



Press release – For immediate release

## Malware discussion in the IT Sector: Does it make sense to clean infected PCs?

**Emsi Software, a provider of security software such as a-squared Malware 4.0, takes up a current discussion topic in the IT security sector: Does it really make sense to clean a computer infected with damaging software? Can the user ever really trust such a system again? To clarify these questions, the technical feasibility of full cleaning must be examined.**

With even the simplest problems in their PCs, many users immediately suspect a Virus. The printer is not working? Must be a Virus! The Internet connection is ponderous? A Spyware program must be sending personal user data to a country that cannot be found in a European atlas!

Most users have little or no knowledge of the structure of damaging software, how it works or what it can do to the PC. They simply install a protection program and abdicate all responsibility to this program. The IT Security Sector is not happy with this level of protection and is currently asking itself the very provocative question: Is it really worth the effort to clean an infected computer?

In plain text, this means that damaging software is not so harmless that the PC user can simply ignore it. The current question revolves around the issue of whether modern protection programs are truly capable of fully cleaning an infected system, or if it is better to completely re-install the system. To make this decision, one must delve somewhat deeper into the material.

### **Basic knowledge: How do Viruses, Trojans and Spyware tools work?**

Viruses need other host applications in order to function. A Virus appends itself to a "benign" program by inserting its own Virus code into an existing executable file. The Virus only becomes active and infects other programs when the benign program is executed.

The major threat in the stampede to infect your hard drive is now represented by **Trojans, Backdoors, Bots and Worms**.

**Trojans and Bots** are independent programs that hide in the depths of the system and attempt to attract as little attention as possible. They exist to provide an external hacker with a back door into the PC, thus allowing the hacker full control over the PC – for example, for secretly mass mailing Spam. Trojans and Bots are only dangerous when they are loaded in RAM. They therefore use various Autostart functions to ensure that they are always started every time the system boots.

**Spyware, Adware, and bogus Security Software:** Spyware programs secretly monitor the user and record (e.g.) online banking activity and the associated access data and then pass this on to the online Mafia. These spy programs are becoming cleverer and cleverer. Sometimes they start multiple active processes that monitor each other. When one of these processes is terminated, it is started again by one of the other processes. Bogus security programs pretend to hunt damaging software, although this is exactly what they are. Some of them inject themselves into essential system processes such as (e.g.)



Press release – For immediate release

winlogon.exe. The system then crashes when an attempt is made to remove the damaging program.

**Rootkits** are the most dangerous of all. These damaging programs manipulate the operating system to such an extent that they are no longer visible in the file manager or process manager. Anti-virus programs can then no longer detect these Rootkits. They are even capable of hiding Registry entries, open ports and active processes.

### **Disinfection: Cleaning is sometimes problematic**

Once damaging software has gained access to your computer and is active, the question must be asked as to whether it can be completely removed without leaving any traces or remnants.

Great: With simple Malware it is possible to completely remove the damaging software from the system with a relatively high level of reliability. With Viruses, the easiest method is to simply delete the infected files. This may mean that the infected programs can no longer run properly. No problem: These can be easily re-installed. With Trojans, it is enough to kill the active processes, delete the Autostart entries and delete the executable Trojan files. Classical Spyware programs can simply be uninstalled. From this point of view, it seems that you too can restore your system back to its original condition when an infection is found.

This is not the case with the latest Spyware programs and bogus Anti-virus programs. These dig themselves so deeply into the system that special tools are needed to delete these files before the system boots. These infections are very difficult to completely overcome. This also applies to Rootkits, which have almost perfect camouflage properties. A user can never really be sure whether all Rootkits on his or her PC have been found. Given this fact, can he or she also be sure that a Rootkit has been completely removed? Hackers are constantly finding new ways of hiding their damaging software.

Often enough, a piece of Malware can be removed but the changes it has made to the system remain. For example, ports may have been opened that still allow a Hacker access to the system from an external source.

### **Once the PC is infected: Install the system from scratch!**

Emsi Software in Austria provides protection software for Windows PCs. General Manager Christian Mairoll: "In our experience, especially Rootkits and bogus Anti-virus programs cannot be removed from infected computers with absolute certainty. We therefore recommend all our customers to make a backup image of the entire partition after the initial installation of all important programs on their computers. In the case of an infection, this can then be copied back onto a freshly formatted hard drive."

Despite all reservations, it is of course still important to install a protection program on your computer that can signal the presence of Malware as soon as it reaches your PC. The Emsi Software program **Mamutu 1.7** monitors your computer for suspicious behavior and can thus detect completely new damaging software that is currently unknown in the security sector.



Press release – For immediate release

**a-squared Free 4.0** is free of charge for private users (currently in beta-testing). This program scans the entire computer, detects existing infections and can immediately remove them.

In the premier league is the program **a-squared Malware 4.0**. It uses two background scanners to detect all types of Malware before they have a chance to dig themselves into the system. This is doubled real-time protection consisting of a Signature scanner and an additional behavior analysis module (Malware IDS). Several updates per day make sure that this weapon is always sharp. An annual software subscription costs € 29.95.

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

**Downloads:** <http://www.emsisoft.com/en/software/download/>

**On the sense and senselessness of Malware cleaning (knowledgebase article):**  
<http://www.emsisoft.com/en/kb/articles/tec081111/>

## ABOUT EMSI SOFTWARE

Emsi Software is a private company based in Austria. The rapidly growing company has had a positive balance since its foundation in 2003 without external investment. Emsi Software aims to be a leading European provider of behavior analysis technology for analyzing 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

Mail: [tg@emsisoft.com](mailto:tg@emsisoft.com)

Ph: +43 664 344 60 68

Fax: +43 6235 200 53