

## Re: Swen.a virus?

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2003-10/3035.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-10/3035.html)

---

**From:** Deborah (*anonymous\_at\_discussions.microsoft.com*)

**Date:** 10/16/03

Date: Thu, 16 Oct 2003 07:23:44 -0700

I too, was receiving several of these screwy e-mails per day. Norton was detecting them as having virus attachments, and I decided to start blocking them by their e-mail address. That wasn't catching them, as each one has a different e-mail address. So I started applying rules to my Outlook e-mails received, and that has all but stopped these nasty virus laden e-mails. I'll probably have to start writing more rules when new names start up, but this has helped. You might want to try this.

>-----Original Message-----

>My understanding is that the Sven virus doesn't SEND to e-mail addresses that have been harvested off of newsgroups,

>although your e-mail address might appear in the FROM.

(I

>hate to be those people!) I think it sends TO e-mail

>addresses that it gets off of the computers it has

>infected. i.e., if your friend has your e-mail address

in

>his address book, and his computer gets infected by Sven,

>you can expect to get a virus-laden message from him (all

>though it won't appear to have come from him, it will

>appear to have come from some poor soul who had his e-mail

>address harvested -- that's where it uses the harvested

>addresses, not in the TO:, but in the FROM:).

>

>Either way, your advice about disguising your e-mail

>address is still valid and important, that's for sure!

>

>Unfortunately, this doesn't answer his original question.

>I don't know of any way to stop receiving these e-mails

>other than to install a filter to check for the key

>words "undelivered, undeliverable, and security." These

>keywords are in all of the infected messages and they are

>not words that people use in every day conversation. I  
>set this up at Yahoo and it works great.  
>  
>I think we will stop receiving these infected messages  
>after everyone who has the virus get's their darned  
>computers scanned for viruses. Personally, I thought of  
>sending a message to all of my friends who might have my  
e-  
>mail address asking them to scan their computers.  
>However, I decided that since I only receive a half dozen  
>messages per day it wasn't worth bugging them.  
>  
>Hope this helps.  
>  
>Mark  
>  
>>-----Original Message-----  
>>  
>>"Craig" <craig3740@SPAMMENOTmsn.com> wrote in message  
>>news:8572a42b.0310150655.1396b376@posting.google.com...  
>>> Is there any way of stopping these "microsoft wannabe  
>attachments"  
>>> containing the swen virus from reaching my server.I  
>receive around  
>>> 5-10 of them a day every time I get one I delete,  
>blacklist and bounce  
>>> them thanks to Mailwasher.Its just becoming annoying  
>now is there  
>>> anything I can do apart from changing my email address.  
>>>  
>>> Please Anyone  
>>>  
>>> Craig  
>>  
>>You need to stop posting to the newsgroups with a valid  
>email  
>>address. Look above to see how I changed yours.  
>>  
>>There are automated programs out there that check  
headers  
>&  
>>bodies of all newsgroup posts, looking for proper email  
>structure:  
>>  
>> you@xxxxxx.xxx  
>>  
>>When you get discovered, you become a valuable commodity  
>>to all the spammers out there, buying and selling your  
>valid  
>>e-mail address. Then there is W32.Swen-a@mm . That worm  
>>looks for your email address in the newsgroups - the

more

>it

>>finds you, the more you'll get those fake MS emails. I

>got a friend

>>who was getting 2-3 per SECOND! You've got to hide your  
>ID!

>>

>>I don't know if Google will let you do this but Outlook

>Express

>>does this easily. Now a new problem - accessing Google

>from

>>Outlook Express. I don't think you can do that, either.

>>

>>Start Outlook Express and set up the news server for the

>following

>>account:

>>

>>freenews.netfront.net (no log on PW/ACCT)

>>

>>That is a free news server (read only). When I want to

>reply to

>>a post, I simply change outbound server to my Giganews

>server.

>>

>>Ken

>>

>>P.S. More info about then Swen-a worm can be found at

>>

>> news:alt.comp.virus

>>

>>

>>

>>.

>>

>.

>