KASPERSKY lab

Preventing emerging threats with Kaspersky System Watcher

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

The purpose of security solutions is to block the activity of any program which has destructive functionality, such as infecting other files or making undesirable changes to the system registry. The 'classic' method of identifying such programs is based on detecting unique code signatures which define previously identified malicious programs. This process is known as signature-based detection. However, using only signature-based methods no longer provides effective protection against malware – according to Kaspersky Lab internal data, about 315,000 new samples of malware appear "in the wild" every day and for many of them there are currently no signatures.

There is an effective method of combating such programs by analyzing the behavior of applications in the system and detecting activity that is typical of malicious software. However, data collected separately on each individual program is fragmented and does not deliver 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 a new stage in the development of 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: 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 indicative of a piece of malicious software, those operations can be blocked and rolled back, preventing further infection.

System event monitoring is versatile: it is effective against any software that displays signs of destructive activity in the system. This means that it can be used to reliably detect new hostile programs for which signatures have yet to become available.

Kaspersky System Watcher: an 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 has been available in the company's consumer solutions since 2009. Subsequently this functionality has further evolved, becoming Kaspersky System Watcher.

Kaspersky System Watcher scans the most relevant system event data. The monitor tracks information about the creation and modification of files, the work of system services, any changes made to the system registry, system calls and data transfers over the network. System Watcher also processes information about operations with symbolic links containing references to files or directories, modifications of the master boot record where the loader for the installed operating system is stored and interception of OS reboots. Moreover, it analyses the contents of the packets transmitted via TCP, the main Internet transport layer protocol, in search of any evidence of criminal activity. The data collection process is automated and does not require user interaction.

Using the BSS (Behavior Stream Signatures) module, System Watcher can independently make decisions as to whether a program is malicious based on the data it analyzes. In addition, Kaspersky Lab's security products include a mechanism whereby the module continually exchanges information with other components – the web antivirus module, the IM Antivirus, the Host Intrusion Prevention System and the firewall. As a result, the security solution delivers better overall detection of malware and security policy breaches, and is better at identifying the sequences of events which lead up to such incidents.

Kaspersky System Watcher can be fully updated: event lists and event monitoring mechanisms, as well as heuristics, can all be adjusted as needed. 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 any time or interaction from the user.

