

OSX.DubRobber

Archived: 2026-04-06 02:01:54 UTC

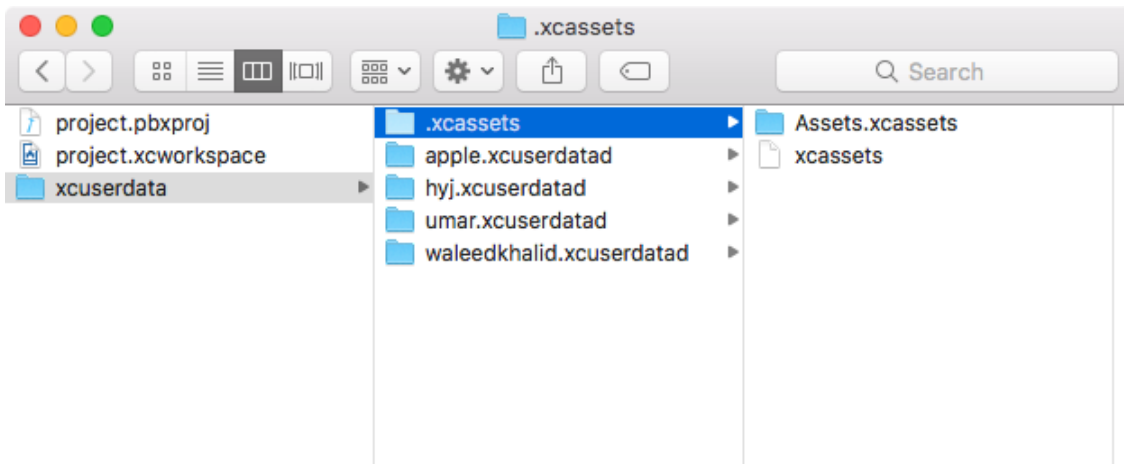


Short bio

OSX.DubRobber (aka XCSSET) is Malwarebytes' detection name for a versatile Trojan dropper that targets macOS systems.

Symptoms

OSX.DubRobber can be found in a hidden .xcassets folder. It downloads and installs other malware so the user may experience an unusually slow system.



Source and type of infection

OSX.DubRobber is a Trojan dropper that is almost entirely written in AppleScript, and downloads components on demand. OSX.DubRobber installs a very powerful backdoor, including all the usual backdoor functionalities, plus capabilities for grabbing data from apps like Telegram and Evernote, ransomware-like encryption and decryption, and more.

Protection

[Malwarebytes for Mac](#) detects and removes OSX.DubRobber.

Remediation

[Malwarebytes for Mac](#) will detect and remove the components of this malware.

Download and install the latest version of [Malwarebytes for Mac](#).

Click the “Scan Now” button to perform a system scan.

If threats are detected during the scan, a count of detected threats is displayed. More detailed threat information is displayed after the scan completes.

Click “Confirm” to move the detected threats to Quarantine.

If a restart is required to complete remediation of threats detected during a scan, you will be notified. When a restart is required, please remember to save all work before clicking “Restart”.

Source: <https://blog.malwarebytes.com/detections/osx-dubrobber/>