What is RegRun?

RegRun is an excellent tool kit for protecting your computer against viruses or Trojans/Spyware/ Adware parasites or Rootkits. The RegRun uses the newest technology in the world.

Fight with the bad guys by the most powerful weapon.

What you should know about RegRun?

RegRun is not an antivirus in a common sense. It does not scan your disk and detect/cure using signature database. There are a lot of antiviral programs that you can choose.

RegRun checks all Windows startup holes and it can detect and remove any UNKNOWN virus. The modern viruses spreads to the millions computers in the world for a pair days. First, a virus kills an antivirus and disables a way to update the antiviral databases.

RegRun prevents a virus auto start. Later you can clean your computer by antivirus to remove virus according files and registry records.

RegRun resolves three main tasks:

1. Makes backups of the registry and important files. Restores a computer even if it does not boot.
2. Detects a virus in your computer.
3. Removes a virus from your computer.

Hope you enjoy it!

Who needs RegRun?

If you are a user who is exposed to sources of viruses and Trojans (e.g. you are an Internet surfer, E-mail recipient, one who buys "safe" software on CD's, or one who receives data on floppy disks), or if you are an experienced user who needs to adjust your startup configuration as a function of testing and debugging new software, you need RegRun.

RegRun is the best choice for users who wants to get maximum security, for power users and computer professionals.

RegRun - an overview

We have designed RegRun Security Suite to be a very effective system, tailored to individual user needs.

We offer three versions of RegRun Security Suite.

- The **Standard** version can be used only for removing dangerous components.
- The **Professional** version can be efficiently used by professionals in computers.
- The **Gold** version is recommended for maximum protection and security.
- The **Platinum** version ie recommended for ultimate protection and security.

If you have Windows 95/98/Me you can use RegRun Gold for ultimate protection.

Yesterday you used several products to do your work; today you need only RegRun.

Getting Started

What do you need to do first?

Open Control Center and choose "Scan for viruses" item (this command will be automatically executed after installing RegRun).

You need identify unrecognized programs, drivers or components.

RegRun's Disinfector will ask you to make a choice: "Good" or "Bad".

Be careful, do not hurry. RegRun will help you in your work.

It will display all information about suspicious program:

1) Version Information. Legitimate programs often includes information about its manufacturer, we address, description of the program.

2) Code signing. RegRun checks if a file is signed by Microsoft. All Microsoft Windows programs, DLL and drivers are signed. If a file is signed it is about 99.99% good file.

3) Application Database information. RegRun uses Application Database installed on your computer during installation. If it found the description for a program it will display text and rating. Application Database is constantly updated automatically or manually using RegRun Control Center.

4) You can send request to Greatis Support team and you will get the reply in one business day.

When does RegRun begin to defend me?

Immediately!

As soon as RegRun starts up, you will be protected by default security settings chosen by the professionals at Greatis Software.

Security Level is a quick way to set up all RegRun's security features. Try to change this level and choose your optimum settings. Open RegRun Control Center and choose "Options".

What will I see when I use RegRun?

Don't worry! You have a right to decline changes and to return to the previous state. RegRun automatically saves your current Windows startup to the profile file. You may restore this profile later.

Do you want to know more?

- WatchDog alerts;
- Anti Replacement alerts;
- Registry Tracer alerts;
- File Protection alerts;
- RunGuard alerts.

Should I say YES?

Alerts occur when a program on your computer wants to modify Windows startup. Choose "Yes" to Accept changes or choose "No" to decline. We suggest you decline all changes if you are not sure that you understand why they are needed.

RegRun sets declined items to the paused state and you can make these items active later.

If you don't want to be asked about several programs again you may add them to the "Exclusion list ". In other words you may create White list.

And on the phone book analogy, you may create the Black list. RegRun will automatically remove all programs listed in the Black list from your startup without any questions.

How do I begin to use RegRun Suite features?

You may always launch RegRun Control Center by clicking on the "Start" button, menu "Programs", "RegRun Security Suite", "RegRun Control Center".

Using RegRun Control Center you may quickly execute RegRun features, customize RegRun's options and check for newer version of RegRun Suite.

Tip!

Don't forget about WatchDog icon near system tray. Right click on this icon to get access to the popup menu. This menu allows you to access RegRun by one click!

Is RegRun compatible with ...?

RegRun Suite is fully compatible with Windows 95/98/Me/NT4/2000/XP/Vista!

RegRun Suite is fully compatible with all known antiviral software.

Note!

RegRun Suite automatically recognizes a lot of known antiviral programs. Antivirus Coordinator feature allows you to quickly check your Windows startup with any antivirus installed on your computer. It's fully customizable.

Tip!

RegRun Suite's files have their own antivirus protection. We suggest you exclude RegRun Suite folder from testing via your antivirus settings. This will increase RegRun performance.

Let's go!

Do not forget to make backup copy of your registry. RegRun Rescue (included with the Gold Edition) can make backup copy of your registry by one click and in fully automatic mode.

1. Quickly remove dangerous and useless programs from your Windows startup with Startup Optimizer.
2. Launch Advanced Optimizer (Windows Core Components) to get rid of advertising spyware and other useless components.

What else should I know?

Startup Optimizer uses RegRun Application Database that contains descriptions of a lot of well known programs. This database is included in with RegRun Suite and updated weekly. All updates are free for you.

If you do have any questions do not hesitate to contact us by e-mail. You will receive a reply from our support team within 24-48 hours. If you do have unknown or strange programs you may send these files to us by e-mail for testing.

To get more information you should simply click on the Help button. Use the table of contents and search engine to quickly locate any information you need!

What's new?

Version 5.70

1) Updated UnHackMe for resolving some BSOD problems.
2) Improved "Virus Scan" for removal Medichi rookits.
3) Fixed bug in RegRun Rescue.
4) Added detection SPTD 1.55 included into the Daemon Tools.
5) Fixed bug with wrong disk names in the Bootlog XP.

6) Fixed bug in Partizan.sys driver.

Version 5.60

1) "**Safe deleting**" feature allows a user to restore the system files deleted by mistake using virus scan.
2) Updated Reanimator for fixing 2 new Windows startup vulnerabilities.
3) Updated UnHackMe for removal modern rootkits.
4) Added feature for quick disabling **autorun** on the fixed and flash drives (in the Start Control, "Reanimator" menu). Required for protecting against flash stick viruses.
5) Added an option for hiding Partizan welcome messages (Start Control, "Features", "Partizan" menu.
6) Updated "Detailed System Report".

Version 5.50

1) New! UnHackMe with Partizan technology detects hidden rootkit by monitoring Windows boot process. Details …
2) Updated UnHackMe for removal modern rootkits.
3) Vista ready!
4) Changed Secure Start. Now it automatically scans for viruses before Windows starts.
5) Updated RegGuard: removed compatibility problem with Windows updating.
6) Updated "Detailed System Report".
7) Updated Auditing module. Now it fixes the registry tracer and virus scan alerts.
8) Added a way to quickly stop all monitoring functions using WatchDog.
9) Added an option to protect RegRun's features and alerts by password.
10) Fixed a lot of small bugs.

Version 5.00

1) New! RegRun Partizan provides you a new the newest rootkit protection of the world.
2) Partizan can detect and remove rootkits before Windows starting. Partizan is a native API application that works on the early stage of Windows boot process like a auto check disks.
3) Updated for fixing new security holes.
4) Updated for compatibility with Windows Vista RTM.
5) Fixing the bugs with working under non-administrative account.

Copyright/License/Warranty Disclaimer

You should carefully read the following terms and conditions before using this software. Use of this software indicates your acceptance of these terms and conditions. If you do not agree with them, do not use the software.

License Agreement

This is not free software. You are hereby licensed to: use the Shareware Version of the software for a 30 day evaluation period; make as many copies of the Shareware version

of this software and documentation as you wish; give exact copies of the original Shareware version to anyone; and distribute the Shareware version of the software and documentation in its unmodified form via electronic means. There is no charge for any of the above.

You may install this program to test and evaluate for 30 days; after that time you must either register this program or delete it from your computer hard drive.

Unregistered use of **RegRun Security Suite** after the 30-day evaluation period is in violation of United States and International copyright laws.

RegRun Security Suite Single License

Recommended if you use the software on one computer.

All users of the computer can use the software.

You may use or execute the licensed software at work, for a commercial purpose, in a commercial context or environment.

RegRun Security Suite Family License

Recommended if you and your immediate family (mother/father, husband/wife, children, sibling) intend to use the software on one or multiple privately used family PCs of one household.

You may use the licensed software on all computers of yours and your immediate family (spouse, parents, children, siblings) that (the computers) are physically located in the non-commercial license household and are solely used for private (non-commercial) purpose. You may use as many copies of the licensed software at the same time as you need to.

You may not use or execute the licensed software at work, for a commercial purpose, in a commercial context or environment.

RegRun Security Suite Business License

Recommended if you are the only user of the software and use the software at work and privately on one PC per time (e.g. on your work PC, your private home PC and on your laptop).

You may use the licensed software on all computers that are used by no one else but yourself.

You may use the licensed software at work, for a commercial purpose, in a commercial context or environment.

You may not use or execute two or more copies of the licensed software at the same time (e.g. on a server and on your home or work PC).

This software may be distributed freely on online services, bulletin boards or other electronic media as long as the files are distributed in their entirety. This software may not be distributed on CD-ROM, disk, or other physical media for a fee without the permission of Greatis Software.

You may not alter this software in any way, including changing or removing any messages or windows.

You may not decompile, reverse engineer, disassemble or otherwise reduce this software to a human perceivable form. You may not modify, rent or resell this software for profit, or create derivative works based upon this software. You may not publicize or distribute any registration code algorithms, information, or registration codes used by this software without permission of Greatis Software.

Disclaimer of Warranty

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OR MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. BECAUSE OF THE VARYING HARDWARE/SOFTWARE ENVIRONMENTS INTO WHICH RegRun MAY BE PUT, THERE IS NO WARRANTY OF SUITABILITY FOR A PARTICULAR PURPOSE.

GOOD DATA PROCESSING PROCEDURE DICTATES THAT ANY PROGRAM BE THOROUGHLY TESTED BEFORE RELYING ON IT. THE USER MUST ASSUME THE ENTIRE RISK OF USING THE PROGRAM. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

How to buy?

We support purchasing via Internet using secure connection, via fax or email.

We accept all ordering methods: credit cards, checks, wire transfer etc.

You can choose your country currency.

Prices:

- RegRun Platinum Business+Family License $119.95
- RegRun Platinum Business $99.95
- RegRun Platinum Family $84.95
- RegRun Platinum Single $69.95
- Upgrade from Gold to Platinum Single $16.95
- Upgrade from Gold to Platinum Family $29.95
- Upgrade from Gold to Platinum Business $39.95
- Upgrade from Gold to Platinum Business+Family $59.95
- Upgrade from Pro to Platinum Single $29.95
- Upgrade from Pro to Platinum Family $39.95
- Upgrade from Standard to Platinum Single $39.95
- Upgrade from Standard to Platinum Family $49.95
- Upgrade from UnHackMe to Platinum Single $39.95
- Upgrade from UnHackMe to Platinum Family $49.95
- RegRun Gold Edition Business+Family $ 109.95 USD
- RegRun Gold Edition Business $ 84.95 USD
- RegRun Gold Edition Family $ 79.95 USD
- RegRun Gold Edition Single $ 49.95 USD
- RegRun Gold Second License $29.95 USD
- RegRun Professional Edition Single $ 29.95 USD
- RegRun Standard Edition Single $ 19.95 USD
- Upgrade from RegRun Standard to RegRun Professional Edition $ 9.00 USD
- Upgrade from RegRun Standard to RegRun Gold Edition $ 24.95 USD

- Upgrade from RegRun II to RegRun Professional Edition $ 9.00 USD
- Upgrade from RegRun II to RegRun Gold Edition $ 24.95 USD

RegRun CD is available for only $9.95 USD.

The latest information you can find on our site:

http://www.greatis.com/security/buy.htm

Education Discounts

The Students, Faculty and Staff of accredited Colleges, Universities, schools and other institutions are able to purchase RegRun Suite for a special price.

RegRun Gold NIVA Single $39.95

RegRun Pro Single $22.95

RegRun Pro Single $16.95

http://www.greatis.com/security/buy.htm

Education Institutions Discounts

Eligible Academic and Educational Institutions are able to get site license for 50%!

Contact us: http://greatis.com/support.

Government Licenses

Greatis Software offers special discounts to government-run institutions at the federal, state and local level. We extend the same offer to not-for-profit organizations.

Contact us: http://greatis.com/support.

Order multi-user license:

You can buy 2,3,5,10,50,100 or site license with large discount.

1. **Purchase on-line**

http://www.greatis.com/security/buy.htm

2. **Telephone and Fax Orders**

Telephone

Toll Free: 877-353-7297

Regular: 425-392-2294

Fax

Toll Free: 888-353-7276

Regular: 425-392-0223

RegRun Product ID: 2078-6

These telephones can be used only for purchasing.

For technical support, please, visit support center:

http://greatis.com/support

3. **Paying by Check via Postal Mail**

Universal Commerce, Inc.

ATTN: Orders
PO Box 1816
Issaquah, WA 98027
United States of America

RegRun Product ID: 2078-6

You will receive your registration code via email shortly after ordering.

Personal Information

If this is your first time purchasing a product with the RegNow system, fill out the following personal information, but leave the UserID blank. When your transaction is complete, the system will automatically assign you a UserID number that you can use for future transactions.

If you already have a UserID with our system, enter it in the UserID field and press the Load Personal Information button. Your personal information (but not your payment information) will be automatically entered in the form. You should always use your UserID and keep your record current so that vendors will be able to provide you with upgrade information about the products you have purchased.

UserID: _____

First Name: _____

Last Name: _____

Company: _____

Billing Address: _____

City: _____

State/Province: _____

Zip/Postal Code: _____

Country: _____

Phone: _____

Email Address: _____("N/A" if none)

REQUIRED

Order Information

Quantity: _____

Price: $

RegRun - Detailed Instructions

How does RegRun work?

1. If you use **Windows NT4/2000/XP/Vista**:

When Windows starts, you can see the following files:

%SYSTEMROOT%\SYSTEM32\config.nt

%SYSTEMROOT%\SYSTEM32\autoexec.nt

Registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunEx

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Values: Shell, Run, Load

HKLM\Software\Microsoft\Active Setup\Installed Components

Additionally registry keys monitored by Registry Tracer:

HKCU\Software\Microsoft\Internet Explorer\Main, Start Page value

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks

HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs value

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, UserInit value

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager, BootExecute value

The number of recommended to tracing registry keys increases every day.

Read the latest information at http://www.regrun.com.

File Extensions (on default):

pif, bat, com, exe.

Device drivers.

NT Services.

2. If you use **Windows 95/98/ME**.

When RegRun is started for the first time, it reads the following files:

- **AUTOEXEC.BAT**
- **CONFIG.SYS**
- **WINSTART.BAT**
- **WIN.INI**
- **SYSTEM.INI**

And the following registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunEx
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\Software\Microsoft\Active Setup\Installed Components

Additionally registry keys monitored by Registry Tracer:

HKCU\Software\Microsoft\Internet Explorer\Main, Start Page value
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs value
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, UserInit value
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager, BootExecute value
The number of recommended to tracing registry keys increases every day.
Read the latest information at http://www.regrun.com.

File Extensions (on default):

pif, bat, com, exe.
VXD and Device drivers.

Finally: **STARTUP and COMMON STARTUP** folders.

Whichever Windows you are using, RegRun remembers the entries in the registry and checks them every time you start. With each start, RegRun lists any changes found in a log file, which you can view at any time.

You may activate **Secure Start**. This has a unique function in that it allows the removal of programs **before loading Windows**!

Open RegRun Control Center, Options, Secure Start. Check "Secure Start DOS" (only for Windows 95/98) or "Secure Start Windows" box.

Secure Start is activated automatically if you selected "High" or "Ultra High" Security Level.

Read more about Secure Start.

RegRun vs Back Orifice 2000

What is Back Orifice?

This is the infamous virus that allows remote operation of any computer on a local network or over the Internet. On the controlled computer, the program "server" is established and typically is started automatically when Windows starts. Then the controlling computer is able to receive complete information (the information on disks, files, passwords, local network etc) about the controlled computer using the Trojan program - client. It is also possible to copy any file, to send a message, to reload the computer, or to start any program. Back Orifice is an excellent program for remote operation. But it is typically used for mercenary purposes and to cause damage.

How it is possible to catch Back Orifice?

Simply start an executable file. The file can be disguised under a useful sounding name. Be careful with starting of files of unknown origin.

Why the traditional ways of protection do not work?

The majority of antiviral programs only check for known viruses. Back Orifice is distributed free-of-charge along with the source code. It is therefore easy to create a new version of the program and the antiviral program will not find it.

***RegRun exploits a major weakness of Trojans*.** The Trojan program should automatically be started together with Windows. Otherwise it is not dangerous!

After the first start, RegRun remembers what programs are started automatically and considers those as safe. We recommend that you review these programs the first time that you use RegRun. After that, any new program that is started will be automatically detected and you will be notified about it.

