

Powersniff (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:30:34 UTC

A malware of the gozi group, developed on the base of isfb. It uses Office Macros and PowerShell in documents distributed in e-mail messages.

► [TLP:WHITE] win_powersniff_auto (20251219 | Detects win.powersniff.)

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