Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:37:51 UTC

Tool: Spark

Names	Spark
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Downloader
Description	(Cybereason) The Spark backdoor allows the attackers to: • Collect information about the infected machine. • Encrypt the collected data and send it to the attackers over the HTTP protocol. • Download additional payloads. • Log keystrokes. • Record audio using the computer's microphone. • Execute commands on the infected machine. The creators of the Spark backdoor use a few techniques that are intended to keep the backdoor under-the-radar, including: • Packing the payloads with the Enigma packer. • Checking for antivirus and other security products using WMI. • Validating Arabic keyboard and language settings on the infected machine.
Information	<https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one>
MITRE ATT&CK	<https://attack.mitre.org/software/S0543/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.spark>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Spark

Changed	Name	Country	Observed

APT groups

	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

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