Example of detection of Back Orifice 2000 on a computer with Windows 98(or Windows 95).

Notice that the unknown program UMGR32. EXE tries to be started through the key

HKLM\Software\Microsoft\Windows\Current Version\Run.

It is the **BackOrifice 2000**!

How did we determine it?

The program is started from the system folder "c:\windows\system".

In this folder there should be only systems programs.

By pressing the button "Get File Info" you will see no information about the manufacturer, or description of the file. There is a possibility, however, that it is required Windows or that is some other legitimate program.

Therefore, we should not delete it, we shall simply suspend its auto running by turning the traffic light yellow.

The program remains in the list, but will not be started automatically.

Now reload the computer.

What has changed?

Do our usual programs work?

If all is good, then suspending the program had no effect, and this program may be a Trojan.

But it is no longer dangerous!

Example of detection the Back Orifice 2000 on a computer with Windows NT.

You see the new service: "Remote Administration Service".

You didn't install this new service

The name "Remote Administration Service" is a default name for Back Orifice 2000.

Remember!

The names of the Trojan programs can seem to be very important; but, that is a dodge!

Be careful!

If the purpose of this service is unknown, then it may be a Back Orifice 2000.

Tip!

If you try to stop "Remote Administration Service" you will receive an error message.

This is a sign! You can easily stop most of the normal services.

The number of running services is not very large. Most are known and you can read about them in the Windows NT help. If you have trouble, contact us http://greatis.com/support and we'll help you.

To suspend running of an unknown service (may be "Trojan" program) you need to click on "Suspend Run" button and choose "Disabled" type of service. After that click on the "Continue" button. Restart your computer to activate changes!

Use RegRun!

See also: RegRun vs "I love you" Trojan.

RegRun vs "I love you" Trojan

RegRun easily detects and terminates the Trojan, "I love you" and all of its clones.

WatchDog will reveal changes to the registry.

Look at the list "Current User Run" and search:

MSKernel32

Win32DLL

Suspend running or even delete these entries.

Trojans also check for the WinFAT32 subkey in the following Registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

If the WinFAT32 subkey key is not found, the Trojan creates it, copies itself to the \Windows\System\ directory as WINFAT32.EXE and then runs the file from that location. If you didn't install WINFAT32, delete the entry in "Current User Run":

WinFAT32

All done!

See also: RegRun vs "Back Oriffice 2000"

Start Control

First experiments

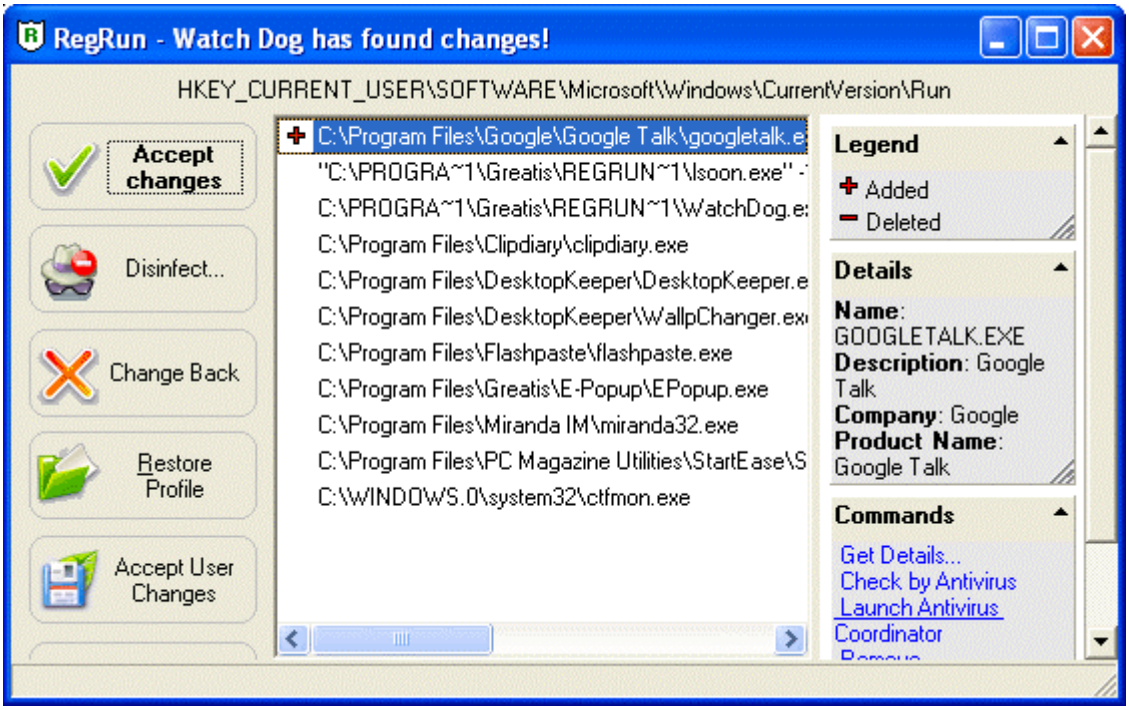
Now, it's a time to experiment with RegRun. Check out its great features!

Auto detection.

Click "Start" button in Windows taskbar, choose "Run" and enter "sysedit". Press Enter. You will see the system editor.

Insert a new line in autoexec.bat, for example "*rem test*".

After that, press F9 or click "tick" button.



You will see "+" on the left of line "rem test".

You have five choices:

- **Change Back.**. This will cancel all of the changes. Any added lines will be removed and deleted items will be restored.
- **Accept changes.** This allows you to accept the changes. RegRun will then accept them and will not refer to them again.
- **Restore profile.** You can restore your RegRun profile by clicking on Change Back.
- **Accept Made Changes.** It allows you to modify and then save the current list manually. If you select this choice, press "Enter" or the "Edit" button. Then, after making any edits, select "Save".
- **Ignore**. Selecting "Ignore" will result in no action being taken. The next time you boot up, the program will detect the same changes again and warn you of them again.

Pause/resume items

You may suspend the running of the program, however not delete it. Select item and click on arrow to change item state.

You will see a popup menu.

Select traffic light and click left mouse button (if you choose red light, you will delete the item). After that, the item light changes to yellow color and you may see the item at the bottom of the list. RegRun shows green items before yellow items.

RegRun uses an algorithm that is compatible with Microsoft technology for suspending programs. If you have Microsoft Windows 98, you may run System Configuration utility

and see that the item shows it has paused. However, RegRun works on Windows 95 and Windows NT 4.0. These operation systems will also have a suspend feature.

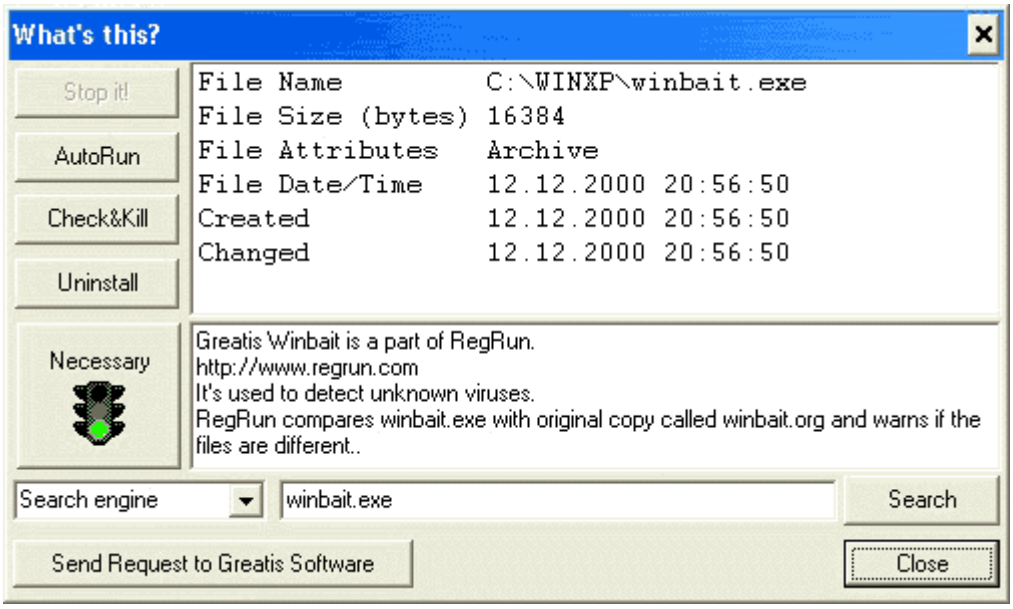
You can pause or resume each item easily. If you use the keyboard, press CTRL+Enter and you will see a menu. Choose item in menu and press Enter to change item state.

You can select the multiple items in list and set it simultaneously.

You need to restart your computer to make changes.

If you want know more about any program, RegRun helps you. Press CTRL+/ (or choose "Properties" in popup menu) and you will see file information window.

For example:



This information is helpful if you are in doubt about file's source.

Operations with multiple items

RegRun allows you to operate with multiple items.

This is a powerful and useful feature.

It works on any list in RegRun.

Selection

To select more than one item, use the key CTRL and Shift.

1. Hold the CTRL key and click on the items by turns.
2. With the Shift button you can fast select many items.

   Click on the first item.

   Press Shift and hold it.

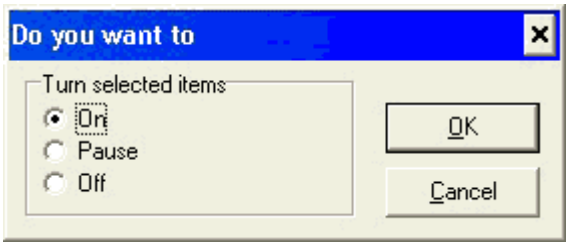
   Click on the last item.

To get the popup menu click the right mouse button.

Select the command.

Command that works with multiple items:

1. Turn On/Pause/Off.



2. Copy to.

3. Move to.

RegRun converts items while moving or copying.

Registry page

In the registry page you can see the contents of the keys:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices. This key contains systems programs such as SYSTRAY etc. These programs start before other keys and the startup folder. If you work in a network, note that these programs run before you enter your user password. All programs are common for all users on the computer.
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run.
  Programs in this key run after that user enters his or her network password. All programs are common for all users on the computer.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
  Programs in this key run only for specific users.
- You can select function by click on the icon or choosing the item in the popup menu (right mouse button click).

Selection

To select more than one item use the key CTRL and Shift keys.

1. Hold the CTRL key and click on the items by turns.
2. With the Shift button you can quick select many items.
   Click on the first item.
   Press Shift and hold it.
   Click on the last item.

All features list.

1) Edit feature.
2) Terminate.
   Allows you to fully removing a file from Windows startup, memory, and from hard disk.
3) New program feature.
   Press INS key if you using the keyboard. Fill in the form and Click on the OK button.
4) Recall deleted.
   Press CTRL+Z to undo last deleted items. Only items deleted in the current session of RegRun!
5) Add to Job. *Only in RegRun Pro and Gold versions.*)
   Allows to add current program to the RegRun Job file. You will be prompted to locate existed job file.
6) To recall long since deleted items, you can press CTRL+R.
7) Export items.
   Press CTRL+S to export all items in the registry page to a "reg" file. This is a text file

with special format. If you double-click on a reg file in explorer, all items will be restored by the Registry Editor.

8) Run. Launch the application associated with the registry key.
9) Copy. Copy the selected items to another folder.
10) Move. Move the selected items to another folder.
11) Sort Order.
12) Explore location. Shows the folder or registry key that contains the item.
13) Antivirus/Commands. Quickly check a file by antiviral software or copy/move/delete it.
14) Add to Application Database. Quickly adds this file to Application Database.

Win.ini page

Win.ini file is often used in Microsoft Windows 3.1, but in later version of Windows it is rarely used. Win.ini is saved for backward compatibility.

There are two lines for running programs: Load and Run. All programs are divided by commas.

Be careful!

Trojan programs often use this file!

System.ini page

The "System.ini" file is often used in Microsoft Windows 3.1 and exists for backward compatibility.

There is one line that is used for launching programs - Shell.

Be careful! Don't change this line if you are not sure.

The normal value of Shell is "Explorer.exe." It is a shell for Microsoft Windows.

If you have another program after the "Explorer.exe," you need to check it.

Most of Trojan programs use the Shell for auto launching.

Config.sys page

Config.sys is an especially important file for MS-DOS. In Windows'95/98 this file is used only to configure some parameters and for backward compatibility. However, you may still run some programs from config.sys. Inspect this file carefully, seek out rows with the prefix: "**device=**" or "**install=**". Any device driver or program located after equal sign in this row may be dangerous. We recommend that you use the minimum number of programs in config.sys. Normally, if you might use, for example:

device=c:\windows\himem.sys
device=c:\windows\emm386.exe NOEMS
device=C:\WINDOWS\COMMAND\display.sys con=(ega,,1)

Check all files that you need.

- If you want to enlarge the font in a window, click the icon with an up arrow. You need to select the Conrol Center Options to make the size and font persistent in the editor.
- When you find a row that you don't need, stay on it and click the traffic-light icon. You will see "**rem** " before item. OK, this program is paused and it does not load with your next start of the computer. To resume, click on the traffic-light icon again or delete "**rem** " manually. We recommend you proceed carefully and do not delete any lines. Remark it!
- To undo your last changes, click the reverse icon or press CTRL+Z. Only one change will be undone!
- If you want to insert a new program click on the open icon.

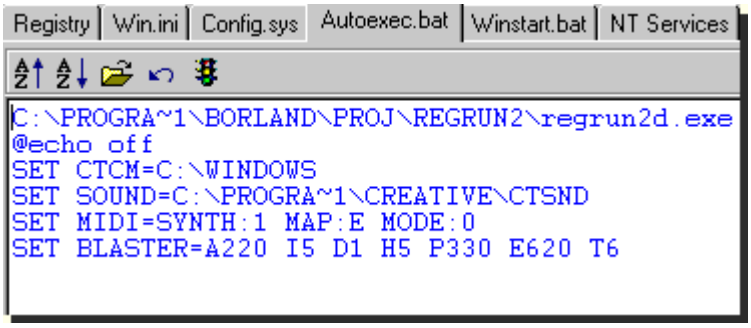
- You may use the clipboard with the editor.
  To copy - CTRL+C or CTRL+Insert.
  To cut - CTRL+X or Shift+Del.
  To Paste - CTRL+V or Shift+Insert.

  Don't forget to **save your changes**!

  Press F2 or click on the diskette icon to save.

  RegRun warns you if you try to exit without saving your changes.

Autoexec.bat page



Autoexec.bat is an especially important file for MS-DOS. In Windows 95 and Windows NT, this file is less used and exists only for backward compatibility. However, you may run some programs before loading the Windows GUI. Inspect this file carefully. We recommend the using a minimum number of programs in autoexec.bat.

Check all the files that you need.

- If you want to enlarge the font in the window, click on icon with an up arrow. You need to select the "Configuration" feature to make the size and font persistent in the editor.
- When you find a row you no longer need, stay on it and click the traffic-light icon. You will see "rem " before the item. OK, this program is paused and it does not load with your next start of the computer. To resume click on the traffic-light icon again, or delete "rem " manually. We recommend that you proceed carefully and do not delete any lines. Remark it!
- To undo last changes, click on the reverse icon or press CTRL+Z. Only one change will be undone!
- If you want to insert a new program click on the open icon.
- You may use the clipboard with the editor.
  To copy - CTRL+C or CTRL+Insert.
  To cut - CTRL+X or Shift+Del.
  To Paste - CTRL+V or Shift+Insert.

  Don't forget to **save your changes**!

  Press F2 or click the diskette icon to save.

  RegRun warns you if you try to exit without saving your changes.

Page winstart.bat

This is an obscure file. Many users don't know that Windows runs programs from it. Command syntax is similar to autoexec.bat. Normally, winstart.bat is empty. If you find any programs, be careful.

Page Startup Folder

This folder is located under the Programs folder.

Usually, at this folder you can see only "lnk" files. This is a link to an actual program.

You can select functions by clicking on the icon or choosing the item in the popup menu (right mouse button click).

1. Edit feature.
   You may see, for example, that a program called corners.exe is used.
   To inspect it, click browse button. After that select program, right mouse click and choose properties.
2. New.
   Press INS key if you use the keyboard.
3. To pause/resume/delete an item, click on the down arrow and choose the appropriate value in the popup menu.

Page Common Startup Folder

This page is active only in multi-user environments.

If you use Windows NT/2000/XP/Vista, it is the default. If you have Windows 95/98/ME, you need use "Control panel" to configure work in multi-user a environment.

All actions are fully alike with the "Startup group page".

Page Windows NT/2000/XP/Vista services

This page is useful for NT/2000/XP/Vista users and administrators.

RegRun shows the startup setting of WIN32 services.

Automatically loaded services are shown with a green light, manually loaded - with a yellow light, and disabled services - with a red light.

You can:

· set the startup of selected services.

· start or stop the selected services.

Select the item in the list and you will see a tip with information about the run status.

