Solar, Software S1166 | MITRE ATT&CK®

Archived: 2026-04-05 18:44:02 UTC

Domain	ID		Name	Use
Enterprise	T1020		Automated Exfiltration	Solar can automatically exfitrate files from compromised systems.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Solar can Base64-encode and gzip compress C2 communications including command outputs.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Solar can XOR encrypt C2 communications.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Solar can send staged files to C2 for exfiltration.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Solar has the ability to delete staged files after they are uploaded to C2.[1]
Enterprise	T1105		Ingress Tool Transfer	Solar has the ability to download and execute files.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Solar can create scheduled tasks named Earth and Venus, which run every 30 and 40 seconds respectively, to support C2 and exfiltration.[1]
Enterprise	T1082		System Information Discovery	Solar can send basic information about the infected host to C2.[1]

Source: https://attack.mitre.org/software/S1166