Subject: Misconceptions
Posted by HeXetic on Fri, 30 Jan 2004 13:59:04 GMT
View Forum Message <> Reply to Message

A couple of misconceptions to clear up.

- MyDoom "works" because it looks like a ZIP file - not the more recognizeable EXE or BAT or VBS or COM or SCR etc. files - to the unfortunate shmuck who gets it in the mail. My own dad double-clicked on it even though I've told him in the past not to do stuff like that (happily, he doesn't have administrative privileges on the computer, so the virus couldn't actually do anything).

- The "from" address in pretty much all virus and spam e-mails is forged. If the mail says it's "FROM: hexetic@planetcnc.com" it was probably sent from a 286 in the mountains of Tibet. Various schemes are used to come up with the fake return address; sometimes it's random, sometimes the viruses use previously harvested e-mail addresses. It's all just to make the virus look a little more real and *also* create more havoc by generating throusands of "bounce" messages (sent by the mailserver when a mesage can't be delivered) or "returned mail" messages (sent by the mailserver when it thinks the e-mail has a virus - of course the guy to whom the mailserver returns the mail is almost certainly not the guy who's infected).

- The #1 best way to improve your safety if you use Outlook Express is to get a virus scanner. All of them are good, provided you get the updates and configure the virus scanner to either clean or delete infected attachments; unfortunately the default action is often "try to clean" (which fails if there's nothing to clean i.e. the file is 100% virus) then pass. I prefer Trend PC-Cillin (comes free with a lot of motherboards) myself. The #2 best way to improve your safety is to turn off the Preview Pane, which is The Root Of All Evil - View->Layout->Preview Pane.

- MyDoom doesn't automagically infect you if you open the e-mail, thank goodness. You have to actually double-click on the attachment to get whacked.

- If you run with User or Power User privileges only (Win2K and WinXP), then you can't get infected as you don't have the ability to install programs - including viruses like MyDoom.