利用 Middlebox 的 TCP 反射放大式攻擊

TWCERT/CC 蕭信仁

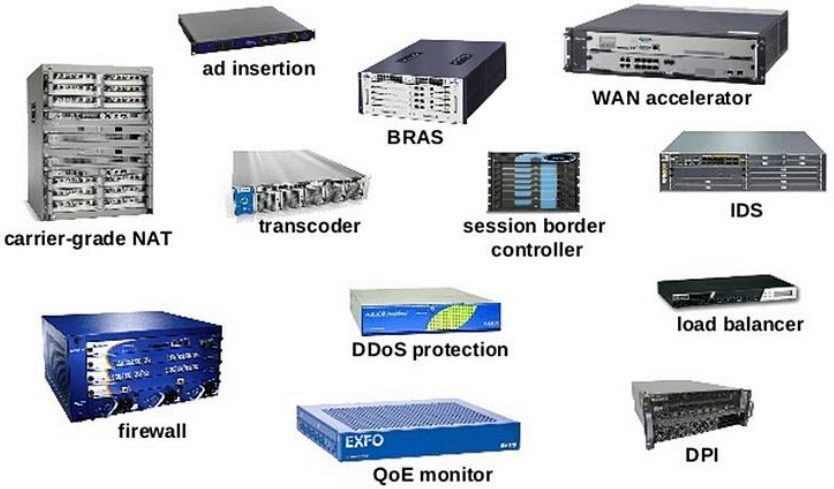
Agenda

- 什麼是 Middlebox?
- UDP 與 TCP 反射放大攻擊
- 使用 TCP SYN 的 Middlebox TCP 反射放大攻擊與案例
- 非 TCP SYN 的 Middlebox TCP 反射放大攻擊與案例
- 建議的防護或緩解方法

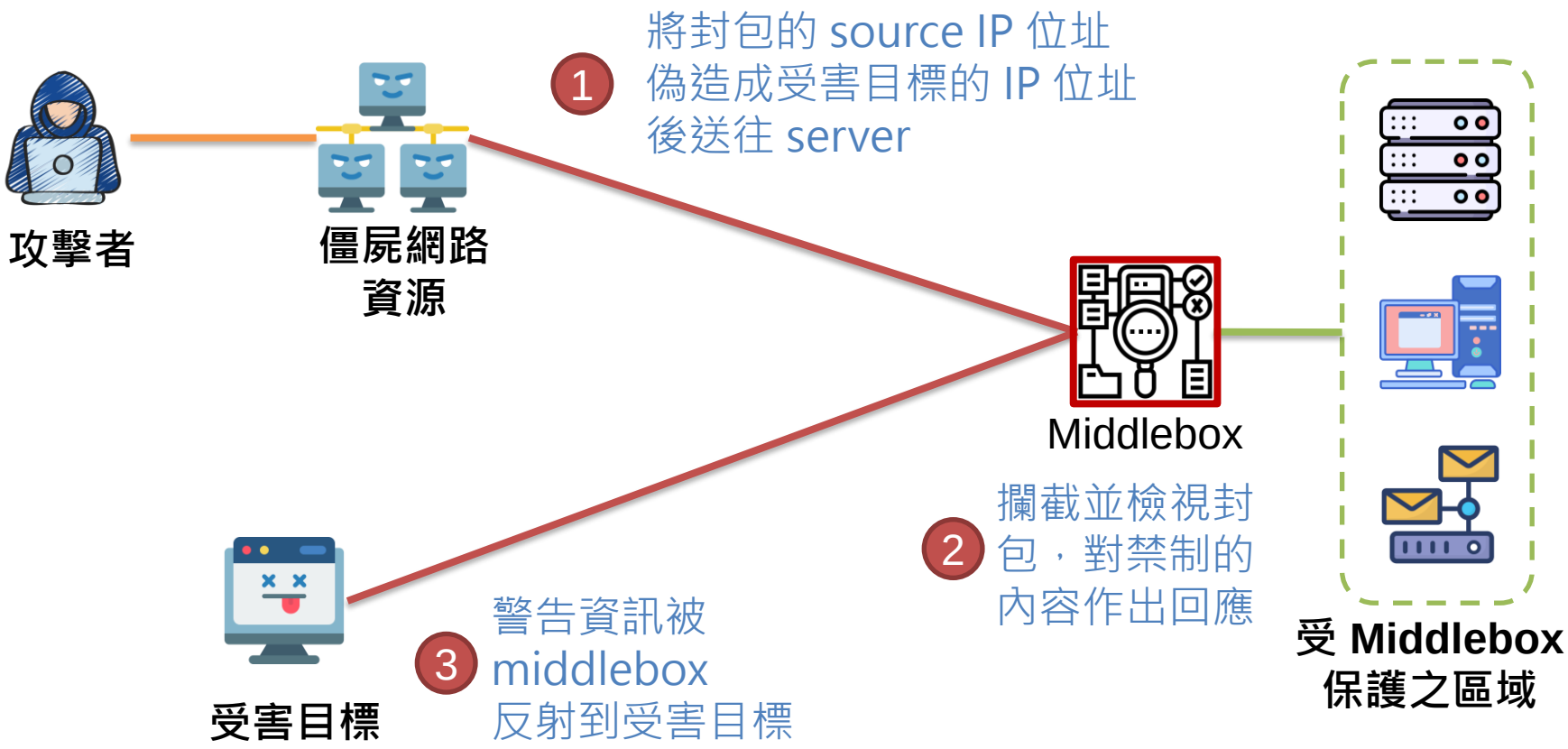
什麼是 Middlebox?

