

How to get rid of new Sobig.F virus?

By Nowshade Kabir

How to get rid of new Sobig.F virus?

Nowshade Kabir
nowshade@rusbiz.com

Rusbiz E-zine <http://ezine.rusbiz.com/>

Title: How to get rid of new Sobig.F virus?

Description: What is Sobig.F virus? How it works? And how to protect yourself against it?

Keywords: Sobig.F,new virus,Rusbiz,e-mail,protecting against virus,antivirus,attached files,Sobig,sobig

adress: <http://ezine.rusbiz.com/newsletters/newsletter16.htm>

How to get rid of new Sobig.F virus?

by Nowshade Kabir, Rusbiz.com

As you know, this time the virus under the name Sobig.F has wreaked quite havoc! No doubt, many of us have suffered from this recent virus outbreak.

According to an online poll conducted by CNN: 32% of respondents were infected with this malicious virus. At the pick, each of every 17 emails contained sobig.F! Internet service provider AOL says it scanned 40.5 million emails and found the virus in more than half of them. Sobig accounted for 98 percent of all viruses found in these emails.

What is Sobig.F virus?

This is a worm type of virus. Which means it is an executable program that installs enhancement to your Windows operating system. The 'F' implies that it is the sixth of the family of Sobig viruses. The first one was launched in the beginning of this year. The latest attack was started on August 19.

According to some experts, Sobig.F was first posted to a porn Usenet group and spread from there. It is timed to deactivate itself on September 10. The pre-built deactivation mechanism

itself is a worrisome factor. Most experts think this means there are more to come!

How it works?

Sobig.F comes along with an email with subject headers like Your details, Thank you!, Re: Thank you!, Re: Details, Re: Re: My details, Re: Approved, Re: Your application, Re: Wicked screensaver or Re: That movie. The body of the message is quite short and usually contains either "See the attached file for details" or "Please see the attached file for details."

Once the file is opened, Sobig.F resends itself using a built-in mailing program to e-mail addresses from the infected computer. As a sender is address it shows one of the e-mails randomly selected from the computer's address book.

The worm was also supposed to attempt to retrieve an URL from a predetermined list of 20 master servers on a certain date and time. The content of that URL was to be downloaded and executed on the infected machines. Luckily those servers were identified right away and shut down.

How to protect yourself against it?

If your computer is infected or you have doubts, first thing you should do is: to check and clean up your computer from this virus. Although, it is set to deactivate on September 10, which means it will no longer multiply itself, however, left untouched, it might attempt to update itself, once the newer version of the virus comes out.

Suggestion One:

1. If you do not have latest version of anti-viruses installed, go to the Symantec's following page:
<http://www.symantec.com/avcenter/venc/data/w32.sobig.f@mm.html> ,
2. Down load the Sobig.F removal tool for completely free of charge.
3. Install and run it by strictly following the steps described on the page.

Suggestion Two:

Download the latest security patches for your version of Windows and install them.

Suggestion Three:

If you are using Microsoft Outlook, follow the steps below to stop

them appearing in your inbox:

- Open Outlook
- Click on "Tools" from main menu
- Choose Rules Wizard from the drop down menu
- On the page "Apply changes to this folder": Click on "New"
- Select "Start creating a rule from Templates"
- Choose "Move messages based on content"
- Click on "specific words" link from the box at the bottom
- A small window will appear, add each and every phrase scrupulously from the list below:

Re: Thank you!

Thank you!

Your details

Re: Details

Re: Re: My details

Re: Approved

Re: Your application

Re: Wicked screensaver

Re: That movie

And

your_document.pif

document_all.pif

thank_you.pif

your_details.pif

details.pif

document_9446.pif

application.pif

wicked_scr.scr

movie0045.pif

- Once finished click on "OK" to close the window.
- Click on the link "specified" at the same box
- Open a new folder by clicking on the "New" button under the name "Virus Spam"
- Click on "OK"
- Click on "Finish"
- From now on all emails with the above mentioned phrases and attachments will be moved to the "Virus Spam" folder.
- All you have to do is delete the emails, which will appear there.

A few more cautions:

Don't open any executable attachment in an email, unless you are hundred percent sure that this is a legitimate file that you have

been expecting.

Install an anti-virus program and update it on time, at the end, this might be the best possible solution to protect ourselves from these ugly online creatures!

About the author

Nowshade Kabir is the founder, primary developer and present CEO of Rusbiz.com (<http://www.rusbiz.com>). He has Ph. D. degree in Information Technology. Dr. Kabir has over 12 years of experience in International Trade and has worked as an advisor to several government projects. You can contact him at <mailto:nowshade@rusbiz.com>, <http://ezine.rusbiz.com/>

[Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.](#)

[Submit your article for reprint.](#)