Sober.D se cache derrière un 'upgrade' Microsoft

Les auteurs de virus ne manquent pas d'imagination ! La dernière version 'D' du ver Sober, qui est apparu pour la première fois en octobre dernier, a été détectée en Allemagne, et pourrait se répandre rapidement, car elle utilise une astuce pour détourner l'attention de l'internaute.

L'objet de l'email est en effet « *Microsoft Alert : Please Read!*« , et le virus est présent sur le fichier attaché au format .exe ou .zip, qui porte le doux nom de *Patch*, *MS-Security* ou *UpDate*. On notera que Microsoft n'a jamais diffusé de mise à jour par email ! Le lecteur qui se fait piéger et ouvre le fichier vérolé, permet au ver de s'installer sur le disque dur, de modifier la configuration de Windows afin de se lancer à chaque démarrage, puis d'ouvrir la base d'adresse emails sur laquelle Sober-D va se répandre. Particulièrement vicieux vis-à-vis de l'utilisateur, Sober-D imite un logiciel de patch officiel, allant jusqu'à afficher un message « *Patch have been successfully installed*« . L'internaute se fait donc piéger sur le message, et ensuite à l'installation du virus. Et en plus il est content d'avoir éradiqué MyDoom avec l'aide de Microsoft ! Par contre, si par hasard ou par inattention vous installez Sober-D, et qu'à l'installation il vous renvoie le message « *Patch does not need to be installed on this system*« , c'est que Sober vous a déjà vérolé. Dommage? Enfin, dernier vice de Sober-D, la version linguistique du message change selon l'extension du domaine auquel il s'attaque. Par exemple, si Sober-D s'expédie sur une boite d'email dont le domaine est —.de, l'objet de l'email devient « *Microsoft Alarm: Bitte Lesen!*« . Attention, nous ignorons à l'heure actuelle si une version française existe.