Les auteurs de virus multiplient les stratégies

Bugbear, Klez, Blaster, Slammer… A l'heure où le ver Sober ressurgit sous forme d'une troisième variante (voir édition du jour), les éditeurs d'anti-virus communiquent leur traditionnel bilan annuel. Et si les virus les plus dangereux varient selon les classements et les méthodes de calcul, les éditeurs s'accordent en général sur un point : l'année 2003 a battu des records en matière de propagation virale.

L'éditeur Kaspersky recense ainsi 9 épidémies de grandes envergures et 26 de moindre ampleur. En 2002, ces chiffres étaient respectivement de 12 et 34. Mais, *"parallèlement à la réduction de la quantité d'épidémies, on note une croissance exponentielle de leur envergure et une augmentation de leurs actions marginales influençant l'activité globale d'Internet"*, remarque l'éditeur.

1 e-mail sur 20 infecté

Deux épidémies majeures ont mis à mal le réseau mondial et nombre de services d'entreprise : Slammer, un ver qui a profité d'une faille de SQL Server, système de gestion de bases de données de Microsoft, pour augmenter (jusqu'à 80 % dans certaines zones) le trafic Internet (voir édition du 27 janvier 2003) et Blaster qui, profitant d'une vulnérabilité dans le service RPC DCOM, a infecté un grand nombre de machines sous Windows 2000 et XP. Si Blaster a donné naissance à plusieurs variantes plus ou moins efficaces, il vit l'arrivée d'un autre ver, Welchia, chargé de le traquer et le détruire et d'installer le correctif de la faille.

Autre record, détenu par Sobig, dont la variante F infecta 1 courrier électronique sur 20 dans le monde. Triste et inquiétant record puisque l'objectif de la famille Sobig était de créer un réseau d'ordinateurs infectés destinés à lancer des attaques DoS (*Denial of service*) ou encore à servir de serveur de pourriels (voir édition du 25 août 2003). Les sites anti-spam ont notamment été victimes de nombreuses attaques DoS. Des petits malins ont profité de l'effroi provoqué par ces activités virale pour tenter de tromper l'utilisateur. Le ver Swen se présentait ainsi sous la forme d'un message émanant de Microsoft et incitait l'utilisateur à mettre à jour son système en activant la pièce jointe… qui n'était autre qu'un virus (voir édition du 19 septembre 2003). Le ver Mimail se faisait passer pour un message du service américain de paiement en ligne PayPal et demandait au destinataire ses comptes d'utilisateur en prétextant une perte des données du client au sein de la société… (voir édition du 3 novembre 2003)

85 % de vers

Selon Kaspersky, les vers ont largement dominé l'activité virale avec plus de 85 % de présence sur le réseau (voir édition du 1er décembre 2003). Les virus occupe moins de 10 % tandis qu'on note l'apparition significative ? même si elle n'atteint pas les 5 % ? des Chevaux de Troie (Troyens) qui autorisent la prise de contrôle à distance de la machine infectée. Mais aussi l'espionnage des données personnelles (vols de mot de passe, de numéro de carte de crédit, etc.) 2003 aura surtout été l'année d'un nouveau genre de Troyen, le TroyanProxy qui infecte les serveurs de cache, très utilisés notamment par les fournisseurs d'accès. Il permet notamment de rediriger les requêtes

vers des sites généralement pornographiques.

Enfin, l'éditeur note le déploiement des rétro-virus qui ont la particularité d'intégrer des fonctions visant à déjouer les antivirus et pare-feu. Pas très rassurant. D'autant que les auteurs de virus exploitent de plus en plus fréquemment les failles systèmes pour lesquelles l'éditeur n'a pas forcément encore publié de correctif. A tel point qu'on peut imaginer que, prochainement, la découverte des failles sera révélée par l'arrivée de nouveaux virus.

Face à ces dangers, l'éditeur Tegam propose Viguard qui, contrairement aux solutions anti-viralles traditionnelles, ne base pas son système de protection sur la signature des virus mais sur leur comportement au sein du système (voir édition du 25 février 2003). Si Viguard ignore à quel type de fichier infecté il fait face, il ne dépend pas des mise à jour des signatures des virus pour être opérationnel. Une autre solution pourrait venir d'une interface matérielle et non plus logicielle. Une équipe de chercheurs de l'Université de Washington ont mis au point le FPX (pour *Field-programmable Port Extender*). Il s'agit d'une plate-forme matérielle ouverte et programmable selon les besoins, et qui se place en entrée/sortie d'un réseau. Le FPX affiche la particularité d'analyser chaque bit des paquets de données qui circulent sur Internet afin de repérer les fichiers infectés en fonctions des signatures des virus. Cela avec une grande rapidité (2,4 milliards de bits par seconde). Bien sûr, ce système, présenté en septembre 2003 mais opérationnel selon ses concepteurs, s'adresse aux opérateurs de réseau, au fournisseurs d'accès et aux grandes entreprises plus qu'aux particuliers. Si le FPX reste tributaire de la signature (et donc la connaissance de l'existence de tel ou tel virus), il pourrait limiter la propagation des applications virales. En attendant, protégez-vous et mettez régulièrement à jour les correctifs de Microsoft.