

個案分析-

UDP DDoS 攻擊分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/2



前言

DoS 攻擊(阻斷服務攻擊, Denial of Service Attack), 如果是多台主機同時進行則為 DDoS (分散式阻斷服務攻擊 Distributed Denial of Service Attack), 可以分為兩大類, 第一類將資源耗盡, 如網路頻寬、主機 CPU 等, 它在短時間內向某特定主機發出大量服務請求或是傳送大量封包, 藉此耗盡網路頻寬或是耗盡主機資源, 使得主機無法提供服務, 暫時癱瘓。第二類藉著異常封包毀損設置不恰當的主機, 例如攻擊設定上有漏洞的路由器(Router 等[1])。

第一類將資源耗盡的 DoS 有以下幾種：

1. ICMP Flood：攻擊者發送超過主機處理上限的 ICMP 封包給主機，使得主機當機或重新開機無法提供服務。
2. SYN Flood：TCP 連線建立之前必須先進行三向交握（Three-Way Handshake）
 - (1) 客戶端送出 SYN 封包給伺服器
 - (2) 伺服器接著送出 SYN+ACK 給客戶端
 - (3) 客戶端送 ACK 給伺服器端

一個合法完整的三向交握，必須 (1) (2) (3) 都進行完畢才是完成。而這種 SYN Flood 攻擊，會進行大量的 (1)，當伺服器進行 (2) 時，(3) 不會被完成，於是伺服器停留在 (3) 等待，若伺服器在短時間內收到由客戶端送來的大量 SYN 封包，但卻得不到客戶端的回應，伺服器就會無法完成連線，耗盡 Session 數量，無法提供服務。

3. UDP Flood：相較於 TCP，UDP 是一種不可靠的傳輸協定，並不需要進行三向交握就可以向伺服器請求服務，當伺服器收到請求服務的 UDP 封包，會交給負責的應用程式，接著回應處理狀況。同樣的，當應用程式收到過多的 UDP 封包，會導致服務無法正常提供。



事件描述

2012 年末，TANet 上出現了幾台主機，發出大量的 UDP 封包，消耗了 TANet 主要骨幹的大量頻寬，使得某些學校的網路頻寬一瞬間被用盡，無法上網，這種癱瘓網路的方法被稱為 UDP Flood 攻擊，本次介紹其中一台主機：

- 作業系統：Windows 7
- 主機上的常駐服務：FTP、Apache、No-ip domain、遠端登入（帳號 z 密碼 z）
- 服務對象：實驗室學生公用主機，主要拿來上傳資料下載資料

主機自安裝之後，並沒有特定的管理者，學生使用 No-ip domain[2]連上該主機，用 FTP 上傳檔案到主機後，利用 HTTP 協定下載檔案。此外該主機也是實驗室的公用電腦，任何人都可以使用，由於使用者眾，為方便記憶，其帳號密碼為皆為「z」。

主機被發現時，已經停止發送大量封包的行為，但是仍可從主機的網路狀況分析發動 UDP Flood 的程式為何，圖 1 為主機被發現時的網路狀態。上面顯示該主機有兩個 IRC Bot 程式，PID 分別為 1732(紅色框)和 1296(綠色框)，其中 PID1296 名稱為「mirc.exe」的惡意程式，為這起 UDP Flood 攻擊的主要惡意程式。由於之後再也沒有出現大規模的 UDP Flood 攻擊，僅能從該主機狀況推斷，駭客透過 IRC 伺服器給予命令，使其發動 UDP Flood 攻擊，其架構圖推測如圖 2。UDP Flood 事件發生之後，該主機上的 mirc.exe 仍會發送少量個 UDP 封包如圖 3，其目的網路位址並沒有明顯規律。

