iThome Tech Talk
一次搞懂 DDoS 是什麼

OuTian Liu
outian@mail.outian.net

關於我

OuTian Liu <outian.liu@forcepoint.com>
Forcepoint 台灣區技術經理

- 曾任 敦陽科技 資安顧問, FireEye技術經理
- 台灣駭客年會講師、Zero-Day發表者
- 豐富滲透測試服務經驗
- 擅長資安事件處理與解決方案規劃
- 各大資安論壇、研討會、教育訓練講師

大綱

- 前言
- DDoS 攻擊手法詳解
- DDoS 案例分析
- 正確的 DDoS 防護觀念
- 問題與討論

WHO IS FORCEPOINT ?

websense

企業市場領導者

with

Content Security & DLP

Cloud / On-Premise / Hybrid

Raytheon

安全前線的先鋒

with

Financial Resources

Deep Understanding of Threat Detection

STONESOFT

網路創新者

with

Advanced Evasion Prevention

Security at Scale

FORCEPOINT

POWERED BY Raytheon

DEFEAT DEFEND DETECT DECIDE 4D SECURITY

FORCEPOINT 解決方案

- URL Filter 、 DLP
- APT
  - WSG
  - ESG
  - Sandbox
- DLP
  - Gateway
  - Endpoint
- UBA
  - Endpoint
- CLOUD
  - WEB / EMAIL / CASB / Sandbox / …
- NGFW

資安人 NO. 65

攻防技術篇

以國內案例為例

DDoS攻擊手法與防禦對策

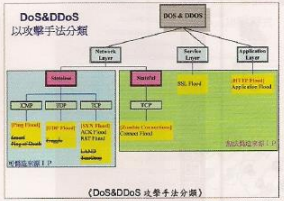
文 | OuTian

許多不肖之徒，利用各式各樣的方式進行DoS(Denial of Service)及DDoS(Distributed Denial of Service)攻擊，以達到破壞服務運作的目的。國際間有多個Botnet提供付費的租用方式，只要攻擊者盯上你的網站，就可能購買服務來發動攻擊再進行勒索。

變化多端的DDoS攻擊手法

DDoS攻擊通常會伴隨Botnet（殭屍網路）進行，攻擊者透過對大量遭植入控制程式的殭屍電腦發送命令，使其同時間對目標發動指定類型的攻擊。也因此DDoS的追查難度非常的高，遇到高明的攻擊者利用Botnet控制Botnet，透過技術層次幾乎不可能確認其身份。而雖然DoS、DDoS已經存在十幾年了，但許多人常存在不當的誤解，例如「只要加大頻寬就好了」、「叫ISP擋啊！」、「買最高貴的設備擋就對了」、「用『機海戰術』跟它拼了！」…等。

DDoS表示由多重來源發起攻擊而導致目標服務癱瘓，而並不單指特定某種攻擊手法。由於攻擊手法繁多，因此也沒有統一的標準解決方案。本文僅就「網路行為」造成的DDoS攻擊進行探討，其他針對程式弱點的攻擊如Buffer Overflow使服務停止運作，或Injection類植入特定命令使服務或主機關閉等，雖說同樣可造成Denial of Service結果，但不於本文中說明。



▲ 圖1：其中［紅色］表較常發生、雙刪除線 表傳統攻擊手法，已難生效。

攻擊分類

依攻擊之層次，可分為以下幾種－（見圖1）

(1) Network Layer：利用常見之標準協定如TCP/UDP/ICMP進行攻擊。其中某些Stateless類之攻擊可偽造位址，因此無法以阻擋來源的方式防禦。而Stateful之完整建立連線類的攻擊通常會與Botnet結合，不斷變換、並來自大量的真實位址，使防守者疲於奔命。目的為使目標頻寬滿載、或使網路設備或主機無法負荷而停止服務。

(2) Service Layer：介於網路層與應用層之間，於服務層進行資料交換處理時、但仍未至應用層實際執行動作前，使其處理錯誤引發例外情況（例如Buffer Overflow）、或因大量進行協議交換處理而無法負荷。

(3) Application Layer：利用製造模擬大量之正常請求至目標主機應用層，使其因無法服務過量使用者而負荷超載。

而大多傳統設備可防護之DoS/DDoS攻擊手法如

6

資安人 NO. 75

網站管理員的惡夢 － HTTP DoS

近來幾家公司發生怪異的被DoS攻擊，「已經建置防火牆、IPS，網路頻寬也沒異常，結果網站還是倒了。」到底怎麼回事？

文‖ OuTian

以往，一般人對防護DoS/DDoS攻擊的想法是：「就是比誰頻寬大嘛！我拉10條線路跟攻擊者玩玩！」、「我有強力的設備守護，在頻寬塞滿前絕對不會倒！」、「即使用人海戰術衝到伺服器層，我用機海戰術守下來！」但筆者近來常聽到的疑問是：「我已經建置了防火牆、入侵防禦系統，網路頻寬也沒異常上升，為何網站仍然倒了？」先前筆者曾在資安人雜誌65期發表過「DDoS攻擊手法與防禦對策」，當中廣泛列舉各式各樣網路層及應用層的攻擊手法剖析及實例探討，其中亦提到應用層的Application Layer DoS，本文即深入探討其中最常發生的「HTTP DoS」。

當發現受到HTTP Flood或CC攻擊時，一定要開啟伺服器的Access Log，以對攻擊行為進行分析。妥善使用腳本程式定時分析，一經發現則直接自動將其封鎖、或限制存取頻率。

「HTTP DoS」是一個泛稱，顧名思義，即針對HTTP協定所進行的Denied of Service攻擊，手法有許多種，目的皆為癱瘓目標網站。以下即提出近年較常見的幾種攻擊手法。

無言的結局－癡癡守候的伺服器

手法1. GET with unended request

此攻擊手法於2007年時開始被討論，而最有名的是2009年由RSnake所撰寫的攻擊程式Slowloris，一支簡短卻殺傷力強大的perl腳本（附錄1）。根據RFC 2616（HTTP協議）之規範，完整之HTTP GET Request結尾為連續兩CRLF，伺服器端即視此請求完成，開始作後續處理。如下為使用IE 8開啟http://www.google.com.tw/ 時送出之HTTP Request －

```
GET / HTTP/1.1[\r\n]
Accept: */*[\r\n]
Accept-Language: zh-tw[\r\n]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1) [\r\n]
Accept-Encoding: gzip, deflate[\r\n]
Host: www.google.com.tw[\r\n]
Connection: Keep-Alive[\r\n]
[\r\n]
```

每一個開啟網頁元件的請求，瀏覽器均依此模式與伺服器溝通，但若此請求永遠不結束呢？若攻擊者使用程式模擬此行為，與伺服器80 port建立連線後，送出以下HTTP Header －

```
GET / HTTP/1.1[\r\n]
Host: www.google.com.tw[\r\n]
Header1: 111[\r\n]
Header2: 222[\r\n]
Header3: 333[\r\n]
.....[\r\n]
HeaderN: NNN[\r\n]
.....[\r\n]
.....[\r\n]
```

由於各伺服器並沒有明確規範及定義

聲明

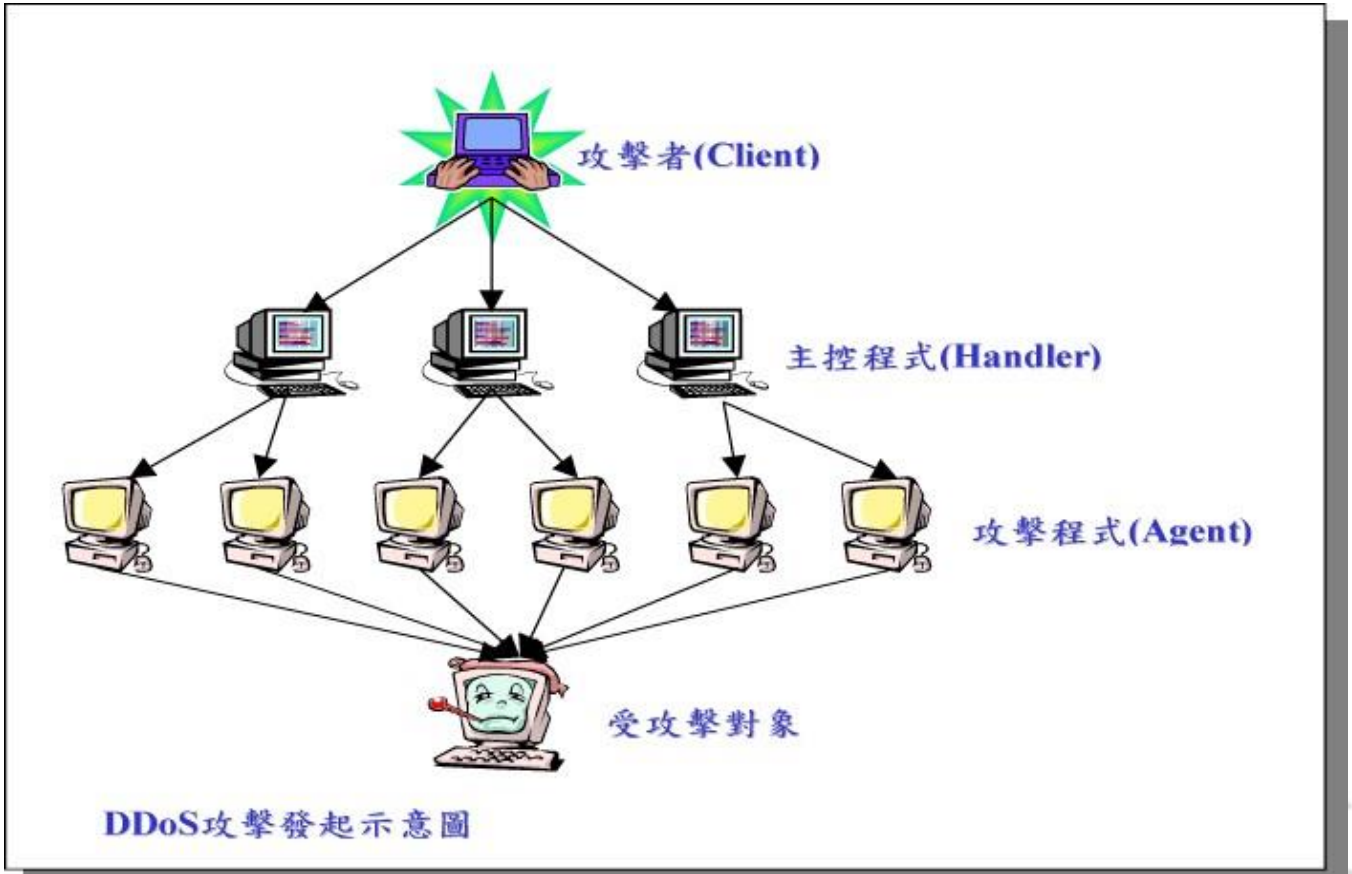
本課程內容，僅用於瞭解攻擊手法以利進行防禦部署，若有任何學員以之進行非法活動，一切與本人及iThome無關，由學員自行負責。

DOS/DDOS

- DOS – Denial Of Service
  - 藉由各種的攻擊手法，使資訊服務無法正常運作

- DDOS – Distributed DOS
  - 由多重的來源進行攻擊，使資訊服務無法正常運作

DDoS - 透過殭屍網路控制多重來源



DDoS 源由

- 分類
  - 偶發
  - 常態
- DDoS 背後目的
  - 商業利益/同業競爭
  - 勒索
  - 政治對立/時事議題
  - 火力展示/恐嚇
  - 練兵

誰常會遭遇 DDoS？

- 開店作生意的的電商
  - 博奕
  - 線上購物
  - 遊戲
- 不可中斷的線上服務
  - 金融業 (銀行、證券商)
  - 基礎建設 (電信、油水電等)
  - 交通 (台鐵/高鐵/航空公司線上查詢、訂票)
  - 媒體
- 形象門面
  - 政府
  - 學校
- 代管服務
  - 主機代管
  - DNS 代管

安全防護的責任在誰？

- 電信商
  - 提供防護服務
  - 與上下游良好溝通配合
- 企業
  - 自我演練受攻擊的應變步驟
  - 隨時準備好受攻擊
  - DDoS Retainer？
- 政府
  - 制定法令？
  - 協助逮補元兇？

問題

- 不要說Tb級、或100Gb，若開店後遭遇
  - 10Gbps 的洪水流量攻擊
  - 10Mpps的SYN攻擊
  - 每秒一百萬次的DNS查詢、HTTP請求、或SSL連線

  - 以上數據再縮小為1/10，國內企業也不見得可以擋
  - 給我 1Gbps 的頻寬 …

肉雞

肉雞市場

	[09.04]網逝銷雲服務器後門 NEW	W1984 2008-09-04	4	53	2008-09-04 23:25 by: 羽de翼
	[09.03]出售流量肉雞	494026212 2008-09-03	1	58	2008-09-04 01:17 by: 3389真黑
	[09.01]出售自己編寫的1433抓雞工具	sloat2008 2008-09-01	1	56	2008-09-03 15:17 by: zwz003
	[07.28]出售大量肉雞並提供DDOS服務！老字號	龍寶寶 2008-07-28	4	120	2008-09-03 15:11 by: simon
	[09.02]急求7位QQ	120115708 2008-09-02	5	74	2008-09-03 12:54 by: ayz
	[09.01]出售幾個免殺遠控，剛更新的 (-5) [1 2]	jzysd 2008-09-01	15	120	2008-09-03 00:50 by: hongonly
	[07.16]要鴿子免殺DAT的來 [1 2]	t.y.p 2008-07-16	11	276	2008-09-02 21:37 by: fendouandy
	[09.02]長期出售盛大金牌帳號激活碼	鬼狼 2008-09-02	0	28	2008-09-02 13:31 by: 鬼狼
	[08.30]出售個日本雞 [1 2]	黑夜幽靈 2008-08-30	12	203	2008-09-02 02:16 by: yycyyc
	[09.01]出售幾台全能能服務器，	l45189946 2008-09-01	1	56	2008-09-01 19:18 by: songjie1230
	[08.31]本人出售抓雞服務器	76514996 2008-08-31	1	41	2008-09-01 00:08 by: ycdd
	[08.31]服務器 專業戶	l45189946 2008-08-31	0	34	2008-08-31 17:05 by: l45189946

DDoS as a service

傳說中只要拔到獅子的鬃毛.....

