

Sécurité : parfois la menace vient de l'éditeur!

Les utilisateurs d'Internet doivent faire preuve de prudence face aux fausses alertes de sécurité, rappelle Sophos, leader mondial de la sécurité et du contrôle des réseaux.

En Corée du Sud, une femme vient ainsi d'être mise en examen pour avoir vendu un faux logiciel antivirus à plus de 4 millions de personnes. La justice du pays accuse en effet cette femme de 41 ans d'avoir gagné plus de 6 millions d'euros en distribuant du « scareware » (fausses alertes de sécurité).

Lee Shin-Ja, ancienne présidente de la société Media Port, est accusée d'avoir gagné plus de 9,2 millions de won (environ 6,4 millions d'euros) depuis 2005 avec un programme de scareware qui affichait de fausses alertes de sécurité. Celles-ci incitaient les utilisateurs à acheter le programme Doctor Virus de Media Port pour 3.850 won (2,67 euros) par mois.

Selon le Bureau du Procureur de Séoul Central District, Madame Lee aurait également engagé deux programmeurs, eux aussi mis en examen, pour l'aider dans cette opération.

« Les utilisateurs d'Internet sont de plus en plus nombreux à se préoccuper de la sécurité de leur ordinateur, et il n'est que trop facile à des gens sans scrupules de les piéger avec une fausse alerte », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud. « Dans cette dernière affaire, près de 4 millions de personnes auraient accepté de tester gratuitement ce logiciel, et 1,26 million l'auraient ensuite acheté. Avec de tels chiffres, il n'est pas surprenant que les autorités cherchent sérieusement à déterminer si des scarwares ont pu tromper un nombre encore plus grand d'utilisateurs. »

Selon les experts de Sophos, le marché sud-coréen comprend des

centaines de logiciels de sécurité concurrents, dont beaucoup sont inconnus dans le reste du monde.

« Contrairement à la plupart des autres pays, les utilisateurs sud-coréens font fréquemment appel à plusieurs logiciels antivirus en même temps, sans doute parce que beaucoup de solutions locales ne disposent pas d'une fonction d'analyse sur accès, poursuit Michel Lanaspèze. Cet environnement particulier augmente la probabilité pour que les gens téléchargent un produit trouvé par hasard sur Internet. Il semble malheureusement que certains cybercriminels soient prêts à tout pour gagner des parts de marché, y compris effrayer les utilisateurs pour leur faire acheter une solution de sécurité sans s'informer au préalable. »

Un porte-parole de Doctor Virus, dont le nom n'est pas cité, a affirmé que leur logiciel n'affichait désormais plus de fausses alertes de sécurité.