Communiqués de presse

Selon la division sécurité d’IBM, 60% des applications de rencontres les plus connues peuvent être piratées

La moitié des entreprises étudiées par IBM ont des employés qui accèdent aux applications de rencontres depuis leurs appareils mobiles professionnels. IBM donne des conseils aux utilisateurs et aux entreprises pour se défendre.

Paris - 11 févr. 2015: Une étude menée aux Etats-Unis par la division sécurité d’IBM révèle que 60% des applications mobiles de rencontres les plus populaires sont potentiellement vulnérables à différentes cyber-attaques, ce qui fait courir un risque aux données personnelles des utilisateurs et aux données sensibles de l’entreprise.

L'étude IBM révèle que nombre de ces applications de rencontres permettent un accès à des fonctionnalités supplémentaires sur les appareils mobiles (tels que l’appareil photo, le microphone, le stockage, la localisation GPS et les informations de facturation du portefeuille mobile) qui, associées aux vulnérabilités, peuvent être exploitées par les pirates. IBM a également révélé que près de 50% des entreprises comptent au moins une application de rencontres connue, installée par un employé sur son appareil mobile qu’il utilise pour accéder à des informations confidentielles de l’entreprise.

Les chercheurs de la division sécurité d’IBM se sont rendus compte que 26 des 41 applications de rencontres analysées sur la plate-forme mobile Android sont soumises à des vulnérabilités de sévérité moyenne ou élevée. Cette étude a été effectuée sur la base des applications disponibles dans l'App Store Google Play en octobre 2014.

Les vulnérabilités découvertes par la division sécurité d’IBM permettent à un pirate de recueillir de précieux

renseignements personnels sur un utilisateur. Alors que certaines applications bénéficient de mesures de protection des données personnelles, IBM indique que beaucoup d'entre elles sont vulnérables à des attaques qui pourraient conduire aux scénarios suivants:

·Les applications de rencontres utilisées pour télécharger des logiciels malveillants : Certaines des applications vulnérables pourrait être reprogrammées par des pirates pour envoyer ce qui ressemble à une alerte demandant aux utilisateurs de cliquer pour effectuer une mise à jour ou pour récupérer un message. En réalité, il s'agit juste d'un piège pour télécharger des logiciels malveillants sur leur appareil.

· Les informations GPS utilisées pour suivre les déplacements : IBM indique que 73% des 41 applications de rencontres connues analysées ont accès aux informations de localisation GPS actuelles et passées. Les pirates peuvent utiliser ces informations pour savoir où un utilisateur vit, travaille ou passe le plus clair de son temps.

· Voler des numéros de carte de crédit depuis l'application : 48% des 41 applications de rencontres analysées ont accès aux informations de facturation enregistrées sur l'appareil d'un utilisateur. Via un simple codage, et grâce à cette vulnérabilité de l'application, un attaquant pourrait s'emparer de ces données et s'en servir pour réaliser des achats frauduleux.

· Prendre le contrôle de l'appareil photo ou du microphone d'un téléphone : Toutes les vulnérabilités identifiées peuvent permettre à un pirate d'accéder à l'appareil photo ou au microphone d'un téléphone même si l'utilisateur n'est pas connecté à l'application. Cela signifie qu'un pirate peut espionner et écouter les utilisateurs ainsi qu'exploiter des réunions d'affaires confidentielles.

· Le pirate peut détourner votre profil sur un site de rencontres : Un pirate peut modifier le contenu et les images d'un profil de rencontre, usurper l'identité de l'utilisateur et communiquer avec les autres utilisateurs de l'application. Il peut également révéler des renseignements personnels à l'extérieur afin de nuire à la réputation d'un utilisateur.

Des mesures pour se protéger contre les attaques sur les sites de rencontres.

Que peuvent faire les utilisateurs ?

· Etre mystérieux : Ne pas divulguer trop d'informations personnelles sur ces sites.

· Gérer les autorisations : Déterminer si l'on souhaite autoriser une application en vérifiant les autorisations requises dans les paramètres de son appareil mobile.

· Un accès unique : Utiliser des mots de passe uniques pour chacun de ses comptes en ligne.

· Corrections ponctuelles : Toujours appliquer les derniers correctifs et mises à jour des applications et de

l’appareil dès qu'ils sont disponibles.

· Connexions fiables : Utiliser uniquement les connexions Wi-Fi fiables et sécurisées lorsque l’on utilise une application de rencontres.

=> Que peuvent faire les entreprises ?