You can quickly run Event Viewer to inspect changes.

I addition you may use Sort feature for displaying services.

Run Once registry keys

The RunOnce subkey of HKEY_LOCAL_MACHINE\SOFTWARE or HKEY_CURRENT_USER\SOFTWARE stores the names of programs that Windows runs at startup the next time the system starts. When these programs are run, their names are deleted from the RunOnce subkey so that they are not run again automatically.

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce.
  Programs in this key run after the user enters his or her network password. All programs are common for all users on the computer.
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServiceOnce.
  Programs in this key run before the user enters his or her network password. All programs are common for all users on the computer.
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce.
  Programs in this key run only for specific users.

You can select function by click on the icon or choosing the item in the popup menu (right mouse button click).

Selection

To select more than one item use the key CTRL and Shift keys.

1. Hold the CTRL key and click on the items by turns.
2. With the Shift button you can quick select many items.

Click on the first item.

Press Shift and hold it.

Click on the last item.

All features list.

1. Edit feature.
2. New program feature.
   Press INS key if you using the keyboard. Fill in the form and Click on the OK button.
3. Run. Launch the application associated with the registry key.
4. What's this feature.
5. Explore location. Shows the folder or registry key that contains the item.

RunEx

Windows 98 (and Windows 2000) includes the RunOnceEx and RunEx registry keys for additional functionality of Run registry keys. The syntax and format used for these keys is different from the RunOnce and Run keys.

Sample Syntax

Note that text in braces ({}) are strings generated by the user.

The following keys are located in the Local_Machine and/or Current_User hive(s).

SOFTWARE\Microsoft\Windows\CurrentVersion\RunEx

-or-

SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

Flags = 0x0000000

Title = "{Status Dialog Box Title}"

Depend\

{PlaceHolder1} = "{DLL/OCX Filename}"

{PlaceHolder...} = "{DLL/OCX Filename}"

{SectionPlaceHolder1}\

Default="{SectionName1}"

{Entry1} = "{EntryFormat}"

{Entry...} = "{ntryFormat}"

Depend\

{PlaceHolder1} = "{DLL/OCX Filename}"

{ceHolder...} = "{DLL/OCX Filename}"

{SectionPlaceHolder...}\

Definition of Values and Subkeys

Name: Flags

Value Type: DWORD

Value Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\

Description: Contains setting to enable or disable certain functions of the RunEx or RunOnceEx key.

Value	Function	Function definition

0x00000000 Default All functions are disabled

0x00000001 Delete Delete registry entries after processing them ((normally only RunOnceEx)

0x00000002 Wait Causes items to be run synchronously

0x00000004 Check Shell Status Verifies that the shell is ready to accept OLE commands

0x00000008 No Error Dialogs Error dialog boxes are not displayed

0x00000010 Create Error Log File Create C:\Windows\RunOnceEx.err file if errors occur

0x00000020 Create Execution Log File Create C:\Windows\RunOnceEx.log file with status of commands

0x00000040 No Exception Trapping Does not trap exceptions that occur when registering DLLs

0x00000080 No Status Dialog Status dialog box is not displayed while RunOnceEx runs

0x00000100 Ignore Flags Flags registry key is ignored

These values are additive.

Example

If you want to create an error log and have no status dialog box, you would set Flags = 0x00000090 (0x0000010 + 0x00000080 = 0x00000090)

Name: Title

Value Type: STRING

Value Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

Description: This value fills in the Status Dialog Box Title

Key Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\Depend

Description: Contains values that point to DLLs that should be kept loaded in memory while all sections of RunOnceEx are being run.

Name: {PlaceHolder1}

Value Type: String

Value Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\Depend

Description: Contains a DLL or OCX file name with or without the path to the file. The text "{PlaceHolder1}" can be any valid

registry value name.

Key Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\{SectionPlaceHolder1}\

Description: Contains entries to be run. Sections are run in alphabetical order. The text "{SectionPlaceHolder1}" can be any valid registry key name.

Name: Default

Value Type: STRING

Value Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\{SectionPlaceHolder1}\

Description: The text "{SectionName1}" can be any valid registry value name.

Name: {Entry1}

Value Type: STRING

Value Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\{SectionPlaceHolder1}\

Description: The text "{Entry1}" can be any valid registry value name. This value contains the string that is actually run.

Format: "<DllFileName>|<FunctionName>|<CommandLineArguements>"

Example:

"Line1" = "||my.exe -quiet -url http://www.microsoft.com/"

"Line2" = "shdocvw.dll|DllRegisterServer"

Line1 runs the command line "my.exe -quiet -url http://www.microsoft.com/" and Line2 runs the DllRegisterServer function in

Shdocvw.dll.

Key Path: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\{SectionPlaceHolder1}\Depend

Description: Contains values that point to DLLs that should be kept loaded in memory while only this particular section of

RunOnceEx is being run.

VxD and Drivers

Why do we need to know about VxD and drivers?

VxD drivers work as part of the operating system and they have absolute power.

A lot of serious problems may be resolved by managing these drivers.

RegRun gives you the unique possibility to get full control of your computer.

Note: If you **are not a computer specialist**, we recommend that you do not change anything.

We recommend that you make a copy of your registry, system files and disk information before making any changes!

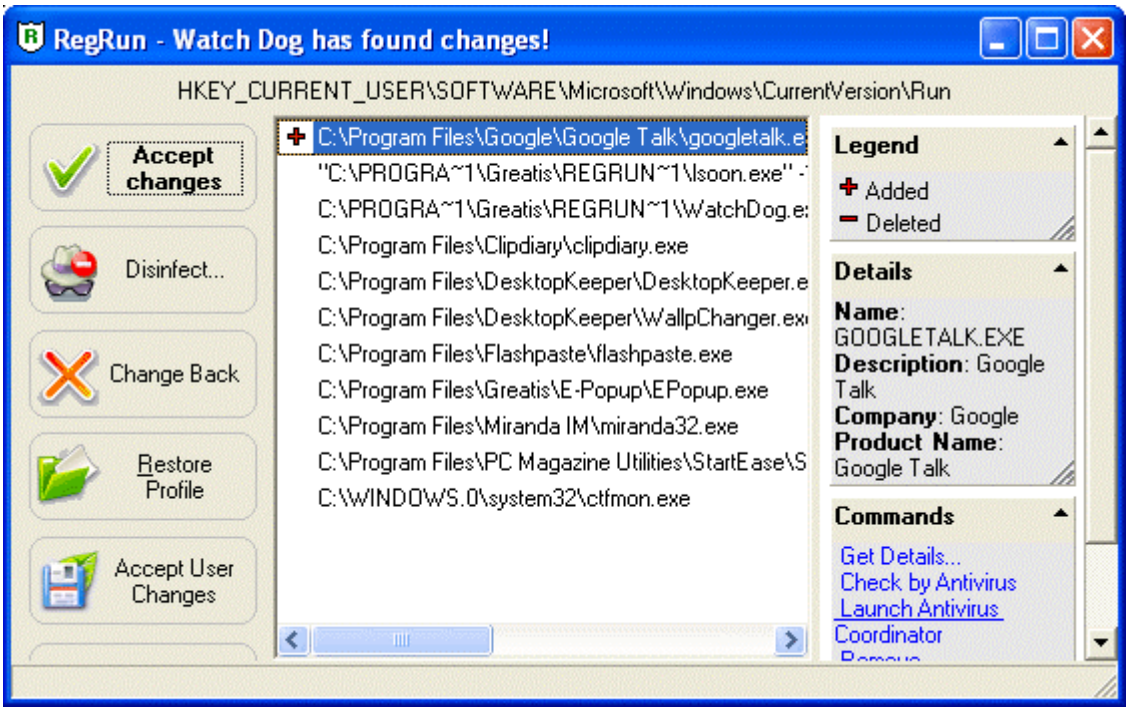
- With Windows 9X/ME, RegRun shows currently loaded VxD modules.
- With Windows NT/2000 RegRun displays the list of currently loaded drivers.

RegRun allows you to monitor changes of this list and warns you.

You should set the **Security Level** (Configuration screen) to **Ultra High Level** to automatically turn on the monitoring of VxDs. When you use the High Level of Security, RegRun only displays the list. If you choose Low Level, you will see no VxD tab.

Note! Don't afraid if Watch Dog popups often. Windows loads a lot of VxDs dynamically.

Use WatchDog Exclusions to skip unwanted popups. Click on the "Scissors" icon.



Look at the example of VxD list:

```
Name      Type    Source       Version VxD ID  In
ACPI      Static  UNKNOWN        040A    0000
AFVXD     Dynamic AFVXD          0000    0001   REG
AGENTCD   Static  agentcd.vxd    0100    0000   REG
AMDIDEPM  Dynamic Amdeidepm.vxd  0100    0001   IOSUBSYS
...
```

The **Source** column displays the file name that contains the VxD.

It may be a standalone file or VMM32. Unfortunately, sometimes RegRun can't find the location of a dynamic VxD. This is a problem, but Windows doesn't give us this information.

The **In** column informs you about the place where the VxD is registered. It may be the Registry (system.ini and registry) or IOSUBSYS folder(C:\WINDOWS\SYSTEM\IOSUBSYS\).

You can edit the registration by double clicking on a selected item or via the context popup menu or by the toolbar button.

Click the "Diskette" button to export the list into the text file with comma delimiters. You may use Microsoft Excel or Notepad to view it.

Click the "Printer" button to print the list.

The "Question": button is used to show you more information about a VxD.

The "Event log" button shows the Bootlog.txt (Windows 9X/Me) or Event Viewer (Windows NT/2000/XP/Vista).

Note:

You may easily sort the table by clicking the header of a column. Use the first letter to quickly find items.

What is a VxD?

Microsoft tells:

"A virtual device is a program that manages a system resource (such as a hardware device or installed software) so that more than one application can use the resource at the same time. Windows uses virtual devices to allow multitasking for Windows-based applications. The virtual devices work in conjunction with Windows to process interrupts, and carry out I/O operations for a given application without disrupting the execution of other applications."

VxD modules are very important for the normal operation of Windows.

Brief issue about VxD to help you understand the VxD list.

Windows 9X/ME supports static VxDs that load during system startup and it also supports dynamically loaded VxDs. VMM32.VXD includes the real-mode loader, the executable Virtual Machine Manager, and common static VxDs. Notice, however, that if a VxD file is in the Windows SYSTEM\VMM32 directory, Windows 95 loads it in addition to the combined VxDs.

Note! If you want to update a VxD that has been bound into the monolithic VMM32.VXD, place the VxD file in the SYSTEM\VMM32 directory. Windows always checks that directory and uses any individual VxDs it finds instead of loading those bound in VMM32.VXD.

The following list contains the VxDs typically combined to create VMM32.VXD. (A custom list is built for each computer.) These drivers used to be specified in the [386enh] section of SYSTEM.INI.

Typical VxDs Combined to Create VMM32.VXD

*biosxlat

*configmg

*dynapage

*ebios

*ifsmgr

*int13

*ios

*parity

*reboot

*vcache

*vcomm

*vcond

*vdd

*vdef

*vfat

*vfbackup

*vkd

*vmcpd

*vmouse

*vmpoll

*vsd

*vtdapi

*vwin32

*vxdldr

VMM32 loads VxDs in three steps:

VMM32 loads base drivers specified in the Registry, which contains entries for every VxD not directly associated with any hardware. VxDs are located in this branch of the Registry:

Hkey_Local_Machine\System\CurrentControlSet\Services\VxD

If VMM32 finds a value StaticVxD= in any Registry key, it loads that VxD and runs its real-mode initialization. For example, the following entry loads *V86MMGR:

SYSTEM\CurrentControlSet\Services\VxD\V86MemoryManger

Description=MS-DOS Virtual 8086 Memory Manager

Manufacturer=Microsoft

StaticVxD=*V86MMGR

EMMEXCLUDE=E000-EFFF

VMM32 loads the static VxDs specified in the device=*VxD lines in the [386enh] section of SYSTEM.INI. These VxDs are actually loaded from VMM32, and appear in SYSTEM.INI only for backward compatibility.

If a specific device conflicts with a device loaded from the Registry, the device specified in SYSTEM.INI takes precedence. However, if the device specified in SYSTEM.INI cannot be found, an error will occur.

Many Windows driver models, such as IOS (for disk drivers) and the network, support dynamically loaded device drivers. These VxDs are not loaded by the VMM32 real-mode loader, but are loaded by a device loader that is responsible for loading and initializing the drivers at the correct time and in the correct order.

For example, for SCSI adapter miniport drivers, the device loader is *IOS. The entries for a SCSI adapter are found in this Registry key:

Hkey_Local_Machine\System\CurrentControlSet\Services\Class

Because there is no StaticVxD=xxx line in this Registry entry, the VMM32 real-mode loader does nothing when Windows 95 identifies this device.

Configuration Manager attempts to find any device node that has a DevLoader= entry in the Registry. The device loader (in the previous example, *IOS) examines the Registry, finds the PortDriver= entry, loads the driver and any associated support drivers, and initializes the adapter.

Windows Core

Why do we need to know about VxD and drivers?

Windows Core Components includes "Active Setup items", "Browser Helper Objects", "Shell Loggers DLLs", "Static VxD" (Windows 9X/Me only) and "Shell DLLs". These components are very important for stable Windows work. You should have administrator privilege to modify these components. Anyway, we suggest you make a backup copy before doing any changes. We give you a simple way to make backup.

Active Setup registry key is used to store information about installed software components and to automatically launch downloaded ActiveX components.

Some examples of the viruses/Trojans that use this method:

SubSeven Trojan, Trojan Oblivion, Backdoor.SchoolBus, I-Worm.Badtrans, etc.

Read more...

The **ShellExecuteHooks** registry key contains the list of the COM objects that trap execute commands.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\ShellExecuteHooks.

Value Name is the GUID of the COM object.

RegRun automatically determines DLL references to the COM server and displays it in the Program column.. By default you must have the "**shell32.dll**" item. **Never delete this item!**

Other objects in this list are not required and may contain viruses and Trojans.

Browser Helper Objects are the COM components that Internet Explorer will load each time it starts up. For example, a BHO could spy all browser events, access the browser's menu and toolbar and make changes, create windows to display additional information, etc.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Browser Helper Objects

Each subkey of the main key contains information about COM components.

By default the BHO list on your computer is empty. There are no required items.

Shell DLLs.

The registry key called "ShellServiceObjectDelayLoad" is used to automatically load DLL related to Microsoft Explorer.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

Each value under this key contains the GUID to the COM objects or to the DLL name. The system will load all DLLs and link them to "explorer.exe" process.

The number of the DLLs used by Explorer is different in different Windows versions.

- Windows 95 and Windows NT4 do not use this key;
- Windows 98/2000 includes only "WebCheck" value. We suppose that the purpose of the "Webcheck" is checking of the Internet Explorer auto updating. Explorer works well without "Webcheck" value.
- Windows XP adds several additional values.

To keep your safety we suggest you to remove all values not related to Microsoft.

VxD tab is visible only under Windows 9X/Me.

"VxD" stands for Virtual "something" Device, where 'x' stands for "something".

Microsoft often names drivers according to this convention, thus "VKD" is the Virtual Keyboard Device. VxDs are loaded into the protected (ring-0) operating system address space, and have full access to the system hardware.

Static VxD are loaded automatically at Windows startup.

Please, do not change required VxD.

Several advanced viruses and Trojans install their own VxD modules to infect your computer.

Remember!

VxD modules work as part of operating system and they have absolute power.

RegRun analyses information about each listed item and displays it on the left pane of the Windows Core window.

In addition to information stripped from the file, RegRun uses Application Database.

Columns description:

1) Type (Necessary/Useless/At your option/Dangerous.)
2) Value Name (Usually this is a unique identifier.)
3) Program/DLL name.
4) Manufacturer (extracted from execution file, may be empty.)
5) Product Name (extracted from execution file, may be empty.)

Tip!

If you have installed **RegRun Gold Edition** you may automatically **monitor changes** in Windows Core Components.

Click on the "**Monitor Key**" link.

Monitoring of the Active Setup Registry Key

What is the Active Setup?

Why monitor this key?

Microsoft uses this key to setup installed Windows components.

You can see a list of the installed components under the key

HKLM\Software\Microsoft\Active Setup\Installed Components

You should launch RegEdit to view it.

As you can see, the registry key of each component has a list of values.

These values are used by Windows to identify a component.

One of these values, **StubPath,** is very important.

This value includes a command that Windows executes every time it starts if a value called "IsInstalled," is not set to 1 (binary value).

