



Forum: Trucs en vrac

Topic: Quand un raccourci Windows peut flinguer votre sécurité

Subject: Quand un raccourci Windows peut flinguer votre sécurité

Publié par: Wullfk

Contribution le : 24/12/2016 14:06:15

Citation :

Un chercheur Français découvre comment il est possible de télécharger et exécuter n'importe quel fichier en utilisant un outil natif de Windows. Une porte ouverte pour des infiltrations malveillantes.

Notre ami Jean-Pierre LESUEUR, le fondateur de Phrozen software n'est plus à présenter. Ce chercheur en sécurité informatique, auteur de nombreux logiciels permettant de contrer pirates et codes malveillants vient de trouver une petite finesse dans l'ensemble des Windows, et cela à partir du SP2 de Windows XP qui risque de faire réagir rapidement le géant américain. Le problème est simple, à travers un raccourci Windows, il est possible de télécharger et exécuter n'importe quel fichier en utilisant un outil natif de Windows. « **Du coup forcé**, explique Jean-Pierre Lesueur, **indétectable par les Antivirus actuels car un raccourci n'est pas directement un fichier exécutable** » .

Seulement, cette première découverte a fait suite à une seconde 100 fois plus vicieuse encore. Réussir à injecter une application directement dans le raccourci, ainsi plus besoin de télécharger et exécuter le code malveillant. Bilan, les pare-feu ne risquent plus de bloquer la potentielle attaque. Bref, une nouvelle couche problématique.

Lire la suite...source : [ZATAZ](#)

Un script .vbs, Je pense qu'un outil comme [Marmiton](#) peut s'avérer utile