Alerte Ver /virus : Sasser-A prolifère, sans e-mail

Les spécialistes redoutaient son arrivée. Il n'aura donc pas fallu attendre longtemps pour observer le premier ver exploitant les dernières vulnérabilités Microsoft Windows LSASS (pour Local Security Authority Subsystem Service). Sasser-A est apparu samedi à 0h00 et sa variante B se propage depuis le début de ce week-end. En quelques heures, ce 1er mai, 423 infections ont été rapportées sur HouseCall contre 140 à Taiwan et 29 au Royaume-Uni. Pendant le week-end, plusieurs centaines de milliers d'ordinateurs auraient été infectés (voir encadré). Et la propagation pourrait prendre beaucoup de vitesse ce lundi à mesure que les bureaux vont se remplir. Contrairement à la majorité des vers, Sasser peut infecter un ordinateur (sous Windows 2000, Windows Server 2003 et Windows XP) simplement s'il est branché sur internet, et non pas par le biais d'un courrier électronique. Il provoque des redémarrages intempestifs du PC connecté (comme le très virulent Blaster) mais n'attaque pas les données de la machine. Ce nouveau parasite exploite une faille récemment notifiée et corrigée (le 13 avril dernier) par Microsoft dans Windows LSASS. Ce ver attaque par saturation des mémoires tampons. Choisissant aléatoirement des adresses IP, il trouve des passages arrières (« backdoors ») dans les systèmes connectés. Le ver exécute du code à distance et peut permettre à un pirate de prendre le contrôle d'une machine infectée. Sasser se propage en cherchant aléatoirement des postes non protégés de cette faille: il scrute le port TCP 9996. Si la vulnérabilité est là, le ver envoie alors un paquet spécialement conçu pour saturer la mémoire tampon du système visé. A la suite de quoi, le programm LSASS.EXE est bloqué, ce qui impose de redémarrer Windows. Le fichier se présente sous la désignation _up.exe, fichier de 16 ko caché dans le répertoire de Windows. Cette faille LSASS est également exploitée par une variante du ver AGOBOT.JF, qui a été détectée 16 jours plus tard. A titre de comparaison, l'été 2003, il avait fallu 26 jours pour détecter, analyser et neutraliser le virus Blaster. Le site anti-virus américain Panda Software a pour sa part indiqué que les pays actuellement les plus affectés étaient le Honduras, les Emirats Arabes Unis, Panama, l'Estonie et Taïwan, selon un pointage ce dimanche 2 mai. Trend Micro propose une détection gratuite : http://housecall.trendmicro.com/ Pour se protéger de cette attaque, il est fortement conseillé de mettre à jour son anti-virus et d'installer le dernier patch (publié le 13 avril) de Microsoft pour Windows. Sasser est par ailleurs facile a repéré. Outre le fait de redémarrer l'ordinateur (en donnant même le nom du composant mis en cause : lsass.exe), il 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. **Une épidémie contestée**

Comme à chaque grande attaque virale, les éditeurs de logiciels de sécurité noircissent largement le trait. C'est normal, c'est le business. Mais les estimations sont pour l'instant très contradictoires.

F-Secure, l'éditeur finlandais évoque *« des millions »* de PC infectés… Plus raisonnablement Trend Micro explique que Sasser ne figure pas parmi les 10 virus les plus virulents actuellement. Symantec de son coté estimait que la propagation était moyenne: de l'ordre de quelques milliers de machines… Panda Software estimait dimanche soir que 3,17% des ordinateurs dans le monde avaient été touchés par Slasser mais ne dit pas combien la planète compte de PC. Il faut dire que la vulnérabilité exploitée par Sasser est corrigée par un patch de Microsoft très largement téléchargé

par les utilisateurs entre le 13 et le 15 avril dernier. Au point d'ailleurs que le site de la firme sature. D'ailleurs, du côté de l'éditeur on minimise l'ampleur de l'attaque. *« Il me parait exagéré de dire que des millions d'ordinateurs ont été infectés »*, a indiqué à l'AFP le directeur technique de Microsoft France Bernard Ourghanlian. Mais il faudra attendre lundi pour observer les vraies possibilités de nuisance de Sasser.