Comment débarrasser votre smartphone des logiciels malveillants qui plombent vos navigateurs Internet en affichant des pubs intempestives

Outre la navigation sur ordinateur, celle sur smartphone est également perturbée par l'affichage de publicités intempestives. Bien que la plupart sont inoffensives, certaines présentent des failles de sécurité que les cybercriminels exploitent en vue de dérober vos données personnelles ou de bloquer votre téléphone. Tous les conseils pour vous prémunir contre cette menace.

Avec Gérôme Billois

Atlantico : Depuis que les téléphones mobiles permettent de naviguer sur Internet aussi rapidement et efficacement que sur les ordinateurs, ils sont devenus une plate-forme pour les campagnes publicitaires. Comment se fait-il que ces publicités pour smartphones soient parfois tellement intrusives qu'elles empêchent la navigation ?

Gérôme Billois : Plusieurs études montrent que les internautes utilisent davantage leur téléphone ou leur tablette que leur ordinateur pour naviguer sur le Web, ce qui en fait une plate-forme privilégiée pour les régies publicitaires. Cela a en effet amené certaines d'entre-elles à être parfois très envahissantes, au point d'empêcher ou de ralentir très fortement la navigation. Si la plupart d'entre-elles n'ont pas pour autre objectif que d'être vues par l'utilisateur, **certaines publicités peuvent représenter un risque plus important en forçant ou tentant de vous faire installer des logiciels malveillants.**

Ces publicités renvoient parfois aux App stores, et demandent de télécharger des applications qui n'ont rien à voir avec les sites qui étaient consultés. Ces publicités intrusives peuvent-elles également servir de "trojans", de logiciels malveillants ?

Le plus généralement, ces publicités malveillantes visent à l'installation d'un "adware" pour afficher la publicité en continu dans votre téléphone.

Mais dans certains cas, oui, des usages plus malveillants ont été rencontré. U**n smartphone regorge d'informations personnelles**. Il est bien connu que certains groupes de cyber criminels – aux motivations plus ou moins lucratives – installent des *"malwares"* en les faisant passer pour des publicités. **Ces logiciels malveillants peuvent en effet être des chevaux de Troie et donner la possibilité aux tiers qui les contrôlent d'agir sur le téléphone sans que l'utilisateur ne s'en rende vraiment compte.**

Les instigateurs de ces pratiques frauduleuses utilisent alors le réseau publicitaire pour distribuer leurs programmes.**Ils identifient les failles présentes dans les processus de publication de publicité** pour ensuite distribuer une publicité piégée qui installera un

logiciel pour prendre la main sur le téléphone, voler des contacts, identifier la localisation etc.

Existe-t-il des solutions pour s'en prémunir ?

Pour les publicités qui s’affichent en plein écran légitimement, il faut essayer d’appuyer sur le bouton qui renvoie au menu principal ou cliquer sur la croix. Cela permet dans la plupart des cas de redémarrer une navigation normale.

Pour les publicités malveillantes, cela se fait avant tout par de**la prévention.** Premièrement à destination des régies publicitaires : celles-ci doivent être attentives aux contournements et détournements malveillants potentiels de leurs publicités pour combler leurs lacunes. Et deuxièmement, à destination de l’utilisateur du mobile. Pour éviter tout tracas, il est, par exemple, recommandé de suivre quelques règles simples comme le fait de **toujours installer les mises à jour des appareils électroniques. Leurs constructeurs s’efforcent en effet à combler les failles de sécurité, et ne pas les installer reviendrait à laisser le champ libre aux logiciels malveillants**. Ensuite, il est vivement déconseillé de télécharger des applications en provenance de "stores" non officiels et privilégier celles qui sont natives, c’est-à-dire installées dès l’achat du téléphone (l’App Store et Google Play respectivement sur iPhone et Androïd). En effet, les "stores" non officiels profitent de l’innocence des utilisateurs pour glisser des malwares dans les dossiers qu’ils téléchargent.

Récemment, on a ainsi vu de **nombreux Français pris au piège lorsqu’ils ont voulu télécharger la fameuse application Pokémon Go** : puisqu’elle n’était pas encore officiellement disponible en France, nombre de jeunes gens ont téléchargé le jeu sur des stores malveillants, qui ont eu accès à leurs informations personnelles, ou qui ont pu tenter de bloquer l’usage de leur téléphone. D’une manière générale et comme souvent, il faut rester vigilant, et se méfier des occasions un peu trop alléchantes.

Une autre solution envisageable peut être l’installation d’un "Ad-block", qui s’utilise aussi sur les ordinateurs. Ces logiciels permettent en effet de limiter les avalanches de publicités mais je ne prônerai pas cette solution car **ils suppriment les publicités sans distinction**, et portent donc atteinte à l’économie du Web dont le principal business model est la publicité légitime.

Propos recueillis par Victoire Barbin Perron