

# SSLoad (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:08:15 UTC

SSLoad is a Rust-based downloader that first emerged in January 2024 and is used to deliver secondary payloads. Early versions of the malware used a first-stage DLL that connected to a Telegram channel named 'SSLoad' to retrieve another URL. It then downloaded a compressed PE file using a hardcoded User-Agent (SSLoad/1.x) and Content-Type over HTTP. The downloaded file was then decompressed and executed directly in memory. The malware has since undergone several updates, including changes to the command-and-control (C2) communication and the supporting executables that load the malware. Recent versions of the malware bypass the first-stage DLL by loading SSSLoad directly onto the victim's machine.

► [TLP:WHITE] win\_ssload\_auto (20251219 | Detects win.ssload.)

---

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