Pourquoi les téléphones sous Android sont les cibles quasi exclusives des malwares et comment s'en protéger au mieux

La quasi-totalité des attaques de virus sur un téléphone mobile contaminent un système Android alors que l'IOS de Mac reste largement préservé. Un schéma similaire était déjà constaté sur les ordinateurs.

Avec Catherine Lejealle

Atlantico : Une récente étude menée par l'entreprise américaine Cisco révèle que 99% des attaques de virus sur des smartphones ont eu lieu sur des systèmes Android tandis que le système IOS de Mac reste épargné. Comment expliquer des chiffres aussi conséquents ?

Catherine Lejealle : Cette étude 2014 de Cisco sur la sécurité révèle en effet deux chiffres intéressants : d'une part, 99% des attaques sur mobile visent des devices Android contre seulement 1% pour l'IOS d'Apple. D'autre part, 71% des usagers d'Android contre 14% des usagers d'Apple seraient potentiellement touchés par une attaque frauduleuse et malveillante quel qu'en soit le type : phishing, likejacking… Au moins deux raisons qui se conjuguent peuvent expliquer ces différences. **La première est technique, à savoir que l'IOS est davantage fermé voire verrouillé que le système Android, ouvert par définition et par philosophie.** L'autre raison est l'effet de parc. Il y a davantage de mobiles Android en circulation. Ceux-ci peuvent échanger, partager des données facilement et donc par viralité se contaminer mutuellement. C'est le principe de la contamination virale.

Le fait que les systèmes IOS soient épargnés s'explique t-il uniquement par la faible utilisation à l'échelle mondiale des produits Apple ?

Non l'effet de parc est une chose. L'ouverture d'Android en est une autre et elle est davantage responsable de la vulnérabilité d'Android. C'est à la fois sa grande force, être ouvert aux développeurs et financièrement moins cher, et sa fragilité. Si l'on poursuit l'analyse de l'étude Cisco, on constate en effet que les 99% de failles observées ne concernent pas des applications disponibles sur Google Play mais des applications repackagées par des tiers « véreux » et mis en ligne sur des sites non officiels. Leur conclusion est que le téléchargement d'applications sur le site officiel qu'est Google Play est tout aussi sécurisé que l'Apple store. Il ne faut donc pas que cet arbre de fraude cache la forêt et face renoncer à privilégier des solutions ouvertes et donc non propriétaires.

Pendant longtemps les utilisateurs d'ordinateur Mac ont pu se vanter de n'être pratiquement pas atteints par les virus, avant que ces derniers finissent par se développer aussi sur les machines à la pomme. Une

tendance similaire peut-elle se dessiner sur les smartphones avec la démocratisation de l'Iphone ?

L'ouverture d'Android rend la conception de virus plus facile mais la fermeture de l'IOS ne signifie pas que les usagers sont ad vitam aeternam à l'abri de tout danger. Il faudra sans doute plus de temps pour en concevoir mais on ne voit pas pourquoi à terme, ils pourraient ne pas être touchés à leur tour. Il faut rappeler le contexte actuel : nous sommes dans un transfert massif des usagers de l'ordinateur vers le mobile. L'an dernier il y a eu plus d'accès à Internet depuis un mobile que depuis un ordinateur. Et Facebook, Twitter et autres médias sociaux sont depuis plus longtemps plus utilisés depuis un mobile que depuis un ordinateur. Ceci ne va pas échapper aux personnes malintentionnées qui ne vont sans doute pas laisser échapper le marché des iPhones.

Les virus dans la téléphonie étaient encore l'exception il y a quelques années. Sont-ils amenés à se développer ?

Effectivement, l'étude Cisco permet de relativiser sur les dangers actuels qu'on court avec un mobile puisque**les fraudes sur mobile ne représentent actuellement que 1,2% des fraudes liées aux accès Internet.** Malheureusement compte tenu de la croissance exponentielle des usagers d'Internet mobile, tout laisse à penser que ce chiffre ne fera que croître. Une fois encore, ne nous privons pas de piocher dans Google Play qui reste entièrement sécurisé comme le montre cette étude Cisco et d'une richesse déjà difficile à épuiser qui s'enrichit toutes les secondes. Alors pourquoi chercher plus loin pour le moment quand on s'arrive déjà pas à épuiser ce qui est disponible en toute sécurité?