Virus: Bagle.B en perte de vitesse

La propagation de la variante B du ver informatique Bagle s'essouffle ce jeudi, selon les experts de la sécurité informatique. Son code de désactivation est programmé pour le 25 février.

Selon la société américaine MessageLabs, Bagle.B a été repéré dans 66 pays ce mercredi et atteignait un taux d'infection des courriers électroniques de 1 sur 16. Les Etats-Unis étaient les plus touchés avec 16% des e-mails contaminés, suivis par la Grande-Bretagne avec 13% et l'Allemagne avec 10%. Des experts placent en troisième position des vers informatiques les plus virulents de l'histoire cette variante de Bagle. Bagle.B a été conçu pour se propager de manière massive via e-mail (mass-mailing). Il utilise le protocole smtp pour se propager et diffuser une copie de lui-même à grande vitesse. Son gros danger réside dans sa capacité à utiliser des adresses d'expéditeurs usurpées, trompant ainsi aisément ses victimes en laissant croire d'une part que les mails piégés proviennent de sources fiables et d'autre part en exécutant automatiquement le fichier attaché contenant le ver. En clair, le ver falsifie le champ « Expéditeur » dans les e-mails qu'il envoie, ce qui signifie qu'il peut sembler provenir de quelqu'un que vous connaissez, et il s'installe et se gère seul! Conséquence, comme avec Mydoom et ses successeurs, c'est encore le réseau qui va supporter une charge anormale de trafic. Les intitulés des objets des messages ainsi que des pièces jointes sont aléatoires. Comme Mydoom, Bagle.B installe des portes dérobées sur les machines des internautes, les ouvrant littéralement à des utilisateurs étrangers. Le ver amène également la machine à ouvrir quatre pages sur l'internet. Le virus Bagle.B, comme ses prédécesseurs est programmé pour disparaître le 25 février prochain. Les deux versions de Bagle étant apparues avec un mois d'écart, un Bagle.C pourrait faire son apparition le 18 mars, avertissaient jeudi les analystes.