

# OSX.ThiefQuest | Malwarebytes Labs

Archived: 2026-04-05 14:34:54 UTC



## Short bio



OSX.ThiefQuest pretends to be ransomware

## Type and source of infection

OSX.ThiefQuest is believed to be a data stealer because of the presence of [keylogging and backdoor code](#) and there are possibly stolen data sent to a [C&C server](#). OSX.ThiefQuest was distributed as a Little Snitch installer available for download on a Russian forum dedicated to sharing torrent links.



## Aftermath

If files were encrypted it is highly doubtful they can actually be recovered. No email address was provided to contact the threat actor and the Bitcoin address is the same for every victim, making it hard to verify who has paid.

- Data/information about the system may have been stolen

## Protection

Malwarebytes for Mac detects and removes OSX.ThiefQuest.

## 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-thiefquest/>