文⊙網擎資訊產品企畫專員 周宇軒

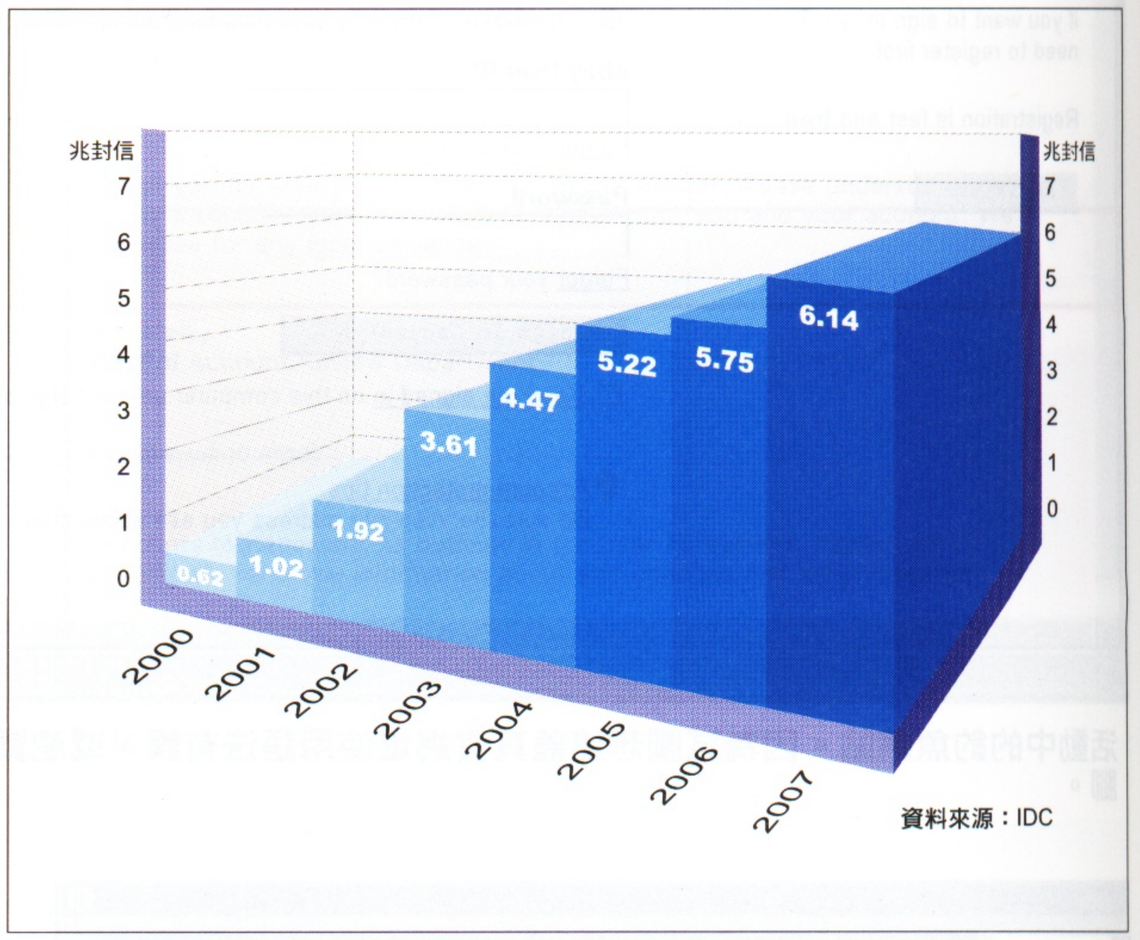
垃圾郵件過濾

廣告信，企業頻寬的頭號殺手

為什麼廣告信防制系統明明已經阻擋了百分之七八十的廣告信，頻寬卻仍然被廣告信佔掉這麼多呢？

企業電子郵件飽受廣告信影響已經是眾所皆知的事實，在各個研究數據中，例如IDC公布的「2003至2007年全球電子郵件使用預估：垃圾郵件與及時傳訊侵蝕電子郵件根基」報告，2003年一整年全球送出的垃圾郵件就有3兆6100億封，到2007年將會成長到1.7倍，達6兆1400億封。在實際經營付費電子郵件服務的Openfind技術副總許志新也說明了廣告信成長的困擾，以Mail2000付費信箱，2005年垃圾信件比率佔全部信件以然高達80%～90%之譜，相較去年垃圾信件數量比例約佔50%的情況看來，成長驚人。

這麼多的廣告信在Internet流竄，企業最直接的感受就是信件傳輸速度變慢了，例如，很明顯的發現客戶的信件往往要延遲好一陣子才能收得到；除此之外，收信匣裡面多了一堆不請自來的電子郵件，每天上班的第一件事就是勾勾刪刪廣告信，才開始一天正常的工作。為了解決廣告信的問題，企業投資大筆的資訊預算在廣告信防制系統上，耗費了許多人力時間的成本，總算還給員工一個乾淨的收信匣，但是員工在收發信時卻感覺到速度還是一樣遲緩，企業的頻寬成本持續高居不下，甚至硬體投資也繼續增加。於是企業就會產生這樣的疑惑，不是已經建立廣告信防制系統了嗎？照理說廣告信應該會排除在系統之外了啊，怎麼電子郵件伺服器網路頻寬與相關之硬體支出還是依然持續增加呢？



SMTP收發信流程簡介

為了解答這個疑惑，我們先簡單說明一下SMTP收發信件的流程。當一封電子郵件傳送到伺服器的時候，整個SMTP收發信件流程可以大致分成兩個階段：

1. SMTP連線階段（Mail Envelope）

這是郵件伺服器收信的第一道程序。郵件伺服器會先得到SMTP連線來源IP、EHLO網域名稱、Mail From（寄件人）以及Rcpt to（收件人）。這些資訊可以歸類成所謂的Mail Envelope，所佔的頻寬相當少，最多就是數十個Bytes而已，但已足夠提供廣告信防制系統進行第一層的過濾了。

