KASPERSKY lab

KASPERSKY LAB'S SYSTEM WATCHER OVERVIEW

Kaspersky System Watcher

Today's computer systems are better than ever at multitasking. They can run numerous programs at the same time, each of these programs having a specific purpose and set of privileges in the system.

The purpose of security solutions is to block the activity of those programs which have destructive functionality, such as infecting other files or making undesirable changes to the system registry. The usual method of identifying such programs is based on detecting unique code signatures which define previously identified malicious programs. However, using only signature-based detection methods no longer provides effective protection from malware and ransomware as new variants of ransomware for which there are no known signatures for appear every day.

An effective method of combating such programs is based on analyzing the behaviour of applications in the system and detecting activity that is typical of malicious software. However, data collected separately on each individual program is fragmentary and does not add up to an accurate and complete description of all the events taking place in the computer system.

Monitoring system events is the recipe for success

System event monitoring is provided as standard in Kaspersky security solutions. The technology provides the fullest possible information about the system as a whole, thereby enabling maximum control of malicious activity and, if necessary, recovery of the computer's normal operating parameters.

System event monitoring tracks all the important events that take place in the system, such as changes to operating system files and configurations, program execution and data exchange over the network, etc. Events are recorded and analyzed and if there is evidence that a program is performing operations typical of a piece of malicious software, they can be blocked and rolled back, preventing further infection. The computer system is rolled back to its last recorded secure state as accurately as possible.

System event monitoring is versatile: it is effective against any software that displays signs of performing destructive activity in the system. This means that it can be used to reliably detect new hostile programs for which signatures are not as yet available.

Kaspersky System Watcher: even higher level of protection

Kaspersky Lab's security products have always been based on advanced, cutting-edge technologies for combating threats. Basic system event monitoring functionality was first introduced in Kaspersky Internet Security 2010 and is standard in all versions of the company's security products including Kaspersky Enterprise Security for Business and this functionality has further evolved, becoming the Kaspersky System Watcher.

The Kaspersky System Watcher collects the most relevant system event data. The monitor tracks information on file creation and modification, changes made to the system registry, system calls and data transfers over the network. The data collection process is automated and does not require user interaction.

Using the BSS (Behaviour Stream Signatures) module, the System Watcher can independently make decisions as to whether a program is malicious based on the data collected. In addition, the latest versions of Kaspersky Lab's security products include a mechanism whereby the module continually exchanges information with other components – the Proactive Defense module, the Network Attack Blocker, the web antivirus module and the firewall. As a result, Kaspersky Internet Security and Kaspersky Anti-Virus provide better overall detection of malware and security policy breaches and are better at identifying the sequences of events leading to such incidents. System

Watcher also monitors legitimate, but potentially vulnerable applications in order to defend the system against exploits, using special Automatic Exploit Prevention technology.

The Kaspersky System Watcher is fully updateable: event lists and event monitoring mechanisms, as well as heuristics, can all be updated. This provides flexibility and speed in adapting to ever changing threats and computer system configurations. System Watcher updates are downloaded as part of regular antivirus database updates without requiring user interaction or taking up any of the user's time.

