2 nouveaux vers menaceraient Windows: peu sérieux

Pour Symantec et McAfee, la menace n'est pas très sérieuse, car les récentes vagues d'attaques virales ont amené une grande majorité d'internautes à mettre à jour leur environnement Microsoft et leur anti-virus, ce qui théoriquement suffit à les protéger.

Plexus semble le plus menaçant, car il cherche à exploiter deux failles connues du système Windows. Tout comme Blaster, il tente d'exploiter un composant de Windows, LSASS (*Local Security Authority Subsystem Service*). Mais aussi une faille plus ancienne dans le composant d'interface DCOM (*Distributed Component Object Model*). Classiquement, ces vers se cachent dans un fichier attaché derrière un e-mail dont l'objet est du type « *RE: order*« , « *For you* » ou « *Good offer*« . Si le fichier est ouvert, le ver est lancé et il altère la configuration de Windows. Et le programme vérolé se relance à chaque ouverture de Windows ! Bien entendu, ils se répandent à l'aide des adresses e-mails stockées sur le disque dur vérolé. L'expédition est gérée par un simple moteur SMTP inclus dans le programme. Plexus va même jusqu'à scanner les disques durs afin de s'immiscer sur les sites Web en http stockés. Une nouvelle fois, même si le danger semble minime, les règles de base de la protection virale s'imposent, pare-feu, mise à jour des systèmes et des anti-virus. Et gare aux communautés de téléchargement en *peer-to-peer*, qui semblent de plus en plus être un vecteur viral !