Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:08:35 UTC

Tool: SparkRAT

Names	SparkRAT
Category	Tools
Type	Backdoor
Description	(SentinelLabs) SparkRAT is a RAT developed in Golang and released as open source software by the Chinese-speaking developer XZB-1248. SparkRAT is a feature-rich and multi-platform tool that supports the Windows, Linux, and macOS operating systems. SparkRAT uses the WebSocket protocol to communicate with the C2 server and features an upgrade system. This enables the RAT to automatically upgrade itself to the latest version available on the C2 server upon startup by issuing an upgrade request. This is an HTTP POST request, with the commit query parameter storing the current version of the tool.
Information	<https://www.sentinelone.com/labs/dragonspark-attacks-evade-detection-with-sparkrat-and-golang-source-code-interpretation/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.spark_rat>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool SparkRAT

Changed	Name	Country	Observed	
APT groups				
	DragonSpark		2022	
	TAG-100		2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b566744a-fe14-45fd-83f9-7ccbf4325fac