La chasse aux auteurs de Sasser est ouverte, les profilers entrent en scène

Les experts en sécurité ont entamé la délicate tâche de remonter à la source du ver Sasser afin de débusquer son ou ses auteurs. Mission difficile, voire impossible aux vues des résultats des enquêtes menées sur les virus qui l'ont précédé.

Ce qui est quasiment acquis aujourd'hui, c'est la proximité entre Sasser et Netsky. Tout d'abord, les auteurs de Netsky avaient anticipé dans leurs messages un autre type d'attaques virales. Ensuite, la dernière version de Netsky revendique la paternité de Sasser. Enfin, certaines similitudes ont été découvertes dans les codes des deux virus. Oui, mais? Les auteurs de Netsky ont rendu public le code de leur ver ! Voilà qui rend probable l'existence de versions de Netsky, et peut être de Sasser ou de nouveaux virus, indépendantes des auteurs de la source principale ! **Mais que fait Microsoft ?** Ces six derniers mois, Microsoft a réagi vigoureusement contre les auteurs des virus qui le ciblaient directement, mais l'éditeur ne semble pas vouloir bouger sur Sasser, rappelant que la mise à jour du 13 avril a fermé la faille. Une démarche qui rappelle celle de Bill Gates qui affirmait que la faute relevait des utilisateurs. Microsoft a par trois fois proposé une prime de 250.000 dollars à qui permettrait l'arrestation des auteurs des précédents virus. Vainement, puisque ces derniers courent toujours. L'absence de réaction contre Sasser tendrait à valider la thèse d'un auteur commun avec Netsky. L'éditeur est aussi particulièrement impliqué auprès des autorités de police américaines et collabore régulièrement avec elles. Et puis, le statut de victime a parfois du bon, à condition de ne pas trop se préoccuper de sa notoriété, ce qui n'est pas le cas chez Microsoft. ***Profiler* le ou les auteurs de Sasser** Après les experts, les autorités, le FBI et autres agences gouvernementales de police ou de renseignement, c'est au tour des profilers d'entrer en scène. La police américaine avance l'hypothèse de groupes criminels originaires d'Europe de l'est. Si le lien entre Sasser et Netsky est confirmé, l'identité des auteurs se rapporterait au « Groupe anti-virus Skynet » ? qui se dit russe – qui a précédemment signé certaines versions de Netsky. Sasser pourrait alors entrer dans la guerre des auteurs de virus qui se livre actuellement. Mais la communication est un élément essentiel de cette guerre des egos, et jusqu'à présent les auteurs ont clairement indiqué leurs cibles, ce qui n'est pas le cas ici. De plus, Sasser attaque, entraîne l'arrêt des postes infectés, mais ne crée pas d'autre dégâts. L'attaque du ver, et la multiplication des versions en l'espace de quelques jours, pourraient donc entrer dans une stratégie plus large de test et de repérage? et anticiper une menace plus grande ! **Virus et crime organisé ?** La collusion, enfin, avec le crime organisé reste une hypothèse séduisante, qui tendrait à démontrer que les auteurs ne seront jamais retrouvés, certes, mais une nouvelle fois laisse sceptique. Qu'ils soient terroristes ou criminels, ces groupes n'agissent pas gratuitement, cherchent toujours à tirer un profit soit médiatique mais identifié, soit purement économique. Ce qui n'est pas le cas avec Sasser qui n'est pas signé; et qui ne renvoie pas vers des système de piratage des cartes bancaires, comme c'est le cas sur beaucoup de spams. Difficile dans ces conditions d'apporter une réponse au profil recherché des auteurs de Sasser. Ce qui est certain par contre, c'est qu'ils seront difficiles à trouver et à arrêter, et que le rythme des attaques laisse présager de la virulence des successeurs.