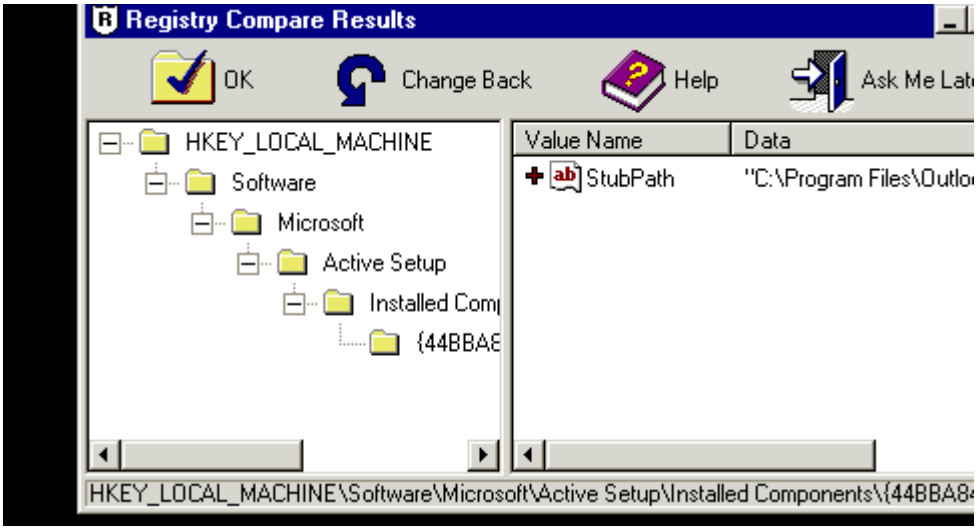
Active Setup is used by new Trojans to install them to the computer.

This is very dangerous because then Windows launches the Trojan **before** other programs ARE loaded.

RegRun will help you!

RegRun saves a copy of Active Setup key and traces the changes.

You will see a picture like this:



On this picture you can see that the StubPath value was added to the key.

Inspect the contents of the StubPath value.

If you have any doubts, contact us to get support.

You have three choices:

1) Accept the changes (OK);
2) Decline the changes (Change Back);
3) Close this Form (Ask Me Later.)

Do not be afraid if you see this window when you change a collection of Windows components. This is normal. Simply click on the OK button.

You can disable the monitoring of this key by RegRun Control Center.

Open Security tab, choose Registry Tracer. After that set/reset the "Check Active Setup Registry Key" checkbox.

RegRun automatically activates monitoring of the Active Setup key if you have chosen "Ultra High Level" or "High Level" of your security level on the Security tab.

Substitution Detector

What for?

This is a very effective tool detecting "masked" Trojans.

These Trojans use the same names as the legitimate programs, but are located in different folders. As a result a user does not suspect deception.

For example: "explorer.exe" is always located in the Windows folder.

The dangerous program can use the full names "c:\windows\system\explorer.exe".

Do you want to know more?

You see: *"explorer.exe"* in the Windows startup. You have two files with "explorer.exe" name. One in the Windows folder and other in the root of drive C.

Which file will be executed? You would be surprised but sometimes the first will be "c:\explorer.exe". This error was fixed in the later Windows versions. But you should be sure that you launch a file that you want to execute.

How it works?

Substitution Detector uses information about the right location of the often-attacked filenames. It compares the real path to the executed file with the stored file path. If they are not equal the user is notified.

How to remove Trojan?

A user has an option to fix the problem. The fixing changes the path of the startup file to right path. Restart the computer is required.

The Trojan program will not be launched at the next Windows startup.

Problems?

If the Trojan program is running it can detect the changes in Windows startup and come back again.

Click on "More Info" button to check if a process is running.

Click on the "Stop it" button to kill a process.

After that you can delete the Trojan by Windows Explorer and fix the substitution problem.

Click on the "Fix it!" button.

Startup Optimizer

Using Startup Optimizer

Startup Optimizer is the handy tool for **newbies and professionals**.

Startup Optimizer allows removing useless and dangerous applications from Windows startup **by one click**.

A user can start Startup Optimizer via Start menu, Control Center or via WatchDog menu.

Startup Optimizer collects full information about startup files. It analyses information included into the execution file and RegRun Application Database reference.

1. Type (Necessary/Useless/At your option/Dangerous.)
2. Value Name. This may be the registry or ini file value name.
3. Section (RegRun tab name where this value is located.)
4. Application Status (Running in memory/Stopped/Not Found.)
5. Manufacturer (extracted from execution file, may be empty.)
6. Product Name (extracted from execution file, may be empty.)
7. RegRun Application Database description (if application exists in the database.)

Startup Optimizer automatically unchecks **useless and dangerous** applications.

A user can simply press Apply button to accept changes.

When applying changes RegRun tries to kill application in memory if this application is working, after that it changes its auto start status to "Paused".

Startup Optimizer works very carefully.

Startup Optimizer saves startup profile before optimizing and allows to a user possibility to restore this profile later.

Additional commands

1. *Display command line*. Shows the full command line for selected application. May be useful to check application parameters.
2. *Know more?* Gets additional information about selected file: file size, date, time, attributes.
3. *Stop it!* Kill a program in memory. Command is available only if application is running.
4. *Auto Start On/Off*. Check or uncheck auto start of this application.
5. *Delete File*. Erase file from hard disk. The program must be stopped before.
6. *More commands*. Displays Windows context popup menu for this file.

Note!

If an application does not exist on your hard disk Startup Optimizer will color Value Name and Status fields red. Startup Optimizer doesn't unmark this application but it notifies you about it. A user should check Command Line to get a right solution.

Scan for Viruses

Search and Remove Rootkits/Trojans/Spyware/Adware

Purpose

Allows users to quickly detect and remove any Spyware, Adware, Trojan or virus.

What is Spyware? What is Adware? What is Trojan? What is a virus?

User can launch Anti-Spyware via Start Control, by Control Center or by WatchDog menu.

How does it work?

Anti-Spyware collects information about potential security holes and analyses results. It inspects Windows startup, Windows kernel drivers, services, Windows Explorer, and Internet Explorer, and ICQ software, etc.

Anti-Spyware uses two types of information:

1) Security Settings.
It suggests how to configure software to eliminate security holes.

2) Program information.
Full information about files using the potential security holes.

How to detect spyware?

Anti-Spyware displays the full list of security items. Suspicious items are located at the top. They have different colors:

1) Red – dangerous.

2) Yellow – need carefully looked at.

3) Light yellow – look at these items, they are probably O.K.

Anti-Spyware shows a hint to each item in the bottom panel.

Removing spyware

Click on the "Fix Problems" button.

You will see a new screen with context menu on the right side.

The menu is different for each item.

Usually you have three choices:

1) Reset to default. Sets a value to default state.
Default value is chosen by Greatis Software experts.

2) Delete. User can delete an item from the list.

3) Ignore. Adds an item to Ignore list.
User can always modify the Ignore List.

Safety

Anti-Spyware automatically backs up all information to the backup directory which is created automatically before any changes are made. Later a user can restore a backup by choosing the "Restore Backup" item in the File menu.

A user can create a new backup at any time by choosing "Make Backup" item in the File menu.

By default the backup folder is located in "My Documents\RegRun2\Backup…"/

How to delete infected files?

Anti-Spyware does not delete infected items.

If you can’t delete it use RegRun Process Manager or consult support.

Need clarification?

If you have questions you can ask RegRun’s staff.

Open RegRun Start Control, go to Reports menu, choose "Detailed System Report". It contains the same information as the Anti-Spyware module. It can be read in any text editor.

Visit our support center:

http://www.greatis.com/support

Open a new ticket.

Describe your problem.

Attach the system report text file.

Tips

A user can mark any items by checking the first column. After that it is possible to use a command in the menu item to change all marked items at the same time. Note, that if a command can not be applied to an item it will be ignored.

Scan for Viruses/Rootkits/Trojans/Adware/Spyware

Important!

"**Scan for Virus**" is not complete hard disk scan. Otherwise to standard antivirus disk scan, "**Scan for Virus " collects information about all files used during Windows boot-up process**.

"Scan for Virus" uses Greatis Application Database to detect which files are useful or dangerous. **Unknown files are marked as suspicious**. These files may be legitimate or not

How to detect the status of these files?

1. Click on the "**Good or Bad**" button. The file will be automatically checked for Microsoft digital sign. Most of Microsoft files are signed.
2. Check the manufacturer of the file. If it is a part of legitimate software, click on the "**It's OK**" button.
3. Contact the Greatis Support for testing the files. It's very useful for you because the description of the file will be added to the next version of Application Database.
4. Google the file name.
5. If the file is hidden or doesn't exist, probably it's a **rootkit**. Hidden rootkit files may be deleted only after reboot.

Why the Scan at reboot is preferred?

"Scan for viruses" on the working computer is not effective, because the rootkit already hide their files and registry keys.

Scan at reboot activates Partizan boot anti-rootkit technology for monitoring Windows boot process. In addition, Scan at reboot will be activated before Windows shell starts and most of rookits started from the "Active Setup", "Run" registry keys will be visible.

Scan at reboot uses Partizan information for detecting and removing rootkits.

Why the Scan detects the rookit drivers again after killing and reboot?

It's **normally if you reboot 2-3 times** to completely remove a rootkit.

You need understand that if a rookit uses boot driver, Partizan can delete the service key and the file at reboot. But the rookit driver may be already in memory. You need to simply reboot again if you find that the file remains in the Drivers section.

Custom Startup Profiles

Profiles

RegRun allows you to save your configuration to a special file - the RegRun profile.

This is a file that has an "rr2" extension and icon:

RegRun profile includes:

1) Registry keys:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run-
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices-
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run-
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunEx

2) Files:

- autoexec.bat (autoexec.nt)
- config.sys (config.nt)
- win.ini
- system.ini
- winstart.bat

3) Shortcuts in folders:

- Startup folder
- Disabled Items in Startup folder
- Common startup folder
- Disabled Items in Common startup folder

How to create a profile?

1. Run Start Control.
2. Open File menu and choose "Save profile as...".
3. Assign any name and click "Save".

RegRun automatically includes this file in the profile list.
The profile list contains the last twenty saved profiles.

How to restore a profile?

1. Run Start Control.
2. Open File menu and choose "Open profile..." (or press CTRL+O).

On the left pane you can see the current profile list.

1. Select the row and click right mouse button to get popup menu.
2. You have a choice:
   a) Read profile directory
   b) Open profile from another location.
   c) Create shortcut to profile on the Windows desktop.

d) Copy profile to floppy disk or another location.

e) Delete it.

f) Show backup copies (RegRun automatically saves nine previous versions of the main profile - regrun2.rr2. File names begin with "backup" string).

3. If you selected the "Read Profile," you will see the profile directory on the right pane and the button "Restore" will become enabled.

4. Be careful! Check the box "Clear all before restoring".

a) If this box is checked the RegRun clear all registry keys, files and directories before restoring.

b) If the box is unchecked the restoring process will overwrite the current contents. This is useful if you want to restore some items. In this case, uncheck all unnecessary items in directory.

5. Click the "Restore" button.

6. RegRun asks you to restart your computer.

This is necessary so that the changes will come on.

Notes:

1) RegRun automatically saves your configuration in profile"regrun2.rr2" when you save your work. The other name of this file is "Last Known Good." The "Last Known Good" profile is used by Secure Start to restore the configuration.

2) RegRun automatically saves the current configuration in the profile "Undo.rr2" before restoring.

It helps you to restore the previous condition.

This file is not included in the profile list, but you can open it from for the disk. It is located in the RegRun directory.

Tips:

1. If your computer works fine, then save the profile with the name, "Successful Configuration" and leave it. If you have trouble later, then you can restore it.

2. Pause all items excluding system utilities and save it to the profile "Clean Configuration." This can help you to diagnose problems.

Clean Boot

Clean Boot

Why do you need it?

Clean Boot allows you to load in **really** clean Windows.

Clean Boot works in two modes:

• DOS

• Windows

To use Clean Boot DOS you need to activate Secure Start DOS.

Clean Boot for DOS is available only for Windows 95/98.

Clean Boot DOS works during DOS mode (autoexec.bat).

Clean Boot for Windows is available for Windows 95/98/ME/2000/XP/Vista.

Run Start Control, choose it in the main menu File->Go to Clean Boot.

When you want to restore to the previous state, RegRun will automatically offer to restore the Last Known Good profile.

Watch Dog

Watch Dog

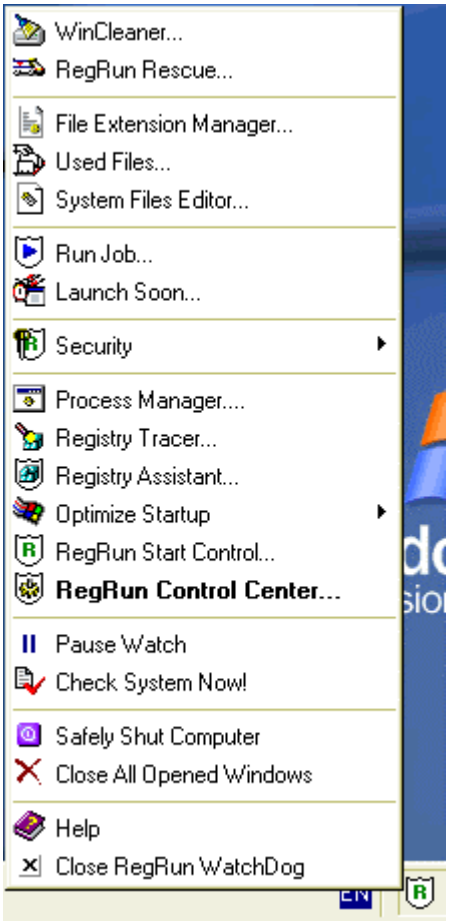
"***WATCH DOG***" - Provides silent monitoring of the startup managers during your Windows working session. Watchdog may be configured to check the startup managers at Windows startup, Windows shutdown, and as recurrent check with specified time interval. If one of these scans detects a change, you are notified with a popup window and a start up of Start Control, along with the option to restore the affected file. WatchDog operates only in the windows mode.

To start Watch Dog select Medium or High or Ultra High Security Level in the RegRun Control Center Security.

After that you will see a small icon in system tray.

If you move mouse pointer on the icon, you will see the Watch Dog information.

Click right mouse button on the icon:



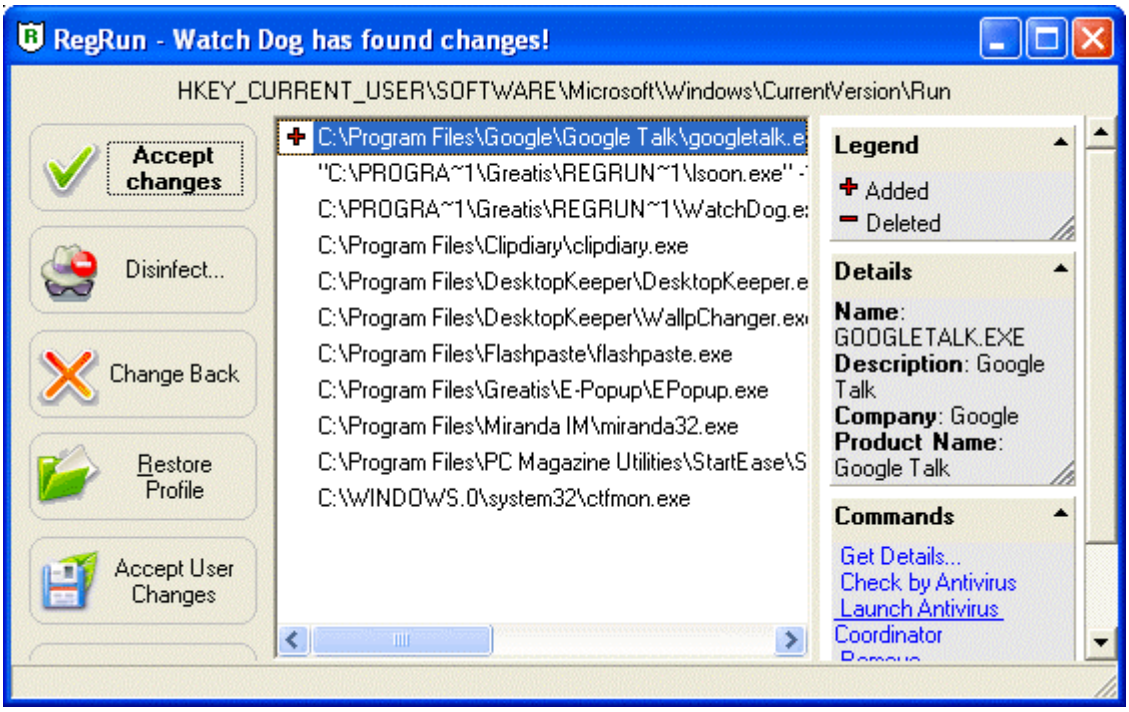
If you want to close WatchDog, use the command line:

watchdog.exe /k

Watch Dog will notify you if it finds any changes.

RegRun Watch Dog found changes

1. If RegRun WatchDog has detected changes to your registry or startup files, you will see a window similar to this:



2. The sign "+" marks lines which have been added.
3. The sign "-" marks lines which have been removed.
4. Look at the top line of the window. This shows where the change has been made.
5. You can choose what action to take:

- **Change Back.**. This will cancel all of the changes. Any added lines will be removed and deleted items will be restored.
- **Accept changes.** This allows you to accept the changes. RegRun will then accept them and will not refer to them again.
- **Restore profile.** You can restore your RegRun profile by clicking on Change Back.
- **Accept Made Changes.** It allows you to modify and then save the current list manually. If you select this choice, press "Enter" or the "Edit" button. Then, after making any edits, select "Save".
- **Ignore**. Selecting "Ignore" will result in no action being taken. The next time you boot up, the program will detect the same changes again and warn you of them again.

