Ver: l'auteur de Netsky prétend avoir créé Sasser

La guerre des auteurs de virus semble repartie. Netsky.AC, une énième variante du ver, circule actuellement par mail et fait croire aux utilisateurs qu'il contient un outil de nettoyage contre le désormais célèbre Sasser.

Pour encore plus tromper les internautes, Netsky.AC comporte une pièce jointe prétendument envoyée par un éditeur d'antivirus. Compte-tenu de la propagation de Sasser, on peut imaginer que de nombreux utilisateurs risquent de tomber dans le panneau et cliquer sur le fichier joint. Erreur fatale: le ver se renvoie alors vers toutes les adresses trouvées sur le disque dur de sa victime, ce qui accroît encore sa diffusion. Mais la véritable originalité de Netsky.AC, c'est son petit texte caché dans son code source. *« 'Hey, av firms, do you know that we have programmed the sasser virus?!?. Yeah thats true! Why do you have named it sasser? A Tip: Compare the FTP-Server code with the one from Skynet.V!!! LooL! We are the Skynet… »*. Traduction: *« Hé! Les firmes d'antivirus, savez-vous que nous avons aussi programmé le virus Sasser?!? Oui, c'est bien vrai. »*. L'auteur de Netsky.AC et de Sasser serait donc la même personne, le même pirate. Après examen et comparaison des codes sources des deux vers informatiques, les éditeurs antivirus ont effectivement noté des ressemblances, notamment dans la façon de générer des nombres aléatoires. Mais la prudence est de mise: *« Il est cependant difficile à ce stade d'être absolument certain que les mêmes personnes sont derrière les deux virus »*, explique Annie Gay, Directeur Général de Sophos France. **Et voici Sasser.D**

La version Sasser.D est apparue lundi, mais, comme la troisième (C), elle est moins menaçante que Sasser.B. Grâce à la médiatisation de ce ver, de nombreux utilisateurs ont mis à jour leurs systèmes d'exploitation et leurs anti-virus. Toutes versions confondues, il semble bien que Sasser soit en perte de vitesse et devrait disparaître ce mercredi.

Selon le finlandais F-Secure, la principale différence entre Sasser D et les précédentes versions est que *« le principal fichier ver est maintenant appelé skynetave.exe au lieu de avserve.exe ou avserve2.exe »*. Comme ses grands frères, Sasser.D exploite une faille de Windows notifiée et corrigée par Microsoft le 13 avril dernier. Il infecte les PC à partir du moment où leur OS n'a pas été mis à jour et s'ils sont connectés au Net. Il provoque des redémarrages intempestifs de la machine.