Sobig a Fool as That?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

It never ends. Automated social engineering by e-mail-enabled worms is a curse that is approaching unsolicited e-mail in its irritation quotient. These worms, like human spammers, generate misleading subject lines to trick victims into opening messages – and in particular, opening the attachments that contain malicious code and thus executing the code.

In the last few days, I’ve been receiving dozens of copies of two particular variants of W32.Sobig.E@mm worm-bearing messages. One type includes the subject line “Re: Application” and the other is “Re: Movie.” It happens that I run a graduate program that is currently receiving lots of correspondence about applications in our pipeline and that one of my hobbies is movies, so you can understand my irritation with these bogus messages. Other topics reported by antivirus companies in versions of the Sobig worm-bearing e-mail messages include

004448554.pif
Application.pif
Applications.pif
movie.pif
new document.pif
Re: document.pif
Re: Documents
Re: Movies
Re: Re: Application ref 003644
Re: Re: Document
Re: ScRe:ensaver
Re: Submitted
Referer.pif
Screensaver.scr
submited.pif
Your application

The text in the messages I have received has uniformly been “Please see the attached zip file for details.” However, other messages have been noted “in the wild.”

The attachment may be called

Application.zip (contains Application.pif)
Document.zip (contains Document.pif)
Movie.zip (contains Movie.pif)
Screensaver.zip (contains Sky.world.scr)
Your_details.zip (contains Details.pif)

However, the files I have received terminated in the double suffix “.zip.htm” which is a giveaway that something funny is going on. Other second-suffixes for the worm-infected attachments include
thus producing, for example, “Application.zip.txt” or “Movie.zip.html” and so on.

Once opened, the active content of the ZIP file can infect the Windows operating system and mail itself to addresses found in various e-mail address books using forged e-mail headers.

The current version has a termination date of Bastille Day 2003 (14 July); however, one can be sure that some creepy wannabe will alter the code to extend the lifetime of this nuisance.

So be sure all your antivirus products are dutifully updating themselves automatically; tell your users to be on guard against these wretched messages; and warn them not to be, ah, sobig a fool as to actually open any attachment from a stranger or any unexpected attachment supposedly from a friend.

* * *

Related links:

Symantec Antivirus Research Center Alert: W32.Sobig.E@mm
http://www.sarc.com/avcenter/venc/data/w32.sobig.e@mm.html

E-securityplanet writers (June 26, 2003). Virus alert: Sobig.E threat level upgraded
http://www.esecurityplanet.com/alerts/article.php/2228511

Vamosi, R. (June 26, 2003). Help & HowTo: Sobig.e worm. New worm gives us yet another reason not to open attached e-mail files.
http://news.zdnet.co.uk/story/0,,t278-s2136630,00.html

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003. See
http://www.dmcyul.com for details in English _et en français_.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.