Le ‘Top 10’ des virus détectés par Panda en août

L’explication principale donnée par l’éditeur Panda Software est que les pirates évitent les attaques massives. Ils préfèrent la discrétion et les attaques ciblées.

La mode n’est donc plus à l’envoi d’une kyrielle de codes malveillants. L’objectif est maintenant de ne pas éveiller les soupçons du public. La solution réside dans l’utilisation de codes malveillants qui discretement permettant de générer des profits considérables.

Selon Panda : *« la vulnérabilité critique MS06-040 constitue un exemple révélateur de la nouvelle dynamique des malwares. »* Cette faille de sécurité est un exemple typique de problème de sécurité que les vers exploitent pour causer de véritables épidémies à grande échelle.

D’après les statistiques de l’antivirus gratuit en ligne Panda ActiveScan, le code malveillant le plus fréquemment détecté en août est une fois de plus **Sdbot.ftp**, un script utilisé par les vers de la famille Sdbot pour se propager d’eux-mêmes sur les ordinateurs via FTP (File Transfert Protocol).

La deuxième place est occupée par **Jupillites.G** et la troisième place par un habitué du classement, **Netsky.P**, un ver qui exploite une vulnérabilité d’Internet Explorer pour s’exécuter automatiquement lorsqu’il atteint un ordinateur.

Vient ensuite Sinowal.BV, suivi de Bagle.pwdzip, comprenant plusieurs variantes du ver Bagle qui se propagent par messagerie électronique dans une archive protégée par un mot de passe.

W32/Parite.B, un ver qui infecte des fichiers exécutables avec une extension .exe, des fichiers .src et des économiseurs d’écran, et Downloader.IOL, un cheval de Troie conçu pour télécharger d’autres fichiers sur le système affecté, sont respectivement à la sixième et septième place.

Les derniers du classement sont Exploit/Metafile, Ailis.A (un ver qui se propage en faisant des copies de lui-même sans infecter d’autres fichiers pour saturer les ordinateurs et les réseaux, empêchant les utilisateurs de travailler) et Qhost.gen (une détection générique d’une modification du fichier hosts).

La présence persistante de Netsky.P, qui exploite une vulnérabilité découverte cinq ans auparavant, indique que de nombreux ordinateurs n’ont toujours pas été mis à jour et peuvent devenir de véritables plateformes de distribution pour toutes sortes de menaces Internet.