Microsoft lance une alerte sur une vulnérabilité ANI sous Windows

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.

Histoire d'un bug en mal de correction

eEye corrige le bug dans les curseurs animés de Windows et bloque la vulnérabilité 'zero-day' qui menace Outlook. Particularité de la correction, elle n'a rien d'officielle?

Première étape, l'éditeur McAfee a le premier signalé mercredi dernier la présence d'un bug dans les fichiers *Animated Cursor*, utilisés pour créer sous Windows des curseurs animés, qui aurait été utilisé dans des attaques Web.

Le premier, vraiment ? Un éditeur de sécurité, Determina, affirme avoir déjà signalé le problème à Microsoft en décembre dernier? En réalité, Microsoft aurait depuis longtemps corrigé une faille (MS05-002) proche de celle qui a été révélée par McAfee, mais le patch, toujours dixit Determina, aurait été incomplet.

Une information confirmée par un autre éditeur de sécurité, eEye, qui quant à lui précise que la première faille a été découverte par ses experts et corrigée en 2005, il y a deux ans donc. Mais qu'à cette occasion, le correctif MS05-002 suscité a bien oublié une partie de la faille.

Microsoft de son côté a reconnu la faille, et indiqué qu'elle ne concerne pas Outlook 2007. En revanche, les versions précédentes d'Outlook, et en particulier Outlook Express sont vulnérables. Il conseille d'ailleurs ne n'ouvrir les e-mails qu'en mode texte?

Il a également indiqué qu'il pourrait 'éventuellement' corriger le problème. Mais il n'a donné aucune indication quant à la publication d'un correctif à Animated Cursor? Le 10 avril, prochain 'Patch Tuesday' ?

En fait, lorsqu'une faille concerne des développements dont il n'a pas la responsabilité, l'éditeur renvoie logiquement vers les tiers auteurs de l'erreur pour réviser leurs produits.

Sauf que dans ce cas, et ce n'est pas la première fois, la correction est venue de l'extérieur, via un patch proposé par eEye Security. Et qui n'a rien d'officiel ! Et sauf qu'ici il y a urgence, car le code permettant d'exploiter la faille a été publié sur plusieurs sites 'underground', dont deux chinois…