chaque nouvelle génération, ils intègrent davantage de fonctionnalités auparavant réservées aux ordinateurs personnels. Et alors même que les téléphones mobiles commencent à faire office d'appareils photo, de caméras vidéo, de navigateurs GPS et de lecteurs de fichiers musicaux, leurs prix baissent : les opérateurs de téléphonie subventionnent en effet leur achat, car ils espèrent que ces nouvelles fonctionnalités encourageront les consommateurs à souscrire à davantage de services.

En outre, les téléphones mobiles intelligents se répandent de plus en plus dans les pays émergents. Certains de ces pays pourraient renoncer à mettre en place une infrastructure Internet câblée pour s'orienter vers un réseau numérique sans fil, beaucoup moins cher à construire et à entretenir – et, du point de vue de la censure, plus simple à surveiller. Si ces prévisions se révèlent correctes, les téléphones mobiles intelligents formeront l'essentiel du parc informatique mondial dans un avenir proche. Une multitude d'utilisateurs peu expérimentés en matière de protection informatique navigueraient alors sur la Toile à l'aide de leurs téléphones. Pour les concepteurs de virus, ils représenteraient une cible de choix.

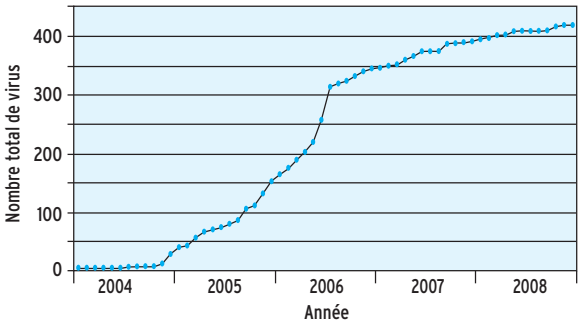
L'un des enseignements apportés par le fléau des virus informatiques est que plus une cible est vaste, plus elle attire les programmeurs mal intentionnés. La grande majorité des virus pour ordinateurs personnels sont conçus pour fonctionner sur le système d'exploitation omniprésent *Microsoft Windows*. Pour la même raison, presque tous les vers et chevaux de Troie de mobiles mis en circulation jusqu'à présent infectent le système d'exploitation *Symbian*, qui domine le marché des téléphones mobiles intelligents, équipant notamment ceux de *Nokia, Samsung, Sony Ericsson* et *Motorola*. À l'inverse, seules quelques variétés de virus menacent les appareils *Pocket PC* ou *Windows Mobile* de *Microsoft*, *Treo* de *Palm* ou *Research in motion* de *Blackberry*.

iPhone : la chasse est ouverte

L'augmentation du nombre de virus sur les *smartphones* a connu une brusque accélération en 2006, en raison des failles du *Bluetooth*, encore récent sur les mobiles à cette époque. Depuis, la plupart de ces failles ont été comblées, et les nouveaux virus sont devenus plus rares *(voir le graphique ci-dessous)*. De surcroît, le marché des systèmes d'exploitation de téléphones mobiles s'est diversifié, avec notamment l'arrivée d'*Android* de *Google* et d'*iPhone OS* (le système d'exploitation de l'*iPhone*) d'*Apple*, ce qui diminue le risque de vastes « épidémies ».

Ces deux systèmes proposent des modèles de sécurité originaux, fondés sur des boutiques en ligne, respectivement *Android market* et *App store*, qui centralisent les applications utilisables. La ressemblance s'arrête là, car *Android* fonctionne sur un principe d'ouverture totale : n'importe qui peut mettre en ligne une application sur *Android market*. Le processus de mise en ligne implique cependant d'inclure une description de tout ce que fait l'application, et lors du téléchargement, l'utilisateur voit cette description et est libre d'accepter ou non. Il voit aussi sur *Android market* le nombre de téléchargements et les éventuels commentaires d'autres utilisateurs, ce qui lui permet de juger de la fiabilité d'une application. Pour l'instant, ce modèle fonctionne et aucun virus n'a été détecté sur *Android* (sans doute aussi parce que ce système ne représente que deux pour cent de part de marché et n'est donc pas une cible très alléchante pour les hackers).

IPhone OS, quant à lui, est beaucoup plus fermé : chaque développeur doit payer une inscription sur *App Store* et faire valider son application par *Apple*, qui contrôle ainsi sévèrement ce qu'il est possible d'exécuter avec un *iPhone*. Mais est-on vraiment sûr qu'aucune application présente sur l'*App Store* n'est malveillante ? *Apple* reste flou sur ses méthodes de validation, de sorte qu'il est difficile d'évaluer leur efficacité. Le problème est complexe, et il n'existe pas à l'heure actuelle de moyen automatique pour reconnaître une application malveillante. Un cas est particulièrement délicat : celui de fonctions cachées qui ne se déclenchent que dans certaines conditions. On parle de bombe logique lorsque ces fonctions endommagent le système infecté, et d'*easter egg* (« œuf de Pâques ») lorsqu'elles sont inoffensives.



L'augmentation du nombre de virus sur les *smartphones* a connu une brusque accélération en 2006, puis s'est essoufflée, comme le montre cette courbe établie par l'entreprise *F-Secure*.

En mai et en août 2009, des développeurs ont réussi à glisser de telles fonctions cachées dans leurs logiciels à l'insu d'*Apple*, qui les a mis en ligne sur l'*App Store*. Il ne s'agissait heureusement que d'*easter eggs*, mais cela révèle tout de même les failles du système. Celui-ci complique malgré tout la tâche des cybercriminels, dont l'application serait retirée de l'*App Store* une fois démasquée.

Ce type de modèle de sécurité pourrait d'ailleurs s'imposer sur les mobiles, même si Mikko Hypponen, qui travaille pour une firme de sécurité informatique – la seule qui ait développé un antivirus pour téléphone mobile – semble préconiser une solution fondée sur des logiciels antivirus. Quoi qu'il en soit, la menace sur les mobiles est bien réelle. L'*iPhone*, en particulier, excite la convoitise des *hackers* du fait de sa grande popularité, garante d'une certaine publicité pour celui qui réussira à le contaminer.

Daniel Reynaud, Laboratoire lorrain de recherche en informatique et ses applications (LORIA)