郵件安全趨勢介紹

Openfind 研發副總 翁嘉頎

隨著垃圾郵件的氾濫，如何有效的阻擋垃圾郵件以及降低誤判比例一直是最近幾年各大 anti-spam 產品的首要目標。包括灰名單 (grey-list) 的配置，包括去年年底吵得沸沸揚揚的反退信攻擊，甚至包括釣魚信件、帳號盜用都已經是各公司需要正視的問題。在這篇文章中 Openfind 將介紹一些近一兩年流行的概念，提供各企業尋求最佳的防禦之道。

首先介紹灰名單的概念。由於 spammer 技術越來越高超可以不斷的修改 source IP 甚至是郵件內容，傳統的黑名單攔截方式往往無法有效的對付，導致龐大垃圾信仍然可以穿透 anti-spam 系統進入員工信箱。灰名單一開始主要的想法是先把不認識的 source IP 所寄送的信件退回並留下記錄，由於 spammer 的系統 (不論是僵屍電腦、單機發信軟體、被 hack 當作 relay 的 mail server、中木馬的電腦) 並沒有耐性去做重新發送的動作，當 spammer 誤認為收信端的 mail server 有問題收不到，自然會跳過繼續去攻擊下個目標。而正常的 mail server 收到退信之後過一陣子會做自動重送的動作，我們在第二次接到這封重送的信件時，才放它通行送到後端的 mail server 中，並且可以將這個 source IP 放入白名單中 cache 一陣子，至少證明對方這台 mail server 是正常的，而且未來一段時間內應該也是可靠的。

當然灰名單要付出的代價就是效率問題。首先很多信件會被先假裝退信然後才能正常收進來，收信的速度一定會變慢，同時 anti-spam server 的工作量也會增加不少。有沒有更聰明的灰名單呢？Openfind 目前採用的就是聰明的灰名單過濾法，首先歸納出垃圾信的規則，一封從不明來源發出的信件會先去核對這些規則，當符合部分幾條規則後才啟用灰名單機制，其他沒有垃圾信嫌疑的信件可以直接放行。除了可以大幅度提升效率，也不會有太多的誤判發生。

再來介紹去年年底比較出名的反退信攻擊。退信攻擊主要發生在 spammer 偽造寄信來源，A 偽裝 C 寄信給 B，由於 B 系統並沒有這個使用者所以直接退信，而且會把這些信件都退給 C，導致 C 的負荷大幅度增加，這就是所謂的退信

攻擊。而防止退信攻擊的標準做法是在 mail server 經過 anti-spam 系統發信出去的時候加入一個特殊的簽章，當 anti-spam 收到退信馬上檢查這個簽章是否存在，簽章不存在就表示這封信件是別人偽造而非經過正式管道發送，如此 anti-spam 系統就可以有效的把這種退信攻擊予以攔截。

黑色蜘蛛人偽裝寄信

收信者找不到產生退信

正牌蜘蛛人遭到退信攻擊

利用反退信攻擊機制有效阻擋

最後要介紹的是學習型的貝式過濾。由於各個產業有自己的生態，一封內容包含威而鋼的信件在大部分公司都是垃圾信，但是在藥廠卻是正常信件。一封充滿了光碟資訊的信件在大部分公司都是垃圾信，但是在傳播業卻會是正常信件。跟防毒軟體不同，防毒軟體判斷是病毒就是病毒，不需要針對每個客戶的狀況做調整。但是一個好的 anti-spam kernel 必須能夠快速的學習並適應客戶的環境。由於 Openfind 擁有多個過濾核心，新版本的貝式過濾引擎能在剛開始安裝的前期處於自動學習階段，待適應使用者環境之後才開始正式發揮功效，如此可以更有效的貼近客戶環境避免誤判還有漏判。

有了灰名單的機制可以讓垃圾郵件大幅度下降，聰明的灰名單更可以提升整體效率；配上反退信攻擊更有效的保護內部；再加上學習型的貝式過濾以符合自己公司內部的需要。當可讓自己公司的郵件安全更上層樓而且效果顯著。