Tribune
Lundi 18 décembre 2006

Natalya Kaspersky
Une sécurité offerte par Microsoft : en route vers un monde nouveau ?

Microsoft et son nouveau système d'exploitation : Windows Vista marquera-t-il la fin des antivirus ?

Récemment, Jim Allchin, un cadre haut placé chez Microsoft, s'est retrouvé dans une situation délicate. Des journalistes qui l'interviewaient ont mal compris une de ses réponses et ont publié une information qui aurait pu être sensationnelle : la protection de Vista, le nouveau système d'exploitation de Microsoft, est telle que l'utilisation d'un logiciel antivirus complémentaire serait superflue.

Cette information fut publiée et rapidement corrigée. Jim Allchin, s'excusant pour le manque de précision dans ses propos, rectifia le tir. On l'avait mal compris : bien que Vista soit sans conteste le système d'exploitation le mieux protégé jamais produit par Microsoft, il ne pourra pas offrir une protection totale aux utilisateurs contre les virus et les autres programmes malveillants.
Ce thème est très largement débattu dans le secteur et les principaux acteurs émettent de temps à autre des avis contradictoires sur la politique de Microsoft et son entrée sur le marché des antivirus. Je souhaiterais exposer dans cet article le point de vue de Kaspersky Lab et mon avis personnel sur Vista et la sécurité.

A propos de la sécurité dans Windows Vista

Avant de commencer, il faut présenter en quelques mots le nouveau système d'exploitation du géant de Redmond.

L'interface utilisateur de Vista a été refondue et améliorée, les fenêtres peuvent défiler en 2D ou en 3D et le moteur intégré au système facilite la recherche de fichiers, de documents et d'applications. Toutes ces modifications aideront les utilisateurs débutants tandis que l'ordinateur deviendra un outil plus confortable pour les utilisateurs chevronnés.

Du point de vue de la sécurité, Vista introduit également de nombreuses améliorations et des composants complémentaires de protection.

Par exemple, Vista permet de réduire le nombre de processus et d'applications exécutés avec des privilèges étendus (c.-à-d. avec les privilèges d'administrateur). Pour des raisons de compatibilité avec diverses applications, dans les versions antérieures de Windows, un trop grand nombre d'utilisateurs avaient accès à des privilèges étendus. Désormais, tous les processus et applications seront lancés par défaut avec des privilèges restreints et même si de sérieuses vulnérabilités sont identifiées dans ces applications, elles n'auront que très peu d'influence sur l'ensemble du système et ne pourront pas vraiment nuire à l'ordinateur.

C'est la technologie de contrôle de compte d'utilisateur (UAC). Chaque fois qu'une action particulière requerra des privilèges plus étendus, le système demandera à l'utilisateur d'autoriser ou non cette action. Autrement dit, ce système d'exploitation, à la différence des versions antérieures (y compris Windows XP), introduit une protection contre les conséquences possibles des actions d'un utilisateur possédant trop de privilèges.

Grâce au mode protégé de la version 7.0 d'Internet Explorer dans Windows Vista, la navigation sur Internet devient plus sûre. Dans ce mode, le navigateur utilise des privilèges système qui empêchent tout code malveillant d'introduire, à l'insu de l'utilisateur, des modifications dans des secteurs critiques du système lors de la consultation de certains sites Internet. Le mode protégé n'offre pas une protection contre tous les types d'attaque mais il réduit considérablement leur chance de réussite. Notons qu'Internet Explorer 7.0 existe également pour Windows XP mais le mode protégé du navigateur ne fonctionne que sous Vista.

Vista propose également le logiciel Windows Defender qui, s'il faut en croire l'éditeur, « protège les utilisateurs contre les logiciels espions et autres programmes malveillants ». Dans la mesure où de nombreux observateurs estiment que Windows Defender assure la protection contre les programmes malveillants, je tiens à souligner qu'il ne s'agit pas d'un logiciel antivirus et qu'il cible uniquement un seul type de programme malveillant parmi la multitude de menaces aujourd'hui répertoriées sans offrir aucune protection contre les virus, les chevaux de Troie, les vers, etc.

Microsoft propose seulement deux logiciels de protection contre les programmes malveillants : Windows Defender (intégré à Windows, c.-à-d. proposé par défaut) contre les logiciels espions et Microsoft One Care, un logiciel autonome contre les virus et autres menaces. One Care ne fait pas partie de Vista. Ce logiciel est vendu séparément selon un système d'abonnement, à l'instar de ce que proposent les autres éditeurs antivirus.

