FALLCHILL, Software S0181 | MITRE ATT&CK®

Archived: 2026-04-05 17:10:32 UTC

Domain	ID		Name	Use
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	FALLCHILL has been installed as a Windows service.[2]
Enterprise	T1001	.003	Data Obfuscation: Protocol or Service Impersonation	FALLCHILL uses fake Transport Layer Security (TLS) to communicate with its C2 server.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	FALLCHILL encrypts C2 data with RC4 encryption.[1][2]
Enterprise	T1083		File and Directory Discovery	FALLCHILL can search files on a victim.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	FALLCHILL can delete malware and associated artifacts from the victim.[1]
		.006	Indicator Removal: Timestomp	FALLCHILL can modify file or directory timestamps.[1]
Enterprise	T1680		Local Storage Discovery	FALLCHILL can collect information about installed disks from the victim.[1]
Enterprise	T1082		System Information Discovery	FALLCHILL can collect operating system (OS) version information, processor information, and system name from the victim.[1]

Domain	ID	Name	Use
Enterprise	T1016	System Network Configuration Discovery	FALLCHILL collects MAC address and local IP address information from the victim.[1]

Source: https://attack.mitre.org/software/S0181/