

New Viruses Attack PCs

Remotely Controlled: Babylonia

I'm getting tired of writing about viruses. Just about half of the technical articles I've researched in the last two months have been about viruses: Melissa, BubbleBoy, MiniZip, MyPics, and now Babylonia. And, even worse, these viruses are starting to show up on the PCs and network servers of our clients. And most of these businesses didn't know they were infected until I ran into the viruses during routine maintenance of their systems.

Here's the bottom line. Get the newest release of a good anti-virus software and keep it updated each week. McAfee, Symantec, and Trend Micro all make good products. I, personally, prefer McAfee's VirusScan. But whichever of the products you choose, make sure you download the periodic updates from the web as soon as they're available. New viruses require new anti-virus data files. Download 'em, install 'em.

The Babylonia virus was upgraded to a higher risk by anti-virus centers and is of interest because it appears that once the virus infects a system, it stays under the control of a web server in Japan and can be updated to do new damage over time. It's the first "remotely updating virus."

Babylonia is sent via chatrooms on the IRC (Internet Relay Chat) network, and it's disguised as a fix for the so-called Y2K, millennium, bug.

MyPics: Y2K to the Max

A new virus, disguised as a Y2K problem was reported by Symantec this morning. The W32/Mypics.worm (a.k.a. Worm.Mypic) is transmitted via email file attachment. The email message has no subject line, and the attachment is a 33Kb file named Pics4You.exe.

When executed the file changes the Microsoft Internet Explorer default homepage to an adult website. It loads into memory and grabs the first 50 names in the Microsoft Outlook address book and mails itself 20 minutes later to the addresses and repeats the itself every 10 minutes.

Currently, infected users may manually delete registry-key files from their computers to eradicate MyPic.

If not cleaned, on 1/1/2000, and possibly again later, the program will create the file C:\CBIOS.COM which will write

over the PC's checksum data in the system BIOS, also known as the CMOS. A message will appear during boot up: "CMOS checksum is invalid."

This message may create the impression of a Y2K problem with this computer, because the CMOS maintains the system clock, which can possibly be affected by the transition to the year 2000.

Then, when the CMOS error message is corrected, during the next boot the worm will format both the C: and D: drives by creating a new file in the FAT (File Allocation Table).

MiniZip Slips Past Anti-Virus Software

First reported by ITinfo in June (see related article below), the ExploreZip worm has returned and it's back with a vengeance.

A new compressed version has attacked several major companies, according to Dan Schrader, Trend Micro's Vice President of New Technology. We already scan for compressed files, but they chose one that we don't [detect] so far."

It's being dubbed MiniZip by some security vendors. It's the same technology as the worm's first iteration, but because it's signature is altered by the Neolite compression, anti-virus programs can't yet detect it.

All three leading anti-virus security firms: Network Associates, Symantec, and Trend Micro have received copies of the virus from infected customers.

If the worm's infection follows the same pattern as the original ExploreZip, Asia will see a marked increase in rates of infection overnight Tuesday evening, and the U.S. and Europe will follow with infections on Wednesday.

The worm's payload is the same as before: deleting files, and automatically sending infected email messages to address book lists. It affects systems running Microsoft Outlook, Outlook Express, and Exchange.

More Information

Subscribe to ITinfo, the computer industry's leading e-zine for tips and tricks to help you combat viruses on the net. Check out dgl.com for a free subscription.