Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:07:08 UTC

APT group: Tomiris

Names	Tomiris *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	(Kaspersky) Tomiris focuses on intelligence gathering in Central Asia. Tomiris's endgame consistently appears to be the regular theft of internal documents. The threat actor targets government and diplomatic entities in the CIS. The occasional victims discovered in other regions (such as the Middle East or South-East Asia) turn out to be foreign representations of CIS countries, illustrating Tomiris's narrow focus. It is characterized by its tendency to develop numerous low-sophistication "burner" implants in a variety of programming languages that are repeatedly deployed against the same targets, using elementary but efficient packaging and distribution techniques. Tomiris occasionally leverages commercial or open-source RATs. Language artifacts discovered in Tomiris's implant families and infrastructure from distinct campaigns all indicate that the threat actor is Russian-speaking. Overall, Tomiris is a very agile and determined actor, open to experimentation – for instance with delivery methods (DNS hijacking) or command and control (C2) channels (Telegram). Kaspersky also asserts that there exists a form of deliberate cooperation between Tomiris and Turla, Waterbug, Venomous Bear.
Observed	Sectors: Government. Countries: Commonwealth of Independent States (CIS).
Tools used	JLOGRAB, JLORAT, KopiLuwak, Meterpreter, RATel, RocketMan, Roopy, Telemiris, Tomiris, Topinambour, Tunnus, Warzone RAT.
Information	<https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/>

Last change to this card: 26 April 2023

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=ddad8bb4-d188-46de-8c2d-2ed50ebbc59f