27 avril 2015
Cheval de Troie

Ces risques qu'on prend à accéder à des applis via ses logins Gmail, Facebook et Twitter

Si les éditeurs d'applications justifient cette méthode de connexion par une amélioration de l'expérience utilisateur, laisser une application accéder aux données détenues par Google ou Facebook n'est pas sans péril. Adresse, numéro de téléphone, paiements effectués... De nombreuses informations sensibles y sont récupérées.

Avec Erwan le Nagard

Atlantico : Les applis, sites et autres services auxquels nous nous connectons via un compte Facebook, Twitter ou Gmail peuvent être très nombreux, en fonction des habitudes de navigation de chacun. Ce faisant, quelles données laissons-nous "en pâture", et à qui ?

Erwan Le Nagard : Les acteurs majeurs du numérique, notamment les réseaux sociaux, proposent aux développeurs de construire des applications utilisant des fonctionnalités issues de leurs plateformes. C'est ainsi que vous pouvez utiliser le bouton "j'aime" sur le site média ou vous connecter à l'aide de vos identifiants Facebook sur votre site de e-commerce favori. Cela représente une part non négligeable de leur activité : plus de 80% du trafic de Twitter provient de ces applications. Facebook dénombre plus de 30 millions d'applications et de sites web utilisant ses fonctionnalités… Bien évidemment, les éditeurs d'applications n'ont pas accès à l'ensemble des fonctionnalités de la plateforme mère ni à toutes les données de ses utilisateurs. Néanmoins, les utilisateurs peuvent partager certaines informations avec les éditeurs d'applications pour bénéficier en retour d'une expérience de navigation simplifiée ou d'un service personnalisé. **Chaque application demande accès à des données différentes mais, d'une manière générale, l'utilisateur peut être amené à partager des éléments concernant son identité (son nom, email, téléphone…), son activité (interactions, paiements…), ses relations ou les services qu'il utilise. Bref, cela représente un vaste ensemble de données dont l'utilisateur ne maitrise pas toujours les aboutissants.**

Quels sont les risques, auxquels nous ne pensons pas forcément ?

Le risque le plus évident concerne des tentatives de phishing, c'est-à-dire lorsqu'une application tente d'accéder à vos données en se faisant passer pour un tiers de conscience. Il sera toujours possible de révoquer l'accès à l'application si l'utilisateur s'aperçoit de la supercherie, mais une fois les données partagées, le mal est fait…

Les éditeurs d'applications sont tenus de maintenir leurs services en état de fonctionnement, et d'assurer la sécurité de leurs utilisateurs. **Néanmoins, la plupart des applications sont créées de manière événementielle, le temps d'une campagne publicitaire ou d'un jeu concours. Il n'est alors pas rentable de maintenir ces applications ni même de les supprimer. Or, les applications tierces connectées à votre compte peuvent être vulnérables à une attaque extérieure**. Pourtant, la plupart des

utilisateurs ne pensent pas à révoquer l'accès à ces applications devenues inutiles.

Enfin, certaines données partagées en ligne peuvent être considérées comme publiques et ne nécessitent pas qu'un éditeur demande une autorisation explicite pour y avoir accès. Par exemple, il est possible que les tweets d'un utilisateur soient collectés et analysés si l'utilisateur n'en a pas restreint l'accès. Par extension, la plupart des utilisateurs méconnaissent les métadonnées, c'est-à-dire des données qui servent à en décrire d'autres. Par exemple, un tweet peut paraitre de prime abord peu intéressant à l'analyse, puisqu'il ne comporte que 140 caractères. **En réalité, ce message est associé à une quarantaine d'autres informations : l'identité de l'auteur, son activité sur le réseau, sa description, sa localisation, depuis quelle source a été publié le message, quels hashtags sont mentionnés, etc.**

En cas de piratage par un tiers de l'un de ces comptes sociaux, et compte tenu des nombreuses portes d'entrée vers d'autres sites que ceux-ci représentent, que peut-il arriver ? Quelles "armes" cela donne-t-il au pirate ?

Nous confions un grand volume et une grande variété de données à des plateformes telles que Facebook, Google ou Twitter, en même temps qu'elles élargissent le périmètre de leurs activités. Facebook n'est plus simplement un simple site de réseautage, Google n'est plus un simple moteur de recherche. **Ce sont aussi des plateformes qui ont développé des services variés par lesquels transitent des données de paiement, d'usage, de localisation, etc.** Mieux vaut se prémunir d'un éventuel piratage en assurant la sécurité de son compte sous peine de déconvenues (paiements frauduleux, usurpation d'identité. Quelques règles de bon sens sont à respecter : modifier régulièrement son mot de passe, ne pas accepter les demandes émises par des tiers inconnus, désactiver les applications tierces inutilisées, etc.

Est-ce à chacun de se prendre en charge, ou les géants que sont Facebook, Twitter et Google ont-ils eux aussi une part de responsabilité dans la préservation de nos données ?

Il existe un cadre juridique strict concernant la collecte, le traitement et le stockage de données, surveillé et régulé par des institutions comme la CNIL. Les éditeurs sont tenus de se conformer à la législation et on observe de nombreux échanges entre les principaux acteurs du marché et ces institutions. **Néanmoins, les utilisateurs doivent jouer un rôle actif dans la préservation de leurs données : avoir conscience des données mises en ligne, développer les bons réflexes en cas de piratage, se prémunir d'éventuelles failles de sécurité …**