Security Task Manager

for Windows XP, 2003, 2000, NT, ME, 9x

Provides advanced information about programs and processes

© A. & M. Neuber Software GmbH, 2006

content

Features of Security Task Manager 3

Using Security Task Manager 3

Process types 4

Risk Rating of processes 5

Viewing process details 7

Learning more about a process 7

Ending a process 8

Using quarantine folder 8

Exporting process list 8

Printing process list 8

Writing a comment 9

Protecting your computer with SpyProtector 9

Changing the language 10

Adding a language file 10

Contacting the Security Task Manager Team 10

Uninstalling Security Task Manager 10

Remarks about the shareware version 11

Switching the shareware to a registered version 11

Features of Security Task Manager

Security Task Manager provides detailed information about programs and processes running on the computer. For each process it shows the following information not shown in Windows Task Manger:

- file name and directory path
- security risk rating
- description, start time, program icon, process type
- CPU usage graph
- contained hidden functions
  (keyboard monitoring, Browser supervision, manipulation)

SpyProtector can eliminate your Internet traces, warn when your registry is changed and disable keyboard and mouse surveillance on your computer.

Using Security Task Manager

Security Task Manager shows all active processes on your computer. The Rating tells you all relevant security functions a process contains.

The listed processes can be sorted by the following properties. Click on the **View** menu to choose which properties are shown.

- Name
  Shows name of the software or name of the driver.
- Rating
  Shows an objective and relevant security process Rating. The longer the red Rating bar, the more dangerous functions the process contains. Highly rated programs are not always dangerous; however, they might contain some typical spyware properties. Click on a process to learn more about it. Then you can assess the trustworthiness of the software.
- CPU
  Shows CPU (processor) usage. Active programs keep the processor more occupied than inactive processes.
- Memory
  Shows working memory usage.
- File
  Shows the directory path and the name of the file.
- Type
  Shows the file type. The file type can be a program, a system tray icon program, a Browser Helper Object, a driver or a service.
- Title and Description
  Shows the title and file description contained in the file. For a visible window the title corresponds to the text in the window's title bar.
- Manufacturer and Product
  Shows the name of the company and product description found in the file.

Click on a process to obtain more information about it. You can:

see properties

end process

place process in quarantine

Note

- Click **Windows processes** button to also display all internal Windows processes. These processes belong to the Windows operating system. Windows system processes are not shown by default.
- A process can be a program, driver, service or PlugIn - i.e. every executed code which is active in your computer's memory.

Process types

Security Task Manager distinguishes the following kinds of processes. Click **Type** in the **View** menu, to display or hide the type as column in the main window.

Software

- Program

Labels a program with a visible window, or an unvisible program without a window.

- Taskbar icon

This is a program with an icon in the system tray (left of the clock). Right-mouse click this icon on the task bar to open a context menu and to get more information.

DLL files

- DLL

  A Dynamic Link Library (DLL) executes program code just like a program. A DLL file contains rarely used functions outsourced by the main program.

- ShellExecute

  This file was started by means of a Hook using the ShellExecute command in the Windows registry. ShellExecute runs a process (mostly a DLL) when any Windows program is started. This process should be examined carefully.

Internet PlugIns

Browser Helpers Objects

A Browser Helper Object (BHO) is a DLL that allows developers to customize and control Internet Explorer. Alexa, GetRight, Go!Zilla and other download managers use a BHO. BHOs can monitor all your Internet activities. To deactivate BHOs, in Internet Explorer click on **Extras** menu in **Internet Options**. Click **Advanced** tab. Under Browsing, clear the **Enable third-party browser extensions** check box.

Drivers and Services (available only in full version)

Drivers and Services execute system functions at lower hardware level.

device driver

A service type flag that indicates a Win device driver to control hardware compo - nents (e.g. graphic adapter, scanner). Some software modules (e.g. Firewall, AntiVirus) are device drivers, and thus you should not terminate these processes.

file driver

A service type flag that indicates a Windows NT file system driver.

Service (own process)

A service type flag that indicates a Win32 service that runs as a process on its own. A Win32 service starts automatically upon start of Windows, is always running and does not depend on users.

