Spark, Software S0543 | MITRE ATT&CK®

Archived: 2026-04-05 13:19:18 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Spark has used HTTP POST requests to communicate with its C2 server to receive commands.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Spark can use cmd.exe to run commands.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Spark has encoded communications with the C2 server with base64.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Spark has used a custom XOR algorithm to decrypt the payload.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Spark has exfiltrated data over the C2 channel.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Spark has been packed with Enigma Protector to obfuscate its contents.[1]
Enterprise	T1082		System Information Discovery	Spark can collect the hostname, keyboard layout, and language from the system.[1]
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	Spark has checked the results of the `GetKeyboardLayoutList` and the language name returned by `GetLocaleInfoA` to make sure they contain the word "Arabic" before executing.[1]

Domain	ID		Name	Use
Enterprise	T1033		System Owner/User Discovery	Spark has run the whoami command and has a built-in command to identify the user logged in.[1]
Enterprise	T1497	.002	Virtualization/Sandbox Evasion: User Activity Based Checks	Spark has used a splash screen to check whether an user actively clicks on the screen before running malicious code.[1]

Source: https://attack.mitre.org/software/S0543/