IBM a constaté que près de 50 entreprises, faisant partie de l’échantillon de cette étude, ont au moins une application de rencontres connue qui est installée soit sur un appareil appartenant à l’entreprise, soit sur un appareil personnel utilisé à des fins professionnelles (BYOD). Pour protéger leurs données confidentielles, les entreprises devraient :

· Adopter la bonne protection : Les solutions Enterprise Mobility Management (EMM), avec les capacités de gestion des menaces mobiles (MTM), permettent aux employés d'utiliser leurs propres appareils, tout en préservant la sécurité de l'entreprise.

· Définir les applications téléchargeables : Permettre aux employés de télécharger les applications seulement à partir de magasins d'applications autorisés, tels que Google Play, iTunes et l’app store de l’entreprise.

· L'éducation est la clé : Former les employés pour qu’ils connaissent les dangers du téléchargement d’applications tierces et qu’ils comprennent ce que cela signifie quand ils donnent à ces applications des autorisations spécifiques d’accès à leurs appareils.

· Communiquer immédiatement les menaces potentielles : Établir des politiques automatisées sur les smartphones et les tablettes, qui prennent des mesures immédiates si un périphérique se trouve compromis ou que des applications malveillantes sont découvertes. Cela permet de protéger les ressources de l'entreprise pendant que le problème est résolu.

A propos de cette étude
Les analystes de la division sécurité d’IBM, issus de l'équipe de recherche sur la sécurité des applications, ont utilisé le nouvel outil IBM AppScan Mobile Analyzer. Cela a permis d’étudier les 41 applications de rencontres les plus populaires disponibles sur les appareils Android et d’identifier les vulnérabilités qui font de l’utilisateur une cible de cyber-attaques et de menaces potentielles. Ces applications ont également été étudiées pour déterminer quelles sont les autorisations accordées et ont dévoilé une multitude de privilèges excessifs. Pour comprendre l’adoption de ces 41 applications de rencontres par des utilisateurs en entreprise, les données de l'application ont été analysées à partir d'IBM MobileFirst Protect, anciennement MaaS360. Avant de dévoiler cette étude au public, la division sécurité d’IBM l’a divulguée à tous les fournisseurs d'applications touchés qui ont été identifiés dans cette recherche.

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

Pour bénéficier d’un essai gratuit de 30 jours d’IBM MobileFirst Protect (précédemment MaaS360), cliquez ici : http://bit.ly/1DG5AtF

A propos d'IBM Security
La plateforme de sécurité IBM apporte la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions et d'autres sujets. IBM dispose d'une des plus importantes organisations au monde de recherche et développement et de mise en œuvre dans le domaine de la sécurité.

Pour plus d'informations : http://ibm.com/fr/security
Suivez notre actualité sur Twitter @IBMSecurityFR ou sur le blog <http://www.lasecuriteintelligente.fr/> La Sécurité Intelligente.

###

IBM Security Finds Over 60 Percent of Popular Dating Apps Vulnerable to Hackers
Half of Enterprises Analyzed by IBM Have Employees Accessing Dating Apps on Work Mobile Devices, IBM offers Tips to Consumers and Businesses to Defend Themselves

ARMONK, N.Y. – February 11, 2015: An analysis conducted by IBM Security found over 60 percent of leading dating mobile apps they studied to be potentially vulnerable to a variety of cyber-attacks that put personal user information and corporate data at risk.

The IBM study reveals that many of these dating applications have access to additional features on mobile devices such as the camera, microphone, storage, GPS location and mobile wallet billing information, which in combination with the vulnerabilities may make them exploitable to hackers. IBM also found that nearly 50 percent of organizations analyzed have at least one of these popular dating apps installed on mobile devices used to access business information.

In today's connected culture, dating apps are a common and convenient way for singles of all ages to meet new love interests. In fact, a Pew Research study revealed one in 10 Americans, or roughly 31 million people, have used a dating site or app and the number of people who dated someone they met online grew to 66 percent.

"Many consumers use and trust their mobile phones for a variety of applications. It is this trust that gives hackers the opportunity to exploit vulnerabilities like the ones we found in these dating apps," said Caleb Barlow, Vice President, IBM Security. "Consumers need to be careful not to reveal too much personal information on these sites as they look to build a relationship. Our research demonstrates that some users may be engaged in a dangerous tradeoff – with increased sharing resulting in decreased personal security and privacy."

Security researchers from IBM Security identified that 26 of the 41 dating apps they analyzed on the Android mobile platform had either medium or high severity vulnerabilities. The analysis was done based on apps

available in the Google Play app store in October 2014.

The vulnerabilities discovered by IBM Security make it possible for a hacker to gather valuable personal information about a user. While some apps have privacy measures in place, IBM found many are vulnerable to attacks that could lead to the following scenarios:

· Dating App Used to Download Malware: Users let their guard down when they anticipate receiving interest from a potential date. That's just the sort of moment that hackers thrive on. Some of the vulnerable apps could be reprogrammed by hackers to send an alert that asks users to click for an update or to retrieve a message that, in reality, is just a ploy to download malware onto their device.

