Chez soi comme au bureau, les applications vampirisent nos données

On n’en peut plus des applis ! Depuis longtemps déjà leur omniprésence est envahissante et nous en avons parlé ici et là. Comme le profit potentiel qu’elles représentent n’a pas diminué, leur harcèlement n’a fait qu’augmenter

Aujourd’hui un bref article attire notre attention sur les applications comme vecteurs d’attaques, dangereuses tant pour la vie privée que pour la vie professionnelle.

Avertissement : l’auteur est vice-président d’une entreprise qui vend de la sécurité pour mobile…aux entreprises, d’où la deuxième partie de son article qui cible l’emploi des applications dans le monde du travail, et où manifestement il « prêche pour sa paroisse ».

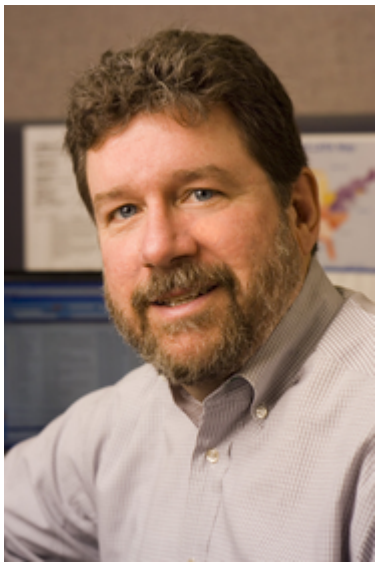
Il nous a semblé que sa visée intéressée n’enlève rien à la pertinence de ses mises en garde.

Article original paru dans TechCrunch : Attack of the apps

Traduction Framalang : dodosan, goofy, savage, xi, Asta

Quand les applis attaquent

par **Robbie Forkish**



Ça paraît une bonne affaire : vos applis favorites pour mobile sont gratuites et en contrepartie vous regardez des pubs agaçantes.

Mais ce que vous donnez en échange va plus loin. En réalité, vous êtes obligé·e de céder un grand nombre d'informations privées. Les applications mobiles collectent une quantité énorme de données personnelles : votre emplacement, votre historique de navigation sur Internet, vos contacts, votre emploi du temps, votre identité et bien davantage. Et toutes ces données sont partagées instantanément avec des réseaux de publicité sur mobile, qui les utilisent pour déterminer la meilleure pub pour n'importe quel utilisateur, en tout lieu et à tout moment.

Donc le contrat n'est pas vraiment d'échanger des pubs contre des applis, c'est plutôt de la surveillance sur mobile contre des applis. En acceptant des applis gratuites et payées par la pub sur nos mobiles, nous avons consenti à un modèle économique qui implique une surveillance complète et permanente des individus. C'est ce qu'Al Gore appelait très justement une économie du harcèlement.

Pourquoi nos données personnelles, notre géolocalisation et nos déplacements sont-ils tellement convoités par les entreprises commerciales ? Parce que nous, les consommateurs, avons toujours et partout notre smartphone avec nous, et qu'il transmet sans cesse des données personnelles en tout genre. Si les annonceurs publicitaires savent qui nous sommes, où nous sommes et ce que nous faisons, ils peuvent nous envoyer des publicités plus efficacement ciblées. Cela s'appelle du marketing de proximité. C'est par exemple la pub du Rite Aid (NdT chaîne de pharmacies) qui vous envoie un message téléphonique quand vous circulez dans les rayons : « Vente flash : -10 % sur les bains de bouche ! »

Ça paraît inoffensif, juste agaçant. Mais cela va bien plus loin. Nous avons

maintenant accepté un système dans lequel un site majeur de commerce en ligne peut savoir par exemple, qu'une adolescente est enceinte avant que ses parents ne le sachent, simplement en croisant les données de ses achats, son activité et ses recherches. Ce site de vente en ligne peut alors la contacter par courrier traditionnel ou électronique, ou encore la cibler via son téléphone lorsqu'elle est à proximité d'un point de vente. Nous n'avons aucune chance de voir disparaître un jour cette intrusion dans notre vie privée tant que le profit économique sera juteux pour les développeurs d'applications et les agences de publicité.

> *Un smartphone compromis représente une menace pas seulement pour l'employé visé mais pour l'entreprise tout entière.*

D'accord, cette forme de surveillance du consommateur est intrusive et terrifiante. Mais en quoi cela menace-t-il la sécurité de l'entreprise ? C'est simple. À mesure que les appareils mobiles envahissent le monde du business, les fuites de ces appareils ouvrent la porte de l'entreprise aux piratages, aux vols de données et à des attaques paralysantes.

