SideTwist, Software S0610 | MITRE ATT&CK®

Archived: 2026-04-02 11:42:04 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	SideTwist has used HTTP GET and POST requests over port 443 for C2.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	SideTwist can execute shell commands on a compromised host.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	SideTwist has used Base64 for encoded C2 traffic.[1]
Enterprise	T1005		Data from Local System	SideTwist has the ability to upload files from a compromised host.[1]
Enterprise	T1001		Data Obfuscation	SideTwist can embed C2 responses in the source code of a fake Flickr webpage.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	SideTwist can decode and decrypt messages received from C2.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	SideTwist can encrypt C2 communications with a randomly generated key.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	SideTwist has exfiltrated data over its C2 channel.[1]
Enterprise	T1008		Fallback Channels	SideTwist has primarily used port 443 for C2 but can use port 80 as a fallback.[1]

Domain	ID	Name	Use
Enterprise	T1083	File and Directory Discovery	SideTwist has the ability to search for specific files.[1]
Enterprise	T1105	Ingress Tool Transfer	SideTwist has the ability to download additional files.[1]
Enterprise	T1106	Native API	SideTwist can use `GetUserNameW`, `GetComputerNameW`, and `GetComputerNameExW` to gather information.[1]
Enterprise	T1082	System Information Discovery	SideTwist can collect the computer name of a targeted system.[1]
Enterprise	T1016	System Network Configuration Discovery	SideTwist has the ability to collect the domain name on a compromised host.[1]
Enterprise	T1033	System Owner/User Discovery	SideTwist can collect the username on a targeted system.[1]
