

Recherche UCLouvain

Les logiciels obscurcisseurs, une solution pour masquer ses recherches sur internet?

EN BREF :

- Les « obscurcisseurs » sont des logiciels qui prétendent **masquer** les requêtes que nous effectuons sur internet
- Comment ? En **générant** automatiquement et **aléatoirement d'autres requêtes**, qui doivent permettre de brouiller les pistes auprès des moteurs de recherche
- Mais fonctionnent-ils ? Une équipe de scientifiques UCLouvain-Imperial College of London vient de démontrer que **l'usage de ces logiciels ne garantit pas l'anonymat**

ARTICLE : [HTTPS://IEEEXPLORE.IEEE.ORG/DOCUMENT/10081382](https://ieeexplore.ieee.org/document/10081382)

CONTACT PRESSE :

Julien Hendrickx, professeur à l'Ecole polytechnique de l'UCLouvain : **0486 80 40 60**

Chaque recherche effectuée sur internet génère des données qui sont collectées par les fournisseurs de service utilisés. Dans un souci de **préserv**er sa **vie privée**, peut-on cacher les requêtes que nous soumettons aux moteurs de recherche ? C'est ce que promettent les *obfuscators* ou **logiciels obscurcisseurs**.

Dans une étude publiée dans la **revue scientifique** *Transactions on Information Forensics and Security*, une équipe de chercheurs issus de l'UCLouvain et de l'Imperial College of London a soumis ces logiciels à un modèle mathématique pour **vérifier leur fiabilité**.

« *Le principe de ces programmes est de **noyer votre requête** sous un tas d'autres requêtes en pensant que le moteur de recherche ne pourra pas distinguer ce qui provient de vous et ce qui provient de ce logiciel. Cela offrirait une certaine protection* », explique Julien Hendrickx, un des chercheurs et professeur en ingénierie mathématique à l'Ecole Polytechnique de l'UCLouvain.

Trois besoins auxquels doivent répondre les logiciels obscurcisseurs ont été identifiés :

1. **Indistinguabilité**. La « vraie » requête de l'utilisateur doit être impossible à identifier. Ce qui n'est pas toujours le cas : « *certains programmes ne vont générer que des requêtes en anglais. **Si vous êtes francophone, vous êtes démasqué.*** »
2. **Couverture** : le sujet de la recherche devrait être difficile à identifier. « *Par exemple, si vous faites des recherches sur des vacances en Méditerranée.* »
3. **Imprecision**. « *La recherche émise doit rester difficile à identifier, même si quelqu'un est au courant du domaine général que vous investiguez. Si votre escapade en Méditerranée est connue, on ne doit pas pouvoir identifier votre recherche sur des hôtels précis.* »

Verdict ? La plupart des obscurcisseurs actuellement disponibles se sont révélés **vulnérables aux attaques**, mettant potentiellement en danger les données des utilisateurs. Plus inquiétant, il semble qu'il soit très difficile, voire théoriquement impossible, de construire un bon obscurcisseur. « *On a pu démontrer de façon mathématique qu'il était impossible d'atteindre simultanément les différents objectifs. On ne peut pas à la fois cacher le domaine général des recherches et des recherches précises. On pourrait éventuellement atteindre un des objectifs, mais pas les deux complètement et simultanément.* »

Les chercheurs mettent en garde contre **un faux sentiment de sécurité** que pourraient éprouver les usagers de ces logiciels. Ils en appellent à une **évaluation approfondie** des propriétés des obscurcisseurs de requêtes et le développement de logiciels fondés sur des principes transparents.