News von Proofpoint

Angriff der Klonkrieger: Sicherheitsrisiko durch illegale Apps

DarkSideLoader verwendet Signierungszertifikate von Unternehmen für illegale App Stores

Die IT-Security-Experten von Proofpoint fanden auf mobilen Geräten von Angestellten Apps, die es im Apple App Store nicht gibt. Sie stammen aus einem illegalen Store, der eine Million kostenpflichtige Apps kostenlos zur Verfügung stellt. Dabei wird eine Methode genutzt, mit der Apps über einen Unternehmens-Store per „Sideloading“ auf Mitarbeitergeräten installiert werden.

Der illegale App Store

Angriff der Klonkrieger: DarkSideLoader verwendet betrügerische oder gestohlene Signierungszertifikate von Unternehmen zur Schaffung riesiger illegaler App Stores. Die Apps sind nicht von Apple geprüft und können Sicherheitsrisiken einführen, selbst auf iOS-Geräten ohne Jailbreak, was bisher nicht möglich war.

Die Story

Beim Scannen der Apps, die auf den Mitarbeitergeräten bei einem Enterprise-Kunden installiert sind, fanden IT-Sicherheitsexperten von Proofpoint eine Lego-Star-Wars-App, die es im App Store von Apple nicht gibt. Bei weiteren Untersuchungen stellte sich heraus, dass diese aus einem illegalen App Store mit einer Million unerlaubten Apps stammt. Darunter sind zahlreiche kostenpflichtige Apps, die hier kostenlos zur Verfügung gestellt wurden.

Die Anbieter missbrauchen eine Methode, mit der Unternehmen Apps über einen Unternehmens-App-Store per „Sideloading“ auf Mitarbeitergeräten installieren

Eskenzi PR Germany
fon + 49.241.43 53 74 84
Sabine Faltmann
faltmann@eskenzipr.com

können, die das Unternehmen selbst entwickelt hat. Diese Gruppe ermächtigt sich illegal der legitimen Zertifikate, die für diese Sideload-Apps genutzt werden, und erstellt damit einen ganzen App Store mit Raubkopien. Die geklonten Apps darin können auf den Geräten, auf denen sie installiert werden, ernsthafte Sicherheitsrisiken schaffen, da sie nicht die stringenten Sicherheitskontrollen von Apple bestehen mussten.

Die Botschaft für Verbraucher

Verbraucher sollten die Empfehlung von Apple beherzigen und nur Apps aus dem Apple App Store installieren. Das Installieren geraubter Apps, auch auf Geräten ohne Jailbreak, setzt die Geräte, Daten und Online-Accounts erheblichen Risiken aus.

Die Botschaft für Unternehmen

Unternehmen sollten auf den Geräten ihrer Nutzer gezielt nach geklonten Apps suchen. Wenn eine dieser Apps auf einem Gerät installiert wird, kann sie Zugriff auf die Unternehmensdaten erlangen, sie stehlen, das Mobilgerät zum Scannen des Netzwerks nutzen oder als Remote-Access-Trojaner innerhalb des Netzwerks agieren. Standard-Tools wie Enterprise-Mobilitätsmanagement-Lösungen bieten keine Information darüber, welche Apps als hochriskant einzustufen sind und welche Funktion die einzelnen Apps auf den Geräten haben.

383 Worte, 2666 Zeichen

Hier geht es zum Corporate Blog von Proofpoint mit dem ausführlichen Blog-Beitrag: http://www.proofpoint.com/de/darksideloader-illegale-appstores-haben-ios-gerate-jailbreak-abgesehen

Proofpoint Germany
Landsberger Straße 302
80687 München
www.proofpoint.com

KONTAKT
Monika Schaufler, Regional Director DACH
mschaufler@proofpoint.com