# Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR

Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR

**Les chercheurs mettent en garde contre une augmentation d'attaques par leurre visant les sites de rencontres venant du réseau TOR.**

Les attaques par leurre sont montées via un site de rencontres concurrent pour détourner les utilisateurs d'un site victime vers celui de l'attaquant. La plupart de ces attaques ciblent de multiples services de rencontres et diffusent des spams à un grand nombre d'utilisateurs, en les invitant à rejoindre d'autres sites, probablement tous contrôlés par le même pirate. La motivation de l'instigateur de ces attaques semble donc claire, écarter les utilisateurs d'un site victime et les attirer vers le sien.

Les chercheurs d'Imperva ont récemment assisté à une augmentation des pirates utilisant le réseau TOR pour dissimuler leur identité et mener à bien ce type d'attaques.

Les attaques par leurre venant du réseau Tor se caractérisent par des messages en provenance de clients Tor à un taux relativement faible (mais régulier), de 1 à 3 demandes chaque jour, probablement pour passer sous le radar des mécanismes de limite de vitesse et éviter les contrôles de détection automatique des navigateurs. Malgré le taux très faible des demandes qu'Imperva a pu observer, il est probable que le nombre total de celles-ci soit beaucoup plus élevé, avec seulement quelques demandes exposées dans l'aperçu du trafic utilisateurs Tor.

Il faut également prendre en compte le déficit d'image que représente ces attaques menées par les centaines de faux profils très attractifs qui harcèlent les utilisateurs du site victime et qui abaissent la crédibilité de celui-ci.

Selon Itsik Mantin, directeur de la recherche de sécurité à Imperva : « ***Ces attaques ont le potentiel de perturber considérablement le business des opérateurs de site de rencontres. En utilisant le réseau TOR les attaquants sont capables de cacher leur emplacement réel et leurs identités, ce qui les rends encore plus difficiles à détecter et à bloquer*** ».

Afin de se protéger contre les attaques par leurre, il est recommandé aux sites de rencontre de surveiller de près les faux comptes et de fermer tout ce qui pourrait être considéré comme illégitime. Il est également conseillé de monitorer l'ensemble du trafic TOR et de bloquer toute activité suspecte.

Article original de Damien Bancal

**Les conseils de Denis JACOPINI**

Quelque soit l'e-mail reçu, ceci nous prouve une fois de plus qu'il est nécessaire de décupler notre vigilance. Sachez que le protocole d'envoi des e-mails, le fameux SMTP, se base sur la norme RFC 821 qui date de 1982. Ceci dit, vous comprendrez mieux si je vous dis que ce protocole ne prévoyait pas les dérives d'usages que nous connaissons aujourd'hui.

De nos jours, cette faille, exploitée à outrance par les pirates informatiques, autorise sans aucune difficulté l'usurpation d'identité. Avec les technologies d'aujourd'hui, n'importe qui peut se faire passer pour n'importe qui, et rien ne vous empêche de vous faire passer pour Larry Page ou Sergueï Brin (les fondateurs de Google en 1998) en créant une adresse e-mail de type larry.page@gmail.com ou serguei.brin@gmail.com pour peu que ces adresses e-mail ne soient pas prises. Pire, vous pouvez recevoir un e-mail indiquant le vrai nom et la vraie adresse e-mail de votre meilleur ami alors que vous répondre à une adresse e-mail légèrement différente, celle du pirate usurpant l'identité de votre ami…

De qui peut-on encore se fier ?

Besoin de conseils ? de formation ?, contactez Denis JACOPINI

Réagissez à cet article

Original de l'article mis en page : ZATAZ Des sites de rencontres touchés par des attaques dites de leurre venant du

réseau TOR – ZATAZ