2. 信件內文接收階段（Mail Body）

接下來的程序就是信件內文的接收，這部分就是信件實際的主體，包括了標題、本文、附檔等相關資料。這些資料是信件真正佔用頻寬的元兇，因為我們在閱讀信件時看到的文字、圖片、附檔、連結等等所有的相關資料，都是在這個階段接收進來的。

廣告信的種類與手法相當多，但追根究底仍是一種電子郵件，也都是建構在SMTP收發信通訊協定上的。因此所有廣告信防制的作法，也都跟SMTP收發信流程脫離不了關係。

除了擋廣告信、更要節省頻寬

對於SMTP收發信件的流程有了簡單的認知之後，我們再回頭想想看，為什麼廣告信防制系統明明已經阻擋了百分之七八十的廣告信，頻寬卻仍然被廣告信佔掉這麼多呢？有概念的讀者應該已經想到問題的癥結了。如果廣告信防制系統是在SMTP收信流程全部完成之

後，亦即將信件全部收入廣告信防制系統，才能開始並完成廣告信的判斷比對，那麼這個系統對於頻寬的節省並沒有實際的助益，因為在這個時候一封電子郵件已經全部完成傳送，進入到企業網路當中了。甚至許多企業也會發現，因為大量信件進入廣告信防制系統，在系統的硬體規格上，也需要較高等級的配備，這些都是企業成本的支出。

如果希望導入的廣告信防制系統除了過濾廣告信之外，能夠節省昂貴的頻寬與處理大量信件所耗費的高規格硬體成本，最好的方式就是在SMTP收發信件流程中的SMTP連線階段，就將判斷出的廣告信並直接排除在系統外，而不是等到整封信件都收下來再執行貝氏過濾、標題及網址過濾等內容比對相關機制，如此可以節省系統資源，讓廣告信處理流程能夠更加快速完成，有效提升電子郵件系統整體運作效能。

系統可以作的比想像中的多很多

或許有人會質疑，光是憑Mail Envelope得到的少量資訊，怎麼能斷定這封信是廣告信呢？事實上，在這個階段中得到的資訊雖然不多，但大多十分重要，某些資訊例如IP、Rcpt to收件人是無法偽造的，因此，這些資訊對於廣告信防制而言是相當有用的。以Openfind MailGates郵件防護系統來說，光是SMTP 來源IP就有系統黑白名單、RBL及時黑名單（Real-time Blocking List）、單一IP來源連線頻率限制，Dynamic IP等等過濾方式可以應用；另外，得到Rcpt to 欄位資料之後，就能採用使用者自定的各類黑白名單進行過濾。如果能夠妥善掌握這些重要的連線資訊，就能在廣告信進入企業網路之前直接排除，讓廣告信防制的效果最佳化。

根據筆者在企業客戶線上實機上統計出的數據，在一般的情況下，廣告信防制系統在SMTP第一階段可以判斷出約25%左右的廣告信。換句話說，如果在這個階段就直接將廣告信排除掉，可以替企業節省四分之一的頻寬！在某些大量SMTP連線的情況下，甚至可以達到75%的攔截率，幫企業節省四分之三的頻寬。

掌握SMTP關鍵，提供企業最佳效益

在SMTP信封接收階段就直接將廣告信排除的作法，對於頻寬成本的節省確實可以帶來相當的助益，但在實作上往往會遭遇到一些困難，我們可以分成技術面以及架構面兩方面來看：

技術面的困難

想在SMTP信封接收階段就開始進行廣告信的過濾，必須對SMTP收發信程式有相當程度的掌握。很多廣告信防制廠商在進行系統研發時，都是直接以開放原始碼如Sandmail、Qmail等等電子郵件系統為收發信件的核心，再附加上相關的廣告信過濾功能。如果對於系統SMTP收發信程式的了解不夠完全，就很難將廣告信過濾的功能深入整合到SMTP底層，讓第一階段判斷出的廣告信能夠直接排除在系統之外。

架構面的困難

有些廣告信防制軟體囿於系統架構方面的限制，就無法做到在第一階段排除廣告信的效果。例如著名的免費擋廣告信軟體SpamAssassin，就一定得等到整封電子郵件完全接收下來之後，才能根據內建的多條規則完成判斷。此外，架構的問題也可能是發生在MTA（Mail Transfer Agent）的信件收發流程上。有些MTA收信的方式就是將整封信直接收取下來，之後才讓整合的廣告信防制軟體進行判斷。若選擇與這樣的MTA整合，較高的頻寬成本當然是免不了的。

因此判斷一個廣告信防制系統，可以考慮一下該公司或產品是否可以掌握比較核心的電子郵件傳輸技術，有助於協助企業確實可以將廣告信阻絕於企業之外。

結論

如果廣告信防制系統能夠帶給企業的助益，單單只是判斷收進來的信件是否為廣告信的話，那未免太過狹隘。以企業的角度來看，花費了大量的金錢、人力與時間成本在廣告信防制系統上，當然會希望發揮的功效越多越好。因此，企業在進行廣告信防制系統導入評估時，除了關心攔截率與誤判率的高低之外，更應該額外考量導入的系統是否能有效幫企業降低頻寬成本。擋廣告信別只作一半，掌握SMTP行為，善用SMTP 獲得的重要資訊，廣告信防制機制，可以做的不只是將信件隔離或是加上特殊標題，如果可以將廣告信拒絕於企業大門之外，其效益才是最大化。