



Mamutu 2.0: Behavior Blocker plugs the virus scanner hole with behavior analysis!

Mamutu 2.0 is here. The Behavior Blocker enhances classical Virus and Malware scanners with an intelligent behavior-based program analysis system capable of detecting and disabling computer pests that are new and currently unknown. Even prying government tools can be detected using this method. The new version significantly reduces the number of false alerts and introduces a new alerting system.

Salzburg, July 2009 - The Online Mafia never sleeps. Their Viruses, Trojans and Spyware programs are becoming ever more clever and intelligent, with the aim of infiltrating the user's computer and accumulating passwords, bank account information and personal data. The classical Virus scanners and Anti-Spyware programs are often only signature based. This means that they manage a database of virtual fingerprints of the pests to be detected and discover these pests via a direct comparison of their program code.



This causes a problem that Mamutu (<http://www.mamutu.com/>) is able to solve: New pest programs are discovered every day. With classical scanners, the computer is unprotected from an attack by these new pests until their "fingerprints" are generated and loaded into the signature database. This is where the Mamutu "Behavior Blocker" service comes into play. The program performs an intelligent behavior analysis that monitors the activities performed by all programs on the computer. If any programs exhibit suspicious behavior then they are immediately frozen and an alert is raised. The user can then decide what is to be done.

Mamutu signals suspicious behavior when a program attempts to insert code into other programs, patches existing software, invisibly installs new programs in the background, starts Rootkit processes or installs new services and drivers. The Mamutu Malware Intrusion Detection System (Malware-IDS) is also triggered by the creation of Autostart entries and simulated mouse and keyboard activity.

Mamutu 2.0: Trigger the smallest possible number of alerts

Christian Mairoll, the General Manager of Emsi Software GmbH, says: "Our aim is to produce as few alerts as possible rather than as many as possible. In contrast to a typical HIPS (=Host Intrusion Protection System), which signals almost everything without analyzing the exact behavior, Mamutu only raises an alert when it is almost certain that a program presents a genuine danger."

Mamutu does not replace classical Virus scanners and Anti-Spyware programs but rather plugs the last remaining security gap. Mamutu thus works well together with all well-known protection programs. The low resource usage means that the performance of the computer does not suffer when using this additional guard system.



Christian Mairoll says: "Strange but true: Those who fear that their Anti-virus program opens a secret back door for government Spyware can close this door with Mamutu. The Behavior Blocker cannot determine the origin of detected Spyware because it does not use a signature database. It therefore signals all damaging behavior, regardless of whether this is caused legally or illegally."

Mamutu 2.0: The latest new features!

The new Version 2.0 of Mamutu has two major new features. There are now fewer false alerts and the alert window has been redesigned.

- **Reduced false alerts:** Mamutu uses numerous different filtering systems to avoid false alerts. Among these are an own Internet community (Cloud Technology), a technical file analysis filter and a certificate check. The last filter recognizes signed programs from trusted suppliers that cannot be manipulated.

- **Redesigned alert window:** All triggered alerts are now divided into two categories. Red alerts are indicated via a dialog window with a red border. These indicate very suspicious behavior that most probably results from some sort of Malware (Backdoors, Worms, Keyloggers, Viruses, Rootkits and Dialers etc.). Orange alerts are more informative in nature and indicate program activity that the user should know about and approve via a mouse click. This includes changes to the Autorun or Browser settings, installation of new drivers and system services, or hidden installation of new programs.

Mamutu 2.0 runs under Windows 2000, XP, 2003 Server and Vista. A free 30-day test version (4 MB) allows you to try the program on your own computer. The full version ("Personal") costs € 20.

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

Mamutu 2.0: <http://www.mamutu.com/>

Download: <http://www.mamutu.com/en/software/download/>

Shop: <http://www.mamutu.com/en/order/mamutu/>



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. Emsi Software was commended with the Austrian "Constantinus" IT prize in 2005 for this innovative business management concept.

The Emsi Software product range comprises the security programs a-squared Anti-Malware, a-squared Free, a-squared HiJackFree, a-squared Anti-Dialer, Mamutu and, since the start of 2009, the Online Armor Personal Firewall.

PRESS CONTACT

Thomas Günther

PR Manager

E-mail: tg@emsisoft.com

Ph: +49 180 590066 3

Fax: +43 6235 20053