Firefox affecté par deux Trojan cachés dans les extensions

La semaine dernière, le 4 février, la Fondation Mozilla a pris la décision de retirer deux extensions parmi les milliers proposées dans la bibliothèques de modules complémentaires à Firefox (notamment), Addon Mozilla (AMO). Ces deux extensions sont **Sothink Web Video Downloader 4.0** (les versions supérieures ne sont pas affectées) et toutes les versions de **Master Filer**.

Ces deux applications *« contenaient un Trojan visant les utilisateurs de Windows »*, justifie l'éditeur du navigateur alternatif. Sothink Web Video Downloader est affecté par le code malicieux **Win32.LdPinch.gen** tandis que Master Filer s'avère héberger le Trojan **Win32.Bifrose.32.Bifrose**. Les utilisateurs des plates-formes Mac OS X et Linux sont donc épargnés par le problème.

Mozilla précise que, installés sur Firefox, ces deux agents malveillants s'exécutent au démarrage du navigateur et l'ordinateur hôte est alors infecté par les Trojan. S'il s'avère indispensables de désinstaller les modules d'extensions, *« leur désinstallation ne supprime pas les Trojan du système »*. **L'utilisateur devra faire appel à un anti-virus** ou les désinstaller à la main pour les supprimer définitivement de sa machine.

Paradoxalement, les anti-virus utilisés par l'éditeur n'avaient pas été en mesure de détecter les menaces contenues dans ces extensions. En conséquence, **Mozilla a décidé de renforcer son système de détection** en ajoutant deux autres scanners de *malware* et de repasser toutes les extensions actuellement proposées sur AMO à la moulinette sécuritaire. Ce qui avait permis de révéler le code malveillant présent dans Sothink Web Video Downloader 4.0. Pour l'heure, aucune autre menace n'a été détectée.

Difficile d'évaluer les dégâts causés par l'intrusion malveillante. Mozilla précise que Master Filer a été retiré de AMO le 25 janvier dernier après avoir été **téléchargé 600 fois** depuis septembre 2009. Détecté grâce aux nouveaux outils de détection, Sothink Web Video Downloader 4.0 n'a été éliminé qu'une semaine plus tard, le 2 février. Proposé depuis février 2008, l'application a été **installée sur Firefox 4000 fois**, selon Mozilla.

C'est la première fois que la sécurité des produits de Mozilla est prise en défaut sur une aussi longue période. Surtout, elle met en évidence les **risques qu'il y a à installer des extensions des navigateurs** et autres clients de messagerie, même quand elles validées par l'éditeur. Mais il s'agit d'un fait rarissime qui ne remet pas en cause la solidité du navigateur Firefox en soi et la réactivité de son éditeur pour en combler les vulnérabilités.