XAgentOSX, Software S0161 | MITRE ATT&CK®

Archived: 2026-04-05 16:36:21 UTC

Domain	ID		Name	Use
Enterprise	T1071	.002	Application Layer Protocol: File Transfer Protocols	XAgentOSX contains the ftpUpload function to use the FTPManager:uploadFile method to upload files from the target system.[1]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	XAgentOSX contains the getFirefoxPassword function to attempt to locate Firefox passwords.[1]
Enterprise	T1083		File and Directory Discovery	XAgentOSX contains the readFiles function to return a detailed listing (sometimes recursive) of a specified directory.[1] XAgentOSX contains the showBackupIosFolder function to check for IOS device backups by running `ls -la ~/Library/Application\ Support/MobileSync/Backup/` .[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	XAgentOSX contains the deletFileFromPath function to delete a specified file using the NSFileManager:removeFileAtPath method.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	XAgentOSX contains keylogging functionality that will monitor for active application windows and write them to the log, it can handle special characters, and it will buffer by default 50 characters before sending them out over the C2 infrastructure.[1]
Enterprise	T1106		Native API	XAgentOSX contains the execFile function to execute a specified file on the system using the NSTask:launch method.[1]

Domain	ID	Name	Use
Enterprise	T1057	Process Discovery	XAgentOSX contains the getProcessList function to run `ps aux` to get running processes.[1]
Enterprise	T1113	Screen Capture	XAgentOSX contains the takeScreenShot (along with startTakeScreenShot and stopTakeScreenShot) functions to take screenshots using the CGGetActiveDisplayList, CGDisplayCreateImage, and NSImage:initWithCGImage methods.[1]
Enterprise	T1082	System Information Discovery	XAgentOSX contains the getInstalledAPP function to run `ls -la /Applications` to gather what applications are installed.[1]
Enterprise	T1033	System Owner/User Discovery	XAgentOSX contains the getInfoOSX function to return the OS X version as well as the current user.[1]