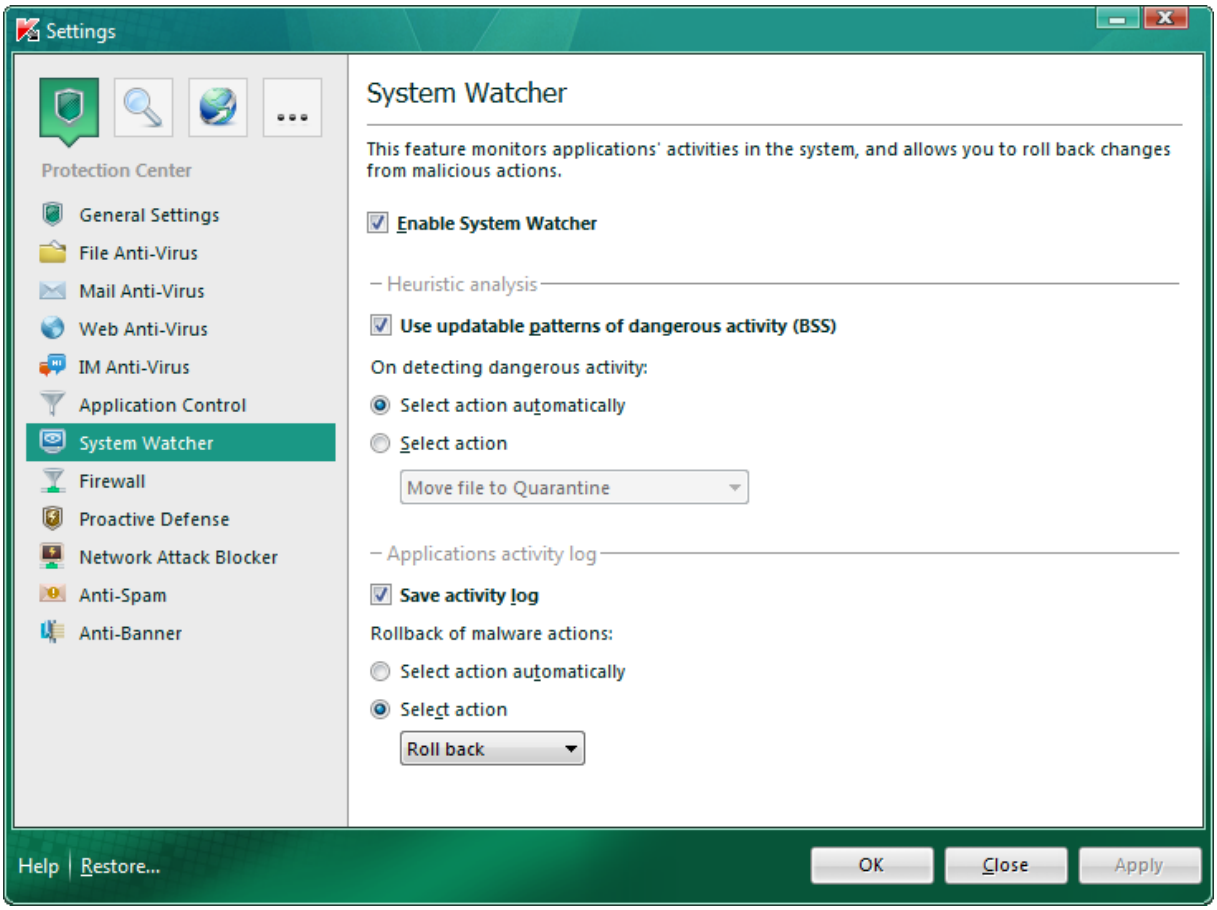


Figure 1: System Watcher settings are available in the Settings menu

Threat detection

Decisions as to whether a program is malicious or not are made using the built-in BSS (Behaviour Stream Signatures) module. The module compares each program's real-life behaviour with malware behaviour models. The module analyzes program behaviour and issues verdicts in real time.

In addition to using standard detection methods, the latest versions of Kaspersky Internet Security and Kaspersky Anti-Virus provide heuristic BSS-based detections which indicate that a program's behaviour is similar to, but may not necessarily be that of malware.

The user can choose between a fully automatic mode and an interactive mode. In the interactive mode, the user has a wider choice of actions.

