About

This function displays information about the software such as the version and the last update date.

Information about new updates is available at www.viruskeeper.com
in the Update section.

Alert : Spyware detected

Spyware has been detected on your computer.

Spyware is a program installed on your computer without your permission by a web site or software.

VirusKeeper boasts two spyware detection systems:
- scanning for known spyware
- monitoring spyware-like activity

The current alert indicates that your computer is really infected with spyware.
It is strongly recommended to remove it by clicking the “Clean” button.

To ignore this alert, click the “Ignore” button.

Alert : Suspicious running program

A suspicious program has been detected in memory.
This program is probably a virus or spyware.

Detailed information (filename, location, size and characteristics) about this program is available in the ProcessWatch tab.

Click the “Stop” button to prevent this program from running.

Analysis

Immediate Behavioral Analysis
VirusKeeper is based on a real-time threat analysis engine.
As soon as VirusKeeper is activated, it permanently protects your computer without requiring user intervention. It alerts the user when a dangerous program is detected.

The behavioral analysis function permits VirusKeeper's analysis engine to make a thorough and immediate check of the computer. This kind of analysis, based on behavior rather than signatures, is very fast.

Use this function when you have doubts about your PC's behavior and you think spyware or a virus might be active.

Antivirus File Analysis (VirusKeeper Pro only)
You can complement the behavioral analysis by a classic antivirus file scan. The VirusKeeper Scanner module scans files using signature analysis.

Antispyware Analysis (VirusKeeper Pro only)
VirusKeeper Pro comes with the VirusKeeper Spyware Scanner module, whose thorough antispyware scan analyzes files and the registry.

Event log

The event log stores all alerts that VirusKeeper records on your computer.

Each line of the event log contains:

- the date of the alert
- the type of the alert
- the program that caused the alert
- the action performed by the user

Use the “Clear” button to clear the event log.

File Alert

A new file has appeared in the Windows system directory.

This action is typical of viruses and spywares.

You should, however, ignore the alert if:
- you have just installed new software
- you have just updated software
- you have just installed a new device (modem, video card, scanner, printer, etc)
- you have just updated a device driver

If one of these is the case, click the “Ignore” button.

Otherwise, this new file might be a virus. Click the “Quarantine” button to quarantine the file.

Quarantined files are stored in the /quarantaine folder of VirusKeeper.

Help

This tab displays the following items:

- Help
- About box: version, copyright
- Ask an expert about removing a virus

Ignore list : friend programs

The ignore list allows the user to define items to be ignored by the VirusKeeper monitor.
Programs in the ignore list are considered safe by VirusKeeper and are not monitored.

When do you need to add an item (program / component) to the ignore list ?
In some rare cases, VirusKeeper can display an alert for a harmless program that has characteristics similar to those of a virus.
To avoid recurring false alerts about this program, the user should add it the ignore list.

Internet Explorer Alert: page change

Microsoft Internet Explorer is the major web navigator in the world.
It is also a target for spyware and pop ups.

Some programs and web sites add components, like web toolbars, to Internet Explorer that can be used to show unwanted web sites and advertising pop-ups.
Some programs record and transmit your browsing habits.

This alert occurs when one of Internet Explorer's default pages (like its search or home page) is changed.
If you have changed these pages yourself, ignore this alert and click the "Ignore" button.
Otherwise, click the "Restore" button to restore the previous pages.

Internet Explorer Alert: Third-party component added

Microsoft Internet Explorer is the major web navigator in the world.
It is also a target for spyware and pop ups.

Some programs and web sites add components, like web toolbars, to Internet Explorer that can be used to show unwanted web sites and advertising pop-ups.
Some programs record and transmit your browsing habits.

The new component alert occurs when a new component is added to Internet Explorer.

If you have just installed new software or drivers, ignore this alert by clicking the “Ignore” button.

Otherwise, click the “Remove” button to get of this new component.

Introduction

Welcome to VirusKeeper 2008 !

VirusKeeper is an anti-virus and anti-spyware solution for Windows.
(works on Windows 95/98/98SE/ME/NT4/2000/XP/2003/Vista)

Computer viruses are dangerous programs pose a permanent threat to your computer.
Viruses can cause a lot of damage: loss of data, mass emailing, infecting other computers on the same network…

Most anti-virus programs use scanners that identify known viruses.

