

## Vous avez toujours voulu savoir comment s'attrape un adware ?

Ce n'est pas très difficile, il suffit d'un peu d'inattention, d'une pincée de naïveté et d'un brin de méconnaissance technique. Suivez le guide pour une infection illustrée.

Début de l'opération : une recherche sur Google pour tenter de retrouver un questionnaire amusant à envoyer aux amis. Le premier site retourné par le moteur de recherche semble convenir, on s'y rend d'un clic.

**Première erreur** : Le site est un .biz, un domaine réputé pour être un nid à escrocs du web. Ce n'est bien entendu pas une règle d'or mais la pratique montre que le domaine .biz plaît particulièrement aux escrocs.

Sitôt arrivés sur le site, une boîte de dialogue surgit à l'écran. Son texte est en français,,,

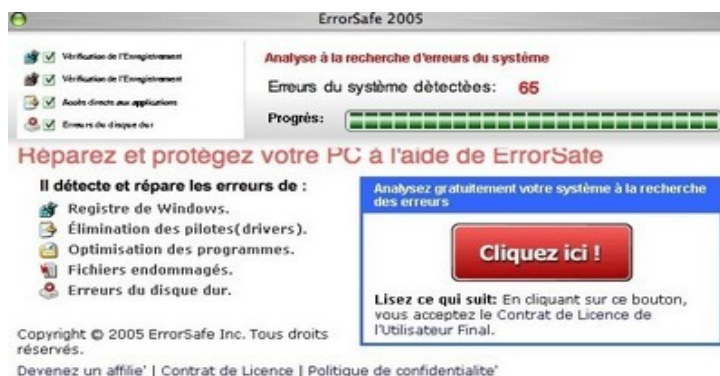


Le site, bien sûr, ne demande pas d'emblée l'autorisation d'installer un adware sur le PC. L'objectif est d'abord de semer le doute en faisant croire qu'un outil (sur votre ordinateur, peut-être ?) est en train de procéder à une analyse du système, ou qu'une telle analyse n'a pas encore été lancée mais qu'elle serait nécessaire (la traduction n'est pas un modèle du genre). Bref, dans tous les cas, que tout cela pourrait avoir des conséquences néfastes.

Techniquement, ce charabia ne veut rien dire. Mais il suffit bien souvent à semer le doute chez l'internaute pas très intéressé par la technique. Et puis, de toute façon, c'est gratuit... alors on clique !

La boîte de dialogue ment afin d'obtenir l'accord de l'internaute pour passer à la suite du programme.

**Seconde erreur** : Répondre "Oui" à une boîte de dialogue de votre navigateur sans réellement comprendre la question est dangereux. Comme souvent en informatique, dans le doute, mieux vaut s'abstenir !



Une fois la pseudo-analyse acceptée, une fenêtre web restée vide depuis le début des opérations s'active soudain. Elle simule l'interface d'un outil ressemblant à un antivirus ou un antispyware et va jusqu'à faire croire à une véritable auscultation de votre système.

Bien entendu, cette dernière relèvera plusieurs dizaines de problèmes sur le PC. Tout ceci est bien sûr un leurre. Aucune analyse n'a lieu, et le seul objectif de cette mascarade est de faire cliquer sur un bouton destiné à télécharger le programme infectieux.

Effrayé par autant d'erreurs, l'internaute naïf cliquera probablement sur le bouton salvateur censé réparer tout ça. Et c'est justement ce qu'attendent les escrocs...  
une fausse analyse antispyware...

Même sur un Mac, l'analyse relèvera des dizaines de problèmes habituellement réservés à Windows, tels ceux de la base de registre...

Troisième erreur : Accepter l'installation d'un logiciel (même, voire surtout, gratuit) que vous n'avez pas demandé revient généralement à infecter votre ordinateur.

Une fois le bouton cliqué, l'affaire est entendue. Le programme ErrorSafe/WinFixer se télécharge et c'est le début d'une longue série d'ennuis.

Si vous tenez malgré tout absolument à lire des histoires d'horreur à son sujet, une simple recherche sur Google achèvera de vous convaincre que, oui, finalement, il est plus sage de ne pas cliquer n'importe où !