

SHIPSHAPE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:21:30 UTC

SHIPSHAPE is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.

► [TLP:WHITE] win_shipshape_auto (20251219 | Detects win.shipshape.)

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