Seduploader (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:58:34 UTC

simple tool to facilitate download and persistence of a next-stage tool; collects system information and metadata probably in an attempt to tell sandbox-environments apart from real targets on the server-side; uses domains of search engines like Google to check for Internet connectivity; XOR-based string obfuscation with a 16-byte key

▶ [TLP:WHITE] win_seduploader_auto (20251219 | Detects win.seduploader.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.seduploader