Virus: Sasser.C plus virulent que ses frères?

En moins de deux jours, le ver Sasser présente déjà trois variantes. La dernière en date, Sasser.C est apparue ce lundi 3 mai. Elle serait plus dangereuse que ses deux aînés car elle déclenche 1024 processus de scan (au lieu de 128) destinés à identifier de façon aléatoire 1024 ordinateurs connectés à Internet pour les infecter.

Conséquence, Sasser.C pourrait se propager plus rapidement. Mais pour le moment (ce lundi soir), cette propagation semblait encore très limitée et les plus grosses nuisances sont toujours générées par Sasser.B (cf. notre article). Sasser exploite une faille récemment notifiée et corrigée (le 13 avril dernier) par Microsoft dans Windows LSASS (Local Security Authority Subsystem Service). Ce ver attaque par saturation des mémoires tampons. Choisissant aléatoirement des adresses IP, il trouve des passages arrières (« backdoors ») dans les systèmes connectés. Il provoque des redémarrages intempestifs du PC infecté sans s'attaquer aux données stockées. La variante B se répandrait rapidement (1 à 3% des PC dans le monde selon les éditeurs de sécurité) et aurait provoqué pas mal de dégâts au sein des grandes entreprises (lire nos articles). Mais cette propagation a été limitée grâce aux nombreuses mises à jours effectuées par les internautes le 13 avril dernier suite à la publication d'un 'patch' de Microsoft comblant la faille utilisée par Sasser. **Repérer Sasser et s'en débarrasser**

-Symptôme Les variantes de Sasser ont toutes les mêmes effets sur les machines infectées: elles provoquent le redémarrage intempestif de la machine mais ne détruit aucun fichier du disque dur.

Sasser touche uniquement Windows 2000, Windows Server 2003 et Windows XP. Windows 95, 98, Me et NT ne sont pas concernés. -Où le trouver? Sasser ne se cache pas dans la liste des tâches en cours. Un simple appel au gestionnaire des tâches de Windows (ctrl+alt+suppr) permettra de découvrir le processus du ver, appelé avserv.exe ou avserv2.exe. -Comment s'en débarrasser? Un ordinateur doté d'un anti-virus mis à jour et dont le système d'exploitation a été patché grâce à la rustine de Microsoft publiée le 13 avril ne craint rien. En cas d'infection, il s'agit d'abord d'installer un pare-feu avant de mettre à jour Windows via le site de Microsoft. Ensuite, l'utilisateur devra installer et mettre à jour un anti-virus.