It's all Geek to Me!!

This Bagle might be toasting a PC near you?

The most recent variations of the Bagle worm family appear to be based on code similar to the Bagle.af variation. This family of viruses are mass-mailing worms that vary in length. It has its own built-in email program so that it can spread mail to people in your address book and you would never know. They use various subject lines and attached files to spread via e-mail. They also attempt to spread via shared network files.

They both try to terminate security apps like your Antivirus software that may be running on the infected machine and install a backdoor Trojan horse. Additionally, Bagle.ai will attempt to terminate any Netsky virus that may be running on the infected machine. This worm does not affect Linux, Unix, or Mac OS systems. This virus is given a moderate warning level from Symantec.

What does it do?
Both versions of Bagle use a different set of subject and body texts, contain their own SMTP engine (which is an e-mail sending program) to send copies of themselves. They also harvest e-mail addresses from infected machines, spoof the e-mail sender's address (which means they use your email address), and password-protect the attached file. These worms contain a remote access Trojan horse, copy themselves to folders that use the string "shar" in the name, and will attempt to terminate security programs and other computer viruses and worms.

How do you prevent this?
Variations of the Bagle worm do not rely on a specific Microsoft vulnerability but on simple social engineering. Remember to never open attached e-mail files without first saving to the hard drive and scanning for known viruses. The latest signature file from your antivirus vendor should protect you against these Bagle variations. Additionally, the use of a personal firewall will prevent the backdoor Trojan from communicating with the virus author.

How do I get rid of this?
Several antivirus software companies have updated their signature files to include this worm. This will stop the infection upon contact and in some cases will remove an active infection from your system. So update your virus definitions and run a system scan.

For more information about **Bagle.ag**--also known as Beagle.ag (Symantec) and Bagle.ah (F-Secure)--you can go to www.sarc.com and look at the links for w32.Beagle.ag.

Viruses like this one and many others occur on a daily basis. If you don't have an up-to-date version of an Antivirus program like Norton Antivirus 2004 or McAfee VirusScan then you put your computer at risk. Remember, having the software is only part of the solution, you have to keep it up-to-date with regular downloads.

If you have an always on Internet solution, your software will probably update automatically if you have the newer versions. If you have a dial-up Internet connection, you should update your virus software a minimum of once a week. I realize the

download can take awhile, but it's better than having your computer wiped out by a virus!!

If you have any questions about computers, please feel free to send them to me at Contact@cbtechserv.com and I will respond in a future column.

Steve Cote is the owner of Copper Beech Technology Services, he has been involved in the computer industry since 1982 and is located in Salem, NH. Started March 2003, Copper Beech Technology provides onsite computer support services to residential and small business customers in the Merrimack Valley and surrounding communities. These services include PC installation, repairs, upgrades, network installations, virus detection/removal as well as web and e-mail hosting services. You can contact Copper Beech Technology by e-mail at contact@cbtechserv.com. Appointments can also be scheduled by calling 866-SOS-GEEK.