Le ver Downadup poursuit ses ravages

Le ver Downadup, aussi appelé Conficker, est en passe de devenir le vecteur de la plus grosse attaque contre les PC Windows depuis des années. Il faut dire que la propagation de ce malware se poursuit à grande vitesse alors que la faille qu'il exploite est corrigée depuis octobre…

Selon Panda Labs, au moins **1 PC sur 16 dans le monde est infecté** par ce ver et 6% des systèmes scannés par l'éditeur sont touchés (soit 111.000 postes sur un parc de 2 millions de machines).

« Ces chiffres sont réalistes », assure Ryan Sherstobitoff, chief corporate evangelist chez l'éditeur espagnol.*« Conficker infecte un nombre toujours plus important de machines dans le monde et sa propagation est de plus en plus rapide ».*On peut alors craindre la constitution d'un réseau botnet colossal dont le but serait de détourner des infos personnelles, d'envoyer du spam ou d'attaquer des réseaux d'entreprise.

L'accélération de l'épidémie est observée depuis une semaine suite à la mise en ligne par des hackers d'un code open-source qui permet d'exploiter encore plus facilement la vulnérabilité. Par ailleurs, de nouvelles méthodes de propagation sont apparues notamment à travers la fonction 'autorun' des clés USB.

Microsoft a tenté de réagir à nouveau en conseillant de désactiver la fonction Autorun. Mais ce conseil est jugé insuffisant par l'US-CERT (Computer Emergency Readiness Team).

Rappelons que Downadup exploite une vulnérabilité dans le service Serveur de Windows qui permet l'exécution de code à distance si un système affecté recevait une requête RPC (Remote Procedure Call) spécialement conçue.

Selon Qualys, qui scanne des centaines de milliers de PC sur la planète, 30% des machines observées sont toujours non patchées et donc vulnérables à la faille. Quant à F-Secure, il estime à 9 millions le nombre de PC touchés.

« Les pratiques de certaines entreprises dont leur gestion des correctifs sont tout simplement inacceptables », commente Wolfang Kandek, CTO de Qualys cité par*Computerworld*. Beacoup d'entreprises n'auraient en effet pas appliqué ce patch, notamment parce qu'il a été publié par Microsoft en dehors des cycles mensuels.

Les utilisateurs et les entreprises auraient-ils relâché leurs efforts en matière de protection ? En tout cas, Downadup aura réussi le tour de force de faire autant de dégâts que les précédents codes les plus malveillants, à savoir Sasser ou Blaster.