Tip! You can customize exclusions to permanently ignore specified programs.

Click **Yes**, when you are asked to setup.

Enter a program name, for example "washidx.exe".

Select "**Include phrase**" and click Save.

- You can setup exclusions for NT services. Change "Files" to "NT Services" in the top combobox.
- Also you can setup exclusions for Anti Replacement checking. Change "Files" to "Anti Replacement" in the top combobox.

To manage the list of exclusions, select "List" tab.

Right click on the list to get a popup menu with commands: New, Edit, Remove.

Additional functions:

- Information about selected item;
- System popup menu for selected item (as shown on the picture);
- Edit;
- Suspend run;
- Launch Antivirus.

Using Black List

RegRun Black List feature works only with the Pro and Gold version.

Black List allows automatically filtering newest detected startup tasks. Tasks listed in Black List will be automatically blocked.

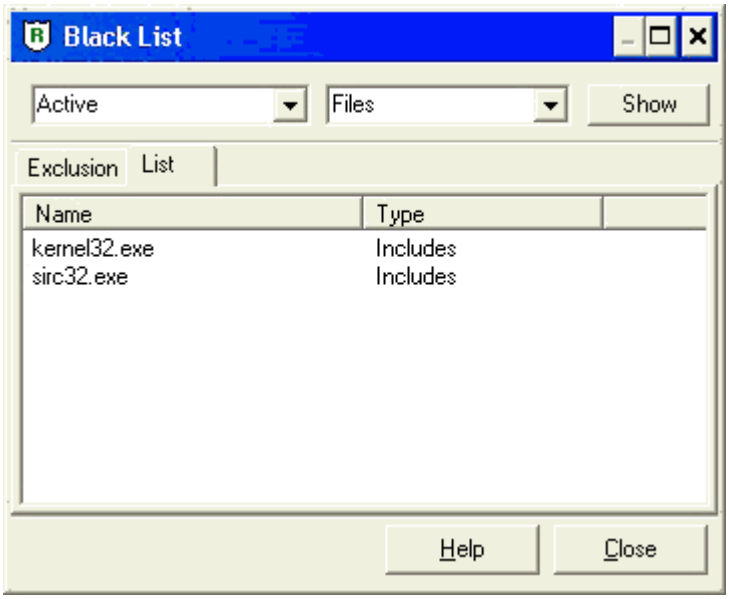
This feature is very useful to get rid of unwanted WatchDog popups and to improve your security.

You may automatically block all new startup tasks or create your Black List.

Open RegRun Start Control->Features->Black List.

Select operation mode:

- **Not Active**
- **Active** (uses your list)
- **Block All New Founded** (blocks all new found startup tasks and services).



We suggest to you "Block All" option if you do have a stable version and don't want to install new software. Also this mode will be useful for newbies who have problems with using WatchDog main window.

RegRun will automatically set all new founded startup items to the disabled (paused) state. Later you may quickly restore auto starting of these items.

Note!

Be sure, that you set "Active" or "Block All" option before using Black List.

You may inspect History Log to view filtered operations.

Open RegRun Start Control, go to File menu after that choose "Show History Log".

Secure Start

Secure Start Windows

Why do you need this?

Notice to current users: Secure Start has been significantly altered, and works with Windows 98/2000/ME/XP/Vista before other programs are launched. This is a superb feature, which, in addition to providing protection from malicious ware, allows you to choose your startup profile AS YOU ARE LOADING - WITHOUT HAVING TO RESTART.

To activate Secure Start, you must first:

Open RegRun Control Center, Options and choose the Secure Start tab.

Window 2000/ME/XP/Vista users: mark the checkbox "Check Startup in Windows mode BEFORE Windows Shell starts". Secure Start activates after you logon to your system and checks for changes in your startup. If any changes are found you will be notified.

Through this validation, you can prevent a dangerous program from starting.

Non-W2k: Win95/98/SE users should select the DOS mode, and set a delay for activating Secure Start. This delay period occurs during the DOS boot up process, and provides you a period to access RegRun features BEFORE Windows.

Note: Secure Start is automatically activated if you selected "High" or "Ultra-High" Security Level.

Secure Start DOS

Why do you need it?

Secure Start works in DOS mode and consists of six utilities:

1. WatchDog;
2. Startup Items editor;
3. Feature to restore Startup Profiles;
4. System files editor;
5. Feature for password protection of Windows;
6. Feature to Save or Restore Registry (Windows 98 only) or launch any DOS program.

Many of these utilities are very useful for experienced users but everyone needs some of them. Read more details about each feature.

WatchDog

WatchDog is your spy into the hidden side of Windows.

In the early stage of Windows startup there are many hidden operations that may be very important to you. But the Windows hides it behind the logo curtain.

Do you want to know about it? WatchDog tells you.

On the first stage of startup the Windows processes the "wininit.ini" file that is located in the "Windows" folder. The structure of "wininit.ini" is similar to other "ini" files.

It has one section [Rename] and any quantity of rows.

A simple example of "wininit.ini":

[Rename]

C:\WINDOWS\system.bak=C:\WINDOWS\system.dat

C:\WINDOWS\user.bak=C:\WINDOWS\user.dat

C:\WINDOWS\system.dat=C:\WINDOWS\system.pak

C:\WINDOWS\user.dat=C:\WINDOWS\user.pak

This file was created by the Microsoft Scanreg utility. The file on the right side is copied to the file on the left side. If on the left side you see "NUL," the file will be deleted. The "system.dat" and "user.dat" files are called "The Registry", i.e. the Microsoft utilities often use the wininit.ini file to modify very important files!

OK! The Microsoft utilities work well, but what do you think about others? Very often the new program that you've installed asks you to reboot the computer. Probably, it needs to replace a system DLL, font or a do something else.

Be observant. As you observe these actions, you will begin to understand.

Note! Windows renames the "wininit.ini" to "wininit.bak" after processing is complete.

Unfortunately, installation programs need more than "wininit.ini".

In many cases, it is necessary to launch special programs. And these programs

use Windows(not DOS) long file names, Windows API etc.

The Windows has the two registry keys for this purpose:

1. "HKLM\Software\Windows\CurrentVersion\RunServicesOnce".

The programs in this key run before the user logs on to the system.

2. "HKLM\Software\Windows\CurrentVersion\RunOnce".

The programs in this key run for every user in the system.

The programs will be launched only once!

After a successful launch, Windows clears the keys.

Unfortunately, any of the programs that start from registry keys may hang and lock the system, because Windows can't continue loading when a program doesn't finish.

You have no remedy other than loading in Safe mode and deleting keys manually.

WatchDog will resolve these problems!

To get know how to do it, read the chapter "Usage Secure Start".

If you know that the items was deleted during this session, you can

find it later in the files: disonce.reg and disonces.reg. So you will have

a chance to restore it if you want.

Using Secure Start DOS

If you configure RegRun to activate Secure Start, you will see this picture when Windows starts.

1) If Secure Start detects no content in RunOnce and wininit.ini, it will bypass the open window. You can optionally open that window by pressing Spacebar.

2) If you want to activate Secure Start, press any key except Spacebar or ESC.
3) Press ESC to exit.

Wait, while RegRun scans the files and registry.

If WatchDog finds any changes you will be prompted to manage it.

After that you will see a menu of utilities.

- Startup Items;
- Startup Profiles;
- System Files;
- Password/DOS command;
- Antiviral Software.

"Startup Items Editor"

Windows uses three registry keys to launch programs.

You may select:

- ❖ HKLM\Microsoft\Windows\CurrentVersion\Run (F3)
- ❖ HKLM\Microsoft\Windows\CurrentVersion\RunServices (F4)
- ❖ HKCU\Microsoft\Windows\CurrentVersion\Run (F5)
- ❖ HKCU\Microsoft\Windows\CurrentVersion\RunEx (F6)

The "Startup Items" editor shows all the programs that start from these registry keys. You get the full control on these items!

Del - allows to disable an item from starting

It has two cases: final erasing or suspending.

If you only suspend an item, it is later possible to resume starting of the program. Use RegRun in Windows mode for resuming.

- F2 - disable all items
- Enter - edit
- Insert - add new item

We presume that you have the advanced computer skills needed to modify registry keys.

But you need to remember these rules:

The name of key is located on the left side and always it has a forward quote and an end quote. The contents of the registry key are located on the right side and always have quotes. If you need to insert a backslash character, insert the double backslash character, insert a double backslash (\\). If you need to insert a quote, insert backslash and after that the quote (\").

Example:

"Norton CrashGuard Monitor"="\"D:\\PROGRAMS\\NORTON CRASHGUARD\\CGMenu.EXE\""

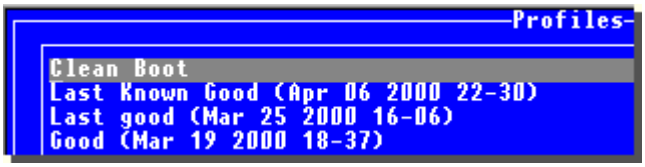
- To save and process changes - F10.
- To exit - ESC.

Startup Profile's editor

Startup Profile's editor is a unique and powerful feature.

It allows choosing the startup configuration before running Windows!

Startup Profiler is the best tool for resolving startup problems!



Please, remember these important rules for using.

1) Run RegRun in Windows mode and save changes.

This operation creates the file called "regrun2.rr2" that has the full information about the startup process. We give it a friendly alias "Last Known Good". If you don't have a "regrun.rr2" file, you can't use the "Clean Boot" feature. You can restore "Last Known Good" profile from DOS mode or from the Windows mode.

We recommend that you to save one more profile (in Windows mode) for safety.

The "Last Known Good" profile is rewritten every time when you save your work.

2) Run "Configuration" feature and choose page "Secure Start".

Activate this feature and click "Save". The RegRun creates the file "regrun2d.ini".

It is a very important file because it contains information about folders. There is no possibility to get long file names of the folders in DOS mode. And RegRun saves the short names of the folders in "regrun2d.ini".

Be careful!

If you change a user's configuration or reinstall Windows, you will need to repeat this operation.

3) RegRun works in Windows mode, and saves the list of the available profiles to "backlist.ini". RegRun in DOS mode reads this list and tries to open each file. If the file is valid, it adds the full name of the profile to the menu.

4) You can create any number of profiles while you are working with RegRun in Windows mode. After that you can restore any one in RegRun for DOS.

How does it work?

It's not magic!

RegRun for DOS creates the subdirectory "PROFILE" and extracts the files from the profile to that directory.

List of files:

- autoexec.bat
- config.sys
- system.ini
- win.ini
- r2repl.reg (modified registry keys)
- restrr2.bat - the main bat file for restoring.
- STARTUP directory contains the shortcut files. The names of these files are not real. The long file names will be created while processing "restrr2.bat".
- COMMON directory contains the shortcut files for all users.

Tip:

You can extract files from profile using the command:

regrun2d.exe profile.rr2

(Remember, you need to use the short names in the profile)

In this case RegRun for DOS creates all files for restoring but doesn't run it. Explore these files to know more.

After you've chosen the profile for restoring, RegRun extracts all files to the PROFILE directory, modifies the registry and adds a line with "restrr2.bat" to the "winstart.bat" file. Microsoft says that the users may use the "winstart.bat" to load special TSR programs. But I think the main advantage of "winstart.bat" is the possibility to use long file names and other advanced DOS functions. If you didn't know, the DOS program was specially designed for Windows, can use long file names just like any other Windows program.

"Password protection"

You can set password to Secure Start to improve security.

The feature has two modes:

a) Global password. You will be prompted to enter a password when your computer starts.

b) Local password. You will be prompted to enter a password when you access the edit mode of Secure Start.

You can select only Global or Local mode.

If you enter an empty password it will be disabled.

"DOS commands"

While using RegRun for DOS you can run a DOS shell or any other command.

If you have Microsoft scanreg (Windows'98) you can backup or restore the registry.

"Antiviral Software"

You can test your computer using any of the registered antivirus utilities.

Use RegRun Windows to register antiviral software.

"Editor commands"

F2 - save

CTRL+F - find string

CTRL+P - print

CTRL+Q - clear all

CTRL+Y - delete line

F4 - begin mark block of lines

F5 - end mark block

F6 - clear marking

CTRL+C - copy block

CTRL+V - move block

CTRL+K - delete block

CTRL+S - save block to file

Infection Detector

Infection Detector

RegRun uses special technology to search for viruses unknown to antiviral software.

This is not signature scanning, but rather "infection scanning". During a session, RegRun opens and monitors a number of "bait" program and macro files, which are vulnerable to infection by any active virus. If any of these files change, RegRun will advise you, and facilitate your communication with your antivirus supplier by providing you before and after samples.

If you activate DOS mode monitoring, RegRun inserts the command "bait.exe" into autoexec.bat. During Secure Start DOS, it compares "bait.exe" and "bait.org".

If you activate Windows monitoring, RegRun inserts the command "winbait.exe" into the Registry-All Users Run list. WatchDog compares "winbait.exe" and "winbait.org".

The files winbait.exe and winbait.org are located in the Windows folders. Many viruses try to infect execution files in the Windows folder.

If the "bait" files are not identical, RegRun warns you.

You can try to test bait.exe and winbait.exe by installed antivirus software.

If it doesn't help, send all bait files to antiviral company for a cure for the virus.

Open RegRun Control Center, Security, Infection Detector to set it up.

Infection Detector is *automatically* activated if you selected "High" or "Ultra High" Security Level.

Antivirus Coordinator

Antivirus Coordinator

Open RegRun Start Control. Go to the main menu, Antivirus, Coordinator.

Click on the "Auto Detect" button to detect many of the known antiviral programs.

1) Antiviral Toolkit Pro.
2) Norton Antivirus.
3) McAffe Virus Scan.
4) F-Secure.
5) PC-cillin.
6) Nod32.

If you have another antiviral software program, click the Add button and fill in the form.

To use registered antiviral software go to the main menu, Antivirus, "Launch Registered Antivirus".

If you use the Antiviral Toolkit Pro, RegRun will help you to do a fast test of the startup files or folders. RegRun creates special text file with file names and launches your AVP with this file. This is very useful because the testing of suspicious startup files is faster than full disk testing.

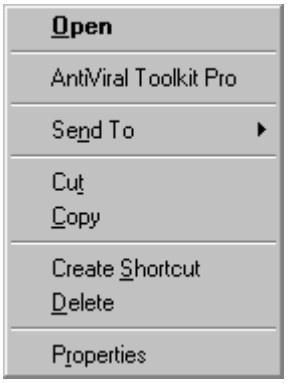
Unfortunately other antiviral software doesn't support command line options to test from a file list. But many of them use a "shell" command to test files or folders using Explorer.

RegRun supports shell commands like Microsoft Explorer.

Select any item and get a popup menu.

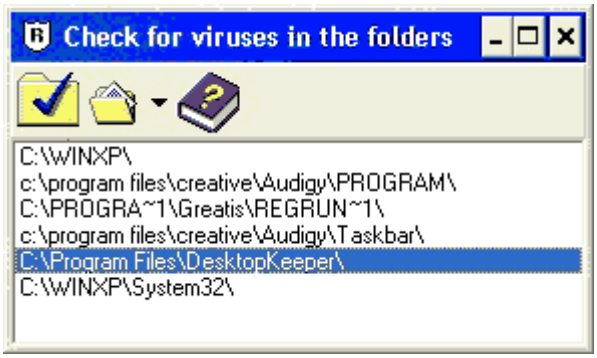
Select "Antivirus&Commands". You will get a system popup menu for executing a file.

For example:



You can use this technique in WatchDog!

To fast test the Startup folders, go to the main menu, "Antivirus", "Check for viruses in the startup folders".



Select a folder and click on the tick icon.

File Protection

File Protection

File Protection is one of the most useful functions serving to protect your computer from viruses, Trojans and malfunctioning programs. We strongly recommend that you the run file protection setting immediately. The sooner you do it, the greater the troubles you can avoid.

How do these troubles arise?

When you receive an email message, containing an interesting screen saver or an executable file, you can't help opening it. Of course, it may turn out to be a virus or a Trojan. Every virus tries to ensure its activity and life-support after the computer is re-started. RegRun is reliable in locating all the programs that try to launch automatically when Windows is starting. Unfortunately, a virus can use the techniques of system files substitution (DLL).

Will RegRun be helpful?

It most certainly will.

File wininit.ini(Windows 95/98) and registry key PendingFileRename (Windows NT/2000/XP/Vista) are employed to substitute files, permanently used by Windows.