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:113	0.0.0.0:0	LISTENING	1732
[spoolv.exe]				
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	996
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
[System]				
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING	432
[alg.exe]				
TCP	████████.71.102:139	0.0.0.0:0	LISTENING	4
[System]				
TCP	████████.71.102:1246	85.17.180.5:6667	ESTABLISHED	1732
[spoolv.exe]				
TCP	████████.71.102:1257	208.83.20.130:6667	LAST_ACK	1296
[mirc.exe]				
UDP	0.0.0.0:500	*:*		748
[lsass.exe]				
UDP	0.0.0.0:445	*:*		4
[System]				
UDP	0.0.0.0:4500	*:*		748
[lsass.exe]				
UDP	0.0.0.0:6753	*:*		1296
[mirc.exe]				
UDP	0.0.0.0:1025	*:*		1144
[svchost.exe]				

圖 1 兩個 IRC 程式，PID 分別為 1732 和 1296

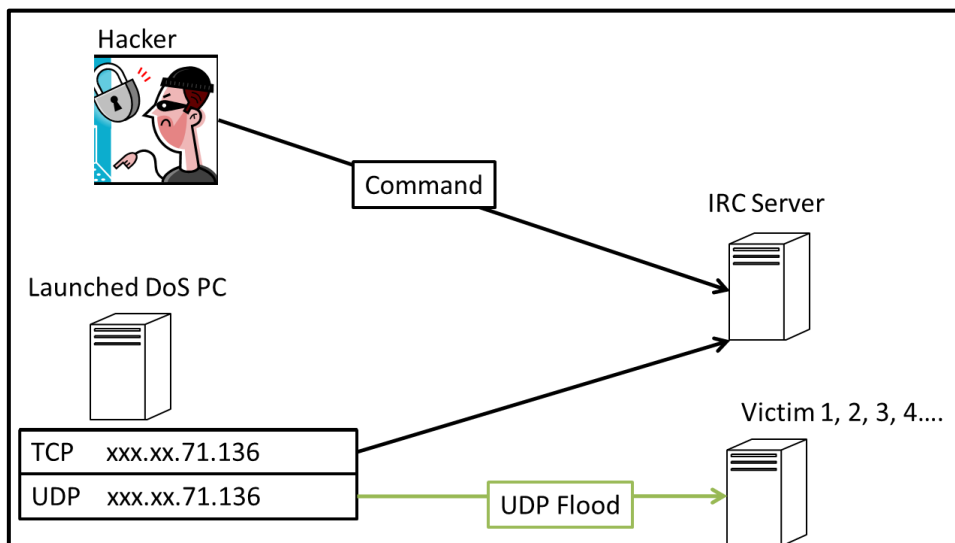



圖 2 mirc.exe 從 IRC Server 接收指令，在特定時間發動 UDP Flood

Source	Destination	Protocol	Info
11:24:45.091075	.71.102 212.12.166.36	UDP	Source port: vrts-ipcserver Destination port: 8079
11:24:45.607172	.71.102 84.114.219.90	UDP	Source port: krb5gatekeeper Destination port: ct2nmcs
11:24:46.654060	.71.102 118.137.42.114	UDP	Source port: amx-icsp Destination port: 6874
11:24:47.169548	.71.102 71.95.133.164	UDP	Source port: amx-axbnet Destination port: 7269
11:24:58.044567	.71.102 85.14.86.35	UDP	Source port: pip Destination port: 8583
11:24:58.559639	.71.102 164.125.131.62	UDP	Source port: novation Destination port: 9674
11:24:59.075552	.71.102 69.47.135.203	UDP	Source port: brcd Destination port: 7601
11:24:59.591786	.71.102 66.176.35.189	UDP	Source port: delta-mcp Destination port: esinstall
11:25:00.106862	.71.102 80.95.21.145	UDP	Source port: dx-instrument Destination port: 6432
11:25:00.622982	.71.102 69.181.155.234	UDP	Source port: wimsic Destination port: 8518
11:25:00.837937	155.234 .71.102	ICMP	Destination unreachable (Communication administratively filtered)
11:25:01.669926	.71.102 98.223.49.72	UDP	Source port: ultrex Destination port: afs3-volser
11:25:02.184788	.71.102 61.61.219.156	UDP	Source port: ewall Destination port: 7358
11:25:13.060275	.71.102 78.9.24.138	UDP	Source port: netdb-export Destination port: 7926
11:25:13.575223	.71.102 118.174.238.24	UDP	Source port: streetperfect Destination port: 8907
11:25:14.091285	.71.102 210.91.146.120	UDP	Source port: intersan Destination port: 7693
11:25:14.607390	.71.102 98.212.104.177	UDP	Source port: pcia-rxp-b Destination port: 6916
