

Re: Rejecting viruses the Right Way[tm]

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2004-02/1769.html>

From: Kjetil Kjernsmo (*kjetil_at_kjernsmo.net*)

Date: 02/09/04

To: debian-user@lists.debian.org

Date: Mon, 9 Feb 2004 19:31:38 +0100

On Monday 09 February 2004 17:52, Steve Lamb wrote:

> *Derrick 'dman' Hudson wrote:*

>> *If a message is either rejected (during the SMTP dialog) or bounced*

>> *(after accepting and queueing the message) then the same innocent*

>> *third party receives some junk mail.[1] The difference is only in*

>> *which server is sending the bounce message.*

>

> *The presumption being, of course, that the other side is a real*

> *MTA and not the virus/worm itself. Rejecting is acceptable as the*

> *onus is on the other side on what to do. You're not generating the*

> *bounce. If it is a virus/worm then it isn't likely to generate a*

> *bounce. If it is an MTA then they had best get their act together*

> *and not propigate viruses.*

Right. This is, I think, the idea behind rejecting the message (both viruses and spam), is that it is not you who are generating the bounce, so unless the virus is programmed to deal with the rejection, nobody will get the bounce.

Same with spam, it is the actual spammer who will get the rejection. He may generate a bounce to whoever he has forged into the MAIL FROM:, but he has no reason to do so, has he? Also, he has to clean his lists now and then, otherwise, he would spam mostly dead addresses. So, one would think that he would use the rejection to clean the lists, but I can't see that happening.

So, basically, if gluck had rejected the message on RCPT TO: rather than send it over to master, a bounce message would presumably not have been generated by (in this case) 213.222.144.148.

But it raises the question, what if viruses are doing something to deal with a rejection, and does it with malice, could they use it to do bad things?

Best,

Kjetil

Debian-User: Re: Rejecting viruses the Right Way[tm]

--

Kjetil Kjernsmo
Astrophysicist/IT Consultant/Skeptic/Ski-orienteer/Orienteer/Mountaineer
kjetil@kjernsmo.net webmaster@skepsis.no editor@learn-orienteeing.org
Homepage: <http://www.kjetil.kjernsmo.net/> OpenPGP KeyID: 6A6A0BBC

--

To UNSUBSCRIBE, email to debian-user-request@lists.debian.org
with a subject of "unsubscribe". Trouble? Contact listmaster@lists.debian.org