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 ».

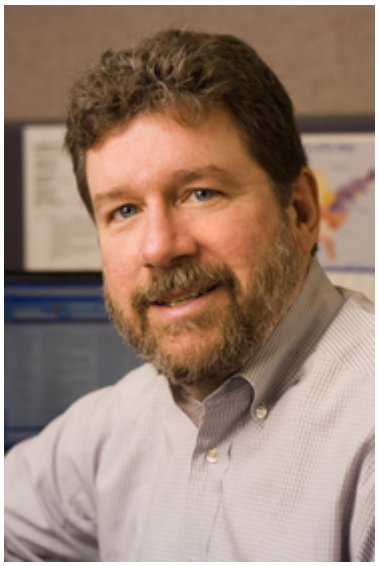
Il nous a semblé que sa visée intéressée n'enlève rien à la pertinence de ses mises en garde.

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.

Comment la NSA déploie des logiciels malveillants

Nouvelles révélations, nouvelles précautions

Nous reprenons ici l'article récemment publié par KoS, il s'agit de la traduction française de l'article de l'Electronic Frontier Foundation : How The NSA Deploys Malware: An In-Depth Look at the New Revelations par : Sphinx, KoS, Scailyna, Paul, Framatophe et 2 auteurs anonymes

– – – – – –

Nous avons longtemps suspecté que la NSA, la plus grande agence d'espionnage du monde, était plutôt douée pour pénétrer les ordinateurs. Désormais, grâce à un article de Bruce Schneier, expert en sécurité qui travaille avec The Guardian sur les documents de Snowden, nous avons une vision bien plus détaillée de la manière dont la NSA utilise des failles pour infecter les ordinateurs d'utilisateurs ciblés.

La méthode utilisée par la NSA pour attaquer les gens avec des logiciels malveillants est largement utilisée par les criminels et les fraudeurs ainsi que par les agences de renseignement, il est donc important de comprendre et de se

défendre contre cette menace pour éviter d'être victime de cette pléthore d'attaquants.

Comment fonctionnent les logiciels malveillants exactement ?

Déployer un logiciel malveillant via le Web nécessite généralement deux étapes. Premièrement, en tant qu'attaquant, vous devez attirer votre victime sur un site web que vous contrôlez. Deuxièmement, vous devez installer un logiciel sur l'ordinateur de la victime pour prendre le contrôle de sa machine. Cette formule n'est pas universelle, mais c'est souvent ainsi que les attaques sont exécutées.

Pour mener à bien la première étape, qui consiste à amener un utilisateur à visiter un site sous le contrôle de l'attaquant, ce dernier peut envoyer à la victime un courriel avec un lien vers le site web concerné : c'est ce que l'on appelle une attaque par hameçonnage (*phishing*). La NSA aurait parfois eu recours à ce type d'attaque, mais nous savons à présent que cette étape était généralement accomplie via une méthode dite de « l'homme du milieu » (*man-in-the-middle*)[1]. La NSA contrôle un ensemble de serveurs dont le nom de code est « Quantum », situés sur les dorsales Internet et ces serveurs sont utilisés pour rediriger les cibles vers d'autres serveurs contrôlés par la NSA et chargés d'injecter le code malveillant.

Dans ce cas, si un utilisateur ciblé visite, par exemple, le site yahoo.com, son navigateur affichera la page d'accueil ordinaire de Yahoo! mais sera en réalité en communication avec un serveur contrôlé par la NSA. La version malveillante du site web de Yahoo! demandera au navigateur de l'utilisateur d'adresser une requête à un autre serveur contrôlé par la NSA et chargé de diffuser le code néfaste.

Quand un utilisateur ciblé visite un site web mal intentionné, quels moyens l'attaquant utilise-t-il pour infecter l'ordinateur de la victime ? Le moyen le plus direct est

probablement d'amener l'utilisateur à télécharger et à exécuter un logiciel. Une publicité intelligemment conçue s'affichant dans une fenêtre pop-up peut convaincre un utilisateur de télécharger et d'installer le logiciel malveillant de l'attaquant.

Toutefois, cette méthode ne fonctionne pas toujours et repose sur une initiative de l'utilisateur visé, qui doit télécharger et installer le logiciel. Les attaquants peuvent choisir plutôt d'exploiter des vulnérabilités du navigateur de la victime pour accéder à son ordinateur. Lorsqu'un navigateur charge une page d'un site, il exécute des tâches telles que l'analyse du texte envoyé par le serveur et il arrive souvent qu'il charge des greffons (plugins) tels que Flash pour l'exécution de code envoyé par le serveur, sans parler du code JavaScript que peut aussi lui envoyer le serveur. Or, les navigateurs, toujours plus complexes à mesure que le web s'enrichit en fonctionnalités, ne sont pas parfaits. Comme tous les logiciels, ils ont des bogues, et parfois ces bogues sont à la source de vulnérabilités exploitables par un attaquant pour prendre le contrôle d'un ordinateur sans que la victime ait autre chose à faire que visiter un site web particulier. En général, lorsque les éditeurs de navigateurs découvrent des vulnérabilités, ils les corrigent, mais un utilisateur utilise parfois une version périmée du navigateur, toujours exposée à une attaque connue publiquement. Il arrive aussi que des vulnérabilités soient uniquement connues de l'attaquant et non de l'éditeur du navigateur ; ce type de vulnérabilité est appelée *vulnérabilité zero-day*.

