XCodeGhost: the iOS haunting

XcodeGhost is an unofficial version of the iOS developer platform, Xcode. This compromised version was altered so that it injects malicious code into any app that was developed and compiled using it.

©Benjamin Haas via 123RF

How can an attacker use XcodeGhost?

Infected apps are capable of receiving commands from the attacker through the server to perform actions such as prompting a fake alert dialog to phish user credentials; hijacking or opening specific URLs based on their scheme, allowing exploitation of vulnerabilities in the iOS system or other iOS apps; reading and writing data in the user's clipboard, which could be used to read content such as the user's password if that password is copied from a password management tool to the clipboard. Reports from attacked users indicate that infected apps try to steal iCloud credentials using phishing attacks.

How did the Xcode developer platform become compromised?

The compromised version of Xcode is not found on iTunes, but can be downloaded elsewhere by developers who may find it hard to use iTunes to download the platform. For example, developers in China with low bandwidth to western hosted services by Apple may find other download sources for Xcode.

How does XcodeGhost work?

The injected code sends app info to a C&C server, allowing the infected app to read the device clipboard (meaning, any information copied by the user from any of the device interfaces or apps), to change browser info (create phishing websites) and more.

How am I affected by XCodeGhost?

Due to the fact that the XcodeGhost platform was uploaded to Chinese facing servers (baidu), the attack is most likely to happen on, but not limited to, apps developed and distributed in China. However, it's possible that Chinese developers working on apps for clients in other nations are affected, and could have published apps to the App Store that include malicious code without their knowledge. Apple has removed over 300 different apps from the App Store with this injected malicious code.

How can I protect myself against this malware?

If an app affected by this vulnerability is installed on an iOS device, Mobile Threat Prevention will detect the app, alert the user and enforce organisational policies to quarantine and protect the device. Threat prevention solutions, for example Check Point Mobile Threat Prevention, is designed to detect and stop malicious apps from being installed on mobile devices.