

Security Update:[node:field_it_status_display_title]

Status Type

Security Update

Private

Public

Date and Time

Tuesday, November 3, 2015 - 15:55

Reason

Security Update

Impact

iPhone, iPad and iPod Touch Users

WHAT HAPPENED?

Just over a month ago, there were reports of a malware; XcodeGhost, targeting iPhone, iPad and iPod touch users. Recent reports indicate XcodeGhost has remained persistent and continues to be modified.

UCSF IT has been receiving reports of iOS devices using the UCSF network and connecting to malicious sites associated with the XcodeGhost malware.

Advanced users: For a complete description of the malware, refer to What You Need to Know About iOS Malware XcodeGhost - <http://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/> ^[1]

AFFECTED SYSTEMS:

- iPhone, iPad and iPod touch models running an iOS version compatible with any of the infected apps.
- The malware affects both stock and ?jail broken? devices.

HOW DOES XCODEGHOST PUT MY iOS DEVICE AT RISK?

- iOS apps infected with XcodeGhost malware may collect and encrypt sensitive information (e.g. Credentials, System Information, etc.) and then connects to Command and Control (C2) server to upload information.

HOW DO I PROTECT MY COMPUTER?

For iOS users:

- OS users should immediately uninstall any infected iOS app on their devices, or update to a newer version that has removed the malware.
- For a list of infected applications visit What You Need to Know About iOS Malware XcodeGhost - <http://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/> ^[1]
- Reset your iCloud password, and any other passwords inputted on your iOS device.

For iOS Developers:

- Install official versions of Xcode 7 or Xcode 7.1 beta from Apple's website for free and avoid downloading the software from unofficial sources.

RELATED LINKS

- **What You Need to Know About iOS Malware XcodeGhost** - <http://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/> ^[1]
- **XCodeGhost S: A New Breed Hits the US** - https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.... ^[2]
- **IT Security** at <http://it.ucsf.edu/security> ^[3]

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

[Site Login](#) [Site Index](#)

[Suggest an IT Improvement](#) | © UC Regents

* / -->

Source URL: <https://it.ucsf.edu/status/2015-11-03>

Links

[1] <http://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/>

[2] https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html

[3] <http://it.ucsf.edu/security>