

Sorgu (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:18:46 UTC

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

Sorgu

Actor(s): Leafminer

There is no description at this point.

References

2018-07-25 · [Symantec](#) · [Network Protection Security Labs](#), [Security Response Attack Investigation Team](#)
Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions
[Imecab Sorgu RASPITE](#)

2018-07-25 · [Symantec](#) · [Critical Attack Discovery and Intelligence Team](#), [Network Protection Security Labs](#)
Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions
[Imecab MimiKatz Sorgu RASPITE](#)

There is no Yara-Signature yet.

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