BitDefender : Un cheval de Troie dÃ©guisÃ© en extension Google Chrome
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 20/4/2010 0:00:00

De plus en plus de personnes utilisant **Google Chrome** et ses fonctionnalitÃ©s pour naviguer sur Internet et organiser des informations, des **cybercriminels ont dÃ©cidÃ© dâ□□exploiter cet environnement** pour diffuser des malwares et dÃ©rober des donnÃ©es personnelles des utilisateurs.

Le principe est simple : les utilisateurs de Google Chrome reÃ§oivent un e-mail non sollicitÃ© leur indiquant quâ□□une nouvelle extension de leur navigateur favori a Ã©tÃ© dÃ©veloppÃ©e afin de simplifier lâ□□accÃ¨s aux documents envoyÃ©s par e-mail.

Un lien Ã lâ□□apparence anodine est indiquÃ©, et les destinataires sont invitÃ©s Ã le suivre afin de tÃ©lÃ©charger la nouvelle extension. Sâ□□ils cliquent dessus, ils sont redirigÃ©s vers une page ressemblant Ã celle des extensions Google Chrome, qui ne leur fournit pas lâ□□extension promise mais une fausse application installant des malwares sur leur systÃ¨me.

Bien que la description de la fausse application soit identique Ã celle de la vÃ©ritable extension Google Chrome, un Ã©lÃ©ment devrait mettre la puce Ã lâ□□oreille des utilisateurs attentifs :

lâ□□application nâ□□est pas une extension Â« crx. Â» mais Â« .exe Â».

IdentifiÃ©e par BitDefender sous le nom de Trojan.Agent.20577, lâ□□application modifie le fichier HOSTS de Windows afin de bloquer lâ□□accÃ¨s aux pages web de Google et de Yahoo.

Lorsque les utilisateurs souhaitent y avoir accÃ¨s et tapent Â« google.[xxx] Â» ou Â« [xx].search.yahoo.com Â» dans le navigateur web, ils sont redirigÃ©s vers une autre IP : 89.149.xxx.xxx .

Cela permet aux auteurs de ce malware dâ□□intercepter les appels des victimes pour se connecter Ã ces sites Internet et de les rediriger vers leurs propres versions de ces sites, infectÃ©es par des malwares.

Pour plus dâ□□informations concernant **les produits BitDefender**