Cyber security updates

Keeping CISOs and CIO's confident about cyber security related issues including threat detection, data protection, breach readiness, security architecture, digital solutions and network security monitoring.

UnityGhost: the ghost adventure continues

06 October 2015

By Michael Yip, Cyber Threat Detection & Response at PwC

Apple iOS has long been purported to be the safest mobile operating system due to the closed access to the underlying source code, the restrictive design of the API and the rigorous review of mobile apps submitted for the App store. However, recent reports have emerged from China that some rogue versions of the Xcode development toolset have been found which inject malicious code (named XcodeGhost) into any apps compiled using the rogue toolset.

Although much have been reported on Xcode since, not much have been said about other mobile app development platforms. This report presents a high level overview of XcodeGhost as well as some of our findings on this threat including additional domains, cloned websites and an online persona we believe to be associated with this threat. We have also uncovered indications that Unity apps have also been compromised in a similar fashion – which is referred to as UnityGhost.

UnityGhost

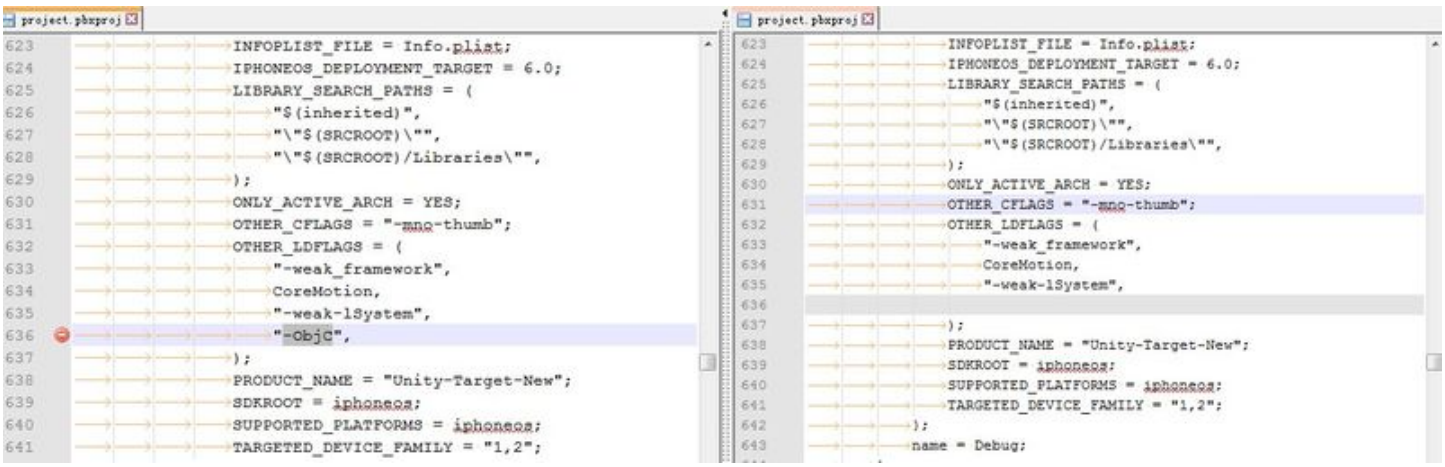
From the websites we have identified as associated with the threat actor (more details in our full report), we found evidence which suggests that the threat actor was interested in not just iOS but also Unity3D and Cocos2d-x. Therefore, we suspected that other app development frameworks may also have been targeted which could be a bigger problem than Xcode, as the Unity platform can be used to create apps for not just iOS but also Android, Windows and Wii.

Our suspicion was supported by a claim made by a user on Weibo, which states that some Unity apps have also been compromised[1] and the C2 domain `init.icloud-diagnostics[.]com` was also observed in conjunction with these applications:

Following the claim, the Baidu Security Team[2] examined some Unity platforms and they found that these were indeed modified in a similar way to XcodeGhost in that malicious code has been added to the framework to infect the generated apps.

More specifically, the attacker made modifications to the `libiPhone-lib-il2cpp.a` archive and added a file called `libiPhone-lib-il2cpp.a-arch-masterx.x.o`. To make sure that the additional file is loaded, the project manifest `project.pbxproj` had also been modified - this can be used to verify if the Unity platform being used has been tampered with.

Below is an image[3] which highlights the extra line `'-ObjC'` which is added in the malicious versions of Unity.



The affected archive file `libiPhone-lib-il2cpp.a` can be found in the following paths:

Mac OS	/Unity/Unity.app/Contents/PlaybackEngines/iossupport/Trampoline/Libraries/libiPhone-lib-il2cpp.a
Windows	Unity/Editor/Data/PlaybackEngines/iossupport/Trampoline/Libraries/libiPhone-lib-il2cpp.a

Download the Report

You can download the full report here:

Download CTO-TIB-20150925-01A

---

[1] http://www.weibo.com/1627825392/CBGopinKh?type=comment

[2] http://xteam.baidu.com/?p=351

[3] Source: http://xteam.baidu.com/?p=351

« Cyber security in engineering and construction | Main

Comments

Verify your Comment

Previewing your Comment

Posted by: |
This is only a preview. Your comment has not yet been posted.
Post Edit
Your comment could not be posted. Error type:
Your comment has been saved. Comments are moderated and will not appear until approved by the author. Post another comment
The letters and numbers you entered did not match the image. Please try again.
As a final step before posting your comment, enter the letters and numbers you see in the image below. This prevents automated programs from posting comments.
Having trouble reading this image? View an alternate.

Continue