電子郵件安全指引 - 電子郵件攻擊篇(下)

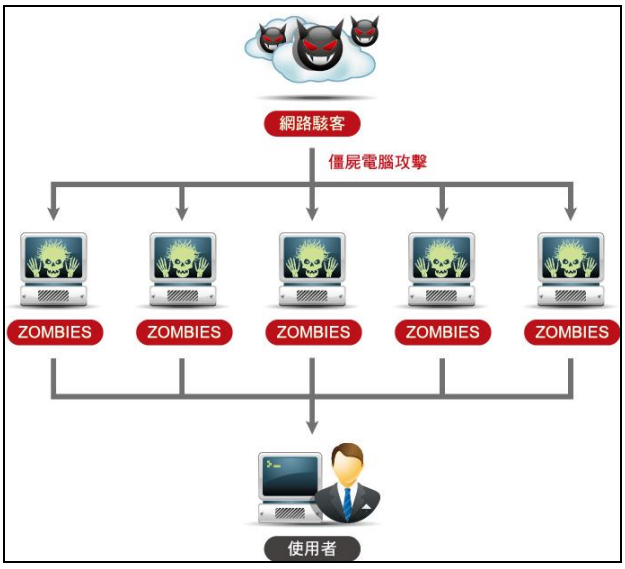
Openfind PM Team

在上一期的電子報當中，我們介紹了幾種常見的郵件攻擊類型，包括社交工程、垃圾信件、以及退信攻擊等，並同時輔以 Mail2000 電子郵件系統、MailGates 郵件防護系統的產品功能作為範例參考，讓大家更能瞭解實際上的應用。本期電子報將接續上次的內容，對其他種類的郵件攻擊方式做更進一步的說明。

DoS/DDoS 攻擊

DoS （Denial of Service） 與 DDoS （Distributed Denial of Service） 均為阻斷服務攻擊，目的是阻斷被攻擊方的正常網路服務。攻擊手法通常是讓被攻擊方的伺服器充斥大量且無意義的封包訊息，消耗它的網路頻寬與系統資源，導致網路癱瘓而無法提供正常的網路服務，目的多半為商業競爭、對手報復以及網路敲詐。

DoS 與 DDoS 兩者的差異在於 DoS 採的是一對一的攻擊方式，可以想像成攻擊與被攻擊方兩個互相比拚彼此的資源 （網路頻寬、CPU、記憶體等） 資源多的就獲勝，但隨著電腦與網路技術的發展，電腦處理能力迅速增長，使得 DoS 攻擊的困難度大增，而漸漸演變為 DDoS 攻擊。DDoS （Distributed Denial of Service） 中文譯為*分散式*阻斷服務，分散指的是由多台電腦一起向目標展開攻擊，攻擊的手法通常是駭客先入侵大量的電腦（一般稱這些電腦為殭屍電腦)，透過這些電腦在同一時間向針對目標發送大量封包，被攻擊方就會像受到洪水侵襲一般，因負荷不了導致系統癱瘓而中斷服務。



