

SQLRat, Software S0390 | MITRE ATT&CK®

Archived: 2026-04-02 11:02:59 UTC

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	SQLRat has used PowerShell to create a Meterpreter session. ^[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	SQLRat has used SQL to execute JavaScript and VB scripts on the host system. ^[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	SQLRat has scripts that are responsible for deobfuscating additional scripts. ^[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	SQLRat has used been observed deleting scripts once used. ^[1]
Enterprise	T1105		Ingress Tool Transfer	SQLRat can make a direct SQL connection to a Microsoft database controlled by the attackers, retrieve an item from the bindata table, then write and execute the file on disk. ^[1]
Enterprise	T1027	.010	Obfuscated Files or Information: Command Obfuscation	SQLRat has used a character insertion obfuscation technique, making the script appear to contain Chinese characters. ^[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	SQLRat has created scheduled tasks in %appdata%\Roaming\Microsoft\Templates\ ^[1]
Enterprise	T1204	.002	User Execution: Malicious File	SQLRat relies on users clicking on an embedded image to execute the scripts. ^[1]

Source: <https://attack.mitre.org/software/S0390/>