



Communiqué de presse – libre à la publication immédiate

Emsi Software met en garde : stationnement interdit déclenche de nouvelles attaques de virus !

Emsi Software, fournisseur du logiciel de protection a-squared Anti-Malware 4.0, vous met en garde d'une nouvelle attaque qui, jusqu'à présent, sévit uniquement aux États-Unis. De plus en plus d'automobilistes après leurs achats trouvent une amende sous leur essuie-glace du pare-brise avant. Les détails pour le stationnement interdit et pour le ticket de contravention, les conducteurs doivent les retirer sur le Web. Les automobilistes qui cliquent sur ce lien hypertexte s'attrapent seulement de nouveaux logiciels malveillants sur le PC.

Salzburg, Février 2009 - Beaucoup de visiteurs d'un centre commercial à Grand Forks (ND), États-Unis, sortant du magasin chargés avec de grands sacs en papier furent très surpris au retour à leur voiture. Coincés sur les essuie-glaces de leur pare-brise, ils trouvèrent une contravention - pour stationnement interdit. Sur la contravention, on pouvait lire :

"PARKING VIOLATION This vehicle is in violation of standard parking regulations. To view pictures with information about your parking preferences, go to website xxx."

On pourrait traduire ceci : "Ce véhicule est en infraction et VIOLE LES RÈGLES DU STATIONNEMENT standard. Pour voir les photos avec des informations sur ce stationnement, allez sur le site web xxx.

Sur la page Web indiquée, les visiteurs ont reçu présentés des photos d'autres pécheurs de stationnement interdit, mais pas la leur. Pour le trouver, il convient d'abord de télécharger et d'installer une barre d'outils d'Images de recherche. Cette page Web, installe essentiellement une DLL de logiciel malveillant invisiblement dans le système qui s'établit comme Internet Explorer Helper Object (BHO). Par cette connexion, un autre fichier DLL sera téléchargé, dont la pertinence comme logiciels malveillants est déjà connue. Elle est également considérée comme un BHO et ouvre après un certain temps, une fenêtre jaillissante (pop-up) avec un faux message de sécurité. Cette fenêtre voudrait que l'utilisateur fasse en sorte d'installer un programme "Rogue scanneur Anti-Spyware" - c'est-à-dire un soi-disant programme de protection contre les logiciels espions qui en réalité ne n'en est pas un, et la même chose, seulement télécharger plus de logiciels malveillants afin d'effectuer sur le système plus de manipulations.

Ingénierie sociale (sécurité de l'information): Contacts avec les "victimes" également hors ligne. Ceci est un bon exemple de l'ingénierie sociale des auteurs de malware. Également hors ligne, les utilisateurs sont confrontés avec des logiciels nuisibles sans failles de sécurité dans le navigateur ou sans que des voies d'infection complexes soient utilisées.

Christian Mairoll, gérant d'Emsi Software: "Avec des logiciels malveillants, qui ici sont utilisés, il y a des programmes de protection comme notre a-squared Anti-Malware 4 qui gère de façon intelligible ce genre de problème. Surprenant et choquant pour nous, est que la Mafia en ligne entre-temps a trouvé de nouvelles voies, et parfois, avec des moyens très coûteux, soient arrivés à berner des utilisateurs, sans que ceux-ci s'en doutent. Le truc avec les fausses contraventions aux États-Unis a entre-temps déjà, été utilisé plusieurs fois. La leçon retenue c'est que, en tant que citoyen, l'on devient encore



Communiqué de presse – libre à la publication immédiate

plus méfiant lorsqu'une adresse Web est à utiliser. Chez nous, en Europe : aucun policier qui vous verbalisera, ne vous demandera s'il vous plaît d'aller visiter un site web pour voir des photos du délit. Ceci est une blague.

a-squared Free 4.0 est disponible pour les particuliers sans frais d'utilisation. Ce Programme fonctionne sous Windows XP, 2003/2008 Server et Vista. Il ne fonctionne plus sous Windows 98, ME et 2000. Le grand frère a-squared Anti-Malware 4.0 coûte 29,90 Euro pour 1 année. L'analyse des comportements d'a-squared Anti-Malware signale par ailleurs activement l'installation de Browser Helper Objects (BHOs) nuisibles.

Site d'Emsi Software: <http://www.emsisoft.fr/>

a-squared Free 4.0: <http://www.emsisoft.fr/fr/software/free/>

a-squared Anti-Malware 4.0: <http://www.emsisoft.fr/fr/software/antimalware/>

SANS Internet Storm Center sur ce thème: <http://isc.sans.org/diary.html?storyid=5797>

À PROPOS EMSI SOFTWARE

Emsi Software est une société privée ayant son siège en Autriche. Le bilan de l'entreprise croît positivement et rapidement depuis sa création en 2003, et sans capital emprunté. L'objectif d'Emsi Software est d'être l'un des principaux fournisseurs européens dans la technologie de l'analyse comportementale, pour étudier les logiciels, notamment les logiciels malveillants.

L'entreprise a été fondée en 2003 par Christian Mairoll, qui avec sa vision d'une société virtuelle et l'a mise en pratique : Les 15 collaborateurs de la société sont disséminés dans le monde entier, mais travaillent ensemble sur l'Internet, comme s'ils étaient assis côte à côte dans un bureau réel. Pour les visions techniques, Georg Wicherski s'en occupe, Georg, en tant que co-fondateur du "Nepenthes" du projet Honeypot, ainsi que de la mwcollect Alliance (fusion de réseaux d'Honeypot pour la capture automatique de logiciels nuisibles de l'Internet) il jouit d'une grande réputation dans le secteur de la sécurité. Dans la gamme, des produits, d'Emsi Software, appartiennent les programmes de sécurité comme a-squared Anti-Malware, a-squared Free, a-squared HiJackFree, a-squared Anti-Dialer et depuis la fin de 2007 notre nouveau programme, Mamutu "Behavior Blocker"

Contact pour la presse

Thomas Günther

PR-Manager

Mail: tg@emsisoft.com

Fon: +43 664 344 60 68

Fax: +43 6235 200 53