11:25:15.122427	.71.102 89.137.131.28	UDP	Source port: passwd-policy Destination port: 7435
11:25:15.638340	.71.102 68.224.251.252	UDP	Source port: writesrv Destination port: 7367
11:25:15.843981	251.252 .71.102	ICMP	Destination unreachable (Port unreachable)
11:25:16.153648	.71.102 76.125.147.168	UDP	Source port: digital-notary Destination port: 6738
11:25:16.669925	.71.102 93.126.150.87	UDP	Source port: ischat Destination port: 6246
11:25:17.185969	.71.102 86.2.176.53	UDP	Source port: menandmice-dns Destination port: ktelnet
11:25:28.060453	.71.102 201.33.57.34	UDP	Source port: wmc-log-svc Destination port: 7127
11:25:28.576401	.71.102 201.74.220.34	UDP	Source port: kjtsiteserver Destination port: 8673
11:25:29.091534	.71.102 89.103.238.141	UDP	Source port: naap Destination port: 6119
11:25:29.607470	.71.102 173.15.100.5	UDP	Source port: qubes Destination port: 5749
11:25:30.123297	.71.102 24.91.191.173	UDP	Source port: esbroker Destination port: 6684
11:25:31.169083	.71.102 86.104.46.27	UDP	Source port: rel01 Destination port: 8203
11:25:31.685229	.71.102 89.44.37.116	UDP	Source port: icap Destination port: 8331
11:25:32.201169	.71.102 98.227.7.235	UDP	Source port: vjpp Destination port: afs3-volser
11:25:34.780606	.71.102 140.117.11.1	DNS	Standard query A Helsinki.FI.EU.Undernet.org
11:25:34.781097	.11.1 140.117.71.102	DNS	Standard query response CNAME EU.Undernet.org A 130.237.188.216 A
11:25:43.075638	.71.102 194.0.126.98	UDP	Source port: sbook Destination port: spramsca
11:25:43.591751	.71.102 190.1.43.48	UDP	Source port: editbench Destination port: smc-https
11:25:44.106878	.71.102 83.82.88.74	UDP	Source port: lotusnote Destination port: 8659
11:25:44.622728	.71.102 89.42.4.50	UDP	Source port: relief Destination port: ldss
11:25:44.639320	43.10 .71.102	ICMP	Destination unreachable (Network unreachable)
11:25:45.138777	.71.102 85.64.189.111	UDP	Source port: intuitive-edge Destination port: 6534
11:25:46.184992	.71.102 122.255.169.57	UDP	Source port: cuillamartin Destination port: 5699
11:25:46.700884	.71.102 89.42.203.160	UDP	Source port: pegboard Destination port: sun-user-https

圖 3 由 mirc.exe 發出的大量 UDP 封包

Mirc 是一個受歡迎的聊天軟體（官網：<http://www.mirc.com/>），台灣國內較少人使用，在國外極常見，從官網下載的 mirc.exe 與本案出現的 mirc.exe 標誌極相似，可以推斷是為了讓使用者混淆，以為它是合法的 mirc.exe。遇到這樣情況，最快的判斷方法就是將 exe 檔上傳到 VirusTotal 上去，交給防毒軟體判斷。圖 6 可以看到該程式在 VirusTotal 上有 39/46 的偵測率。