Service (own process with desktop interaction)

A service type flag that indicates a Win32 service (e.g. Firewall, AntiVirus) that runs as a process on its own and can interact with the desktop. A Win32 service starts automatically upon start of Windows, is always running and does not depend on users.

Service (shared process)

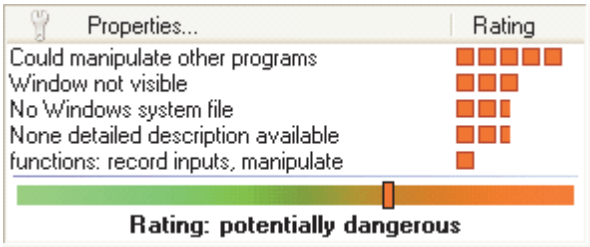
A service type flag that indicates a Win32 service that shares a process with other services. A Win32 service starts automatically upon start of Windows, is always running and does not depend on users.

Service (shared process with desktop interaction)

A service type flag that indicates a Win32 service that shares a process with other services and can interact with the desktop. A Win32 service starts automatically upon start of Windows, is always running and does not depend on users.

Risk Rating of processes

Security Task Manager uses objective criteria to judge the safety risk of a process. Security Task Manager examines the process to determine if it contains critical function calls or suspicious properties. Points are allocated depending on the potential danger of these functions and properties. The sum of the points results in the Security Task Manager Risk Rating (0 to 100 points).



Security Task Manager examines the processes with respect to the following functionalities (sorting by dangerousness):

- Able to record keyboard inputs
  The process monitors each keyboard input. This is realized by a Hook function. Serious programs do not use this Hook function.
- File is hidden
  The file hides from the Windows Explorer. Should not be confused with the harmless file attribute "hidden".
- Keyboard driver, could record inputs
  It is a keyboard driver and can read each keyboard input you make.
- Could manipulate other programs
  The process can manipulate any program running on Windows, or any program that is part of the Windows operating system. A Hook is set for this one. A Hook is a Windows internal function that can forge a list of files on your hard drive, for example, by manipulating the dir command. The program that starts the process is not visible to other programs like AntiVirus software.
- Able to monitor Internet browser
  A Browser Helper Object (BHO) is a DLL that allows developers to customize and control Internet Explorer. Alexa, GetRight, Go!Zilla and other download managers use a BHO. BHOs can monitor all your Internet activities. To deactivate BHOs, in Internet Explorer click on **Extras** menu **Internet Options**. Click **Advanced** tab. Under Browsing, clear the **Enable third-party browser extensions** check box.
- Starts when other programs are started
  This file was started by means of a Hook using the ShellExecute command in the Windows registry. ShellExecute runs a process (mostly a DLL) when any Windows program is started. This process should be examined carefully.
- Listen on port *<No.>*
  The process can receive information from the Internet. Hackers use such leaks to take control over your computer. You can prevent such attacks with a good firewall.
- Send to *<computer name>* on port *<No.>*
  The process connects to the named computer or IP address and can send any information to it. You can prevent such connections with a good firewall.
- Unknown program listens or sends
  A port was opened to receive or send information over the network or the Internet. You should try to find out which program it is. With a good firewall such connections can be prevented.
- Monitoring of program starts
  The process monitors when, and which, programs are started or closed.

- Window not visible
  The program does not have any visible window and runs in the background. In the most favourable case it may e.g. be a device driver software.
- Start when Windows starts
  The program is started at each Windows start since it writes an autostart key in the registry.
- No detailed description available
  Some important standard descriptions in the file were not found. By default, each file internally contains fields for descriptions.
- No Windows system file
  The file is not part of the Windows operating system. Windows system files are subject to special checks and protection by Windows.
- No description of the program
  Descriptions were not found in the file. By default, each file internally contains fields for descriptions.
- Functions: Internet, monitor, record inputs, hide, manipulate
  The file contains function calls with the named properties. Since there is no evidence this function is utilized, it doesn't have much influence on the Rating.
- Functions: not determinable
  No dangerous function calls were found in the file. However, such calls could be hidden within the file.
- Unknown manufacturer
  The software manufacturer cannot be identified from the file description fields. By default, each file internally contains fields to identify the software manufacturer.

