Étude sur les comportements intrusifs des applications Android et iOS

Bitdefender a lancé Clueful pour permettre aux utilisateurs d'appareils mobiles de savoir ce que font leurs applications avec leurs données personnelles. Un an plus tard, après avoir analysé plusieurs centaines de milliers d'applications, Bitdefender Clueful a constaté une tendance intéressante : **les applications sont tout aussi intrusives et indiscrètes sous iOS que sous Android, même si l'on peut affirmer que l'un des systèmes d'exploitation est plus sûr que l'autre.**

Depuis environ un an, Bitdefender recueille des applications sur Google Play et l'Apple Store afin de les analyser à la fois de manière statique et dynamique. **Pas moins de 314 474 applications gratuites Android et 207 843 applications iOS ont été analysées par Bitdefender Clueful**. Ces applications ont ainsi été passées au crible afin que les utilisateurs soient clairement informés du comportement de leurs applications : à quelles données essaient-elles d'accéder ? quels sont les privilèges requis ? comment sont gérées les données auxquelles elles accèdent au moment où ces données transitent sur Internet ?

Aperçu des permissions des applications

Avant d'aller plus loin, rappelons que les permissions des applications sont différentes d'un système d'exploitation à un autre. Ainsi, alors que les permissions Android sont présentées au moment de l'installation et ne peuvent pas être modifiées ultérieurement, les permissions iOS sont accordées lors de l'exécution, lorsque les propriétaires des appareils doivent autoriser ou refuser l'accès à différentes ressources, comme la localisation. Les applications pour Android et iOS ont toutefois en commun le fait de pouvoir interagir avec l'appareil de l'utilisateur ainsi qu'avec des services Internet tiers.

Données comparables

Notre analyse porte sur les comportements les plus intrusifs que les développeurs d'applications intègrent parfois dans leurs logiciels. Nous avons également considéré des comportements très proches à la fois sous Android et iOS :

1. Localisation

La localisation est une préoccupation majeure sous Android comme sous iOS. Son implantation et son utilisation sont en effet similaires sur les deux plates-formes et souvent demandées par les publicitaires via l'intégration de composants API (frameworks APIs) afin de connaître les

habitudes des utilisateurs. L'analyse de Bitdefender Clueful révèle que **45,41% des applications iOS intégraient des services de localisation, même si cela n'est pas nécessaire au bon fonctionnement de l'application**, **contre seulement 34,55% des applications Android.**

Exemples d'applications Android :

- **Latest Nail Fashon Trends** (v. 3.1) – com.nail.fashion.trends - avec une base d'utilisateurs estimée entre 100 000 et 500 000.

Exemples d'applications iOS :

- **PokerStars TV** (v. 2.2.2.0) - utilise la géolocalisation pour connaître l'emplacement exact de ses utilisateurs.
- **Cheezburger** (v. 1.2.2) - utilise la géolocalisation pour connaître l'emplacement exact de ses utilisateurs.

2. Lecture de la liste de contacts

Si seulement 7,69% des applications Android pouvaient accéder à la liste de contacts de votre appareil, les applications iOS se sont montrées beaucoup plus indiscrètes : 18,92% des applications conçues pour iOS étaient techniquement capables d'accéder à la liste de contacts.

Exemples d'applications Android :

- **Longman Contemporary English** (v. 1.81) - com.flexidict.data.longmancontemporary, retirée de Google Play.
- **Cambridge American Idiom** (v. 1.81) - com.flexidict.data2.cambridgeamericanidioms – retirée de Google Play.

Exemples d'applications iOS :

- **OLJ (**v. 1.1) - lit les noms de contacts et leurs adresses e-mail et les envoie à un serveur distant.
- **3D Badminton II** (v. 2.026) - lit les adresses e-mail des contacts et les envoie à un serveur à Hong Kong.

3. Transmission de votre adresse e-mail / identifiant de votre appareil

Les adresses e-mail et les identifiants uniques des appareils/IMEI constituent des informations extrêmement intéressantes pour un réseau publicitaire. Selon un récent rapport de la Federal Trade Commission, ces données peuvent également être partagées ou revendues à des tiers pour, par exemple, envoyer aux utilisateurs des publicités ciblées en fonction de leur comportement et profil.

14,58% des applications Android pouvaient divulguer l'identifiant de votre appareil et 5,73% transmettre votre adresse e-mail. De nouveau, les applications iOS semblent recueillir plus de données personnelles que celles conçues pour Android. Suite aux incidents de sécurité de 2012 concernant la mise en ligne d'un million d'UDID de l'agence publicitaire Blue Toad, Apple a décidé de déprécier l'API UDID.

Exemples d'applications Android divulguant des adresses e-mail :

- **Logo Quiz Car Choices** (v. 1.8.2.9) – car.logo.quiz.game.free – entre 100 000 et 500 000 installations.
- **Blowing sexy girl's skirt** (v. 1.6.0) – yong.app.blowskirt – entre 100 000 et 500 000 installations.

Exemples d'applications Android divulguant l'identifiant de l'appareil :

- **Football Games - Soccer Juggle** (v. 1.4.2) – com.madelephantstudios.BallTapp – entre 100 000 et 500 000 installations.
- **Logo Quiz NFL NHL MLB NBA MLS** (v. 1.0.2.8) – com.fesdra.logoquiz.ussport – entre 100 000 et 500 000 installations.