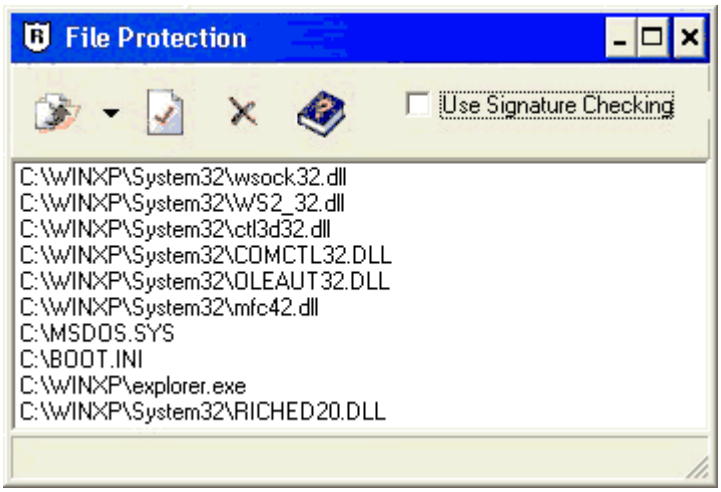
Be sure to mark "Check wininit.ini" checkbox in the Control Center, Options, Secure Start.

File Protection uses another protection technique.

The protected file is saved in the folder RegRun2\Files.

Check the box named "Enable File Protection" and activate the "Secure Start" option.

To select files, press the "Tune File Protection" button.



You can add any files for protection. We suggest you protect the most vital ones. Press the arrow button and select files in the scroll menu.

RegRun supports full file comparison or signature checking. If you check the box "Use Signature Checking" RegRun makes an MD5 signature of the source file and saves it. While comparing, it compares the original signature with a calculated signature. When you select an item in the list, you will see the current signature, if it is assigned. To apply a signature to a currently protected file, you must remove it from storage, check the "Use Signature Checking" box, and then add it again. You can copy the signature to the clipboard and save it in its own location (use context popup menu). The MD5 signature is commonly used to check the integrity of files. You may use freely available MD5 utilities to make a signature and compare.

Recommended protection:

Viruses often use Winsock (Socket API for Windows). By substituting Winsock, any virus can get control over your Internet access and do whatever it wants.

CTL3D 3D Windows Control Library, Common Controls library, Microsoft OLE library, MFC42 DLL lots of programs by exterior implementers try to substitute these libraries to provide their own working efficiency. Yet, as a rule, these programs don't check versions of libraries and substitute them anyway, even if a newer and better working version is already installed. As result, Windows operates slowly and/or malfunctions. Errors may appear while downloading and it may misrepresent some of the elements.

MSDOS.SYS is an important file for Windows startup.

When it is missing Windows cannot launch at all. In this case the standard error "VMM32.VXD not found" occurs. MSDOS.SYS contains paths to your Windows folder. Our recommendation is to have a copy of the file to secure yourself.

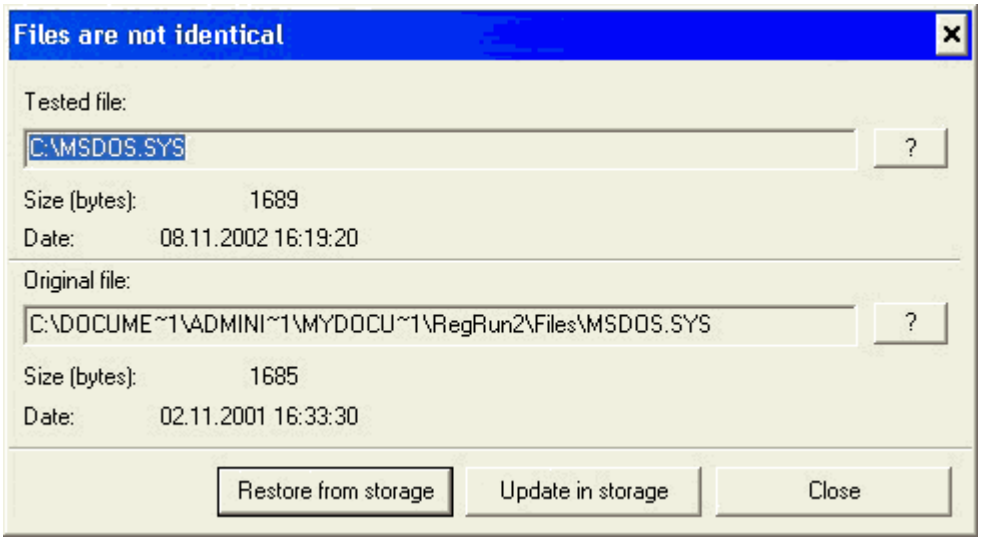
Boot.ini is an important file for Windows NT/2000 startup or if several operating systems startup on one drive. Windows NT/2000 can't start when boot.ini is missing or contains errors.

How does File Protection work?

File Protection automatically runs simultaneously with Secure Start.

In Windows 95/98 we advise to use of Secure Start DOS. In this case you will be able to restore damaged files before Windows is launched.

It is necessary to restart your computer to restore files when using Secure Start Windows.



If any disagreement of files is detected, you will see a warning message. You can see the date and the size of both of the files. By pressing "?" you access scroll menu, that contains commands of this file. With the help of this menu you can scan the file for viruses, and copy, delete, rename or view it.

Press the "Restore from storage" button to restore the initial file. If you find it necessary to update the file in storage, press the "Update in storage" button. If you want to decide later, then press the Close button.

Application Database

Application Database

Some of the most frequently asked user questions are:

What kind of program is it?

Why is it launched? and

Is it possible to cancel its autorun and not to interfere with the usual work of the computer?

RegRun *answers* any of these questions.

We analyzed the programs that often occur in loading and registered them in the database.

All the programs are divided into 4 groups:

1) **Necessary** - it is strongly recommended to leave these programs in Windows startup.

2) **Useless** - some useless programs can slow down operations of the computer, so you should stop their auto launch.

3) **Dangerous** - viruses and Trojans.

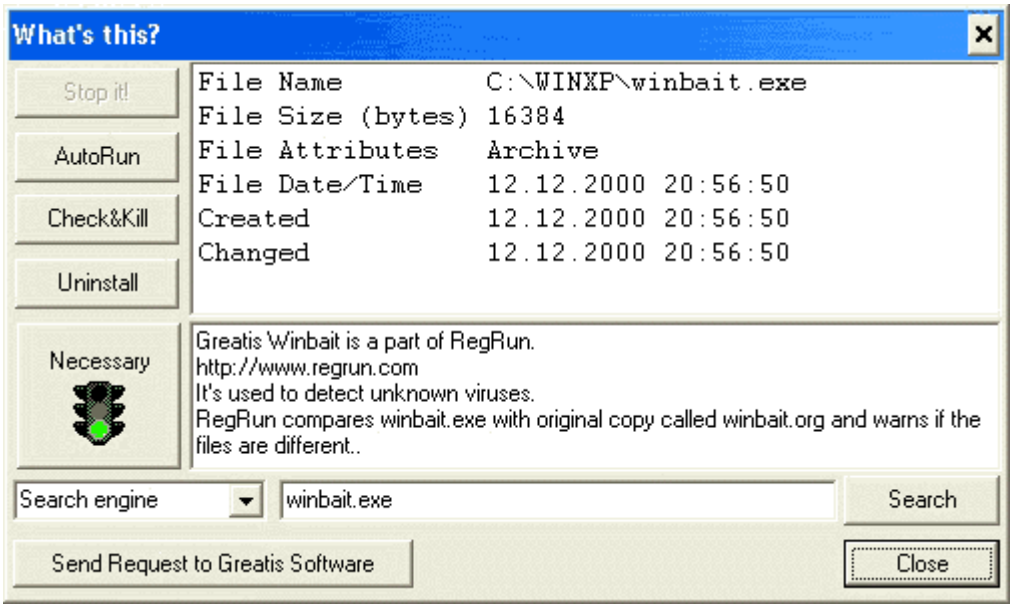
4) **At your opinion** - its up to you to suspend running these programs or not, without damaging Windows.

We constantly update our programs database. Registered users will be provided with timely new versions of the database.

RegRun checks by set if there are any potentially threatening programs and it informs the user about them.

To view a program's description, click on the item in the list. You will see full detailed information on the information panel on the right side.

Right click the mouse to get "What's this?" option in the popup menu if you are interested to get more information.



You will get complete information on the product. If you already have it in your database then you will find out its type and get its brief description.

Now you can:

1. Stop it! Kill the program if it is running at the moment.
2. AutoRun. Break autorun.
3. Check with antivirus , delete file.
4. Uninstall the application.
5. Terminate.

If the information about the type of the program is missing, you can also try to obtain it via Internet.

Check Search option in the scroll list:

- Search Engine
- Google News (Usenet news)
- Microsoft DLL archive contains information about all the programs and DLL, which are used by Windows.
- Microsoft Knowledge Base entries and useful info.

Press the Search button to initiate your search.

If you are a registered RegRun user, press "Send Request to Greatis Software" button. Your request will be sent to RegRun technical support. You will receive the reply to your request as quickly as possible.

To view the database press "Your opinion" program button.

You can view the contents of the database and also add new programs to it or remove programs. Press the Insert button, type in the name of the program and its description.

Right click on an item to get a popup menu of commands.

Anti Replacement

Anti Replacement

RegRun automatically detects files that will be replaced with the next restarting of Windows. The Windows needs to use special technology to replace opened files a like system DLL or executable files.

Note! If a program asks you to restart your computer after setup, it tries to replace system files.

The Anti Replacement feature of RegRun allows you to manage replacements:

- Declining changes;
- Removing unwanted changes;
- Adding new replacements.
  This may be required for you if you want to delete a Trojan file that you could not delete using Windows Explorer.
  Tip! You can do it easily using Terminator feature.
- Creating exclusions.
  It is useful if a program creates a replacement every time when Windows shuts down. This will stop annoying alerts during Windows shutdown.

Technical details:

- Windows 95/98 and Windows ME uses "wininit.ini" file located in Windows folder to replace or delete teh files.
- Windows NT/2000 uses registry value - "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations".

Process Manager and Network Monitor

Process Manager/Network Monitor

Open Start menu, RegRun Security Suite, Process Manager.

A Process Manager window has two pages:

- The First page, "Process list," is used to show all running processes on the computer. You are able to see full information about each process and all DLL used.
  This information includes: **parent process name** (only for Windows NT4/2000/XP), descrition, list of used DLLs.
- On the other page, you can view all DLL loaded on your computer and all processes that use these DLLs.

Click the right mouse button on an item and you will see a popup menu.

You can get a process' property window by pressing CTRL+ENTER.

Killing process.

Process manager allows you to kill any process excluding Windows core services.

Be careful! You can kill the LSASS.EXE, SVCHOST.EXE and other non-system processes. This is not fatal but you must restart your computer after that.

Click on the "Kill Process" button.

Note!

Process Manager can kill the processes that you could not end with Task Manager (using debug priviledge). We suggest you to use Process Manager to end a process.

Additional features:

1. Use Refresh button to renew information.
2. Set the refresh interval in seconds and click on the Start button to begin auto-refreshing information.

Network Monitor

Network Connections Monitor works with Windows XP/2003 only.

Click on the "Network Activity" tab.

You can see the list of the processes that use network.

This is the simple way to detect a new worms or Trojans.

You can kill a process using "Kill Process" funtion.

Information listed:

1) Process name.
2) Protocol (TCP/IP or UDP).
3) Local IP address.
4) Local port.
5) Remote IP address.
   If you want to get domain name for this IP address, right click on this item and choose "IP to Host Name" command.
6) Remote Port.
7) Connection State.

System Files Editor

System Files Editor

The System Files Editor allows you to manage with text files such as autoexec.bat, system.ini, etc.

The user can:

- edit files;
- search the text;
- open and save files;

All opened files will be automatically restored on the next launching of the System Files Editor.

The editor makes editing "read-only" files easy.

When you save a file, the editor will clear the "read-only" attribute, then after saving it, the editor will reset the read-only attribute again.

Launch Soon

Using Launch Soon

Launch Soon is a feature that allows you to launch applications:

- with delay
- recurrent
- one time for day

Launch Soon has two work modes:

1) Interactive

2) Automatic

Use Start menu (RegRun Security Suite) to open Launch Soon. You will see "Launch Soon" window. This is an **interactive mode**.

Fill in all necessary fields and click on the Start button to begin.

To run in **automatic (or batch) mode**, use the command line and enter the parameters.

Full syntax:

lsoon.exe [option] [time in seconds] [program name in short mode]

Option:

-c - one time launch

-r - recurrent launch

-1 - one launch for day

For example:

lsoon.exe -c 15 notepad.exe

You can create a shortcut to the "**lsoon"** and add the necessary parameters.

To make it quickly, run Launch Soon and fill in the form, click on "Save Shortcut" and enter the name and location of the shortcut.

Run Job

Using Run Job

RegRun Run Job allows you launch several applications simultaneously.

Open Start menu, RegRun Security Suite, Run Job.

Use right click on left panel to get popup menu for jobs.

Use right click on left panel to get functions for the programs located in the current job.

Press Ins or use "Insert" command to insert new Application.

Fill in the Application form.

You may specify starting parameters, window options, delay before execution, waiting type before the next application will be started.

File Extension Manager

File Extension Manager

File Extension Manager is a feature that helps manage file extensions.

Microsoft Explorer allows you to fully manage the file types. But when you want to reassign an extension you will have a problem. Microsoft Explorer shows you the file types, such as Microsoft Word Document and display linked extensions, such as DOC.

File Extension Manager shows all available extensions and appropriate file types and execution commands. If you want to assign WAV extension to Winamp or to the Media Player - no problem, it's easy.

Use Start Menu, choose RegRun Security Suite submenu and click on the File Extension Manager icon.

Choose WAV extension in the list and click on the Change button.

Select desired file type. You may use Search option (CTRL+F) to find it quickly.

Click on the **Change Now** button.

Used Files

Used Files

Purpose

Used Files allows you to browse a list of files that are currently opened on your computer.

This feature is useful if you want know what these files are opened for.

Used Files is easy to use.

Unique feature - Close File.

If you have Windows NT4/2000/XP/Vista you can **close opened file or folder** handle.

Right click on it and choose "Close Handle".

Be careful! This can cause the system crash. You need to be sure that you understand that you are doing.

Right click and choose "Display folders" to show opened folders.

You can close folder handles as well as files.

Additional Features:

You may use Search feature to find particular file.

Also Save to text file, Printing, Sorting, File Properties features will be useful for researchers.

To sort the list by the column simply click on the column header.

Registry Assistant

Registry Assistant

The new Registry Assistant feature of RegRun is a straightforward, yet extraordinarily useful feature - of which we are very proud!

Includes registry search and replace, tips and tricks collection, registry shortcuts, useful links and utilities. This includes a full, 32-bit application that allows fast, multi-threaded searches of the Registry; a very useful tool for those accustomed to working with the MS programs.

Open Start menu, RegRun Security Suite, Registry Assistant.

Try to use its features.

Open Bookmarks tab according your operation system.

Tip:

You can make a shortcut to the registry key and place it on the desktop or in another folder.

The shortcut has an icon:

Double click on icon and RegRun Registry Assistant will open Regedit and proceed to the key.

Note: you must set English as default language.

Registry Tracer

Using Registry Tracer

Purpose

Registry Tracer monitors selected registry keys, and advises of changes. It allows you to reverse any modifications, additions, or deletions.

How it works?

It things were changed Registry tracer will alert you.

1) If a new key was added - it will show a '+'
2) If a new key was deleted - it will show a '-"
3) If an existing key was modified it will show a ‘?’
   All you do is click the key and you will see the added, deleted or modified values in the right panel.

How does RegRun use Registry Tracer?

RegRun adds recommended registry keys to trace list during installation.

How can I stop tracing or add a new tracing?

Open RegRun Control Center, choose Registry, Registry Tracer.

You can add a key to trace list using registry viewer located in the bottom panel.

Right click and choose "Delete" to remove unwanted Traces.

Internal Tracing

RegRun monitors tracing changes in the file extensions and in the Active Setup key.

Open RegRun Control Center, Options, Registry Tracing.

Additional information

Click on the "What’s this" button to get information about monitored registry key or send a request to support team.

Note!

Registry Tracer is available only in the Professional or Gold versions.

Rescue

Using Rescue

RegRun Rescue is **very useful tool** for each user.

It allows you to **easily** create the backup copies of your registry or system files on the hard drive, network or floppy disks.

First of all, **create a copy of your registry before any registry operations**!

It's very simple with RegRun Rescue.

Backing up

Open RegRun Control Center, choose Registry, Backup Registry.

You will see the RegRun Rescue main window.

Click Run to create a copy of your registry on the floppy disks.

Automatic Backup

Learn how to create a storehouse.

Recommended for backup registry and important files.

Restoring

If you have get a computer crash, you can restore your registry quickly!

Windows 95/98/ME users:

Go to the DOS mode or boot with floppy. Insert first disk with Rescue copy.

Enter a command:

a:restore

You will be prompted to restore your files. Press any key.

You will be prompted to insert other disks if need.

After unpacking files to the hard disk, you will be prompted to restore registry files.

Press any key. Restart your computer.

Windows NT4/2000/XP/Vista users:

Microsoft tells:

You can start your system using either the Windows Setup disks or the Windows CD or using Windows 2000 Recovery console.

