QuiteRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:31:42 UTC

After sending preliminary system information to its C&C server, it expects a response containing either a supported command code or an actual Windows command (like systeminfo or ipconfig with parameters) to execute.

It was deployed in a campaign exploiting a ManageEngine ServiceDesk vulnerability (CVE-2022-47966).

▶ [TLP:WHITE] win_quiterat_auto (20251219 | Detects win.quiterat.)
