Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:12:10 UTC

Tool: Tomiris

Names	Tomiris
Category	Malware
Type	Backdoor
Description	(Kaspersky) Tomiris is a backdoor written in Go whose role is to continuously query its C2 server for executables to download and execute on the victim system. Before performing any operations, it sleeps for at least nine minutes in a possible attempt to defeat sandbox-based analysis systems. (Kaspersky) The backdoor, dubbed Tomiris, bears a number of similarities to the second-stage malware, Sunshuttle (aka GoldMax), used by DarkHalo last year. However, there are also a number of overlaps between Tomiris and Kazuar, a backdoor that has been linked to the Turla APT threat actor. None of the similarities is enough to link Tomiris and Sunshuttle with high confidence. However, taken together they suggest the possibility of common authorship or shared development practices.
Information	<https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/> <https://securelist.com/apt-trends-report-q3-2021/104708/> <https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0671/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tomiris>

Last change to this tool card: 26 April 2023

Download this tool card in JSON format

All groups using tool Tomiris

Changed	Name	Country	Observed
APT groups			

	Tomiris	[Unknown]	2020	

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