Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:44:21 UTC

Tool: Colibri Loader

Names	Colibri Loader
Category	Malware
Type	Loader
Description	(CloudSEK) On 27 August 2021, cybersecurity researchers discovered a malware loader dubbed Colibri being sold on an underground Russian forum. The actors claim that the loader is stealthy and can be used to target Windows systems, to drop other malware onto the infected system.
Information	<https://cloudsek.com/in-depth-technical-analysis-of-colibri-loader-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.colibri>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Colibri Loader

Changed	Name	Country	Observed	
APT groups				
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

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