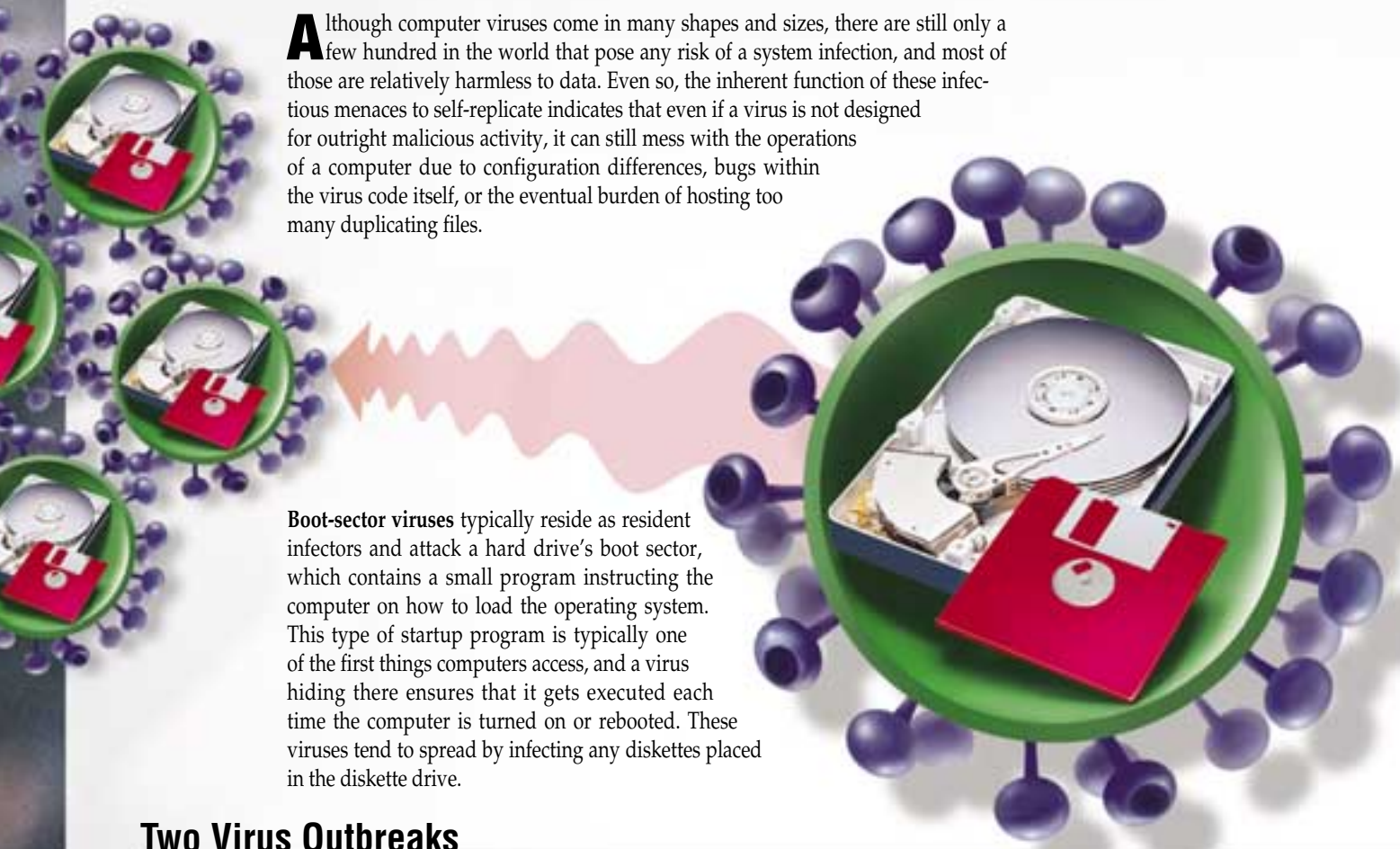
How Viruses Work

Although computer viruses come in many shapes and sizes, there are still only a few hundred in the world that pose any risk of a system infection, and most of those are relatively harmless to data. Even so, the inherent function of these infectious menaces to self-replicate indicates that even if a virus is not designed for outright malicious activity, it can still mess with the operations of a computer due to configuration differences, bugs within the virus code itself, or the eventual burden of hosting too many duplicating files.



Boot-sector viruses typically reside as resident infectors and attack a hard drive's boot sector, which contains a small program instructing the computer on how to load the operating system. This type of startup program is typically one of the first things computers access, and a virus hiding there ensures that it gets executed each time the computer is turned on or rebooted. These viruses tend to spread by infecting any diskettes placed in the diskette drive.