常見的謬思

- 防火牆可以保護我的網路免受攻擊影響
  - 大多數的情況下，防火牆會先掛！
- 用「機海戰術」跟他拼了！
  - 前面頻寬滿了、或設備掛了，再多服務器也無用
- ISP 可以幫我阻擋並過濾攻擊的封包
  - 來源均可能為偽造，難以追蹤上游真正來源
- 我可以找出攻擊的來源並阻擋、或打回去
  - 來源可能不存在、或為真實之他人IP，不要亂打

DDoS 攻擊手法詳解

傳統的 DDOS Attack

- Teardrop
- Land
- Smurf 早已失效 ！
- Fraggle
- Ping of Death

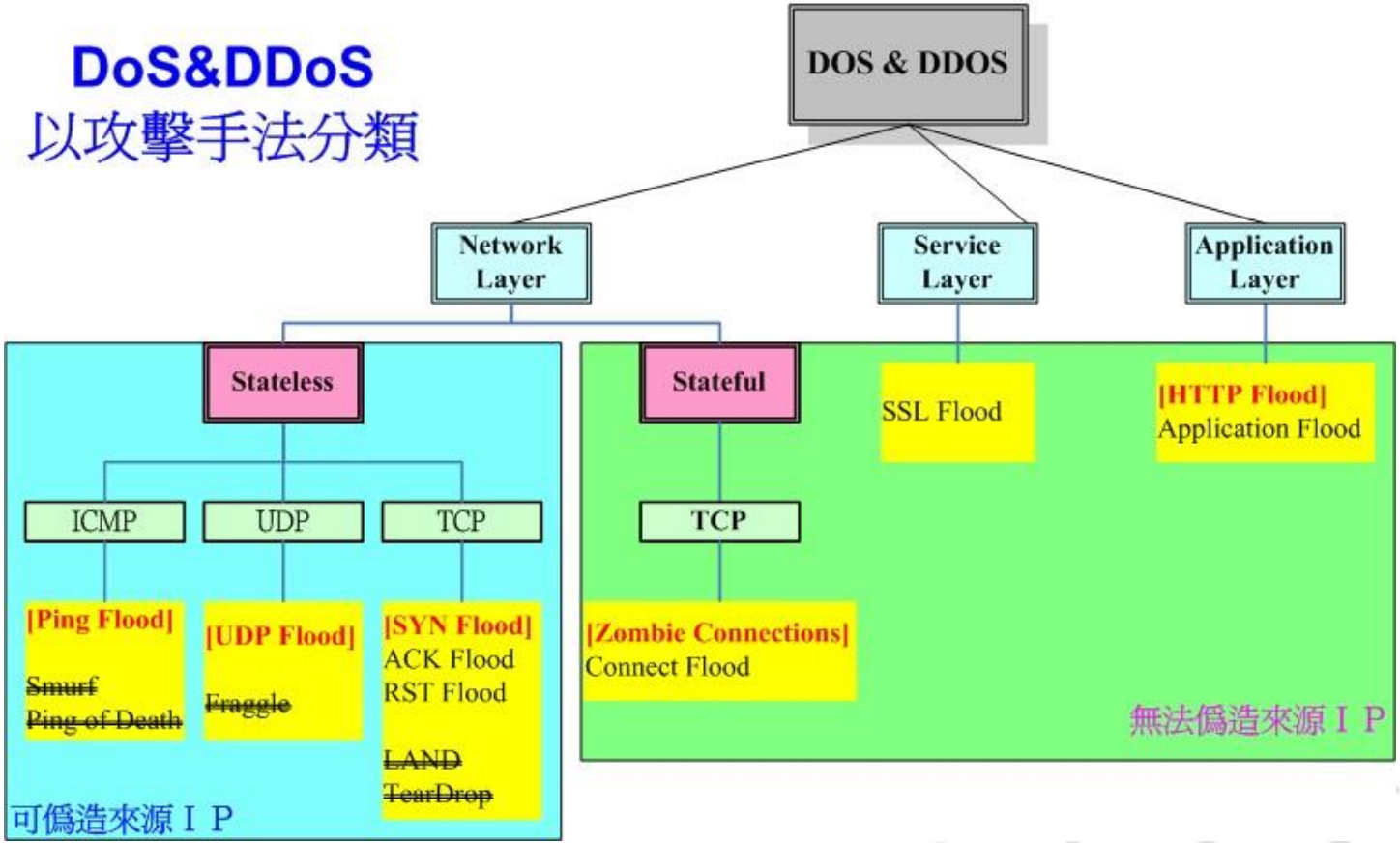
DDoS 的攻擊層次

- Bandwidth-level Attack
  - 灌爆頻寬
    - 各類 packet flooding (ip/tcp/udp/icmp/…)
    - 各類 Amplification/Reflection Attack
- Infrastructure-level Attack
  - 癱瘓路由器、防火牆、負載平衡器、入侵防禦系統 … 等網路設備
    - Syn/ack/rst/connection … etc
- Service-level Attack
  - 癱瘓伺服器服務
    - 各類 Applicatin Flooding (http/dns/smtp/…)
    - SSL/HTTP/DNS/exploit … etc

22

- 打得"大"
  - 1:1 換頻寬
  - Reflection & Amplification
  - IoT Botnet
  - …
- 打得"巧"
  - SYN Flood
  - Fragment Packet Flood
  - Application Flood
  - Slow Attack
  - Exploit
  - …

今天的 DDoS 攻擊手法



24

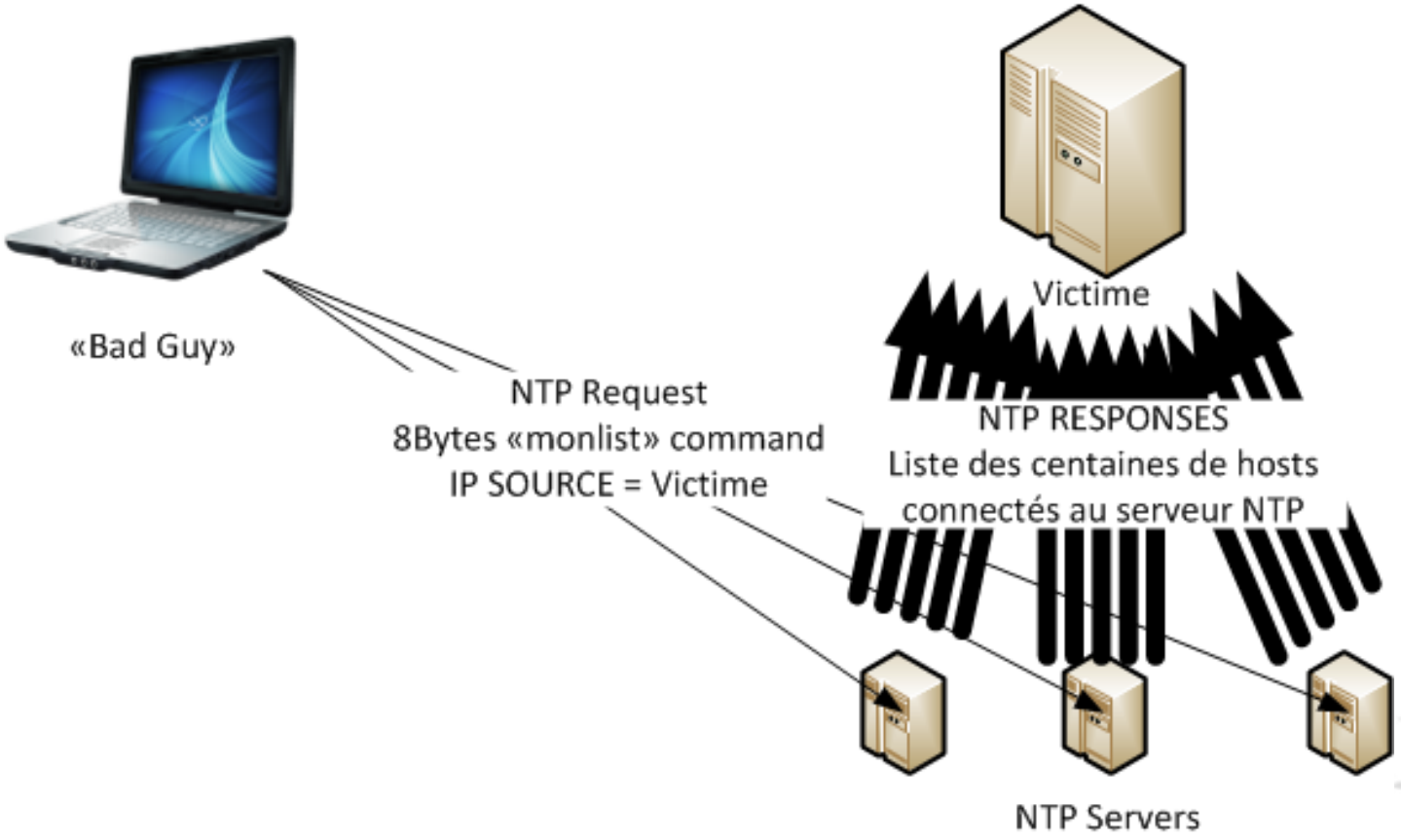
Bandwidth-level – UDP/ICMP Flood

- 假造來源發送大量的UDP/ICMP封包
- 多數攻擊程式在刻製封包的overhead較TCP為低，故封包發送速度快、內容易客製
- 攻擊目的 – 使目標頻寬滿載

Bandwidth-level – Amplification / reflection

- NTP
- DNS
- SNMP
- UPnP
- RIP
- SSDP
- CHARGEN
- ……

NTP Amplification/Reflection Attack



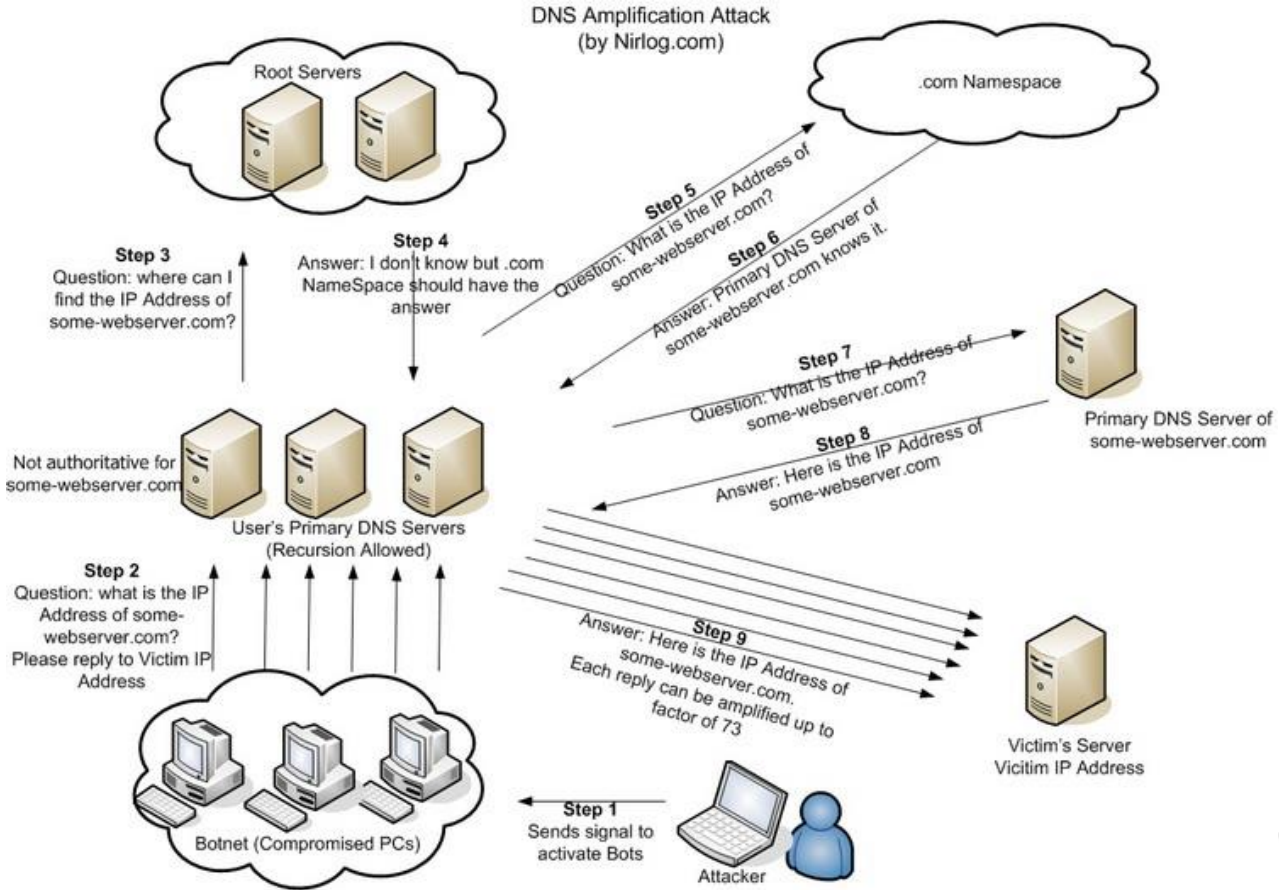
27

```
root@kali:~# ntpdc -n -c monlist 192.168.220.130
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
192.168.220.155        42215 192.168.220.130        5 7 2       0    313       0
8.8.8.199              30083 192.168.220.130        1 7 2       0      0      24
8.8.8.198              30083 192.168.220.130        1 7 2       0      0      24
8.8.8.197              30083 192.168.220.130        1 7 2       0      0      24
8.8.8.196              30083 192.168.220.130        1 7 2       0      0      25
8.8.8.195              30083 192.168.220.130        1 7 2       0      0      25
8.8.8.194              30083 192.168.220.130        1 7 2       0      0      26
8.8.8.193              30083 192.168.220.130        1 7 2       0      0      26
8.8.8.192              30083 192.168.220.130        1 7 2       0      0      26
8.8.8.191              30083 192.168.220.130        1 7 2       0      0      27
8.8.8.190              30083 192.168.220.130        1 7 2       0      0      27
8.8.8.189              30083 192.168.220.130        1 7 2       0      0      28
8.8.8.188              30083 192.168.220.130        1 7 2       0      0      28
8.8.8.187              30083 192.168.220.130        1 7 2       0      0      28
8.8.8.186              30083 192.168.220.130        1 7 2       0      0      29
8.8.8.185              30083 192.168.220.130        1 7 2       0      0      29
8.8.8.184              30083 192.168.220.130        1 7 2       0      0      30
8.8.8.183              30083 192.168.220.130        1 7 2       0      0      30
8.8.8.182              30083 192.168.220.130        1 7 2       0      0      31
8.8.8.181              30083 192.168.220.130        1 7 2       0      0      31
8.8.8.180              30083 192.168.220.130        1 7 2       0      0      31
```

