Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs | Le Net Expert Informatique

Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs

Face à la diversité des outils de détection de malwares, les pirates informatiques n'hésitent pas à faire preuve d'inventivité pour atteindre leurs objectifs. En effet, une société du nom de Claralabsoftware a mis en œuvre un navigateur du nom d'eFast. Ce navigateur est censé améliorer l'expérience de navigation en fournissant des résultats de recherche les plus pertinents, en affichant des réductions et bonnes affaires disponibles sur la toile, et en fournissant des outils de protection contre les phishings et divers malwares. Il est basé sur Chromium, le navigateur open source sur le lequel sont fondés plusieurs autres navigateurs dont Chrome, Opera, Vivaldi, etc.

Les utilisateurs voyant donc les caractéristiques d'eFast pourraient croire à une application dénuée de tout code malveillant, mais tant s'en faut. Selon le rapport de Malwarebytes, l'entreprise de sécurité informatique, lorsque vous installez eFast, ce dernier essaie automatiquement de prendre le contrôle du terminal sur lequel il est installé en cherchant à devenir le navigateur par défaut.

En plus de cette action, eFast s'associe par défaut avec les extensions de fichiers suivantes : gif, htm, html, jpeg, jpg, pdf, png, shtml, webp, xht, xhtml. La même association est effectuée pour les schémas, protocoles, et autres objets URL suivants : ftp, http, https, irc, mailto, mms, news, nntp, sms, smsto, tel, urn, webcal.

Lorsque ces extensions sont associées par défaut à eFast, pour toute tentative d'ouverture de fichier, d'appel d'un protocole ou toute action utilisant les objets listés plus haut, c'est le navigateur eFast qui exécutera l'action souhaitée.

En plus de cela, eFast redirigeraient les internautes vers des pages publicitaires ou d'autres pages web qui pourraient héberger des malwares. En outre, PCrisk rapporte qu'eFast est un aspirateur de données de navigation. Ces informations une fois collectées pourraient être partagées avec d'autres personnes et utilisées à mauvais escient afin de gâcher la vie d'un internaute.

Selon PCrisk, ce programme pourrait s'installer lors de l'installation de certains programmes. En effet, les développeurs pourraient cacher l'option d'installation de ce programme dans les paramètres personnalisés. C'est pourquoi il est recommandé de ne pas installer les applications en utilisant les paramètres de recommandation, mais plutôt les paramètres personnalisés.

Une des choses à ne pas négliger par ailleurs est que lors de l'installation d'eFast, celui-ci se charge de supprimer les raccourcis de Chrome sur le bureau et la barre des tâches et installe par la même occasion des raccourcis de YouTube, Amazon, Facebook, Wikipedia et Hotmail sur le bureau. Il faut noter qu'il est très similaire à Chrome aussi dans la présentation générale que dans les couleurs de l'icône.

Enfin, nous précisons qu'en voulant nous rendre sur le site de l'éditeur clara-labs afin d'effectuer des recherches supplémentaires, Chrome nous a envoyé une alerte afin de signaler que le site que nous voulons ouvrir contient des programmes dangereux. Ce n'est donc pas uniquement le produit de l'entreprise qui est étiqueté comme dangereux, mais même le site l'est également.

Source :
http://www.developpez.com/actu/91354/Des-chercheurs-decouvrent-un-navigateur-malveillant-base-sur-Chromium-il-se-presente-comme-une-imitation-de-Chrome-afin-de-tromper-les-utilisateurs/
par Olivier Famien