網際網路DDoS的防禦機制

03 17 2011

Agenda

- DDoS的現況說明
  - DDoS的現況說明
  - DDoS的常見的手法
  - DDoS的防禦機制說明
- Backhole機制說明
  - Blackhole說明
  - Blackhole優點
  - Case Study
- 結論

DDoS的現況說明

- Y10較Y09 DDos的成長102%
- Attack Size > 49Gbps
- Average < 90 sec one attack

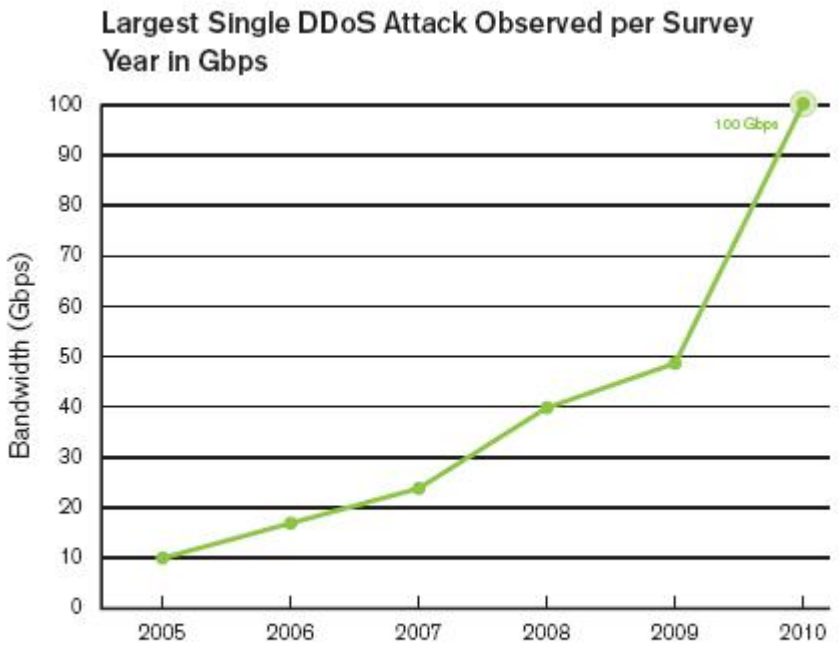


Figure 1
Source: Arbor Networks, Inc.

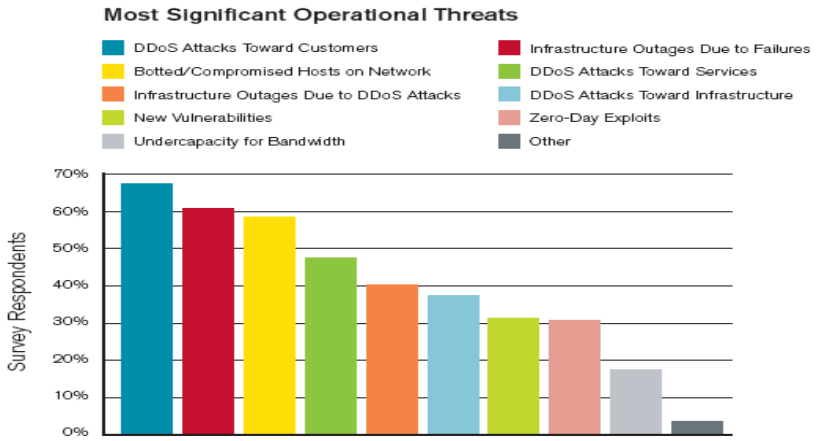


Figure 7
Source: Arbor Networks, Inc.