KALI LINUX

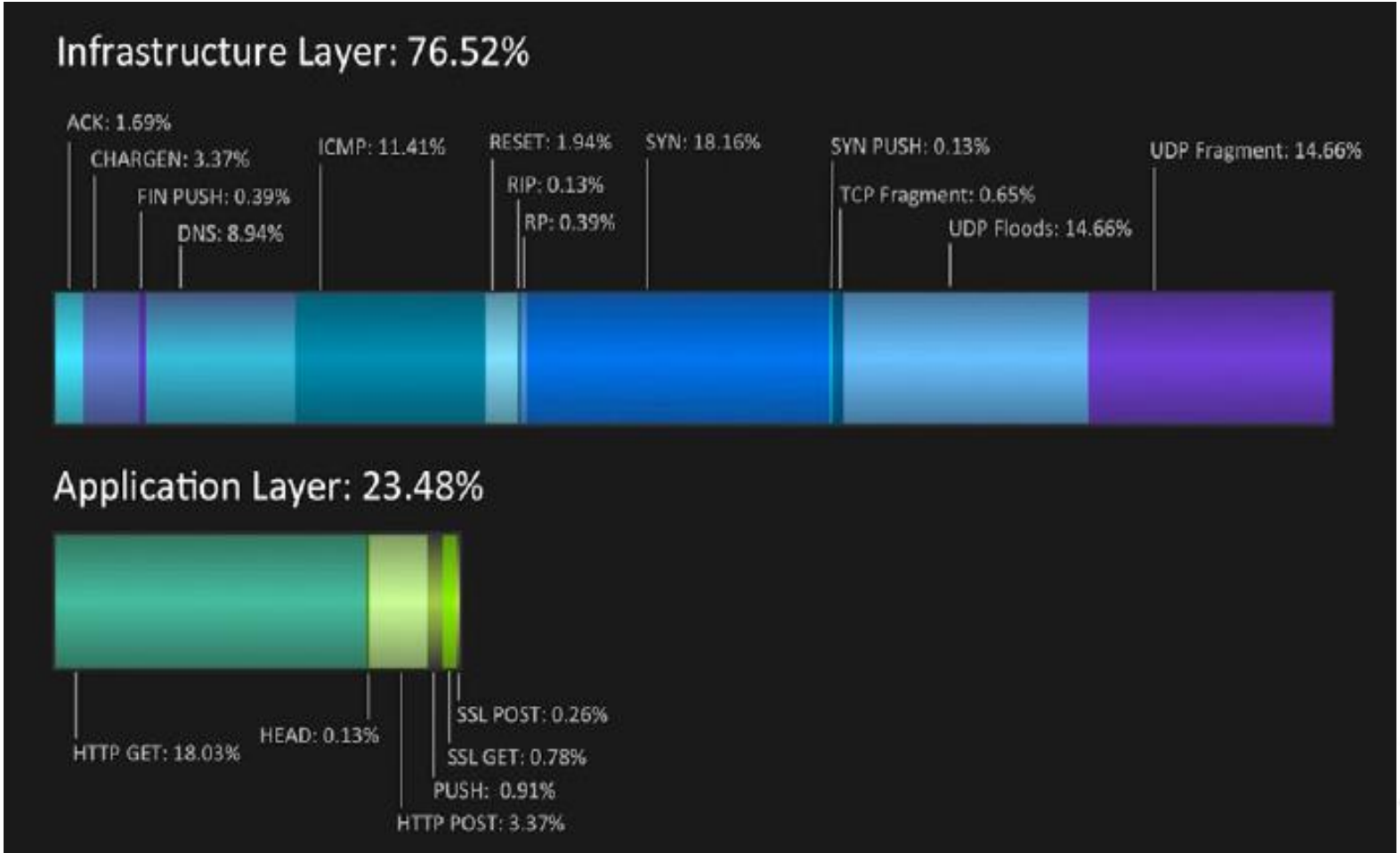
28

DNS Amplification/Reflection Attack



29

攻擊類型分佈 (Q3 2013) from Prolexic



30

攻擊類型分佈 (Q4 2016) from Akamai

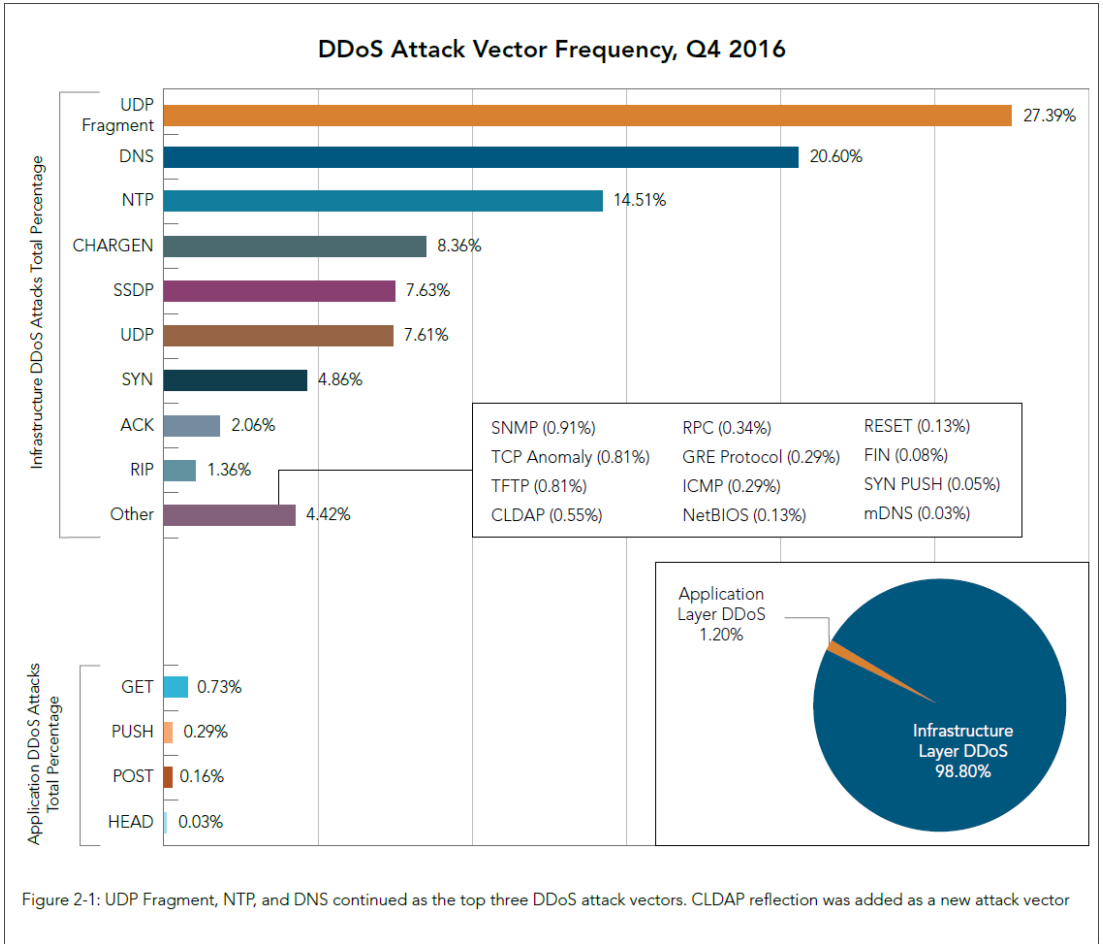
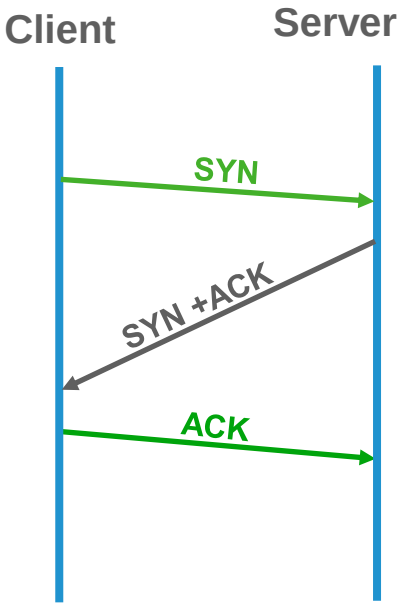
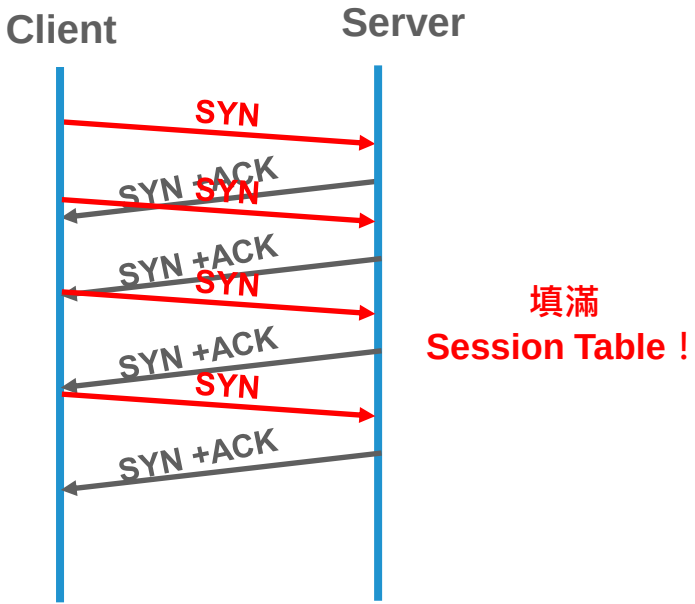


Figure 2-1: UDP Fragment, NTP, and DNS continued as the top three DDoS attack vectors. CLDAP reflection was added as a new attack vector

Infrastructure-level – SYN Flood DDOS Attack

- 正常建立TCP連線

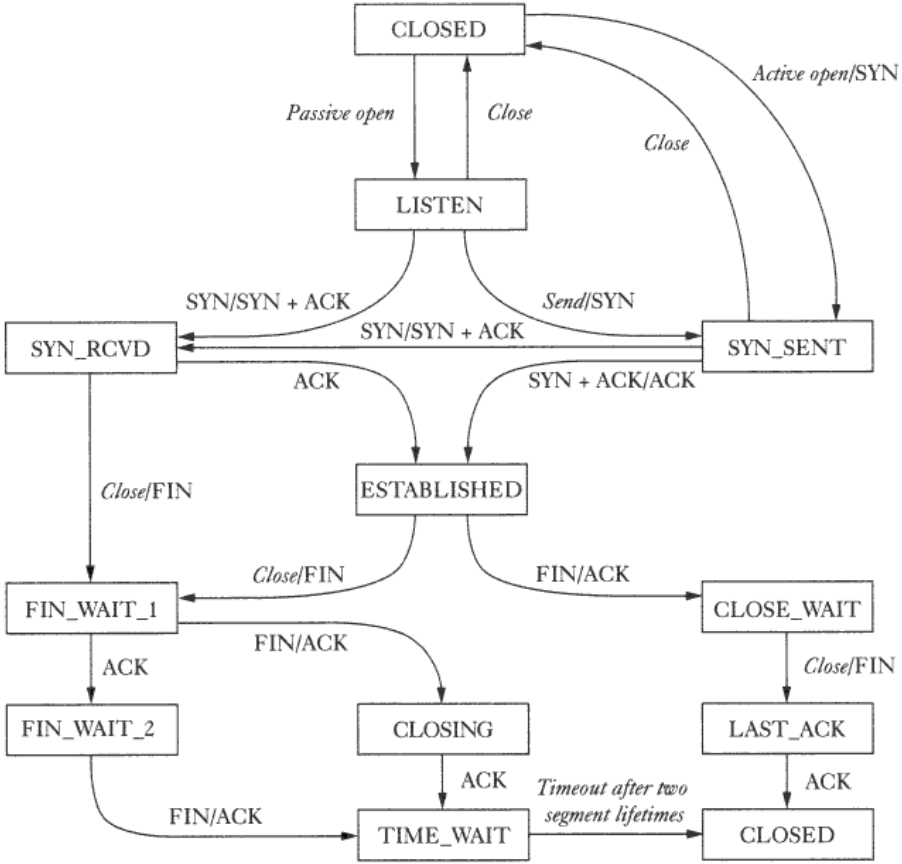




填滿
Session Table！

SYN Flooding

TCP State

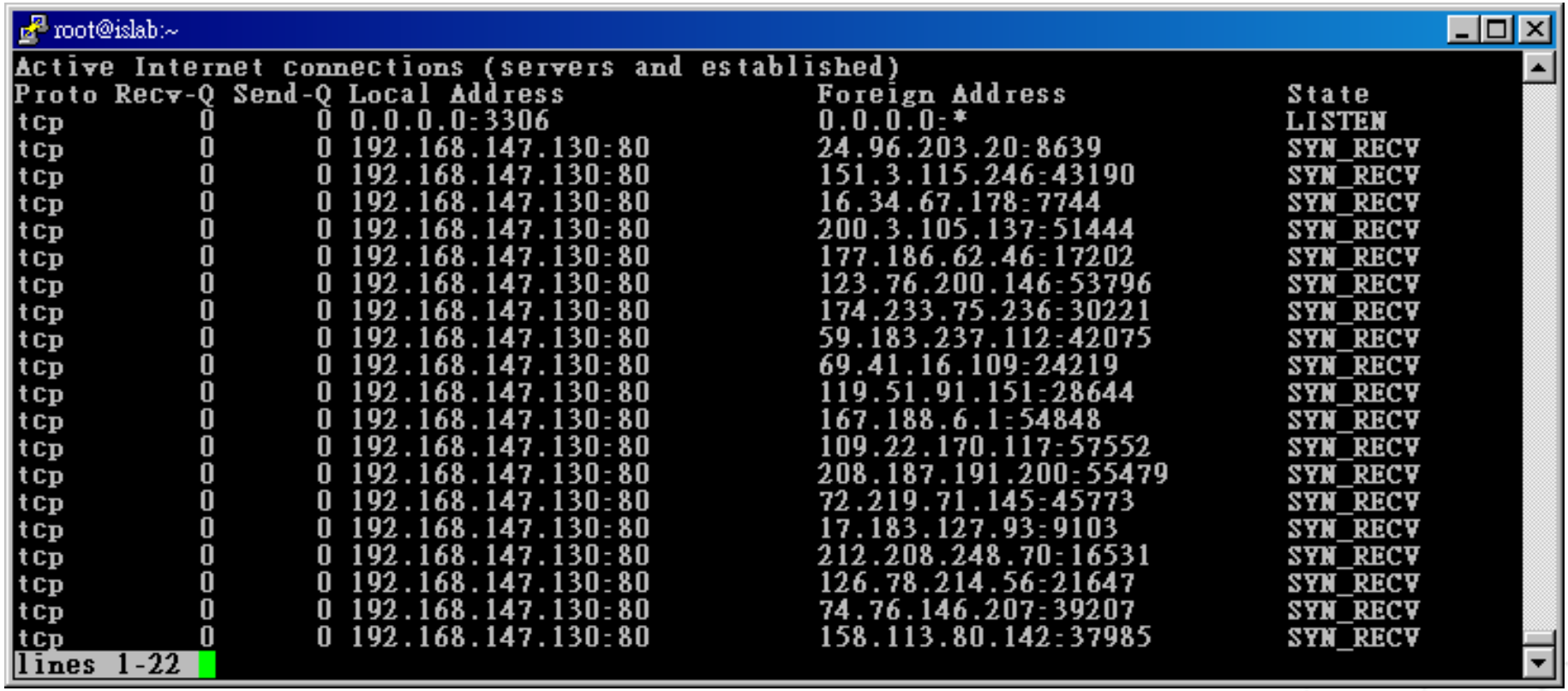

CLOSED
Active open/SYN
Passive open
Close
Close
LISTEN
SYN/SYN + ACK
Send/SYN
SYN/SYN + ACK
SYN_RCVD
SYN_SENT
ACK
SYN + ACK/ACK
Close/FIN
ESTABLISHED
Close/FIN
FIN/ACK
FIN_WAIT_1
CLOSE_WAIT
FIN/ACK
ACK
Close/FIN
FIN_WAIT_2
CLOSING
LAST_ACK
ACK
ACK
Timeout after two segment lifetimes
FIN/ACK
TIME_WAIT
CLOSED

