Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:24:21 UTC

APT group: DragonSpark

Names	DragonSpark *(SentinelLabs)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(SentinelLabs) SentinelLabs has been monitoring recent attacks against East Asian organizations we track as 'DragonSpark'. The attacks are characterized by the use of the little known open source SparkRAT and malware that attempts to evade detection through Golang source code interpretation. The DragonSpark attacks represent the first concrete malicious activity where we observe the consistent use of the open source SparkRAT, a relatively new occurrence on the threat landscape. SparkRAT is multi-platform, feature-rich, and frequently updated with new features, making the RAT attractive to threat actors. The Microsoft Security Threat Intelligence team reported in late December 2022 on indications of threat actors using SparkRAT. However, we have not observed concrete evidence linking DragonSpark to the activity documented in the report by Microsoft. We observed that the threat actor behind the DragonSpark attacks uses Golang malware that interprets embedded Golang source code at runtime as a technique for hindering static analysis and evading detection by static analysis mechanisms. This uncommon technique provides threat actors with yet another means to evade detection mechanisms by obfuscating malware implementations.
Observed	
Tools used	BadPotato, China Chopper, GotoHTTP, SharpToken, SparkRAT.
Information	<https://www.sentinelone.com/labs/dragonspark-attacks-evade-detection-with-sparkrat-and-golang-source-code-interpretation/>

Last change to this card: 15 February 2023

Download this actor card in PDF or JSON format
