MacMa, Software S1016 | MITRE ATT&CK®

Archived: 2026-04-05 15:10:48 UTC

Enterprise T1123 Audio Capture

MacMa has the ability to record audio.[3]

Enterprise T1059 .004 Command and Scripting Interpreter: Unix Shell

MacMa can execute supplied shell commands and uses bash scripts to perform additional actions.[1][3]

Enterprise T1543 .001 Create or Modify System Process: Launch Agent

MacMa installs a `com.apple.softwareupdate.plist` file in the `/LaunchAgents` folder with the `RunAtLoad` value set to `true`. Upon user login, MacMa is executed from `/var/root/.local/softwareupdate` with root privileges. Some variations also include the `LimitLoadToSessionType` key with the value `Aqua`, ensuring the MacMa only runs when there is a logged in GUI user.[1][3]

Enterprise T1555 .001 Credentials from Password Stores: Keychain

MacMa can dump credentials from the macOS keychain.[1]

Enterprise T1005 Data from Local System

MacMa can collect then exfiltrate files from the compromised system.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

MacMa has stored collected files locally before exfiltration.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

MacMa decrypts a downloaded file using AES-128-EBC with a custom delta.[1]

Enterprise T1573 Encrypted Channel

MacMa has used TLS encryption to initialize a custom protocol for C2 communications.[1]

Enterprise T1041 Exfiltration Over C2 Channel

MacMa exfiltrates data from a supplied path over its C2 channel.[1]

Enterprise T1083 File and Directory Discovery

MacMa can search for a specific file on the compromised computer and can enumerate files in Desktop, Downloads, and Documents folders.[1]

Enterprise T1070 .002 Indicator Removal: Clear Linux or Mac System Logs

MacMa can clear possible malware traces such as application logs.[1]

.004 Indicator Removal: File Deletion

MacMa can delete itself from the compromised computer.[1]

.006 Indicator Removal: Timestomp

MacMa has the capability to create and modify file timestamps.[1]

Enterprise T1105 Ingress Tool Transfer

MacMa has downloaded additional files, including an exploit for used privilege escalation.[1][3]

Enterprise T1056 .001 Input Capture: Keylogging

MacMa can use Core Graphics Event Taps to intercept user keystrokes from any text input field and saves them to text files. Text input fields include Spotlight, Finder, Safari, Mail, Messages, and other apps that have text fields for passwords.[3][4]

Enterprise T1680 Local Storage Discovery

MacMa can collect information about a compromised computer's disk sizes.[1]

Enterprise T1106 Native API

MacMa has used macOS API functions to perform tasks.[1][3]

Enterprise T1095 Non-Application Layer Protocol

MacMa has used a custom JSON-based protocol for its C&C communications.[1]

Enterprise T1571 Non-Standard Port

MacMa has used TCP port 5633 for C2 Communication.[1]

Enterprise T1057 Process Discovery

MacMa can enumerate running processes.[1]

Enterprise T1021 Remote Services

MacMa can manage remote screen sessions.[1]

Enterprise T1113 Screen Capture

MacMa has used Apple's Core Graphic APIs, such as `CGWindowListCreateImageFromArray`, to capture the user's screen and open windows.[1][3]

Enterprise T1553 .001 Subvert Trust Controls: Gatekeeper Bypass

MacMa has removed the `com.apple.quarantineattribute` from the dropped file, `$TMPDIR/airportpaird`.[1]

.002 Subvert Trust Controls: Code Signing

MacMa has been delivered using ad hoc Apple Developer code signing certificates.[5]

Enterprise T1082 System Information Discovery

MacMa can collect information about a compromised computer, including: Hardware UUID, Mac serial number, and macOS version.[1]

Enterprise T1016 System Network Configuration Discovery

MacMa can collect IP addresses from a compromised host.[1]

Enterprise T1033 System Owner/User Discovery

MacMa can collect the username from the compromised machine.[1]
