Les cybercriminels créent des moteurs de recherche conçus pour amener les internautes sur des sites malveillants

- Cette nouvelle tendance reflète la professionnalisation des pirates.

- La plupart des sites web dans les pages de résultats de ces moteurs de recherche sont des sites malveillants.

- Un des moteurs de recherche contrefait détecté par PandaLabs a déjà été utilisé par près de 195 000 internautes qui peuvent être infectés.

Paris, le 25 mai 2009

PandaLabs, le laboratoire de détection et d'analyse de Panda Security, a remarqué que les cybercriminels utilisent maintenant leurs propres moteurs de recherche pour amener les utilisateurs sur des sites malveillants, généralement conçus pour propager des malwares.

Cette nouvelle tendance souligne la professionnalisation croissante des pirates. Par le passé, les cybercriminels utilisaient des techniques SEO[1], légales ou prohibées, pour améliorer le classement de leurs pages malveillantes dans les résultats des moteurs de recherche les plus populaires. Maintenant, ils utilisent leurs propres moteurs de recherche pour conduire les utilisateurs sur ces pages web conçues pour les infecter. Un de ces moteurs de recherche détectés par PandaLabs compte près de 195 000 visiteurs.

Ces moteurs de recherche fonctionnent de la façon suivante. Lorsqu'un visiteur tape un terme dans le moteur, celui-ci ne produit que cinq ou six résultats. Quand l'internaute clique sur un de ces résultats, il arrive sur un page web spécialement développée pour propager le logiciel malveillant. Le visiteur peut regarder des vidéos sur ces sites mais, pour cela, il doit d'abord télécharger une nouvelle version d'un lecteur média. S'il le fait et télécharge ce programme qui est en fait fictif, son ordinateur est immédiatement infecté par un code malveillant. Vous pouvez en voir un exemple sur : http://www.flickr.com/photos/panda_security/3504323344/

Prévenir l'ingénierie sociale

Cette technique, connue sous le nom d'ingénierie sociale, consiste à tromper l'utilisateur pour, par exemple, le faire cliquer sur un lien malveillant ou exécuter un malware.

« Nous avons pu identifier ce mode de fonctionnement en cherchant sur des moteurs de recherche des termes couramment utilisés par les pirates, par exemple la « grippe porcine » ou le nom de célébrités telles que « Britney Spears » ou « Paris Hilton ». Les résultats de ces recherches nous amenaient sur des pages utilisées pour la diffusion de logiciels malveillants. Nous avons ensuite constaté que le fait de taper nos propres noms conduisait également à des pages frauduleuses. », explique Luis Corrons, le directeur technique de PandaLabs. « Il arrive parfois que des pages web tout à fait normales se glissent dans les résultats de la recherche, probablement pour donner l'illusion que le moteur de recherche est "honnête". »

Pour se protéger contre ces attaques, PandaLabs conseille d'utiliser les moteurs de recherche avec une extrême prudence, de privilégier les moteurs reconnus et d'être vigilant lorsque vous surfez sur des sites proposant des informations et vidéos spectaculaires.

[1] SEO (Search Engine Optimization) : optimisation du référencement sur les moteurs de recherche

« S'il vous est demandé de télécharger un codec ou tout autre type de programme de lecture de vidéo sur ce genre de site web, il y a de grandes chances qu'il s'agisse en réalité d'un code malveillant. », prévient Luis Corrons.

Retrouvez des images illustrant cette tendance à l'adresse :
http://www.flickr.com/photos/panda_security/tags/adwarewebmediaplayer/

Plus d'informations sur le blog de PandaLabs :
http://pandalabs.pandasecurity.com/archive/Swin-flu-and-the-Blackhat-SEO-techniques.aspx

A propos de PandaLabs

Depuis 1990, la mission de PandaLabs est d'analyser les nouvelles menaces le plus rapidement possible pour assurer une totale sécurité à nos clients. Pour cela, PandaLabs a développé un système automatisé et innovant qui analyse et traite les milliers de nouveaux échantillons reçus chaque jour et renvoie automatiquement un verdict (logiciel malveillant ou inoffensif). Ce système repose sur l'Intelligence Collective Antimalware, le nouveau modèle de sécurité de Panda Security, qui détecte même les codes malveillants capables de passer au travers des autres solutions de sécurité.

Actuellement, 94 % des malwares détectés par PandaLabs sont analysés par l'Intelligence Collective Antimalware. Cette analyse automatique est complétée par le travail de plusieurs équipes spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, rootkits, etc.) qui travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Grâce à ce système, Panda peut offrir à ses clients des solutions plus sûres, plus simples et consommant moins de ressources.

Pour plus d'informations, visitez le blog de PandaLabs : http://www.pandalabs.com