danbot (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:35:17 UTC

Danbot is a backdoor malware that is originally written in C#. Recent versions of Danbot are written in C++. Danbot is capable of giving a remote attacker remote access features such as running a cmd command, upload and download files, move and copy files. The backdoor commands are transmitted by either using HTTP or DNS protocols. The commands are encapsulated in an XML file that gets stored in disk. Danbot's backdoor component picks up the XML file where it decodes and decrypts the commands.

▶ [TLP:WHITE] win_danbot_auto (20251219 | Detects win.danbot.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.danbot