Date de publication Vendredi 30 mars 2007 à 21:00:42 **par** colok
Catégorie Nouveautés

Microsoft lance une alerte sur une vulnérabilité ANI sous Windows

Source: Yves Grandmontagne du site Silicon.fr Des hackers exploitent activement une vulnérabilité 'zero day' qui leur permet de prendre le contrôle total des systèmes Windows. Un patch existe, mais il n'a rien d'officiel ! Les attaques sont réelles, même si elles sont encore limitées. Peu importe, la menace est là, touche tous les systèmes Windows, dont Vista et Windows Server, et Microsoft vient de lancer une alerte. Cette nouvelle menace est proche des attaques associées aux fichiers Windows Metafile (WMF) qui avaient défrayé la chronique l'an passé. Aujourd'hui, les hackers exploitent une vulnérabilité 'zero-day' présente dans les fichiers .ANI des curseurs animés sous Windows. Cette proximité avec les attaques WMF en 2006, ou encore le ver Zobot en 2005, confirme la dangerosité de la nouvelle menace. McAfee a d'ailleurs démontré qu'il suffit de ' glisser-déposer' un fichier .ANI vérolé sous Vista pour que s'enchainent crashs et redémarrages en boucle. Microsoft aurait conseillé, pour limiter le risque des attaques, de configurer le client e-mail en mode plein texte. De son côté, eEye Security propose un patch qu'il a développé en interne, mais ce dernier n'a rien d'officiel et s'annonce 'temporaire', et comme le confirme son éditeur ne remplacera pas le correctif à venir de Microsoft. Les logiciels malveillants sont désormais détectés par le scanner de Microsoft Live OneCare. En revanche, les postes sous Windows Vista et Internet Explorer 7 utilisés en mode protégé ne sont pas menacés, car le niveau de sécurité de Vista n'autorise pas d'accéder ou de modifier un fichier système sans autorisation. Lire la suite