

Priorité : Haute

Description :

Attaque de type SQL Injection, aujourd'hui automatisée. Nihorr1 ne consiste pas en un vol de données mais dans l'exploitation d'informations à des fins détournées.

Qui est impacté ?

On dénombre près de 500 000 pages Web.

Des milliers de sites piratés distribuent aujourd'hui des javascripts tentant d'infecter les utilisateurs réguliers de ces sites. Citons quelques sites connus dont le site officiel du service civil anglais ou un des sites des nations unies.

Taper Nihorr1 dans Google renvoie plus de 300 000 résultats dont la plupart sont des sites touchés par l'attaque (la chaîne de caractères Nihorr1 apparaît dans ce cas dans le code HTML des pages infectées).

Comment se produit l'attaque ?

Les URL en elles-mêmes ne sont pas modifiées. Ce sont les éléments qui constituent les pages qui vont contenir le texte et s'activer suites aux actions des utilisateurs.

Chaque page Web qui sera consultée, après avoir été attaquée par Nihorr1 infectera à son tour, l'ordinateur de l'internaute.

Autres conséquences de l'attaque Nihorr1

Cette attaque remet en cause l'intégration de la norme PCI-DSS.

D'autres dangers corrélés à Nihorr1 impactent les sociétés ayant intégré la norme PCI ou souhaitant l'envisager. C'est ainsi que dans le respect de la mesure obligatoire 6 du Payment Card Industry (PCI) Data Security Standards (DSS), il est requis de : développer et gérer des systèmes et applications sécurisés (correctifs, mises à jours officielles, évolutions de configurations, failles courantes).

Si les sites Web sont infectés par Nihorr1, il devient possible de contrôler les données. Par exemple, des codes de cartes de crédit peuvent être copiés et communiqués sur des pages Web...

La solution avec rWeb :

rWeb apporte la solution pour protéger vos applications de cette nouvelle attaque grâce à sa liste noire et sa fonctionnalité de scoring list (permet de définir et hiérarchiser plusieurs critères afin de bloquer des familles d'attaques et non plus uniquement une signature spécifique).

rWeb de Deny All, répond aux exigences de la mesure 6 de la norme PCI avec un éventail très large de fonctionnalités de filtrage (normalisation d'adresse, liste noire, liste pondérée, liste blanche, surveillance de comportement, suivi de session, fonctionnalités XML) qui protègent contre les attaques connues et certaines attaques non référencées, ainsi qu'envers les modification logicielles non validées et les évolutions applicatives.

Pour plus d'informations sur comment rWeb contribue à une démarche de normalisation PCI et en quoi ce firewall applicatif facilite le processus de certification, vous pouvez consulter notre récent livre blanc « Conformité PCI avec le pare-feu applicatif rWeb de Deny All » disponible sur notre site Web :

http://www.denyall.com/index.html?option=com_form_download&cfid=10&Itemid=200

Plus d'informations sur rWeb

Pour mieux découvrir notre firewall applicatif rWeb, <http://www.denyall.com/rWeb.html>

Pour détailler les fonctionnalités du produit rWeb,

http://www.denyall.com/data/pdf/fr_rweb_fiche_produit.pdf