RTM (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:35:20 UTC

RTM Banker also known as Redaman was first blogged about in February 2017 by ESET. The malware is written in Delphi and shows some similarities (like process list) with Buhtrap. It uses a slightly modified version of RC4 to encrypt its strings, network data, configuration and modules, according to ESET.

▶ [TLP:WHITE] win_rtm_auto (20201014 | autogenerated rule brought to you by yara-signator)
