Les sites internet voient tout ce vous faites

Certains des sites internet les plus importants utilisent des logiciels tiers pour pister tout ce que vous faites pendant que vous les visitez, y compris ce que vous tapez, où vous cliquez et ce que vous faites défiler.

Quiconque prête attention aux questions de confidentialité et de sécurité en ligne est déjà conscient du pistage basique des sites internet (pages affichées, recherches). L'étendue et la profondeur du pistage peuvent toutefois désarçonner même les lecteurs les plus désabusés. De nouvelles recherches se sont intéressées à l'utilisation de scripts de relecture de sessions qui pistent exactement ce que font les utilisateurs lorsqu'ils naviguent sur certains des sites internet les plus populaires.

Ces sites capturent ce que vous tapez, ce que vous survolez à l'aide de la souris et ce sur quoi vous cliquez. Un peu comme un enregistreur de frappes. Pour les diagnostics de performance, certaines de ces méthodes sont logiques : si vous avez un site internet qui peut compter des centaines de milliers de pages, vous devez apprendre ce que les gens y font et si certaines pages sont défectueuses ou ne fonctionnent pas comme prévu.

Ce qui pose problème, c'est quand le logiciel est capable de pister un grand nombre d'informations qui ne sont pas nécessairement utiles pour les développeurs de sites internet, et que des tiers ont accès à ces informations. Un groupe de chercheurs de l'Université de Princeton a fait un rapport sur ce

phénomène , et affirmé : *» La collecte du contenu des pages par des scripts de relecture tiers peut causer la fuite d'informations confidentielles telles que les problèmes médicaux, les données de carte de crédit et d'autres informations personnelles affichées sur une page à un tiers, dans le cadre de l'enregistrement. Cela peut exposer les utilisateurs à des vols d'identité, des escroqueries en ligne et d'autres comportements indésirables.*

Comme l'ont également souligné les chercheurs, ce type de logiciel de lecture est *« comme quelqu'un qui regarde par-dessus votre épaule »*, pendant que vous êtes en ligne.

Ce type d'enregistrement fournir aussi des informations supplémentaires qui, si (ou quand) elles sont divulguées, peuvent se montrer vraiment dangereuses. Les recherches ont signalé que le logiciel avait la capacité de :

- Enregistrer les mots de passe saisis – et cela bien que les développeurs aient essayé de s'assurer que tous les mots de passe saisis étaient supprimés ; la programmation n'était pas parfaite et cette fonction ne marchait pas complètement sur les versions mobiles des sites.
- Saisissez des données confidentielles comme des numéros de carte de crédit et des dates de naissance.
- Enregistrez les données saisies dans des boîtes de texte, même si ces données ne sont pas envoyées au site – en d'autres termes, même si vous ne cliquez pas sur » Rechercher » ou » Envoyer » et n'appuyez sur Entrée.

Alors, que pouvez-vous faire pour arrêter ce genre de pistage ? Contactez-moi et je vous proposerai des solutions.