



SEARCH

[Help](#) | [Advanced](#)

SCM ONLINE

- **[News](#)**
- **[Reviews](#)**
 - [Hardware](#)
 - [Software](#)
 - [Books](#)
- **[Features](#)**
- **[Opinions](#)**
- **[SCM News](#)**

NEWS HEADLINES

- [Activision Cancels New Survival Horror Title](#)
- [Panasonic Updates Lumix Digital Camera Range](#)
- [Old Viruses Make A Comeback](#)
- [Sony Releases New 5.1 Megapixel Digital Camera](#)
- [Chinese Author To Publish New Novel Using SMS](#)

NEWS

Old Viruses Make A Comeback

[28/07/2004]

Bagle and MyDoom are just some of the viruses that were terrorising computer users worldwide at the beginning of this year and have now resurfaced with new variants.

Both Bagle.AI and MyDoom.N are mass-mailing worms that utilise an SMTP (Simple Mail Transfer Protocol) engine to send emails to addresses found on systems that they infect. Emails sent by Bagle.AI have a subject line of "Re_", content that varies from "foto and MP3" to "Lovely animals", and the From field is spoofed to appear to be sent by a known correspondent. The attachment has a name that varies, often referring to MP3s or animals and has one of the following extensions: .com, .cpl, .exe, .scr, or .zip.

Once the attachment has been opened the virus infects the user's system, shuts down anti-virus software, and deletes variants of the [Netsky](#) virus that might be on the computer. It opens a back door on port 1080, which could allow crackers to run programs remotely and use the computer in DoS (Denial-of-Service) attacks. The worm also spreads via P2P (Peer-to-Peer) networks by copying itself to folders with names containing the characters "shar". After 5th May 2006 the virus removes itself from infected computers automatically.

Aliases for Bagle.AI include WORM_BAGLE.AH, W32.Beagle.AG@mm, W32/Bagle-AI, Bagle.AH, W32/Bagle.AH@mm, W32/Bagle.ai@MM, Worm.Bagle.ai, W32/Bagle.AI@mm, Win32.Bagle.AE, and Worm/Bagle.AI.

As well as using spoofed email addresses, MyDoom.N may also send infected emails that seem to be sent by a Postmaster, Mail Administrator, Mailer-DAEMON, or a Mail Delivery Subsystem. The subject line varies and includes "hi", "Message could not be delivered", "Returned mail: see transcript for details", "error", and "Delivery reports about your e-mail". The content is also variable but generally mentions that an email sent by the user couldn't be delivered and he should refer to the attachment for more information. The attachment may have a name similar to the domain name of the email address. Examples of the extension include: .bat, .com, .exe, .pif, .scr, and .zip.

MyDoom.N opens a port to allow remote access to a user's computer by crackers. The virus also copies itself into folders that could enable it to spread via P2P networks. These copies are renamed to make them more desirable to people who connect to the infected computer. Names include Harry Potter, index, and Winamp 5.0 (en).

W32.Mydoom.L@mm, W32/MyDoom-N, WORM_MYDOOM.L, W32/MyDoom.L@mm, MyDoom.L, W32/Mydoom.M@mm, and Win32.Mydoom.N are some of the aliases for MyDoom.N.

Both viruses affect all [Microsoft Windows](#) systems including [Windows 95](#), [Windows 98](#), [Windows 2000](#), [Windows Me](#), [Windows NT](#), and [Windows XP](#).

Users are advised to update their anti-virus software definitions. One of the companies that publishes anti-virus software is MicroWorld. [eScan](#) and [MailScan](#) are real-time anti-virus and security programs published by the company,

ISSUE ARCHIVE

SHOP

which actively protect a computer from viruses and unsolicited spam.

Free removal tools and instructions for the worms are also from [MicroWorld](#), [Panda Software](#), [Sophos](#), and [Symantec](#).

Contact Details

More Details: [MicroWorld Removal Tool For Bagle.AI](#)

More Details: [MicroWorld Removal Tool For MyDoom.N](#)