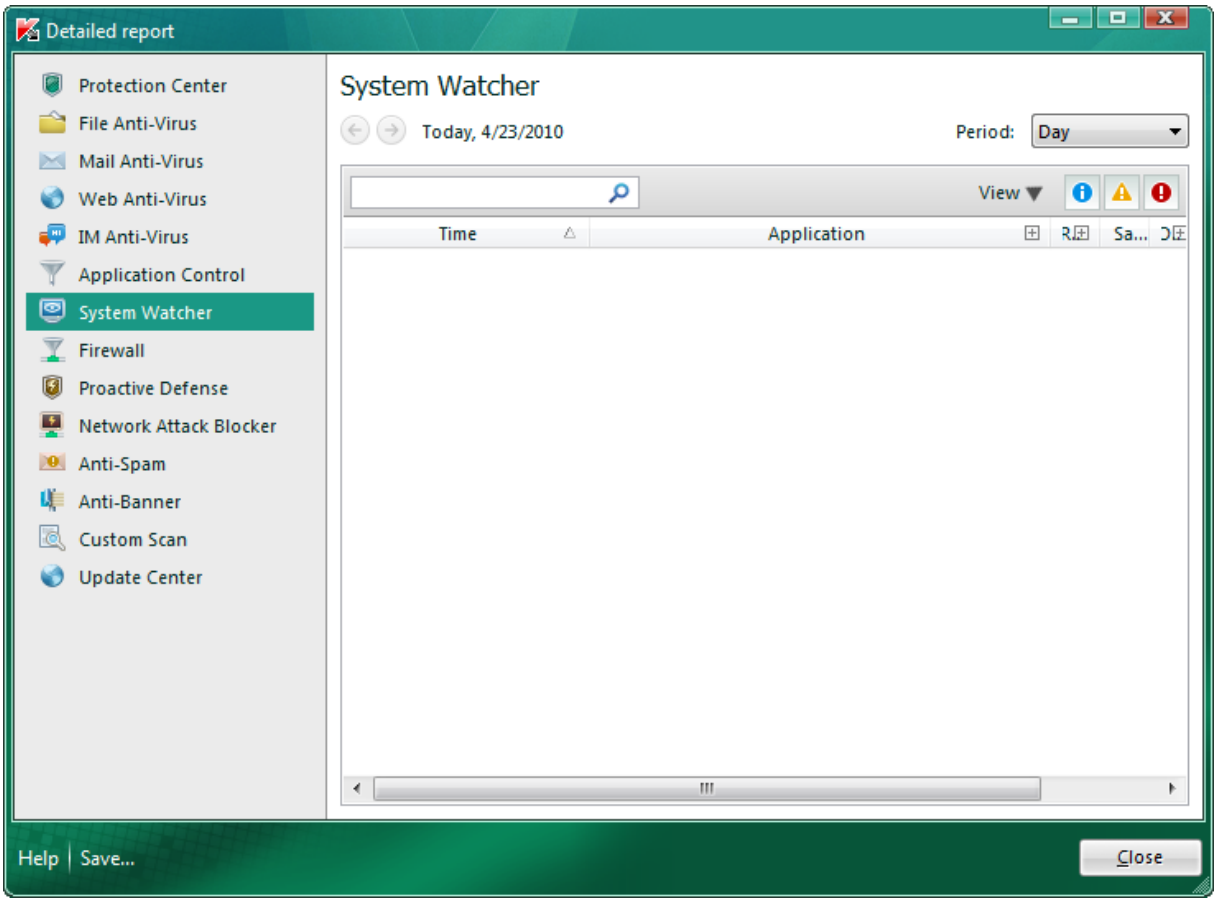


Figure 2. Reports on the actions performed by the System Watcher can be viewed in the Detailed report window, which opens by pressing the Reports link in the main window and then the Detailed report button.

The System Watcher Investigator subsystem

Users who make their own decisions regarding the handling of suspicious programs can get the necessary information from the System Watcher Investigator subsystem, which reconstructs the logical sequence of events leading to an incident and presents the data to the user. Information that the feature is able to provide can include a description of how the suspicious object appeared in the system, which operations the object performed on other files, which system functions it called, which processes it launched, etc.

