G-Data, Microsoft Windows 7 plus rapide, mais pas mieux sÃ©curisÃ©
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 26/10/2009 0:00:00

Les ventes de **Windows 7** dÃ©butent officiellement. Le nouveau du systÃ¨me d'exploitation est clairement plus rapide que Vista, mais **quelles sont les avancÃ©es en termes de sÃ©curitÃ© ?** Windows 7 fait-il mieux que son prÃ©dÃ©cesseur? G Data a soumis le systÃ¨me Ã un contrÃ´le de sÃ©curitÃ©. Le rÃ©sultat : Windows 7 nâ□□a rien de nouveau Ã offrir sur le plan de la protection.

Avec ce nouveau systÃ¨me, Microsoft a voulu rÃ©pondre aux multiples critiques qui ont entachÃ©es Vista. Le pari semble gagnÃ© concernant la lÃ©gÃ¨retÃ© du systÃ¨me, Windows 7 Ã©tant beaucoup plus rÃ©actif. Mais les

mÃ©canismes des protections nâ□□ont quant Ã eux que trÃ¨s peu Ã©voluÃ©. Selon l'Ã©valuation de **Ralf BenzmÃ¼ller**, le directeur du G Data Security Labs, les innovations de sÃ©curitÃ© dans Windows 7 sont Ã peine diffÃ©rentes de celles de Vista. Certaines Ã©tant de nature purement cosmÃ©tique.

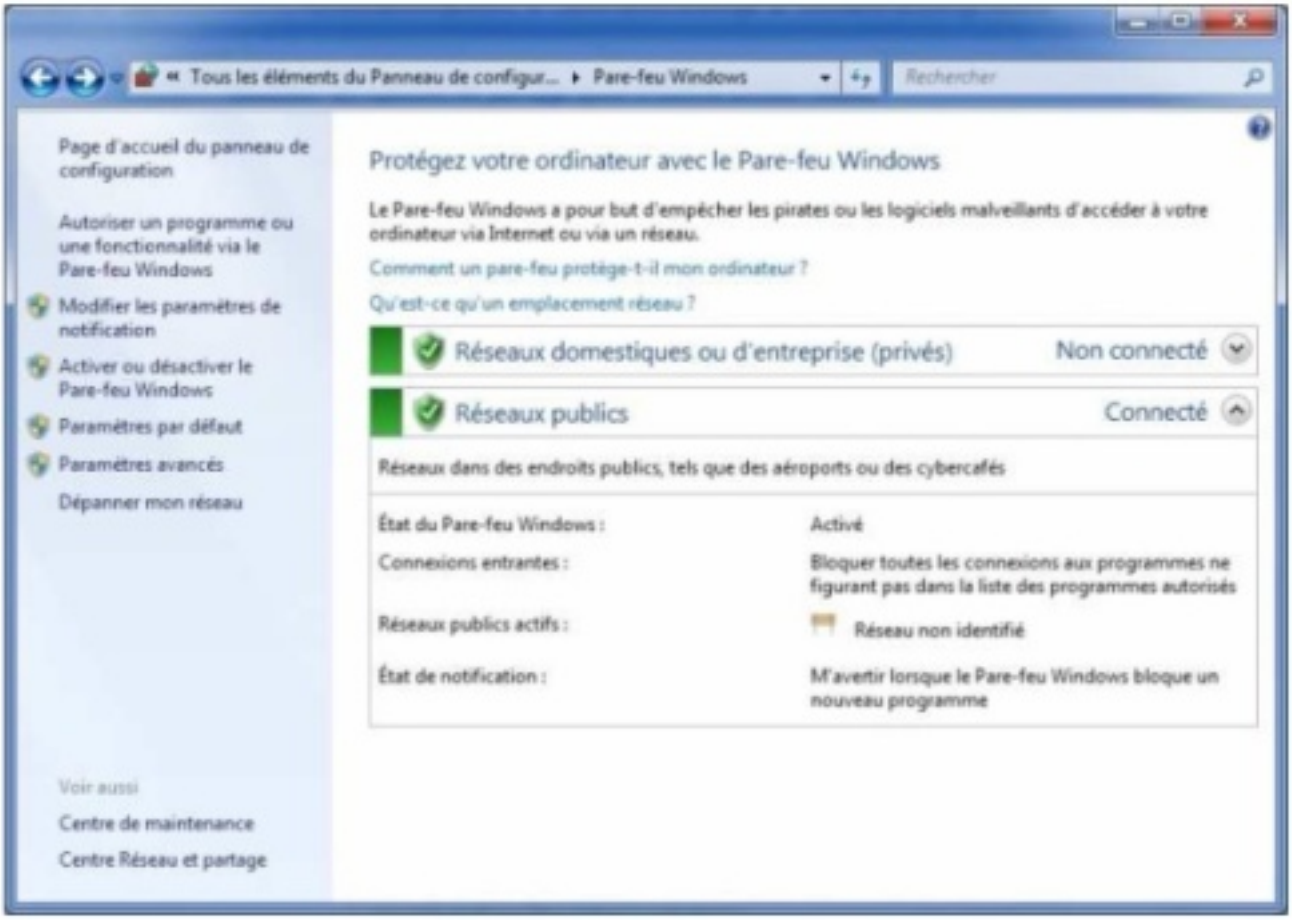
Â« *Pour les utilisateurs particuliers, Microsoft a essayÃ© de faciliter lâ□□utilisation des technologies de protection dÃ©jÃ prÃ©sentes dans Vista. Mais ces modifications ne tendent pas toutes vers une plus grande sÃ©curitÃ©. Ainsi, avec ces diffÃ©rents niveaux, le contrÃ´le de compte utilisateur (UAC) peut par exemple produire des abus de la part dâ□□utilisateurs. Un autre problÃ¨me important concerne les extensions de fichiers. Ceux-ci sont toujours cachÃ©s par dÃ©faut ce qui permet de camoufler des programmes malveillants avec les icÃ´nes de programmes inoffensifs. Windows 7 fait donc Ã peine mieux que Vista. Câ□□est pourquoi nous ne nous attendons pas Ã une grande amÃ©lioration Ã lâ□□avenir en ce qui concerne la vulnÃ©rabilitÃ© des PC sous Windows.* Â»

G Data a soumis Windows 7 Ã un contrÃ´le de sÃ©curitÃ© complet. Il livre les points forts et les points faibles du nouveau systÃ¨me.

Lâ□□ UAC (User Account Control) plus flexible, mais moins sÃ»r Vista demandait trop dâ□□autorisations. De lâ□□installation dâ□□un nouveau programme Ã la modification de lâ□□horaire de lâ□□ordinateur, une majoritÃ© dâ□□actions dÃ©clenchait lâ□□apparition dâ□□une fenÃªtre de validation. Une contrainte qui poussait beaucoup dâ□□utilisateurs Ã dÃ©sactiver cette protection et qui les exposait Ã des attaques.

Sous Windows 7, Microsoft a rendu ce contrÃ´le plus flexible : lâ□□utilisateur dispose dâ□□une Ã©chelle de quatre paliers quâ□□il peut modifier Ã sa guise. Si les deux plus hauts niveaux de protection sont acceptables, passer aux deux niveaux infÃ©rieurs est une dÃ©marche dangereuse

puisque des programmes peuvent Ãªtre dÃ©marrÃ©s avec des droits administrateurs sans aucune alerte. En laissant ce choix Ã lâ□□utilisateur, Microsoft ouvre une brÃ¨che de sÃ©curitÃ© importante.



Le pare-feu plus accueillant, mais encore trop bavard

Lâ□□ergonomie du pare-feu intÃ©grÃ© Ã Windows 7 a Ã©tÃ© amÃ©liorÃ©e par lâ□□ajout de rÃ¨gles automatiques. Avec lâ□□assistant de rÃ¨gles, un utilisateur peut facilement autoriser ou interdire la communication de programmes avec le rÃ©seau. Les configurations multiples du pare-feu en fonction du lieu de connexion (rÃ©seau Public, RÃ©sidentiel ou Professionnel) sont aussi un plus.

Plus complet, le pare-feu nâ□□est toujours pas assez convivial. Trop dâ□□alertes remontent encore Ã lâ□□utilisateur. Un grand nombre de programmes courants ne sont pas reconnus automatiquement par le pare-feu. Câ□□est donc Ã lâ□□utilisateur de savoir sâ□□il doit ou non autoriser tel ou tel programme. Câ□□est autant de failles dans la sÃ©curitÃ© du systÃ¨me.

Des extensions de fichiers toujours cachÃ©es

Par dÃ©faut Windows cache toutes les extensions de fichiers connues. Un moyen de rendre le systÃ¨me plus convivial, mais qui pose des problÃ¨mes de sÃ©curitÃ©. Il est ainsi possible de

