ISPadmin

by Robert Haskins

Robert D. Haskins is currently employed by Renesys Corporation in Hanover, NH.

rhaskins@usenix.org

Recent Spam-Fighting Developments

Introduction

In this edition of ISPadmin, I will look at a wide range of recent developments in the fight against spam. The following topics are covered:

- DSPAM
- Sender Policy Framework (SPF) and related ideas
- Selective port 25 blocking
- "Filters That Fight Back"
- Being paid to spam
- The CAN-SPAM law (and Do Not Email registry)
- Recent spam-related prosecutions and lawsuits
- L.L. Bean and overstock.com anti-spyware cases

DSPAM

"DSPAM (as in De-Spam) is an extremely scalable, open-source statistical hybrid anti-spam filter," according to its Web site. They recently announced that the newest version (3.0) is nearing production release. This software is essentially a sophisticated statistical filter designed for high-volume mail systems. It is written in a compiled language (C), which makes it very scalable with low overhead. DSPAM uses a database back end for saving and tracking scores. Some of the benefits of the DSPAM approach over its competitors are:

- Speed/performance
- Scalability
- Low administrative overhead
- All major MTAs supported

However, it would be nice if DSPAM included support for some of the features in SpamAssassin, namely:

- Support for distributed blacklists (i.e., MAPS, SPAMHAUS)
- Support for distributed checksum networks (DCC and Vipul's Razor)

Nice as these would be, DSPAM as it currently exists is certainly very useful for anyone who needs a scalable, easy-to-use statistical analyzer for their mail infrastructure.

Sender Policy Framework (SPF)

Sender Policy Framework (formerly Sender Permitted From) has garnered a lot of press lately. SPF uses DNS records that indicate the hosts from which a mailserver should accept email for a given domain. For example, if an email envelope had the from address "bob@aol.com" but the actual SMTP server sending the message wasn't listed in AOL's SPF record, the receiving server would reject the message, presuming the header to be "faked." The larger the email-box hosting provider, the more helpful something like SPF is going to be.

AOL adopted the SPF protocol in December 2003. Microsoft's proposal (in its unfortunately named Caller ID for Email proposal/standard) has been merged with the SPF. Yahoo's DomainKeys standard (one of the proposals backed by Sendmail) is a similar approach, though more difficult to implement in the short term due to the need for signed keys. However, this is arguably more secure, as each message would be signed, thus improving the trustworthiness of email being sent using the DomainKeys protocol. Both Caller ID for Email and DomainKeys have been submitted to the IETF for adoption as a standard.

While anything that can be done to reduce the amount of spam is a good thing, the SPF protocol (and related solutions) suffers from a few shortcomings:

- Email forwarding is problematic.
- It doesn't do anything about the "spam zombie" problem.
- It binds email address owners closely to their providers.
- SPF is much more likely to be adopted by the large email-box hosting providers than smaller ones.

The real way to fix email is to replace RFC822 with a more secure protocol. Unfortunately, until there is a critical mass, this is unlikely to happen. As a result of not having a standard, we will have to rely on incremental approaches such as SPF.

Selective Port 25 Blocking

In June 2004, the large US-based cable-modem ISP Comcast began blocking SMTP (port 25) on customer cable modem connections that generate a large amount of traffic. This is an effort to block the many customer machines that have been turned into "spam zombies." Comcast should be commended for taking a bold step against spam.

Many ISPs have globally blocked port 25 on their networks for years. However, this type of global blocking can cause no end of headache for legitimate customers who host their own email server that connects to the Internet via the ISP's network connection. If they take the proper precautions (such as not being an open relay), there should be nothing wrong with hosting a mail server so long as the ISP's terms of service are not violated.

Selectively blocking port 25 on those customer connections who are most likely compromised and being actively used by spammers is a big step in the right direction. If every provider followed Comcast's lead, there would be a significant reduction in the amount of spam (at least until the spammers found the next method to use).

"Filters That Fight Back"

In his August 2003 essay, Paul Graham argues for using email-client–based filters that follow the links listed in spam messages and then pound the spammers' sites with HTTP requests. While this is a noble idea and would probably achieve the goal of putting (some of) the spammers out of business, it suffers from a number of shortcomings.

