Chapitre 8 :

Android et logiciels malveillants pour Android

Android est un système d'exploitation pour les appareils mobiles. Il s'agit de l'une des deux principales options de système d'exploitation, le système iOS d'Apple étant son principal concurrent[1]. Si vous voulez en savoir plus sur Android et son lien avec le projet open source Android, l'article de Wikipédia pourra vous être utile.

Veuillez noter que les exercices de ce chapitre nécessitent que vous ayez accès à un téléphone Android. N'importe quel téléphone fera l'affaire, y compris votre propre appareil personnel. Il ne vous sera pas demandé d'apporter des modifications au téléphone. Si vous n'avez pas accès à un tel téléphone et que vous souhaitez tout de même réaliser les exercices, il est possible d'installer une version machine virtuelle d'Android dans VirtualBox, bien que cela soit un peu délicat.

Versions d'Android et remarque concernant Google

Au moment de la rédaction du présent document, ce contenu était à jour. Cependant, Google, qui développe Android, met continuellement à jour le système d'exploitation. En général (mais pas toujours !) ces mises à jour améliorent la confidentialité et la sécurité ainsi que votre capacité à contrôler les paramètres de sécurité et de confidentialité. Gardez cela à l'esprit lorsque vous lisez ce texte, surtout si vous le lisez longtemps après sa dernière mise à jour. Pour connaître les dernières mises à jour, vous pouvez consulter le site officiel d'Android et son guide du développeur.

N'oubliez pas non plus qu'une grande partie de l'apparence externe d'Android peut varier grandement entre les téléphones, même lorsque les téléphones utilisent la même version d'Android. Parfois, la façon dont les choses fonctionnent « sous le capot » peut également varier. Il est possible que les éléments abordés dans ce chapitre soient légèrement différents sur le téléphone que vous utilisez, bien qu'ils aient été testés sur divers téléphones.

Il faut également garder à l'esprit que ce chapitre est consacré aux applications malveillantes et qu'il a été écrit en supposant que Google ne fait pas partie du modèle de menace de l'utilisateur. Si vous ne sauvegardez pas vos données sur le cloud de Google, Google ne peut pas lire les messages Signal ou WhatsApp. Cependant, Google peut voir quelles applications vous avez installées sur votre téléphone et pourrait être obligé de remettre ces données aux autorités.

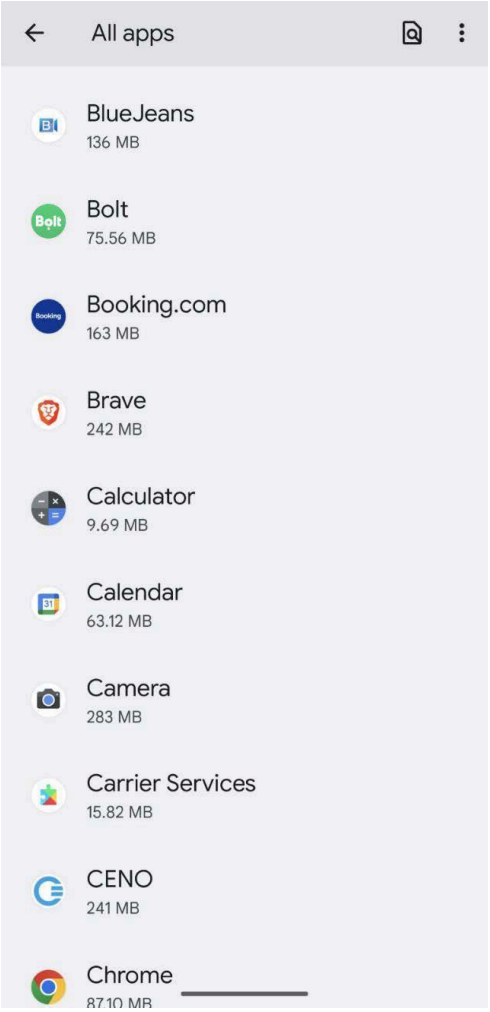
Quelle est la probabilité de tomber sur un logiciel malveillant Android ?

