分散式 Denial-of-Service 攻擊事件的觀察

張智晴　林盈達
交通大學資訊科學系
ydlin@cis.nctu.edu.tw
6/5/2000

摘要

今年年初 Yahoo、Amazon、CNN 和 eBay 的被攻擊事件是採用一種所謂的分散式阻斷服務攻擊(Distributed Denial of Service attacks)，不同於去年 8 月間，兩岸的政府網站被入侵者竄改網頁的是，這次電腦系統並沒有真正的被入侵，資料也沒有被盜取或是竄改，而是攻擊者利用分散於不同地方且已侵入的多部電腦主機做爲"打手"，發送大量僞造來源地址的封包，癱瘓受害者所在的主機伺服器，使得該網站無法服務正常的使用者。本文探討這類攻擊手法以及使用的幾種工具。

關鍵字：DoS、DDoS、Trinoo、TFN、TFN2K。

1. 駭客任務 -- DDoS

關於這次引起 Yahoo、Amazon、CNN、eBay 等知名網站癱瘓，導致無法提供正常服務的事件，並非是直接入侵該網站所引起的，而是利用所謂的 DoS(Denial of Service)[1]所發動的網路攻擊。其方法是利用程式在瞬間產生大量的網路封包，癱瘓對方之網路及主機，使得正常的使用者無法獲得主機提供的服務。此外，這次攻擊是採用分散式方法的 DDoS(Distributed DoS)[2]，攻擊者事先入侵 Internet 主機安裝攻擊程式，發動攻擊時，同時產生連續性的攻擊，造成目標主機所提供之服務癱瘓。

造成這次事件的主因，到現在還沒有定論，一個可能的說法[3]是，爲了 Y2K 這個特別的時間點，駭客們計劃了一個想讓世人注意的行動。這個行動的內容是在 2000/0/0 00:00:00 時癱瘓美國重要網站，但是因爲 CERT 在之前就收到有關 DDoS 攻擊和相關程式的訊息，加上美國對 Y2K 保持高度警戒，使得這個原本應在千禧年發動的癱瘓任務暫時打住。而就在大家慶幸於安全通 Y2K 危機後，這個早已計劃的癱瘓任務就在大家失去戒心下開始行動。先是雅虎入口網站(Yahoo)，然後是拍賣網站電子灣(eBay)、購書網站亞馬遜(Amazon)以及新聞網站美國有線電視新聞網(CNN)，都慘遭癱瘓而不能提供應有的服務。

受到 Open Source 概念的影響，駭客們也開始公開自己開發和使用的程式，使得入侵工具的發展更快更成熟。大約在 1999 年 6 月時，DDoS 及其他入侵工具已被發展出來，並先後利用這些工具攻擊了英國、德國、韓國網站與美國太空指揮部 NASA，接著有計劃的展開 Y2K 駭客任務，儘量在 Y2K 前入侵爲數龐大的機器裝置之後門(back door)，以便在 Y2K 當天進行大規模的癱瘓行動。不過由於入侵太空指揮部 NASA 的行動引起了 CERT 的高度重視，並在 1999 年 12 月份發出好幾次警訊提醒所有官方與民間的系統管理人員，又由於 Y2K 當天許多單位的 Router 關閉以避免 Y2K 危機。這兩個因素導致 Y2K 的癱瘓任務暫時打住。

