Rook (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:13:24 UTC

According to PCrisk, Rook is ransomware (an updated variant of Babuk) that prevents victims from accessing/opening files by encrypting them. It also modifies filenames and creates a text file/ransom note ("HowToRestoreYourFiles.txt"). Rook renames files by appending the ".Rook" extension. For example, it renames "1.jpg" to "1.jpg.Rook", "2.jpg" to "2.jpg.Rook".

▶ [TLP:WHITE] win_rook_auto (20251219 | Detects win.rook.)