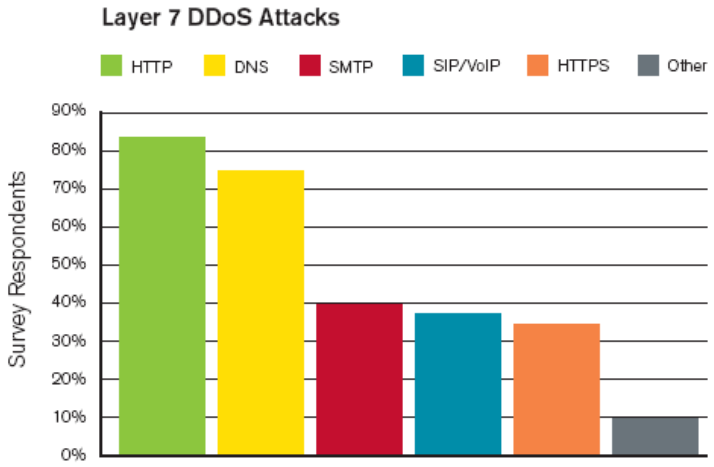
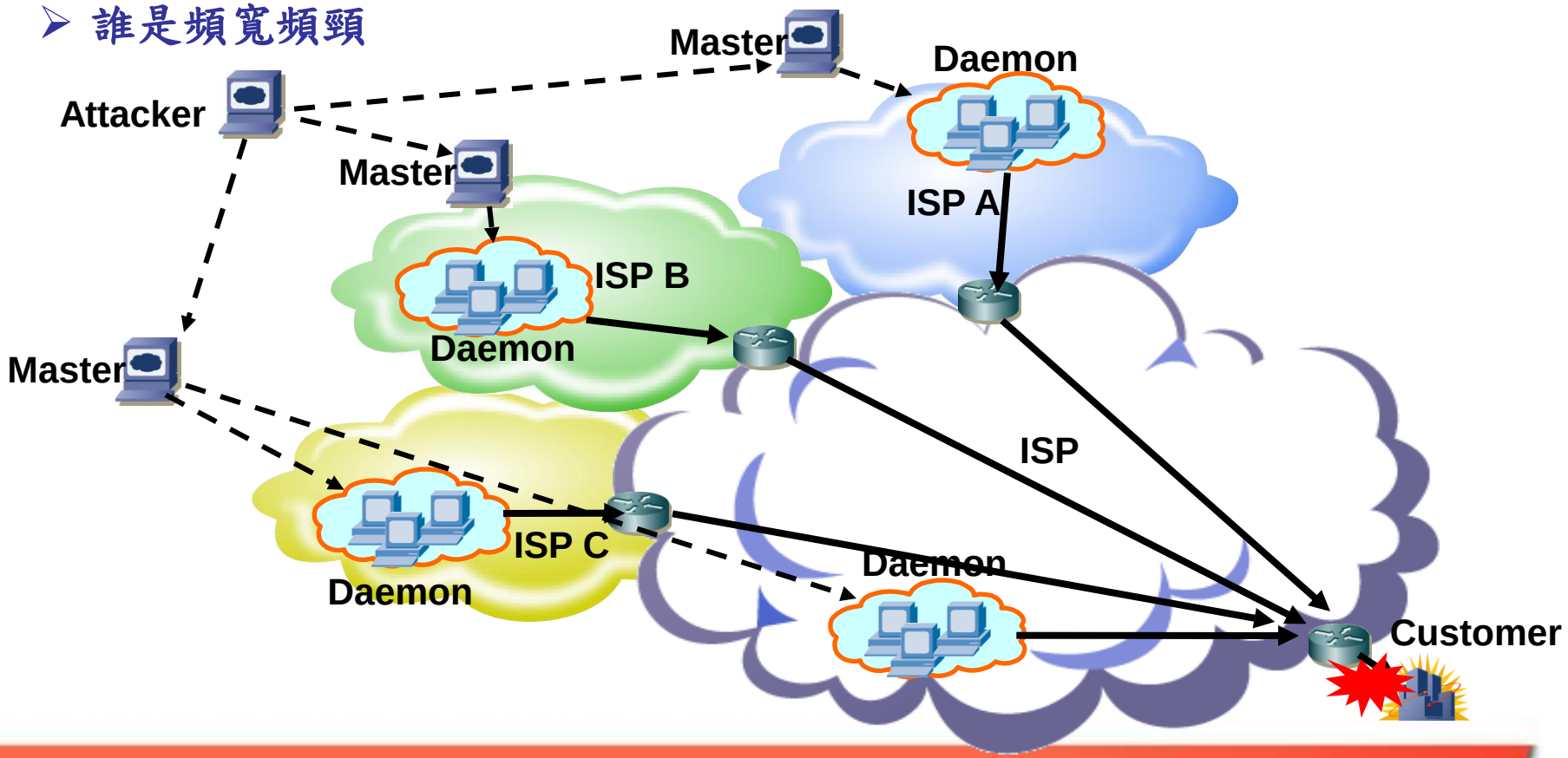


Figure 8
Source: Arbor Networks, Inc.

