Cyber-attaque : une centaine de milliers de sites Web pris d'assaut

- Informatique - Internet -

Date de mise en ligne : vendredi 3 octobre 2008

Spyworld Actu

Le "Mr sécurité" d'Aladdin Knowledge Systems a repéré cette offensive cyber-criminelle d'envergure mondiale. La France n'est pas épargnée.

Considéré par certains experts IT comme hors d'état de nuire, Neosploit 3.1 du nom d'un logiciel de piratage signe pourtant un retour remarqué. Une enquête menée par Aladdin Knowledge Systems (fournisseur de solution de sécurité IT) du Computer Emergency Response Team (CERT) couvrant 86 pays a révélé que plus de 200 000 coordonnées de serveurs ont été trouvées sur un serveur utilisé par les cyber criminels. Ces données servent à intégrer un contenu malicieux mis en place par Neosploit dans des sites légitimes pour les infecter.

Dans les 200 000 coordonnées de serveurs, 107 000 ont été validées par le serveur criminel. Et, dans cet échantillon, 82 000 ont été utilisés pour modifier le contenu Web afin d'attaquer les utilisateurs de ces sites.

C'est Iam Amit, Responsable des recherches en sécurité au sein de la cellule Aladdin eSafe installé au siège social israélien d'Aladdin Knowledge Systems, qui a découvert cette vaste opération de piratage.

1000 coordonnées de serveurs compromis en France

Nul n'est à l'abri, estime l'expert en sécurité IT : dans cette liste de coordonnées de serveurs figurent des sites gouvernementaux, d'universités renommées, des firmes mondiales, et des organisations nationales et internationales. Si l'on trouve des sites d'envergure dans la cible côté Etats-Unis (comme usps.gov, le site du service postal américain), Aladdin estime que la menace est encore plus grande en Europe.

Et notamment la France avec plus de 1000 coordonnées de serveurs compromis qui ont leur nom de domaine en ".fr" : des sites personnels proposés par des portails comme Lycos ou Free mais aussi des sites Internet de marques ou de groupes industriels connues (TF1.fr, Bouyguestelecom.fr, 3suisses.fr...

"Nous sommes actuellement en train de travailler avec les agences gouvernementales compétentes du monde entier pour déterminer les infections et informer les groupes industriels ou organisations concernés", indiquait Iam Amit dans un contribution sur le blog eSafe CSRT en date du 26 septembre. Les enquêtes de police à travers le monde sont en cours.

Post-scriptum :

http://www.vnunet.fr/news/cyber_att...