First of all, it would be easy to "joe job" someone if the plan was implemented widely enough. (A "joe job" occurs when an unsuspecting third party is listed as the From: address in a spam message and is inundated with complaints from email users who don't know better.) There would be nothing to stop a prankster (or anyone else, for that matter) from sending out a wide message that gets defined as spam, causing the innocent party's Web site or other electronic presence to be interrupted.

Second, any spammer who didn't have a URL listed in their message would be immune. If the spammer used a telephone number to collect sales, there would be no easy way for filters to fight back.

Third, most providers would not take kindly to this type of network traffic on their networks. If the plan were implemented and successful, service providers would be the ones who would bear the brunt of the cost, by virtue of having to buy additional bandwidth on their networks to handle the increase in network load.

A company called VirtualMDA is offering to pay $1 per CPU hour of time to use your computer and network connection to send marketing messages on behalf of its clients.

Being Paid to Spam

A company called VirtualMDA is offering to pay $1 per CPU hour of time to use your computer and network connection to send marketing messages on behalf of its clients. This rate of pay is a big win for VirtualMDA, as it would take a huge number of messages before the user would get paid for his/her effort. In any case, before they ever saw a penny from VirtualMDA, the user's ISP would probably shut the the account off for violating the ISP's terms of service.

The CAN-SPAM Law

Disclaimer: I am not a lawyer!

The US CAN-SPAM Act went into effect on January 1, 2004, with much fanfare. Marketers are required to do the following under this law, according to the spamlaws.com site:

- Label their email
- Include opt-out instructions and the sender's physical address
- Refrain from using deceptive subject lines and false headers

Unfortunately, no standard label for bulk email was specified in the law, which makes this provision almost meaningless. The act also authorizes the FTC to establish a "Do Not Email" list. I believe the establishment of a "Do Not Email" list could result in much *more* spam reaching users' email boxes. The temptation for a confirmed email list such as this to be abused by spammers is simply too great, no matter what controls are placed on it.

Has this law had any effect on spam to date? Not much. Enforcement of the law is now only beginning. Time will tell, unfortunately. At best, laws are only part of the solution. At worst, they are part of the *problem*!

Recent Spam-Related Prosecutions and Lawsuits

On April 29, 2004, the FTC announced the first four prosecutions under the US CAN-SPAM law. At an average of one prosecution per month, there will be no effect on the average user. However, I believe the FTC and FBI are just beginning their work, and we will start to see much more of an impact once large numbers of spammers are brought to justice. Of course, a small percentage of the spammers are responsible for a large percentage of the spam.

In a May 24, 2004, Boston Globe article, Hiawatha Bray makes the point that phishing (scammers who pretend to be credit card companies in order to get a victim's credit card numbers and other personal information) will be good for the fight against spam. When the scammers, spammers, and spyware marketers target the companies with deep pockets and lots of market share (and money) to lose, only good things can come of it.

In fact, L.L. Bean and overstock.com both recently announced lawsuits against advertisers who used spyware in their marketing efforts. The marketing companies utilized spyware to generate pop-unders for the named advertisers when users (who had the spyware software installed on their computers) visited the L.L. Bean site. It is only a matter of time until the spammers market the wrong product and get sued by the product's trademark holders.

References

DSPAM: *http://www.nuclearelephant.com/projects/dspam/*

MAPS RBL: *http://www.mail-abuse.com/services/mds_rbl.html*

SPAMHAUS: *http://www.spamhaus.org/*

DCC: *http://www.rhyolite.com/anti-spam/dcc/*

Vipul's Razor: *http://razor.sourceforge.net/*

SPF: *http://spf.pobox.com/*

Yahoo DomainKeys: *http://antispam.yahoo.com/domainkeys*

AOL SPF: *http://postmaster.aol.com/info/spf.html*

MS Caller ID for Email: *http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx*

Comcast selective port-25 blocking: *http://zdnet.com.com/2100-1104_2-5230615.html*

"Filters that Fight Back": *http://www.paulgraham.com/ffb.html*

VirtualMDA: *http://www.virtualmda.com*

spamlaws.com CAN-SPAM: *http://www.spamlaws.com/federal/108s877.html*

First CAN-SPAM prosecutions: *http://www.cnn.com/2004/LAW/04/28/internet.spam.ap/index.html*

Boston Globe phishing article: *http://www.boston.com/business/globe/articles/2004/05/24/best_news_in_the_war_on_spam_phishing/*

L.L. Bean spyware lawsuit: *http://biz.yahoo.com/prnews/040517/nem044_1.html*