Si par exemple une entreprise laisse ses employés synchroniser leurs agendas et comptes mail professionnels avec leurs appareils mobiles personnels, cela ouvre la porte à toutes sortes de risques. D'un coup, les téléphones des employés contiennent les informations de contact de tout le monde dans l'organisation ou ont la possibilité d'y accéder. À fortiori, n'importe quelle autre application mobile qui demandera l'accès aux contacts et agendas des employés aura accès aux noms et titres des employés de la compagnie, aussi bien qu'aux numéros de toutes les conférences téléphoniques privées. Cette information peut facilement être utilisée pour une attaque par hameçonnage par une application malveillante ou un pirate.

Elles sont jolies les applis, non ? – Image créée par Tanja Cappell (CC BY-SA 2.0)

Pire, de nombreuses applications monétisent leurs bases d'utilisateurs en partageant les données avec des réseaux publicitaires qui repartagent et mutualisent les données avec d'autres réseaux, aussi est-il impossible de savoir exactement où vont les données et si elles sont manipulées de manière sécurisée par n'importe laquelle des nombreux utilisateurs y ayant accès. Tous ces partages signifient qu'un pirate malveillant n'a même pas besoin d'avoir accès au téléphone d'un employé pour attaquer une entreprise. Il lui suffit de pirater un réseau publicitaire qui possède les informations de millions d'utilisateurs et de partir de là.

Les informations volées peuvent aussi être utilisées pour pirater une entreprise au moyen d'une attaque de point d'eau. Supposons par exemple que des membres du comité de direction déjeunent régulièrement dans le même restaurant. Un attaquant qui a accès à leurs données de localisation pourrait facilement l'apprendre. L'attaquant suppose, à raison, que certains membres vont sur le site du restaurant pour réserver une table et regarder le menu avant le repas. En

introduisant du code malveillant sur ce site mal défendu, l'attaquant peut compromettre l'ordinateur de bureau ou le téléphone d'un ou plusieurs membres du comité de direction, et de là, s'introduire dans le réseau de l'entreprise.

Un smartphone compromis représente une menace non seulement pour l'employé ciblé mais pour l'entreprise dans son entier. Des informations sur les activités des employés, à la fois pendant leur temps de travail et en dehors, combinées à des courriels, des informations sensibles ou des documents liés à l'entreprise, peuvent avoir des effets dévastateurs sur une organisation si elles tombent entre de mauvaises mains.
Que doivent donc faire les entreprises pour lutter contre cette menace ?

La première étape est d'en apprendre plus sur votre environnement mobile. Votre organisation doit savoir quelles applications les employés utilisent, ce que font ces applications et si elles sont conformes à la politique de sécurité de l'entreprise. Par exemple, existe-t-il une application de partage de documents particulièrement risquée que vous ne voulez pas que vos employés utilisent ? Est-elle déjà utilisée ? Si vous ne savez pas quelles applications vos employés utilisent pour travailler, vous naviguez à l'aveugle et vous prenez de gros risques.

Il est essentiel que votre entreprise inclue la protection contre les menaces sur mobile dans sa stratégie de sécurité générale.

Deuxièmement, vous allez avoir besoin d'une politique sur l'utilisation des appareils mobiles. La plupart des organisations ont déjà mis en place une politique pour les autres plateformes, y compris pour la gestion des pare-feux et le partage de données avec des partenaires de l'entreprise. Par exemple, si vos employés utilisent la version gratuite d'applications approuvées par l'entreprise mais avec publicité, imposez aux employés d'utiliser la version payante afin de minimiser, sinon éliminer, l'envoi aux employés de données non approuvées sous forme de publicités, même si cela n'éliminera pas la collecte incessante de données personnelles et privées.

Ensuite, votre organisation doit informer les employés sur les risques liés aux applications utilisées. Il est dans votre intérêt de donner du pouvoir aux utilisateurs en les équipant d'outils et en les entraînant afin qu'ils puissent prendre de meilleures décisions quant aux applications téléchargées. Par exemple, incitez vos employés à se poser des questions sur les applications qui

demandent des permissions. Il existe beaucoup d'applications qui veulent accéder aux données de localisation, aux contacts ou à la caméra. Les employés ne doivent pas dire automatiquement oui. La plupart des applications fonctionneront très bien si la requête est rejetée, et demanderont à nouveau aux utilisateurs si la permission est vraiment nécessaire. Si une application ne dit pas pourquoi elle a besoin de cet accès, c'est mauvais signe.

Enfin, toutes ces questions peuvent être traitées avec une bonne solution de sécurité pour appareils mobiles. Toute entreprise sans solution de protection des appareils mobiles est par définition inconsciente des informations qui lui échappent et ignore d'où viennent les fuites. Elle est donc incapable de répondre aux risques présents dans son environnement. Il est donc essentiel que votre entreprise inclue la protection des appareils mobiles dans sa stratégie de sécurité afin de protéger la vie privée des employés et les données de l'entreprise de la menace toujours plus grande que représentent la surveillance des téléphones et la collecte de données.