

## Virus Warning, Again!

By the time this article goes to press it will be old news that there was a new e-mail virus last week called the “Mydoom” virus officially known as the [W32.novarg.A@mm](mailto:W32.novarg.A@mm) mass mailing worm. This worm was released Monday January 26<sup>th</sup> and by Tuesday morning I had received eight infected e-mails with this virus in it. I received many calls Tuesday concerning this virus and that’s when I realized I needed to write an update to the virus article I wrote a couple of months ago.

This particular virus, actually a worm comes disguised as a technical e-mail. The authors of this worm decided to use a technical slant to trick users into activating the worm. The subject of the e-mail may have been “Hi”, “Mail Delivery System”, or “Mail Transaction Failed”. The text of the message most commonly states that the “mail transaction failed” or it may even say something about the “message cannot be represented in 7 bit ASCII encoding”. Attached to the e-mail is a file named “document”, “readme”, “text”, “file”, “message”, or a half dozen other titles? The attachment will always end in “.pif”, “.scr”, “.exe”, “.cmd”, “.bat” or “.zip”.

The user believes that the e-mail was returned because it was undeliverable. The user then opens the attachment to determine who the message was originally sent too. Of course we now know that by clicking on the attachment the worm is activated. Once the worm is activated the worm has the ability to send out 100 infected e-mails to people in your address book in just 30 seconds. This type of mass mailing can slow company networks and the Internet down to a snails pace. One of the anti-virus companies found code in the worm that indicated that all infected machines should attack the SCO Group Inc’s web site on February 1<sup>st</sup>. SCO Group has been in the news because they have been threatening to sue Linux users. If you do receive a suspicious e-mail with the above text, simply play it safe and delete the e-mail without opening the attachment.

An important attribute about this worm and the main reason I choose to write this article concerns the use of Kazaa as a way to spread itself. I have been telling my customers for over a year that file-swapping services such as Kazaa and Imesh are awful for your computer because they make your system vulnerable to both spy ware and virus. This particular worm copies itself into the share folder of Kazaa as “winamp5”, “icq2204-final”, “office\_crack” or any number of other popular download software. Any unsuspecting person can download one of these files only to be infected with this unscrupulous virus.

So just remember the next time your planning on downloading some new popular song for “FREE” using one of those file swapping services you may actually find out that professional virus removal costs a lot more then a music CD. I learned a long time ago that there is no such thing as a free lunch. Sooner or later downloading “Free” music or software will end up costing you in some way.

Well that wraps up the lecture, if you have any questions concerning your computer or have an interest you would like to see me write about in this column, please phone or e-mail Thomas Hill at [ComputerDepotOnline@att.net](mailto:ComputerDepotOnline@att.net).