Une nouvelle variante du virus Lovgate dans la nature

Lovgate est de retour. Comme ses précédentes variantes, le ver W32/Lovgate se copie à travers les partages Microsoft mal sécurisés en balayant des plages d'adresses IP à la recherche de machines offrant des répertoires avec des droits en écriture.

Une fois installé, il en crée un nouveau sans restriction nommé « MEDIA », envoie une copie de lui-même à l'ensemble des correspondants présents dans le carnet d'adresses Outlook sous forme d'un mail avec un fichier d'extension .zip attaché. De plus, il infecte les exécutables du système et renomme les originaux avec l'extension « .zmx ». La grande nouveauté pour cette version est qu'il se répand également grâce à la vulnérabilité « RPC Interface Buffer Overflow » découverte en septembre 2003 qui touche Microsoft Windows. Il est conseillé de maintenir son antivirus à jour et si ce n'est pas encore fait, de corriger cette vulnérabilité sur l'ensemble des postes de l'entreprise car une fois le « ver » dans le fruit, il sera difficile de l'empêcher d'?uvrer et d'accomplir la tâche pour laquelle il a été programmé. La combinaison de l'exploitation de la faille « RPC » et l'utilisation du carnet d'adresses Outlook pourrait permettre à ce ver d'atteindre l'antre des entreprises et de contaminer l'ensemble des serveurs et postes fixes vulnérables disposés sur un même réseau. Une fois encore, les parades sont simples. Un antivirus à jour déployé sur l'ensemble des postes, éventuellement un filtrage antiviral au niveau du serveur de messagerie, mais surtout l'installation systématique des correctifs de sécurité vous permettront de contrer ce type de fléau. **Aurélien Cabezon pour Vulnerabilite.com**