DDoS的常見的手法

DDoS常見的攻擊手法

- 被供擊者往往受到來自四面八方 souce ip ?
- Target IP(Customer) 為ISP 所有
- 誰是頻寬頻頸



DDoS防禦機制說明

- DDoS偵測
  - 許多ISP 均採用Arbor Peakflow 來作DDoS偵測機制
- DDoS防禦與清除
  - Clean Pipe
  - Network wash Machine
  - IDS(Next IDS)
- ISP聯防
  - Black hole (BGP community)
  - Clean Pipe 2.0 or above

Blackhole說明

Blackhole的說明

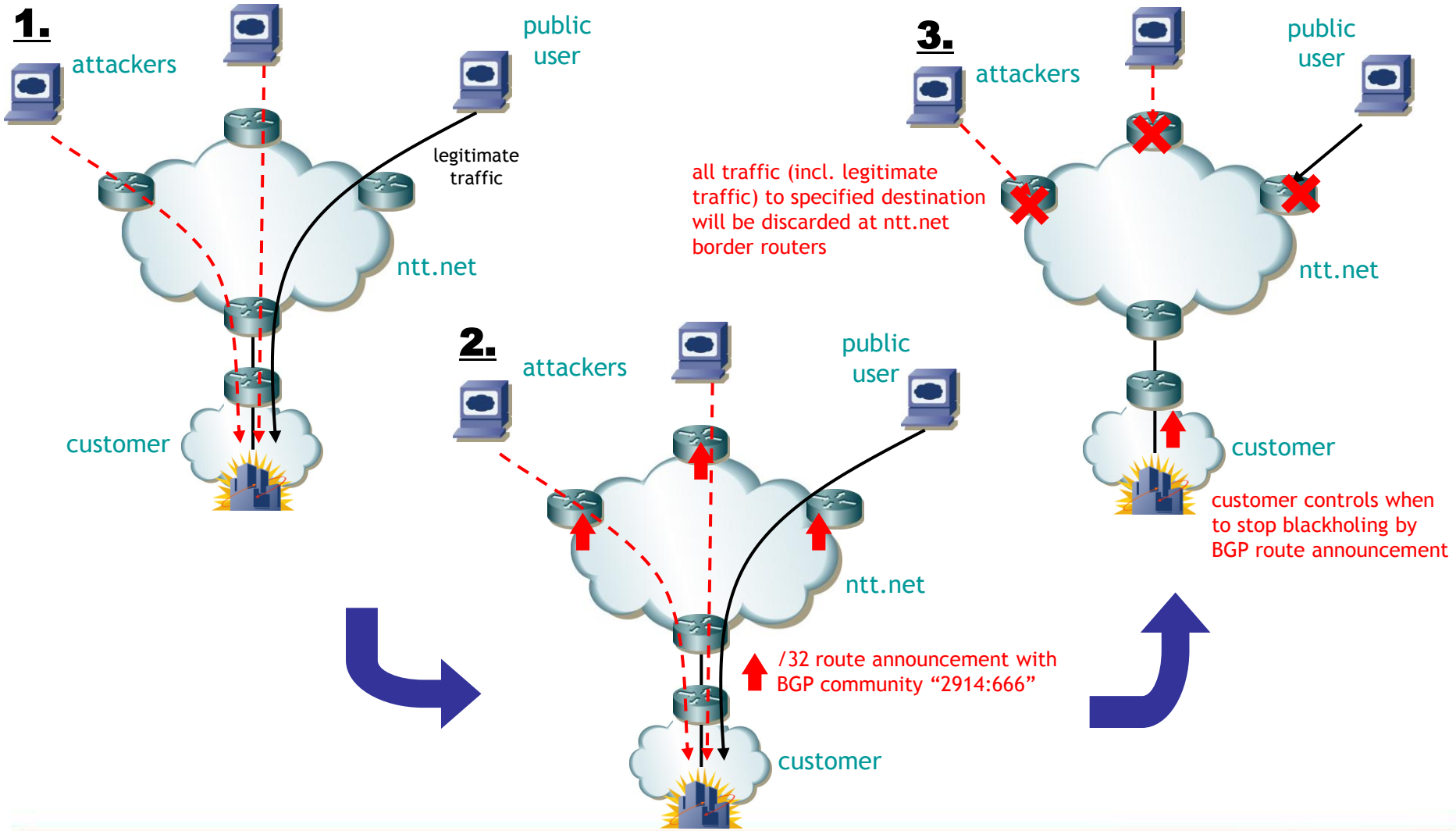
- 採用BGP Community機制達到快速防禦(通常執行後能在5分鐘之內完成)
- 世界知名ISP (NTT、PCCW、Flag等)均有提供此機制