La NSA dispose d'un ensemble de serveurs sur l'internet public désignés sous le nom de code « FoxAcid », dont le but est de déployer du code malveillant. Une fois que des serveurs Quantum ont redirigé une cible vers une URL spécialement forgée et hébergée sur un serveur FoxAcid, un logiciel installé sur ce serveur se sert d'une boîte à outils d'exploitation de failles pour accéder à l'ordinateur de

l'utilisateur. Cette boîte à outils couvre vraisemblablement des vulnérabilités connues, utilisables contre des logiciels périmés, et des vulnérabilités *zero-day*, en règle générale réservées à des cibles de haute valeur [2]. Nos sources indiquent que l'agence utilise ensuite ce code malveillant initial pour installer d'autres logiciels à le plus long terme.

Quand un attaquant réussit à infecter une victime avec du code malveillant, il dispose d'ordinaire d'un accès complet à l'ordinateur de cette dernière : il peut enregistrer les saisies du clavier (qui peuvent révéler mots de passe et autres informations sensibles), mettre en route la webcam ou lire n'importe quelle donnée conservée sur cet ordinateur.

Que peuvent faire les utilisateurs pour se protéger ?

Nous espérons que ces révélations pousseront les éditeurs de navigateurs à agir, que ce soit pour renforcer leurs logiciels contre les failles de sécurité ou pour tenter de détecter et de bloquer les URL utilisées par les serveurs FoxAcid.

Entre-temps, les utilisateurs soucieux de leur sécurité s'efforceront de suivre des pratiques de nature à assurer leur sécurité en ligne. Gardez toujours vos logiciels à jour, en particulier les greffons des navigateurs tels que Flash, qui nécessitent des mises à jour manuelles. Assurez-vous de bien faire la différence entre les mises à jour légitimes et les avertissements sous forme de pop-ups qui se font passer pour des mises à jour. Ne cliquez jamais sur un lien suspect dans un courriel.

Les utilisateurs qui souhaitent aller un pas plus loin – selon nous, tout le monde devrait se sentir concerné –, utiliseront l'activation en un clic de greffons Flash ou Java de manière à ce que ces derniers ne soient exécutés sur une page web qu'à la condition que l'utilisateur l'approuve. Pour Chromium et

Chrome, cette option est disponible dans Paramètres => Afficher les paramètres avancés => Confidentialité => Paramètres du contenu => Plug-ins.

La même chose peut être faite pour Firefox à l'aide d'une extension comme Click to Play per-element. Les greffons peuvent également être désactivés ou complètement désinstallés. Les utilisateurs devraient également utiliser un bloqueur de publicité afin d'empêcher les requêtes superflues du navigateur destinées aux publicitaires et aux pisteurs du web. Ils devraient en outre utiliser l'extension HTTPS Everywhere afin d'utiliser le chiffrement des connexions associées à HTTPS sur le plus de sites possibles.

Si vous êtes un utilisateur prêt à supporter quelques désagréments au bénéfice d'une navigation plus sûre, regardez du côté de NotScripts (Chrome) ou de NoScript (Firefox), qui permettent de limiter l'exécution des scripts. Cela signifie qu'il vous sera nécessaire d'autoriser par un clic l'exécution des scripts un à un. JavaScript étant très répandu, attendez-vous à devoir cliquer très souvent. Les utilisateurs de Firefox peuvent s'orienter vers une autre extension utile, RequestPolicy, qui bloque le chargement par défaut des ressources tierces sur une page. Ici aussi, votre navigation ordinaire pourrait être perturbée car les ressources tierces sont très utilisées.

Enfin, pour les plus paranoïaques, HTTP Nowhere permettra de désactiver l'ensemble du trafic HTTP, avec pour conséquence que votre navigation sera entièrement chiffrée et, par la même occasion, limitée aux seuls sites offrant une connexion HTTPS.

Conclusion

Le système de la NSA pour déployer les logiciels malveillants n'a rien de particulièrement novateur, mais avoir un aperçu de la façon dont il opère devrait aider les utilisateurs et les éditeurs de logiciels et de navigateurs à mieux se défendre

contre ces types d'attaques, et contribuer à une meilleure protection de tous contre les criminels, les agences de renseignement et une pléthore d'autres attaquants. C'est pourquoi nous jugeons vital que la NSA soit transparente quant à ses capacités et aux failles ordinaires de sécurité auxquelles nous sommes exposés — notre sécurité en ligne en dépend.

---

1. Le terme « homme du milieu » est parfois réservé aux attaques sur les connexions sécurisées par cryptographie, par exemple au moyen d'un certificat SSL frauduleux. Dans cet article, toutefois, on entend plus généralement toute attaque où l'attaquant s'interpose entre un site et la victime.
2. D'après l'article de The Guardian, « Les exploits les plus précieux sont réservés aux cibles les plus importantes ».