SPACESHIP (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:11:56 UTC

SPACESHIP searches for files with a specified set of file extensions and copies them to a removable drive. FireEye believes that SHIPSHAPE is used to copy SPACESHIP to a removable drive, which could be used to infect another victim computer, including an air-gapped computer. SPACESHIP is then used to steal documents from the air-gapped system, copying them to a removable drive inserted into the SPACESHIP-infected system

▶ [TLP:WHITE] win_spaceship_auto (20251219 | Detects win.spaceship.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.spaceship