



Forum: Sécurité

Topic: De dangereux malwares ont infecté Chrome par le biais d'extensions

Subject: De dangereux malwares ont infecté Chrome par le biais d'extensions

Publié par: Wullfk

Contribution le : 25/08/2017 16:27:49

Citation :

Huit extensions malveillantes ont été détectées sur le navigateur web de Google. Celles-ci peuvent vous dérober du trafic et des identifiants.

Ce n'est pas directement Google Chrome, plutôt paré en matière de sécurité, mais des extensions pour ce dernier qui sont visées par cette attaque. En effet, les développeurs de huit extensions ont été victimes de vols d'identifiants via phishing, menant les cybercriminels à utiliser leurs accès pour ajouter du code malveillant à leurs extensions.

Ce sont les équipes de Proofpoint (une compagnie américaine œuvrant pour la sécurité informatique des entreprises) qui ont repéré les huit applications touchées. Parmi celles-ci : **Chrometana 1.1.3**, **Infinity New Tab 3.12.3**, **Web Paint 1.2.1**, **Social Fixer 20.1.1**, **TouchVPN**, **Betternet VPN** ainsi que des extensions de **Copyfish** et **Web Developer**.

D'autres attaques potentielles sont à prévoir

Le malware redirige le trafic vers certains sites à l'insu de l'utilisateur, remplaçant les publicités présentes sur les sites par des publicités choisies par les pirates. Il fait aussi apparaître des pop-up indésirables sur le bureau de la cible, affirmant que son ordinateur rencontre un problème et le redirigeant vers des services d'assistance en ligne, contre une éventuelle commission pour les attaquants.

Son but est aussi de dérober des identifiants de connexion au service d'hébergement et de sécurité internet Cloudflare, ce qui pourrait engendrer à l'avenir une autre vague d'attaques sur les sites utilisant ce service.

Source : proofpoint.com

Source : [http://geeko.lesoir.be/2017/08/24/de- ... wares-ont-infecte-chrome/](http://geeko.lesoir.be/2017/08/24/de-...-wares-ont-infecte-chrome/)