Blaster se répand: il n'en veut qu'à Microsoft !

L'attaque était annoncée et attendue ! Le ver/virus W32.Blater, qui cible exclusivement les systèmes Windows de Microsoft, vient de mettre fin à sa période d'incubation. Comme nous l'avions signalé, les premiers effets du ver ont commencé à se faire sentir dès mardi avec virulence aux Etats-Unis, et depuis ce vendredi 15 août en Europe.

Les serveurs européens de téléchargement de Microsoft, dont les services de mise à jour, ont commencé à enregistrer des baisses significatives vendredi. Les serveurs sous Linux ne sont pas concernés, même chez Microsoft, qui a créé des miroirs afin de maintenir un accès aux fichiers nécessaires à la fixation de la faille de sécurité sur les systèmes Windows. **60 secondes pour réagir avec sans froid!** Blaster se répand sans intervention humaine. L'utilisateur est pris au dépourvu! Mais un simple message, '*System Shutdown*' l'avertit de l'infection de son poste, s'il fonctionnent sous Windows; car le ver n'en veut qu'aux utilisateurs de ce système d'exploitation. A l'apparition du message, W32.Blaster décompte 60 secondes, qui ne peuvent théoriquement pas être interrompues. A zéro, le système est bloqué, sans offrir la possibilité de sauvegarder les documents ouverts. Les utilisateurs aguerris et rapides ont cependant 60 secondes pour empêcher le 'crash': il faut ouvrir le 'prompt' de commande DOS, et lancer la commande '*shutdown ?a*'. Mais, le système est tout de même infecté par le ver! Pour rappel, W32.Blaster se duplique lui-même et se diffuse vers d'autres machines en exploitant une faille de sécurité dans le protocole RPC des variantes de Windows à partir de NT 4.0. Sont donc concernés: -Windows XP toutes versions, -Windows Server 2003 32 et 64 bits, -Windows 2000 Professional, -Windows NT 4.0 Server et Terminal, victimes alors d'attaques par dénie de service. **Il est pourtant si simple de se protéger!...** Une nouvelle fois, la simple règle d'actualisation régulière des « patchs » de Microsoft Windows suffit prévenir toute attaque de W32.Blaster. D'autre part, si ce n'est encore fait sur les nouvelles versions, le ver ne peut pas contourner les pare-feux, dont le 'firewall' de Windows XP qu'il suffit d'activer. Enfin, la majorité des antivirus suffisent à intercepter W32.Blaster, ainsi qu'à désinfecter un poste victime d'une attaque ! **Formater le disque? Pas si vite?!** Microsoft Israël a publié une recommandation de formatage des disques vérolés ! Mais la rapidité avec laquelle l'information a disparu des sites qui l'affichaient tend à rappeler que le formatage du disque n'est pas exactement la bonne solution à adopter! W32.Blaster est aussi connu sous les noms de MBlaster, Balster-A et LoveSan. Selon RedSiren, plus de 2 millions d'ordinateurs auraient été infectés dans le monde durant la semaine écoulée, occasionnant une perte de productivité de 329 millions de dollars aux Etats-Unis, uniquement pour la journée de mardi dernier ! **Enquête du FBI et apparition de nouvelles versions**

Le FBI s'est joint à la chasse aux sources du ver (

worm) W32.Blaster, qui rien qu'aux Etats-Unis aurait infecté en quelques heures plus de 250.000 ordinateurs mardi dernier. L'attaque de Blaster serait devenu une affaire d'Etat, après que le ver ait entraîné la perte de plusieurs douzaines d'ordinateurs au Sénat américain, bloqué la banque de la Réserve fédérale d'Atlanta, et immobilisé durant deux jours les services de CBS New York, ce qui justifie l'intervention du FBI. L'éditeur d'antivirus Symantec a constaté que l'intensité de l'attaque se

serait réduite de moitié après le pic du lancement aux Etats-Unis mardi, la zone de conflit se déplaçant vers l'Europe, avec une sortie d'incubation vendredi, ainsi que vers l'Asie. Les vagues d'attaques pourraient cependant continuer à se succéder, car deux nouvelles versions de Blaster ont déjà été détectées, avec des modifications de codes pour le moment mineures.