Microsoft warns of new XCSSET macOS malware variant targeting Xcode d

Data: 2025-09-25 22:51:47

Autor: Inteligência Against Invaders

Microsoft Threat Intelligence reports that a new variant of the XCSSET macOS malware has been

detected in limited attacks, incorporating several new features, including enhanced browser targeting,

clipboard hijacking, and improved persistence mechanisms.

XCSSET is a modular macOS malware that acts as an infostealer and cryptocurrency stealer, stealing Notes, cryptocurrency wallets, and browser data from infected devices. The malware spreads by searching for and infecting other Xcode projects found on the device, so that the malware is executed when the project is built.

“The XCSSET malware is designed to infect Xcode projects, typically used by software developers, andrun while an Xcode project is being built,” explains Microsoft.

“We assess that this mode of infection and propagation banks on project files being shared among developers building Apple or macOS-related applications.”

In a new variant observed by Microsoft, researchers have noted several changes.

It now attempts to steal Firefox browser data by installing a modified build of the open-sourceHackBrowserData tool, which is used todecryptand exportbrowser data from browser data stores.

The new variant also includes a clipboard-hijacking component update that monitors the macOS clipboard for regular expression patterns associated with cryptocurrency addresses.

When a crypto address is detected, it will replace the address with one belonging to the attacker. This causes any cryptocurrency sent by the user on an infected device to be sent to the attackers instead.

[IMAGEM REMOVIDA]including zero-days.

Microsoft also recommends that developers always inspect Xcode projects before building them, especially when they have been shared with you by others.

[IMAGEM REMOVIDA]