簡單的算式

- SYN 封包
  - IP + TCP Header length = 46 bytes
  - Ethernet Frame size = 64 bytes
  - 實際運作時加上overhead平均長度 = 84 bytes
- 1Mbps 的頻寬約可發出 1560 pps SYN
  - 100Mbps ＝＞ 156,000 pps SYN
    - 已足已癱瘓大部份中階之防火牆
  - 500Mbps ＝＞ 780,190 pps SYN
    - 許多高階設備亦無法承受
- 一般資安設備的 New Session/s 大部份不高

34

攻擊結果


root@islab:~
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN
tcp 0 0 192.168.147.130:80 24.96.203.20:8639 SYN_RECV
tcp 0 0 192.168.147.130:80 151.3.115.246:43190 SYN_RECV
tcp 0 0 192.168.147.130:80 16.34.67.178:7744 SYN_RECV
tcp 0 0 192.168.147.130:80 200.3.105.137:51444 SYN_RECV
tcp 0 0 192.168.147.130:80 177.186.62.46:17202 SYN_RECV
tcp 0 0 192.168.147.130:80 123.76.200.146:53796 SYN_RECV
tcp 0 0 192.168.147.130:80 174.233.75.236:30221 SYN_RECV
tcp 0 0 192.168.147.130:80 59.183.237.112:42075 SYN_RECV
tcp 0 0 192.168.147.130:80 69.41.16.109:24219 SYN_RECV
tcp 0 0 192.168.147.130:80 119.51.91.151:28644 SYN_RECV
tcp 0 0 192.168.147.130:80 167.188.6.1:54848 SYN_RECV
tcp 0 0 192.168.147.130:80 109.22.170.117:57552 SYN_RECV
tcp 0 0 192.168.147.130:80 208.187.191.200:55479 SYN_RECV
tcp 0 0 192.168.147.130:80 72.219.71.145:45773 SYN_RECV
tcp 0 0 192.168.147.130:80 17.183.127.93:9103 SYN_RECV
tcp 0 0 192.168.147.130:80 212.208.248.70:16531 SYN_RECV
tcp 0 0 192.168.147.130:80 126.78.214.56:21647 SYN_RECV
tcp 0 0 192.168.147.130:80 74.76.146.207:39207 SYN_RECV
tcp 0 0 192.168.147.130:80 158.113.80.142:37985 SYN_RECV
lines 1-22

Infrastructure-level – ACK/RST Flood

- 假造來源發送大量的ACK/RST封包
- Firewall、Proxy、L4、或任何主機，將需搜尋本身之 Session Table，若未存在該連線則回應 RST (或 Drop 封包)
- 攻擊效果 –
  - 使網路設備、或主機負荷升高
  - 使Outbound頻寬滿載

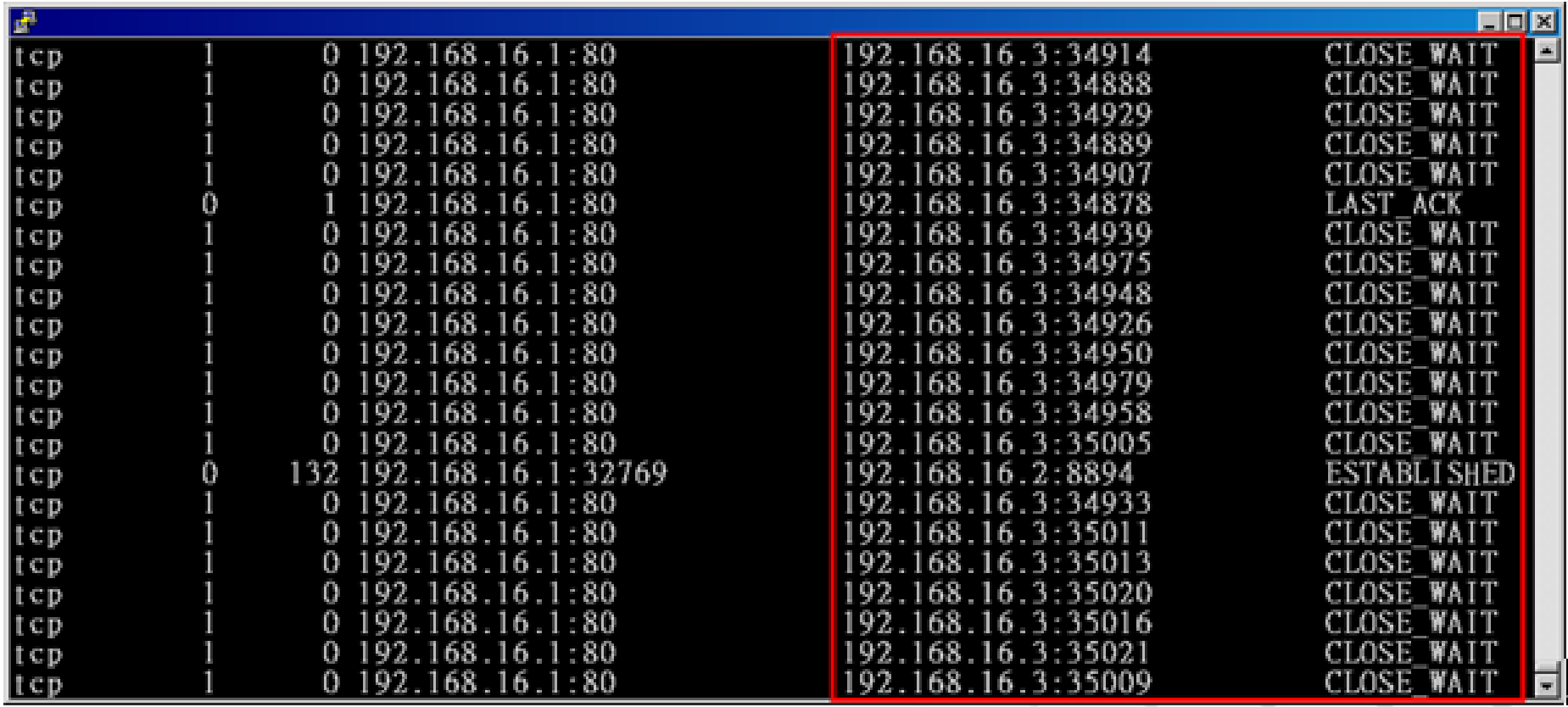
Infrastructure-level – Fragment Packet Flood

- 發送大封包時，切割為眾多小封包進行傳送
- 使主機或網路設備虛耗大量時間於重組封包，而導致負荷升高、處理速度降低

Infrastructure-level – Connect Flood

- 以大量之攻擊來源，與目標服務不斷重覆建立TCP連線、切斷連線、建立連線、切斷連線……等動作
- 網路設備/主機 將因虛耗許多資源於連線之處理，而使負荷升高、服務緩慢

攻擊結果

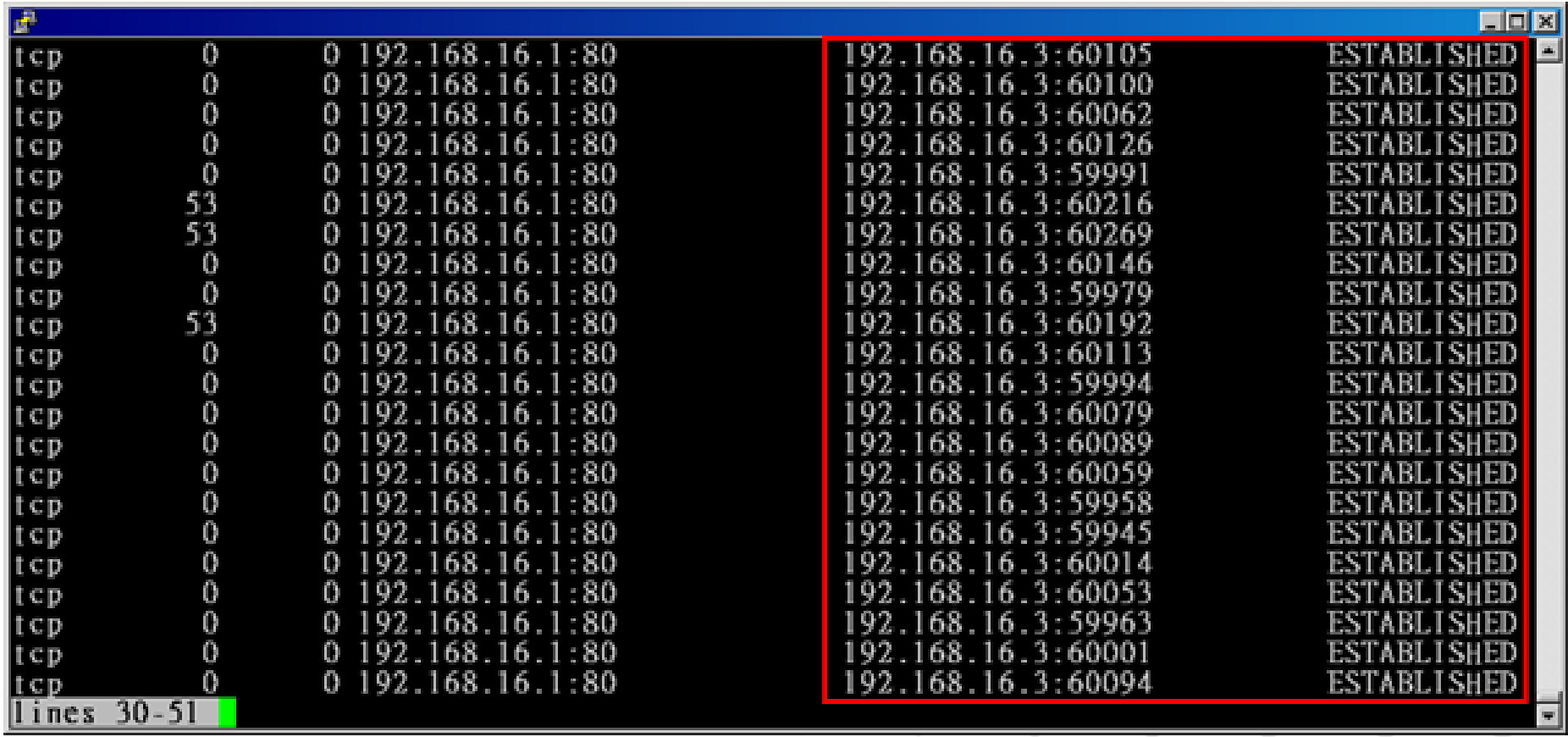


```
tcp        1      0 192.168.16.1:80         192.168.16.3:34914      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34888      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34929      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34889      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34907      CLOSE_WAIT
tcp        0      1 192.168.16.1:80         192.168.16.3:34878      LAST_ACK
tcp        1      0 192.168.16.1:80         192.168.16.3:34939      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34975      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34948      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34926      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34950      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34979      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:34958      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35005      CLOSE_WAIT
tcp        0    132 192.168.16.1:32769      192.168.16.2:8894       ESTABLISHED
tcp        1      0 192.168.16.1:80         192.168.16.3:34933      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35011      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35013      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35020      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35016      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35021      CLOSE_WAIT
tcp        1      0 192.168.16.1:80         192.168.16.3:35009      CLOSE_WAIT
```

Infrastructure-level – Zombie Connections

- 以大量之攻擊來源，與目標建立 TCP 連線，並定時發送封包保持連線不切斷
- 網路設備/主機 將因 Session Table 被建滿而導致負荷升高、無法服務
- 阻擋方式 –
  - Firewall/IPS – 限制同一 IP 之可連線數
  - 縮短 idle timeout 時間
  - 定時抓出建立過多連線的來源直接阻擋
  - 以效能較好之 Proxy/L4 設備代替主機建立連線

攻擊結果


tcp 0 0 192.168.16.1:80 192.168.16.3:60105 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60100 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60062 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60126 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:59991 ESTABLISHED
tcp 53 0 192.168.16.1:80 192.168.16.3:60216 ESTABLISHED
tcp 53 0 192.168.16.1:80 192.168.16.3:60269 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60146 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:59979 ESTABLISHED
tcp 53 0 192.168.16.1:80 192.168.16.3:60192 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60113 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:59994 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60079 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60089 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60059 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:59958 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:59945 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60014 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60053 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:59963 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60001 ESTABLISHED
tcp 0 0 192.168.16.1:80 192.168.16.3:60094 ESTABLISHED
lines 30-51

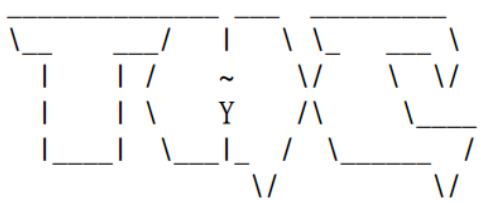
Service-level – Application Flood

- 以大量之攻擊來源，對目標不斷進行應用層之正常行為
- 主機將因不斷處理過量之請求而導致負荷升高、無法服務
- 常見攻擊方式
  - SSL Flood
  - HTTP Flood
  - DNS Flood
  - LOGIN Flood

Service-level – SSL Flood

- 以大量之攻擊來源，對目標不斷進行SSL Handshake
- 受攻擊主機將因不斷進行SSL協議交換而導致負荷升高、無法服務
- 加強攻擊效率：SSL Renegotiation

THC-SSL-DOS



http://www.thc.org

THC-SSL-DOS is a tool to verify the performance of SSL.

Establishing a secure SSL connection requires 15x more processing power on the server than on the client.

THC-SSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet.

This problem affects all SSL implementations today. The vendors are aware of this problem since 2003 and the topic has been widely discussed.