Les logiciels malveillants pour Android sont réels et c'est certainement quelque chose que toute organisation de la société civile devrait inclure dans son modèle de menace. Ce chapitre vous aide à analyser les appareils Android pour détecter des applications potentiellement malveillantes.

[1] Ils ne fonctionnent pas sur les mêmes appareils : un iPhone ne peut pas fonctionner avec Android et un téléphone conçu pour Android ne peut pas exécuter iOS

Cependant, avant de commencer, il peut être judicieux de considérer dans quelle mesure les logiciels malveillants Android sont probables. Les logiciels malveillants pour Android, bien que plus courants que ceux visant iOS, sont relativement rares. Les logiciels malveillants Android les plus courants sont ceux qui se livrent à des fraudes publicitaires et ont relativement peu d'impact sur l'appareil[2].

Cela est dû à la façon dont les applications Android fonctionnent. Il n'est pas facile de faire installer une application malveillante par un utilisateur, surtout si le cybercriminel veut qu'une personne spécifique l'installe. Si le cybercriminel n'exploite pas les vulnérabilités du système d'exploitation Android (ce qui est rare et peut nécessiter une grande sophistication technique), les applications installées sont limitées dans ce qu'elles peuvent faire. Donc, avant de conclure qu'il y a des logiciels malveillants sur un appareil Android, il est utile d'envisager d'autres options (par exemple, un compte compromis par un mot de passe volé), en particulier si l'action commise par l'intervenant suspecté ne semble pas suffisamment sophistiquée pour être une campagne de logiciel malveillant.



Question 8.1. Une journaliste reçoit un e-mail anonyme indiquant que l'expéditeur sait qu'elle se trouvait dans un bar particulier la nuit dernière. C'était effectivement le cas. Elle trouve donc l'e-mail assez troublant, ce qui est compréhensible. Avec cette seule information, pensez-vous vraiment qu'un logiciel malveillant installé sur son téléphone a probablement partagé sa localisation ? (Consultez l'annexe pour connaître la réponse.)

Applications et autorisations Android

Les programmes sur Android sont généralement appelés « applications ». En tant qu'utilisateur d'Android, vous connaissez certaines applications que vous utilisez régulièrement et qui ont des icônes sur votre écran d'accueil, mais il y a également des applications que vous connaissez moins, comme les applications installées par le fabricant du téléphone (Samsung, HTC, Huawei, etc.) ou les applications système qui fournissent certaines fonctionnalités tout en étant cachées à l'utilisateur.

Pour des raisons de confidentialité et de sécurité, le système d'exploitation Android utilise les autorisations pour limiter les ressources que les applications peuvent utiliser. Par exemple, une application ne peut pas accéder aux contacts stockés sur le téléphone sans avoir obtenu la permission de le faire.

[2] Cliquer sur les annonces en arrière-plan ou afficher un grand nombre d'annonces à l'utilisateur

À l'exception possible de certains logiciels malveillants très avancés (plus d'informations seront disponibles dans un chapitre ultérieur), cela est également vrai pour les applications malveillantes, qu'elles soient installées à partir de Google Play ou **chargées indépendamment** sur le téléphone[3].

Il est possible de voir les autorisations accordées à une application en parcourant les paramètres et en cherchant l'application individuelle dans la liste des applications. Cela peut vous aider à déterminer si une application suit, par exemple, votre position ou écoute vos conversations : elle aura besoin de votre permission pour le faire.

Une façon naturelle de rechercher des applications malveillantes sur un téléphone Android serait donc de parcourir toutes les applications installées (les paramètres du téléphone vous permettent de le faire) et de voir si l'une d'elles a des autorisations inhabituelles. Cette approche présente certains inconvénients :

- Un téléphone comprend facilement plus de 100 applications installées. Parcourir l'ensemble de ces applications peut donc prendre beaucoup de temps.
- Les applications malveillantes se font souvent passer pour quelque chose de totalement innocent (comme une application de calculatrice), et vous pourriez ne pas les voir lors d'un contrôle des applications.
- Il y a de nombreuses applications installées sur les téléphones Android dont les propriétaires n'ont jamais entendu parler, généralement parce qu'elles sont fournies avec le système d'exploitation. Les utilisateurs deviennent parfois anxieux lorsqu'ils voient ces applications (« Mon téléphone a une application de navigation. Je n'ai même pas de voiture ! Ce doit être un logiciel espion. »)

