Vague de sites piratés dont celui des Nations Unies

Le groupe qui a compromis le site Web du Super Bowl 2007 au Dolphin Stadium pourrait être responsable de cette nouvelle attaque.

Les Websense Security Labs indiquent que des centaines de milliers de sites Web légitimes, et donc à bonne réputation, y compris certains sites Web des Nations Unies et de l'administration britannique, ont été compromis par une attaque massive à injection de code JavaScript visant à voler les informations des utilisateurs.

Le procédé employé démontre que les attaques des cybercriminels exploitent désormais les failles laissées par les solutions traditionnelles de sécurité reposant sur l'identification de signatures ou la réputation des sites.

En infectant simultanément des centaines de milliers de sites Web à forte réputation et à fort trafic, les hackers n'ont besoin que d'une fenêtre de quelques heures pour obtenir un grand nombre de victimes potentielles. Les utilisateurs du Web et les entreprises n'ayant pas mis en place une solution de sécurisation en temps réel sont vulnérables.

Cette attaque généralisée et bien orchestrée semble émaner du même groupe à l'origine d'une attaque similaire en mars 2008 qui a infecté des dizaines de milliers de sites Web à excellente réputation avec des liens malveillants.

Dans cette attaque, outre les milliers de nouveaux sites Web qui ont été ciblés, les cyber criminels utilisent des sites compromis par l'attaque de mars et qui n'ont pas été nettoyés, pour héberger le code malveillant.

Pour Dan Hubbard, vp de la division Recherche sur la sécurité de Websense, *« cette attaque vise à abuser les utilisateurs se fiant à la sécurité de leurs sites Web légitimes favoris. Hélas, nous pensons que les attaques ciblant des sites Web fréquentés, ceux avec le plus grand nombre de visites uniques, vont se multiplier. Dans cet environnement de menaces en rapide mutation, les entreprises doivent disposer d'une sécurité Web capable de s'adapter en temps réel. »*