ChannelWeb The B2B Network For Solution Providers

CRN

Building Technology Solutions for the New Economy »

MyDoom Predicted To Be As Bad As Sobig

(URL: http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=47488)

By Christina Torode
CRN

1:32 PM EST Tues., Jan. 27, 2004

Beginning last night, solution providers and security vendors scrambled to stem the latest major virus outbreak, MyDoom, a virus that many say will have as large an impact as last summer's Sobig worm.

MyDoom propagates when a user opens an infected attachment. Once the attached message is opened, the virus will copy itself in the system directory, look for Domain names on the machine and gather e-mail addresses, to start generating a glut of infected e-mail messages to valid recipients.

The virus also pieces different names and Domain names together from a user's system to send out infected e-mails.

"The end result is a significant amount of e-mail emitting from infected machines on an ongoing basis," said Craig Schmugar, virus research manager with Network Associates' McAfee Avert Team. "This virus just continuously keeps generating names and sending messages as long as the system is up."

Within four hours of identifying the virus, 27,000 machines were infected, Network Associates said. The amount of infected e-mails received by McAfee's customers range from one in three being infected, to one in eight e-mails being infected, Schmugar said.

McAfee, Trend Micro, Sophos and other security vendors released patches for the virus, either last night or this morning, which can be downloaded from the vendors' Web sites.

Security solution provider Conqwest sent out an alert last night, and steered its customers to its own Web site or Sophos' and Trend Micro's to download the patch for MyDoom.

"It's crazy because what's happening is this virus is coming in so many different types of executable files and the messages are all different," said Michele Drolet, CEO of Conqwest, Holliston, Mass.

Conqwest also sent out the following warning and explanation to its customers:

"W32/MyDoom-A is a worm which travels by e-mail. The worm harvests e-mail addresses from your hard disk and uses randomly chosen addresses for both the "to" and "from" fields. This means that the "from" address is spoofed and does not tell you where the mail really came from.

"W32/MyDoom-A arrives in e-mails with the following characteristics:

"Subject lines include: error, hello, hi, mail delivery system, mail transaction failed, server report, status, test.

"Attachment names include: body, data, doc, document, file, message, readme, test, and random collection of characters.

"Attachment extensions include: bat, cmd, exe, pif, scr and zip.

"W32/MyDoom-A attaches itself to e-mails in either EXE (Windows program) or ZIP (Zip archive) format.

"W32/MyDoom-A drops itself to your System folder under the name taskmon.exe. W32/MyDoom-A also drops a file named shimgapi.dll, which is a backdoor program loaded by the worm. The backdoor allows outsiders to connect to TCP port 3127 on your computer.

"W32/MyDoom-A adds the value: Taskmon = taskmon.exe to the following registry key:
HKLM%5CSoftware%5CMicrosoft%5CWindows%5CCurrentVersion%5CRun

"This means that W32/MyDoom-A loads every time you log on to your computer."

Paul Rohmeyer, partner and COO of Icons, an information security services firm based in North Brunswick, N.J., is similarly telling customers to download security vendors' patches to combat the virus, but is also recommending that customers temporarily block zip files.

"Beyond that, everyone is in a wait-and-see mode as to the real severity of the attack," said Rohmeyer.