Orz, Software S0229 | MITRE ATT&CK®

Archived: 2026-04-05 16:51:03 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Orz can execute shell commands.[1] Orz can execute commands with JavaScript.[1]
Enterprise	T1083		File and Directory Discovery	Orz can gather victim drive information.[1]
Enterprise	T1070		Indicator Removal	Orz can overwrite Registry settings to reduce its visibility on the victim.[1]
Enterprise	T1105		Ingress Tool Transfer	Orz can download files onto the victim.[1]
Enterprise	T1112		Modify Registry	Orz can perform Registry operations.[1]
Enterprise	T1027		Obfuscated Files or Information	Some Orz strings are base64 encoded, such as the embedded DLL known as MockDll.[1]
Enterprise	T1057		Process Discovery	Orz can gather a process list from the victim.[1]
Enterprise	T1055	.012	Process Injection: Process Hollowing	Some Orz versions have an embedded DLL known as MockDll that uses process hollowing and Regsvr32 to execute another payload.[1]
Enterprise	T1518		Software Discovery	Orz can gather the victim's Internet Explorer version.[1]

Domain	ID		Name	Use
Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	Some Orz versions have an embedded DLL known as MockDll that uses Process Hollowing and regsvr32 to execute another payload.[1]
Enterprise	T1082		System Information Discovery	Orz can gather the victim OS version and whether it is 64 or 32 bit.[1]
Enterprise	T1016		System Network Configuration Discovery	Orz can gather victim proxy information.[1]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	Orz has used Technet and Pastebin web pages for command and control.[1]

Source: https://attack.mitre.org/software/S0229/