COMPUTER WORMS

Panchenko Oksana, *IN-41*,
Plokhuta T.M., *EL advisor*

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program.

Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms have been created which are only designed to spread, and don't attempt to alter the systems they pass through. However, as the Morris worm and Mydoom showed, the network traffic and other unintended effects can often cause major disruption. A "payload" is code designed to do more than spread the worm - it might delete files on a host system (e.g., the ExploreZip worm), encrypt files in a cryptoviral extortion attack, or send documents via e-mail.

A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" under control of the worm author - Sobig and Mydoom are examples which created zombies. Networks of such machines are often referred to as botnets and are very commonly used by spam senders for sending junk email or to cloak their website's address. Spammers are therefore thought to be a source of funding for the creation of such worms, and worm writers have been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threatened DoS attacks.

Beginning with the very first research into worms at Xerox PARC there have been attempts to create useful worms. The Nachi family of worms, for example, tried to download and install patches from Microsoft's website to fix vulnerabilities in the host system — by exploiting those same vulnerabilities. In practice, although this may have made these systems more secure, it generated considerable network traffic, rebooted the machine in the course of patching it, and did its work without the consent of the computer's owner or user.