

Attention aux fausses copies de Windows 7

A l'heure où Microsoft propose au grand public [la version RC](#) (*Release Candidate*) de Windows 7, des **copies pirates infectieuses** circulent sur les réseaux d'échanges P2P depuis le 24 avril. C'est du moins ce qu'annoncent plusieurs internautes sur les forums de plates-formes d'échange BitTorrent.

Sur le [forum](#) de Neowin.net, un certain Franck Fontaine prévient que « *un grand nombre de téléchargements [de Windows 7 RC] contiennent un cheval de Troie dans le fichier Setup.exe. [...] si vous avez fait la mise à jour, vous êtes peut-être infectés* ». L'internaute a décelé dans le programme d'installation un fichier 'codec.exe' qui s'avère être l'agent malveillant au côté du 'setup.exe' apparemment sain. D'autres constatations du même acabit se lisent sur les forums de Mininova.org.

Les mécanismes du fichier infectieux sont encore mal connus. Mais selon WuNgUn, sur Mininova.org, codec.exe cacherait un cheval de Troie « générique » qui téléchargerait **un faux logiciel anti-virus** et installerait un rootkit indétectable par les solutions de sécurité légitimes. Faux anti-virus qui alertera l'utilisateur que son système est infecté (effectivement ou non) et l'invitera à acheter une nouvelle version du logiciel de sécurité pour désinfecter son environnement. Une forme moderne de racket connue sous le terme de *scareware*.

« *C'est arrivé rapidement, bien qu'il ne faille pas s'en étonner* », commente Alex Kochis, directeur de Windows Genuine, le programme de certification des versions de Windows. « *Cela montre hélas qu'il y en a qui voient dans Windows 7 une opportunité pour tirer profit des autres* », écrit-il sur son [blog](#).

L'utilisation de fausses copies de logiciels comme vecteur d'infection n'est pas nouvelle ni récente. De Microsoft à Apple en passant par Adobe, les versions piratés des logiciels phares du marché sont **régulièrement porteurs d'agents infectieux**. Dans le cas de Windows 7 RC, il est plutôt conseiller de le [télécharger](#) depuis le site officiel de Microsoft. Cette version RC restera opérationnelle jusqu'en juin 2010 avec une dégradation des services à partir de mars. Cette offre de téléchargement gratuite ouverte à tous devrait, espérons-le, mettre un terme aux diffusions des versions infectieuses de Windows 7.