Derusbi (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:52:26 UTC

A DLL backdoor also reported publicly as “Derusbi”, capable of obtaining directory, file, and drive listing; creating a reverse shell; performing screen captures; recording video and audio; listing, terminating, and creating processes; enumerating, starting, and deleting registry keys and values; logging keystrokes, returning usernames and passwords from protected storage; and renaming, deleting, copying, moving, reading, and writing to files.

▶ [TLP:WHITE] win_derusbi_auto (20251219 | Detects win.derusbi.)
