Anti-Virus Comparative

Proactive test

Kaspersky Internet Security 8.0

Date: June 2008

Last revision: 1st June 2008

Website: http://www.av-comparatives.org

1. Tested product

KasperskyLab (www.kaspersky.com) will soon release Kaspersky Internet Security 2009 (v8). This new version includes a further improved heuristic analyzer (emulator) and detection of suspicious packers, as well as the AVZ-heuristics at HIPS level. Kaspersky Internet Security v8 with signature updates of the 4th February 2008 and with highest settings was tested. The used test-set is the same as the one used for the retrospective test of May 2008 (http://www.av-comparatives.org/seiten/ergebnisse/report18.pdf). In the retrospective test of May 2008, **KAV v7** detected **~21%** and got a **"STANDARD"** rating (probably because it was a product targeted by malware authors).

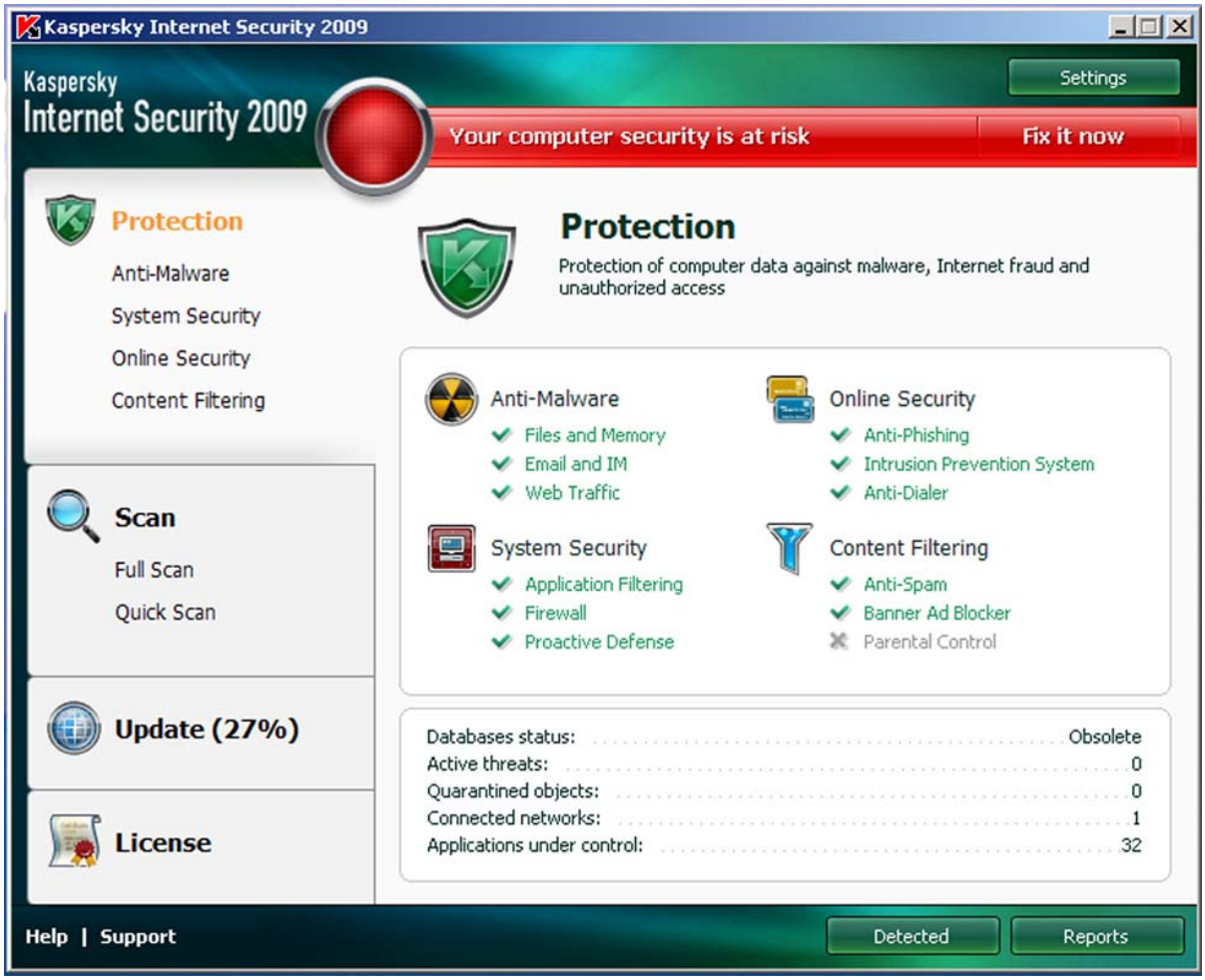
2. Test results

Below the proactive detection rates of KIS 8.0:

