. 2014）, PP 28-33.

16.Oikarinen, J. and Reed, D.（1993）.Internet Relay Chat Protocol,Network Working Group,1993.

17.Schaffer, G.（2006）. "Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats", IEEE Security & Privacy, 2006.

18.Zang,X., Tangpong, A., Kesidis,G. and Miller,D. J.（2011）, "Botnet detection through fine flow classification," Unpublished, Report No. CSE11, vol. 1, 2011