

GraphSteel (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:33:49 UTC

This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

► [TLP:WHITE] win_graphsteel_auto (20251219 | Detects win.graphsteel.)

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.graphsteel>