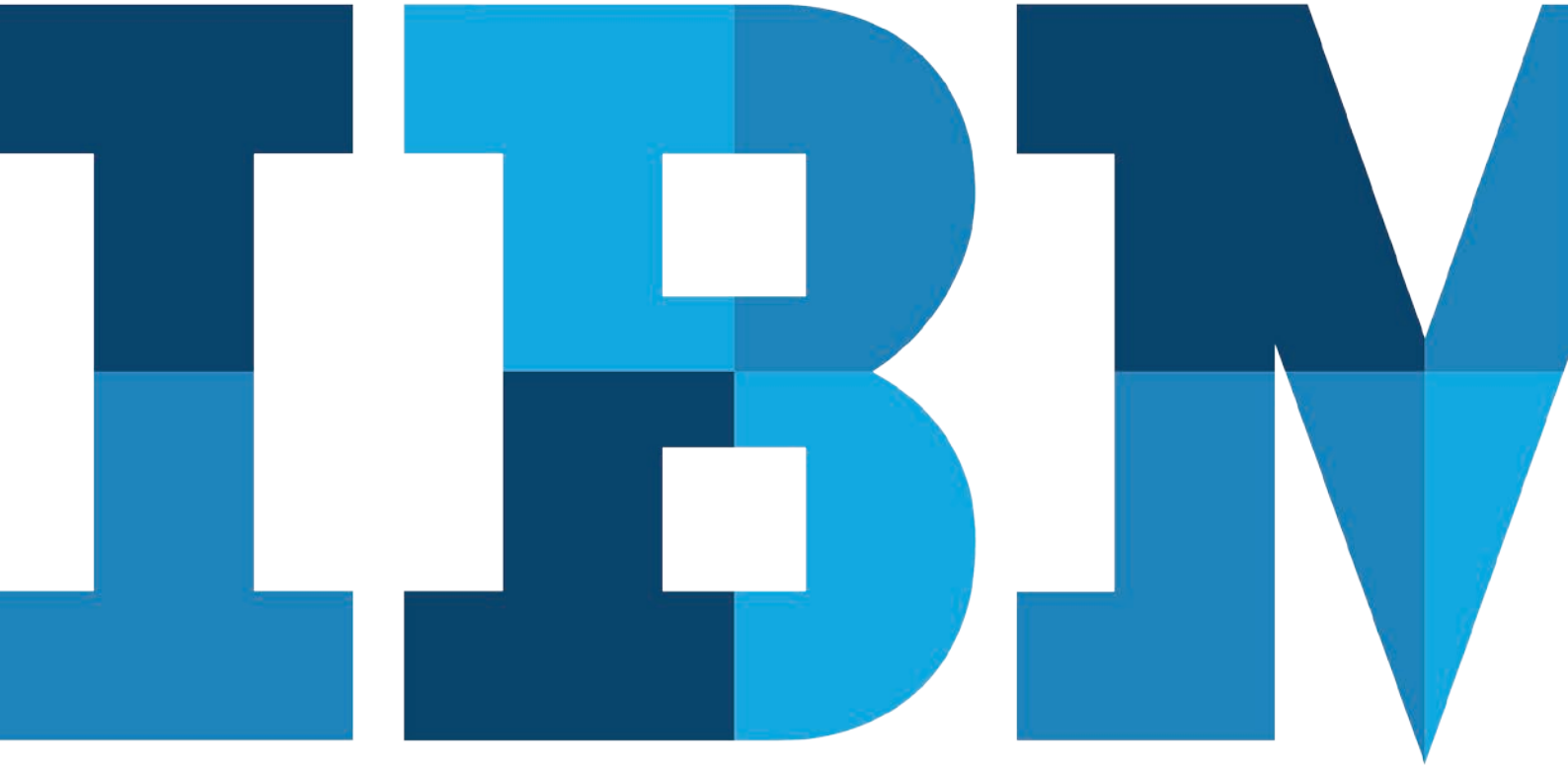
Août 2015

Analyse IBM Security : Vulnérabilités liées aux applications de rencontre et risques pour les entreprises