DDoS 攻擊示意圖

MaiGates - *DoS 防禦設定介紹*

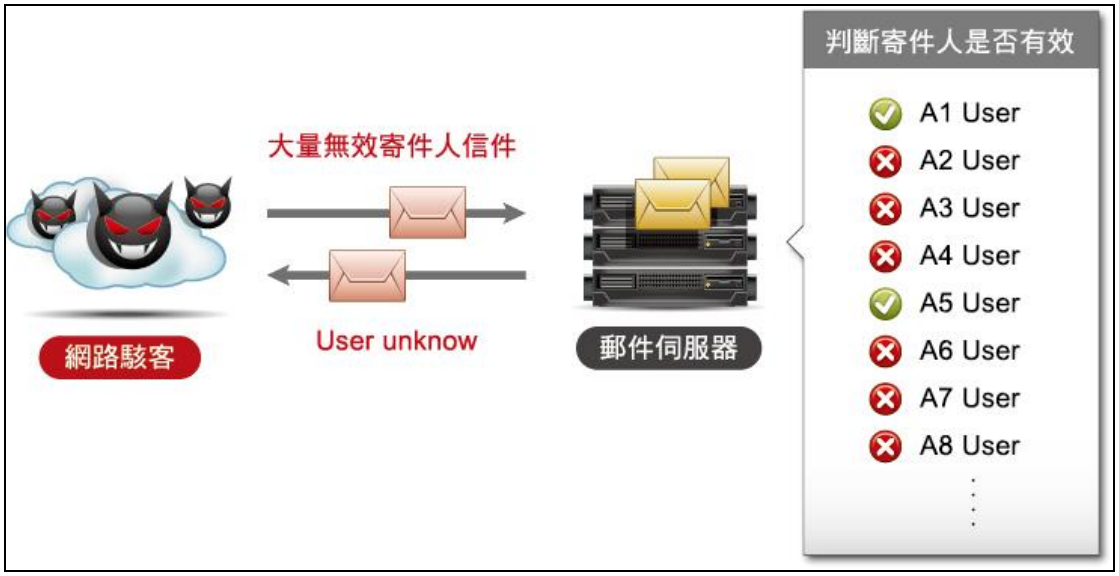
DoS 攻擊主要是透過不斷的發送大量封包來進行攻擊，MailGates 可透過設定同一個來源 IP 特定時間內允許的最大連線數，來對此種攻擊進行防禦。

舉例來說，MailGates 郵件防護系統中，若設定「在 10 秒內，允許 2 個同時連線」，則表示同一個 IP 在 10 秒內只能連線 2 次，第三次就會由系統自動阻斷連線，這樣一來就可以避免系統遭受 DoS 攻擊。

DoS 防禦設定

字典檔發送攻擊

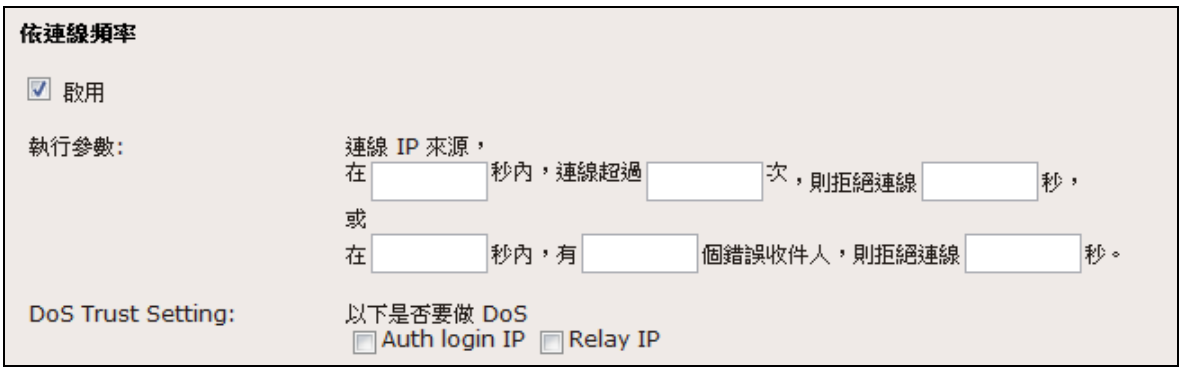
「字典檔發送攻擊」也屬於一種 DoS 攻擊，指的是駭客發送的信件中，含有超大量的收件人數量，因為像是從字典中一字不漏的抄取所有字母去組成亂數帳號，所以叫做字典檔發送攻擊，由於此類信件中充滿了大量的收信人，所以收件端伺服器要一再地核對收信人帳號並判斷帳號是否存在，並還要對外發出 user unknown 的系統服務訊息，讓收件端伺服器處理不勝負荷而導致當機。



