SparkRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-29 08:06:59 UTC

win.spark_rat (Back to overview)

SparkRAT

SparkRAT is a cross-platform, open-source Remote Administration Tool (RAT) written in Go and released on GitHub in 2022. Compatible with Windows, macOS, and Linux systems, it offers extensive remote access capabilities, including file and process management, file transfer, remote desktop monitoring, system information collection, and command execution via terminal access.

References

2025-09-24 · The Hacker News · Ravie Lakshmanan
Chinese Hackers RedNovember Target Global Governments Using Pantegana and Cobalt Strike
Cobalt Strike Leslieloader Pantegana SparkRAT Storm-2077

2025-01-28 · Hunt.io · Hunt.io
SparkRAT: Server Detection, macOS Activity, and Malicious Connections
SparkRAT

2024-12-18 · Kaspersky Labs · Kaspersky
Analysis of Cyber Anarchy Squad attacks targeting Russian and Belarusian organizations
Babuk LockBit Revenge RAT SparkRAT Cyber Alliance Ukrainian Cyber Alliance

2024-11-13 · ClearSky · ClearSky
CVE-2024-43451: A New Zero-Day Vulnerability Exploited in the wild
SparkRAT UAC-0194

2024-11-13 · ClearSky · ClearSky
New Zero-Day Vulnerability Detected: CVE-2024-43451
SparkRAT

2024-07-16 · Recorded Future · Insikt Group
TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies
SparkRAT Storm-2077

2023-09-05 · · AhnLab · Sanseo

BlueShell malware used in APT attacks targeting Korea and Thailand

BlueShell SparkRAT

2023-05-18 · AhnLab · ASEC

SparkRAT Being Distributed Within a Korean VPN Installer

SparkRAT

2023-03-28 · ExaTrack · ExaTrack

Mélofée: a new alien malware in the Panda's toolset targeting Linux hosts

HelloBot Melofee Winnti Cobalt Strike SparkRAT STOWAWAY

2023-01-24 · SentinelOne · Aleksandar Milenkoski

DragonSpark | Attacks Evade Detection with SparkRAT and Golang Source Code Interpretation

SparkRAT DragonSpark

2022-12-21 · Microsoft · Microsoft Security Threat Intelligence

Microsoft research uncovers new Zerobot capabilities

ZeroBot SparkRAT

2022-03-16 · Github (XZB-1248) · XZB-1248

Github Repository for Spark RAT

SparkRAT

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.spark_rat