G-Data : De faux logiciels dâ□□optimisation du systÃ¨me disponibles sur Internet
Internet
PostÃ© par : JPilo
PubliÃ©e le : 13/12/2010 11:00:00

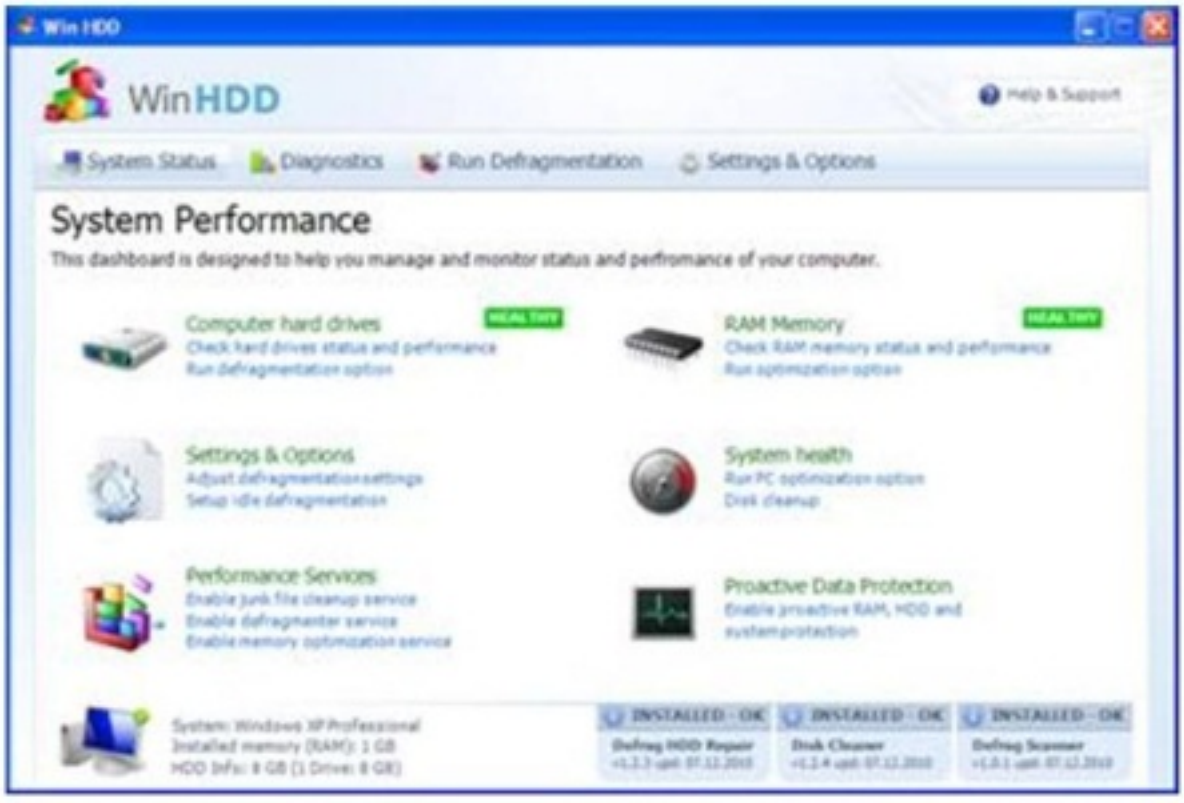
Un nouveau type de faux logiciel fait son apparition sur Internet. Depuis quelques semaines, la catÃ©gorie des Â« scarewares Â», ces logiciels dits Â« de la peur Â», compte en plus des trÃ¨s rÃ©pandus faux antivirus, de faux logiciels dâ□□optimisation.

Sous la promesse de rÃ©parer et dâ□□optimiser le systÃ¨me dâ□□exploitation, ces logiciels nâ□□ont quâ□□un but : allÃ©ger la victime dâ□□une cinquantaine dâ□□euros.

Les premiÃ¨res variantes de ce nouveau type de logiciels malveillants sont apparues il y a quelques semaines sous diffÃ©rentes appellations : System Defragmenter, Scan Disk, Check Disk ou encore Win HDD.

Ralf BenzmÃ¼ller, Directeur du G Data SecurityLabs commente cette arrivÃ©e : " *les cybercriminels Ã©voluent du faux antivirus aux faux logiciels dâ□□optimisation systÃ¨me. Ils ciblent les utilisateurs qui veulent garder leur systÃ¨me rÃ©actif. Les outils systÃ¨me sont faux, mais le vol dâ□□argent bien rÃ©el.*

Les victimes de ce type dâ□□arnaque auront beaucoup de mal Ã prouver que ces outils systÃ¨mes sont faux. Sur ce domaine, les cybercriminels exploitent les lacunes lÃ©gislatives de la zone grise dâ□□Internet."



Â

Les moyens de propagation de ces scarewares sont multiples. Un possible moyen dâ□□infection est le drive by download Ã partir dâ□□un site Internet contaminÃ©. Mais le programme peut aussi Ãªtre diffusÃ© par un fichier joint Ã un email.

Win HDD en action

La variante la plus rÃ©cente sâ□□appelle **Win HDD**. Les experts du G Data SecurityLabs montrent lâ□□effet de ce faux logiciel dans une vidÃ©o disponible ici .

Comme il est possible de le voir dans cette vidÃ©o, ce faux logiciel a un fonctionnement trÃ¨s proche dâ□□un faux antivirus : une fois installÃ©, le programme gÃ©nÃ¨re de fausses alertes Ã lâ□□utilisateur et lâ□□invite continuellement Ã acheter la version complÃ¨te.

Vrai moyen de paiement pour faux logiciel

Le systÃ¨me de paiement mis en place par les crÃ©ateurs de ce scareware imite parfaitement les systÃ¨mes officiels. Ainsi, comme il est possible de le voir Ã la fin de la vidÃ©o, la fenÃªtre de paiement contient la barre verte, le cadenas et le prÃ©fixe HTTPS devant lâ□□adresse Internet. Tous ces signes sont faux, jusquâ□□Ã lâ□□adresse affichÃ©e !

Lâ□□adresse rÃ©elle est totalement diffÃ©rente, mais contient tout de mÃªme un certificat SSL enregistrÃ© en septembre 2010 auprÃ¨s de Comodo. Il est fort probable quâ□□il sâ□□agisse dâ□□une version gratuite 90 jours. Ce certificat est valable jusquâ□□au 28 dÃ©cembre 2010. Une information qui montre le cÃ´tÃ© Ã©phÃ©mÃ¨re, mais trÃ¨s structurÃ© de cette arnaque.