Dok, Software S0281 | MITRE ATT&CK®

Archived: 2026-04-05 14:29:10 UTC

Domain	ID		Name	Use
Enterprise	T1548	.003	Abuse Elevation Control Mechanism: Sudo and Sudo Caching	Dok adds `admin ALL=(ALL) NOPASSWD: ALL` to the `/etc/sudoers` file.[2]
Enterprise	T1557		Adversary-in-the-Middle	Dok proxies web traffic to potentially monitor and alter victim HTTP(S) traffic.[1][3]
Enterprise	T1547	.015	Boot or Logon Autostart Execution: Login Items	Dok uses AppleScript to install a login Item by sending Apple events to the `System Events` process.[2]
Enterprise	T1059	.002	Command and Scripting Interpreter: AppleScript	Dok uses AppleScript to create a login item for persistence.[1]
Enterprise	T1543	.001	Create or Modify System Process: Launch Agent	Dok installs two LaunchAgents to redirect all network traffic with a randomly generated name for each plist file maintaining the format `com.random.name.plist`.[1][3]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Dok exfiltrates logs of its execution stored in the `/tmp` folder over FTP using the `curl` command.[2]
Enterprise	T1222	.002	File and Directory Permissions Modification: Linux and Mac File and Directory	Dok gives all users execute permissions for the application using the command `chmod +x /Users/Shared/AppStore.app`.[3]

Domain	ID		Name	Use
			Permissions Modification	
Enterprise	T1056	.002	Input Capture: GUI Input Capture	Dok prompts the user for credentials.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Dok is packed with an UPX executable packer.[2]
Enterprise	T1090	.003	Proxy: Multi-hop Proxy	Dok downloads and installs Tor via homebrew.[1]
Enterprise	T1553	.004	Subvert Trust Controls: Install Root Certificate	Dok installs a root certificate to aid in Adversary-in-the-Middle actions using the command `add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /tmp/filename`.[1][2]

Source: https://attack.mitre.org/software/S0281/