Lookout-Entdeckung: das Plug-in BeiTaAd

Zum Schutz und zur Beratung unserer Kunden erkennt und untersucht Lookout kontinuierlich neue Bedrohungen.

Hintergrund und Ablauf der Entdeckung

Ende 2018 entdeckten Lookout-Experten ein Werbe-Plug-in, das sich in einer Reihe beliebter Google Play-Apps versteckt hatte. Das Plug-in erzwingt die Anzeige von Werbung auf dem Sperrbildschirm, löst selbst im Ruhezustand des Handys Video- und Audiowerbung aus und zeigt appexterne Werbung an, die die Nutzung anderer Anwendungen auf dem Gerät beeinträchtigt. Insgesamt zählten die Experten 238 mit BeiTaAd verseuchte Anwendungen, die zusammen mehr als 440 Millionen Mal installiert wurden.

Das Wichtigste in Kürze

1. Bisher ungekanntes Maß an Verschleierung
2. Funktionsweise: Entschlüsselung einer in einer App versteckten Datei zum Laden und Speichern des Plug-ins
3. Keine Installation auf dem betroffenen Gerät; kann daher nur durch die Deinstallation der verseuchten App entfernt werden

Funktionen und betroffene Stellen

Dieses Plug-in macht Smartphones nahezu unbrauchbar. Anwender bekommen nicht sofort alle Werbeanzeigen zu sehen, erst rund 24 Stunden nach dem Start der betroffenen Anwendung. In manchen Fällen dauert es sogar bis zu zwei Wochen nach Anwendungsstart, bevor die Belästigung einsetzt. Seit seiner ersten Version 2018 wurde das Plug-in mehrmals überarbeitet. Neuere Varianten bestehen aus einer AES-verschlüsselten .dex-Datei, die sich als gutartige .renc-Datei ausgibt. Mit der Zeit wurden die Verschlüsselungs- und Verschleierungsmethoden zum Verbergen des Plug-ins immer raffinierter. Mittlerweile sind aktivitätsbezogene Zeichenketten XOR-verschlüsselt und Base64-kodiert. Beim Start einer verseuchten Anwendung wird ein SDK initialisiert, das den Ressourcenpfad zu BeiTaAd abruft. Daraufhin prüft es, ob die Adware entschlüsselt und geladen wurde, um sie dann auf dem Gerät zu speichern. Da BeiTaAd selbst nicht auf dem Gerät installiert wird, kann das Plug-in nur durch die Deinstallation der ursprünglich heruntergeladenen Trägeranwendung entfernt werden. Seit dem 23. Mai 2019 wurden die mehr als 230 betroffenen Google Play-Apps entweder von dort entfernt oder auf Versionen ohne BeiTaAd-Plug-in aktualisiert.

Erkennung BeiTaAd-ähnlicher Bedrohungen durch Lookout und Schutz

Im Fall von BeiTaAd deckten die Lookout-Experten den Einflussbereich des Plug-ins und seine im Lauf der Zeit immer ausgefeilteren Verschleierungsmethoden auf, indem sie mehrere Anwendungen unter die Lupe nahmen, die auf dem Startbildschirm Werbeanzeigen im Vollbildmodus präsentierten. Seit der Entdeckung von BeiTaAd sind dank Lookout bereits Hunderttausende Geräte vor der Adware geschützt worden. Dass andere Entwickler ähnliche Verschleierungstechniken anwenden werden, ist recht wahrscheinlich. Dieses Plug-in bietet daher einen Ausblick auf die Zukunft von Adware für Mobilgeräte.

Lookout Threat Advisory Service

So dynamisch, wie die Welt der mobilen Sicherheit nun einmal ist, verliert man schnell den Überblick. Der Lookout-Dienst Threat Advisory nutzt deshalb den enormen Datensatz aus dem globalen, Millionen Geräte umfassenden Lookout-Sensorennetzwerk und verknüpft ihn mit den Erkenntnissen seiner Top-Sicherheitsexperten, damit Sie alle nötigen Informationen bekommen, um angemessen auf die neuesten mobilen Bedrohungen und Risiken zu reagieren.