

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:57:48 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool RTM


Tool: RTM

Names	RTM RTM Banker Redaman
Category	Malware
Type	Banking trojan , Backdoor , Keylogger , Info stealer , Downloader , Exfiltration
Description	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.
Information	< https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf >
MITRE ATT&CK	< https://attack.mitre.org/software/S0148/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.rtm > < https://malpedia.caad.fkie.fraunhofer.de/details/win.redaman >

Last change to this tool card: 22 May 2020

Download this tool card in [JSON](#) format

All groups using tool RTM

Changed	Name	Country	Observed
APT groups			
	RTM		2015

1 group listed (1 APT, 0 other, 0 unknown)

Source: <https://apt.eta.dia.or.th/cgi-bin/listgroups.cgi?u=fd9ceb37-fbda-4946-9e69-c83de7ecb1d0>