

PICKPOCKET (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:34:10 UTC

PICKPOCKET is a credential theft tool that dumps the user's website login credentials from Chrome, Firefox, and Internet Explorer to a file. This tool was previously observed solely utilized by APT34.

► [TLP:WHITE] win_pickpocket_auto (20251219 | Detects win.pickpocket.)

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