

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:58:54 UTC

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

Tool: Telemiris

Names	Telemiris
Category	Malware
Type	Backdoor
Description	(Kaspersky) Telemiris is a Python backdoor originally packed with PyInstaller (we later identified some Nuitka-packaged samples as well). Its name derives from the fact that it uses Telegram as a C2 channel. After setting up persistence (copying itself under %AppData%/service/ and creating a RUN key entry), the malware enters its main loop where it waits for Telegram messages and replies to them.
Information	< https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.telemiris >

Last change to this tool card: 22 June 2023

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

All groups using tool Telemiris

Changed	Name	Country	Observed
APT groups			
	Tomiris	[Unknown]	2020

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d0baa819-6460-425e-b5f0-e64fe8ea18db>