Sécurité : quand les experts se trompent de cibles

Dans le monde de la sécurité informatique, il est tentant de crier au loup, en particulier quand on est un acteur proposant des solutions permettant d'éviter que le loup en question ne vienne voler vos données.

Mais y a-t-il vraiment danger ? Parfois, la cupidité des éditeurs de solutions de sécurité prime sur leur sens de la mesure. En témoigne le discours opéré autour du système d'exploitation mobile **Android.** Et les spécialistes de clamer qu'il est le plus attaqué, et que l'on y découvre de nouvelles menaces chaque jour. Le plus attaqué, c'est une affirmation gratuite, mais probablement exacte : il est vrai qu'Android est le plus utilisé des OS mobiles et donc une cible de choix pour les pirates.

Le robot de tous les dangers

Quant aux menaces… c'est ici que la désinformation survient. De nombreux mécanismes de protection empêchent les programmeurs de créer des applications malveillantes. Les logiciels sont principalement écrits en **Java** et tournent au sein de la machine virtuelle Dalvik. Or, cette dernière filtre très efficacement toutes les interactions entre l'application et l'OS.

Lorsque vous installez une application, vous savez exactement ce qu'elle aura le droit de faire. Les logiciels malveillants les plus dangereux doivent impérativement disposer **de droits élargis**, voire d'un terminal â€˜rooté'. Bref, ce n'est pas en téléchargeant une application depuis Google Play sur un terminal â€˜non bidouillé' que vous risquez quoi que ce soit. à€ condition toutefois de regarder avec soin ce que l'application exige. Si elle demande à accéder à votre liste d'appels, il semble logique qu'elle le fasse.

Et c'est bien ce point qui est gênant. La prolifération d'applications indiscrètes – principalement pour des raisons marketing liées à l'exploitation de vos données personnelles – devient un réel souci. Aujourd'hui vous n'avez que deux choix : accepter cette fuite de données ou refuser d'installer l'application. Ennuyeux.

Des failles vieilles de 10 ans

Régulièrement la presse se fait l'écho de corrections de failles se trouvant dans les logiciels depuis des années. Dernier exemple en date, « Un algorithme de compression corrige une faille vieille de 20 ans ». Doit-on en déduire que des pirates pouvaient utiliser cette faille depuis 20 ans ? Bien sûr que non.

Pour exploiter une faille, il faut au préalable connaître son existence. L'éternelle histoire de la charrue et des bœufs. Le véritable problème est de savoir si les experts en sécurité qui ont trouvé cette faille en premier se trouvent du bon (white hat) ou du mauvais (black hat) côté de la barrière.

Bref, une faille vieille de â€˜xx' années n'est pas fondamentalement un problème. Tout dépend des

cas. Sur un algorithme complexe, c'est la remise en cause d'un raisonnement passé admis comme fiable qui permet de découvrir les biais contenus dans le code. Avant cette remise en cause, nous n'avions pas les moyens de savoir que le code concerné n'était pas sur, ni les moyens de le mettre en défaut.

La situation est totalement différente avec les oublis évidents, mais que personne n'a vus. Par exemple le fait que les rapports de bogues de Windows soient émis en clair sur Internet (voir l'article « Un milliard de PC touchés par une faille béante dans l'outil de rapport d'erreur de Windows »). Autre souci, les failles trouvées, mais non corrigées par les éditeurs. Peu importe alors que la vulnérabilité date de seulement trois jours : si un â€˜exploit' existe, le danger est immédiat. Sinon, il est imminent.

Voir aussi

Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales