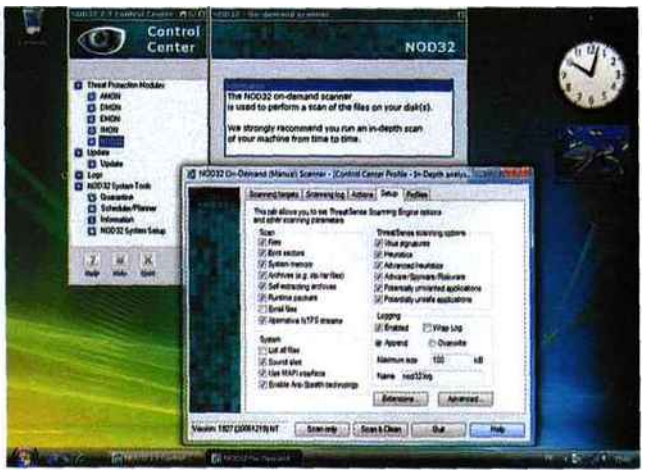
01 Réseaux
01 44 25 31 40
JAN 07
Mensuel
OJD : 21795
Surface approx. (cm²) : 339

L'arrivée de Vista relance la guerre des antivirus

Adopter Vista oblige à adapter son logiciel antivirus. Il y a quelques mois, certains éditeurs se sont élevés contre la politique mise en place par Microsoft. Outre ce scénario, récurrent à chaque sortie d'un nouveau système d'exploitation, il peut être bon de réfléchir à sa politique antivirale.

Les premiers antivirus dédiés au nouveau système d'exploitation de Microsoft arrivent sur le marché. L'objectif de leurs éditeurs est d'être fin prêts pour la sortie officielle de Vista à destination du grand public, prévue le 30 janvier 2007. L'enjeu est de taille : le gâteau à se partager se chiffre en milliards de dollars. La quasi-totalité des utilisateurs disposent en effet d'un antivirus sur leur poste de travail.
Bien avant sa sortie, Vista a déchaîné les passions. Symantec et McAfee ont accusé Microsoft de créer des difficultés en coupant l'accès au noyau par sa technologie PatchGuard, intégrée à Vista 64 bits.



NOD32, édité par Eset, est l'un des premiers antivirus disponibles pour Vista Il gère notamment BluePill, le *rootkit* « indetectable », presente en juillet dernier par Joanna Rutkowska, de Coseinc.

De la place pour tout le monde

Plus conciliateur, Sophos s'est contenté de défendre la politique de sécurité mise en œuvre. Comme par le passé, il y a de la place pour tout le monde, même si la firme de Redmond propose sa propre solution antivirale, baptisée Windows Live OneCare (non disponible en France pour le moment) « *Les résultats ne sont pas très probants* », écrit Natalya Kaspersky, p-dg de Kaspersky Lab, dans sa note du 18 décembre 2006 intitulée *Une sécurité offerte par Microsoft, en route vers un monde nouveau ?* Pour rendre ce diagnostic sur Windows OneCare, elle s'appuie sur le laboratoire de Magdebourg, en Allemagne. « *Certains utilisateurs pensent que les solutions de Microsoft seront mieux adaptées que les solutions équivalentes d'autres éditeurs, compte tenu du prétendu haut degré d'intégration avec le système d'exploitation. Car OneCare utilise des fonctions non documentées du système, tandis que les éditeurs tiers n'ont pas accès à de telles données. C'est un mythe,* lâche-t-elle. *Du point de vue des applications, les développeurs de Microsoft font référence aux mêmes bibliothèques et fonctions que celles, documentées et décrites, qui sont accessibles aux autres éditeurs de logiciels.* »
De son côté, l'éditeur slovaque Eset vient de lancer la version 2.7 de son logiciel NOD32, compatible avec Vista. Encore peu connu en France, NOD32 fait partie des très bons antivirus du marché. À son palmarès, on note le record des récompenses décernées par *Virus Bulletin* – il est le seul du marché à avoir obtenu toutes les certifications mensuelles du *Virus Bulletin* depuis 1998 – et le titre de meilleur antivirus de l'année 2006 décerné par le site av-comparatives.org. Son scanner, l'un des plus rapides du marché, a l'avantage d'être peu gourmand en puissance. Il est l'un des rares antivirus permettant de poursuivre son travail de manière satisfaisante lors de l'examen de son PC.
Safe Protect intègre le moteur NOD32 dans son boîtier de gestion unifiée des menaces (ou UTM). Pour Christophe Lamy, chargé d'affaires chez Safe Protect, « *NOD32 2.7 est le premier antivirus à détecter BluePill* [le *rootkit* «indétectable» de Joanna Rutkowska, NDLR] ».
Eset n'inclut pas un pare-feu complémentaire, comme nombre de ses concurrents, mais Athena Global Services, son distributeur en France, propose un lot avec le pare-feu Outpost Firewall Pro d'Agnitum. Sa version 5.0 n'étant pas encore compatible avec Vista, cette offre n'est actuellement disponible qu'avec Windows XP. ■

OLIVIER MÉNAGER

Notoriété ne rime pas forcément avec efficacité

En juillet 2006, Graham Ingram, directeur général du Cert australien, a explique que « *les antivirus les plus populaires du marche ont un taux d'echec de 80 %* » Autrement dit, huit codes malicieux sur dix passent Est-ce dû a une qualite moindre des developpeurs chez Symantec, McAfee ou Trend Micro, les trois premiers editeurs de solutions antivirales sur le plan mondial ? Pas du tout, selon Graham Ingram, « *les auteurs testent specifiquement leurs chevaux de Troie et virus sur ces logiciels antivirus bien connus et s'assurent qu'ils passent au travers des defenses avant de lâcher leurs attaques* » Graham Ingram a ajoute, a titre d'exemple, qu'avec la même serie de tests, 90 % d'un *malware* etait bloqué par l'antivirus de Kaspersky, crédité de 0,7 % de parts de marche par le Gartner Si l'on ajoute que les attaques ciblées perceront, quel que soit l'antivirus, on comprend alors que les approches monolithiques preconisees par certains editeurs ne peuvent être efficaces, même sous couvert d'une reduction du coût et d'une meilleure facilite d'administration.

Eléments de recherche : ATHENA GLOBAL SERVICES : société de distribution de logiciels, toutes citations