Fin du piratage via la version RC de Windows 7 ?

Selon une équipe de chercheurs de la société Damballa, notamment spécialisée dans la sécurité informatique, un **réseau *botnets*(comprendre ordinateur zombies organisés en réseau) aurait été établi avec des postes infectés d'une version piratée de la *Release Candidate* de Windows 7.**

A en croire le site *Clubic*, ces pirates auraient placé un **cheval de Troie au sein du système d'exploitation de Microsoft**. Ensuite distribué illégalement *via* les réseaux de téléchargement tels que **BitTorrent**, la **version de l' OS de Microsoft aurait alors permis d'infecter nombre d'autres ordinateurs.**

A la loupe, les mécanismes du fichier infectieux, à savoir **codec.exe** cacherait un cheval de Troie « générique » qui téléchargerait un faux logiciel anti-virus et installerait un rootkit indétectable par les solutions de sécurité légitimes. **Faux anti-virus qui alertera l'utilisateur que son système est infecté** (effectivement ou non) et l'invitera à acheter une nouvelle version du logiciel de sécurité pour désinfecter son environnement. **Une forme moderne de racket connue sous le terme de *scareware*.**

La société de sécurité affirme aujourd'hui que le serveur de commande du botnet aurait été fermé le 10 mai dernier. Ce même jour, les chercheurs ont estimé que **le taux d'infection était de l'ordre de 552 machines par heure…**

De même, on estime à l'heure actuelle que le botnet regroupait sous sa coupe pas moins de 27.000 machines contrôlables depuis son serveur CetC (*Command and Control)*. Toujours est-il qu'à l'heure actuelle, **les experts ont enregistré 1.600 nouvelles installations de cette version piratée par jour**. Les pays les plus touchés seraient ainsi les Etats-unis (10% de la totalité des machines infectées), les Pays-bas et l'Italie (7%).