MagicRAT, Software S1182 | MITRE ATT&CK®

Archived: 2026-04-05 16:28:38 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	MagicRAT uses HTTP POST communication for command and control.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	MagicRAT can persist using malicious LNK objects in the victim machine Startup folder.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	MagicRAT allows for the execution of arbitrary commands on the victim system.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	MagicRAT stores command and control URLs using base64 encoding in the malware's configuration file.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	MagicRAT exfiltrates data via HTTP over existing command and control channels.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	MagicRAT can delete files on victim systems, including itself.[1]
Enterprise	T1105		Ingress Tool Transfer	MagicRAT can import and execute additional payloads.[1]

Domain	ID		Name	Use
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	MagicRAT stores configuration data in files and file paths mimicking legitimate operating system resources.[1]
		.008	Masquerading: Masquerade File Type	MagicRAT can download additional executable payloads that masquerade as GIF files.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	MagicRAT stores base64 encoded command and contorl URLs in a configuraiton file, with each URL prefixed with the value `LR02DPt22R`.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	MagicRAT can persist via scheduled tasks.[1]
Enterprise	T1082		System Information Discovery	MagicRAT collects basic system information from victim machines.[1]
Enterprise	T1016		System Network Configuration Discovery	MagicRAT collects system network information using commands such as `ipconfig /all`.[1]

Source: https://attack.mitre.org/software/S1182