  Une approche très différente consiste à connecter le téléphone à un PC et à scanner le téléphone avec un logiciel spécialement conçu pour détecter les logiciels malveillants. Cela peut s'avérer utile dans certains cas, mais il y a aussi des inconvénients :

- Il faut que l'analyste ait un accès physique au téléphone, alors que la plupart des services d'assistance sont fournis à distance.
- Elle place la barre de l'analyse assez haute en termes d'outils, de connaissances et d'expérience. Bien que la plupart des problèmes puissent être détectés par l'utilisateur du téléphone s'il est guidé à travers les étapes nécessaires, ces outils avancés sont moins accessibles pour les utilisateurs de base.
- Peu de gens, et certainement pas les personnes présentant un risque élevé, feront confiance à un tiers pour qu'il connecte leur téléphone à son ordinateur.

Une meilleure approche : examiner les autorisations des applications

Il existe cependant une meilleure approche, à savoir l'utilisation du gestionnaire d'autorisations disponible dans les paramètres du téléphone Android. Cette fonctionnalité

[3] Le chargement indépendant est l'acte d'installation des applications en dehors de la boutique officielle, dans ce cas Google Play. Il est possible sur Android, mais nécessite que l'utilisateur clique pour confirmer certains avertissements. Cela nécessite donc un minimum d'ingénierie sociale pour qu'un cybercriminel obtienne un accès de courte durée à l'appareil déverrouillé.

montre la plupart[4] des autorisations que les applications peuvent demander et quelles applications ont reçu quelles autorisations. Dans certains cas, elle montre également une certaine granularité pour l'autorisation.

Par exemple, si vous craignez qu'une application malveillante installée sur le téléphone écoute le microphone, vous pouvez consulter les applications qui ont obtenu cette autorisation et vérifier si elles sont légitimes. Notez que, malheureusement, même les applications légitimes demandent parfois trop d'autorisations. Le fait qu'une application de lampe de poche demande l'accès à votre emplacement ne signifie pas automatiquement qu'il s'agit d'un logiciel malveillant, même si vous ne voudrez probablement pas lui accorder cette autorisation.

La meilleure façon de procéder est de rechercher le gestionnaire des autorisations dans les paramètres, puis de vérifier les autorisations individuelles.

Pour savoir si la demande d'autorisation d'une application constitue un problème, considérez la façon dont vous utilisez habituellement l'application. Si vous utilisez l'emplacement, le microphone, les SMS, les contacts et les fichiers avec cette application, les autorisations peuvent être raisonnables. Lorsque vous n'utilisez pas ces autorisations avec une application, l'utilisation de ces parties de votre appareil peut signifier que quelque chose ne va pas. Dans ce cas, recherchez les demandes d'autorisation inattendues.

Le but ici n'est pas de comprendre complètement ce que font les applications, mais de limiter votre enquête à un petit nombre (parfois zéro) d'applications inconnues que vous voudrez peut-être examiner plus en détail. En prime, vous découvrirez également quelles applications légitimes nécessitent des autorisations que vous ou la personne à qui appartient le téléphone ne considérez pas comme étant justifiées. Vous devriez pouvoir désactiver ces autorisations.

Parfois, il est impossible de changer les autorisations d'une application préinstallée (le site officiel d'Android fournit quelques informations[wayback machine] à ce sujet. Étant donné que les utilisateurs sont généralement moins familiers avec ces applications préinstallées, ils peuvent soupçonner qu'elles sont de nature malveillante. Si vous ne connaissez pas ce téléphone, vous devrez peut-être faire des recherches sur ces applications pour comprendre leur fonctionnement et pour rassurer l'utilisateur (et vous rassurer vous-même).

