

Spam

by:
Billy Vierra

Billy Vierra

- Became Systems Administrator in 2002 for Rapid Grid
- Became Sr Systems Administrator in 2003 for Touch Support
- Began Working for cPanel in 2004 in PA
- Moved with cPanel to Houston in 2005

Topics Covered

- The problem
- How to prevent spammers from using my server
- How to track down a spammer if I get one on my server
- How to filter / block spam

The Problem

- In 2004 the California Legislature released a study that showed spam costs United States organizations more than \$10 billion.
- Spam is known to be more than just annoying to the end user as well, it is known to carry virus, trojans, and spyware.

The Problem (cont.)

- Spam causes additional load on mail servers
 - Extra network usage
 - Extra processing power needed
 - Additional Disk Space used to store the spam

Methods to Stop Spam

- Securing your server
- Blocking outgoing spam
- Filtering spam
- Tightening your SMTP server

Securing your Server

- Make sure that you do not have scripts that are vulnerable to spammers
- Verify that the user “nobody” cannot send out email
- Make sure that you are not an open relay

Watch the Scripts that your Users Install

- Keep an eye on the scripts that your users install
- Make sure they keep them up to date!

Verify that “nobody” Cannot Send Out Email

- Enable suExec
- Enable phpSuExec
- Prevent the user “nobody” from being able to send out email
- Adding X-source headers
- Include a list of POP before SMTP headers when relaying email

Enable suExec

- By default suExec is installed on all cPanel® servers
- suExec makes it so that all perl scripts (cgi/pl) run as the user on the account as opposed to the nobody user
- This is enabled in WHM™ under Service Configuration -> Enable/Disable SuExec

Enable phpSuExec

- phpSuExec makes it so that all PHP scripts run as the user on the account as opposed to the nobody user
- You can enable this under WHM -> Software -> Apache Update

Adding X-Source Headers

- You can track the origin of all email that is sent through your server by adding X-source headers
 - Enable this in WHM -> Server Configuration -> Tweak Settings

Adding X-PopBeforeSMTP Headers

- This causes all email that is relayed through your server using SMTP to show you who was authenticated via pop first
 - Enable in WHM -> Server Configuration -> Tweak Settings

What Exactly is an Open Relay?

- An open relay is a server that allows anyone to send an email through it.

How Do I Tell if I am an Open Relay?

- Well first remember that cPanel by default makes it so that you are not an open relay.
 - Custom configurations can cause you to open up Exim to become an open relay
- There are many websites available to test and see if your server is an open relay
 - <http://www.abuse.net/relay.html>

What if I Become an Open Relay?

- Start by removing the modifications that you have made to Exim

Searching for Spammers on your Servers

So you have locked down your server and you are sure that you are not an open relay however you are still getting abuse reports about spam coming from you server.

What do you do now?

Make Sure it was Sent from or Relayed from your Server!

- Check the headers
 - Is your hostname in there?
 - Is your IP in there?
 - Use the extra headers you enabled to help track down the spammer for you!

Lets Start with the Logs

- Lets start by knowing where Exim keeps it logs
 - Linux
 - /var/log/exim_mainlog
 - FreeBSD
 - /var/log/exim/mainlog

Enabling Extended Logging

- In the Exim Configuration add
 - `log_selector = +arguments + subject`

What Exactly Do Extended Logs Do for Me but Take Up Space?

- It makes looking through the logs easier
 - Take a look at the following example. You can see exactly where the email was sent from.
 - 2006-05-08 17:24
cwd=/home/user/public_html/phpBB 5 args: /usr/sbin/exim -Mc 19Z8vf-0023mp-E2

So the Spammer Did Not Send the Email from localhost

- In the following example the user was john@domain.com
 - 2006-05-22 17:32:21 1MV7FQ-03022-P1 <<
john@domain.com H=ispexample.com
([192.168.1.1]) [4.2.2.5] P=esmtpa
A=fixed_plain:john@domain.com S=231
id=ABCDEFGFG T="Buy me!"
 - The key here is
A=fixed_plain:john@domain.com



Spammers Also Connect to the Server via smtp from the Server

- The best way to check this is to run
 - `netstat -cen 2>/dev/null | grep 127.0.0.1:25`
 - Look for the number that will report after established
 - grep through `/etc/passwd` for this # to get the username

Blocking / Filtering Spam from Coming into my Server

- There are 2 major methods for helping prevent spam from getting to your users
 - Blocking spam using things such as Box Trapper and RBL's
 - Filtering spam using things such as spamassassin
- We will also go over some additional ACL's that will help you prevent spam

Why Would I Want to Block Spam?

- Blocking spam is one method used to prevent spam.
- When blocking spam you are less likely to get spam through however you are more likely to block ham (non spam) as spam.

Using BoxTrapper to Block Spam

- BoxTrapper is included with cPanel
- It uses the challenge response method to block email
 - All email that is not on the white list is held in a queue
 - All email held in the queue will get a response back asking the owner of the address to verify it
 - Once verified it will be released and the email address added to the white list
 - Email addresses with no real owners (such as registration emails) will get blocked.

Using RBL's to Block Spam

- An RBL is a Realtime Black List
 - An RBL is a list of IPs that are known to allegedly house spammers on them or be owned by someone who allegedly harbors spammers
 - All emails coming from these IP's are blocked immediately

Why Would I Want to Filter Spam?

- Filtering email is the other method used to help prevent spam
- When filtering email you are more likely to let spam get through however you are less likely to stop ham completely.

SpamAssassin

- SpamAssassin is a program used for e-mail filtering which is an e-mail spam filtering software based on content-matching rules
 - You can enable SpamAssassin in WHM -> Server Configuration -> Tweak Settings

SpamAssassin: Vipul's Razor

- A checksum-based, collaborative, distributed spam detection and filtering network. Spam is submitted by user contribution. Detection is done with statistical and randomized signatures that efficiently spot mutating spam content.
 - More information on this is available at <http://razor.sourceforge.net>

SpamAssassin: SARE

- SpamAssassin Rules Euporium (SARE)
 - These are several sets of SpamAssassin Rules that are not included with the default distribution. These rules are constantly updated, improved, generalized and cleansed as the spammers modify their devious method to send mail.
 - More information on this is available at:
<http://www.rulesemporium.com>

SpamAssassin: SARE - RulesDuJour

- A bash script is available to automatically download and install new rulesets as they become available.
 - More information on this is available at <http://exit0.us/index.php?pagename=RulesDuJour>

Additional ACLs

- Exim Dictionary Attack ACL
- Helo ACL
- Data ACL

Additional ACLs: Dictionary Attack ACL

- A dictionary attack is when a SMTP connection attempts to send email from a spam source to a random set of names on a particular domain. They hope with this that it will reach a legitimate user. This is a common method spammers use.
 - This ACL is available at <http://configserver.com/free/eximdeny.html>

Additional ACLs: HELO ACL

- When a remote system connects to your mail server, it is suppose to say “HELO domain.com”. A spammer might try to HELO with your own IP address. This ACL will prevent this.
 - This ACL is available at <http://vamos-wentworth.org/exim-tricks.html>

Additional ACLs: Data ACL

- A valid email address should always contain a message id. There is spamming software (and viruses too) that often do not. This ACL will refuse them.
 - This ACL is available at <http://vamos-wentworth.org/exim-tricks.html>

Additional ACLs

PLEASE REMEMBER

Please remember that when installing an ACL into Exim you could potentially break Exim or even worse make your server an open relay.

Please take the time to research what you add in and fully test it once its added in!

Questions / Answers

Ask Away!