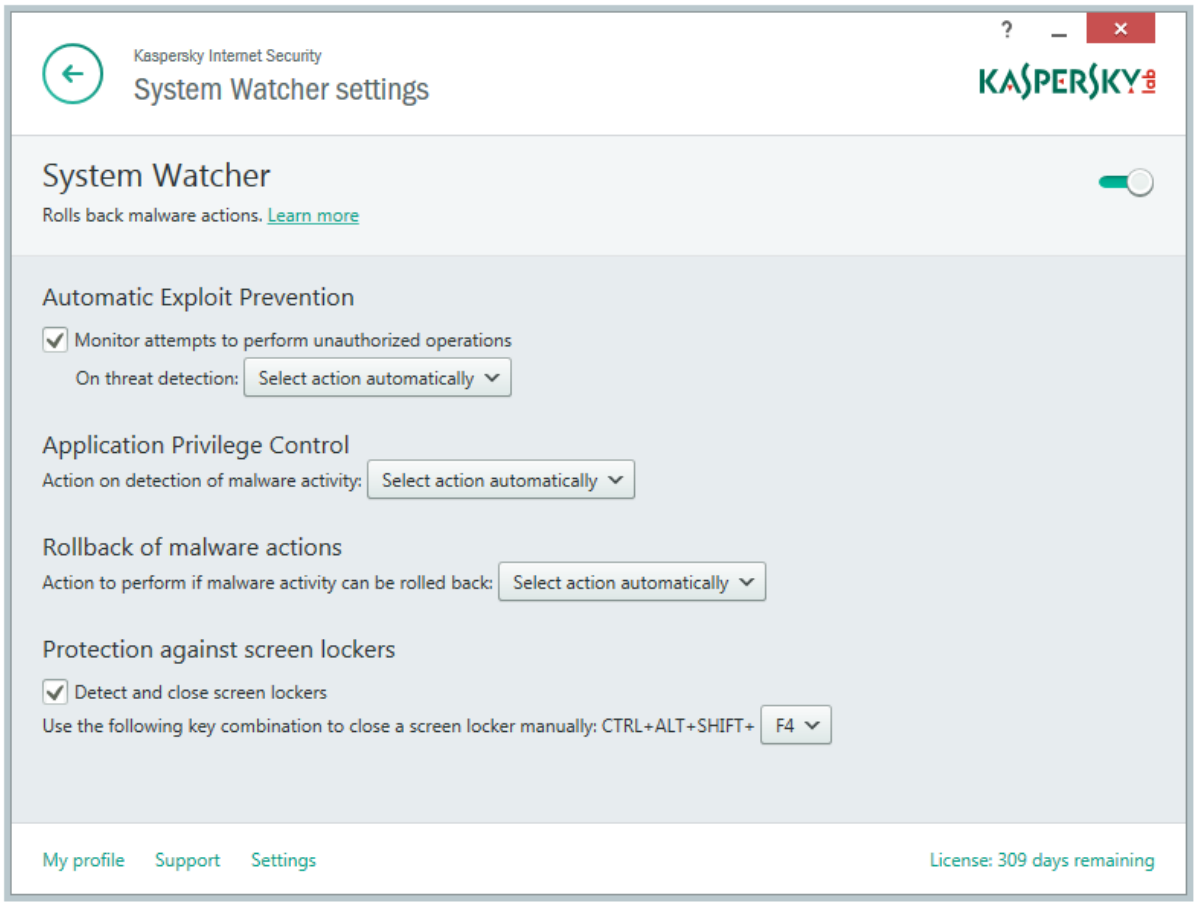

Figure 1. System Watcher settings are available in the Settings menu.

Threat detection

The built-in BSS module decides whether a program is malicious or not. The module compares each program's real-life behavior with models of typical malware behavior. The module analyzes program behavior and issues verdicts in real time. Kaspersky Lab's security solutions also provide so-called heuristic BSS-based detections which indicate that a program's behavior is similar to, but may not necessarily be, that of malware. In addition to using standard detection methods, System Watcher can identify potentially malicious actions. For example, if a trusted application runs unsafe code due to an exploit attack, the security product detects this action and advises blocking the suspicious activity.

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.

Cryptomalware countermeasures subsystem

The increasing spread of cryptomalware, which encrypts user data and demands a ransom for the decryption key, led to an urgent need for countermeasures, and the corresponding technology was implemented in the System Watcher. It negates the consequences of crypto-attacks by making local protected backup copies of user data files as soon as they are

opened by suspicious program. Therefore, there is no need to decrypt any affected data — it will be replaced from the backup copies.

Protection against Screen Lockers

Screen lockers are another type of ransomware, programs that try to block user access to computer functions with a supposedly immobile banner demanding a ransom. System Watcher has a built-in protection against this type of malware. In System Watcher's settings menu there is a corresponding entry that turns this function on and sets a key combination that will close the screen locker manually. Pressing this combination will get rid of the annoying banner and delete the malware that caused its appearance. This protection against screen lockers is enabled by default.

Automatic Exploit Prevention subsystem

Another part of the System Watcher is the Automatic Exploit Prevention module made to deal with malware that utilizes software vulnerabilities, even zero-day vulnerabilities. This module controls various applications, especially the most frequently targeted ones, and starts additional checks if they attempt to launch any suspicious code. Information gathered in this way helps to detect the actions of an exploit and block them. Additionally, Automatic Exploit Prevention uses Forced Address Space Layout Randomization technology that makes it difficult for exploits to locate their own malicious code in the memory and therefore prevents the use of vulnerabilities. Detailed information on this technology can be found in the AEP whitepaper.

Java applications control module

Protection against vulnerabilities in the Java platform has always been a critical security issue due to the popularity and opacity of the Java Virtual Machine environment, where every Java program is executed. To detect attacks via Java, System Watcher has a special module called Java2SW that has direct access to the platform and adds an extra element of security in every JVM. Java2SW analyzes the code from within and stops it running if any suspicious activity is detected.

Rolling back unwanted changes in the system

Upon detecting an infection, System Watcher initiates a roll-back (i.e. a return of the computer system to its previous, safe parameters). The roll-back system works with created and modified executable files, MBR modifications, important Windows files and registry keys. In the latest versions of Kaspersky Lab's security products, the roll-back mechanisms can be updated.

Availability

System Watcher technology is integrated into products for home users and business:

For home users

- Kaspersky Internet Security
- Kaspersky Internet Security – Multi-Device
- Kaspersky PURE
- Kaspersky Anti-Virus

For business

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security

Conclusion

Computer system monitoring and its implementation – via Kaspersky System Watcher – is another approach to protection. All important system activities are monitored and malicious programs are detected based on the monitoring data.

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 behavior is the most reliable characteristic of a malicious program.

Continual and detailed monitoring of the computer system allows for a very accurate roll-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.