Alerte au ver Zotob.A

La trêve estivale, avec un calme relatif sur le front des attaques virales, se termine. FrSIRT révèle une nouvelle menace, le ver Zorob.A, qui cible Windows 2000.

Une menace plutôt limitée, donc, même si de nombreuses entreprises sont encore équipées du système d'exploitation de Microsoft. Mais une menace réelle qui incite une nouvelle fois à être à jour sur les correctifs. Ce dérivé de Mytob infecte les poste Windows 2000 via le port 445/TCP, utilisé par le service Windows Plug and Play, à partir duquel une fois installé il tentera d'infecter d'autres postes. Zorob.A installe un fichier 'botzor.exe' dans le répertoire %SYSTEM%. Puis il crée le mutex 'B-O-T-Z-O-R' et ajoute une entrée au registre qui lui permettra de s'exécuter à chaque démarrage. Enfin il ouvre un shell et un serveur FTP, puis se connecte à un canal IRC contrôlé par son auteur afin de lui permettre d'exécuter des commandes à distance. Lorsqu'il se transmet sur d'autres postes en exploitant son serveur FTP, Zotob.A se transfère dans un fichier nommé 'hha.exe'.