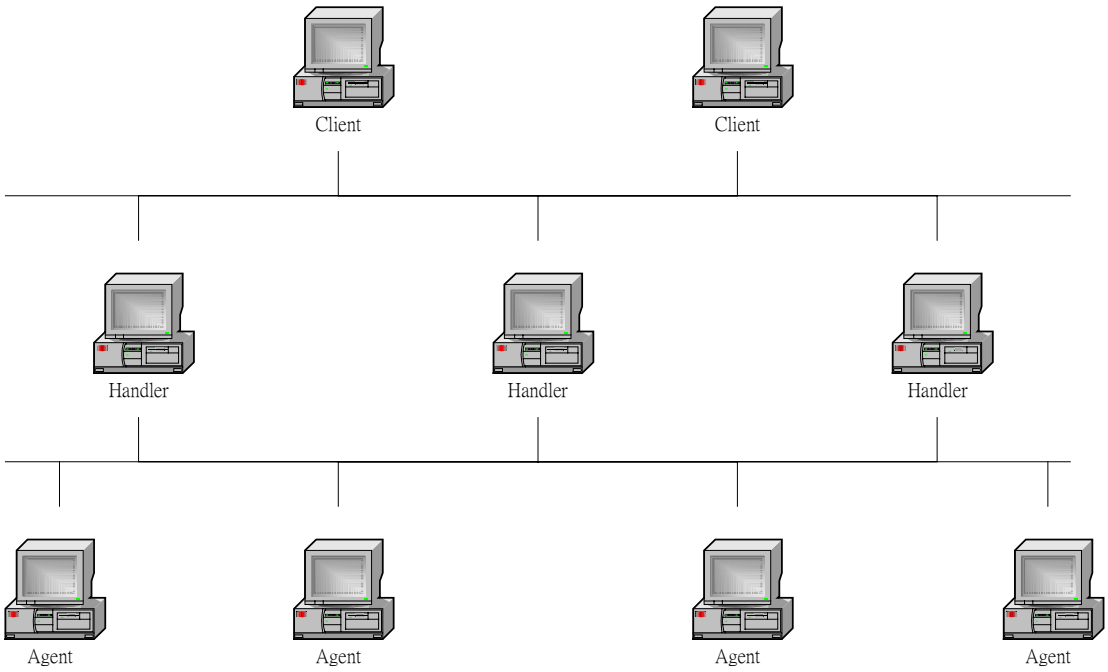
2. 攻擊方法

這次攻擊 Yahoo、Amazon、CNN 和 eBay 的事件是採用一種所謂的分散式阻斷服務攻擊(Distributed Denial of Service attacks)，不同於去年 8 月間，兩岸網站被入侵者竄改網頁的是，這次電腦系統並沒有真正的被入侵，資料也沒有被盜取或是竄改，而是入侵者利用分散於不同地方的多部電腦主機，發送大量僞造來源地址的封包，癱瘓受害者所在的網路電腦主機伺服器，使該網站無法服務正常的使用者。

所謂的阻斷服務攻擊是指在特定攻擊發生後，被攻擊的對象不能及時提供應有的服務，例如全球資訊網網站無法接受使用者的要求提供資訊，電子郵件伺服器不能提供收發信件服務等。一個最常見的模式是，攻擊者用大量的網路封包癱瘓對方之網路或主機，使得正常的使用者無法獲得主機及時的服務。

阻斷服務攻擊由於是用單點發送僞造的大量網路封包，使用簡單的流量監測系統就能根據來源找到攻擊者，爲了改善這個缺點，也爲了更好遙控阻斷服務攻擊的發動，駭客們將原本單純的阻斷服務攻擊改成多層式架構(multi-tier)並發展分散式多點技術。也就是說，透過流量監測系統的過濾後，您只能將駭客發動攻擊的區域縮小，而且就算您找出這些位址，也可能只是駭客的一些事先入侵成功的主機，而真正的駭客可能躲在好幾層受害主機後面。駭客可以用許多入侵手法佔領一些主機，例如尋找主機上的伺服程式之漏洞或寄含有病毒程式的精彩圖檔之郵件，許多主機的主人都不知道自己已被入侵。

分散式阻斷服務攻擊可以用圖一來解釋，攻擊者從 client 端控制 handler，每個 handler 控制許多 agent，因此攻擊者可以同時命令多個 agent 來對被害者做大量的攻擊。而且 client 與 handler 間的溝通是經過加密的。



