

SOBIG.F VIRUS PROMISES "I'LL BE BACK"

By Karin Manning

SOBIG.F VIRUS PROMISES "I'LL BE BACK"

Karin Manning
karin@reprinrights4u.com

reprinrights4u.com <http://www.reprinrights4u.com>

"SOBIG.F" PROMISES – "I'LL BE BACK"

On 21 August 2003 Symantec Security Response upgraded the W32.SOBIG.F threat to a category 4.

It is the sixth version of this worm.

SOBIG.F follows a computer worm known as "Blaster," or "MSBlaster," which infected at least 500,000 computers all over the world only a week ago. The "Nachi" worm which is designed to protect pcs from "Blaster" caused its own havoc including infiltrating unclassified computers on the Navy-Marine intranet and the collapse of the check-in system of Air Canada.

Associated Press has stated that 1 in 17 emails sent around the world has been infected.

According to Paul Wood of MessageLabs it took anti-virus companies at least 12 hours to release updated software to combat the worm.

W32.Sobig.F@mm is, in fact, a worm, not a virus. This worm sends itself to every email address it finds in files with the following extensions:

.TXT
.WAB
.MHT
.HTML
.HTM
.HLP
.EML
.DBX

The "SOBIG" worm is found in emails in your inbox with the following subject headings:

RE: DETAILS
RE: THANK YOU!
RE: YOUR APPLICATION
RE: YOUR DETAILS
RE: DETAILS
RE: APPROVED
RE: THAT MOVIE
RE: WICKED SCREENSAVER

I have personally received emails with all of these subject headings on a daily basis. The body of the email simply refers you to an attached file. It is absolutely critical that you DO NOT open this attachment. It is this attachment that contains the "SOBIG" worm.

The "SOBIG" worm is attached to files with the following names:

Movie0045.pif
Your_document.pif
Thank_you.pif
Document_all.pif
Details.pif
Document_9446.pif
Wicked_scr.scr
Application.pif

The last day on which the "SOBIG" worm will spread is 9 September, 2003. Although this means email address collection and mass-mailing will stop at that date a computer infected with the worm will still try to download updates from master servers even after this date.

The worm affects Windows 95, 98, Me, Nt, 2000 and XP but leaves Unix, OS/2, Windows 3.x, Macintosh and Linux unaffected.

Thankfully Symantec Security Response has created a removal tool which is free to clean an infected computer. To access Symantec's free removal tool visit:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.html>

For a free virus scan visit:

<http://www.stop-sign.com>

This past month's computer attacks follows a historical trend – virus activity surges when college students have free time on their hands in the summer.

However, there is a suspicion that these kind of virus attacks

may be driven by profit motives because worms such as SOBIG.F place a "trojan horse" on infected drives of unsuspecting pc owners which allows spammers to quickly distribute millions of unsolicited emails around the world.

Poorly designed software is declared the main cause of increased virus activity by computer designers as software is often distributed without appropriate amounts of testing.

Microsoft last year announced its intention to slow down software development so that software can be made more safe from infiltration.

Regardless of the cause, here is the reality:

Sobig.A was found on January 9 2003 with no expiry.

Sobig.B was found on May 18, expiring May 31 2003.

Sobig.C was found on May 31, expiring on June 8 2003.

Sobig.D was found on June 18, expiring on July 2 2003.

Sobig.E was found on June 25, expiring on July 14 2003.

Sobig.F was found on August 19, to expire 10 September 2003.

The spread of the SOBIG.F worm is being hailed the fastest ever.

History, therefore, tells us that Sobig.G is, in fact, just around the corner, faster and stronger than each of its predecessors.

As Sobig.F nears its expiry on 10 September 2003 I can almost envisage its evil grin as it declares, "I'll be back."

Copyright 2003. Karin Manning. All Rights Reserved. Karin Manning is the webmistress of <http://www.reprinrights4u.com> and the publisher of Net Wealth, filled with up to the minute tips and techniques for growing your business online. To subscribe visit <http://www.reprinrights4u.com> and fill in the Newsletter Popunder on entry.

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

[Submit your article for reprint.](#)