Localisation

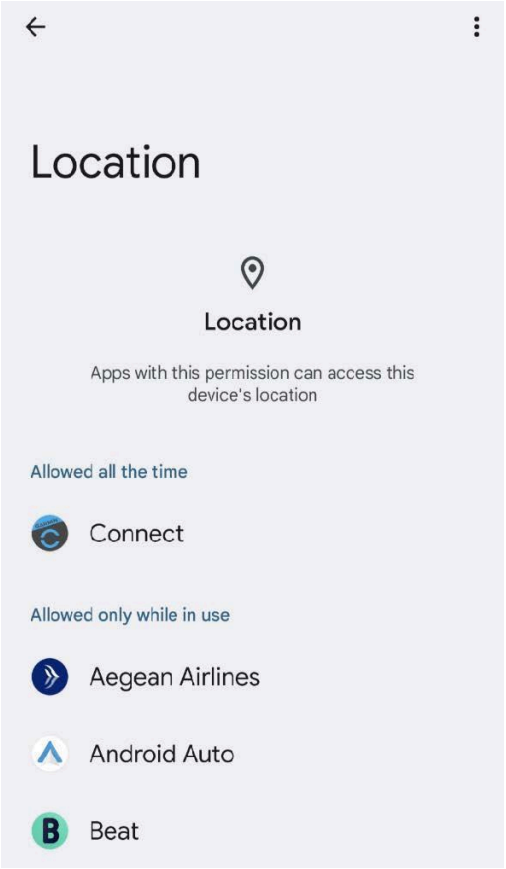
Les applications qui ont obtenu cette autorisation peuvent accéder à la localisation GPS du téléphone. Les applications de navigation et de covoiturage en sont des exemples évidents : elles ont besoin de l'emplacement de l'appareil pour fonctionner correctement.

Une application peut avoir accès à l'emplacement en permanence ou uniquement lorsque l'application est utilisée. Elle peut aussi être forcée de demander l'autorisation chaque fois qu'elle est utilisée. Les applications qui font des choses secrètement, comme les logiciels espions, demanderont probablement d'avoir une autorisation permanente. Faites particulièrement attention aux applications qui ont reçu ce type d'autorisations !

La question de savoir si les entreprises derrière ces applications peuvent et doivent être fiables concernant vos données dépasse le cadre de ce chapitre. Cependant, peu importe si

[4] Certaines autorisations sont très obscures et peu pertinentes dans ce contexte. Deux autres approches sont discutées plus loin dans le chapitre.

vous faites confiance aux entreprises concernées, il existe plusieurs façons pour les cybercriminels d'accéder aux données de localisation obtenues par les applications.



La façon la plus évidente est d'avoir accès au téléphone et donc à l'application elle-même, ou à un compte en ligne correspondant qui offre la possibilité de consulter l'historique des emplacements. Google, par exemple, permet cette fonction pour Google Maps. Un cybercriminel peut également faire des demandes légales pour obtenir ces données par le biais d'une assignation à comparaître.

Si vous voulez donc évaluer si les données de localisation d'une personne sont sûres, vous devriez examiner dans quelle mesure il est facile pour cette personne (et donc pour toute personne qui se fait passer pour elle) d'accéder à l'historique des emplacements et comment la société répond aux demandes de données. De nombreuses grandes entreprises publient des rapports de transparence.

Quoi qu'il en soit, pour la plupart de ces applications, il devrait être acceptable de définir l'autorisation uniquement lorsque l'application est utilisée ou de demander l'autorisation à chaque utilisation. Cela signifie que l'application n'aura pas accès aux données de localisation en permanence.

Enfin, notez que le GPS est très précis. Il peut indiquer un emplacement avec une précision de 30 cm (environ 1 pied). Dans certains cas, une personne peut s'inquiéter de la fuite de sa localisation grossière, par exemple, dans quelle ville ou quel pays elle se trouve. Ces informations peuvent être divulguées de plusieurs façons explicites (par exemple, par l'intermédiaire de l'adresse IP) et parfois aussi implicites (par le biais d'informations partagées publiquement). La façon d'éviter que cela se produise est très difficile et hors de la portée de ce chapitre.

