

# L'Intérieur américain se dote d'un outil anti-Conficker

Si la question de savoir si la [blague du 1er avril](#) sera celle du retour de [Conficker](#) se pose encore, les Etats-Unis semblent avoir décidé de prendre les choses au sérieux.

Le département américain de sécurité (Intérieur) a donc publié un outil permettant de savoir si sa machine est infectée. Sous la forme d'un patch, l'outil a été conçu par l'**US Computer Emergency Readiness Team**. Dans la foulée, l'US CERT a recommandé aux internautes de l'appliquer afin d'éviter que le malware ne continue de se diffuser.

Il faut dire que même si l'on ne connaît pas encore le nombre exact de personnes infectées, la menace semble importante. Pour exemple, même **Microsoft** s'est toujours [refusé à évoquer le nombre de victimes](#). Lors d'une conférence, les responsables de Redmond estimaient : « *Nous ne pouvons pas, à l'heure actuelle, mesurer le nombre de victimes à travers le monde. Si on s'y essayait, on ferait sûrement des doubles comptages. On peut juste imaginer que l'échelle est très large...* ».

Les responsables évoquaient alors le chiffre de 3 millions de victimes. Les éditeurs de sécurité préférant parler de plus de **10 millions de postes infectés**.

Toujours est-il que les contre-mesures s'organisent pour empêcher la diffusion du ver. **Microsoft s'est**

**vu forcé de trouver une solution** en développant une **rustine spécifique qui corrige le bogue dans la fonction AutoRun**. Elle est ainsi [diffusée en mode push](#) à travers **Windows Update**.

Concernant le patch de l'US CERT, il a pour mission d'effectuer un scan de la machine pour trouver l'éventuelle présence du ver. En cas de détection, l'organisation recommande de couper la connexion Internet et de suivre les consignes. Ces dernières sont alors visibles à cette [adresse](#).