Battle Against Spam Shifts to Containment

By *srlinuxx*
Created *16/04/2005 - 3:57pm*
Submitted by srlinuxx on Saturday 16th of April 2005 03:57:36 PM Filed under Security [1]

There's a new strategy in the spam battle: Call it containment. Filters for blocking junk e-mail from inboxes have improved to the point that doing much more will needlessly kill legitimate e-mail, said Carl Hutzler, America Online Inc.'s anti-spam coordinator. So e-mail gatekeepers are shifting gears.

Now they're getting more aggressive at keeping spam from leaving their systems in the first place.

EarthLink Inc., for instance, is phasing in a requirement that customers' mail programs submit passwords before it will send out their e-mail.

Like most Internet providers, EarthLink previously made sure only that a computer was associated with a legitimate account. Now that viruses can co-opt computers and use them to send spam, that's no longer secure enough.

So Earthlink sent out new software, made automated tools available for download and walked customers through manually changing their mail settings when they called tech support for other reasons. A year into the initiative, EarthLink has 80 percent of its customers converted.

"Any action can be a little daunting when you're trying to migrate millions of people," said Stephen Currie, EarthLink's director of communications products.

It also costs time and money - not insignificant considering that direct benefits don't necessarily go to EarthLink but to its competitors, whose customers might otherwise receive more spam.

But more than altruism was involved.

"If there's a lot of spam or abusive mail coming from a particular network, in the future you're going to see that e-mail having low rates of deliverability," Currie said.

In other words, other Internet service providers, or ISPs, might start blocking EarthLink e-mail if it doesn't adopt the outbound controls.

The pressure to improve outbound controls comes as viruses infect more and more home computers and convert them into spam-relayng "zombies."

These zombies allow spammers to pose as legitimate customers and get around blocks that Internet providers might have had in place.

Although antispam advocates say Internet providers can do more to stop spammers from signing up for accounts - sometimes fraudulently, but too often because they mean revenues and sales commissions - Hutzler blames zombies for 90 percent of the spam problem.

Traditional spam controls, the inbound filters, don't work as well with zombies because they can block mail from legitimate customers, too. Outbound controls can target specific zombies.

"The best place to stop spam is before it's sent," said John Reid, a volunteer with The Spamhaus Project anti-spam group. "If you can keep it in the bag, bottled up, that's where it's the least expensive."

Outbound controls aren't entirely new.

For years, anti-spam advocates have been pressuring Internet providers to configure mail servers so spammers can't use them to relay junk e-mail. The leading vendor of mail server software, Sendmail Inc., closed such relays by default in 1998, and most ISPs now have the newer software.

EarthLink and AOL also have long implemented a technique that forces customers to route e-mail through the providers' own mail servers, instead of sending messages directly to the Internet.

Other ISPs are starting to adopt it as well, giving them the ability to monitor outgoing mail, trace any problems to specific accounts and even block or place speed limits on e-mail that exceeds some hourly or daily threshold.

ISPs can also run the spam and virus filters on outbound mail.

And when users of Microsoft Corp.'s Hotmail try to send a large number of messages, they are prompted to type in random letters displayed on the screen. Presumably, spammers with automated tools wouldn't be able to do it.

If all ISPs were to implement outbound controls, spam wouldn't be such a headache.

But outbound measures are often difficult to justify because they don't directly pare down the junk in customers' inboxes as inbound filters do, said Anne Mitchell, who runs the Institute for Spam and Internet Public Policy, an antispam consultancy.

Mitchell said ISPs are businesses and "have to look at the bottom line and their profitability."

Besides implementation costs, outbound measures can hurt legitimate customers.

Businesses and some individuals might have a legitimate need to access third-party mail servers, and being forced to go through their providers' systems might cause their e-mail to be mistakenly tagged as spam by the recipient.

Anytime ISPs make changes, they will invariably discover a few customers who use their service in an unanticipated, but legitimate manner, said John Levine, co-author of "Fighting Spam for Dummies."

Martin Deen, manager of messaging engineering at Cox Communications Inc., likens outbound measures to vaccination. They may be good for the overall health of the Internet if all ISPs do it, Deen said, but individual ISPs take a personal risk.
ISPs sometimes grant exceptions for businesses and power users.

AOL has a few thousand customers, out of more than 28 million, who are exempt from caps on multiple mails.

Desert Express Internet Services, a small ISP serving California and Nevada, waived its restrictions for one of its business customers - but only if it agreed in writing to run spam filters on outgoing mail and meet other requirements.

Ultimately, ISPs may require customers with special needs to buy a premium service.

"We don't do that, (but) that would be a possibility certainly," EarthLink's Currie said. "EarthLink and other ISPs are just going to define their services, and certain things will be permitted and certain won't."

By ANICK JESDANUN, AP Internet Writer
Source [2].

Security

Source URL: http://www.tuxmachines.org/node/629

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=1&u=/ap/20050416/ap_on_hi_te/new_spam_battl