# Un cheval de Troie cible les anciennes versions de Windows

Des chercheurs de l'éditeur Symantec ont annoncé avoir découvert un cheval de Troie dont la fonction est d'usurper l'identité de l'utilisateur de l'OS en se présentant comme un processus de réactivation (ndlr : WGA) des produits Microsoft. Il demande aux utilisateurs de saisir leurs identifiant bancaires pour réactiver la machine…

*« Surnommé**Kardphisher**, ce cheval de Troie n'est pas si technique qu'il en a l'air »* déclare Takashi Katsuki un ingénieur de Symantec. Par contre, l'auteur de ce code malveillant *« s'est donné beaucoup de mal pour donner un aspect authentique à son attaque »*poursuit Katsuki.

Une fois ce malware installé, des messages commencent à apparaître. Ces derniers ont pour mission de faire croire à l'utilisateur que sa version de l'OS n'a pas été enregistrée. L'on peut par exemple lire le message suivant *» pour nous aider à réduire le piratage de Windows, veuillez réactiver votre copie de Windows. »*

En réalité, le but de la man?uvre est de persuader la cible du caractère authentique de l'alerte puis de lui demander ses informations bancaires confidentielles pour réactiver l'OS…

*« Si la victime coche la case non »* indique Katsuki, *« son ordinateur va s'éteindre. En cliquant sur Oui l'utilisateur est redirigé vers une page lui demandant des informations confidentielles, nom adresse, numéro de carte de crédit… » Bien entendu, ses informations ne vont pas chez Microsoft, mais elles sont stockées sur le serveur du hacker. »*

*« Le seul mérite de ce trojan est de nous donner une bonne leçon »* ajoute Katsuki : *« Sur le Web il ne faut faire confiance à personne ».*

D'après le chercheur, les OS ciblés par ce cheval de Troie sont : Windows 95, 98, 2000, NT et Server 2003.

Si pour l'instant Vista n'est pas touché par Kardphisher, Katsuki pour sa part estime que le risque reste élevé pour cet OS qui est encore plus adepte du principe de réactivation. Preuve en est au mois de janvier 2007, Microsoft a publié un correctif concernant un bogue dans le système anti-piratage de Vista.