

Sécurité : plus de 11 millions de smartphones infectés en permanence

Environ 11,6 millions de smartphones sont infectés à tout moment par des logiciels malveillants dans le monde. C'est ce qui ressort du rapport 2013 ([disponible en PDF](#)) de **Kindsight Security Labs, filiale d'Alcatel-Lucent**, qui tire ses données des solutions de sécurité réseau déployées chez les clients (et profitera du Mobile World Congress 2014 pour présenter une solution de sécurité). L'analyse des trafics réseaux permet ainsi au fournisseur de détecter les attaques de logiciels malveillants et les risques pour les systèmes d'informations, depuis les PC, les terminaux mobiles, et les réseaux résidentiels.

60% des infections pour Android

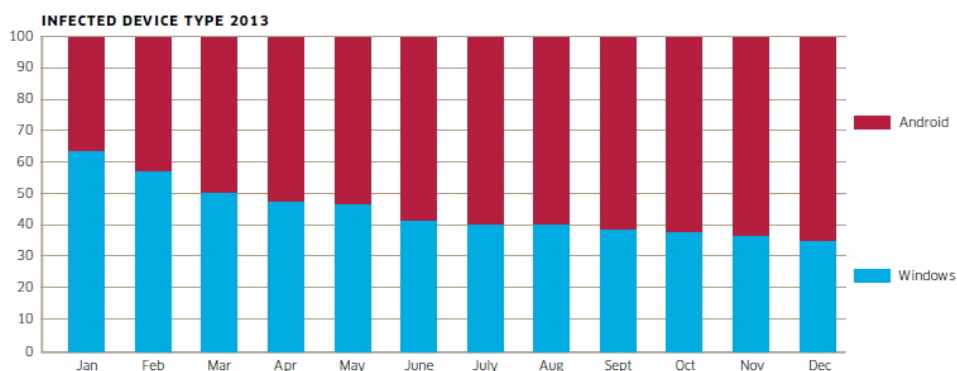
Sans surprise, une large majorité (60%) des infections des réseaux mobiles provient des smartphones Android. Un phénomène qui s'explique par le poids de cet OS sur le marché (avec [plus de 80% des ventes de smartphones](#)), hégémonie qui attire évidemment l'attention des cybercriminels. Mais aussi par la facilité avec laquelle il est possible de **propager les agents infectieux depuis des magasins applicatifs alternatifs à l'Android Market**.

« Les pirates informatiques bénéficient ainsi d'un mécanisme non réglementé pour distribuer leurs logiciels malveillants, qui peuvent aisément échapper à la détection des anti-virus basés sur les terminaux. C'est pourquoi nous observons en 2013 une tendance croissante d'opérateurs qui proposent à leurs abonnés un service de sécurité avec un anti-virus basé sur le réseau », commente Kevin McNamee, architecte sécurité et directeur de Kindsight.

L'infection par installation d'applications douteuses n'est pas le seul mode de propagation des maliciels. Ces derniers peuvent aussi **se propager depuis le store de Google** (ça arrive) ou **un e-mail, voire un SMS de phishing**.

iPhone, BlackBerry et Windows Phone épargnés

Les 40% restant d'infections des réseaux mobiles proviennent d'ordinateurs portables Windows connectés par partage de connexion (tethering) à un téléphone ou directement depuis une clé USB mobile ou un routeur portable wifi. Mais la tendance est à la **forte baisse**, la plate-forme Windows passant d'un taux d'infection de plus de 60% en début d'année à environ 35% en décembre. Android suivant, lui, le chemin inverse. *« Au final, les iPhone, BlackBerry et Windows Phone représentent moins de 10% des infections répertoriées », note Kindsight.*



Vols de données et attaques DDoS

Les malwares, dont **le nombre a été multiplié par 20 en 2013** pour approcher les 450 000 au total, permettent essentiellement aux attaquants de voler des données (personnelles ou professionnelles) des utilisateurs et d'exploiter leurs terminaux à des fins criminelles. Le rapport note que les malwares sont également utilisées à des fins d'attaques par déni de service (DoS) ciblant les entreprises et gouvernements. Nouveauté 2013, l'arrivée massive de *spywares* **transformant smartphones et tablettes en appareils espion** pour localiser, télécharger des listes de contacts, intercepter/envoyer des messages, enregistrer des conversations ou encore prendre des photos à l'insu du propriétaire de l'appareil. Charmant.

Si les infections mobiles augmentent, celles affectant les réseaux fixes restent stables, autour de 10% du total sur l'année. On observe même une baisse entre octobre (9,6%) et décembre (8,7%). Mais 6% du total des clients résidentiels sont infectés par **des virus de niveaux élevés**: bots (tâches automatisées), root-kits (présence invisible), chevaux de Troie bancaires (vol de données financières). Parmi ceux là, ZeroAccess, Alureon, the Zeus banking Trojan, Uapush, Coogos, NotCompatible et QDPlugin.

crédit photo © Slavoljub Pantelic – shutterstock

En complément :

[Toute l'actualité sécurité sur Silicon.fr](http://silicon.fr)