Microphone

Les applications qui ont obtenu cette autorisation peuvent accéder à votre microphone et ainsi enregistrer tout ce que vous dites, ainsi que les sons ambiants.

Il existe de nombreuses raisons légitimes pour que les applications utilisent cette fonctionnalité, par exemple, les applications qui vous permettent d'envoyer des messages vocaux, les applications qui enregistrent des vidéos ou celles auxquelles vous pouvez accéder via des commandes vocales.

Comme l'autorisation de localisation, l'accès au microphone peut être accordé en permanence, uniquement lorsque l'application est en cours d'exécution ou chaque fois l'application est utilisée. Il n'y a pas beaucoup de bonnes raisons pour qu'une application ait

cette autorisation en permanence. Une application qui a obtenu cette autorisation devrait être un signal d'alerte.

SMS

Une application qui a reçu l'autorisation de lire les messages SMS peut espionner ces derniers. Si l'utilisateur utilise activement les SMS pour communiquer, cela peut représenter un problème dans le cas des logiciels espions.

Cependant, les SMS sont également utilisés pour l'authentification multifactorielle, de sorte qu'une application ayant accès aux SMS peut lire en toute tranquillité les codes envoyés par ce biais[5]. Dans ce contexte, certaines applications utilisent les SMS pour confirmer le numéro de téléphone de l'appareil et demandent cette autorisation afin d'éviter que l'utilisateur saisissent les codes manuellement. Cette autorisation peut donc être utilisée de manière malveillante par une application qui veut se faire passer pour l'utilisateur.

L'application par défaut du téléphone a naturellement cette autorisation, ainsi que d'autres applications qui peuvent être utilisées pour traiter les SMS, comme Signal.

Étant donné que les SMS arrivent en arrière-plan, les applications ayant accès aux SMS auront besoin de cette autorisation en permanence. Il n'est pas possible d'accorder cette autorisation uniquement lorsque l'application est en cours d'exécution ou à chaque utilisation.

Contacts

Les applications ayant cette autorisation peuvent accéder aux contacts du téléphone. Cette autorisation est également utilisée par les applications téléphoniques elles-mêmes, par exemple par les applications de messagerie telles que Signal et WhatsApp qui identifient les utilisateurs en fonction de leurs numéros de téléphone. Les contacts comprennent généralement des numéros de téléphone, mais selon la façon dont le téléphone est utilisé, ils peuvent également inclure des adresses e-mail. Pour de nombreux utilisateurs à risque élevé, la liste de contacts est une information très sensible.

Comme pour les SMS, cette autorisation est soit permise de façon permanente, soit refusée.

Fichiers

Cette autorisation donne aux applications l'accès aux fichiers stockés sur l'appareil. Les gestionnaires de fichiers ou les produits de sécurité sont des exemples d'applications légitimes nécessitant cette autorisation. L'autorisation d'accès aux fichiers a beaucoup changé dans les versions récentes d'Android et devient plus granulaire. Si vous voulez rechercher une application malveillante, au moins initialement, il est préférable de supposer que si l'application a la permission d'accéder aux fichiers, elle peut accéder à n'importe quel fichier stocké sur l'appareil.

Notez que cela ne donne pas aux applications accès aux discussions de Signal, WhatsApp, etc.

---

[5] C'est l'une des raisons pour lesquelles l'utilisation des SMS pour l'authentification multifactorielle est moins sûre que les autres options, telles qu'une application d'authentification ou un jeton matériel

Cette autorisation est également accordée de façon permanente ou refusée

Exercice 8.2. Pour chacune des cinq autorisations énumérées, vérifiez sur un téléphone Android quelles applications ont obtenu cette autorisation.

Exercice 8.3. Le gestionnaire d'autorisations sur Android énumère plus que ces cinq permissions. Examinez les autres autorisations et imaginez leur utilisation par des logiciels malveillants.