Trusted properties (reduces risk):

- Microsoft signed file
  This file was signed by Microsoft. You can trust this file like you also trust Microsoft.
- Verisign signed file
  This file was signed by VeriSign. You can trust this file like you also trust VeriSign.
- Belongs to <*software product*> from <*manufacturer*>
  You can trust the file. It's a part of the mentioned and installed software. When you deinstall that software, the file will be removed.
- Certified by <*registrar*> for company <*manufacturer*>
  This file was signed by a registrar. You can trust this file like you also trust this registrar and the software manufacturer.
- Own comment
  You can write your own comment in order to influence the risk rating.

Note

- Highly rated programs are not always dangerous; they may just contain properties typical of some known spyware programs.
- Click **Windows processes** button to also display all internal Windows processes. These processes belong to the Windows operating system. Windows system processes are not shown by default.

Viewing process details

Click on a process to display detailed information about the process. The following properties are shown:

- Name
  Shows the name of software or the name of driver.
- Rating
  Shows an objective and relevant security process Rating. The longer the red Rating bar, the more dangerous functions the process contains. Highly rated programs are not always dangerous: They just have some typical spyware properties. Click on a process to display details and to assess the trustworthiness of the software.
- File
  Shows the directory path and the name of the file.
- Type
  Shows the file type. The file type can be a program, a system tray icon program, a Browser Helper Object, a driver or a service.
- Title and Description
  Shows Title and file description contained in the file. For a visible window the title corresponds to the text in the windows' title bar.
- Manufacturer and Product
  Shows the name of the company and product description found in the file.

Note

- Click **Windows processes** button to also display all internal Windows processes. These processes belong to the Windows operating system. Windows system processes are not shown by default.
- Click on **View** menu to choose which properties should be shown as column in the main window.

Learning more about a process

1 Click on the process you wish to examine.

2 Click **Google** button on tool bar.

An information web page is displayed on www.neuber.com/taskmanager where you can submit your opinion about this software/driver software or read other user's comments. You can search for further information about this process at Google.com from this web page.

Note

- Your Internet Browser transmits information (e.g. operating system, language setting). Neither the program Security Task Manager nor any of its components make a connection to the Internet.
- Google.com is one of the mostly used search engines and provides relevant results.

Ending a process

1 Click on the process you want to close.

2 Click the button **Remove**.

3 Then select one of following options:

- End process
  The process will be removed from memory. If the process has written its own autostart entry in the Registry (Windows configuration data base), then it will however become active again at the next start of Windows.
- Move file to quarantine
  Also in this case the process will be removed from memory. In addition, Security Task Manager puts the corresponding file into the quarantine folder and deletes any corresponding Autostart entries in the Registry. File and registry entries are saved, so you can restore the process at any time.

Note

- Ending a process can cause system instability, including crashes. Software that needs Adware programs may no longer work. Please save opened documents.

Using the quarantine folder

The quarantine folder works like the Windows Recycle Bin (trash). When you put a file into the quarantine folder, the file is renamed and moved to an isolated folder. Corresponding Autostart keys in Windows registry will be deleted. Thus the process can no longer be started. However, restoring the whole process is possible at any time:

Restoring processes

1 Click **quarantine** button on the tool bar.

2 In the quarantine folder, click on the process you want to restore.

3 Click **Restore** button.

Exporting the process list

1 In the File menu click **Export to**.

2 Choose a file type:

- Text file (*.txt)
- Website (*.html)

Printing the process list

1 In the File menu click **Print**.

2 Choose a printer and any properties that may be required (e.g. duplex print).

Note

- Click **Windows processes** button to also display all internal Windows processes. These processes belong to the Windows operating system. Windows system processes are not shown by default.
- Please save a process list from time to time. A saved process list can serve as a point of comparison to help you find new processes in the future.

Writing a comment

You can write your own comment for each process, this will then be visible in the process properties. You can also make your own risk assessment to influence the Security Task Manager Rating.

To write a comment

1 Right mouse click the relevant process.
2 In the context menu, click on **Comment**.
3 Enter you comment and any risk assessment you may have.