· GPS Information Used to Track Movements: IBM found 73% of the 41 popular dating apps analyzed have access to current and past GPS location information. Hackers can capture a user's current and past GPS location information to find out where a user lives, works, or spends most of their time.

· Credit Card Numbers Stolen From App: 48% of the 41 popular dating apps analyzed have access to a user's billing information saved on their device. Through poor coding, an attacker could gain access to billing information saved on the device's mobile wallet through a vulnerability in the dating app and steal the information to make unauthorized purchases.

· Remote Control of a Phone's Camera or Microphone: All the vulnerabilities identified can allow a hacker to gain access to a phone's camera or microphone even if the user is not logged into the app. This means an attacker can spy and eavesdrop on users or tap into confidential business meetings.

· Hijacking of Your Dating Profile: A hacker can change content and images on the dating profile, impersonate the user and communicate with other app users, or leak personal information externally to affect the reputation of a user's identity. This poses a risk to other users, as well, since a hijacked account can be used by an attacker to trick other users into sharing personal and potentially compromising information.

Some of the specific vulnerabilities identified on the at-risk dating apps include cross site scripting via man in the middle, debug flag enabled, weak random number generator and phishing via man in the middle. When these vulnerabilities are exploited an attacker can potentially use the mobile device to conduct attacks.

For example, hackers could intercept cookies from the app via a Wi-Fi connection or rogue access point, and then tap into other device features such as the camera, GPS, and microphone that the app has permission to access. They also could create a fake login screen via the dating app to capture the user's credentials, so when they try to log into a website, the information is also shared with the attacker.

Steps to Protect Against Dating App Hacks

While IBM discovered a number of vulnerabilities in over 60 percent of popular Android dating apps, both consumers and businesses can take steps to protect themselves against potential threats.

What Can Consumers Do?

· Be Mysterious: Don't divulge too much personal information on these sites such as where you work, birthday or social media profiles until you're comfortable with the person you are engaging with via the app.

· Permission Fitness: Figure out if you want to use an app by checking the permissions it asks for by viewing the settings on your mobile device. When updating, apps often automatically reset the permissions determining what phone features they have access to, like your address book or GPS data.

· Keep it Unique: Use unique passwords for every online account you have. If you use the same password for all your accounts it can leave you open to multiple attacks if one account is compromised.

· Punctual Patching: Always apply the latest patches and updates to your apps and your device when they become available. This will fix any identified bugs in your device and applications, resulting in a more secure experience.

· Trusted Connections: Use only trusted Wi-Fi connections when on your dating app. Hackers love using fake Wi-Fi access points that connect you directly to their device to execute these types of attacks. Many of the vulnerabilities found in this research can be exploited via Wi-Fi.

What Can Enterprises Do?

Businesses also need to be prepared to protect themselves from vulnerable dating apps active inside their infrastructure, especially for Bring Your Own Device (BYOD) scenarios. IBM found that nearly 50 percent of organizations sampled for this research have at least one of these popular dating apps installed on corporate-owned or personal mobile devices used for work. To protect confidential corporate assets, businesses should:

· Adopt the Right Protection: Leverage Enterprise Mobility Management (EMM) offerings with mobile threat management (MTM) capabilities to enable employees to utilize their own devices while still maintaining the security of the organization.

· Define Downloadable Apps: Allow employees to only download applications from authorized app stores such as Google Play, iTunes, and the corporate app store.

· Education is Key: Educate employees to know the dangers of downloading third party applications and what it means when they grant that app specific device permissions.

· Immediately Communicate Potential Threats: Set automated policies on smartphones and tablets, which take immediate action if a device is found compromised or malicious apps are discovered. This enables protection to corporate resources while the issue is remediated.

About This Research

IBM Security analysts from the IBM Application Security Research team used its new IBM AppScan Mobile Analyzer tool to analyze the top 41 dating apps available on Android devices to identify vulnerabilities that can leave users open to potential cyber-attacks and threats. These apps were also analyzed to determine the granted permissions, unveiling a large number of excessive privileges. To understand enterprise user adoption of these 41 dating apps, app data was analyzed from IBM MobileFirst Protect, formerly MaaS360. In advance of

releasing this research to the public, IBM Security has disclosed all impacted app vendors identified with this research. For more information on this research, please visit: www.securityintelligence.com/datingapps

To try a free 30-day trial of IBM AppScan Mobile Analyzer, click here: http://ibm.co/1zNBl6u

For a free 30-day trial of IBM MobileFirst Protect (formally MaaS360), click here: http://bit.ly/1DG5AtF

About IBM Security
IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations.
For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.