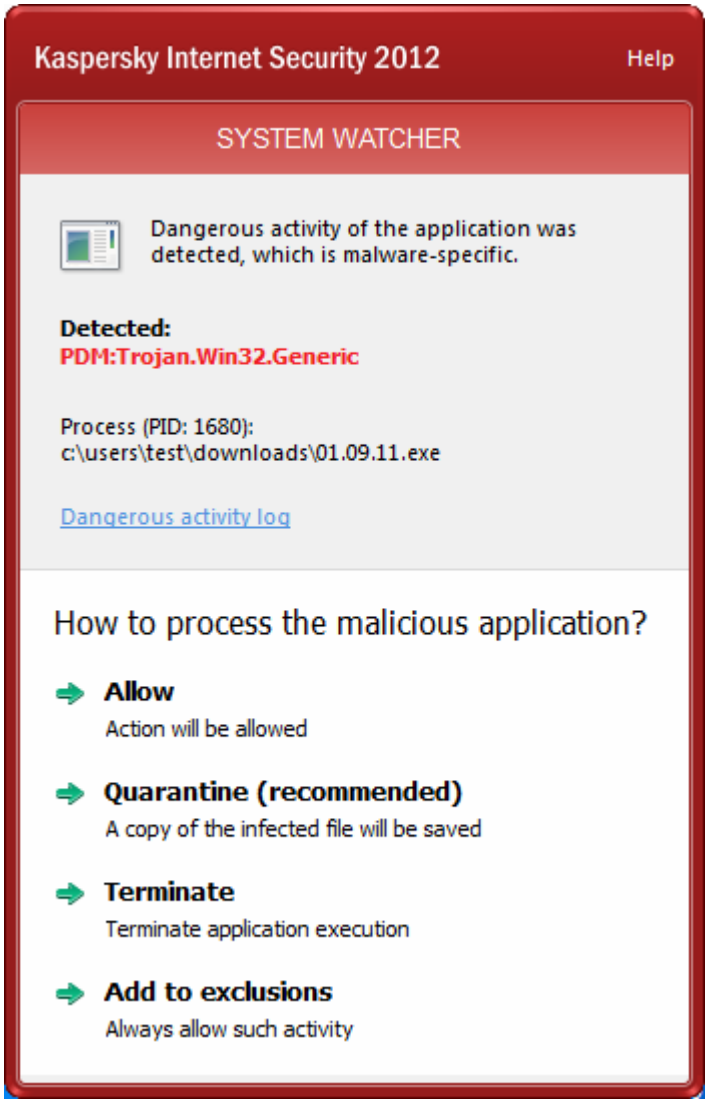
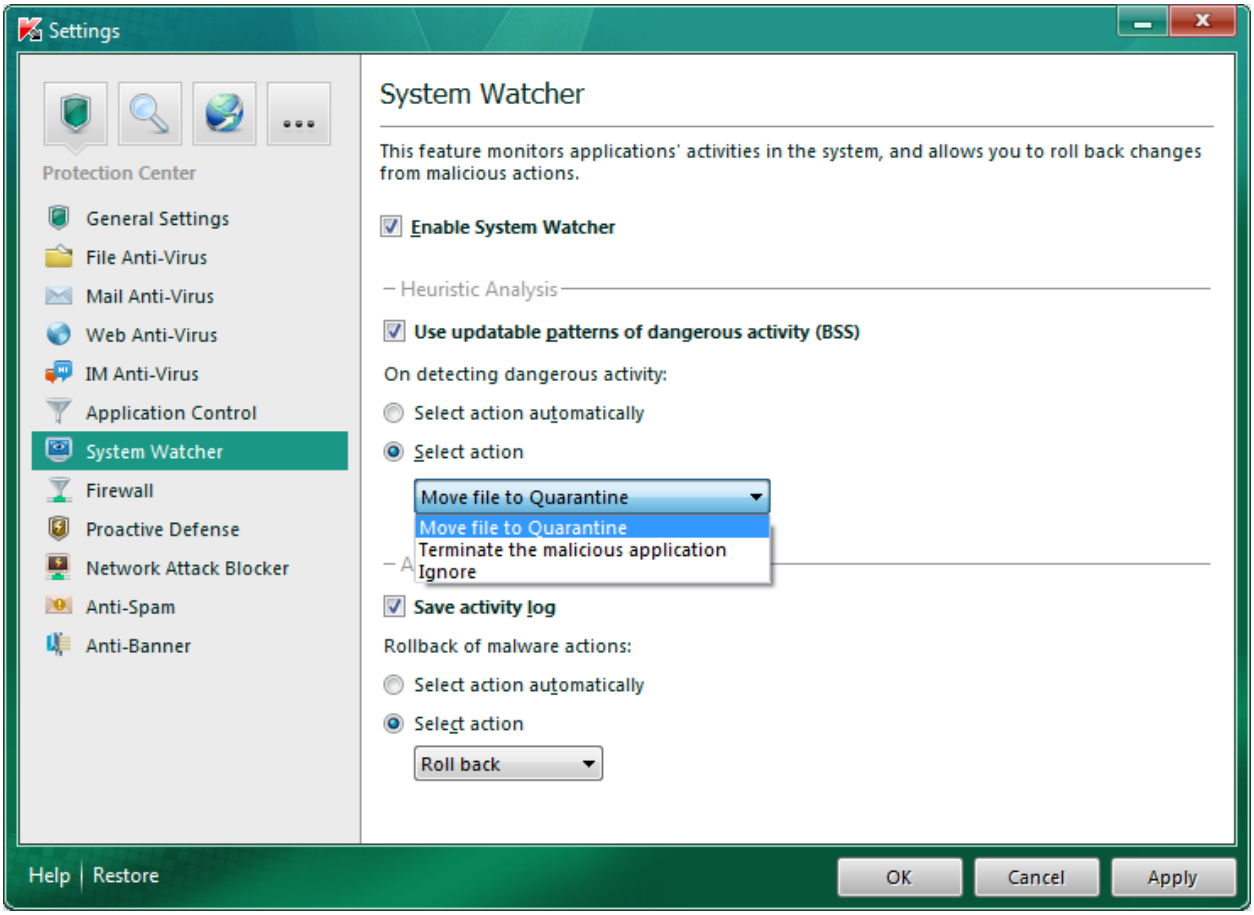
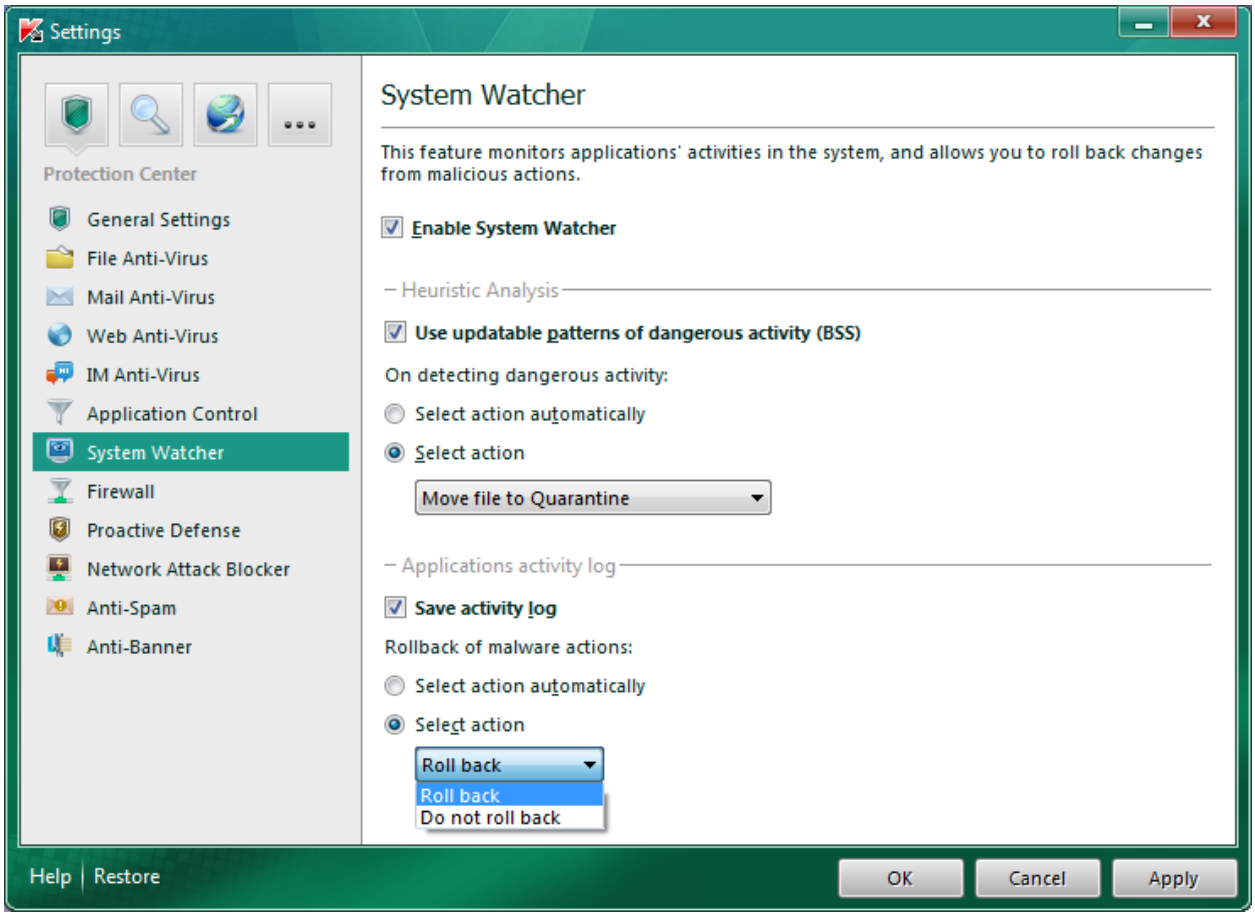


