Smartphones et applications : cibles de choix pour les attaquants

La collecte et l'exploitation des données hébergées sur nos smartphones est un sujet qui revient régulièrement à la une des journaux, comme avec Whatsapp et son prochain changement de conditions d'utilisation. Objets indispensables du quotidien de la plupart de nos concitoyens, ceux-ci renferment une grande partie des données personnelles et confidentielles de leurs utilisateurs : photos/vidéos, SMS, historique de déplacement, courriels, jeux, etc.

Ces dernières sont toutes particulièrement intéressantes du point de vue des publicitaires, car elles mettent en lumière des habitudes de consommation. Le but final ? Servir la bonne publicité au bon moment, au bon endroit afin d'inciter à l'acte d'achat.

Un bon moyen pour un développeur de monétiser l'audience de son application est de mettre en place des bannières de publicité dans son application. Et pour cela, des sociétés proposent des boites à outils pre□tes à l'emploi, appelées SDK (Software Development Kit).

Concrètement, les SDK sont des outils d'aide à la programmation pour les développeurs afin de concevoir une application mobile, qui se présentent sous la forme de fragments de code.
Ces SDK publicitaires facilitent l'affichage des publicités, le suivi des clics des utilisateurs dans une application, mais aussi la collecte des données du téléphone.

Si la majorité des applications sont dotées de SDK qui ne posent pas de problème, il faut néanmoins se montrer vigilant vis à vis du traitement des données réalisé par ces logiciels.

SDK et données personnelles : attention au siphonage

Certaines des fonctionnalités sont légitimes pour un développeur car elles facilitent l'amélioration de son application ou sa partie monétisation. Toutefois, la question des données agrégées est souvent négligée. De plus en plus d'applications utilisent les SDK pour récupérer – sans demander clairement le consentement de l'utilisateur – la localisation, la liste des applications utilisées ou encore des données qui servent ensuite au ciblage publicitaire. Si ces données n'ont que peu d'intére□t lorsqu'elles sont prises une par une, elles prennent tout leur intére□t lorsqu'elles sont corrélées.

Dans certains cas, ces SDK peuvent également se révéler malveillants: récemment, Snyk une entreprise de cybersécurité américaine a dévoilé la nocivité d'un SDK publicitaire utilisé par plus de 1200 applications [(1)]. Dans ce cas, la société éditrice du SDK, sous couvert d'une activité légitime, pratiquait de la fraude publicitaire en favorisant les publicités de leur réseau pluto□t qu'un autre.

En plus de ces activités frauduleuses, la société, via le SDK, traquait les utilisateurs des applications en récupérant certaines données de navigation. Si cet exemple illustre un cas extre□me, il illustre

bien la capacité de collecte de ces SDK.

En réponse à ces pratiques abusives de plus en plus courantes, Apple a récemment décidé de s'attaquer au pistage des utilisateurs par les publicités dans les applications. Le nouveau système iOS 14 limite le suivi des déplacements et des actions des utilisateurs lorsqu'ils ouvrent une application. Cette mise à jour n'est évidemment pas du gou□t des régies publicitaires qui traquaient les utilisateurs à travers les différents périphériques (smartphone, tablette, ordinateur) et collectaient ainsi des milliers de données personnelles.

Régies publicitaire et SDK : des cibles privilégiées pour une attaque amplifiée

Les SDK constituent une cible intéressante pour les attaquants potentiels. En effet, une erreur de code peut aboutir à une faille, susceptible d'e□tre exploitée par une personne malveillante si elle est découverte. Un SDK est présent dans plusieurs applications. Pour un attaquant qui cherche à installer son malware sur le maximum de smartphones, chercher une faille dans un SDK pluto□t que dans une seule application permet de toucher un bien plus grand nombre d'utilisateurs.

De la me□me manière, une régie publicitaire est une cible particulièrement intéressante, car en cas de piratage, elle permet d'intercepter des informations et des données confidentielles ainsi que la possibilité d'atteindre des millions de cibles d'un coup. Dans le cas d'un attaquant étatique, celui-ci pourra ainsi choisir ses cibles selon leurs intére□ts ou espionner à distance des journalistes par exemple.

Pour d'autres attaquants, l'objectif sera de récolter un maximum de données personnelles. En effet, la masse de données facilitera la corrélation d'informations et la possibilité de les utiliser par la suite pour des attaques de type social engineering par exemple ou de les revendre au marché noir.

En résumé, le SDK ou la régie, facilite pour un individu malveillant l'amplification de son attaque pour toucher davantage de personnes.

Ne pas appliquer la politique du « j'accepte » par défaut

Comme le dit le célèbre adage « si c'est gratuit, c'est que vous e□tes le produit ».

Et me□me si beaucoup estiment n'avoir « rien à cacher », les données personnelles récoltées méritent que chacun y porte une attention particulière. Longtemps, la pédagogie en matière de protection des données personnelles a été ignorée non pas par négligence, mais parce que l'ampleur de l'impact de Facebook ou de Google sur la vie privée des internautes n'a pas clairement été comprise. Combien de fois avons-nous créé un compte sur un site ou une application en acceptant toutes les conditions d'utilisation sans égard aux données collectées ?

Aujourd'hui, la pédagogie doit continuer. Pour limiter la collecte des données personnelles sur le téléphone, quelques bonnes pratiques sont à adopter. Ainsi, chaque fois qu'une application

demande l'accès à une donnée personnelle, l'utilisateur doit se demander si celle-ci sera réellement utile ou s'il s'agit d'une fac□on de récupérer un maximum d'informations personnelles à son égard. Par exemple, une application de jeux a-t-elle vraiment besoin d'accéder au répertoire de contacts ?

D'autres mesures peuvent s'avérer efficaces : faites le tri des applications installées, supprimer celles qui ne sont pas utilisées, effacer régulièrement l'historique de navigation et désactiver la géolocalisation par défaut.

Plus les utilisateurs prendront ces réflexes, plus cela permettra à chacun de prendre conscience de l'ampleur de la collecte des données personnelles. Mais l'utilisateur n'arrive qu'au bout de la chai□ne. C'est à l'ensemble de l'écosystème d'e□tre particulièrement vigilant.

Tout d'abord, les développeurs d'applications qui sont encouragés à réaliser des audits poussés et vérifier que les SDK utilisés ne contiennent pas de manquement de sécurité. Puis, évidemment les développeurs du système d'exploitation responsables de la mise en place des mesures de sécurisation.

Les smartphones renferment une énorme quantité de données personnelles et confidentielles. Quels que soient l'identité, l'activité, les photos ou les fichiers de l'utilisateur, il est toujours possible de trouver le moyen d'en faire un usage malveillant en les revendant ou en usurpant l'identité de la personne concernée. C'est seulement au travers d'une prise de conscience générale qu'il sera possible de répondre aux enjeux de la protection des données personnelles.

(1) https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/