LitePower, Software S0680 | MITRE ATT&CK®

Archived: 2026-04-05 18:22:48 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	LitePower can use HTTP and HTTPS for C2 communications.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	LitePower can use a PowerShell script to execute commands.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	LitePower can send collected data, including screenshots, over its C2 channel.[1]
Enterprise	T1105		Ingress Tool Transfer	LitePower has the ability to download payloads containing system commands to a compromised host.[1]
Enterprise	T1680		Local Storage Discovery	LitePower has the ability to list local drives.[1]
Enterprise	T1106		Native API	LitePower can use various API calls.[1]
Enterprise	T1012		Query Registry	LitePower can query the Registry for keys added to execute COM hijacking.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	LitePower can create a scheduled task to enable persistence mechanisms.[1]
Enterprise	T1113		Screen Capture	LitePower can take system screenshots and save them to `%AppData%`.[1]

Domain	ID		Name	Use
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	LitePower can identify installed AV software.[1]
Enterprise	T1082		System Information Discovery	LitePower has the ability to enumerate the OS architecture.[1]
Enterprise	T1033		System Owner/User Discovery	LitePower can determine if the current user has admin privileges.[1]

Source: https://attack.mitre.org/software/S0680