IBM

Résumé

Une étude Pew Research datant de 2013 a révélé qu'un Américain sur 10 a utilisé un site ou une application de rencontre et que, pour eux, le nombre de personnes qui se sont rencontrées en ligne a atteint 66 pour cent[1]. Pour comprendre la pertinence de ces statistiques du point de vue du risque pour l'entreprise, il est nécessaire de tenir compte de notre mode de vie actuel. Le modèle « travailler d'abord, s'amuser ensuite » n'est plus d'actualité. Quelques années en arrière, notre objectif était de parvenir à un juste équilibre entre la vie professionnelle et la vie privée. Aujourd'hui, l'objectif est devenu la conciliation entre la vie professionnelle et la vie privée. Les employés jonglent en mode multi-tâches entre leurs obligations professionnelles, la gestion de leurs comptes bancaires, les jeux, les tweets, les réseaux sociaux et même les rencontres en ligne. Tout cela est devenu possible en grande partie grâce au phénomène du BYOD « Bring your own device ».

Le BYOD est devenu une pratique populaire, voire même une obligation, dans les entreprises. Les employés ne veulent pas être obligés d'utiliser deux téléphones, l'un pour le travail, l'autre personnel, et de nombreuses entreprises font des économies en évitant d'avoir à acheter des appareils mobiles pour leurs employés. Le fait d'autoriser les employés à apporter leur propre appareil, dédié à la fois à l'utilisation privée et à l'utilisation professionnelle, facilite autant la vie des entreprises que celle des employés.

Le problème du BYOD, s'il n'est pas géré correctement, est qu'il expose les entreprises à la fuite de données métier sensibles à travers les appareils des employés. Si un utilisateur a la possibilité de télécharger des applications à partir de sites tiers non fiables ou même sur des app stores traditionnels, il est possible que des informations sensibles, telles que le carnet d'adresses de l'employé, ses numéros de téléphone, ses données de géolocalisation, et d'autres données, soient exposées à des risques à travers ces appareils.
IBM a analysé 41 des applications de rencontre les plus populaires disponibles pour les appareils Android, y compris celles qui aident les utilisateurs à trouver l'âme soeur par géolocalisation ou en consultant différents profils d'un simple glissé du doigt.

L'analyse portait sur les applications disponibles dans l'App Store Google Play en octobre 2014. Avant même la publication de cette étude, IBM Security a informé tous les fournisseurs concerné par des risques potentiels.

Pour comprendre l'adoption par les utilisateurs d'entreprise de ces 41 applications de rencontre, les données d'application ont été analysées à partir d'IBM® MobileFirst™ Protect, anciennement IBM MaaS360®. IBM a constaté que les employés utilisaient les applications de rencontre vulnérables identifiées dans près de 50 pour cent des petites, moyennes et grandes entreprises échantillonnées pour cette étude, et que ces utilisateurs sont ainsi exposés à un risque potentiel de cyber-attaques et d'intrusions.

Par ailleurs, l'équipe de recherche a analysé les autorisations accordées à chaque application téléchargée, de façon à comprendre quelles sont les données auxquelles elle a accès sur l'appareil du consommateur. Les applications vulnérables peuvent divulguer des renseignements personnels, or si des données d'entreprise se trouvent également sur le terminal, l'entreprise peut également être touchée.

Vulnérabilités des applications de rencontre et conséquences

L'étude d'IBM Security a constaté que plus de 60 pour cent des principales applications de rencontre étaient vulnérables aux menaces de gravité moyenne et/ou élevée qui mettent à risque les données d'application, ainsi que les données stockées sur l'appareil. Les vulnérabilités décelées par IBM peuvent affecter l'utilisation de ces applications de rencontre de différentes manières :

- **Intégrité :** Un pirate peut modifier les données et les informations stockées dans les applications.
- **Confidentialité :** Des informations peuvent être divulguées à partir de l'appareil auquel l'application a accès.
- **Disponibilité :** Un pirate peut empêcher l'utilisateur d'accéder à l'application.

