Les hackers profitent (évidemment) de Noël

La période des Fêtes est propice à la diffusion de code malveillant. Un fichier de Noël diffusé sous la forme d'un puzzle et nommé Christmas_Puzzle.exe est actuellement en train de se propager sur la Toile.

Bien entendu il s'agit en réalité d'un code malveillant, plus précisément d'un cheval de Troie (Ardamax-E ou Warezov). Ce dernier utilise une technologie de rootkit pour se dissimuler.

Au même instant, un fichier PowerPoint nommé Christmas+Blessing-4.ppt utilise des vulnérabilités dans Internet Explorer pour installer du code malveillant sur les machines Windows.

Cet exploit a été dissimulé dans un fichier PPT qui circule sur le Web, indique dans une note l'éditeur F-Secure.

F-Secure a été la cible d'un de ces fichiers de Noël. Le groupe indique qu'il a reçu un document nommé Christmas.exe qui une fois qu'il est activé diffuse une image sur le thème de Noël. En réalité, l'ordinateur ciblé devient un PC zombie sous le contrôle d'une armée de Hackers via un réseau de Botnets.

Selon F-Secure, une nouvelle vague de spam par image sur le thème de la nouvelle année devrait arriver dans nos boîtes de réception.

Le fonctionnement reste le même, du code est dissimulé dans une image histoire de piéger un maximum d'internautes. Les précautions standards permettent de se prémunir contre ses attaques.

Les utilisateurs doivent impérativement mettre à jour leurs antivirus, mais surtout ils doivent résister à la tentation d'ouvrir un mail contenant les mots Christmas_Puzzle ou Christmas.exe.