KIS v8 with maximum emulator settings: ~42%

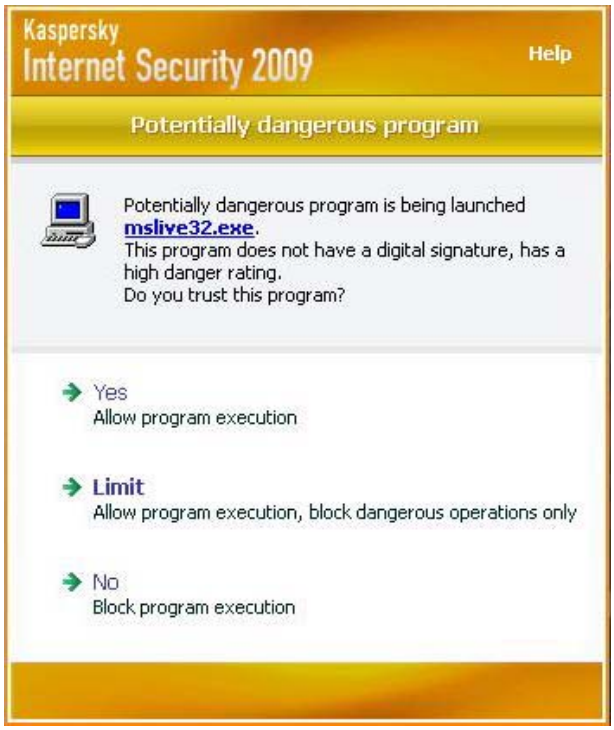
KIS v8 with emulator settings like in HIPS: ~49%

With a total **on-demand detection rate of ~42%**[1] in the retrospective test and a **very low rate of false alarms**, **Kaspersky Internet Security version 8.0** would in our retrospective test have reached the **"ADVANCED"** certification level.

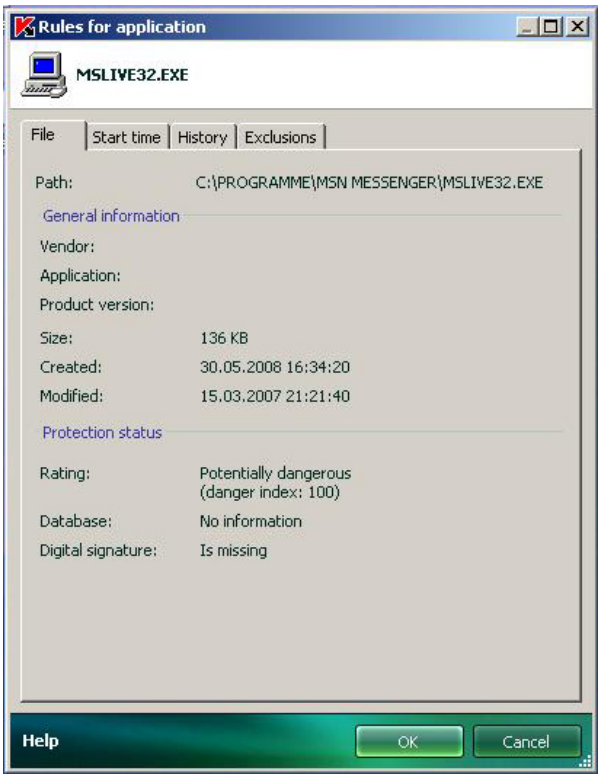


[1] *this is a very similar result to the November 2007 retrospective test of Kaspersky Anti-Virus 7.0*

When the malware is executed, the **current HIPS** (Application control) included in Kaspersky Internet Security v8 **would automatically block** (or strongly recommend to block) **around 68%** of the samples from the retrospective test-set, which is a good score.
Kaspersky v6 and v7 had the Proactive Defense Module (PDM) to stop malicious samples based on patterns of "bad behaviour".



The new v8 includes a HIPS module to put some restrictions on applications execution. When a potentially dangerous program is being launched, KIS v8 will recommend to block the program execution – it is also possible to limit the program execution, by blocking the dangerous operations. Classic HIPS-solutions usually require huge knowledge and time from the user to configure them properly (and have usually a high level of false alarms at the beginning), KasperskyLab has circumvented the false alarms problem by combining the power of the now included AVZ-engine scripts and the Emulator to the classic HIPS-approach: a heuristically determined danger rating.



Based on this rating KIS v8 assigns a security group to any new running application and for all the four groups a predefined vector of privileges which cover all potentially dangerous actions exists.
E.g. samples with a danger index of 100 get blocked automatically. So, about 2/3 of the samples used in the retrospective test were blocked automatically during first execution.
The rules for the security rating calculation (the AVZ-engine scripts) are updatable – in fact they will be updated/improved during next weeks.

For more information about Kaspersky Internet Security 2009, please visit http://www.kaspersky.com

3. Copyright and Disclaimer

Andreas Clementi, AV-Comparatives (June 2008)