To add the Recovery Console to existing installations of Windows 2000, on the Start menu, click Run, and then type:

F:\I386\Winnt32.exe /cmdcons

where F is the CD-ROM drive letter.

This installation requires approximately 7 megabytes (MB) of disk space on your system partition.

The Recovery Console provides system repair and recovery functionality.

If there is more than one installation of Windows 2000 or Microsoft® Windows NT® 4.0 or earlier, they are also shown in the Recovery Console startup menu.

To access the disk by using the Recovery Console, press the number key representing the Windows 2000 installation that you want to repair, and then press ENTER. The Recovery Console then prompts you for the administrator password. If you press ENTER without typing a number, the Recovery Console exits and restarts the computer.

To use the Recovery Console, you must know the password for the local Administrator account. If you do not have the correct password,

Recovery Console does not allow access to the computer. If an incorrect password is entered three times, the Recovery Console quits and restarts the computer. However, you can use either the Group Policy snap-in or the Security Configuration and Analysis snap-in to specify automatic administrative logon.

Once the password has been validated, you have full access to the Recovery Console, but limited access to the hard disk. You can only access the following folders on your computer:

%SystemRoot%. If you have multiple Windows installations, this is on the partition that contains Boot.ini and other Windows files required to start the system.

%Windir% and subfolders of the Windows 2000 installation that you are currently logged on to.

%SystemRoot%\Cmdcons and its subfolders.

The Recovery Console prevents access to other folders such as Program Files or Documents and Settings, as well as to folders containing other installations of Windows 2000. However, you can use the logon command to access an alternate installation. Alternatively, you can gain access to other installation folders by restarting the Recovery Console, choosing the number representing that installation, and then entering the administrator password for that installation.

You cannot copy a file from the local hard disk to a floppy disk, but you can copy a file from a floppy disk or a CD-ROM to any hard disk,

and from a hard disk to another hard disk. However, with the **set** command enabled, you can copy files to a floppy disk. The Recovery Console displays an "Access is denied" error message when it detects invalid commands.

We strongly recommend enabling "set command policy" immediately. Open Start menu, Settings, Control Panel, Administrative Tools, Local Security Policy, locate for Recovery Console options.

When using Recovery Console you may get know more about commands with using "help" command.

To restore your registry:

type in the command line:

chdir system32\config\regback

batch restore.bat

Registry will be restored without prompt.

Type "*exit*" to logout and restart your computer.

Note:

you can't expand your registry files from diskette with Recovery Console.

But if you do have another working operation system on your computer you may restore files to the hard disk and copy them to desired location. Use restore.bat located on the first disk for help.

Advanced Backup

If you want to make a backup copy of your files and/or folders and/or registry, click on the New Scenario button. Give a name for your scenario and add files or folders or registry to your backup. Choose a location of your backup copy.

To automate creation of backup copies you may use command line to launch Rescue:

Rescue ScenarioName

It will be launched immediately!

If you wish to make backup to the different than default folder, use this syntax:

Rescue ScenarioName FolderName

If the folder is not exists it will be created.

The main window of Rescue will be hidden.

You can use Launch Soon, RunJob, Start Control or Scheduler to automate creation of the backup copies.

Advanced Restoring

Note! If you want to restore particular files of your Rescue copy.

Go to the command prompt.

Enter a command like this:

EXPAND 1.cab -F:*.* C:\Temp

This example allows to extract all files to the C:\Temp folder.

Full syntax:

EXPAND [-r] Source Destination

EXPAND -r Source [Destination]
EXPAND -D Source.cab [-F:Files]
EXPAND Source.cab -F:Files Destination

-r Rename expanded files.
-D Display list of files in source.
Source Source file specification. Wildcards may be used.
-F:Files Name of files to expand from a .CAB.
Destination Destination file | path specification.
Destination may be a directory.
If Source is multiple files and -r is not specified,
Destination must be a directory.

Note:

The function "Create Emergency Recovery Floppy" doesn't work with Windows 95

Automatic Backup

Recommended for backup registry and important files.

Automatic Backup will be performed every day when starting Windows.

1. Open RegRun Rescue
2. Choose "Send to" folder. Recommends clicking on the Browse button and choosing a folder on your hard disk. We suggest you to create new subfolder with any name.
3. Click on the AutoRun button.
4. Choose Storehouse parameters.
5. Check "Launch with Delay" switch. We suggest you to add a delay to reduce system resource using.
6. Click on the OK button.
7. That's all. This backup will be started when next Windows starts.

Note!

RegRun WatchDog will notify you about new changes at startup. Accept this change.

Each backup will be created in own subfolder with system generated name.

For example:

20034216_11_1

This means:

November 1 2003

2003 year Fourth quarter Second month First week Sixth day (since Sunday) Eleventh month (or twelve) 1 day in month.

To restore backup:

Go to the selected folder and launch "restore.bat".

Get more information.

Registry Compressor

Using Registry Compressor

Registry Compressor can decrease the size of your registry and the memory it uses by removing deleted records from registry files.

How does it work?

Registry compressor is not a registry cleaner. It will not delete anything from the registry.

Since Windows does not remove deleted registry records from registry files these records will be used again with creating new records, which takes up space.

The fragmentation can cause the small delays with creating new keys. Also the deleted records occupy computer memory.

Sometimes the percent of deleted records is not more than ten percent. But if you rarely add and delete dozen records you need to compress your registry.

First step

Click on the Calculate button to calculate estimated benefit.

This is absolutely a safe operation.

The Registry Compressor creates the clean copy of your registry.

Please, be patient. This operation takes no more than one minute.

Second step

Click on the Optimize button to start replacing your registry with the clean copy. After that you must restart your computer.

Note!

Although the registry compression is safe, we always suggest you to make registry backup before any registry operation.

Use Rescue.

WinCleaner

Using WinCleaner

WinCleaner is a useful tool to improve the security of your computer.

WinCleaner allows cleaning your system by one click, or in fully automatic mode.

WinCleaner give you the possibility to clear:

- Windows Temporary Files
- Recycle Bin
- Windows Recent Documents Folder
- Scandisk Temporary Files
- Internet Explorer Cache
- Internet Explorer History
- Internet Explorer Cookies
- Netscape Navigator Cache
- Opera Cache
- Any User Defined Folder

Select items to be cleaned by mouse click, or by pressing the Spacebar key.

Use File menu to choose Cleaner Wizard.

It allows to automatically choose user mode:

❖ Low Level mode allows to quickly clean your hard drive

- Medium Level allows to quickly clean all embedded items;
- High Level allows to wipe all files before deleting them.

Be careful!

If you selected High Level mode you can't restore files by Unerase or another utilities, because WinCleaner fills the files with zero bytes and after that deletes them.

Tips!

- You may delete only files older than specified number of days.

Double-click on selected item and enter number of days in the Properties dialog.

- You may exclude some files from deletion. For example: "cookies".

Double-click on selected item and click on the Exclude Files "Change" button.

Select files that you want to save.

- If you want to clean your system before computer shutdown.

We suggest you to click on the "Create 'Safe Shutdown' shortcut" button. You will see a new shortcut on your desktop. Click on this shortcut. WinCleaner will be launched in auto mode. After finishing its work WatchDog will check your system for a safe shutdown. If OK, system will be shut immediately.

- In addition you may run WinCleaner in fully automatic mode.

Clicks on the Schedule button to customize time and date of the cleaning.

- How to create Cleaning Shortcut.

Create shortcut to WinCleaner.

Open its properties, add parameter:

cleaner.ini

Trojan Analyser

Using Trojan Analyser

Trojan Analyser allows determining if a suspicious file is **useful or harmful**.

It traces all files that the application tried to open or write, and all registry operations.

Trojan Analyser has two methods to begin tracing:

1) You may browse for a execution file. Trojan Analyser will run this file and watch until it finishes, or while you stop.

2) You may choose one or all of the processes that are already working (excluding system processes.) To trace all process set the option "**Monitor All Processes**".

Note! Only for Windows 95/98/Me users:

1) You may enable option "**Enable Write-Protect Mode**".

This option prevents creating, deleting, renaming files with extensions:

- exe
- com
- dll
- sys
- 386
- vxd
- cpl

This feature will protect your system files against dangerous actions.

Be careful, if you try to launch the installation package with this option enable. It may cause an abnormal working of the installation program.

After finishing tracing Write-Protection mode will be automatically cancelled.

2) Trojan Analyser automatically checks your execution file extensions (exe, com, pif, bat) before starting tracing and after finishing. If the file extensions will be changed, Trojan Analyser will restore them. This will protect you against viruses' actions.

We suggest you to check your system by WatchDog or run Start Control to restore changes in the startup.

After the application finished, or you stop its work, you will see the results in the Results window. You may quickly inspect changes by using search and sort operations. Also, you may export results to CSV file format. You may use Excel or another application to analyze them.

Also you may use CSVED software by Sam Francke for free.

Visit: http://home.hccnet.nl/s.j.francke/t2t/text2table.htm

Bootlog Analyser

Using Bootlog Analyser

Bootlog Analyser allows you troubleshooting of Windows startup and shutdown with **Windows 95/98/Me/NT4/2000/XP/Vista**.

Bootlog Analyser uses the log generated by Windows startup (*bootlog.txt or* ntbtlog.txt).

The Bootlog.txt file records the progress of the Windows startup (boot) process. It is created if you request a logged boot, and is also created automatically by Windows if Windows detected that the previous boot was unsuccessful.

You can create a new Boot Log file by choosing option [2] "Logged (\BOOTLOG.TXT)" from the Windows 95 Startup Menu. You can display this menu manually by pressing the F8 (or CTRL) key during system startup, just after the system beep and before the Windows logo appears.

Press on the tick button to read current Bootlog file. Usually it is located in the c:\bootlog.txt or in the c:\windows\ntbtlog.txt.

Choose File-Open to open file from another location.

You can see used file name and its date in the status bar at the bottom of the window.

Boot duration parameter determines how long the Windows startup process runs.

To analyze the failures click on the Failure column and go to the top of the list.

The failed items are marked with a "!!!" signature.

What has failed? Why? How do I resolve the problems?

Bootlog.txt may contain the following lines, even though your computer is running properly:

LoadFailed = dsound.vxd

LoadFailed = ebios

LoadFailed = ndis2sup.vxd

LoadFailed = vpowerd

LoadFailed = vserver.vxd

LoadFailed = vshare

InitCompleteFailed = SDVXD

A computer that is running Windows 98 may also contain the following lines:

Deviceinitfailed = MTRR

SysCritInitFailed = JAVASUP

DeviceInitFailed = MTRR

These load failures do not necessarily indicate a problem. It is common for some, if not all, of these load attempts to fail, depending on your system configuration. You may get

more information about the causes of specific types of load failures in the Microsoft Knowledge Base Article - Q127970.
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q127970&

Other errors may be very important for Windows startup.

If you have a LoadFailed error check that the file really exists.

The core drivers are located in the \WINDOWS\SYSTEM\IOSUBSYS\ folder.

Also check the \WINDOWS\SYSTEM\VMM32\ and C:\WINDOWS\SYSTEM.

Optimizing startup

To optimize your startup, check the delays.

Click on the Delay column to sort this table by delays.

Inspect the delays.

Be careful. If you see a large delay on the item "Enumerating ..." this doesn't mean that this action cause the delay. This delay was caused by the previous item. Below the "Enumerating" event you should find the associated "Enumerated" event. The enumeration delay is printed on the "Enumerated" event.

Useful Tips

To quickly restore the original sort order of Bootlog.txt file click on the "Show in Unsorted Order" button.

To analyze "bootlog" file in spreadsheet software click on the Save button to export this file to the CSV file format. This file format may be easily opened with Microsoft Excel and other software.

To search the list press CTRL+F or click on the Search button.

Note!

Bootlog Analyser is included in the RegRun Suite Gold version only.

Startup Analyser

Using Startup Analyser

Startup Analyser allows to unhide Windows startup processes (**Windows 95/98/Me**.)

1. Launch Startup Analyser using Control Center Startup or via WatchDog popup menu.

2. Follow instructions to activate Startup Analyser.

3. Restart your computer.

Startup Analyser runs on the early stage of Windows startup, immediately after your desktop will be displayed. Startup Analyser works in the background. You will never see its presence. This is done especially to protect you against malfunctions during startup.

However you will see a stop icon on your desktop.

When you click on this icon Startup Analyser will stop and it will show results.

After that the icon will be automatically cleared from your desktop.

Note:

If you didn't stop Startup Analyser it will stop after restarting your computer.

Startup Analyser runs only one time.

Analyzing Results

Startup Analyser records full information about opening files.

Look at this example:

EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:61	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHDOCVW.DLL	14:52:8:61	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:181	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:181	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:181	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:181	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHDOC401.DLL	14:52:8:196	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\OLE32.DLL	14:52:8:236	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\DDEML.DLL	14:52:8:241	OPEN	Success
EXPLORER	C:\WINDOWS\SHELLICONCACHE	14:52:8:256	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\IERNONCE.DLL	14:52:8:22	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\ADVPACK.DLL	14:52:8:57	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\NTDLL.DLL	14:52:8:106	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\VERSION.DLL	14:52:8:121	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:241	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:251	WRITE	Success
EXPLORER	C:\WINDOWS\SYSTEM.DAT	14:52:8:396	WRITE	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:416	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:416	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:416	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:416	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:426	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\SHELL32.DLL	14:52:8:426	OPEN	Success
EXPLORER	C:\PROGRAM FILES\DESKTOP.INI	14:52:8:461	OPEN	Success
EXPLORER	C:\WINDOWS\SYSTEM\MSI.DLL	14:52:8:476	OPEN	Success
EXPLORER	**C:\GAMES\STINKY\STINKY.EXE**	**20:40:33:225**	**OPEN**	**Not Found**
EXPLORER	**C:\WINDOWS\RUNDLL32.EXE**	**20:40:35:750**	**OPEN**	**Not Found**
EXPLORER	C:\PROGRA~1\GREATIS\REGRUN~1\REGRUN2.EXE	14:52:8:476	OPEN	Success
REGRUN2	C:\WINDOWS\SYSTEM\RICHED32.DLL	14:52:10:65	OPEN	Success
REGRUN2	C:\WINDOWS\WIN.INI	14:52:10:90	OPEN	Success

Now you can know what really happened during Windows startup.

It is useful to detect fully invisible applications (Trojans, viruses, keyloggers)

Give your attention to the "Not found" status of operations. This may a source of the problems. If the application can't find the file it can't work correctly.

If you are not a computer specialist you may send this file for analyses to the support.

Open File menu and choose "**Save to"** menu item.

RunGuard

RunGuard

RunGuard is a tool allows you to automatically **check a file before its execution**. If the file will be suspicious, RunGuard will warn a user **to proceed execution or decline** it.

RunGuard uses own "ScriptCheck" technology to determine if a file is useful or harmless.

RunGuard can check:

- Microsoft Office files (doc, dot, xls, xlt, ppt);

- HTML files (htm, html, shtml, asp, mhtml);
- Windows script and batch files (vbs, wsh, js, bat pif, cmd);
- Windows HTA (hta);
- Windows registry files (reg.)

Note!

RunGuard is included to the Gold Edition only.

When does RegRun begin defend you?

Immediately after installation RegRun Gold if you chosen "High" or "Ultra High" Security Level.

What will I see when I use RunGuard?

You will see nothing while you do not launch a suspicious file. RunGuard will display an alert if it decides that you must pay attention to this file.

What can I do when I got alert?

You can:

1. Quickly check this file by antiviral software installed on your computer.
2. View file source code.
3. Block file execution. You may send this file to Greatis Software or to another antiviral company for testing.
4. Safely view file contents. This allows you to see Microsoft Word files in WordPad without macros execution. If you check HTML file RunGuard will strip all dangerous tags and will create the safe file in the temporary folder. You can see a text without images.
5. Cure file. This feature is valid for HTML files only. RunGuard will strip dangerous tags and replace the original file.

How can I block execution of the file?

Add this file to the Black List.

Click on the "Stop this file from running" button and choose "Never run this file" option.

Also you can choose "Delete File" and "Quarantine File" (move to Quarantine folder) options.

I know that the file is good. How to skip its testing?

Add this file name to Allowed list.

Click on the "Allow to Run" button and choose "Always run this file. Add it to Allowed list.

Manual Testing

You can manually check a file. Open RunGuard, click on the "Check File" button and locate for a file.

Execution History

RunGuard logs files execution. You can view log file by launching RunGuard, Show History.

What are the "PIDL" records?

Windows uses special item ID identifiers to execute virtual links such "My Computer". The PIDL may do not be related to executable file. The PIDL is not constant value it is variable and it has the defined value only during current Windows session.

Note!

You can disable writing History via RunGuard configuration.

Why RunGuard sometimes doesn't trap file execution?

1. RunGuard traps execution files according you configuration. You should select which types you want to trap. It checks file extension to determine file type. Open RunGuard, Configuration.

2. RunGuard can’t trap if you open a file in the application. For example, if you open a file in Microsoft Word via File, Open method, RunGuard do not check the file. The same will be if you launch it from Start menu, "Run": winword.exe doc1.doc.