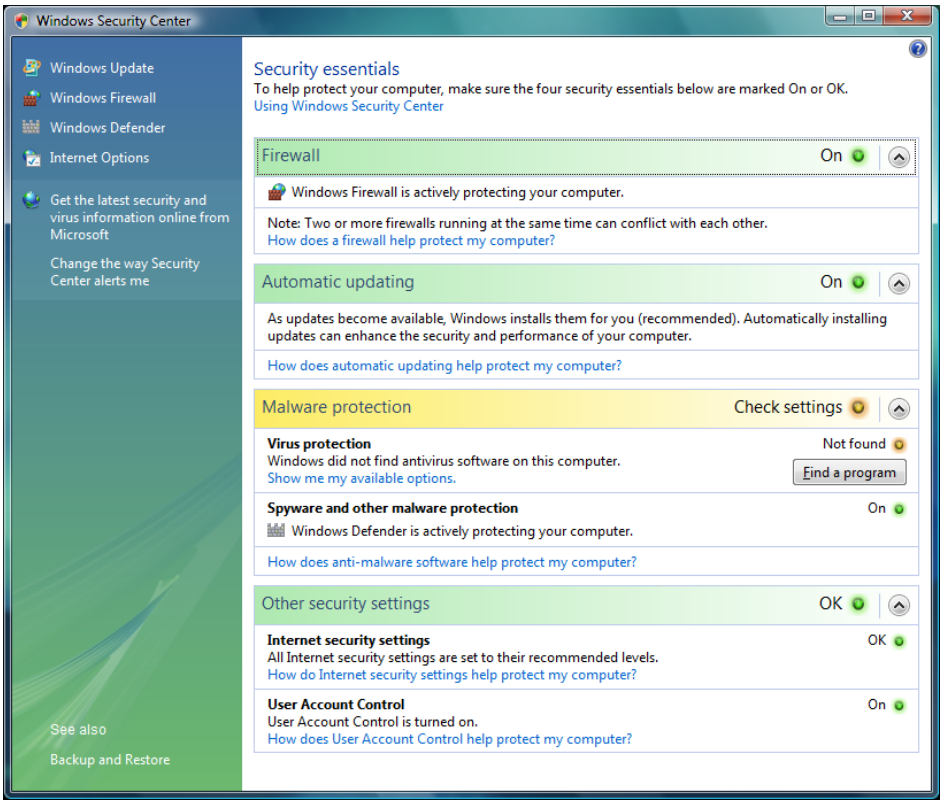
Classement des programmes malveillants selon Microsoft :

Pour rappel, le classement de Microsoft répartit tous les programmes malveillants entre les logiciels espions et les virus (tout autre type de programmes malveillants).
La répartition est une démarche assez subjective dans la mesure où d'autres éditeurs de logiciels antivirus utilisent d'autres classifications et interprètent différemment le terme logiciel espion. Pour cette raison, il est très difficile de faire la distinction entre plusieurs catégories. Selon la terminologie de Kaspersky Lab, un logiciel espion est un logiciel qui recueille, à l'insu de l'utilisateur, différentes informations sur l'utilisateur et qui les transmet à son créateur.

Ces derniers temps, on observe une augmentation du nombre de programmes malveillants qui renferment un mélange de technologies, ce qui empêche de les classer dans une catégorie bien précise. La catégorie dans laquelle Microsoft range les logiciels espions qui s'introduisent dans les ordinateurs via un ver Internet, un courrier indésirable ou un cheval de Troie n'est pas claire. Dans ce sens, l'existence d'un module de protection dans Vista qui protège uniquement contre un type de menace a de quoi déboussoler les utilisateurs car cela crée un faux sentiment de sécurité, ce qui pourrait se traduire par une augmentation du nombre d'ordinateurs dépourvus de protection.

A la différence de Microsoft, la majorité des éditeurs de logiciels antivirus offre une protection contre tous les types de menaces et les solutions très spécialisées telles que Anti-Spyware appartiennent au passé. Il y a quelques années, la lutte contre les logiciels espions était très à la mode et on a pu assister à l'explosion du nombre de jeunes entreprises spécialisées dans la lutte contre ce type de logiciel. L'agitation est ensuite retombée, les entreprises les plus actives ont été rachetées par des éditeurs de logiciels antivirus et les autres ont quitté le marché.

Mais, revenons à Windows Vista et à la lutte contre les virus, Microsoft lui-même recommande aux utilisateurs du nouveau système d'exploitation d'installer des logiciels de protection antivirus complémentaires. Ainsi, le Windows Security Center dans Vista signale à l'utilisateur que l'ordinateur n'est pas doté d'un logiciel antivirus tant que ce dernier n'a pas été installé. Une fenêtre de ce type s'affiche :



Dans la perspective des développeurs de Microsoft, l'utilisateur qui clique sur Find a programme (« Trouver un logiciel ») ouvre une page du site de Microsoft sur laquelle il pourra acheter One Care ou le logiciel antivirus d'un éditeur tiers.

Quels sont les logiciels antivirus compatibles avec Windows Vista ?

Les utilisateurs ont appris depuis longtemps qu'il était déconseillé d'installer en parallèle deux logiciels antivirus issus d'éditeurs différents. Cela peut en effet engendrer de graves problèmes, des gels du système ou l'apparition de l'écran bleu en raison du conflit existant entre les parties résidentes de l'application qui se battent pour les mêmes ressources. Lorsqu'ils verront Windows Defender dans le système d'exploitation, les utilisateurs pourraient croire qu'il est dangereux d'installer un autre logiciel antivirus sous Vista.

Toutefois, Windows Defender a été expressément développé afin d'être compatible avec les logiciels antivirus traditionnels.
Certains utilisateurs pensent que les solutions de Microsoft telles que One Care seront mieux adaptées que les solutions équivalentes d'autres éditeurs, compte tenu du soi-disant haut degré d'intégration avec le système d'exploitation car il utilise des fonctions non documentées du système tandis que les éditeurs tiers n'ont pas accès à de telles données.
Il s'agit une fois de plus d'un mythe. Tout ce que Microsoft développe peut être réparti entre la plate-forme (le système d'exploitation) et les applications qui fonctionnent avec ce système d'exploitation. Du point de vue des applications, les développeurs de Microsoft font référence aux mêmes bibliothèques et fonctions que celles, documentées et décrites, accessibles aux autres éditeurs de logiciels. Ces conditions et ces règles sont clairement décrites dans la rubrique Windows Principles à la page :
http://www.microsoft.com/presspass/newsroom/winxp/windowsprinciples.mspx.

De plus, le succès commercial phénoménal de Microsoft s'explique en grande partie par la mise au point d'un modèle de partenariat avéré : cela fait longtemps que la société offre de grandes possibilités aux développeurs d'applications sur ses plates-formes.

Le fait que Microsoft décide parfois d'entrer en concurrence avec ses développeurs pour décrocher des parts sur un marché est une autre histoire. Donc, d'un point de vue technologique, les développeurs de Microsoft et les développeurs indépendants évoluent dans des conditions égales.

Quelques mots sur Windows One Care

On me pose souvent des questions sur One Care, l'antivirus commercialisé par Microsoft. Où se situe-t-il par rapport aux logiciels développés par d'autres éditeurs ? Afin de se faire une idée sur le produit, je conseille de consulter les tests des laboratoires indépendants. A l'heure actuelle, ce logiciel est en vente uniquement aux Etats-Unis et selon les informations en ma possession, a été par deux fois testé par AV-test.org - un groupe de recherche de l'université de Magdebourg (Allemagne), un des laboratoires indépendants de tests parmi les plus respectés au monde. Ce test permet de tirer les premières conclusions quant à la qualité de la détection.

Selon moi, il existe trois facteurs qui vont compliquer la tâche de Microsoft en termes de concurrence avec les principaux éditeurs de logiciels antivirus.

1. *La réputation dans le domaine de la sécurité*

   Jusqu'à présent, Microsoft ne s'est pas particulièrement distingué dans le domaine de la sécurité. Les solutions de Microsoft sont considérées par défaut comme « trouées », soit dépourvues de protection. La présence de « trous » dans Windows et les logiciels de la suite Office s'explique avant tout par leur popularité immense : les pirates du monde entier sont intéressés par les applications les plus utilisées. Je crains par conséquent que ce nouveau logiciel antivirus ne subisse le même sort. Je veux dire par là que les auteurs de virus vont créer des programmes malveillants capables de contourner la défense offerte par One Care.

2. *La vitesse de réaction face aux nouvelles menaces est un autre élément de poids*

   Chaque éditeur est confronté à un choix : identifier un maximum de programmes malveillants en acceptant le risque de considérer un fichier sain comme un virus ou éviter au maximum les faux positifs (c.-à-d. les fichiers sains considérés comme des virus) en prenant le risque de laisser passer des virus. Il suffit de se rappeler les histoires liées aux faux positifs de Google Mail par le logiciel antivirus de Microsoft qui ont fait beaucoup de bruit ou l'identification erronée du logiciel russe Dr. Web par le logiciel de Microsoft. De par sa marque et sa renommée, Microsoft ne peut pas se permettre de faux positifs. Donc, comme chaque cas douteux devra être minutieusement examiné avec des juristes, la vitesse de réaction face aux nouvelles menaces sera assez lente.

3. *La qualité de n'importe quelle solution antivirus est toujours déterminée par le niveau de détection des programmes malveillants*

   Le laboratoire indépendant de Magdebourg a testé One Care en septembre et novembre 2006. Les résultats (le dernier était de 81.22%) ne sont pas très probants même pour un antivirus moyen.

Sur la base d'une synthèse des trois facteurs repris ci-dessus, je me risque à formuler la proposition suivante. Le logiciel antivirus de Microsoft, lorsqu'il aura amélioré ses capacités de détection des programmes malveillants, trouvera sa place à l'avenir parmi les autres solutions antivirus. Il sera caractérisé par de bonnes fonctions pour les utilisateurs (ce qui a toujours été un point fort de la société). Toutefois, ce logiciel sera loin d'occuper la première place en termes de réaction face aux nouvelles menaces ou de détection des programmes malveillants.

Que doit donc maintenant faire l'utilisateur ?

Je souhaiterais dresser le bilan de ce qui a été dit.

Tout d'abord, Windows Vista possède quelques caractéristiques utiles du point de vue de l'amélioration de la sécurité mais il ne protège toujours pas les utilisateurs contre les programmes malveillants. Par conséquent, l'installation d'un logiciel antivirus isolé est indispensable.

Deuxièmement, la protection contre ces programmes malveillants pourra être confiée à une solution de Microsoft ou à une solution d'un autre éditeur.

Quelle solution choisir ?

- Celle en qui vous avez confiance.
- Celle qui, d'après vous, offrira une protection fiable contre les programmes malveillants (si vous avez la curiosité de lire les résultats des tests indépendants, ce serait l'idéal).
- Celle qui sera la plus compatible avec le nouveau système d'exploitation (les éditeurs de logiciels sont obligés de mentionner ce point dans la configuration requise).

Je vous souhaite une agréable découverte de Vista et une navigation sur Internet en toute sécurité !

Cordialement,
Natalya Kaspersky.

Kaspersky Lab France
Immeuble l'Européen Bât C
2 Rue Joseph Monier
92500 RUEIL MALMAISON

☎ 0825.888.612
RCS 478 315 872
www.kaspersky.fr

A propos de Natalya Kaspersky :

Natalya Kaspersky a obtenu un diplôme en mathématiques appliquées en 1989 à l'Institut d'ingénierie électronique de Moscou. Après ses études supérieures, Natalya Kaspersky a occupé les fonctions d'assistante de recherches au Bureau central de conception scientifique. En 1994, Natalya Kaspersky se retrouve au Centre des technologies de l'information KAMI où elle sera chargée de la gestion d'un projet antivirus dénommé AVP (qui allait devenir Kaspersky Anti-Virus en 2000). Natalya occupe aujourd'hui les fonctions de Président-Directeur Général de Kaspersky Lab. Figure d'autorité dans le secteur des technologies de l'information en Russie, Natalya Kaspersky participe fréquemment à des séminaires de développement commercial et à des conférences dans le monde entier.

A propos de Kaspersky Lab

Kaspersky Lab est un éditeur russe de solutions logicielles indispensables pour contrer toutes les formes de cyber-menaces en perpétuelle évolution. Depuis de nombreuses années, les meilleurs experts mondiaux travaillent dans les laboratoires de Kaspersky Lab afin d'offrir des services de hauts niveaux appréciés par les éditeurs et les utilisateurs. 24 h sur 24 h, 7 jours sur 7, les chercheurs analysent et traitent les codes malicieux. Des antidotes sont rapidement développés et validés puis proposés aux utilisateurs via les dizaines de mises à jour quotidiennes.

Kaspersky Lab dispose de bureaux à Moscou, en Allemagne, en Grande Bretagne, au Benelux, en Chine, en Corée du Sud, aux Etats-Unis, en France, au Japon, aux Pays-Bas, en Pologne et au Royaume-Uni.

Fondée en 1997, Kaspersky Lab concentre ses efforts sur le développement de solutions de pointe permettant de protéger les informations et les utilisateurs. Kaspersky Lab développe des logiciels de sécurité destinés à un large spectre d'applications et de clients, de l'utilisateur familial aux grands comptes. Kaspersky Lab distribue, supporte et assure la promotion de ses produits dans plus de 50 pays dans le monde.

Pour plus d'informations concernant Kaspersky Lab : http://www.kaspersky.fr
Pour plus d'informations sur l'actualité virale : http://www.viruslist.com/fr

Toute l'actualité de Kaspersky Lab est accessible aux journalistes sur : http://presse.kaspersky.fr

Contacts presse :

MEDIASOFT COMMUNICATIONS
Emmanuelle Bureau du Colombier
Ebdc@mediasoft-rp.com
Carole Scheppler
Carole.scheppler@mediasoft-rp.com
Tél : 01 55 34 30 00

KASPERSKY LAB France
Stéphane Le Hir / Directeur
Jean-Philippe Bichard / Directeur Marketing
Jean.philippe.bichard@fr.kaspersky.com
Tél : 01 41 39 04 89