Un ver exploite Mp3 piégé et pages Web infectées

Pas de répit pour ceux qui téléchargent. De nouveau types de malwares contiennent des liens vers des pages Web. Ces derniers infectent alors les dossiers relatifs au lecteur propriétaire de Windows (Media Player).

« *Cette**possibilité est apparue depuis peu de temps**mais c'est la première fois que nous la voyons se réaliser* » explique David Emm, consultant en technologie pour Kaspersky. Explications. Le format ASF de Microsoft (format propriétaire) a été créé pour donner la possibilité de lire des flux audio et vidéo. Il peut néanmoins supporter d'autres contenus comme des images ou des liens placés sur des pages Web.

Lorsqu'un utilisateur lance une musique infectée, automatiquement Internet Explorer s'ouvre vers une page Web. Sur cette dernière, on vous demande de télécharger un codec… La technique n'a vraiment rien de révolutionnaire. Elle est même bien connue pour obliger l'internaute à télécharger n'importe quel malware sur son poste. **Le codec dévoile alors sa vraie nature, celle d'un Trojan**. Celui-ci peut permettre à un pirate de détourner du trafic via l'ordinateur infecté. Il sert de moyen pour le hacker de brouiller sa piste.

Les Trojans venant de réseaux P2P s'étaient fait un peu plus discrets ces derniers temps. Après » Whistler « , un cheval de Troie destructeur qui supprimait un maximum de fichiers mp3, la mode semble être revenue à la propagation de fichiers malveillants.

D'autant que ce « ver mp3 » possède d'autres caractéristiques bien particulières. Une fois confortablement installé sur votre poste, **il recherche tous les fichiers mp3 et mp2 et les transforme au format de Microsoft.** Ensuite, des liens vers des sites piégés sont automatiquement placés à chaque copie du dossier infecté.

Le risque est d'autant plus important que désormais, les lecteurs de médias nécessitent des mises à jour régulières ce qui rend plus aisé l'intervention d'éventuels malwares.

Ce nouveau venu de la famille des Trojans a été baptisé de différentes façons. Trend Micro l'a appelé « Troj_Medpinch.a, », Secure Computing a préféré « Trojan.ASF.Hijacker.gen ». Enfin Kaspersky a choisi pour sa part le doux nom de « Worm.Win32.GetCodec.a. ».

Le seul remède reste toujours de veiller aux mises à jour des bases de vos Antivirus, et autres Firewall… et surtout de regarder où vous mettez les pieds. Un peu comme à la plage finalement.