TECHNOLOGY ADVICE YOU CAN TRUST
PC WORLD

Topics > Privacy & Security > Viruses & Worms > Worms >

Mydoom Sets Speed Records

New worm is spreading faster than Sobig.F, experts say.

Paul Roberts, IDG News Service
Tuesday, January 27, 2004

Mydoom, a new computer virus spreading by e-mail, is breaking records for new infections, antivirus vendors and security companies say.

Infected e-mail messages carrying the Mydoom virus, also known as "Shimgapi" and "Novarg," have been intercepted from over 142 countries and now account for one in every 12 e-mail messages, according to Mark Sunner, chief technology officer at e-mail security company MessageLabs.

That surpasses the Sobig.F virus record, which appeared last August and, at its peak, was found in one of every 17 messages intercepted by MessageLabs, he says.

Since first detecting the new virus at 1:00 PM GMT on Monday, MessageLabs intercepted almost 1 million infected e-mail messages carrying the virus, Sunner says.

The virus has "followed the sun," hitting hard in the U.S. and Canada late on Monday, then working its way through Asia and Europe on Tuesday, he says.

F-Secure of Helsinki estimates that around 100,000 computers have been infected with Mydoom so far, says Mikko Hypponen, manager of antivirus research at F-Secure.

Antivirus experts expect another large wave of infections in the U.S. and Canada on Tuesday morning, as workers who missed the virus late Monday return to their desks, he says.

Tech Talk

The worm arrives as a file attachment in an e-mail with a variety of senders and subjects, such as "Hello," and "test." The message body is often technical sounding, imitating the look and feel of an automatically generated message from an e-mail server, Sunner says.

For example, some e-mail messages telling recipients that "the message contains unicode characters and has been sent as a binary attachment," or "The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment."

Users who click on the attachment, which uses a variety of file extensions such as ZIP, SCR, EXE, and PIF, are infected with the virus.

The technical pitch is a new twist on so-called "social engineering" techniques used by virus writers to trick users into opening malicious file attachments. Mydoom's authors may have been counting on the fact that people trust the authenticity of computer generated messages more than those purporting to come from other humans, Sunner says.

Mimicking the language of a computer-generated administrative message may have also helped Mydoom spread within large corporations, where employees are used to receiving such messages from administrative systems, according to David Perry, public education director at antivirus company Trend Micro.

Going to Work

Trend Micro saw evidence on Monday of infections from 12 of the Fortune 100 companies, he says.

Once inside such companies, Mydoom could use the enormous bandwidth of those corporate networks and huge e-mail address books as a "springboard" to the rest of the Internet, Perry says.

While Mydoom has shattered Sobig.F records, in many ways the two viruses are the same, antivirus experts agree.

Both viruses scan infected computers for e-mail addresses that are then targeted by infected e-mail. Also, both Sobig.F and Mydoom are small and contain highly efficient SMTP engines for sending out copies of themselves. The efficiency of their mail engines means that even a small number of infections can generate a massive amount of e-mail traffic, Hypponen says.

Finally, both Sobig.F and Mydoom contain a Trojan horse program that gives remote attackers full control of the infected system, he says.

In the case of Sobig.F, experts theorized that the virus was being used to assemble "zombie" networks of machines for distributing spam e-mail. A similar motive may be behind Mydoom, though the virus writer's intentions are not yet clear, says Perry.