The way they operate is simple: anytime a new virus appears, an anti-virus lab studies it and extracts its signature to update the signature database.
This approach has two significant limitations. First of all, you need to constantly update the anti-virus definitions to detect the most recent viruses. The scanners are also unable to detect new viruses!
This is why some viruses, such as “I Love You,” “Blaster,” “MyDoom,” and “Sasser,” infected millions of computers worldwide within days, though most of them were “protected” by an anti-virus scanner!

The newest threat to personal computers is spyware, which is not detected by most anti-virus software.

VirusKeeper provides an innovative and efficient solution: real-time threat analysis.
The analysis engine bases its conclusions on the standard attack patterns of viruses and spyware.
VirusKeeper constantly monitors the computer and provides several protection systems.

VirusKeeper keeps close tabs on all running programs, the Windows system files, the Windows Registry and the I/O ports.
VirusKeeper also automatically detects any spyware installation attempts and protects Internet Explorer from changes to its default pages and unsolicited component installation.
When spyware or a virus attempts to infiltrate the system, VirusKeeper detects it and displays an alert.
VirusKeeper provides features to stop and remove the infected file(s).

VirusKeeper does not detect threats with signatures. It detects any virus-typical activity.

You can use VirusKeeper Standard as your only anti-virus program or in conjunction with standard anti-virus software.
Used together, VirusKeeper Standard and a classical anti-virus scanner provide the highest level of protection.

VirusKeeper Pro combines the best protection technologies available in a single product:

- Real-time shield: permanent threat detection
- Real-time protection of Windows system folders
- Real-time protection of Internet Explorer
- Behavioral analysis detection of viruses and spyware
- Automatic scanner that inspects new or suspicious files
- Traditional, ultra-fast anti-virus scanner
- Anti-spyware scanner

Password Protection

Password protection can be used to restrict access to some of VirusKeeper’s functions. This protection is especially useful if your computer is used by several people.

This function allows, for example, a company’s network administrator to block the access of other users to prevent them from configuring VirusKeeper incorrectly.
In the home, it allows parents to prevent their children from modifying VirusKeeper’s settings.

Password Protection can restrict access to the following functions and settings of VirusKeeper:

- Deactivation
- Shutdown
- Real-time protection options

Once Password Protection is activated, you will be asked to enter your password every time you access one of these functions.

ProcessWatch : identify programs in memory

ProcessWatch is a powerful tool that shows all programs running in memory.

ProcessWatch identifies all running programs and provides information on each program.
(file name, location, memory usage, dlls used ...)

ProcessWatch also detects any malicious programs.

Real-time Protection

VirusKeeper includes a real-time shield that permanently protects your computer from harmful programs like viruses, worms, Trojan horses, and spyware.

VirusKeeper uses a behavioral analysis engine to detect known and unknown threats.

In addition to this behavioral analysis, VirusKeeper includes many other methods of detecting dangerous software:

Monitoring of Windows system files and resources
The Windows files are vital to the functioning of the system. VirusKeeper therefore permanently regulates access to and protects the system files, where many viruses try to hide themselves. VirusKeeper keeps a close eye on your Windows folders and immediately detects suspicious new files.

Monitoring of the registry
The registry contains all the settings and configuration information necessary to the running of Windows. Windows therefore needs a clean registry to function properly and many viruses and spyware programs modify or attack the registry. When this monitor is active, VirusKeeper protects the registry from these attacks.

Monitoring of active processes
When this option is active, VirusKeeper constantly scrutinizes the programs running in memory and identifies all harmful software (viruses, worms, Trojan horses, spyware, etc.).

Monitoring of communication ports
Some harmful programs, like viruses, worms, and spyware, propagate themselves or transmit information through networks or over the internet. When this option is active, VirusKeeper scans your computer’s communication ports and detects any suspicious activity.

Real-time detection of spyware
Most antispyware programs are scanners that only detect spyware long after it has been installed and has started doing damage to your computer.

