CoinTicker, Software S0369 | MITRE ATT&CK®

Archived: 2026-04-05 16:05:30 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	CoinTicker executes a bash script to establish a reverse shell.[1]
		.004	Command and Scripting Interpreter: Unix Shell	CoinTicker executes a bash script to establish a reverse shell.[1]
		.006	Command and Scripting Interpreter: Python	CoinTicker executes a Python script to download its second stage.[1]
Enterprise	T1543	.001	Create or Modify System Process: Launch Agent	CoinTicker creates user launch agents named .espl.plist and com.apple.[random string].plist to establish persistence.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	CoinTicker decodes the initially-downloaded hidden encoded file using OpenSSL.[1]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	CoinTicker downloads the following hidden files to evade detection and maintain persistence: /private/tmp/.info.enc, /private/tmp/.info.py, /private/tmp/.server.sh, ~/Library/LaunchAgents/.espl.plist, ~/Library/Containers/.[random string]/[random string].[1]
Enterprise	T1105		Ingress Tool Transfer	CoinTicker executes a Python script to download its second stage.[1]

Domain	ID		Name	Use
Enterprise	T1027		Obfuscated Files or Information	CoinTicker initially downloads a hidden encoded file.[1]
Enterprise	T1553	.001	Subvert Trust Controls: Gatekeeper Bypass	CoinTicker downloads the EggShell mach-o binary using curl, which does not set the quarantine flag.[1]
