Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:27:47 UTC

Tool: RedShawl

Names	RedShawl
Category	Malware
Description	REDSHAWL is a session hijacking utility that starts a new process as another user currently logged on to the same system via command-line.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf> <https://content.fireeye.com/apt/rpt-apt38>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.redshawl>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool RedShawl

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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