ZIPLINE, Software S1114 | MITRE ATT&CK®

Archived: 2026-04-05 14:00:12 UTC

Domain	ID		Name	Use
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	ZIPLINE can use `/bin/sh` to create a reverse shell and execute commands.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	ZIPLINE can use AES-128-CBC to encrypt data for both upload and download.[2]
Enterprise	T1083		File and Directory Discovery	ZIPLINE can find and append specific files on Ivanti Connect Secure VPNs based upon received commands.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	ZIPLINE can add itself to the exclusion list for the Ivanti Connect Secure Integrity Checker Tool if the `--exclude` parameter is passed by the `tar` process.[1]
Enterprise	T1105		Ingress Tool Transfer	ZIPLINE can download files to be saved on the compromised system.[1][2]
Enterprise	T1095		Non-Application Layer Protocol	ZIPLINE can communicate with C2 using a custom binary protocol.[2]
Enterprise	T1057		Process Discovery	ZIPLINE can identify running processes and their names.[1]
Enterprise	T1090		Proxy	ZIPLINE can create a proxy server on compromised hosts.[1][2]

Domain	ID	Name	Use
Enterprise	T1205	Traffic Signaling	ZIPLINE can identify a specific string in intercepted network traffic, `SSH-2.0-OpenSSH_0.3xx.` , to trigger its command functionality.[1]

Source: https://attack.mitre.org/software/S1114