MESSAGETAP (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:35:51 UTC

MESSAGETAP

Actor(s): APT41

MESSAGETAP is a 64-bit ELF data miner initially loaded by an installation script. It is designed to monitor and save SMS traffic from specific phone numbers, IMSI numbers and keywords for subsequent theft.

References

Yara Rules

▶ [TLP:WHITE] elf_messagetap_w0 (20191113 | Detects MESSAGETAP malware through strings)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/elf.messagetap