Two Virus Outbreaks

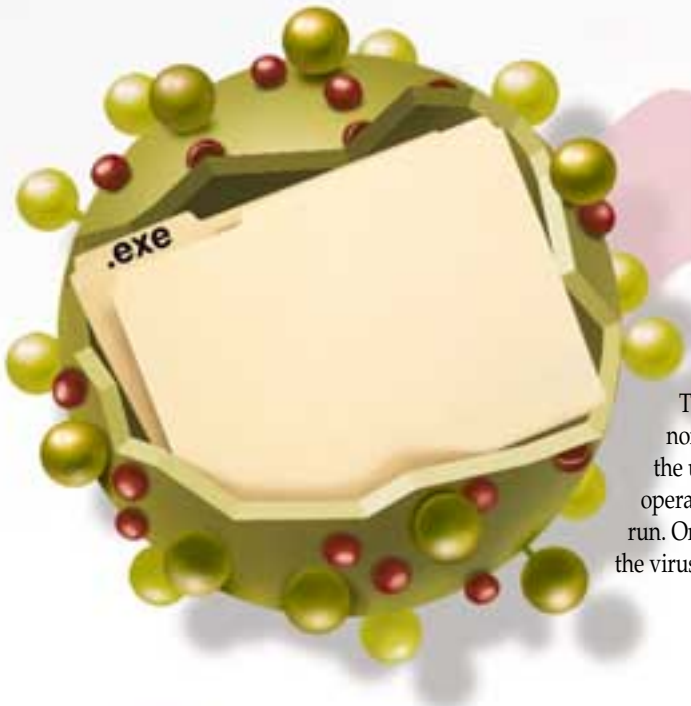
ExploreZip

The ExploreZip virus outbreak hit in early June of 1999. Because it arrived as a zipped attachment in an e-mail message, this virus spread quickly and created a significant amount of damage in its wake.

1 Users sending e-mail messages to someone with an ExploreZip-infected computer almost immediately receive a fake reply and an e-mail attachment called Zipped_files.exe (sometimes including the WinZip icon). The subject line varies, but the message typically says: "Just got your e-mail and I'll send you a reply ASAP. Until then, take a look at the attached zipped documents."

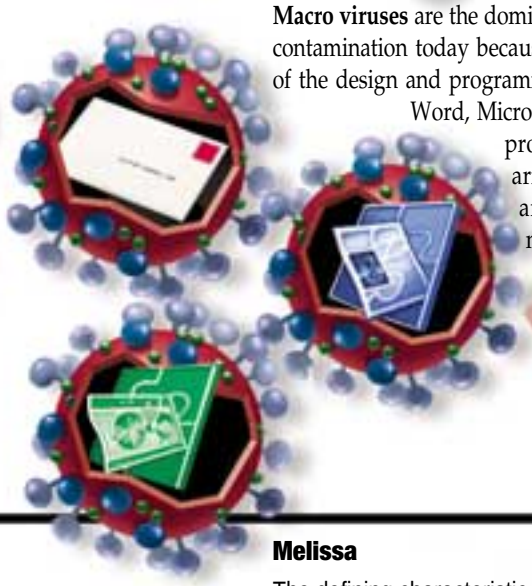
2 After opening the attachment, an error message states: "Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help."

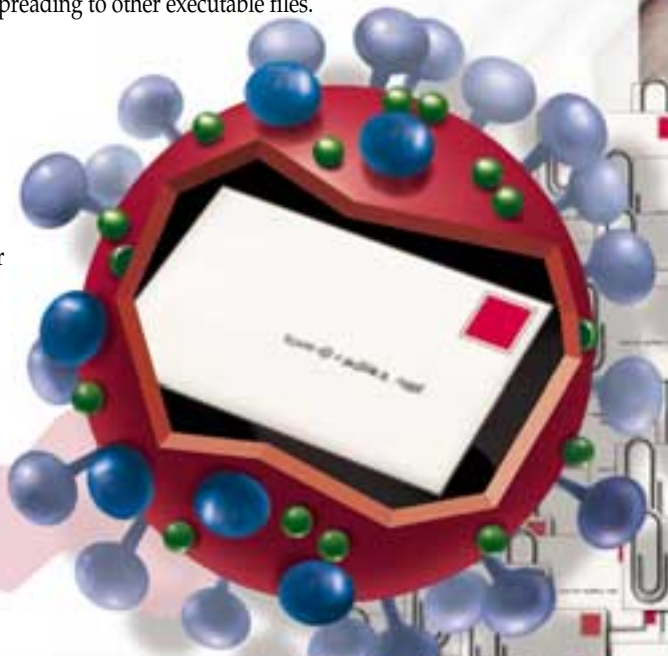
3 The virus then searches local and networked drives for specific file types (such as .DOC, .XLS, and .PPT) so it can erase the contents of these files and assign a zero byte count to them (usually prevents lost data from being recoverable).



File viruses attach themselves to executable files (such as files with extensions of .EXE, .DLL, etc.) and can arrive via a diskette, Internet download, or e-mail attachment. These viruses, which can be either resident or non-resident, activate behind the scenes without the user's knowledge, performing their intended operations before permitting the actual program to run. Once users restart newly infected applications, the virus can begin spreading to other executable files.

Macro viruses are the dominant form of mass computer contamination today because they take full advantage of the design and programming language of Microsoft Word, Microsoft Excel, and other popular programs. These viruses often arrive via e-mail attachments and, once activated, infect newly created documents.





Melissa

The defining characteristic of any virus is its ability to self-replicate and spread. The Melissa virus certainly achieved that goal in March 1999, becoming one of the fastest-spreading viruses observed to date.

1 Melissa sends recipients an e-mail message with a tainted Word attachment, as well as a subject line that appears to be from someone the recipients recognize. The e-mail message says: "Here's the document you asked for . . . don't show anyone else. ;-)"

2 Once the unlucky recipient opens the tainted attachment, Melissa creates and attaches itself to a Microsoft Word object and then searches through the recipient's address book.

3 Melissa accesses the first 50 names it finds in the recipient's address book and e-mails a message containing the tainted Word attachment to all of them.

Compiled by Lori Robison
Graphics & Design by Lori Garris