Sécurité: Aladdin s'attaque aux pièges des 'proxy' anonymes

Pour s'attaquer au problème des ces 'proxy' suspects, l'éditeur Aladdin annonce la mise à disposition d'une nouvelle fonctionnalité de sa solution de sécurité des passerelles **eSafe Secure Web Gateway**, qui permet de bloquer les 'proxy' anonymes.

Cette solution tire profit d'une approche proactive de la sécurité des contenus. Point important, elle est intégrée à eSafe (donc, sans surcoût).

On retiendra également que ces 'proxy' changent fréquemment d'adresse, et qu'il est donc impossible aux filtres d'URL de suivre ces serveurs insaisissables. Outre les méthodes traditionnelles de filtrage, **eSafe Anti-Anonymizer** bloque proactivement ces dangereux 'proxy' en fonction du code de leur site et de leur comportement de communication, même chiffrés par des protocoles SSL.

Pourquoi les proxy anonymes sont-ils si dangereux?

Les 'proxy' anonymes sont des sites Web qui permettent aux Internautes de se connecter à Internet par l'intermédiaire d'un site Web externe et donc de passer outre les restrictions mises en ?uvre en général sur le réseau local.

Ce mécanisme de contournement -conçu à l'origine pour assurer une navigation sûre et anonyme sur Internet- s'avère aujourd'hui dangereux pour les entreprises. Ces « ***anomyzers*** » ouvrent n'importe quel ordinateur à tous les logiciels malveillants habituellement filtrés et bloqués par le dispositif de passerelle.

Dans la plupart des cas, les utilisateurs de 'proxy' anonymes veulent simplement accéder sur leur lieu de travail à MySpace, YouTube et d'autres sites non autorisés par leur employeur. Ils n'ont aucune idée des risques que l'usage de ces serveurs fait courir à leur organisation.

« N'importe qui peut s'abonner à un 'proxy' anonyme pour 9,99 dollars par mois « précise Ofer Elzam, directeur de la gestion des produits pour Aladdin eSafe. *« Et cet abonnement de 9,99 dollars est capable de réduire à néant une protection réseau de 100.000 dollars. Cela revient à****tenir la porte ouverte aux pirates****et aux cybercriminels et à les inviter à s'emparer du réseau de votre organisation. »*