WIREFIRE, Software S1115 | MITRE ATT&CK®

Archived: 2026-04-05 17:44:13 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	WIREFIRE can respond to specific HTTP `POST` requests to `/api/v1/cav/client/visits`.[1][2]
Enterprise	T1554		Compromise Host Software Binary	WIREFIRE can modify the `visits.py` component of Ivanti Connect Secure VPNs for file download and arbitrary command execution.[1][2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	WIREFIRE can Base64 encode process output sent to C2.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	WIREFIRE can decode, decrypt, and decompress data received in C2 HTTP `POST` requests.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	WIREFIRE can AES encrypt process output sent from compromised devices to C2.[1]
Enterprise	T1105		Ingress Tool Transfer	WIREFIRE has the ability to download files to compromised devices.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	WIREFIRE is a web shell that can download files to and execute arbitrary commands from compromised Ivanti Connect Secure VPNs.[1]