Santy.C s'attaque aux sites Web écrits en php

Santy poursuit son offensive. L'objectif du ver est toujours le même: défigurer sites Web avec le message:

« *This site is defaced!!! NeverEverNoSanity WebWorm generation* » (voir photo). Il n'a donc aucune incidence sur le poste de l'utilisateur. Au départ, Santy.A s'attaquait aux forums Internet utilisant « phpBB », une application open-source en ligne utilisée pour créer des forums. Le ver profitait d'une faille dans des anciennes versions non patchées du logiciel pour défigurer le site. 40.000 d'entre eux auraient été attaqués. Mais plus original, Santy.A utilisait Google pour trouver ses victimes. Rapidement, l'équipe technique de Google a bloqué les requêtes générées par Santy.A ce qui a gelé l'attaque. Un simple contre-temps pour les pirates. Puisque à peine deux jours après, une variante de Santy est découverte par les éditeurs de sécurité (F-Secure, Symantec). Et ce n'est pas un cadeau. Egalement programmé en Perl, Santy.C ou E (selon les éditeurs, K-Otik estime qu'il n'appartient pas à la même famille) s'attaquerait à tous les sites contenant des pages PHP vulnérables à la faille « include/require » afin d'y installer un IRC-Bot contrôlé par des pirates. Il exploite une palette plus large de failles dites « de programmation » selon K-Otik. Et d'expliquer: Ces fonctions sont normalement utilisées par les programmeurs afin d'inclure des pages web spécifiées en arguments. Malheureusement, la non vérification de ces arguments peut permettre l'inclusion et l'exécution de fichiers externes, et donc la compromission du serveur web. Le ver recherche donc des pages du type « *.php?*= », puis tente d'y insérer différentes commandes permettant l'installation de robots IRC et la constitution d'une armée de machines zombies. Ces failles courantes sont liées aux applications web et non à la plate-forme ou à la version de PHP, explique encore K-OTik Security. Un bon cadeau de Noël pour les webmasters. Free aurait déjà été victime de cette variante, puisque une page de son site Web a été piratée à deux reprises vendredi et samedi (voir notre article).