圖一、DDoS 多層架構

這次入侵事件使用的攻擊工具有兩種，一種是 Trinoo[4]，另一種爲 Tribe Flood Network(TFN)[5]和 TFN2K。

Trinoo 是一個主從式架構的分散式阻斷服務攻擊程式，攻擊方式是 UDP flood 攻擊(UDP flood attacks)。一個 Trinoo 攻擊網路包含數個主控端(masters)與數量更多的守護神常駐程式(daemons)。駭客首先連接上主控端，下達攻擊命令(如攻擊目標的 IP 位址，何時發動攻擊和其它參數)。主控端獲得攻擊命令後，會連接上所有守護神常駐程式，由守護神常駐程式來做真正攻擊。

以下是攻擊的步驟：

1.駭客連接主控端：利用連接埠 27665/TCP

2.主控端連接守護神常駐程式：利用連接埠 27444/UDP

3.守護神常駐程式回應主控端：利用連接埠 31335/UDP

4.守護神常駐程式開始攻擊被害者：開始 UDP port 阻斷服務攻擊。

TFN 是一種更強的主從式架構的分散式阻斷服務攻擊程式，它的攻擊網路架構與 Trinoo 類似，不過它提供更多種類攻擊方式，而且它的主從程式間是利用 TCP/IP 的 ICMP 來溝通。

TFN 提供的攻擊方式有：

UDP 洪水型攻擊(UDP flood attack)[6]

TCP 同步訊號洪水型攻擊(TCP SYN flood attack)[7]

ICMP 回應要求洪水型攻擊(ICMP echo request flood attack)

Smurf 攻擊(Smurf attacks)[8]

而 TFN2K 增加了：

混合型攻擊(M attack)

Targa3 攻擊(Targa3 attack)

這些攻擊的概述如下：

UDP 洪水型攻擊(UDP flood attack)：攻擊者送出大量 UDP 封包(可能僞造來源位址以避免被追蹤)給被害者，使被害者的網路擁塞甚至中斷。

ICMP 洪水型攻擊(ICMP echo reply flood attack)：攻擊者產生大量的 ICMP echo request 封包(可能僞造來源位址以避免被追蹤)給被害者，被害者會回應等量的 ICMP echo reply 封包，使被害者的網路擁塞甚至中斷。

TCP 同步訊號洪水型攻擊(TCP SYN flood attack)：TCP 建立連線需要三個步驟(three-way handshake)，攻擊者對被害者發出連續的連線要求(SYN 封包)，並將這些 SYN 封包填入不存在或不正確的來源位址，被害者接著會送出 SYN ACK 封包並等待 ACK，但是由於來源是不存在或不正確，所以被害者不可能收到要求端的 ACK，造成被害者的等候佇列被填滿而無法再接受建立連線的要求。

Smurf 攻擊(Smurf attack)：攻擊者將僞造來源的 ICMP echo request 封包送到 IP broadcast addresses，而來源位址設成被害者的位址，造成 broadcast addresses 回傳大量的 ICMP echo reply 封包給被害者，使被害者的網路擁塞甚至中斷。

混合型攻擊(Mix attack)：攻擊者依序使用 UDP 洪水型攻擊、ICMP 洪水型攻擊和 TCP 同步訊號洪水型攻擊法，以避免 Router 偵測單一型式的攻擊。

Targa3 攻擊(Targa3 attack)：由於各個作業系統廠商在實作 TCP/IP 時，有些灰色區域 RFC 並沒有定義的很清楚，如 OOB 的處理，IP stack 的作法，IP 封包切割與回組等等。攻擊者送出這些介於臨界點的封包，可能會導致作業系統當掉，網路停止運作或其它不可預期的行爲發生。而 Targa3 是收集 19 種這類型程式的程式。

