J-magic, Software S1203 | MITRE ATT&CK®

Archived: 2026-04-05 17:55:53 UTC

Domain	ID		Name	Use
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	The J-magic agent is executed through a command line argument which specifies an interface and listening port.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	J-magic can communicate back to send a challenge to C2 infrastructure over SSL.[1]
Enterprise	T1070	.003	Indicator Removal: Clear Command History	J-magic can overwrite previously executed command line arguments.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	J-magic can rename itself as "[nfsiod 0]" to masquerade as the local Network File System (NFS) asynchronous I/O server.[1]
Enterprise	T1040		Network Sniffing	J-magic has a pcap listener function that can create an Extended Berkley Packet Filter (eBPF) on designated interfaces and ports.[1]
Enterprise	T1095		Non-Application Layer Protocol	J-magic can monitor incoming C2 communications sent over TCP to the compromised host.[1]
Enterprise	T1016		System Network Configuration Discovery	J-magic can compare the host and remote IPs to check if a received packet is from the infected machine.[1]
Enterprise	T1205		Traffic Signaling	J-magic can monitor TCP traffic for packets containing one of five different predefined parameters and will spawn a reverse shell if one of

Domain	ID	Name	Use
			the parameters and the proper response string to a subsequent challenge is received.[1]

Source: https://attack.mitre.org/software/S1203