

Re: Pesky virus

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2004-07/5364.html>

From: Scot L. Harris (webid_at_cfl.rr.com)

Date: 07/23/04

To: Fedora List <fedora-list@redhat.com>

Date: Fri, 23 Jul 2004 11:24:03 -0400

On Fri, 2004-07-23 at 11:14, Michael Sullivan wrote:

> *I've got a small problem. Last week I received in my
> non-espersunited.com email account an email from someone I don't know
> with an .exe file as an attachment. Naturally I assumed that this was a
> virus, and wrote back to the email address it was from informing them
> that they had a virus. I've received several similar emails on through
> the week, most were unique but all followed the same format: One line
> of text and then the attachment link, usually a .exe or a .zip file. I
> haven't opened any of them, but in the past couple of days I've begun
> seeing them in my espersunited.com email accounts. I wasn't too worried
> about it until this morning, when I received a message from another SMTP
> server saying that my mail was undeliverable to some person's email
> account. I looked at the message sent and it was indeed from me, but
> the message body held the same one line and the same EXE/ZIP file
> attachment as the ones I'd received from multiple sources. I use
> evolution as my email client. Could I be infected with this virus? I
> didn't think Linux was susceptible to virii - only hostile shell
> scripts. Is there a way I can test if I am infected, and if I am, is
> there a way to find the virus so that I can destroy it?*

Most likely you do not have a virus, mainly because most viruses are written for Windows platforms. But there are virus (or more properly trojan) like programs for linux, just not very many.

It is common practice for virus and spam programs to forge the from address on any messages sent out. They will use legitimate addresses and in some cases the systems receiving those messages will contact the forged from address telling them they are infected etc.

For the most part you can just ignore those messages.

Possibly because you wrote back to the sender they collected your email address and have used it to send out forged emails to others. They collect email addresses in many different ways.

However, to check your system you can run the program chkrootkit. This program performs a number of tests on your system looking for known

Fedora: Re: Pesky virus

rootkits and exploits.

You may also want to load tripwire on your system. It won't let you know if your system is currently compromised, but it will let you know when critical files get changed on your system. It is a little finicky to setup the first time but once it is in place it will report when config files get changed or libraries are modified or even when log files get truncated.

You may also want to look at spam filters such as spamassassin that can identify such emails and isolate them so you don't get them in your inbox.

--

Scot L. Harris
webid@cfl.rr.com

if it GLISTENS, gobble it!!

--

fedora-list mailing list
fedora-list@redhat.com

To unsubscribe: <http://www.redhat.com/mailman/listinfo/fedora-list>