3. 結語

這次入侵事件造成的影響層面相當廣，可以分成三部分討論：

對被攻擊者的影響：

直接影響：因爲無法繼續服務使用者，交易無法進行，造成金錢的損失。

間接影響：可能有使用者認爲這次入侵事件是真正的入侵，資料已被盜取及修改，造成對該公司的不信任，使該公司的信譽損失。

對使用者的影響：無法使用該服務，可能是查詢(Yahoo)、交易(Amazon, eBay)、

取得資訊(CNN)或其它服務，造成使用者的不方便。
其他的影響：因爲這次的入侵事件，使得大家更重視網路安全的重要性。

分散式阻斷服務攻擊，必須先在許多機器上裝置 DDoS 的守護神常駐程式，利用位於網際網路上不同的主機系統來發送大量的僞造來源地址的封包，癱瘓受害者所在的網路和系統主機，因此解決方法有以下幾點：

1.避免自己成爲 DDoS 的守護神常駐程式：避免自己的機器被安裝 DDoS 的守護神常駐程式，系統管理者必須經常注意系統漏洞及修補(patch)漏洞，經常性的注意及掃瞄系統有無異常現象，讓自己的機器不被植入 DDoS 的守護神常駐程式。

2.避免自己成爲 DDoS 的主控端:同上，讓自己的機器不被入侵而成爲 DDoS 的主控端。

3.避免自己被 DDoS 攻擊：基本上 DoS 類的攻擊是無法避免的，因爲你無法判斷使用者的位址是否合法。就算可以，攻擊者還是可以僞造 IP 位址(IP spoofing)。但是有一些位址是不可能或不合法的，例如 10.0.0.0/8 、172.16.0.0/12 與 192.168.0.0/16，可以調整主機或 Router，把這些不合法的位址過濾掉。

由這次的事件，我們發現網際網路上 page view 較高的主機系統都可能成攻擊的目標，但所有主機的管理者，都要非常正視網路安全的重要性。千萬不可認爲自己所管的主機上並沒有存放重要資料或 page view 不高，就認爲無所謂，卻不知本身雖無重要資訊外流的危險或損失，但是卻可能造成有心者攻擊其他重要服務主機的一個"跳板"。而這種情形對網際網路上整體安全性來說，是一個非常大的威脅。網際網路創造了一個無國界的環境，這次的事件提醒大家，爲了整體網路的安全，地球村的每一位公民都應當要善盡維護網路安全的一份心力與責任，避免成爲打手。

另一方面，爲了保障日益活躍的電子商務環境能夠健康的發展，在未來免於受到入侵，降低網路攻擊所造成的威脅與損失，政府相關單位與網站經營者應該投入更多的經費在網路安全的政策擬定、安全軟體工具之研發及網路安全之專業認證及服務上，讓網路世界更安全。

大家必須要知道一個事實—**沒有絕對的安全。**

參考資料

[1] CERT Coordination Center, "Denial of Service Attacks", Feb 12 1999, http://www.cert.org/tech_tips/denial_of_service.html

[2] CERT Coordination Center, "Internet Denial of Service Attacks and the Federal Response", 29 Feb 2000, http://www.cert.org/congressional_testimony/Fithen_testimony_Feb29.html

[3] Internet Security Systems, “從 Yahoo 事件看網路攻擊方法 --- DDoS”, Feb 14 2000, http://www.iss.com.tw/Press/News/detail.php3?News=local&ID=3

[4] David Dittrich, “The DoS Project's "trinoo" distributed denial of service attack tool”, Oct 21 1999, http://staff.washington.edu/dittrich/misc/trinoo.analysis

[5] David Dittrich, “The "Tribe Flood Network" distributed denial of service attack tool”, Oct 21 1999, http://staff.washington.edu/dittrich/misc/tfn.analysis

[6] CERT Coordination Center, “UDP Port Denial-of-Service Attack”, Set 24 1997, http://www.cert.org/advisories/CA-96.01.UDP_service_denial.html

[7] CERT Coordination Center, “TCP SYN Flooding and IP Spoofing Attacks”, Aug 24 1998, http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html

[8] CERT Coordination Center, “"smurf" IP Denial-of-Service Attacks”, Mar 13 2000, http://www.cert.org/advisories/CA-98.01.smurf.html