CookieMiner, Software S0492 | MITRE ATT&CK®

Archived: 2026-04-05 14:45:29 UTC

Domain	ID		Name	Use
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	CookieMiner has used a Unix shell script to run a series of commands targeting macOS.[1]
		.006	Command and Scripting Interpreter: Python	CookieMiner has used python scripts on the user's system, as well as the Python variant of the Empire agent, EmPyre.[1]
Enterprise	T1543	.001	Create or Modify System Process: Launch Agent	CookieMiner has installed multiple new Launch Agents in order to maintain persistence for cryptocurrency mining software.[1]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	CookieMiner can steal saved usernames and passwords in Chrome as well as credit card credentials.[1]
Enterprise	T1005		Data from Local System	CookieMiner has retrieved iPhone text messages from iTunes phone backup files.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	CookieMiner has used Google Chrome's decryption and extraction operations.[1]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	CookieMiner has used the `curl --upload-file` command to exfiltrate data over HTTP.[1]

Domain	ID		Name	Use
Enterprise	T1083		File and Directory Discovery	CookieMiner has looked for files in the user's home directory with "wallet" in their name using `find`.[1]
Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	CookieMiner has checked for the presence of "Little Snitch", macOS network monitoring and application firewall software, stopping and exiting if it is found.[1]
Enterprise	T1105		Ingress Tool Transfer	CookieMiner can download additional scripts from a web server.[1]
Enterprise	T1027	.010	Obfuscated Files or Information: Command Obfuscation	CookieMiner has used base64 encoding to obfuscate scripts on the system.[1]
Enterprise	T1496	.001	Resource Hijacking: Compute Hijacking	CookieMiner has loaded coinmining software onto systems to mine for Koto cryptocurrency. [1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	CookieMiner has checked for the presence of "Little Snitch", macOS network monitoring and application firewall software, stopping and exiting if it is found.[1]
Enterprise	T1539		Steal Web Session Cookie	CookieMiner can steal Google Chrome and Apple Safari browser cookies from the victim’s machine. [1]