Ratankba (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:38:09 UTC

This is a backdoor that establishes persistence using the Startup folder.
It communicates to its C&C server using HTTPS and a static HTTP User-Agent string. QUICKRIDE is capable of gathering information about the system, downloading and loading executables, and uninstalling itself. It was leveraged against banks in Poland.

▶ [TLP:WHITE] win_ratankba_auto (20251219 | Detects win.ratankba.)