- Middlebox 是位於網路通訊兩終端路徑中的網通設備，具有下列一種或多種功能：
  - 檢查封包
  - 過濾封包
  - 更改封包內容
  - 採用廠商各自的 DPI (Deep Packet Inspection)

- 常見的 Middlebox 設備
  - 網路位址轉譯器 (NAT)
  - 入侵偵測/防護系統 (IDS/IPS)
  - 防火牆 (Firewall)
  - 代理/反向代理器 (Proxy/Reverse Proxy)
  - 內容過濾系統 (Content Filtering System)

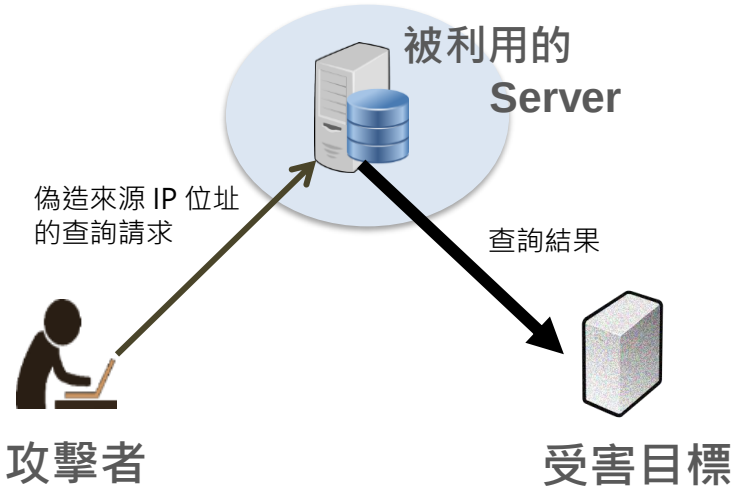


利用 Middlebox 的 TCP 反射放大攻擊



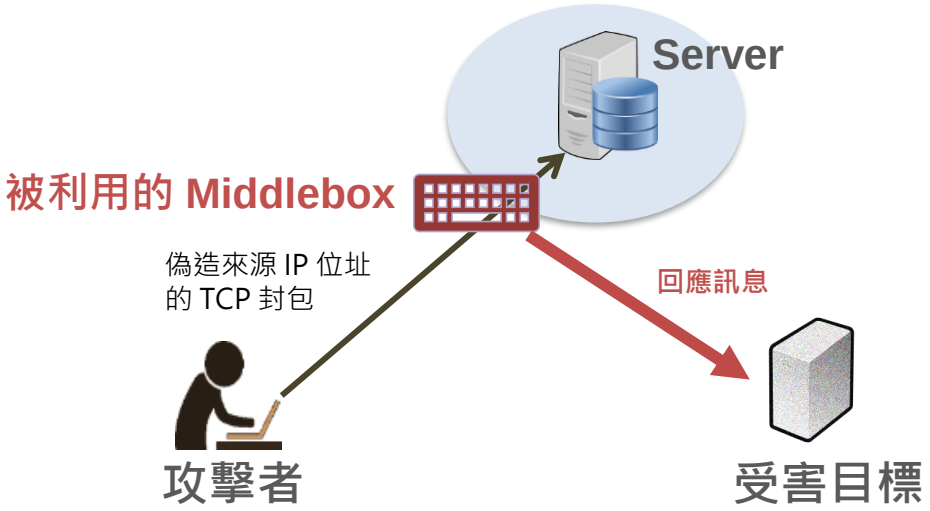
反射放大攻擊比較

傳統的反射放大攻擊



- 使用 UDP
- 利用伺服器本身作為反射
- 藉由應用層協定的特性 (如DNS)

利用 Middlebox 的 TCP 反射放大攻擊



- 使用 TCP
- 利用 Middlebox，而非伺服器
- 藉由對敏感資訊或關鍵字的 HTTP request

防護或緩解思路

傳統的反射放大攻擊

- 讓 client 再送一顆封包
  - 如關閉 DNS server 的 recursive query
- 限制能存取服務的來源

利用 Middlebox 的 TCP 反射放大攻擊

- 讓 client 再送一顆封包
- **使 Middlebox 有能力判斷 TCP connection 的有效性**

能否判別 source IP address spoofing?

