Découverte Lookout : plug-in BeiTaAd

Lookout découvre en permanence de nouvelles menaces pour protéger nos clients des attaques mobiles

Contexte et chronologie de la découverte

Fin 2018, les chercheurs de Lookout ont découvert que plusieurs applications populaires de Google Play contenaient un plug-in publicitaire judicieusement obfusqué. Ce plug-in impose l'affichage de publicités sur l'écran de verrouillage d'un utilisateur, déclenche la lecture de publicités vidéo et audio, même lorsque le téléphone est en veille, et affiche des publicités lorsqu'un utilisateur interagit avec d'autres applications sur son appareil. Les chercheurs ont identifié un total de 238 applications uniques contenant le plug-in BeiTaAd, avec plus de 440 millions d'installations cumulées.

Informations clés

1. Unique par la prévalence et le niveau d'obfuscation utilisé pour masquer son existence
2. Sert à déchiffrer un fichier masqué dans l'application pour charger et enregistrer le plug-in
3. N'est jamais installé sur l'appareil et ne peut être désinstallé sans supprimer l'application infectée

Fonctionnalités et parties concernées

Ce plug-in rend les téléphones quasi inutilisables. Les publicités n'assaillent pas directement l'utilisateur, mais commencent à apparaître environ 24 heures après le lancement de l'application, voire jusqu'à deux semaines plus tard. Le plug-in a été remanié plusieurs fois depuis sa version initiale en 2018. Cependant, les nouvelles itérations contiennent un fichier .dex AES chiffré qui se cache derrière un fichier .renc tout à fait anodin. Avec le temps, les techniques de chiffrement et d'obfuscation ont évolué pour masquer ce plug-in, notamment avec des chaînes de caractères associées à son activité utilisant un chiffrement XOR et un codage Base64. Lors du lancement d'une application, un kit de développement logiciel est démarré pour extraire le chemin d'accès vers l'archive dans laquelle se trouve BeiTaAd et le déchiffre avant de le stocker sur l'appareil. Le plug-in BeiTaAd n'est jamais installé sur l'appareil, donc il ne peut pas être supprimé sans désinstaller l'application principale que l'utilisateur a initialement téléchargée. Le 23 mai 2019, les 230 applications affectées sur Google Play ont été supprimées ou mises à jour vers des versions exemptes du plug-in BeiTaAd.

Comment Lookout détecte des menaces telles que le plug-in BeiTaAd et protège vos appareils

Dans le cas du plug-in BeiTaAd, plusieurs applications affichant des annonces sur l'écran d'accueil d'appareils mobiles ont fait l'objet d'une enquête qui a permis aux chercheurs de Lookout de découvrir toute l'étendue de ce plug-in et les efforts d'obfuscation mis en œuvre au fil du temps. Depuis que Lookout a commencé à détecter et à alerter la présence du plug-in BeiTaAd, des centaines de milliers d'appareils ont ainsi été protégés de cet adware. Cette famille de plug-in fournit des informations sur le développement futur des adwares mobiles et d'autres développeurs essaieront très probablement d'utiliser des techniques similaires pour déjouer tout système de détection.

Service Lookout Threat Advisory

Dans le monde en constante évolution de la sécurité mobile, être à l'affût de la moindre menace n'est pas de tout repos. Lookout Threat Advisory s'appuie sur l'immense ensemble de données provenant du réseau mondial de capteurs de Lookout, composé de millions d'appareils, qu'il associe à des informations que lui fournissent ses chercheurs chevronnés en sécurité pour vous donner des renseignements exploitables sur les dernières menaces et risques mobiles.