Un million de smartphones Android victimes d'un malware en 2011

Android est-il en train de devenir le Windows des plates-formes mobiles? Non pas en termes de part de marché, bien que l'OS de Google tourne sur un smartphone sur deux, mais bien en termes de risques face aux agents malveillants et attaques pirates.

Selon le rapport des menaces sur les mobiles de Lookout Mobile Security, société spécialisée dans la protection des mobiles, les smartphones sous Android sont aujourd'hui 2,5 fois plus exposés aux *malwares* qu'en début d'année. Et plus de trois utilisateurs sur dix sont susceptibles de croiser une menace sur leur téléphone chaque année.

Entre 500.000 et 1 million de personnes infectées

Ce tableau alarmiste est renforcé par l'annonce que, toujours selon Lookout Mobile Security, entre 500.000 et 1 million de personnes ont vu leur terminal Android infecté en 2011. Une fourchette un peu large projetée à partir des données récoltées dans le cadre de l'activité de l'entreprise. Laquelle s'appuie sur son réseau de surveillance basé sur une variété de sources de mesures dont les boutiques en ligne des éditeurs (Android Market et App Store essentiellement) et d'autres alternatives de distribution d'application.

Selon Lookout, son réseau permet de constituer *« la plus grande base de données des applications et des résultats de détection des agrégats à partir d'appareils mobiles à travers le monde »*. Au total, l'entreprise revendique quelques 700.000 applications et 10 millions de smartphones (Android et autres) sous surveillance.

400 malwares en circulations

La cause de phénomène d'amplification s'explique évidemment par le nombre toujours grandissant d'utilisateurs qui se tournent vers Android (Google déclare 550.000 activations par jour) qui entraîne inévitablement l'attrait des cybercriminels. Si Lookout comptait 80 *malwares* actifs en début d'année, il en recense plus de 400 aujourd'hui (en juin 2011).

« Les attaquants déploient une variété de techniques de plus en plus sophistiquées pour prendre le contrôle du téléphone, les données personnelles, et d'argent, explique l'entreprise de sécurité. *En outre, les auteurs de malwares utilisent des techniques de distribution, telles que les attaques par fausses publicités [malvertising comme GGTracker, NDLR] et mises à jour applicatives. »* L'appât du gain est d'autant plus actif que les paiements mobiles vont exploser. De 170 milliards de dollars de transactions en 2010, il devrait passer à 630 milliards en 2014. Ce sera l'occasion, pour les pirates, de tester les barrières de protection que les éditeurs mettront en place (l'offre Google Wallet notamment).

Android ou iOS ?

Les utilisateurs doivent-ils abandonner leur Android pour un iPhone, un BlackBerry ou autre? Difficile de juger lequel des OS est le plus sécurisés sachant que, par définition, les programmes informatiques sont rarement infaillibles. Certes, l'ouverture de l'OS de Google permet de créer et d'installer librement une application sur la plate-forme de distribution (Maket Place). Ainsi qu'à partir de nombreuses autres sources, de partenaires (Amazon's Appstore for Android, notamment)

si l'utilisateur active l'option. Mais Google compte sur les dizaines de milliers d'yeux de la communauté d'utilisateurs (plus ou moins avancés) pour repérer les logiciels dangereux. De plus, le système informe l'utilisateur qui installe une applications des services du téléphone qu'elle exploitera. Ce qui permet de repérer les bizarreries (l'accès aux conversations ou aux contacts, par exemple) et de rejeter l'installation en cas de doute. A condition d'être vigilent. Permissions que le système valide (ou non) et qu'il est normalement impossible de modifier par la suite.

Sur iOS, moins ouvert, la distribution d'une application passera par un contrôle humain (ou plus exactement un processus de contrôle manuel). Ce qui, *a priori*, tend à garantir l'inocuité de l'application (mais à aussi renforcer la censure). Sauf si l'utilisateur installe une application non issue de l'App Store après avoir dévérouillé (*jailbreaké*) son iPhone. Jailbreak qui s'appuie sur des vulnérabilités du système pour opérer. Un mode opératoire que l'on retrouve en ligne à l'image de la page, non infectieuse, de JailBreakMe. Vulnérabilité qu'Apple entend corriger à chaque nouvelle version d'iOS. En vain jusqu'à présent.

—

Sondage express