名稱	修改日期	類型	大小
defaults	2013/1/22 下午 12:06	檔案資料夾	
ircintro.chm	2012/10/20 下午 08:33	編譯的 HTML 說...	75 KB
license.txt	2012/10/20 下午 08:33	文字文件	6 KB
mirc.chm	2012/10/20 下午 08:33	編譯的 HTML 說...	191 KB
mirc.exe	2012/10/20 下午 08:33	應用程式	3,205 KB
readme.txt	2012/10/20 下午 08:33	文字文件	2 KB
uninstall.exe	2012/10/20 下午 08:33	應用程式	146 KB
versions.txt	2012/10/20 下午 08:33	文字文件	41 KB

圖 4 正版 mirc.exe

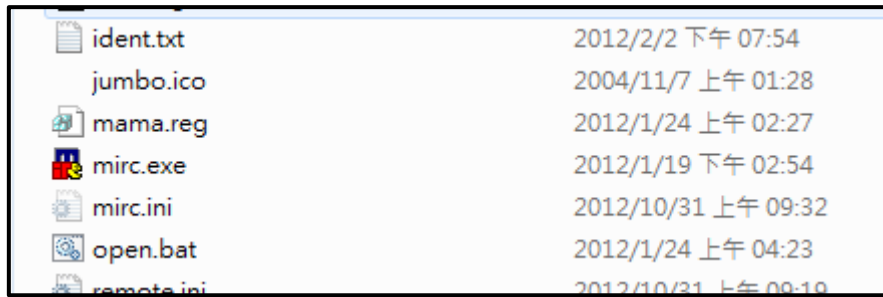


圖 5 惡意 mirc.exe，圖示與正版 mirc 極為相似



SHA256: c7c65c21e9c9d43d6af6c31b3e142fd6a730bfde9dd509a90af550d26753fafa

File name: mirc.exe

Detection ratio: 39 / 46

Analysis date: 2012-12-14 06:50:13 UTC (0 分鐘 ago)

More details

Analysis Comments Votes Additional information

Antivirus	Result	Update
Agnitum	Win32.Sality.BL	20121213
AhnLab-V3	Win32/Kashu.E	20121213
AntiVir	W32/Sality.AT	20121214
Antiy-AVL	-	20121213
Avast	Win32:Sality	20121214
AVG	Win32/Sality	20121214
BitDefender	Win32.Sality.3	20121214
ByteHero	-	20121212
CAT-QuickHeal	W32.Sality.U	20121214
ClamAV	-	20121214
Commtouch	W32/Sality.gen2	20121214
Comodo	Virus.Win32.Sality.Gen	20121214
DrWeb	Win32.Sector.22	20121214
Emsisoft	Win32.Sality.3 (B)	20121214
eSafe	-	20121212
ESET-NOD32	Win32/Sality.NBA	20121213

圖 6 惡意的 mirc.exe 在 VirusTotal 上的掃描結果

建議措施

- 定期更改主機服務登入密碼



以此事件為例，實驗室的學生表示，公用主機因為使用者眾多，為了方便，設置簡單易記憶的密碼，且密碼極少更改。當密碼被駭客得知入侵之後，管理員發現異常刪除惡意程式或重灌主機，但卻沒有更改原本的帳號密碼，仍會被駭客再度入侵。

● 對提供遠端存取的服務限定存取網路位址

主機的網路位址及主機上的服務，由於網路的特性，駭客只要利用自動掃描工具，馬上就可以知道主機位址及上面運行的服務，像 SSH 服務與 FTP 服務，帳號密碼很容易被暴力破解。因此，主機上任何可以遠端登入的服務，應該對其登入對象限定網路位址，尤其是 root 帳號，Linux 主機提供 su 命令可以切換帳號，建議把可以遠端登入的帳號權限設定在安全的範圍內，登入之後再切換 root 便可。各種保護措施雖然會增加不便，但可減少被駭客入侵的機率。

參考

[1] http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1869

[2] <http://www.noip.com/>