Symantec s'inquiète de la menace des faux antivirus

L'éditeur de sécurité Symantec rend son rapport annuel sur les tendances en matière de méthodes de piratage et **les techniques d'infection.** L'étude, élaborée par le Security and Technology Response de Symantec, se porte sur les anti-virus factices entre le 1er juillet 2008 et le 30 juin 2009.

Sur le terrain des **faux antivirus**, Symantec explique comment nombre d'internautes se font piéger par une offre de faux antivirus. Grâce à des publicités ou à des pop-up dans le navigateur, les internautes sont invités à télécharger un logiciel afin de prévenir une pseudo-infection de leur système. La duperie est alors double puisque l'infection est réelle alors que l'utilisateur se croît protégé par son pseudo antivirus.

Dans ce cadre, **Laurent Heslaut**, directeur des technologies de Sécurité chez Symantec. explique que 93% de ces installations sont de type intentionnelles : « *Ces logiciels factices sont en général proposés autour de 30 à 100 dollars et représentent environ* ***43 millions de d'installations****. Par simple calcul, il s'agit là d'un gros marché.*» L'univers Mac ne serait d'ailleurs pas étanche à ce phénomène avec notamment le faux logiciel **Mac Sweeper.**

De quoi amener encore un peu plus de flou chez les internautes. D'autant qu'en règle générale, ces faux logiciels disposent d'une interface similaire aux véritables versions des antivirus connus.

A propos du *modus operandi* des hackers (quelques centaines tout au plus, selon Symantec), il est intéressant de noter qu'ils agissent *via* des serveurs Web payants plutôt que par le biais des ordinateurs zombies (botnets). **Marc Dacier**, directeur des Research Labs en Europe confie : « *Plus de la moitié des ces facticiels sont* ***hébergés aux Etats-Unis****, loin devant les autres Etats. Ils sont en général enregistrés dans des registrar qui protègent la vie privée, donc difficiles à atteindre.* »

Le responsable s'appuie ici sur les conclusions du **projet WOMBAT** (observatoire mondial des codes malicieux et des menaces). Un consortium d'universités, de professionnels et d'instituts nationaux européens milite ainsi pour connaître les nouvelles pratiques de sécurité par exemple mais aussi de pouvoir analyser les contenus infectés.

Toujours est-il que ce trafic peut rapporter gros. **Jusqu'à 300.000 dollars par mois** pour les plus actifs. Symantec recommande donc de privilégier les solutions antivirus les plus connues du marché…