Figure 3. The System Watcher Investigator subsystem allows experienced users to make well-informed decisions related to handling suspicious programs by activating the 'Dangerous activity history' function and viewing the main operations performed by the suspicious program which led to the detection.

Rolling back unwanted changes in the system

Upon detecting an infection, the System Watcher initiates a roll-back with the computer system returning to its former safe parameters.





Summary

Kaspersky System Watcher monitors all of the important system activities of the computer network that it is installed on providing for malicious program detection and appropriate action.

This approach is capable of blocking the destructive actions of any program, regardless of whether a signature is available for its code or not. It provides high detection rates with few false positives, since destructive behaviour is the most reliable characteristic of a malicious program.

Continual and detailed monitoring of the computer system provides for very accurate rolling-back of malware activity. It also ensures a more reliable assessment of the computer's overall security level, which allows for more accurate diagnoses to be made about the states and processes that are anomalous from the security viewpoint.

The threat landscape is constantly developing, and Kaspersky Lab is committed to keeping pace with every new threat generation, providing multi-layered security to protect businesses. Ransomware threats are mitigated on both workstations and servers and Kaspersky Labs constantly renews its arsenal of technologies powered by proven security intelligence.

Proof of performance can be seen through independent test results and the views of analytical agencies. In 2015 Kaspersky Lab products participated in 94 independent tests and reviews and were awarded 60 firsts and achieved 77 Top-three finishes.