Protection of Internet Explorer
Harmful programs, spyware in particular, very often target your web browser. When this option is active, VirusKeeper safeguards Internet Explorer and its settings. It detects any change in configuration or installation of third-party software, such as toolbars, spyware components, and changes of the default search and home pages.

Automatic scan of new or suspect files (VirusKeeper Pro only)
When this option is active, VirusKeeper Pro identifies suspect programs using signature analysis and scans them along with all other programs installed on your computer. This function is only available with the professional version of VirusKeeper.

All these protections are activated by default; they should be left running so that VirusKeeper can work most efficiently.

In very rare cases, you may need to deactivate one of them to prevent a conflict between

VirusKeeper and another program.

Quarantine

When VirusKeeper detects a program that poses a moderate risk to your computer, it gives you the option of quarantining it. A program in quarantine cannot be run and cannot do any damage to your system.
Files stored in Quarantine cannot infect your computer.

You can permanently delete a quarantined program by clicking the Delete button.

If you accidentally put an uninfected program in quarantine, you can restore it to its original place by clicking Restore.

Registry Alert

A program has added a new key to the Windows registry that will allow it to start with Windows.

This action is typical of spyware and viruses.

You may, however, have received this alert in error if:
- you have just installed new software
- you have just updated software
- you have just installed a new device (modem, video card, scanner, printer...)
- you have just updated a device driver

If one of these is the case, click the “Ignore” button.

Check the name of the program that will be run at Windows start-up
If you are unfamiliar with the name, click the “Remove” button to get rid of it.

Program Report

The Program Report highlights areas where the majority of harmful programs, like viruses, worms, and spyware, install themselves.

The report can be generated in plain text or HTML format. It can be easily saved, printed, or transferred.

The Program Report is especially useful for asking another person about the set-up of the software on your system.
It can be used, for example, to exchange information with other users over email or on on-line forums.

Ask an expert about removing a virus

Is your computer is infected with a virus or spyware? Do you need help to remove it?

You can ask an expert! See VirusKeeper's "Help" tab.

Scan Scheduler
(VirusKeeper Pro only)

The scan scheduler allows you to schedule regular system analyses.

You can schedule an analysis (antivirus or antispyware) to run automatically as often as you want:

- every day at a certain time
- every week on a certain day
- every month on a certain day
- when Windows starts
- only once at a certain day and time

The Scan Scheduler is only available with the professional version of VirusKeeper.

Tools

This tab displays the following items:

- ProcessWatch II
- Report
- Password protection
- Scan scheduler (VirusKeeper Pro only)

Update VirusKeeper

VirusKeeper can be updated via the internet.
VirusKeeper updates provide bug fixes and new protection technologies.

An internet connection is required to use the update feature.

The time required to download an update is generally less than one minute with a DSL connection.

By default, updates are automatically performed at VirusKeeper start-up.
You can change the update settings in VirusKeeper's "Update" tab.

Information on VirusKeeper updates is also provided on the VirusKeeper web site at www.viruskeeper.com.

What is a computer virus ?

A computer virus is a program that shares some of the aspects of biological viruses:
- it is dangerous
- it is small
- it is difficult to detect
- it is self-replicating

Viruses are propagated through the internet (email, downloads, etc), networks and disks.

Once a virus is present on a system, it will try to spread itself. It might, for example, email itself to all of the contacts in a user's address book.

Viruses can cause different types of damage. They can:

- destroy data
- drastically reduce system performance
- use contaminated systems to send spam or attack another systems
- open backdoors to give remote users access to the computer

To get rid of a virus, you need to detect which file has been infected and then delete it.

VirusKeeper provides the solution by detecting and removing the viruses.

What is spyware ?

Spyware is a small program that installs itself without user knowledge or permission.
Spyware can be installed from software or a web page.

A spyware program can:
- display ad pop-ups when you are browsing the internet
- collect data on your computer and your browsing habits
- add unwanted tool bar or button to Internet Explorer
- slow down your computer

Spyware programs are not viruses and are not detected by classical anti-virus scanners.

VirusKeeper, however, can detect them and displays an alert whenever spyware attempts to install itself on your computer.