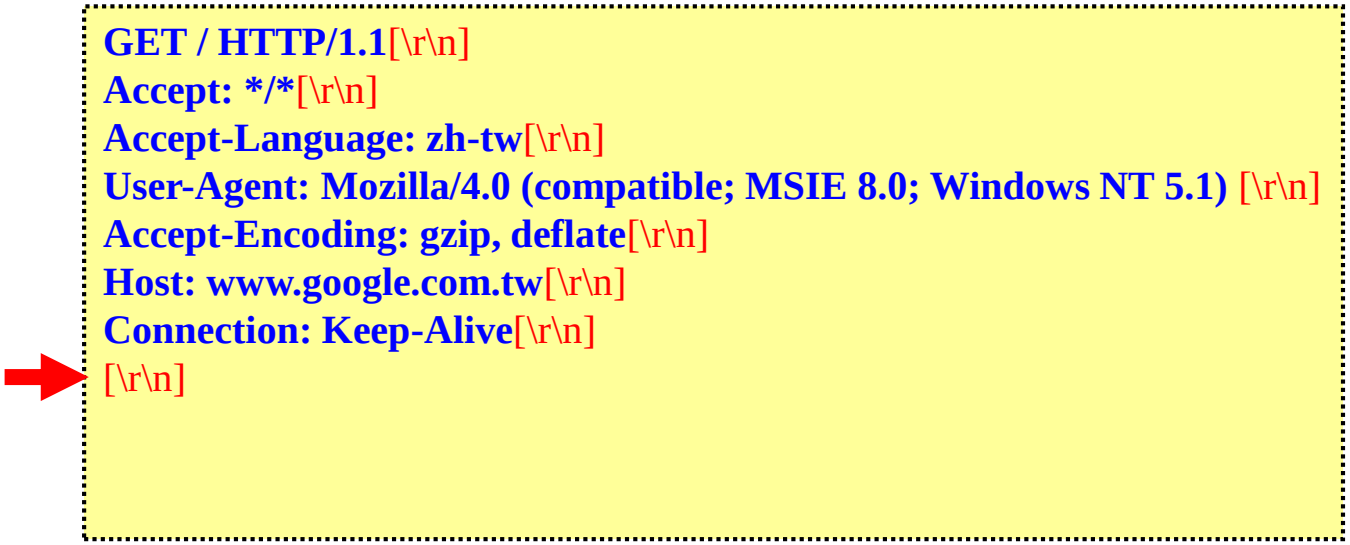
This attack further exploits the SSL secure Renegotiation feature to trigger thousands of renegotiations via single TCP connection.

```
Usage:
./thc-ssl-dos 127.3.133.7 443
Handshakes 0 [0.00 h/s], 0 Conn, 0 Err
Secure Renegotiation support: yes
Handshakes 0 [0.00 h/s], 97 Conn, 0 Err
Handshakes 68 [67.39 h/s], 97 Conn, 0 Err
Handshakes 148 [79.91 h/s], 97 Conn, 0 Err
Handshakes 228 [80.32 h/s], 100 Conn, 0 Err
Handshakes 308 [80.62 h/s], 100 Conn, 0 Err
Handshakes 390 [81.10 h/s], 100 Conn, 0 Err
Handshakes 470 [80.24 h/s], 100 Conn, 0 Err
```

Service-level – HTTP DoS

- GET with unended request
  - ex: Slowloris
- POST with unreached body
  - ex: OWASP HTTP Post Tool
- HTTP Flood
- CC攻擊
  - Proxy
  - iframe

正常的 HTTP GET



- 連續兩CRLF後視為請求結束

Slowloris

- GET / HTTP/1.1
- Host: www.google.com
- Connection: keep-alive
- User-Agent: Mozilla/5.0
- X-a: baaaaaaa
- X-a: b
- X-a: b
- X-a: b
- X-a: b
- X-a: b

正常的 HTTP POST

```
POST /accounts/ServiceLoginAuth HTTP/1.1[\r\n]
Host: www.google.com[\r\n]
Content-Length: 38[\r\n]
Connection: Keep-Alive[\r\n]
[\r\n]
Email=http.dos@gmail.com&Passwd=123456[\r\n]
```

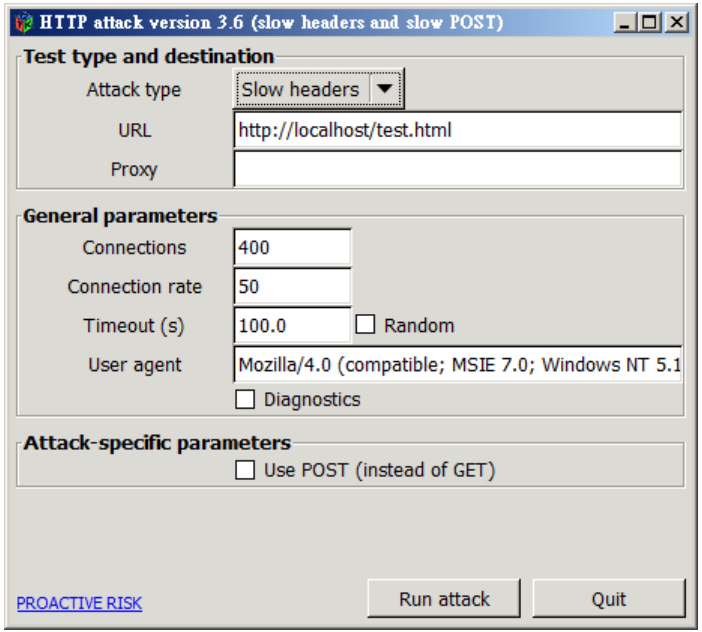
- 需於post body區接收到Content-Length指定的長度

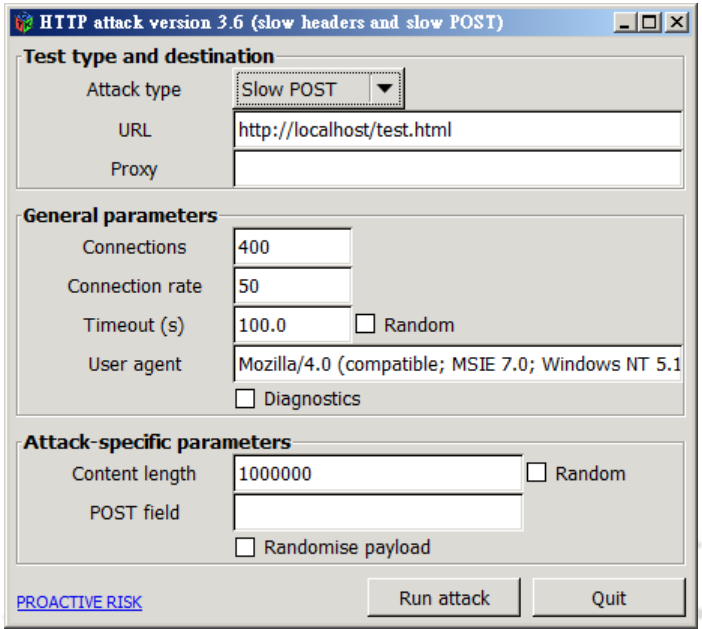
OWASP HTTP Post Tool

- POST / HTTP/1.0
- Host: victim.com
- Connection: keep-alive
- Content-Length: 10000000
- User-Agent: Mozilla/5.0

- username=AAAAAAAAAAAAAAAAAAAAA…

OWASP HTTP Slow Attack Tool





50

Service-level – Exploit

- Ex: ApacheKiller
- https://www.exploit-db.com/dos/

Apache Killer 測試方法

- 送出不正常的 Range Request

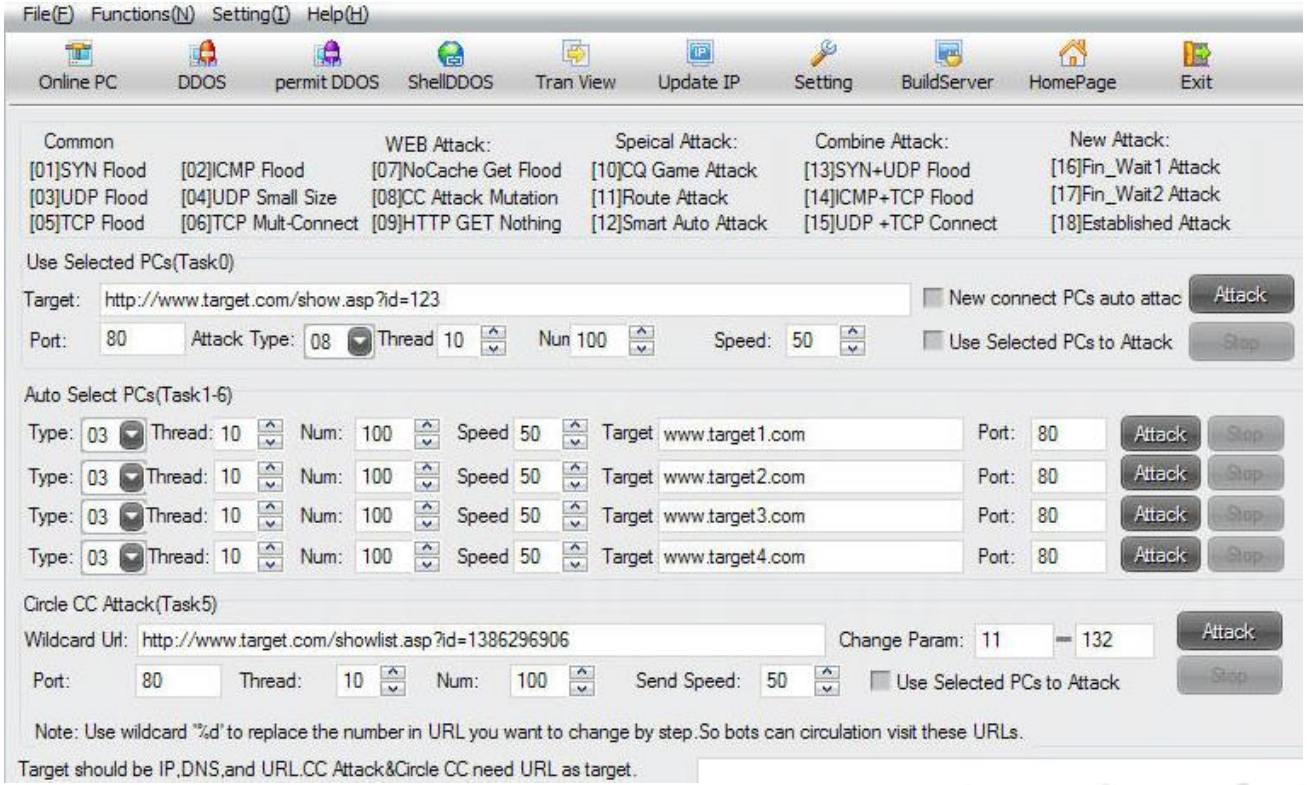
```
GET / HTTP/1.0[\r\n]
Host: default[\r\n]
Accept-Encoding: gzip
Range: bytes=0-,5-0[\r\n]
[\r\n]
```

- 若伺服器回應 206 Partial Content，則代表”可能”存在此弱點
- 經 Patch 過之伺服器應回應 200 OK

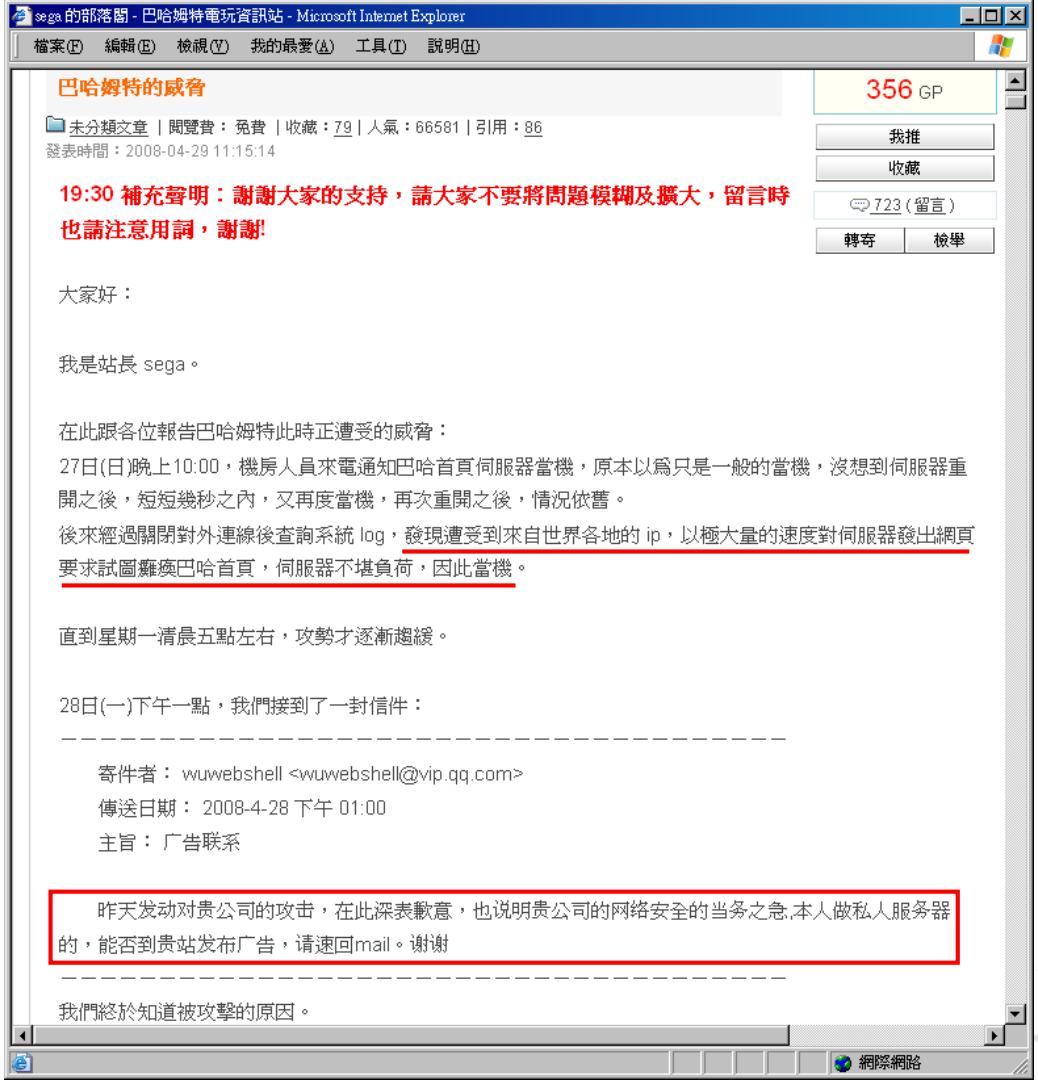
HTTP Flood

- 以大量之攻擊來源，對目標不斷發送 HTTP Request
- 主機將因不斷處理過量之請求而導致負荷升高、無法服務
- 阻擋方式 –
  - Firewall/IPS – 限制同一 IP 之可連線數/CPS
  - Reverse Proxy -限制同一 IP 之 Req/s
  - 限制同一 IP 之存取頻率 (ex: mod_evasive)
  - 以 L7 層之機制 (如Cookie/script) 阻擋
  - 辨識特徵

DDoS 工具控制台


File(F) Functions(N) Setting(I) Help(H)
Online PC
DDOS
permit DDOS
ShellDDOS
Tran View
Update IP
Setting
BuildServer
HomePage
Exit
Common
[01]SYN Flood
[02]ICMP Flood
[03]UDP Flood
[04]UDP Small Size
[05]TCP Flood
[06]TCP Mult-Connect
WEB Attack:
[07]NoCache Get Flood
[08]CC Attack Mutation
[09]HTTP GET Nothing
Speical Attack:
[10]CQ Game Attack
[11]Route Attack
[12]Smart Auto Attack
Combine Attack:
[13]SYN+UDP Flood
[14]ICMP+TCP Flood
[15]UDP +TCP Connect
New Attack:
[16]Fin_Wait1 Attack
[17]Fin_Wait2 Attack
[18]Established Attack
Use Selected PCs(Task0)
Target: http://www.target.com/show.asp?id=123
New connect PCs auto attac
Attack
Port: 80
Attack Type: 08
Thread 10
Num 100
Speed: 50
Use Selected PCs to Attack
Stop
Auto Select PCs(Task1-6)
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target1.com Port: 80 Attack Stop
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target2.com Port: 80 Attack Stop
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target3.com Port: 80 Attack Stop
Type: 03 Thread: 10 Num: 100 Speed 50 Target www.target4.com Port: 80 Attack Stop
Circle CC Attack(Task5)
Wildcard Url: http://www.target.com/showlist.asp?id=1386296906
Change Param: 11 - 132
Attack
Port: 80
Thread: 10
Num: 100
Send Speed: 50
Use Selected PCs to Attack
Stop
Note: Use wildcard "%d" to replace the number in URL you want to change by step.So bots can circulation visit these URLs.
Target should be IP,DNS,and URL.CC Attack&Circle CC need URL as target.