Il existe deux types d'autorisations qui sont listées séparément, car elles ne se trouvent pas dans le gestionnaire des autorisations : l'accessibilité et les notifications. Elles sont toutefois très pertinentes, car elles sont souvent utilisées de façon abusive par les applications malveillantes. La façon dont ces paramètres peuvent être accessibles varie selon les téléphones : si vous ne pouvez pas les trouver facilement dans le menu Confidentialité dans les Paramètres, utilisez la fonction de recherche dans les Paramètres.

Accessibilité

L'accessibilité rend les applications d'un téléphone plus accessibles pour les personnes ayant certains handicaps, par exemple en leur permettant de s'intégrer aux lecteurs d'écran. Une application enregistrée en tant que service d'accessibilité est capable de contrôler le téléphone dans une certaine mesure : elle peut cliquer sur des boutons, s'enregistrer lorsqu'un bouton est utilisé, remplir des formulaires de texte ou enregistrer ce qui a été rempli dans les formulaires.

Plusieurs applications légitimes qui ne fournissent pas de services aux personnes handicapées s'inscrivent tout de même comme un service d'accessibilité. Un exemple est celui des gestionnaires de mots de passe, qui exigent que cette fonctionnalité remplisse les mots de passe stockés dans les applications.

Vous pouvez trouver les applications enregistrées comme service d'accessibilité en recherchant « Accessibilité » dans les paramètres du téléphone, puis en recherchant les services installés.

Notez qu'à partir d'Android 13, sorti en août 2023, seules les applications installées via Google Play seront autorisées à demander des autorisations d'accessibilité.

Notifications

Les notifications sont des fenêtres contextuelles que vous recevez sur votre téléphone lorsque vous recevez un nouveau message ou en cas d'alerte. Les notifications que vous recevez dépendent des paramètres de chaque application.

Les applications peuvent demander l'accès aux notifications, ce qui signifie qu'elles peuvent consulter toutes les notifications et les applications qui les ont envoyées. Une application qui synchronise un téléphone avec une montre connectée et affiche des notifications est un exemple d'application légitime nécessitant l'accès aux notifications.

Un logiciel malveillant peut utiliser et utilise parfois cette fonctionnalité pour espionner les

activités de l'utilisateur, même si les notifications ne montrent que les messages entrants, pas les messages sortants.

Exercice 8.4. Comme auparavant, vérifiez sur votre téléphone Android les applications auxquelles vous avez accordé des autorisations de notification et d'accessibilité.

Analyse des logiciels malveillants Android et des logiciels malveillants avancés Android

Dans le chapitre précédent, vous avez appris comment utiliser VirusTotal pour obtenir des informations sur les logiciels malveillants via l'utilisation en pivot. Par exemple, vous pouvez constater qu'un logiciel malveillant Android se connecte à un certain domaine auquel un autre logiciel malveillant qui a été analysé se connecte également. Cela suggère que le fichier que vous analysez peut être une version différente de ce logiciel malveillant, bien qu'il y ait, comme toujours, beaucoup de mises en garde à prendre en compte.

Il y a également apklab, un service fourni par la société de sécurité Avast. Il est similaire à VirusTotal, mais plus adapté à Android et peut être très utile pour analyser les logiciels malveillants Android. Le site nécessite un compte, qui est gratuit mais qui doit être approuvé par ses administrateurs. Nous vous recommandons de demander un compte.

Vous pouvez également exécuter le fichier dans un bac à sable (plus d'informations à ce sujet sont disponibles au chapitre 10). Cela suffit souvent pour comprendre le comportement d'un fichier particulier.

Pour obtenir une compréhension approfondie de l'analyse des logiciels malveillants Android, il existe un excellent cours de la chercheuse Google Maddie Stone.

Il est également important de noter qu'il existe des logiciels espions avancés qui se cachent si profondément dans les téléphones qu'ils ne fonctionnent pas comme des applications. Faire des analyses sur les téléphones à la recherche de ce type de logiciels espions s'avère très compliqué, surtout sur les téléphones Android. Vous devrez probablement travailler avec des experts, comme ceux du Citizen Lab ou d'Amnesty Tech, jusqu'à ce que vous développiez vos propres compétences.

Nous espérons approfondir l'analyse des logiciels malveillants Android dans les ajouts futurs à ce guide.