Third-Party Mail Relay - An Email Threat

SANS GIAC Level One

Terri Kring
IS Security Officer
Our Lady of the Lake Regional Medical Center
5000 Hennessy Blvd
Baton Rouge, Louisiana 70810

Tkring@ololrmc.com

September 4, 2000

Third-Party Mail Relay - An Email Threat

This document is written for the email administrator who received notification from MAPS stating that his/her email server has been blacklisted for allowing Third-Party Mail Relay. Over the next few pages, I will explain what Third-Party Mail Relay is, who is MAPS, how you get listed with MAPS and how to get your site removed from MAPS.

What is Third-Party Mail Relay?

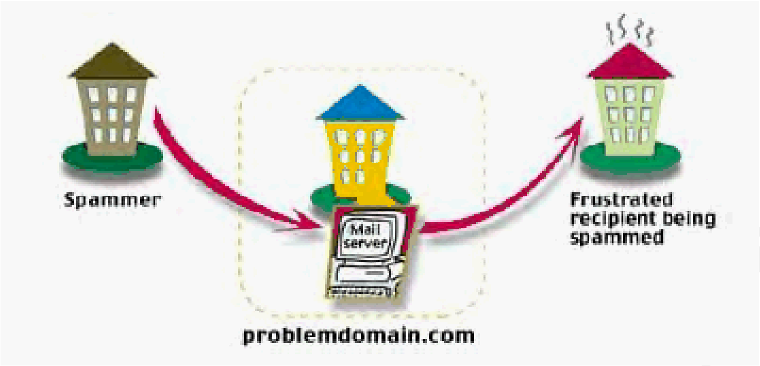
Third-Party Mail Relay, a.k.a. open relay, "occurs whenever a mail server processes a message where neither the originator or the receiver is a local user." [1] This practice was the norm in the early days of the Internet before we had sophisticated DNS databases. However, with today's Internet, the service is no longer needed. Unfortunately, many email administrators have not turned the service off. Therefore, Spammers are taking advantage of this vulnerability and flooding millions of mailboxes with unwanted, unsolicited emails.

When Spammers first started, they used to send thousands of emails from their own IP address. However, as email administrators became smarter and started blocking email from their sites, Spammers had to find other methods of sending their junk email. Third-Party Mail Relay was considered an easy way to accomplish this with little or no cost to the Spammer.

Consider the following: Let's say that you want to send an email to 1,000,000 people; however, your PC is not very powerful. You will need to connect to 1,000,000 mailboxes to send your 1,000,000 emails. This could take you many days. However, if you can connect with a high-powered mail host with high-speed access, you can push through hundreds of more mail in less time. Using Third-Party Mail Relay, you would only have to connect to 1,000 mailboxes to push your email to the 1,000,000 recipients 1,000 at a time. This saves the Spammer both computer power and bandwidth. [2] Why should the Spammer pay for expensive hardware and networks when they can steal it.

How does Third-Party Mail Relay work?

You have a Spammer who wants to send junk email. However, he knows that he can't send it directly from his IP address because too many sites have either blocked or filtered it. Through probing, he learns that your site accepts Third-Party Mail Relay. Therefore, he sends the junk email through your local domain, switches addresses so that it appears to originate from your local domain and sends the message to thousands of external users. [3] This usually works well for the Spammer until email administrators begin blocking your site and reporting your IP address to MAPS (Mail Abuse Prevention System) as a Spammer.



Who is MAPS (Mail Abuse Prevention System)?

MAPS, founded in 1998, is a member supported, not-for-profit organization whose mission is to eliminate Internet email abuse through various mail abuse prevention activities. Activities include education, maintenance of databases and management of complaints about electronic mail. The California organization consists of volunteers who are tired of the unwanted junk filling up their mailboxes.

A Spam victim can report the offending IP Address to MAPS.[4] MAPS will respond by testing the IP address to verify if the address is "Spam Friendly." If the IP address passes their tests, MAPS will place the IP Address in the MAPS RBL (Realtime Blackhole List) database, which is a list of networks that are known to be Spam Friendly. Once listed in the RBL, the site immediately becomes unavailable to the approximate 40% of the mail servers on the Internet.[5] MAPS also sends an email to the email administrator notifying him that his site has been listed and includes instructions on how to respond. Blacklisting is apparently very effective. According to ORBS, another validated database of open mail relays, approximately 75% of open relays are usually secured within 7 days of discovery.[6]

Why Should I Stop Third-Party Mail Relay?