Blackhole的優點

- 是一個最基本且最有效的DDoS防禦方式
- 對各ISP並無需要投資額外的CPEX
- 各ISP對自己的服務能有自控權

台湾大哥大

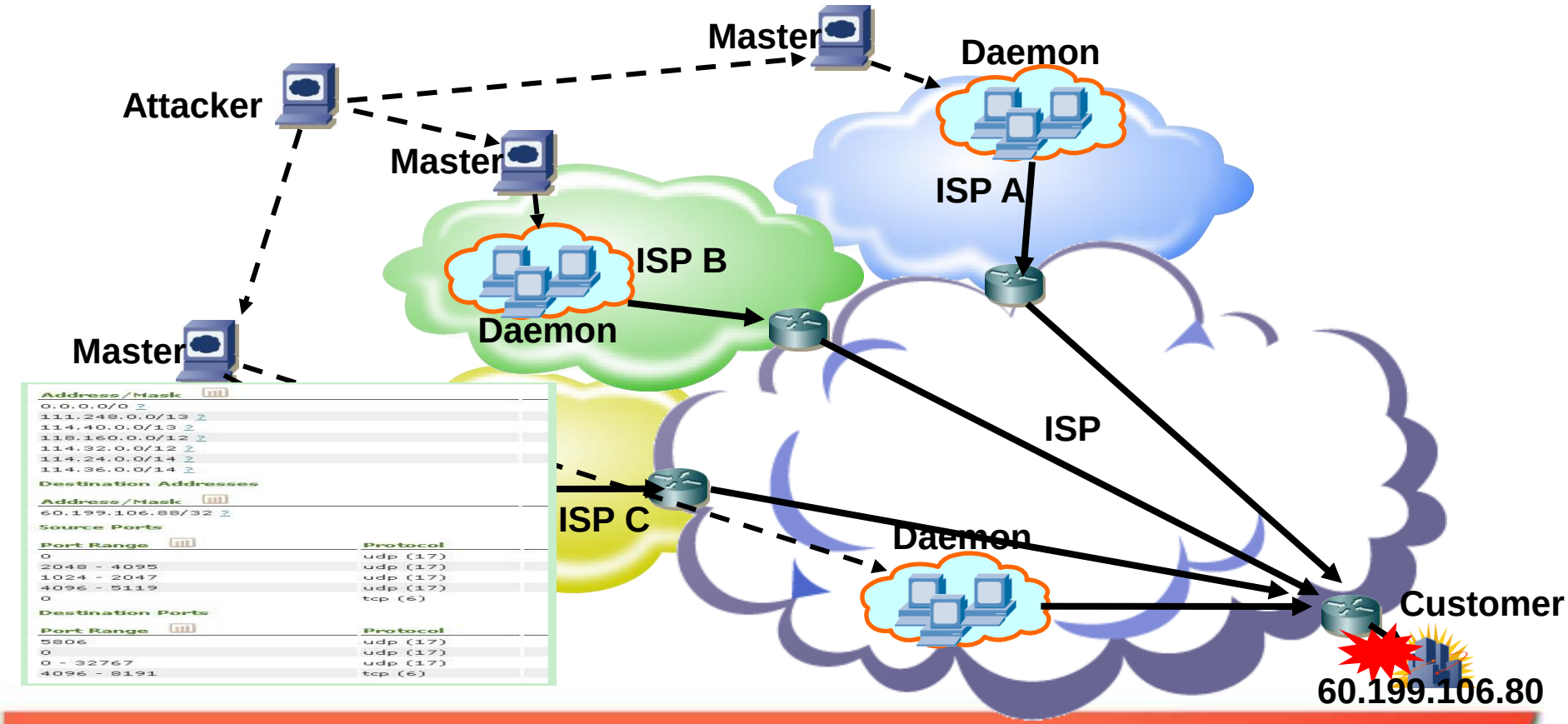
Blackhole說明



Case Study

ISP 受到國內其它ISP的DDoS攻擊

- 現況是採用email通知 or 電話通知，但往往時程需要數個小時以上
- 若採用blackhole機制，只要短短5分鐘內即能完成防禦



結論

- 由於Blackhole是一套透過基本的BGP community達到各ISP聯防的機制，且國外大型ISP均有此機制，建議國內各ISP業者也能建立此Blackhole機制
- 由於Blackhole並不需要額外的CPEX，且建立後各ISP對於自己的客戶受到DDoS攻擊有較高的自主權，對於國內ISP發展是有正面的幫助
- 提昇國內DDoS的防禦能力是大家共同的期望，還望各長官能多多支持

END