

Les 'WebWorms', une nouvelle génération de vers informatiques ?

Ces derniers jours, nous avons pu assister à la naissance d'un nouveau malware, le « WebWorm ». La principale caractéristique de ce type de ver est qu'il s'attaque exclusivement aux applicatifs web, comme Santy (voir nos articles).

Il s'appuie donc sur des failles de programmation présentes dans les script PHP, ASP ou encore JSP afin de se répandre. Pour débusquer ses victimes, le ver interroge tout simplement les moteurs de recherche comme Google, Yahoo ou Altavista. Aubaine pour les éditeurs de « reverse-proxy » et véritable casse tête pour les administrateurs de serveurs web, les « WebWorms » n'ont pas fini de faire parler d'eux. Peu importe la nature de la faille qui touche l'applicatif web, si celle-ci permet l'exécution de code arbitraire, elle peut alors devenir un vecteur de propagation pour le ver. Plus cet applicatif est utilisé plus il risque de devenir la cible de l'un de ces vers (ex: Phpnuke, Xoops ...). Peu après l'apparition du ver « santy » sur la toile, son code source était déjà rendu public. Simple mais efficace diront certains. Néanmoins, il montre ses limites en terme de rapidité et de portabilité. Ce qui est sur, c'est qu'à cette heure, des développeurs peu scrupuleux planchent déjà sur de nouvelles versions encore plus performantes... Une nouvelle voie s'ouvre pour les créateurs de virus et de vers. Avis aux développeurs et webmasters, auditez la sécurité de vos applications et ne pariez jamais sur la sécurité des scripts gratuits que vous utilisez pour construire vos sites. (*)
pour Vulnerabilite.com