Les menaces spécifiques de gravité moyenne et élevée décelées parmi les 60 pour cent des principales applications à risque sont notamment :

- **Cross Site Scripting (XSS) à travers une attaque Man in the Middle (MiTM) :** Cette menace agit, pour le pirate, comme une passerelle vers l'application et même vers d'autres fonctionnalités de l'appareil. Elle permet au pirate d'intercepter des cookies et d'autres informations depuis l'application via une connexion Wi-Fi ou un point d'accès illicite, et de puiser des données dans d'autres fonctionnalités de l'appareil, telles que la caméra, le GPS et le micro, auxquelles l'application a accès.
- **Indicateur de débogage activé :** Si l'indicateur de débogage est activé dans une application, cela indique qu'une application dont le mode débogage est activé sur un appareil Android peut se connecter à une autre application et effectuer des opérations de lecture ou d'écriture dans la mémoire. Le pirate peut alors intercepter des informations transmises à l'application, modifier ses actions et injecter des données malveillantes à destination ou en provenance de l'application.
- **Générateur faible de Nombres Aléatoires (RNG) :** Certaines applications de rencontre utilisent le chiffrement à l'aide d'un générateur de nombres aléatoires, mais IBM a constaté que les générateurs de ces applications étaient faibles et facilement prévisibles. Un pirate peut prédire l'algorithme de chiffrement et parvenir à accéder à des informations sensibles à travers l'application.
- **Hameçonnage par MiTM :** Un pirate peut proposer un faux écran de connexion par le biais des applications de rencontre dans le but de capturer vos données d'identification utilisateur, de telle sorte que lorsque vous essayez de vous connecter à un site de leur choix, vos données d'identification sont divulguées au pirate à votre insu. Par la suite, le pirate peut accéder à vos contacts en se faisant passer pour vous et leur envoyer des messages de hameçonnage contenant du code malveillant pouvant potentiellement infecter leurs appareils.

Les vulnérabilités identifiées peuvent permettre à un pirate d'accéder à la caméra ou au micro d'un téléphone si l'application a été autorisée à accéder à ces fonctionnalités lors de son téléchargement. Un agresseur peut prendre le contrôle du micro du téléphone aussi longtemps que l'application de rencontre s'exécute à l'arrière-plan et ne nécessite pas que l'utilisateur soit connecté à l'application. Cela signifie que l'agresseur peut espionner les conversations personnelles et même les réunions d'affaires confidentielles à l'insu de l'utilisateur.

Un pirate peut également parvenir à accéder à la caméra du téléphone et au dossier de photos qui peut inclure des images sensibles, personnelles et embarrassantes de l'utilisateur, voire même des images de propositions et de projets d'affaires confidentiels. Si une appli a accès à la caméra de l'utilisateur, l'utilisateur a la possibilité de prendre un selfie à télécharger automatiquement dans son profil sur le site. Un pirate pourrait ainsi prendre le contrôle de la caméra et prendre des photos ou des vidéos de l'utilisateur sans qu'il s'en aperçoive. Cela peut constituer une énorme violation de la vie privée de l'utilisateur.

Lorsqu'un consommateur télécharge une application, il est invité à accorder des autorisations d'accès à certaines fonctionnalités du téléphone, telles que la localisation par GPS, la caméra, les fichiers multimédia et le carnet d'adresses, entre autres. La Figure 1 ci-dessous illustre le pourcentage d'applis qui autorisent divers accès ou actions. Certaines applications demandent même plus d'accès que nécessaire pour permettre leur utilisation ; les consommateurs sont ainsi amenés à autoriser l'accès à des informations non requises. Cela crée une situation où des informations sensibles sont exposées à un risque à travers ces applis de rencontre vulnérables.

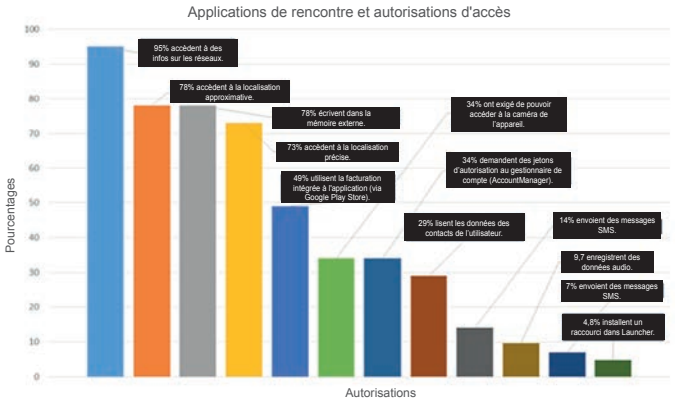


Figure 1 : Applications de rencontre et autorisations d'accès.

