Les malwares évoluent trop rapidement face aux antivirus

En matière de sécurité informatique, il n'existe pas encore de solution universelle capable de surveiller l'ensemble des menaces et de déjouer les techniques de piratage. Et face à une attaque ciblée, menée par des 'hackers' déterminés, il est quasiment impossible de se protéger.

Si la menace est bien réelle, il faut reconnaître que de nombreux informaticiens qui travaillent depuis plus de vingt ans sur différentes machines n'ont jamais été touchés par des attaques très dangereuses. Du coup, certains estiment qu'il ne sert à rien de se protéger…

Aujourd'hui, la tendance est à l'utilisation de techniques de contamination inspirées de celles utilisées par les éditeurs de sécurité dans leurs laboratoires. Aussi, la question mérite-t-elle d'être posée: les antivirus sont-ils encore efficaces ?

Pour en savoir plus sur le niveau réel de la menace, de nombreux laboratoires ont analysé les méthodes de défenses des solutions vendues par les éditeurs de sécurité.

Une de ces études, commandées par 'PC World' montre que les solutions disponibles sur le marché ne bloquent qu'une fois sur quatre les nouveaux codes malveillants et que d'une manière générale quand la menace est nouvelle, elle traverse sans difficulté les barrières de sécurité des logiciels en place sur un système. Selon le magazine spécialisé, les solutions actuelles ne bloquent que la moitié des codes malveillants.

Et ce combat semble perdu d'avance pour les éditeurs de sécurité, car de nos jours, ce sont les cybercriminels qui ont les cartes en mains, ils ont l'avantage de l'effet de surprise et ils connaissent suffisamment les solutions de protection disponibles sur le marché pour les contourner. Hacker et éditeurs sont donc en guerre. Et pour l'instant l'avantage est aux malfaiteurs du Net.

Et des sites Web comme VirusTotal.com facilitent le travail des voyous de la Toile. Rappelons que ces URL permettent aux chercheurs en sécurité informatique et aux consommateurs de poser des questions sur des vulnérabilités et de soumettre des fichiers douteux à des scans utilisant une trentaine de moteurs différents.

Les hackers n'ont qu'à utiliser la même technique pour tester leurs nouveaux codes malveillants et voir comment ils se comportent face aux antivirus du marché.