



Press release – Released for immediate publication

## **Emsi Software issues a warning: Illegal parking triggers a new virus attack!**

**Emsi Software, provider of the a-squared Anti-Malware 4.0 protection software, warns of a new type of virus attack that, up to now, has only been used in the USA. In this case, after returning from shopping, drivers find a parking ticket on their windscreen. The drivers are then supposed to fetch the details of the illegal parking, and the penalties incurred, from a particular website. Drivers who actually follow the printed link are then promptly attacked and receive new Malware on their PCs.**

**Salzburg, February 2009** - Many visitors at a shopping mall in Grand Forks (ND), USA, were astounded as they returned fully loaded with shopping bags to their cars. A parking ticket was placed under their windscreen wipers. Written on the ticket was:

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

This gave the following impression: The car was illegally parked. The driver was then supposed to use the Internet to visit a specific website and obtain a photo of the parking violation and more information on the penalties.

At the specified website, the visitors could see photos of other parking violators but not themselves. To find their own photo, they were asked to download and install a "picture search" toolbar. However, this invisibly installed a Malware DLL in the system that functioned as an Internet Explorer Browser Helper Object (BHO). This connection was then used to download another DLL, already identifiable as Malware. This was then also installed as a BHO and, after a while, opened a popup window containing a bogus security warning. This attempted to motivate the user to install a so-called rogue anti-Spyware scanner, which is actually a bogus protection program that makes further Malware modifications to the system.

### **Social Engineering: The "victims" are now being contacted offline**

This is a good example of social engineering by Malware authors. Users are now being confronted with damaging software offline, without requiring the use of security holes in the browser or other complicated infection vectors.

Christian Mairoll, the General Manager of Emsi Software, says: "Protection software such as our a-squared Anti-Malware 4 has no problem dealing with the Malware used here. The most surprising and shocking aspect of this to us is that the online Mafia are resorting to completely new and involved ways of tricking unsuspecting users. The trick with forged parking tickets has now been used several times in the USA. The lesson to be learned from this is that all citizens must exercise a healthy skepticism when a web address is to be used. In Germany, the following applies: A policeman never requests the recipient of a parking ticket to visit any kind of homepage. This is complete rubbish."

a-squared Free 4.0 can be used free of charge by private users. The program runs under Windows XP, 2003/2008 Server and Vista. It no longer runs under Windows 98, ME and 2000. Its big brother a-squared Anti-Malware 4.0 costs US \$39.90 per year. The behavior



Press release – Released for immediate publication

analysis feature of a-squared Anti-Malware also detects and signals the installation of damaging Browser Helper Objects (BHOs).

**Emsi Software Homepage:** <http://www.emsisoft.com/>

**a-squared Free 4.0:** <http://www.emsisoft.com/en/software/free/>

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

**SANS Internet Storm Center on this topic:** <http://isc.sans.org/diary.html?storyid=5797>

## ABOUT EMSI SOFTWARE

Emsi Software is a private company based in Austria. The rapidly growing company is a leading European supplier of behavioral analysis technology for analysis of software, especially Malware.

The company was founded in 2003 by Christian Mairoll, realizing his vision of a virtual company: The 15 company employees are distributed all over the world but work together as if they are sitting together in a real office. The technical vision is implemented by Georg Wicherski, who enjoys a high level of respect in the security sector as a co-founder of the "Nepenthes" Honeypot project and the mwcollect Alliance (an amalgamation of Honeypot networks for automated trapping of malignant software from the Internet).

The Emsi Software product range comprises the security programs a-squared Anti-Malware, a-squared Free, a-squared HiJackFree, a-squared Anti-Dialer and, since the end of 2007, Mamutu.

## PRESS CONTACT

Thomas Günther

PR Manager

E-mail: [tg@emsisoft.com](mailto:tg@emsisoft.com)

Ph: +43 664 344 60 68

Fax: +43 6235 200 53