China Chopper, Software S0020 | MITRE ATT&CK®

Archived: 2026-04-05 14:28:55 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	China Chopper's server component executes code sent via HTTP POST commands.[3]
Enterprise	T1110	.001	Brute Force: Password Guessing	China Chopper's server component can perform brute force password guessing against authentication portals.[3]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	China Chopper's server component is capable of opening a command terminal.[6][1][7]
Enterprise	T1005		Data from Local System	China Chopper's server component can upload local files.[3][1][7][5]
Enterprise	T1083		File and Directory Discovery	China Chopper's server component can list directory contents.[3][5]
Enterprise	T1070	.006	Indicator Removal: Timestomp	China Chopper's server component can change the timestamp of files.[3][1][7]
Enterprise	T1105		Ingress Tool Transfer	China Chopper's server component can download remote files.[3][1][7][5][8]
Enterprise	T1046		Network Service Discovery	China Chopper's server component can spider authentication portals.[3]

Domain	ID		Name	Use
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	China Chopper's client component is packed with UPX.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	China Chopper's server component is a Web Shell payload.[1]

Source: https://attack.mitre.org/software/S0020