DDoS 案例分析


sega 的部落閣 - 巴哈姆特電玩資訊站 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
巴哈姆特的威脅
356 GP
未分類文章 | 閱覽費：免費 | 收藏：79 | 人氣：66581 | 引用：86
發表時間：2008-04-29 11:15:14
我推
收藏
723 (留言)
轉寄
檢舉
19:30 補充聲明：謝謝大家的支持，請大家不要將問題模糊及擴大，留言時也請注意用詞，謝謝!
大家好：
我是站長 sega。
在此跟各位報告巴哈姆特此時正遭受的威脅：
27日(日)晚上10:00，機房人員來電通知巴哈首頁伺服器當機，原本以為只是一般的當機，沒想到伺服器重開之後，短短幾秒之內，又再度當機，再次重開之後，情況依舊。
後來經過關閉對外連線後查詢系統 log，發現遭受到來自世界各地的 ip，以極大量的速度對伺服器發出網頁要求試圖癱瘓巴哈首頁，伺服器不堪負荷，因此當機。
直到星期一清晨五點左右，攻勢才逐漸趨緩。
28日(一)下午一點，我們接到了一封信件：
寄件者： wuwebshell <wuwebshell@vip.qq.com>
傳送日期： 2008-4-28 下午 01:00
主旨： 广告联系
昨天发动对贵公司的攻击，在此深表歉意，也说明贵公司的网络安全的当务之急,本人做私人服务器的，能否到贵站发布广告，请速回mail。谢谢
我們終於知道被攻擊的原因。
網際網路

發表人	標題 / 內容

張貼時間: 2008/11/07 21:14

【公告】優仕網遭駭客攻擊事件相關處理

親愛的優仕網會員們：

這陣子以來，我們收到許多詢問為何系統不穩定的客服信，以及類似像這樣的抱怨文章。大家的責備，代表的是對優仕網的關心，因為大家喜歡使用、想要登入，才會知道我們近日發生的問題。對於所有的責難，優仕網在此致上最深的謝意。

事實上，優仕網正遭受不明駭客的攻擊。

・第一波攻擊發生於2008-10-18星期六上午10點。當時，值班的客服人員突然收到大量客服信，表示無法進入優仕網首頁(自然也無法登入會員)。值班的客服人員立即通知公司技術主管與網管人員處理。我們到機房後，發現優仕網遭受到來自世界各地的ip、以極大量的速度(每秒4萬～10萬次)對伺服器發出網頁要求(DDOS攻擊)，試圖癱瘓優仕網。優仕網的硬體防火牆由於不堪負荷而停擺，造成網站無法對外服務，經工程師緊急處理，並請ISP公司協助之後，於當日下午1:30逐漸回覆正常。

・接下來，2008-10-20星期一上午10點、10-23星期四上午10點、10-24星期五下午6點、10-27星期一下午5點、10-31星期五下午6點多，分別遭受陸續幾波的攻擊。其中，我們多次尋求網路同業、防火牆供應廠商、ISP公司協助對抗駭客，也曾改變優仕網網站網址與伺服器IP，工程師晝夜不休，但仍無法有效抵擋。最後，我們因為借到極昂貴的防DoS攻擊的硬體設備、並在經銷商協助設定後，終於暫時成功阻擋駭客攻擊。

・2008-11-01星期六下午5點，我們接到署名「陳昊」、來自「hacker-tw@hotmail.com」的威脅Email。指稱「你們的網站這段時間遭受的攻擊是我們攻擊小組做的...」要求優仕網付錢給該“攻擊小組”，否則將繼續發動攻擊。由內文簡體字型、中文文法以及勒索金錢以美元計算判斷，駭客可能來自對岸。

・2008-11-02星期日上午，我們向刑事警察局偵三隊完成報案，案類為「恐嚇取財」。

・報案之後的本週內，我們仍持續受到不定期的攻擊，但由於防禦措施發揮作用，優仕網自11月以來，在各項網站功能與服務上，已經完全正常。

Babyhome網站遭DDoS爆量攻擊，搶修開放國內連線

文/劉哲銘 (記者) 2008-12-31

我要收藏

國內知名的親子網站Babyhome昨日（12月30日）遭受大量的DDoS癱瘓攻擊，現已緊急搶修回復提供服務

國內知名的親子網站Babyhome（寶貝家庭親子網），在昨日（12月30日）遭受大量的DDoS癱瘓攻擊，經緊急搶修，在今日（12月31日）下午3點陸續回復提供服務。

寶貝家庭親子網總經理江立群表示，該網站在上周五傍晚就先遭受到一波試探性的DDoS攻擊，但對網站的運作並沒有造成太大的影響。然而30日中午，又遭受到大量的連線攻擊，每秒同時有數萬個連線，而且攻擊來自於多個國家，因而癱瘓了整個網站的運作。

在遭受到DDoS攻擊之後，江立群指出，該公司的技術人員立刻透過放在電信服務商租用的IPS，過濾掉可疑的IP，並將之封鎖。同時也調整防火牆的設定，將攻擊的來源位址封鎖。然後就立刻針對10多臺伺服器上的系統進行維修，並且修復資料庫，確保資料沒有遺失。

PushDo殭屍網路對315個網站發動DoS攻擊

文/陳曉莉 (編譯) 2010-02-02 我要收藏

Adair發現，PushDo最近更改它的程式碼以打造無用的SSL連結並藉以影響約315個網站，涵蓋了last.fm、微軟網站、paypal、紅帽，以及政府/教育機構與SANS等。

ShadowServer研究人員Steven Adair在上周指出，PushDo殭屍網路透過傳遞SSL封包而對全球315個知名的網站展開阻斷式服務（DDoS）攻擊。

根據趨勢科技（TrendMicro）的說明，PushDo殭屍網路始於2007年1月，它是全球第二大的垃圾訊息殭屍網路，未具名遠播的原因在於作者使用了許多不同的技術使它難以被偵測，然而PushDo不但主導全球大量的垃圾訊息發送，同時也是犯罪集團用來散布惡意程式的主要管道。

Adair發現，PushDo最近更改它的程式碼以打造無用的SSL連結並藉以影響約315個網站，這些數量龐大的殭屍電腦持續傳遞無用的SSL連結然後斷線，周而復始，而且嘗試把這些活動埋沒在正常的流量中，使之不易被偵測到。但事實是這些網站的流量激增到數百萬，如果網站原本每天只有數十萬的連結，或是網站並未具備無限制的頻寬，便可能形成阻斷式服務攻擊而使得正常流量無法存取。

Adair認爲，就技術上而言，上述網站遭到了攻擊，但看起來讓這些網站無法運作並非PushDo的真正目的。Adair列出受到攻擊的網站，涵蓋了last.fm、微軟網站、paypal、紅帽，以及政府/教育機構與SANS等。

此外，Adair也指出目前尚無完整的解決之道，網站業者雖然可以更改IP位址，但PushDo終究可以發現新的IP位址而再度展開攻擊。（編譯/陳曉莉）

DNS業者遭DoS攻擊　殃及Amazon等購物網站

文/陳曉莉 (編譯) 2009-12-25

我要收藏

Neustar仍在調查攻擊來源，初期認為該攻擊應該不是針對特定的網站，不過Neustar亦未透露被殃及的網站業者。

本周三（12/23）美國加州的網路用戶一時無法連上Amazon或Wal-Mart等其他電子商務網站，隨後相關網站DNS服務供應商Neustar證實，是該公司遭受阻斷式服務攻擊（denial-of-service，DoS）所致。

大量的異常查詢導致Neustar旗下的UltraDNS服務失常，Neustar表示，該公司在幾分鐘內就發現攻擊行動，一小時內就控制了情況。此外，該攻擊僅影響美國北加州地區的網路使用者。

所謂的阻斷式服務攻擊是駭客透過多台傀儡電腦發出大量封包，以癱瘓業者的系統，因而影響其他使用者的存取。

Neustar仍在調查攻擊來源，初期認爲該攻擊應該不是針對特定的網站，不過Neustar亦未透露被殃及的網站業者。

根據外電報導，在上周三傳出使用者無法存取網站服務的業者包括Amazon、Amazon AWS、Wal-Mart、Salesforce及Expedia等。（編譯/陳曉莉）

美國及南韓政府網站相繼遭到駭客攻擊

文/陳曉莉 (編譯) 2009-07-09 我要收藏

駭客主要的目的似乎只是想要癱瘓官方網站並引起注意。因為研究人員發現在這些攻擊中並未夾雜獲利或其他目的。

就在美國國慶日（7/4）的周末，傳出美國政府網站遭到分散式阻斷服務（DDoS）攻擊，隨之南韓政府網站也受到攻擊，導致許多網站無法運作。南韓國家情報院指出，相關的攻擊可能來自北韓或支持北韓政府的組織。

傳出受到攻擊的二十多美國網站包括白宮、美國財政部、美國聯邦貿易委員會、美國交通部、聯邦航空總署、國防部、國土安全部等官方網站，以及紐約與那斯達克證交所，與華盛頓郵報等私人網站。另外，南韓政府機構、銀行及報紙等網站也蒙受同樣手法的攻擊。

目前遭受攻擊的網站皆漸次恢復正常，研究人員估計，駭客是透過數萬台的僵屍電腦進行DDoS攻擊，企圖癱瘓這些網站。

安全研究人員認爲駭客所使用的攻擊手法並不複雜，先是透過惡意程式感染個人電腦，再指使這些電腦進行流量攻擊。南韓國家情報院指出，駭客掌控了2萬台以上的殭屍電腦，其中多數位於南韓。但另有其他研究人員指出此次攻擊所透過的殭屍電腦多達5萬台。

但駭客主要的目的似乎只是想要癱瘓官方網站並引起注意。因爲研究人員發現在這些攻擊中並未夾雜獲利或其他目的；同時美國政府組織也表示並沒有任何資料流失，並強調每天都有針對聯邦網絡的攻擊行動發生。（編譯/陳曉莉）

Sony網路服務受DDoS攻擊癱瘓

向Sony抗議 駭客組織發動DDoS攻擊

作者：廖珮君 -04/11/2011

Sony遭到Anonymous的DDoS攻擊，包括PSN(PlayStation Network)、PS Store(PlayStation Store)、以及官方網站的連線皆受到影響。

整件事源起於2011年初，Sony向兩名破解PS3的駭客正式提出告訴，引起駭客組織Anonymous的不滿，不僅在網路上公開對Sony下戰帖，更於4月初持續發動DDoS攻擊，按照過往手法，由志願者下載開放源碼工具LOIC(Low Orbit Ion Cannon)，並與IRC伺服器連結，同步發動攻擊，癱瘓Sony旗下網站及PlayStation相關服務。

其實，Anonymous應用LOIC發動DDoS攻擊，已經不是第一次了，包括Amazon、Paypal、MasterCard等企業都曾經是Anonymous的攻擊目標，不同的是，Anonymous這次的攻擊對象不只是Sony本身，還包括高層主管的個人資料，外電表示，Sony已經延聘專家研擬因應之道。

高頻寬NTP 放大DDoS攻擊 30天內劇增371%

作者：本篇文章內容由廠商提供，不代表資安人科技網觀點 -03/13/2014

Prolexic Technologies提供領先全球的分散式阻斷服務(DDoS)攻擊保護服務，現為Akamai (NASDAQ交易代號：AKAM) 旗下公司，今天針對日益嚴重的透過網路時間協定 (NTP) 的DDoS攻擊，提出高度警戒建議書。近年來，DDoS攻擊日益猖獗，隨著新型DDoS工具套組的問世，攻擊者能輕易針對線上目標發動高頻寬、高流量的DDoS攻擊。

Akamai 安全部門資深副總裁暨總經理Stuart Scholly表示：「觀察結果指出，針對我們客戶群的NTP放大攻擊在2月攀升了371%。事實上，今年我們在網路上觀察到的最大型攻擊類型均為NTP放大攻擊。」

NTP 放大攻擊早已構成為威脅，隨著一些新型DDoS攻擊工具套組問世，惡意入侵者能更輕易地透過數個伺服器發動攻擊。惡意入侵者只要利用現有的NTP 放大攻擊工具套組，配合數個容易入侵的NTP伺服器，便能輕易發動100 Gbps或更大規模的攻擊。

令人不安的DDoS攻擊趨勢

僅一個月內 (2014年2月與2014年1月比較):

- NTP 放大攻擊數字上升371.43%
- DDoS攻擊頻寬平均高峰上升217.97%
- DDoS攻擊平均高峰流量上升807.48%

NTP 放大攻擊與過去兩年出現的最大型攻擊不同，並非集中於某個特定產業。2月份NTP 放大攻擊針對的產業涵蓋金融、遊戲、電子商務、網際網路及通訊、媒體、教育、軟體即服務 (SaaS) 供應商及保全。

63

歐洲遭遇史上最大DDoS攻擊

文/陳曉莉 (編譯) 2013-03-28

讚 231 Share g+1 14 我要收藏

此一攻擊主要透過開放的DNS解析器，流量從一開始的10Gbps、90Gbps，逐漸擴大至300Gbps，成為網路史上最嚴重的一次DDoS攻擊，差點癱瘓歐洲網路。

歐洲反垃圾郵件組織Spamhaus近來遭到阻斷式服務攻擊（DDoS），負責Spamhaus網站效能與安全服務的業者CloudFlare協助減輕攻擊威脅時發現，此一攻擊主要透過開放的DNS解析器，流量從一開始的10Gbps、90Gbps，逐漸擴大至300Gbps，成為網路史上最嚴重的一次DDoS攻擊，差點癱瘓歐洲網路。

根據外電報導，Spamhaus是因為把垃圾郵件業者Cyberbunker納入黑名單後遭受其報復攻擊行動。

此波攻擊從上周一（3/18）展開，一直到今天（3/28）才結束。CloudFlare共同創辦人暨執行長Matthew Prince說明，從第一天起他們便發現駭客主要透過開放的DNS解析器進行攻擊，第一天的攻擊流量只有10Gbps，第二天的攻擊高峰達到90Gbps，第三天則維持在30Gbps至90Gbps之間，然後駭客休息了一天。

