VRAI OU FAUX

Les *Mac* résistent-ils mieux aux virus que les *PC* ?

Non, ou à peine mieux. Les Mac *étaient moins victimes de virus, car leur nombre assez faible en faisait des cibles moins intéressantes pour les pirates informatiques, mais la situation commence à changer…*

Jean-Yves Marion

Récemment, plusieurs virus ont attaqué les *Mac*. Le virus *Flashback*, démasqué en mars de cette année, aurait contaminé environ 600 000 de ces ordinateurs. Dès lors, on s'interroge : les *Mac* sont-ils aussi résistants aux virus qu'on le dit parfois ?

On désigne souvent les programmes malveillants (cheval de Troie, vers…) par le terme générique de virus. Les virus infectent les ordinateurs à des fins variées : voler des informations, envoyer des spams, récolter de l'argent par des mécanismes divers… Ainsi, *Flashback* envoie les internautes vers des sites « pirates », dont les propriétaires paient 0,65 centime d'euro aux concepteurs du virus chaque fois qu'un internaute arrive sur leur site. De tels virus ont donc intérêt à contaminer le plus d'ordinateurs possible.

Pour infecter un système informatique (navigateur Internet, système d'exploitation…), un virus utilise deux méthodes, souvent combinées. La première consiste à inciter l'internaute à cliquer sur un fichier contenant un programme caché, qui s'exécute alors. Le fichier peut être un lien Internet (prétendument destiné à télécharger une mise à jour, par exemple), une image, un document PDF ou *Word*…

La seconde méthode exploite les failles – ou bugs – d'un logiciel. L'utilisateur est vulnérable dès qu'il est connecté à Internet. Par exemple, une faille de *Word*, aujourd'hui corrigée, « ouvrait une porte » lorsque le logiciel chargeait des polices ; un programme malveillant pouvait alors s'infiltrer dans l'ordinateur et dicter ses instructions.

Les *Mac* sont-ils moins vulnérables face à ces deux méthodes ? Leurs utilisateurs risquent moins de cliquer sur des liens frauduleux, car ils passent le plus souvent par l'*Appstore* (une plateforme de téléchargement contrôlée par *Apple*), mais le risque n'est pas nul. Quant à la seconde méthode, l'exploitation des failles, il est difficile de se prononcer. À l'origine, *Mac OS*, le système d'exploitation des *Mac*, a été élaboré à partir d'un système *Unix*, qui contient *a priori* moins de failles que les autres : en effet, c'est un logiciel libre (son programme est public), de sorte qu'il est en permanence analysé et corrigé par une vaste communauté d'utilisateurs. Cependant, depuis, *Mac OS* a évolué de façon notable et plus ou moins opaque, perdant probablement cet avantage, tandis que la sécurité de *Windows* a progressé.

Pas de système infaillible

Plus généralement, il est impossible de garantir qu'un programme n'a pas de faille et Fred Cohen, de l'Université de Californie, a montré dans les années 1980 qu'il ne peut exister d'antivirus infaillible. Ces résultats sont liés à l'indécidabilité algorithmique, découverte par le père de l'informatique, Alan Turing, qui aurait eu 100 ans en 2012. Dès lors, tous les systèmes informatiques sont vulnérables : les ordinateurs, les tablettes, les smartphones, les imprimantes… C'est aussi le cas des systèmes industriels, qui sont connectés aux réseaux informatiques et pilotés par des programmes. Ainsi, le virus *Stuxnet* s'est attaqué aux centrifugeuses des centrales nucléaires iraniennes.

La rareté des virus pour *Mac* résulte donc plus de raisons économiques – les *Mac* étant environ 13 fois moins nombreux que les *PC* en 2012, les virus rapportent moins – que d'une solidité informatique intrinsèque. Les *Mac* sont peut-être un peu plus résistants, notamment grâce à leur système d'exploitation fondé sur *Unix*. Toutefois, si elle existe, cette supériorité est faible et ne résistera pas longtemps lorsque les enjeux économiques justifieront des attaques massives. C'est ce qui commence à se produire. Selon l'entreprise de sécurité informatique *Symantec*, *Flashback* aurait rapporté plus de 8 000 euros par jour à ses concepteurs !

Un moyen simple de limiter les risques d'infection est d'avoir un comportement « raisonnable » sur Internet. Un antivirus est-il utile ? Un *PC* sans antivirus est vite envahi par les codes malveillants. Ce n'est pas le cas des *Mac* pour l'instant, mais, nous l'avons vu, c'est surtout en raison d'un relatif désintérêt des concepteurs de virus. Si les *Mac* acquièrent des parts de marché comparables aux *PC*, les antivirus deviendront nécessaires… ■

Jean-Yves MARION dirige le Laboratoire de haute sécurité (LHS) et est codirecteur du Laboratoire lorrain de recherche en informatique et ses applications (LORIA), à l'Université de Nancy.