Middlebox TCP 反射放大攻擊 - 使用 TCP SYN

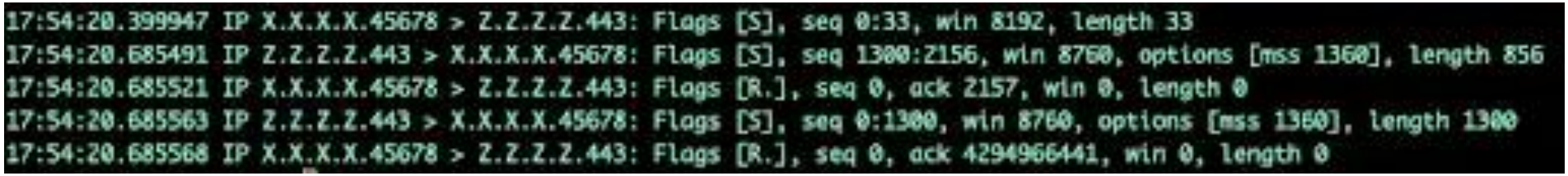
① 攻擊者在 TCP SYN 封包內夾帶 HTTP request
- Source IP 偽造成受害目標之 IP 位址
- HTTP request 內包含對敏感資訊的請求

② Middlebox 對此 TCP SYN 仍予以檢查

③ Middlebox 對服務請求內的敏感資訊作出放大回應

Middlebox 位於防火牆內，則有機會於防火牆處阻斷此類攻擊

TCP SYN 檢測 Middlebox 弱點
國外的特殊案例



https://www.akamai.com/blog/security/tcp-middlebox-reflection

① 攻擊者將 source IP 位址偽造成受害目標的I P 位址(X.X.X.X)後，將夾帶 HTTP request 的 TCP SYN 送往 Z.Z.Z.Z

② Middlebox 代表 Z.Z.Z.Z ，對受害目標 X.X.X.X 發送一長度為 856 bytes 的 TCP SYN

③ 受害目標 X.X.X.X 因未開啟 port 45678 而回傳 RST

④ Middlebox 再次發送長度為1300 bytes 的 TCP SYN 給受害目標，形成**無限放大攻擊。攻擊者若事先得知受害目標的監聽 port 清單，還能另外展開資源消耗攻擊。**

Middlebox TCP 反射放大攻擊 – 其他形式

① **<SYN; PSH+ACK>**

- 先對 Middlebox 發送一正常的 TCP SYN，其 sequence number 為 s
- 立刻再向 Middlebox 發送 PSH+ACK 封包，包含 HTTP request，sequence number 為 s+1

② **<SYN; PSH>**

- 與 <SYN; PSH+ACK> 同，但第二顆封包不帶 ACK

③ **PSH**

- 單純送出一個 HTTP request

④ **PSH+ACK**

- 送出一個 HTTP request + ACK

Middlebox TCP 反射放大攻擊 – 其他形式 *cont.*

Strategy	Response %	Max Amplification
⟨SYN; PSH+ACK⟩	69.5%	7,455×
⟨SYN; PSH⟩	65.7%	24×
PSH	44.6%	14×
PSH+ACK	33.1%	21×
SYN (with GET)	11.4%	572×

https://www.usenix.org/system/files/sec21-bock.pdf

- <SYN; PSH+ACK> 基本上可涵蓋 <SYN; PSH>、PSH、PSH+ACK
- 目前對 Middlebox TCP 反射放大攻擊的檢測，以 TCP SYN 及 <SYN; PSH+ACK> 為主

建議的防護或緩解方法

- 更新 **Middlebox** 的韌體至最新版本
- 採用具 **TCP State Table** 監控功能的 **Middlebox**
- 將警告或說明資訊實作在另一台網頁伺服器上，而 **Middlebox** 僅送出一個 **HTTP redirect** 封包
- 將注入的警告或說明資訊，降到最小
- 不作任何的放大
  - 只讓 Middlebox 回送一個 RST 來關閉連線也是一個簡潔有力的方式。
- 丟棄任何流入的、帶有載荷的 **TCP SYN** 封包
  - Firewall ACL

    deny tcp any eq **80** host x.x.x.x match-all **+syn** -ack packet-length gt **100**

    - 攻擊者發送的 TCP 封包，不限定於 SYN。上述防火牆 ACL 作為參考用途，只顯示作用於 TCP SYN 封包的情況。
    - 攻擊者可能對任一埠發送帶有載荷的 TCP SYN 封包。上述防火牆 ACL 作為參考用途，只顯示作用於埠 80 的情況。
    - 攻擊者發送給的偽造封包不一定會大於100 bytes。

Thank You