Scénarios de menaces pour les consommateurs et les entreprises

La fonction principale d'une application de rencontre est de mettre en relation des utilisateurs, et pas de les protéger contre la cyber-criminalité. Bien que certaines applications aient mis en place des mesures de protection de la vie privée, IBM a constaté qu'elles restent vulnérables à des attaques qui peuvent donner lieu aux scénarios suivants :

Hameçonnage intégré à l'application

Les utilisateurs d'applications de rencontre attendent une réponse de leur conquête potentielle. Par l'intermédiaire de l'application compromise, un agresseur peut envoyer une notification à l'utilisateur qui semble émaner directement de l'application de rencontre, et donc considéré comme digne de confiance. Étant donné que les consommateurs ne s'attendent pas à recevoir des notifications malveillantes sur leur téléphone, surtout provenant d'applications de rencontre, un pirate peut facilement inciter un utilisateur à partager des informations sensibles à travers elle. Un pirate peut aussi utiliser la fausse notification pour amener un utilisateur à télécharger un logiciel malveillant pour infecter l'appareil.

Usurpation de profil

À l'aide de données d'identification volées, le pirate peut se connecter à l'application d'un utilisateur et modifier son profil, envoyer des messages compromettants à des utilisateurs et divulguer son historique. Si l'utilisateur a stocké des informations personnelles sur son profil concernant sa situation amoureuse, sa localisation, des photos sensibles, ou d'autres informations potentiellement embarrassantes, le pirate peut s'en saisir et les partager à grande échelle. Cela peut nuire à la réputation du véritable utilisateur. Par exemple, si un PDG qui utilise une application de rencontre est piraté, les messages personnels échangés avec ses conquêtes, ou même les opinions qu'il peut avoir sur d'autres personnes peuvent être divulgués et donner lieu à des publications d'articles embarrassants sur le PDG et son entreprise.

Traque par GPS

Ces applications présentent le risque pour l'utilisateur d'être traqué par un pirate à l'aide de ses informations de géolocalisation. Comme la Figure 1 ci-dessus le met en évidence, IBM a constaté que 73 pour cent des applications de rencontre étudiées avaient accès aux informations de localisation GPS actuelles et passées. Certaines applications permettent d'accéder à des informations de géolocalisation très spécifiques pour déterminer où l'utilisateur dort chaque nuit, où il travaille, ses habitudes quotidiennes, etc. Un agresseur peut établir des références croisées entre ces informations, des données publiques, les données de leur profil et d'autres réseaux sociaux (auxquels les utilisateurs peuvent se connecter depuis leur profil) pour révéler leur identité. En utilisant les données GPS, l'agresseur peut retracer les déplacements d'un utilisateur ou identifier sa localisation actuelle. Si un membre du bureau de la direction possède un téléphone compromis et que la géolocalisation GPS révèle qu'il s'est fréquemment rendu au siège d'une autre entreprise, cela peut laisser supposer qu'une fusion/acquisition ou une autre opération majeure est en cours de négociation.

Facturation frauduleuse

IBM a observé que 48 pour cent des applications de rencontre étudiées avaient accès aux informations de facturation qui sont stockées sur l'appareil d'un utilisateur. De nombreux consommateurs sauvegardent leurs informations de facturation dans leur porte-monnaie électronique afin d'effectuer facilement et rapidement des achats dans l'application. Un pirate pourrait accéder à ces informations à travers la vulnérabilité de l'application de rencontre et les subtiliser dans le but de faire des achats non autorisés ailleurs.

Recommandations et mesures d'atténuation

Dans la culture connectée actuelle, les applications de rencontre sont devenues un moyen courant pour trouver des partenaires, mais les consommateurs en quête de romance ne se méfient pas des cyber-menaces potentielles de ces applications. Les gens sont prudents face aux messages douteux dans leur boîte e-mail, mails ils sont moins suspicieux concernant les messages reçus sur leur téléphone. Les pirates en tiennent compte et ciblent les téléphones mobiles pour capturer des informations. Pour cette raison, le BYOD est un domaine où les décideurs en matière de règles de sécurité de l'entreprise et les employés assument la même responsabilité dans la protection des informations personnelles et celles de l'entreprise.

Que peuvent faire les employés ?