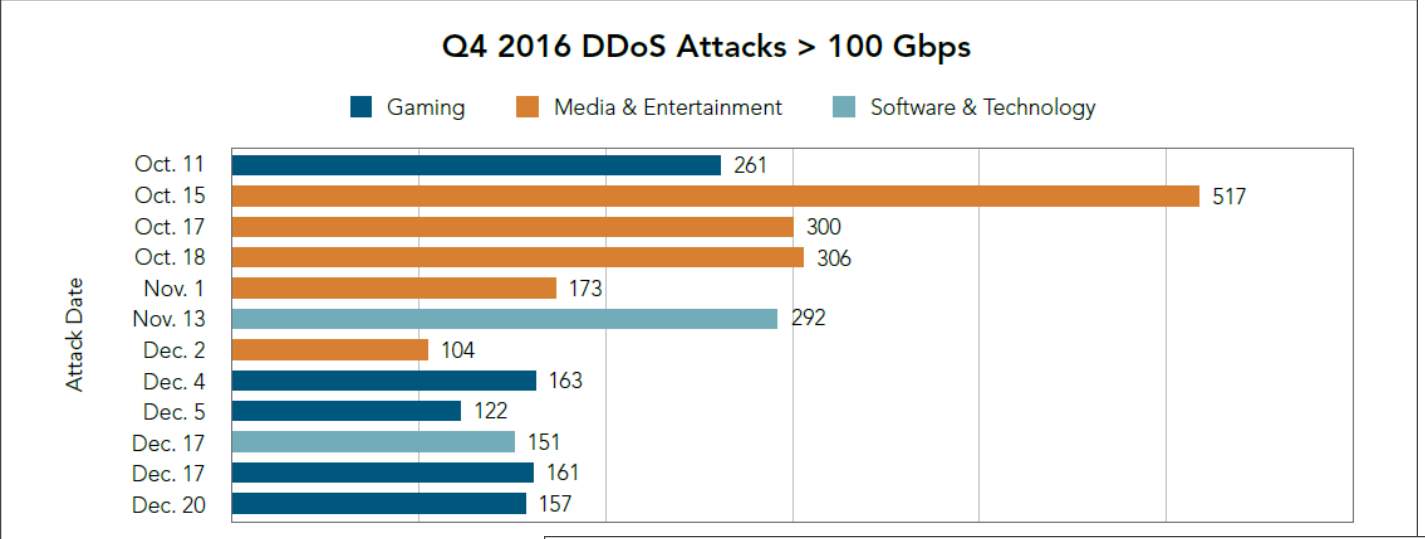


Figure 2-3: Twelve DDoS attacks exceeded 100 Gbps ir

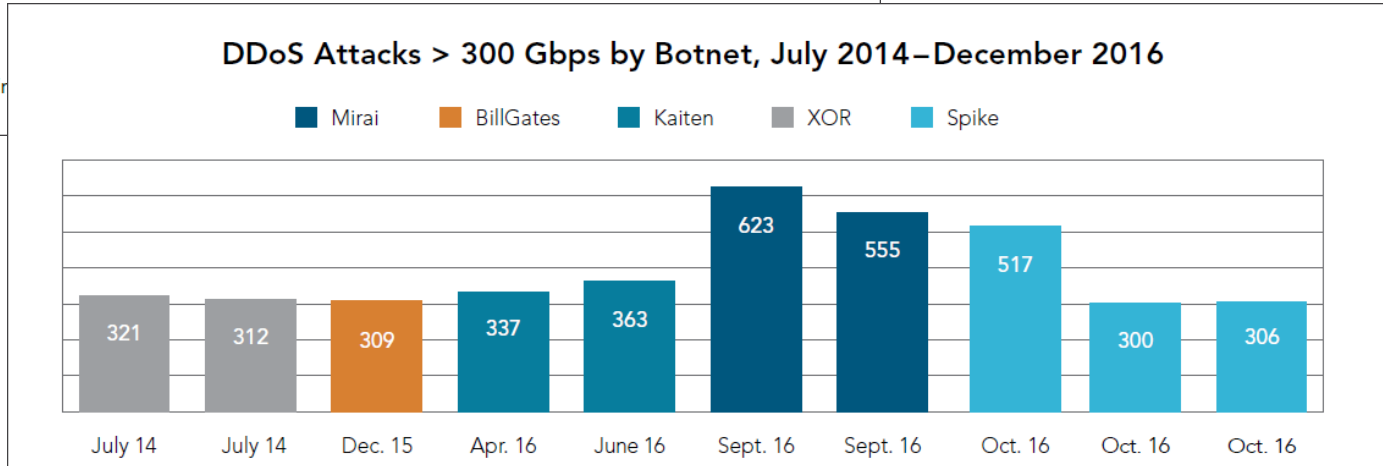


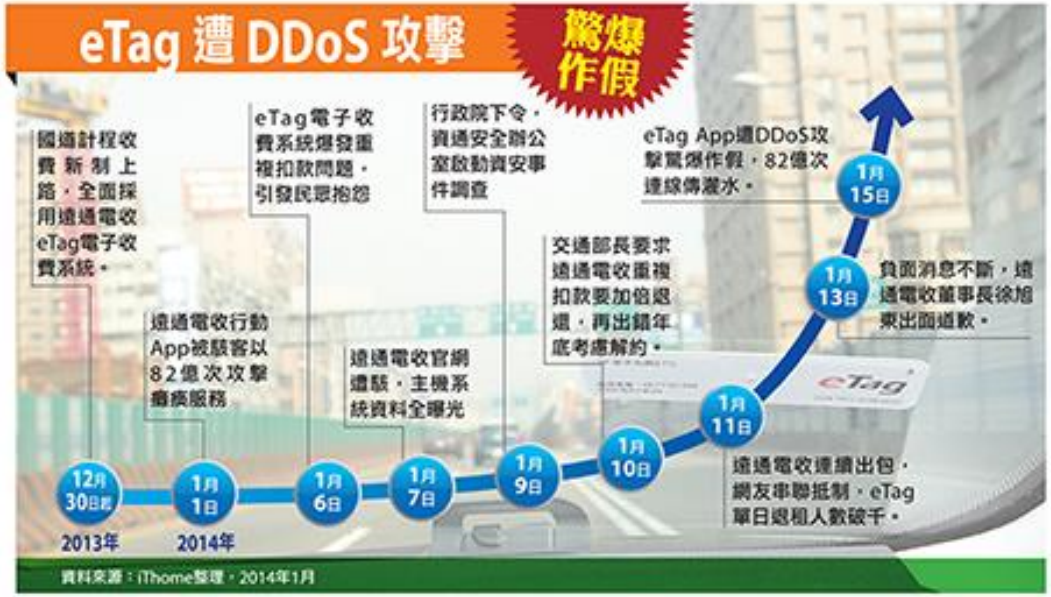
Figure 2-4: Four botnets generated 10 DDoS attacks exceeding 300 Gbps between July 2014–December 2016. Seven of these occurred in 2016

eTag遭DDoS攻擊驚爆作假，82億次攻擊傳灌水

文/[黃彥棻](#) (記者) 2014-01-15

讚 81 Share g+1 10 我要收藏

據遭外傳的技服中心調查報告初稿結果，遠東電收App遭DDoS攻擊傳作假，82億次攻擊連線次數傳灌水，遠通用瞬間最大連線推算3.5小時明顯不合理。遠東電收也於傍晚承認，一開始誤以為遭駭而報警，但調查過程中還原資料發現並非大量網路攻擊。



66

香港公投網站DDoS攻擊內幕大公開，連Google、亞馬遜都擋不住

一開始投票，PopVote線上投票網站就遭遇到了超大規模的DDoS攻擊，攻擊流量達網路史上第二高，連找Amazon或Google網路服務支援都擋不住，CloudFlare最後靠著全球網路服務業者聯手，才撐過了這10天投票過程。

文/ 余至浩 | 2014-08-20 發表

+1 208

67

香港線上投票網站 PopVote 攻擊數據

- 2014/06 公投活動前
  - SYN Flood Attack　100M packet/s
  - SSL Flood Attack
  - HTTP Flood Attack
  - DNS Flood Attack　250M query/s
  - 128Gbps

  - DNS Reflection Attack　> 100Gbps
  - NTP Reflection Attack　> 300Gbps

中國網路大砲又爆新招，綁架Facebook登入服務流量作為DDoS攻擊子彈

4月26日時，不少中國網友連上使用了Facebook登入機制的網站時，發現瀏覽器還打開了wpkg.org與ptraveler.com這2個小網站，他們不知道，自己可能成為了中國防火長城DDoS大砲的子彈，成了中國對外發動DDoS攻擊的幫兇

文/ 李建興 | 2015-04-29 發表

讚 1.4 萬 按讚加入iThome粉絲團 讚 分享 737

資安業者發現大量SOHO路由器變殭屍，淪為DDoS攻擊大軍

資安業者Incapsula指出，可能有數十萬甚至上百萬台的SOHO族專用路由器已成為殭屍路由器，被駭客用來執行大規模的DDoS攻擊。在為期111天的調查中，Incapsula就找到超過4萬個不重覆攻擊IP，

文/ 陳曉莉 | 2015-05-13 發表

讚 1.4 萬 按讚加入iThome粉絲團 讚 分享 864 g+1 22

殭屍路由器及C&C中心的全球分佈圖。

70

Akamai：1988年的路由器老舊協定漏洞被拿來進行高效率的DDoS反射式攻擊

在最近的攻擊行動中，駭客偏好那些RIPv1路由表上擁有大量可疑路徑的路由器，利用了500個仍採用RIPv1的路由器，並讓每個單一請求都傳送504位元的封包到目標網站，造成該站最多每秒收到320萬個封包，尖峰攻擊流量達到每秒12.8Gb。

文/ 陳曉莉 | 2015-07-03 發表

讚 1.4 萬 按讚加入iThome粉絲團 讚 分享 217 g+1 7

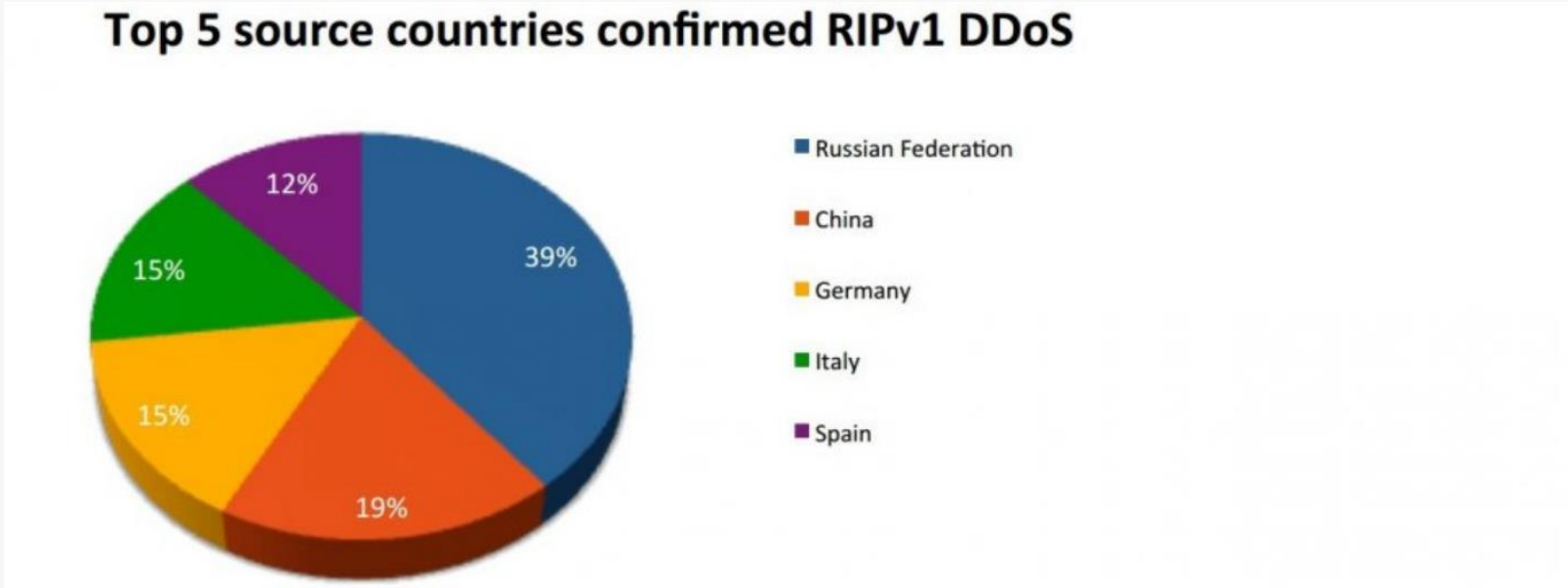


Figure 9 - Top 5 countries observed during largest RIPv1 DDoS reflection attack

新聞

史上最大DDoS攻擊來襲， 逾14萬台網路攝影機帶來近1Tbps的巨量攻擊

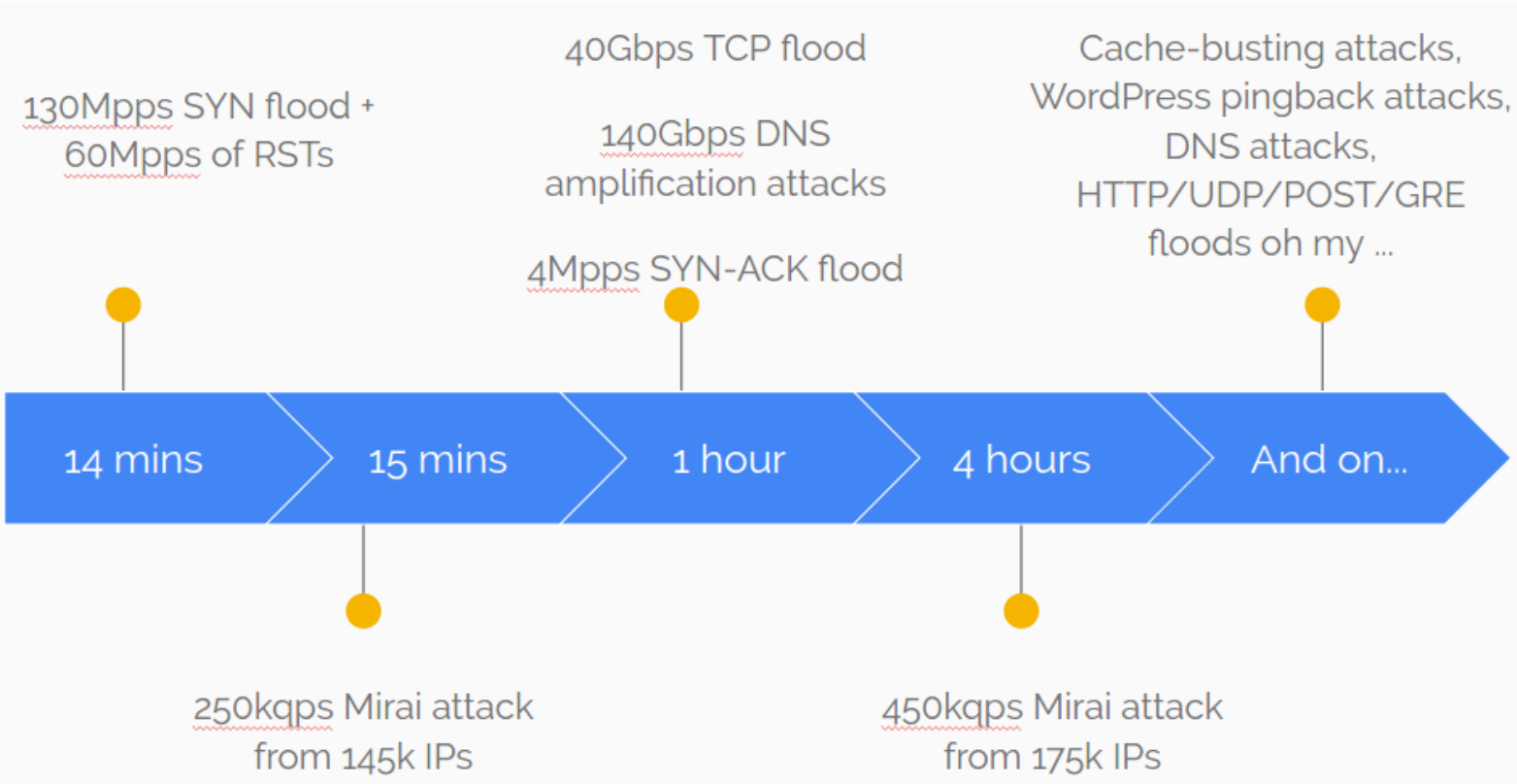
法國網站代管業者OVH指出在9月18日到22日，遭14.5萬台網路攝影機組成的殭屍網路發動DDoS攻擊，其顛峰攻擊流量接近1Tbps。

