Fast Flux 攻擊手法簡介

一、 攻擊概述：

Fast Flux 基本上是 load-balancing 的新花樣。他是在 DNS Resource Record(RR)中將 TTL(Time To Live)設定的非常短，並以循序(Round-robin)的方式於一群 IP 中做替換，而這群 IP 則扮演了流量導向(Proxy)的角色，而通常這群 IP 便是一堆受到感染的 Bot 機器（通常是家庭電腦）。這些電腦不斷地輪流改變它們的 DNS 紀錄的目的是以避免被研究者、ISPs 或執法單位查獲。此技術使得基於 IP 封鎖清單的方法在預防攻擊上變得英雄無用武之地。也因為不管合法還是非法的 Fast Flux 持有一些相同的功能，如短 TTL 和擁有大量的 IP，因此很難區分它們。

二、 攻擊平台：

由於該技術是讓有心人士所提供含有惡意程式碼的頁面或網站不斷地輪流改變它們的 DNS 紀錄使其無法被封鎖，因此除非有辦法將該 SERVER 的所有 IP 一次封鎖，否則任何平台都有可能因為進入含有惡意程式碼的頁面或網站而受到攻擊。

三、 攻擊手法介紹：

Fast Flux 從 2006 年出現至今，已成為網址名稱管理單位一個頭痛的問題，除了會影響網址名稱解析服務的運作之外，更讓殭屍網路變得難以偵測，惡意人士甚至把殭屍網路變成一種出租服務，只要願意付出一些費用，就可以利用它來達到非法目的，更讓整個犯罪行為就像船過水無痕一樣難以追查。

錢騾時常在涉及欺詐行為的轉讓或撤回資金作為中間人。例如，罪犯再竊取他人銀行帳戶裡的錢以後，將金錢轉移到錢騾的銀行賬戶。而錢騾在抽取傭金之後會再協助罪犯將剩餘的款項運送至他們指定的位置，很有可能是在同的國家。然而錢騾並不知道他們參與了洗錢計劃，他們可能會認為他們正在為一個合法的公司執行正當程序。

也有針對流行的社交網站，MySpace 所進行的釣魚攻擊。攻擊者創建一個假的釣魚網站 login.mylspacee.com。而這個假網站看上去就像是真正的 MySpace 網站，無一不同，因此便可欺騙使用者登入此假網站，進而竊取該 MySpace 用戶的身份驗證憑據。而為了使其更難被安全專業人員關閉，無論是 NS 還是 A DNS 記錄都在不斷地變化。

四、 實際事件：

Warezov/Stration:

基於這些惡意代碼變種構建的網路提供了一個用於發送大量垃圾郵件的健壯平台。它們在發送垃圾方面表現是很成功的，並且採用先進的技術，比如不停的自動生成惡意代碼變種以應對基於特徵碼的反病毒技術。被感染的主機定期下載這些更新的軟件，目的是為了延長系統被清除和隔離的時間。這些升級後的軟件必須上傳到網站上，如果升級網站的公網 IP 地址仍然是靜態的話，則能容易被關閉。最近，一種偽隨機域名自動產生的策略被用來保護這樣的下載網站。從 2007 年 5 月開始，在這些發送垃圾郵件行為後面的犯罪組織轉向 Fast Flux 服務網絡模型。這些組織現在通過 Fast Flux 服務網絡部署他們的 DNS 服務和惡意代碼下載網站，並且在他們的犯罪努力下似乎總是成功的。

Storm:

Warezov/Stration 的最大競爭對手，也許是操縱基於家庭用戶的 Storm/Peacomm/Peed 惡意代碼變種構建大規模垃圾郵件發送網路的犯罪組織。他們採用基於 UDP 協定的 P2P 模型實現殭屍網絡的命令和控制。這是操作大規模分佈式網絡的一個非常靈活高效的方式，如果能克服節點列表維護的複雜性和時間開銷的最小化。他們也採用創新技術來應對反垃圾郵件方案，比如在代理節點終端自身生成基於圖像的垃圾郵件，而不是簡單的依賴於模板。這些圖像採取隨機方式生成，以應對在有些反垃圾郵件產品中採用的 OCR（目標特徵識別）技術，並且是在垃圾郵件發送方案中最普遍用於增加欺騙性的技術。在 2007 年 6 月這個組織被發現時正試圖改進他們的 P2P 網絡用於支持 Fast Flux 方式的網絡。這對垃圾郵件發送軟件來說是重大改進，需要進行進一步的跟踪和研究。

五、 檢測方法：

在台灣科技大學資通安全研究與教學中心的網路應用安全知識庫網站中也有另外提出兩個方法，第一個方法是叫做 SSFD : Spatial Snapshot Fast-flux Detection system，他利用了 A Record 及 NS Record 所對應的 IP 位址去找出所其對應的地理座標資訊，不需要等待 TTL，就能即時的去對 FFSN（Fast Flux Service Network）做偵測；第二個則是叫做 FSD : Flux-Score based Detection，需要利用到 TTL 去查詢 A Record , NS Record 及 ASN 代碼，因要查詢兩次以上才能偵測 FFSN，所以需要可能要花許多時間在做查詢，但在延遲時間時，可能會造成更多受害主機的出現。

六、 防護方法：

在 Measuring and Detecting Fast-Flux Service Networks 這篇論文中有提到他們所提出的方法可以自動地找到 Fast Flux 的 Domain，進而產生一個 Domain 黑名單。有了這個黑名單後有許多好處，他可以交給有權限關閉 Domain 的單位，將這有問題的 Domain 關閉；或是將他交給 ISP 業者，請他們在資訊還沒到達用戶端時就逕行過濾；更可以在收 Email 時先檢查來源，若來源存在於黑名單上便直接刪除，進而達到保護使用者系統安全的訴求。

七、 參考資料：

1. http://www.securityfocus.com/news/11473
2. http://www.wretch.cc/blog/fsj/8106356
3. http://www.i-security.tw/topic/topic_sg.asp?id=159
4. http://whatis.techtarget.com/definition/fast-flux-DNS
5. http://hi.baidu.com/witholive/blog/item/1b01d335e38abe315bb5f52e.html
6. http://knowledge.twisc.ntust.edu.tw/doku.php?id=4%E7%94%A8%E6%88%B6%E7%AB%AF%E5%AE%89%E5%85%A8:4-3%E5%81%B5%E6%B8%AC%E6%96%B9%E6%B3%95%E8%88%87%E5%B7%A5%E5%85%B7:%E5%88%86%E6%9E%90%E6%96%B9%E6%B3%95:fast-flux%E7%B6%B2%E8%B7%AF%E6%9C%8D%E5%8B%99%E5%8D%B3%E6%99%82%E5%81%B5%E6%B8%AC%E5%BB%BA%E7%AB%8B%E5%9C%A8%E7%A9%BA%E9%96%93%E6%A9%9F%E5%99%A8
7. http://honeyblog.org/junkyard/paper/fastflux-ndss08.pdf
8. http://www.honeynet.org/papers/ff/
9. http://wenku.baidu.com/view/8010f6eeaeaad1f346933fc6.html