- **Ne pas divulguer trop d'informations personnelles sur ces sites :** Votre travail, votre date d'anniversaire, vos profils de médias sociaux, etc. doivent demeurer des informations privées.
- **Utiliser des mots de passe uniques pour chaque compte en ligne que vous possédez :** L'utilisation du même mot de passe pour plusieurs sites, comptes et plateformes peut vous exposer à plusieurs attaques si un seul compte est compromis.
- **Toujours appliquer les correctifs les plus récents à vos applications et à votre appareil :** Cela permettra de corriger tous les bogues identifiés dans votre appareil et vos applications, et d'assurer une expérience plus sécurisée.
- **Effectuer régulièrement des analyses d'autorisations :** Chaque fois que votre application se met à jour, elle peut obtenir des autorisations d'accès supplémentaires sur votre appareil mobile. Vérifiez régulièrement ce à quoi vos applications mobiles ont accès, et si vous constatez quelque chose d'alarmant, désélectionnez-le ou supprimez l'application intégralement.
- **Examiner vos contacts et vos notes sur votre appareil :** Vérifiez la présence d'éléments qui ne devraient pas y figurer, comme des mots de passe ou des notes relatives à des contacts personnels ou professionnels.

Que peuvent faire les entreprises ?

- **Mettre en place les solutions métier appropriées :** Tirez parti des solutions Enterprise Mobility Management (EMM) qui comprennent des fonctions de gestion des menaces mobiles afin de permettre aux employés d'utiliser leurs propres appareils tout en préservant la sécurité de l'entreprise.
- **Limiter l'accès aux applications à risque :** Comprenez quelles applications sont vulnérables aux attaques et prenez des mesures pour mettre sur liste noire les applications à risque et les empêcher ainsi de s'exécuter sur un appareil contenant des données d'entreprise.
- **Informer vos collaborateurs :** Sensibilisez vos employés aux dangers liés au téléchargement d'applications tierces et conseillez leur vivement de ne télécharger que des applications provenant d'app stores autorisés.
- **Veiller à mettre en place une procédure adéquate à suivre en cas de menace :** Adoptez une stratégie à l'échelle de l'entreprise afin de prendre des mesures automatiques, telles que la notification immédiate de l'utilisateur et du service informatique interne, si jamais un logiciel malveillant était détecté sur un terminal de l'entreprise.

À propos de cette recherche

Les analystes IBM Security de l'équipe IBM Application Security Research ont utilisé le nouvel outil IBM AppScan Mobile Analyzer pour analyser les 41 principales applications de rencontre disponibles sur les appareils Android afin d'identifier les vulnérabilités susceptibles d'exposer les utilisateurs à des cyber-attaques et des menaces potentielles. Ces applications ont également été analysées dans le but de déterminer les autorisations accordées, ce qui a permis de révéler un grand nombre de privilèges excessifs. Pour comprendre l'adoption par les utilisateurs d'entreprise de ces 41 applications de rencontre, les données d'application ont été analysées à partir d'IBM MobileFirst Protect, anciennement MaaS360. Avant même la publication de cette étude, IBM Security a révélé à tous les fournisseurs d'applications concernés les failles que l'étude a permis d'identifier.

Pour bénéficier d'un essai gratuit d'IBM AppScan Mobile Analyzer pendant 30 jours, cliquez ici : http://ibm.co/1zNBl6u

Pour un essai gratuit d'IBM MobileFirst Protect pendant 30 jours (anciennement MaaS360), cliquez ici : http://bit.ly/1DG5AtF

À propos de l'auteur

Michelle Alvarez est chercheur et rédactrice dans le domaine des menaces pour IBM Managed Security Services ; elle a plus de dix ans d'expérience dans ce rôle. Dans le cadre de sa fonction, elle se concentre sur les efforts de communication concernant la recherche sur les menaces et les mesures d'atténuation. Michelle a rejoint IBM à travers l'acquisition d'Internet Security Services (ISS) où elle occupait la fonction d'analyste dans l'équipe chargée de la base de données des vulnérabilités X-Force.

Contributeurs

- Roee Hay
- Caleb Barlow
- Diana Kelley
- Michael Montecillo
- Eitan Worcel
- Neil Jones

Références

Manifest.permission | Android Developers
http://developer.android.com/reference/android/Manifest.permission.html

IBM BYOD : Bring your own device
http://www.ibm.com/mobilefirst/us/en/bring-your-owndevice/byod.html

Compagnie IBM France
17, Avenue de l'Europe
92275 Bois-Colombes Cedex

Produit en France
Août 2015

[1] Online Dating & Relationships, Pew Research Center, Aaron Smith and Maeve Duggan, Octobre 2013

WGL03072FRFR