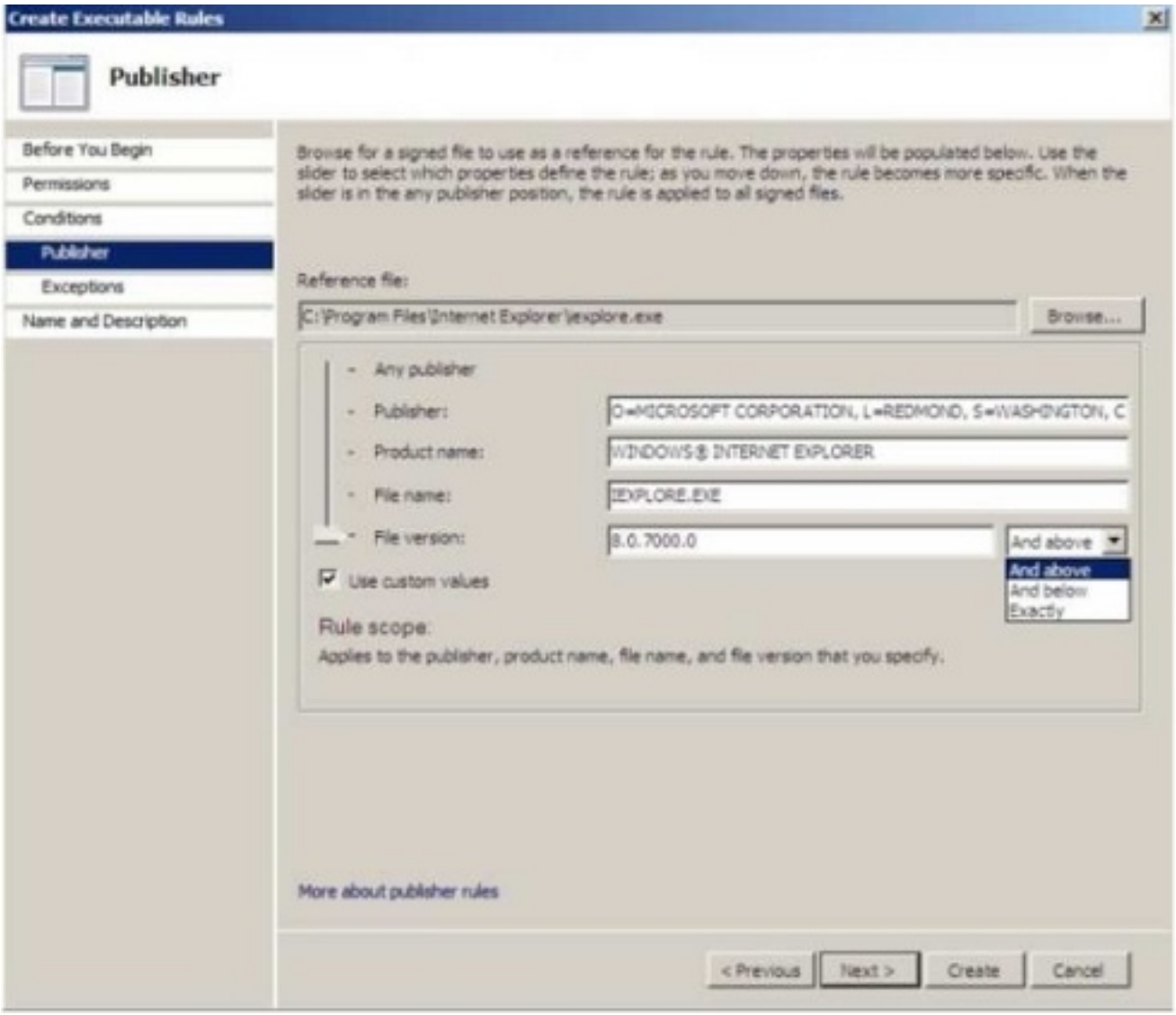
cacher un fichier dangereux

(un .exe renfermant un code nuisible par exemple) sous couvert dâ□□un faux fichier inoffensif (.pdf par exemple). Une situation incomprÃ©hensible : le problÃ¨me est connu et remontÃ© depuis des annÃ©esâ□¦

Windows Defender, rien de nouveau

Disponible depuis Windows Vista, ce scanner antispyware utilise seulement une reconnaissance basÃ©e sur les empreintes (Hash). Lâ□□absence de filtre URL ne permet pas une protection totale. En se croyant totalement

protÃ©gÃ© contre les spywares, et sans lâ□□ajout dâ□□une solution de sÃ©curitÃ© Ã part entiÃ¨re, lâ□□utilisateur sâ□□expose Ã lâ□□infection de son systÃ¨me.



App Locker enfin efficace, mais le restera-t-il longtemps ?

App Locker est une fonction qui permet aux administrateurs de bloquer lâ□□exÃ©cution de programmes. Une manipulation trÃ¨s compliquÃ©e sur les versions prÃ©cÃ©dentes, mais largement facilitÃ©e sous Windows 7. Le nouvel outil Publisher Rules prend en charge les signatures digitales des programmes, ce qui facilite lâ□□identification des applications Ã bloquer. Mise en place dans le rÃ©seau, cette politique permet de limiter lâ□□exÃ©cution des codes malveillants. Une inconnue demeure toutefois : la signature digitale des applications ne sera-t-elle pas rapidement dÃ©tournÃ©e par les malwares ?

BitLocker, simple Ã administrer, mais moins sÃ©curisÃ©

Cette fonction de cryptage intÃ©grÃ©e Ã Windows est une avancÃ©e importante dans le domaine de la sÃ©curitÃ©. Mais cette option est seulement disponible dans les versions Ultimate et Entreprise de Windows 7 et repose sur le chipset TPM (Trusted Platform Module). Des limites pour la diffusion de cette option de sÃ©curitÃ©. DÃ©jÃ disponible dans Vista, BitLocker a Ã©tÃ© amÃ©liorÃ©e sous Windows 7. Plus simple Ã mettre en place, la fonction est aussi facilement administrable.

La clÃ© de cryptage peut maintenant Ãªtre archivÃ©e dans Active Directory. Une nouvelle commoditÃ© qui a toutefois un impact important sur la sÃ©curitÃ© puisquâ□□elle implique une sÃ©curisation forte dâ□□Active Directory.

En conclusion

Windows 7 nâ□□est pas mieux sÃ©curisÃ© que Vista. G Data ne prÃ©voit donc aucune amÃ©lioration de la vulnÃ©rabilitÃ© des PC sous Windows. Lâ□□utilisation dâ□□une solution de sÃ©curitÃ© dÃ©diÃ©e, performante et facile dâ□□accÃ¨s reste indispensable pour un utilisateur souhaitant une protection optimale de son systÃ¨me.