

## **XcodeGhost, un gran número de apps del Apple Store ha sido comprometido.**

**by javier - Sábado, septiembre 26, 2015**

<http://memoriasdeunsysadmin.tk/2015/09/26/xcodeghost-un-gran-numero-de-apps-del-apple-store-ha-sido-comprometido/>

Especialistas en Seguridad detectaron Versiones modificadas(por terceros) del Ambiente de desarrollo de software de Apple, Xcode, el cual inyecta código a las apps construidas con dicha versión. Identificaron además las apps afectadas que ya existen en el AppStore de Apple y publicaron la lista el pasado 17 de Septiembre.

El malware fue nombrado XCodeGhost por agregar varias funciones ocultas a las apps infectadas que pueden ser confundidas con frameworks de análisis ya que recolectan todo tipo de información acerca del dispositivo y envía luego a un servidor remoto. De acuerdo a la información obtenida, el servidor remoto envía instrucciones que pueden abrir la appstore de una determinada app a voluntad.

De acuerdo con appthority, firma que se dedica a análisis de malware en dispositivos móviles y protección, este sería un caso de AdWare, más bien y NO de malwae, ya que hasta el momento, de todas las versiones del mismo que analizaron, no encontraron código que fuera más allá del comportamiento anteriormente citado. Debo decir que estoy muy en desacuerdo, por el gran potencial que tiene este "ataque" como exploit en el momento que el autor desee agregar código más dañino.

También hay que resaltar el impacto de este ataque. Si bien inicialmente se habló de no más de 40 apps afectadas, solo appthority ya identificó alrededor de 480 apps y no hay seguridad de que no hayan más.

---

memoriasdeunsysadmin.tk