Bandook (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:04:22 UTC

Bandook malware is a remote access trojan (RAT) first seen in 2007 and has been active for several years. Written in both Delphi and C++, it was first seen as a commercial RAT developed by a Lebanese creator named PrinceAli. Over the years, several variants of Bandook were leaked online, and the malware became available for public download.

▶ [TLP:WHITE] win_bandook_auto (20251219 | Detects win.bandook.)
