Calisto, Software S0274 | MITRE ATT&CK®

Archived: 2026-04-05 16:39:49 UTC

Domain	ID		Name	Use
Enterprise	T1098		Account Manipulation	Calisto adds permissions and remote logins to all users.[2]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	Calisto uses the `zip -r` command to compress the data collected on the local system.[1][2]
Enterprise	T1217		Browser Information Discovery	Calisto collects information on bookmarks from Google Chrome.[1]
Enterprise	T1136	.001	Create Account: Local Account	Calisto has the capability to add its own account to the victim's machine.[2]
Enterprise	T1543	.001	Create or Modify System Process: Launch Agent	Calisto adds a .plist file to the /Library/LaunchAgents folder to maintain persistence.[1]
Enterprise	T1555	.001	Credentials from Password Stores: Keychain	Calisto collects Keychain storage data and copies those passwords/tokens to a file.[1][2]
Enterprise	T1005		Data from Local System	Calisto can collect data from user directories.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Calisto uses a hidden directory named .calisto to store data from the victim’s machine before exfiltration.[1][2]

Domain	ID		Name	Use
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	Calisto uses a hidden directory named .calisto to store data from the victim’s machine before exfiltration.[1][2]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Calisto has the capability to use `rm -rf` to remove folders and files from the victim's machine.[1]
Enterprise	T1105		Ingress Tool Transfer	Calisto has the capability to upload and download files to the victim's machine.[2]
Enterprise	T1056	.002	Input Capture: GUI Input Capture	Calisto presents an input prompt asking for the user's login and password.[2]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Calisto's installation file is an unsigned DMG image under the guise of Intego’s security solution for mac.[1]
Enterprise	T1016		System Network Configuration Discovery	Calisto runs the `ifconfig` command to obtain the IP address from the victim’s machine.[1]
Enterprise	T1569	.001	System Services: Launchctl	Calisto uses launchctl to enable screen sharing on the victim’s machine.[1]

Source: https://attack.mitre.org/software/S0274