CNN.com - SoBig.F breaks virus speed records

Friday, August 22, 2003 Posted: 0625 GMT (2:25 PM HKT)

SoBig.F is set to expire next month but until then will wreak more havoc.

SoBig.F is set to expire next month but until then will wreak more havoc.

Story Tools

VIDEO


The SoBig virus is the latest in a series of attacks on computers that are costing increasingly more time and money.

SoBig.F Alert

Be on the lookout for the following attachments:

application.pif
details.pif
document_9446.pif
document_all.pif
movie0045.pif
thank_you.pif
your_details.pif
your_document.pif
wicked_scr.scr

QUICKVOTE

Have you been hit by the SoBig worm?

Yes	
No	

(CNN) -- The SoBig.F computer virus -- which has already overwhelmed hundreds of thousands of computers worldwide -- has become the fastest spreading virus ever with experts warning the worst is yet to come.

Already the worm has caused an estimated $50 million of damage in the United States alone.

Among its casualties: It briefly brought freight and computer traffic in Washington, D.C. to a halt, grounded Air Canada and slowed down computer systems at many major companies such as advanced technology firm Lockheed Martin.

The sixth or "F" version of the SoBig infection disguises itself in e-mails which once opened scan a computer for e-mail addresses before sending scores of messages to the addresses it collected via its own inbuilt sending program.

The SoBig.F outbreak, first detected Monday, began 10 days after the Blaster worm (which itself infected an estimated 500,000 users) and has already beaten other infamous viruses such as LoveBug, Klez and Kournikova in terms of spread.

The first SoBig variant was released in January.

U.S.-based e-mail security group MessageLabs says the virus originated and is most prevalent in the United States.

"This is the most severe e-mail virus we've ever seen," MessageLabs' Josh White said.

"At its peak 1 out of 17 e-mails that we were processing was a copy of the SoBig.F virus. Certainly we haven't seen numbers like this before. It is spreading at a very fast rate and the volumes are high."

Internet service provider AOL (part of the AOL Time Warner group which includes CNN) says it scanned 40.5 million e-mails and found the virus in more than half. SoBig accounted for 98 percent of all viruses found.

The e-mail-borne worm arrives with various subject headers, such as: 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 short and usually contains either "See the attached file for details" or "Please see the attached file for details."

Fooled that the e-mail is legitimate, the user opens the e-mail and triggers the worm, which then goes hunting for addresses. The flood of messages it then sends are capable of succumbing other users' inboxes or computer systems by the sheer volume of e-mails.

Worrying sign

The virus also implements a background program that turns an infected computer into a relay system for further messages from the virus' creator.

This part of the virus has led many computer security experts to believe the virus was written to try and beat spam filters.

Experts are predicting that though it will soon be brought under control, the infection is likely to spike early next week as many people in Europe and the U.S. return to work from (northern hemisphere) summer holidays to awaiting e-mail inboxes.

However, the worm is set to deactivate September 10 and halt further propagation. This itself is a worrying sign.

"The SoBig virus writer's use of an inbuilt expiry date indicates he is committed to inventing new and improved versions," MessageLabs' chief technology officer Mark Sunner said.

"Each variant released so far has exceeded the previous one in growth and impact during the critical initial window of vulnerability."

-- *CNN Correspondent Bill Tucker contributed to this report.*
