reGeorg, Software S1187 | MITRE ATT&CK®

Archived: 2026-04-05 15:07:05 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	reGeorg can use HTTP to tunnel connections in and out of targeted networks.[1]
Enterprise	T1059	.006	Command and Scripting Interpreter: Python	reGeorg is a Python-based web shell.[2]
Enterprise	T1105		Ingress Tool Transfer	reGeorg has the ability to download files to targeted systems.[3]
Enterprise	T1095		Non-Application Layer Protocol	reGeorg can tunnel TCP sessions into targeted networks.[1]
Enterprise	T1572		Protocol Tunneling	reGeorg can tunnel TCP sessions including RDP, SSH, and SMB through HTTP.[1][4][5]
Enterprise	T1090		Proxy	reGeorg can establish an HTTP or SOCKS proxy to tunnel data in and out of a network.[2][1][4]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	reGeorg can be used to tunnel RDP connections.[1]
		.002	Remote Services: SMB/Windows Admin Shares	reGeorg has the ability to tunnel SMB sessions.[1]
		.004	Remote Services: SSH	reGeorg can communicate using SSH through an HTTP tunnel.[1]

Domain	ID		Name	Use
Enterprise	T1505	.003	Server Software Component: Web Shell	reGeorg is a web shell that has been installed on exposed web servers for access to victim environments.[4][5]

Source: https://attack.mitre.org/software/S1187