



SmartScreen de Microsoft

évitez les sites malicieux

Pour plus de sécurité, adoptez les réflexes CASES !

SmartScreen

Internet nous offre des opportunités uniques, mais représente aussi une plateforme de choix pour les malfaiteurs. De fait, le navigateur est une fabuleuse porte d'entrée pour les programmes malveillants. L'une des manières d'infecter un ordinateur est de faire ouvrir à l'internaute une page web qui exploite les vulnérabilités techniques du navigateur utilisé. La vulnérabilité étant une brèche permettant à des logiciels malveillants de s'installer et de prendre ainsi le contrôle de la machine. Néanmoins, l'une des manières d'infection les plus répandues reste de leurrer les internautes afin que ceux-ci téléchargent et installent eux-mêmes des codes malicieux sans s'en rendre compte.

En exploitant des sentiments humains comme la curiosité ou encore la peur, on pousse les internautes à installer « faux antivirus », scareware ou autres malwares en tous genres. Le malfaiteur fait p.ex. croire à la victime potentielle que son ordinateur est infecté, instaurant ainsi un sentiment de peur. Grâce à ce vecteur, le criminel incite alors l'utilisateur à télécharger un « anti-virus » qui, en fait, n'est pas un programme de protection, mais bien le code malicieux. Il va donc installer lui-même ce code en croyant installer un logiciel utile.

Plusieurs logiciels peuvent aider les internautes à reconnaître ces différentes formes d'attaque basées sur l'ingénierie sociale. Il y a p.ex. l'ajout du navigateur WOT (Web of Trust), qui met l'internaute en garde lorsque celui-ci visite une page web de pauvre réputation, ou lorsqu'il consulte un moteur de recherche.

Depuis Internet Explorer 8, Microsoft propose un service qui s'appelle « Smart Screen ». Ce service « cloud » analyse chaque URL que le navigateur veut visiter et met en garde l'internaute avant qu'un logiciel malveillant ne soit téléchargé.

[D'après le laboratoire de sécurité NSS Labs](#), qui vient de tester les différents filtres intégrés dans les navigateurs, « Smart Screen » de Microsoft serait de loin le plus performant. Lors du test, il aurait reconnu 96% des sites malicieux.

Quant aux considérations liées à la protection de la vie privée, chaque internaute doit décider s'il veut profiter à tout moment ou seulement sporadiquement de ces services. Vu que les URLs sont envoyées vers des applications cloud de Microsoft, il est possible qu'un profil de l'internaute soit ainsi établi.

Pour activer ce service, il suffit cliquer sur le bouton Sécurité, sur Filtre SmartScreen, puis sur Activer le filtre SmartScreen ([voir le site de Microsoft](#)).

Cette solution présente cependant un autre avantage manifeste. En effet, l'internaute n'est pas obligé d'attendre la mise à jour des bases de signatures antivirus, qui se font selon la configuration, toutes les quelques heures voire plus rarement encore.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur: