

Graphiron (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:15:59 UTC

win.graphiron ([Back to overview](#))

Graphiron

Actor(s): [SaintBear](#)

Downloader / information stealer used by UAC-0056, observed since at least October 2022.

References

2023-05-16 · [Secureworks](#) · [Counter Threat Unit ResearchTeam](#)

The Growing Threat from Infostealers

[Graphiron GraphSteel Raccoon RedLine Stealer Rhadamanthys Taurus Stealer Vidar](#)

2023-02-08 · [Broadcom](#) · [Threat Hunter Team](#)

Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine

[Graphiron SaintBear](#)

There is no Yara-Signature yet.

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