MyDoom (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:36:43 UTC

When executed, the worm opens up Windows' Notepad with garbage data in it. When spreading, the infectious email used to distribute the worm copies use variable subjects, bodies and attachment names.

The worm encrypts most of the strings in it's UPX-packed body with ROT13 method, i.e. the characters are rotated 13 locations to the right in the abecedary, starting from the beginning if the position is beyond the last letter.

Mydoom also performs a Distributed Denial-of-Service attack on www.sco.com. This attack starts on 1st of February.

The worm opens up a backdoor to infected computers. This is done by planting a new SHIMGAPI.DLL file to system32 directory and launching it as a child process of EXPLORER.EXE.

Mydoom is programmed to stop spreading on February 12th.

▶ [TLP:WHITE] win_mydoom_auto (20251219 | Detects win.mydoom.)