字典檔攻擊示意圖

MaiGates - *DoS 防禦介紹*

字典檔攻擊主要是透過不斷寄送內含大量錯誤收件人的信件來試圖耗盡收件端的系統資源，針對此類攻擊可以透過 MailGates 郵件防護系統設定允許錯誤收件人的上限進行防禦。舉例來說，將 MailGates 設定成「60 秒內，有 2 個錯誤收件人，則拒絕連線 60 秒。」這樣當系統收到信件包含 2 個以上錯誤收件人時，就會拒絕該 IP 的來信 60 秒，這樣就可以避免因不斷收到大量錯誤收件人的信件而造成系統服務中斷。

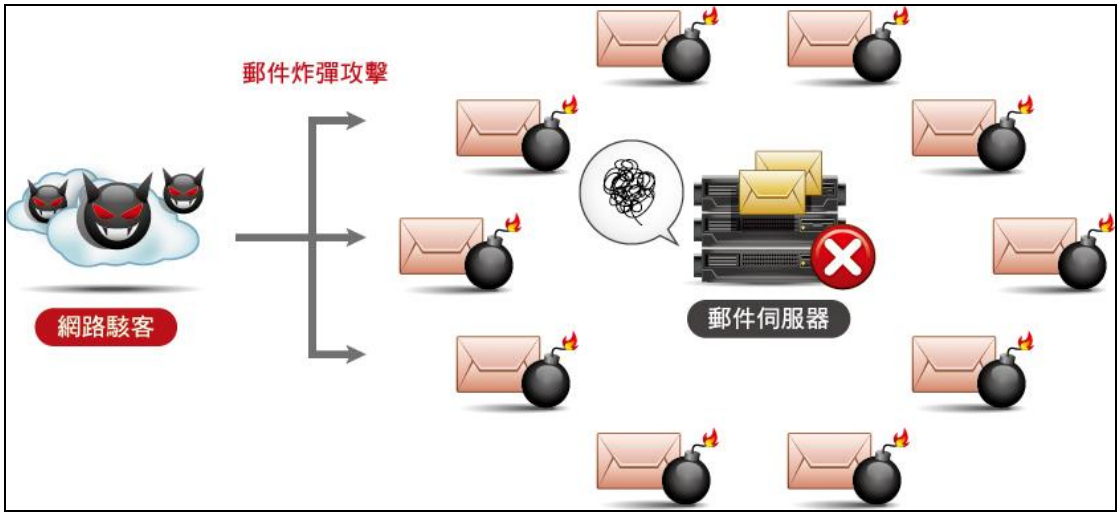


字點檔攻擊防禦設定

郵件炸彈攻擊

「郵件炸彈」也屬於一種 DoS 攻擊，指在短時間內連續寄發大量郵件給同一收信人，就像是利用炸彈對同一個地方進行大轟炸，因此稱為郵件炸彈攻擊。電子郵件炸彈與垃圾郵件看起來有些相似，但兩者的發送目的和造成危害大不相同。垃圾郵件是發件者在同一時間內將同一封電子郵件寄出給上萬個不同的用戶，目的是為了散播與宣傳特定資訊，不會對

收件端造成損害。電子郵件炸彈則是在短時間內大量寄信給同一收信人，目的就是為了癱瘓對方的郵件系統，因收件端信箱容量以及伺服器效能有限，同一時間收到大量的信件很容易就會超過負荷，造成收件端郵件系統無法正常使用。



郵件炸彈示意圖

MaiGates - *DoS 防禦介紹*

郵件炸彈是透過短時間內寄送大量信件來癱瘓收件端郵件系統，MailGates 郵件防護系統可設定在某段時間內同一 IP 允許寄出的最大訊息數量。

舉例來說，將 MailGates 設定成「在 10 秒內，允許寄出 2 次訊息」，就代表同一個 IP 10 秒內只能寄出兩封信，超過兩封信就會被系統自動拒絕，透過這樣的設定就可以避免系統遭受郵件炸彈攻擊。

郵件炸彈防禦設定

經過了這兩期電子報的說明，大家是不是對郵件安全的預防有了更深的瞭解呢？下期電子報我們將會繼續介紹，在郵件傳遞的過程中，該如何避免機密資料的外洩？對於郵件加密與驗證等相關技術都會有更詳細的解說，敬請期待！