文/ 陳曉莉 | 2016-09-26 發表

法國的網站代管服務供應商OVH坦承在上週遭到大規模的分散式阻斷服務攻擊（DDoS），其顛峰攻擊流量接近1Tbps，成為史上最大的DDoS攻擊。

這波攻擊從9月18日持續到9月22日，OVH創辦人Octave Klaba指出，該攻擊行動是藉由14.5萬台的攝影機或監視器所組成的殭屍網路所發動， 雖然OVH的最高可見攻擊流量只接近1Tbps，然而該殭屍網路的攻擊能力應可達1.5Tbps。

KrebsonSecurity



正確的 DDoS 防護觀念

DDoS 阻擋？

- 很難完全，可擋到80%以上已經很好
- 準確率 & 誤擋率
- 不同攻擊手法有不同的阻擋方式，也存在差異很大的偵測方式及準確率/誤判率
- DDoS “Mitigation”
  - 緩解受到的攻擊量，使服務可正常運行，而非完全阻擋

理想的防護模式

- 雲端清洗 + 本地防護
  - 本地防護
    - Infrastructure (FW, IPS, …)
    - Application (ADC, WAF, …)

- 無雲端清洗中心，只有本地防護的情況
  - Muti ISP + Smart DNS
  - Multi DC + GSLB
  - BGP black-hole

阻擋 DDoS 的對策

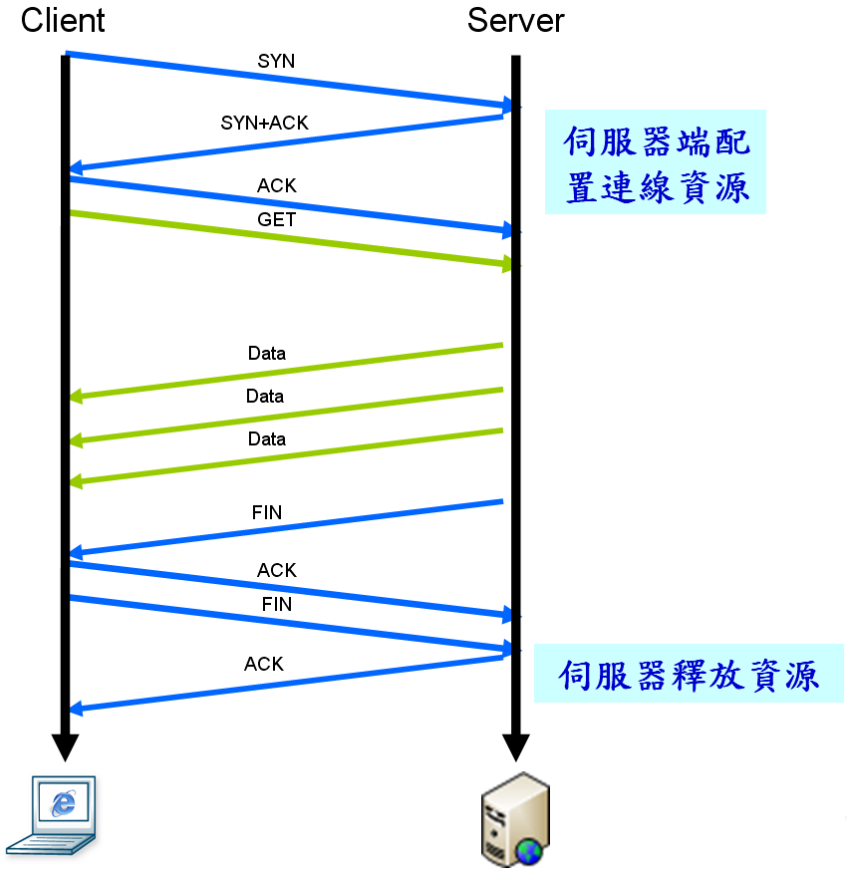
- 特徵辨識
  - IP Header
  - TCP/UDP Header
  - Application Header
- 網路層行為限制
  - Limit Connect/s (per IP)
  - Limit Concurrent Connections (per IP)
- 網路層正常回應處理
  - SYN Proxy
  - SYN Cookies

77

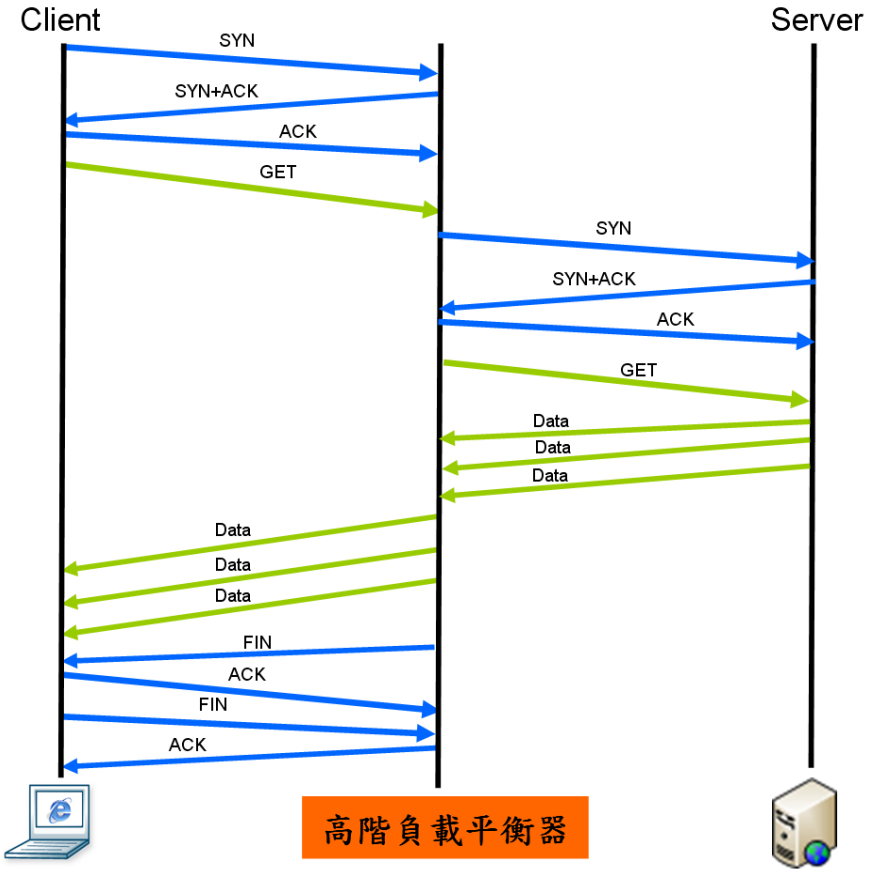
阻擋 DDoS 的對策 (續)

- 應用層行為限制
  - Limit Request/s (per IP)
- 應用層回應探測
  - 302 Redirect
  - HTML/JavaScript Redirect
  - JavaScript/Cookie Challenge
- 統計

一般的 HTTP Request 過程



支援 delayed binding 的設備



臺灣常見廠商

- 清洗商
  - Akamai
  - Arbor
  - CloudFlare
  - F5
  - Google
  - NexusGuard
  - Radware

  - ISP (CHT / TWM / FET)

- 設備商
  - Arbor
  - A10 / Citrix / F5
  - Checkpoint / Radware
  - FW / NGFW / IPS

  - 綠盟、黑洞、傲盾 …

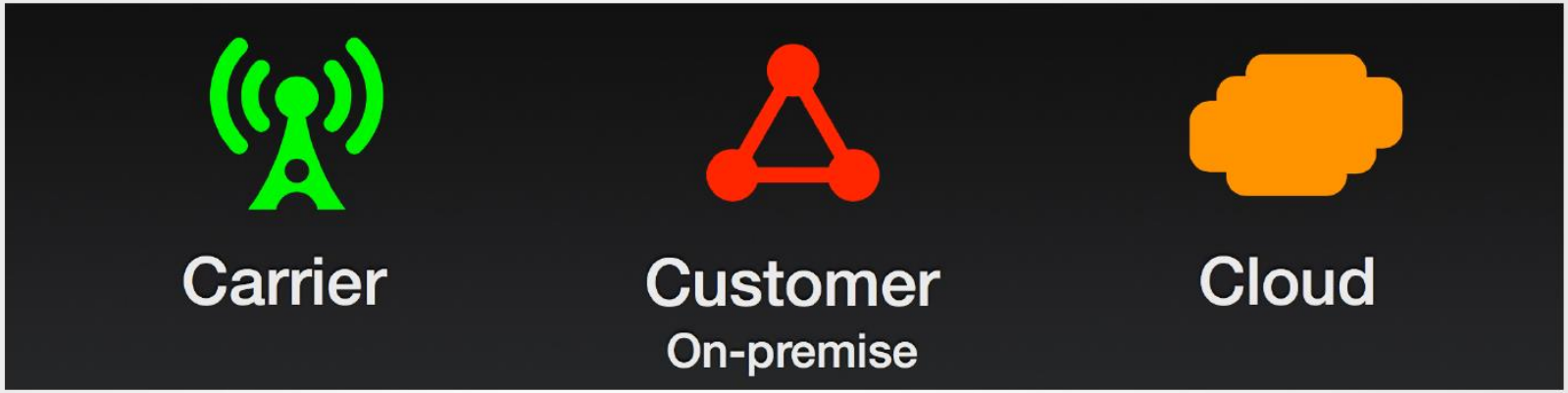
其他對策

- 台灣 ISP 常見協助防禦方案 –
  - Black Hole
    - 由境外 Core Router 直接將受攻擊目標 IP/網段 設至 Null Route
  - BGP
    - 棄用受攻擊 IP/網段
  - DNS
    - 配合 Dynamic DNS / GSLB 機制更換服務 IP

82

DDoS 防護位置比較

資料比較：F5



	Carrier	Customer On-premise	Cloud
優點	• 容易增加DDoS 防禦 • 位於網路上游	• 迅速辨識與阻擋攻擊 • L 7防護位於App 附近 • SSL 金鑰自我管理	• 大頻寬承受能力 • 與全球級電信業合作 • 世界級攻擊防禦與應變能力
缺點	• 清洗能耐有限(頻寬限制與L7 能力缺乏) • 缺少資安專家協助應變 • 單一路徑阻擋攻擊	• 無法阻擋海量攻擊 • 單一BOX不易全面兼顧 • 需雇用資安專家，以及自行管理DDoS 防禦系統 • 使用自己的線路	• “依需啟用模式” 需要較長時間才能發揮效果 • SSL 金鑰須交出才能保護加密流量 • 共用服務，有連鎖影響的風

DDoS攻擊處理流程

- 診斷
- 對症下藥
  - 洪水攻擊 – 請求 ISP/清洗商 協助
    - Black Hole
    - 更換 IP / Multi ISP / GSLB
  - 網路層攻擊 –更換設備/關閉功能/調整系統參數
  - 應用層攻擊 – 增加服務能量、減少異常存取
- 辨識特徵 + 過濾
  - 網路層特徵
  - 應用層特徵
- Redirection / Challenge / Authentication
- 同時協調廠商借調設備
  - DDoS Retainer ?

前置作業

- 使用監控工具收集各網路節點、以及主機之運作資訊
  - 主機運作狀態紀錄
    - cpu/memory/sessions/bandwidth/packets/…
  - 網路設備狀態紀錄
    - loading/vlan/bandwidth/packets/protocol/sessions/events/…
  - 日誌紀錄集中收集
    - access log/error log/events/…
- 建議軟體
  - cacti
  - opennms
  - nagios / zabbix
  - OSSIM

診斷

- 懷疑受到攻擊時，儘速調閱受影響系統、及前方相關設備之

1) 運作效能狀態
2) 網路流量
3) 日誌紀錄
4) 應用程式存取紀錄
5) 及其他前置作業中有收集之資訊

側錄封包

- 若既有之資訊不足以判斷遭受何種攻擊，則於系統進出口處之路由器或交換器上，啟動Port Mirror機制，並以封包側錄軟體收集一定量封包後，交由專業人員進行分析。

- 使用軟體
  - tcpdump
  - wireshark / tshark

對症下藥

- 判斷出攻擊的手法後，採取相對應的阻擋措施。（如前述原則）
- 若既有主機、或設備無功能可防禦，則儘快協調專業廠商借調設備作防禦。

請 ISP/IDC 協助

- 若線路頻寬滿載，則需儘速請 ISP/IDC 協助
  - 暫時加大頻寬
  - 過濾攻擊封包（需提供特徵）
- 如果攻擊者之初始行為與正常連線無異，無特徵可供辨識，則通常ISP/IDC可處理的範圍仍有限，需雙方配合，前面過濾、後方也擋，才可有效防禦。

事件檢討

- 於攻擊事件結束後，將所發生的原因、過程、處理方式，撰寫為事件紀錄簿，供後續發生類似情況時有處理方式可遵循。
- 若原有之資訊建設無法阻擋遇到的攻擊類型，則告知管理階層需增加適當之防禦設備，否則往後同樣的事件仍可能再度發生。

DDoS 防護能力的養成

- 久病成良醫
- 熟知各種攻擊方式及防護對策
- 不斷更新全球趨勢及攻擊方式
- 定時測試自家的防護能力
  - VA/PT => DDoS評估及演練
- 多看 iThome 文章 [無誤]

Q
A

Thanks