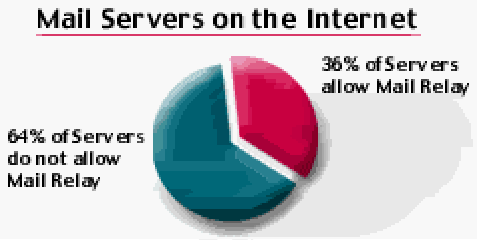
As an email administrator, you might wonder why you should bother closing Third-Party Mail Relay. It hasn't affected your network and you are already behind schedule on other projects. Here are five basic reasons why you should decide to close this hole:

1. Relays can cause a denial of service. When someone is using your resources without your permission they are stealing from you. Many times they can use so much of your computing resources that your system literally comes to a halt which causes your email server to become unavailable (a denial of service).

2. Recovering from this type of attack can be very expensive. Think of the time and energy required in order to recover from a crash. You will have to spend

countless unplanned hours getting your email server back on line. You will also have to explain to your users and management why their email was unavailable. It's easier to fix the problem before it occurs.

3. It's only a matter of time before your site is attacked. Spammers are using automated tools to locate servers with Third-Party Mail Relay capabilities. According to statistics, only 36% of servers allow Third-Party mail relay.[7] Therefore, once they find you they will continue to use your server until the open relay is closed.



Source: www.imc.org/ube-relay.html

4. Your server can be blacklisted which can cut your organization off from various services they will need.

5. It will soon be against the law.[8] There is a bill working its way through Congress that will amend the already successful junk fax law (47 USC Section 227) to include unsolicited commercial email. This amendment can be found at http://www.cauce.org/amendment.html.

What to Do if Your Site is Listed in the RBL

As soon as you learn that your site is listed in the RBL, you should contact MAPS by telephone (1-650-770-7080) or by email. MAPS will ask you for the affected IP Address and then direct you to their web site http://www.net-abuse.com. This site has a database search screen that allows you to search MAPS by an IP address. If your site is found, detailed information about the Spam and test results will be available in order to assist you with your research. They will also point you to various articles located on the Internet on how to secure your servers. If you are interested in learning more on your own, you may want to check out http://www.orbs.org/otherresources.html which lists fixes for various types of email servers.

Unfortunately, many people respond in anger to MAPS saying, "how dare they blacklist my email server". MAPS even has a page on how to sue them. However, they are doing all of us a favor when they list a site. If sites weren't blacklisted, with already overburden workloads, there would be little incentive for administrators to take corrective action and thus Spamming would be allowed to continue.

How to Get Off the MAPS RBL List

In the early days, unsecured servers were automatically removed from the RBL after 20 or 30 days. However, this is no longer practiced since open relays are still vulnerable to abuse. Now, once your site is listed in the RBL, it will remain listed until the email administrator notifies MAPS that the server is secured.

MAPS will run tests again to determine if the server is indeed secured. If the site does not allow Third-Party Mail Relay, the site is removed within a few minutes of the phone call or email. However, the site will remain in the RBL if it still processes Third-Party Mail Relay mail.

Subscribing to MAPS RBL

Now that you secured your server against open relay you should consider whether or not to subscribe to MAPS RBL to further protect it from Spammers. MAPS provides this service for free in order to enlist sites to help in the fight against Spam. By subscribing to MAPS you will be blocked from known open relay servers. However, remember that this could potentially block you from legitimate services. For more information, please see http://www.mail-abuse.com/rbl/usage.html. For a listing of ISPs that subscribe to MAPS, please see http://www.mail-abuse.com/rbl/participants.html.

Summary

No one likes to be spammed. Our critical resources are already limited without having additional unwanted, unsolicited junk email using up our resources. As an email administrator, you have a responsibility to keep your sites free from mail abuse techniques. This can be anywhere from having strict policies that promote good email practices to disabling your Third-Party Mail Relay service. In the end, we all want the same thing ...open connectivity.

[1] Rosenthal, Chip;. "What is Third-Party Mail Relay?". 31 July 1997. URL: http://mail-abuse.org/tsi/ar-what.html (31 August 2000)
[2] Vixie, Paul; "MAPS RBL Rationale", 19 July 2000. URL:http://mail-abuse.org/rbl/rationale.html (31 August 2000)
[3] "What is Mail Relay". URL:http://menandmice.com/infobase/mennmys/vefsidur.nsf/index/6.2.2.1 (31 August 2000)
[4] "Reporting Abuse to the MAPS RBL Team", 18 June 2000. URL: http://www.mail-abuse.com/rbl/reporting.html (31 August 2000)
[5] "What is ORBS?", URL: http://www.orbs.org/whatisthis.html (31 August 2000)
[6] "What is ORBS?", URL: http://www.orbs.org/whatisthis.html (31 August 2000)
[7] Hoffman, Paul; "Allowing Relay in STMP: A series of Surveys"; 5 July 1999. URL: http : www.imc.org/ube-relay.html (31 August 2000)
[8] "The Email Abuse FAQ". URL: http://members.aol.com/emailfaq/emailfaq.html, Version 2.0 (31 August 2000)