Croxloader (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 15:28:45 UTC

According to Trend Micro, this is a custom loader for win.cobalt_strike, used by Earth Longzhi (a subgroup of APT41).

▶ [TLP:WHITE] win_croxloader_auto (20251219 | Detects win.croxloader.)