Protecting your computer with SpyProtector

To run SpyProtector, click on the icon in the system tray of your task bar.

SpyProtector offers the following tools to protect your computer from keylogger, spyware and trojans:

Delete history
Check this option to eliminate the traces of Internet activities (cookies, cache, history, typed URLs) in Internet Explorer. You can also delete the list of recently used programs (e.g. Word, ACDSee, PDF, WinZip, Mediaplayer) and the list of recently used documents in the Windows Start menu.

Disable keyboard monitoring
Check this option to block most of keyloggers for the current Windows session. The redirection of all keyboard inputs to other programs will be blocked. Such a keyboard redirection could be realized by programming a Hook function. Not even keyboard utilities like macro and autotext programs make use of such dirty Hooks.

Disable other monitoring
Check these options to block programs which log data for the current Windows session:

Keyboard inputs (indirect)
This prevents monitoring of internal Windows messages (e.g. keyboard inputs) by other programs.

Mouse activities
This prevents monitoring of mouse movements and mouse clicks

Macro
This prevents recording of user activities. This method, often used by macro programs, is not typically used by keyloggers.

Starting and ending of programs
Program starts and stops are logged. This function is frequently used by tutorial programs (CBT) for the purpose of interaction with the software to be learned.

Attention: Even some safe and valid programs (e.g. some Macro programs) use these Hook functions. If such a program should no longer work properly, then please deactivate the corresponding option or restart your computer.

Warning when registry is changed
Check this option to display a message box if a program attempts to enter its name in the Windows registry as autostart key. With such an entry, which may be visible or invisible, the software will start secretly at each start of Windows. All dangerous programs need such a registry key to become active at computer restart!

Changing the language

Security Task Manager recognizes automatically the used language (English, Deutsch, Espanol, ...). To change the language, please do the following:

1. In the **View** menu click Language ▸
2. Then click the language of your preference.

Note

- The software can easily be translated to any language. Simply translate the lgs_english.txt text file in the program's folder and send it to info@neuber.com. You will receive a free registration for your translation.

Adding a language file

You can download additional language files at www.neuber.com/taskmanager.

1 Go to www.neuber.com/taskmanager.
2 Here you can see all available languages.
3 Copy the lastest version in the Security Task Manager directory.
for exapmle C:\Program Files\Security Task Manager
4 Change the language and then run Security Task Manager.

Note

- The German and English language files lgs_deutsch.txt and lgs_english.txt are contained by default.

Contacting the Security Task Manager Team

Technical Contact:

address:	A. & M. Neuber Software GmbH PF 11 05 25 D-06019 Halle Germany
fax:	(+49) 0700-11 777 000
Internet:	
WWW:	www.neuber.com/taskmanager
email:	info@neuber.com

The registration is executed by the international registration service ShareIt (Greensburg/U.S.A, Köln/Germany, London/UK, Roissy/France, Upplands Väsby/Sweden).

Uninstalling Security Task Manager

1 Click Start-Settings-Control panel.
2 Click **Software**.
3 Click the **Remove** button to delete Security Task Manager from your Computer.

Note

- You can also run uninstal.exe in the Security Task Manager directory

Remarks about the shareware version

Security Task Manager is distributed as shareware. Shareware is a distribution method based on honor, and is not a type of software. You are free to use it for a trial period of up to 30 days. If you find this program useful and would like to continue using Security Task Manager, then you are required to register for $29 (29 EUR). You will receive a registration code that you can use to unlock the shareware. The registration code will turn off all nag screens and shareware limitations, and work with future updates.

As a registered user, you will get:

- legal license for the software
- your personal key to unlock trial version
- free minor updates
- free software SpyProtector
  Spyprotector eliminates your Internet traces, warns when Autostart key in the registry is changed and disables keyboard and mouse surveillance
- free technical support (via email or regular mail)

On **Help** menu click **Info...** to see whether your version is registered.

Switching the shareware to a registered version

1 In the **REGISTER** menu click **Unlock the shareware version**.

2 Enter the Name and Code in the registration dialog **exactly** as shown in the information sent to you.

3 Click **Unlock**.