Exemples d'applications iOS divulguant l'identifiant de l'appareil :

- **Ringtone Maker** (v. 1.7) - envoie l'identifiant de l'appareil à "adfonic.net"
- **Paradise Island: Exotic** (v. 1.3.14) - envoie l'identifiant des appareils à des sites web tiers (à « offer.17bullets.com », « islandexotic.17bullets.com », « ma.mkhoj.com », « 1.trace.multiclick.ru », « a.jumptap.com », « soma.smaato.com »).

4. Divulgation de votre numéro de téléphone

Les numéros de téléphone sont le lien entre l'identité physique de l'utilisateur et la personne virtuelle. Cela permet à un tiers qui recueille des informations d'établir une corrélation entre les données relatives au comportement des utilisateurs dans les applications (quel contenu les intéresse, quelles applications ont-ils installées, etc.) et éventuellement, d'y associer une personne existante, désignée par un prénom et un nom. 8,82% des applications analysées par Bitdefender Clueful pour Android pouvaient divulguer le numéro de téléphone d'un appareil à des publicitaires tiers. Les applications intégrant les frameworks AirPush et (dans certaines circonstances) LeadBolt permettent au développeur de recueillir, de crypter et d'envoyer le numéro de téléphone de l'appareil. Dans certains pays, les opérateurs bloquent cette possibilité afin de protéger les données des utilisateurs.

Exemples d'applications essayant de divulguer des numéros de téléphone :

- **Football Games - Soccer Juggle** (v. 1.4.2) – com.madelephantstudios.BallTapp – entre 100 000 et 500 000 installations.
- **Button Football (Soccer)** (v. 1.10.3) – com.sicecommentr.buttonfootball – entre 1 000 000 et 5 000 000 d'installations.

L'une des principales différences d'Android est que ce système ouvert permet aux utilisateurs d'installer leurs applications à partir de plates-formes tierces et également de télécharger les fichiers APK directement sur les sites web des développeurs. Ces applications échappent donc au système de sécurité mis en place par Google sur Google Play (Google Bouncer), et peuvent ainsi recueillir bien plus de données que nécessaires pour leur bon fonctionnement.

Les zones d'ombre dans le comportement des applications

Si l'accès à des données de localisation peut être utilisé de façon légitime par certaines applications, l'envoi de ces informations sur Internet n'est pas indispensable pour toutes et peut présenter des risques pour les utilisateurs si l'entreprise qui récolte leurs informations est victime par la suite d'une violation de données. Cela constitue typiquement une zone d'ombre, lorsque des informations qui ne sont pas indispensables au fonctionnement d'une application sont récupérées simplement pour compléter les données des utilisateurs dont on dispose déjà.

Environ 10% des applications Android analysées peuvent se comporter ainsi, en ayant ou non informé l'utilisateur au préalable, selon leur SDK et leur configuration au démarrage initial. D'autres applications, qui envoient des informations de localisation, divulguent également le numéro de téléphone et l'adresse e-mail des utilisateurs à des publicitaires.

Le comportement négligent et malveillant des applications

Si la localisation, l'accès aux contacts ou l'interaction avec les sites de réseaux sociaux, peuvent être nécessaires à certaines fonctionnalités, d'importantes menaces sont la conséquence de mauvaises implémentations de technologies, telles que les protocoles pour l'envoi de données de l'appareil des utilisateurs vers le cloud. Par exemple, transmettre des identifiants d'appareils non cryptés ou envoyer des mots de passe lors du processus d'authentification est extrêmement dangereux pour un appareil mobile qui est souvent connecté à des points d'accès Wi-fi publics qui peuvent être surveillés.

Conclusion

Si l'on en croit un vieux proverbe, si vous ne payez pas, c'est que c'est vous le produit. Il existe en effet un écosystème d'applications gratuites pour l'utilisateur, mais il est largement monétisé par les développeurs. En d'autres termes, l'application ne devient gratuite qu'une fois que l'utilisateur « paye » avec ses données personnelles. La situation est même pire puisque payer l'application ne bloque pas le flux d'informations confidentielles et ne renvoie pas non plus à l'utilisateur ses données privées déjà stockées dans des fichiers. De plus, la collecte de données est faite sans que l'utilisateur ait connaissance des autorisations données lors de l'installation de l'application.

Le modèle financé par la publicité existe depuis la création d'Internet et a fortement contribué au développement du Web tel que nous le connaissons. Des sources ont participé à des campagnes publicitaires à travers le monde afin de payer le trafic et de permettre de distribuer le contenu gratuitement aux utilisateurs.

Les adwares mobiles sont totalement différents car ils s'intègrent étroitement aux appareils ; ils ne s'exécutent pas au sein du navigateur, isolés des autres applications. Sur les appareils mobiles, les composants publicitaires peuvent connaître vos habitudes de communication, vos amis, les contacts de vos amis, l'endroit où ils se trouvent et, en général, tout cela à la fois. On peut donc les considérer comme des logiciels espions, intégrés à l'appareil que vous utilisez le plus pendant la journée.

La mission de Bitdefender Clueful consiste à rendre plus transparent l'écosystème des applications pour l'utilisateur et de leur donner une information compréhensible concernant les menaces auxquelles ils s'exposent à l'installation d'une banale application.