CrypticConvo (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:39:36 UTC

CrypticConvo is a dropper trojan which appears to be embedded in an automatic generator framework to deliver the FakeM trojan. According to PaloaltoNetworks CrypticConvo and several additional trojans are believed to be included in a meta framework used by the "Scarlet Mimic" threat actor in order to quickly evade AV systems.

▶ [TLP:WHITE] win_cryptic_convo_auto (20251219 | Detects win.cryptic_convo.)