What is the "rrshell.dll"?

This DLL is used to trap file execution.

You can see it in the Start Control, "Windows Core Components", "Shell Loggers" tab. This DLL is required to use RunGuard in auto mode.

If you are being asked by WatchDog about "rrshell.dll" you should decide do you want to use RunGuard in auto mode or not.

RegGuard

Protecting using RegGuard

Purpose

RegGuard disable write/delete access to the Windows startup registry keys for all applications excluding RegRun Start Control and Control Center.

RegGuard allows you to easily remove dangerous programs using "Scan for Viruses" feature.

Often dangerous programs control their autostart status by adding to the registry startup keys every second. RegGuard blocks these attacks and the dangerous programs could not start after computer reboot. You need only delete their files.

Easy in use

RegGuard requires no user assistance.

After installing RegGuard will started using RegRun Secure Start or using WatchDog.

You will see that WatchDog icon will be like this:  .

Stop

Open WatchDog main menu, and click on the "RegGuard" item.

The menu item will be unticked. WatchDog icon will be in green color.

RegGuard will be stopped.

Repeat the same to reactivate RegGuard.

Installing new applications

If you are not sure that application is good, activate RegGuard.

Later you can set auto start of application using its settings.

How RegGuard works?

RegGuard uses kernel system driver regguard.sys.

RegGuard.sys intercepts access registry and checks for protected registry keys and calling application. It will give access or decline it.

All options you can set up using RegRun Start Control, Features, RegGuard.

Uninstall

Open RegRun Start Control, Features, RegGuard.

Click on the "Remove RegGuard driver" button.

Partizan

Detecting hidden rootkits using Partizan

Looking to the progress of rootkit development since last year we have the opinion that the rootkit detection on the working computer is not real. We can not get you the 100% guarantee free of rootkits on the working computer connected to network.

Partizan is a boot watch anti-rootkit.

Rootkits authors like to play games.

"We hide rootkit files/drivers/registry keys and after that try to find us" – they said.

We didn't play the games.

Our strategy is different:

You hide yourself while we're watching how you do it.

Each rootkit need a way to automatically start after computer reboot.

We can detect it and remove a rootkit from auto start.

What are the user benefits?

1) Detecting kernel rootkits **without a lot of BSOD**.
2) Partizan checks the computer **automatically** during every Windows boot.
3) Partizan uses **small number of computer resources**.
4) Partizan **takes only a couple seconds** for checking. Compare it with full disk scan.
5) **Partizan is a powerful**. It can detect a remove any kernel/usermode rootkit, Trojan/Spyware/Adware components.
6) You can use other anti-rootkit software in addition to Partizan as well.

How does the Partizan work?

Partizan activates several agents for monitoring the Windows boot process.

1. **Anti-Bootkit**. Used against Bootkit rootkits located in the boot sectors (in development).

2. **Partizan boot driver**. Used against Rustock clone rootkits. It can trace registry services and delete a service. Partizan driver starts on the early stage of the Windows boot process.

3. **Partizan Native application**. It is started from the **BootExecute** registry key. Used against Rustock clone rootkits. It can trace registry services and delete a service. Partizan driver starts on the early stage of the Windows boot process. Partizan driver has additional "safe" mode allows to skip processing of the Winlogon and similar registry keys by Windows operation system to avoid infection and for easy removing infection.
4. **Secure Start**. It starts before Windows shell starts using RunOnceEx key.

Secure Start executes **UnHackMe** application for rootkits testing using information from the Partizan boot driver.

Get Rid off Unwanted Explorer Windows at Startup

Remove Unwanted Explorer Windows from Startup

This feature allows you to eliminate annoying explorer windows at startup.

Often this situation may be caused by incorrect registry value **DesktopProcess**.

This value is located under registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer.

If you see **Windows** folder at startup, we suggest you to remove **DesktopProcess** value. RegRun can do it for you quickly.

Also if you see Program Files folder at startup this may be caused by the program registered to launch at startup in registry. Often such programs use long file names in registry and it may produce the problem. In addition, the next situation may take place. You deleted a program from hard disk but did not remove from startup. This also may cause a problem.

RegRun gives you the **full list of the lost startup programs and allows to resolve the problem.**.

If it can't help, you may use RegRun **Clean Boot** feature. Clean Boot allows you to eliminate a lot of problems at startup.

If you do not resolve your problem, do not hesitate to contact us:

http://www.greatis.com/regrun3support.htm

Terminator

Terminator

This is built-in to Start Control feature that allows you to fully remove an application from your computer.

To use Terminate feature you should:

1. Open RegRun Start Control.
2. Select an item to terminate.
3. Right click on the item to get popup menu.
4. Choose "Terminate" (also you can choose "Terminate" command on the Information Panel.)
5. Set termination options and click on the Terminate button.

How it works?

1) It kills application in memory (if it is running);
2) Removes from startup (or set to pause state);
3) Tries to delete from disk or move to Quarantine folder. If a file is used by another application, Terminator will add new replacement to process operation after restarting computer. Don't forget that you can control replacement by AntiReplacement feature.
4) Adds file name to Black list.

Where is located Quarantine folder?

This folder is auto created in "My Documents\RegRun2\Quarantine".

Note!

You can choose "Terminate" feature from "What's this" dialog. This may be useful if you want call "Terminator" from WatchDog alert dialog.

Recovering Winsock registry key

Recovering Winsock2 registry key

Purpose

Resolving Internet connection problems.

Symptom

Damage to the Winsock2 registry key causes a very slow Windows boot-up. After finishing startup a user can not connect to Internet sites.

Why?

The problem may be caused by new Spyware or Adware software. This software takes control on the Internet and can block access to a user.

Note!

Removing spyware without restoring the Winsock key may cause the damage. If a user simply deletes the spyware file he will have a problem.

Safety

A user must not change if he is not sure.

Make a registry backup using RegRun Rescue.

A user may use the "Make Backup" option to create a copy of the Winsock registry key in the "reg" file. Later a user can restore a copy by launching the "reg" file in Windows Explorer.

How to use recovering?

Open RegRun Start Control, go to the Reanimator menu, "Recover Winsock".

Mark unwanted items and click on the "Remove Marked". That’s all!

You must restart the computer to the changes take effect.

Technical Details

WinSock registry key is located at:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2

It contains the Winsock options values and LSP modules stack. Each LSP module is a DLL.

Which files are good?

Windows 2000/XP:

- mswsock.dll
- winrnr.dll
- rsvpsp.dll

Windows 95/98:

- rnr20.dll
- mswsosp.dll
- msafd.dll
- rsvpsp.dll

Need help?

Registered users can contact support without any limits.

Visit our support center:

http://www.greatis.com/regrun3support.htm

Open a new ticket.

Describe your problem.

Detailed System Report

Detailed System Report

Purpose

Gives a user full information about Windows startup programs, drivers, services, etc. Useful to analyze Windows startup problems and to detect Spyware, Adware components.

How to use it?

Open RegRun Start Control, go to the Reports menu, and choose "Detailed System Report".

Users have an option to view result text file.

Analyzing Results

Users can post the result text file to the Greatis Software support center to resolve his problems.

http://www.greatis.com/regrun3support.htm

Open a new ticket.

Describe your problem.

Attach result text file.

Technical support

FAQ

Where can I find RegRun's latest version?

Homepage: http://www.greatis.com

Download: http://www.greatis.com/security/download.htm

How can I install RegRun?

1. Shut down (Close) any currently running RegRun programs.

2. Run the downloaded file by clicking on regrunXXX.exe and following the setup instructions. You should not uninstall a previous version.

You must unsinstall RegRun 2.X before installing RegRun 3.

How can I install RegRun on the Windows NT/2000/XP/Vista?

You must login as an administrator for installation, registration, and uninstallation.

Other users can use one registered copy of RegRun on the same machine.

RegRun automatically determines user rights and automatically configures itself.

The common user cannot write access to the sections of RegRun if s/he doesn't have rights in the system.

Power Users of Windows NT/2000/XP have full access to the following:

1. Registry - Current User Run

2. Startup folder

3. Current user RunOnce

4. Read-only access for other parts.

Each user has his own folder, My Documents\RegRun2, which contains a backup of startup profiles and the log file.

What does an evaluation time mean?

You can use RegRun for 30 days to test its functionality and reliability.

After that you must order RegRun or uninstall it.

What does RegRun do with my computer after evaluation time expire?

Nothing. Your computer is safe.

RegRun only warns you that you forgot to purchase it. That's all!

I heard that the registry programs are dangerous. How does RegRun work?

Indeed, a mishandled registry can result in severe problems! For that reason, RegRun is a wise investment - we at Greatis Software are registry specialists, and have tried to make RegRun a powerful, but **SAFE** tool to make the most of your computer. RegRun provides a user-friendly interface and always the additional possibility to undo changes. RegRun doesn't process any operation without your knowledge and confirmation. You can restore a previous condition at any time.

I am registered user and I lost my registration information.

Contact us: http://greatis.com/support and we'll send you registration information. You don't need order again.

If you change your e-mail address, please notify us.

How can I download the upgrade for RegRun?

Download new version of RegRun http://www.greatis.com/security/download.htm

and install it over old. If you uninstall it, you will need register it again.

The new versions are free for registered users.

Why did I lose several of my configuration sets after installing version 2.7?

Version 2.7 is a major change to RegRun, and we want you to review your current configuration in addition to reviewing new configuration options.

RegRun hangs when running and uninstalling?

If you set a 16-color mode of screen, RegRun 2.7-2.8 or higher doesn't hang up. But it doesn't work. There are no problems with using Windows NT4/2000/XP.

To run Start Control in the Windows 98/Me, open Start menu, Run, browse to the regrun.bat in the RegRun Suite folder. You will be switched to the full screen mode for couple of seconds After that Start Control will be executed.

If you use Windows 9X/ME and a lot of programs run simultaneously the system can hang because the system resources have run out.

How to uninstall RegRun?

There are many ways to do it:

1. Open Start menu, Settings, Control Panel, Add/Remove Programs.

2. Open Start menu, Programs, RegRun Security Suite, Uninstall.

You must restart your computer to finish uninstallation.

What is Secure Start?

Secure Start is active BEFORE Windows is fully activated, and allows a controlled startup process.

There are two version of Secure Start: Secure Start working in DOS mode and Secure Start working in the Windows mode.

Secure Start DOS works with Windows 95/98.

Secure Start Windows works with Windows 98/2000/ME.

Note! Secure Start doesn't work with Windows NT4.

Within Windows 2k, only the administrator has the privilege to setup Secure Start. This setup is applied for all other users.

How does Secure Start work?

Secure Start for DOS uses "autoexec.bat" to launch.

Secure Start for Windows uses registry key HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx.

What is WatchDog?

"WATCHDOG" - Provides silent monitoring of the startup managers during your Windows working session. Watchdog may be configured to check the startup managers at Windows startup, Windows shutdown, and as a recurrent check with a specified time interval. If one of these scans detects a change, then you are notified with a popup window and a start-up of Start Control, along with the option to restore the affected file.

What is STARTUP PROFILER?

"STARTUP PROFILER" - Creates a specially designed file, called startup profile, that contains all of the startup information. Users may create their own profiles and restore them in WINDOWS and DOS. "STARTUP PROFILER" has a unique feature for startup troubleshooting - "Clean Boot". Using the "Clean Boot," the user will boot in really clean Windows.

Startup Profiler works in two modes: DOS and Windows.

Startup Profiler for DOS allows you to choose a custom profile before Windows starts and allows you to use special Clean Boot feature.

Startup Profiler for Windows allows you to create custom profiles and restore them. You must restart your computer to see the changes.

How to use "rbm" files?

RegRun has a unique feature to work with registry - Registry Assistant.

"REGISTRY ASSISTANT" allows instant access to any key in the registry. Users can create their own bookmarks or use the specially designed packet for improving performance, Windows enhancement and troubleshooting. Packet contains the description of many registry keys, tips and tricks. REGISTRY ASSISTANT loads information from "rbm" files.

You do have Greatis registry package for Windows 9X/ME and NT/2000/XP.

This feature is a WONDERFUL tool for advanced users - novices should deactivate it, or explore it carefully and backup the registry first!

WatchDog finds new started or paused NT services each time Windows is launched

Windows NT/2000 initializes RAS, Telephony and several other services after the user logs on. Curiously, services such Telephony start in spite of setting "Manual" - these services will be stopped after a short small time. RegRun will find these "stealth" services and warn you. While RegRun II 2.6 can't refresh service status and notify the user again, newly enhanced version 2.7 can! When you use the Refresh button, NT services will be refreshed too. (Note: We use parameter string "/c 1" to initialize RegRun for the first time. For example: "C:\Program Files\Greatis Software\Regrun2\regrun2.exe /c 1".) RegRun will skip testing NT services at starting. The refresh occurs automatically with the recheck and you will see actually changes..

Problems with registration

After purchasing RegRun you will receive a letter with registration information.

The registration key is built on the basis of the user data.
You must fill the registration form Exactly as in the registration message. You may use Copy/Paste (CTRL+C/CTRL+V) to clipboard commands to enter information correctly. After the pressing Register you will need restart RegRun. After the next starting of RegRun you will see a your name in the About dialog.

How much CPU time does RegRun use?

RegRun does not monitor the registry and files continuously. It will check your system periodically, based upon Watch Dog's period. The checking is very fast. RegRun uses very little CPU time and system resources.

I have restored the RegRun profile, but I want to go back to the previous condition

If you restored a profile or used Clean Boot, you may return back by using undo profile.

RegRun saves this profile with name "Undo.rr2". Choose File -> Open Profile -> right Click and choose "Open from" -> Locate "Undo" profile and restore it.

The last saved RegRun profile named "Regrun2.rr2". RegRun will backup previous profiles and save the new one when you use the Save button. RegRun keeps the nine copies of your profile.

Technical support

If you discover an error in the program or you have problems, please, visit our on-line support center:

http://www.greatis.com/support

You will find a list of frequently asked questions and probably it can resolve your problem. Also, you can ask RegRun experts on-line in the forums.

Please, do not hesitate to contact us. Fill in the support form to request help from our support team.

Try, as far as possible to accurately describe all actions that you carried out leading up to the occurrence of the error.

After analysis of the report you will receive a reply with our recommendations for addressing the problem by e-mail.

Registration

You are urged to register your copy of RegRun to ensure support and notification of updates.

Please, follow instructions in the registration message.

If your RegRun evaluation is out and you can't open Control Center, do this:

1. Open Start menu, Programs, RegRun Security Suite.
2. Choose Register RegRun Gold (or Pro or Standard.)
3. Paste your registration code from registration message or click on the Browse button to locate for key file. You should save regkey.key file to your hard disk from registration message before this operation.
4. Click on the Register button.
5. Launch RegRun Control Center, Help, About dialog to check your license.

If you purchased RegRun Security Suite on CD-ROM you should register your copy as described above. Please, do not forget it.

The legal users of the program receive the right to technical support via e-mail, free-of-charge program fixes and upgrades to the new versions of the program.

About Greatis Software

Greatis Software.

WWW:

http://www.regrun.com

http://www.greatis.com

http://www.greatissoftware.com

E-mail: greatissupport@gmail.com

Support center: http://greatis.com/support

Send fax: 1-419-735-3518

Historical antecedent - why we need RegRun today?

The need to automatically initiate programs at computer startup has existed continuously, beginning with the earliest PC operating systems. For example, in MS DOS a file called config.sys was run early in the start up process to load required device drivers and start DOS command processing. After DOS command processing was initiated, a file named autoexec.bat was run. Autoexec.bat contained a list of commands to DOS to further prepare the system environment for the particular requirements of the user and to start programs automatically without requiring the user to do individual initialization - or even having to know what was being done.

With Windows 3.0 there was a need to add the capability of further initialization for the Windows environment. This was done with the addition of a file named win.ini.

The improvements introduced by Windows 95 and Windows NT came with an increase in complexity, including more centralization of function within the system Registry (a sophisticated database referenced by most modern Windows programs). Along with other functions, the Registry also acquired the ability to initialize and start programs - along with win.ini and autoexec.bat.

So today there are many places within which programs can be started automatically. This is fine for useful programs, but what of unnecessary programs, or worse still, harmful programs? For example, Internet Explorer is configured, by default, to start automatically when the computer is started. For many users, this is unnecessary and undesirable. Worse, other programs known as Trojans can be secretly started by these startup mechanisms - resulting in a full range of undesirable effects.

We think the user should have complete control of what is started or not started on their system.

Who would not want to know if a dangerous program was installed on their computer? One that might, for example, facilitate the transfer of personal data to an intruder?

RegRun allows the user to see and control all the programs listed in the above mentioned sources. With it you can delete the undesirable programs, change start parameters and add entries of your own, all with the greatest facility from one window.

But that is not all! RegRun also makes periodic scans of the startup mechanisms during Windows sessions, and advises the user of any changes. At the next Windows startup, if any program entries have been added, changed, or removed RegRun will alert you then as well.

So, use our program to control what is running in your computer without your having to be a computer expert!

This choice blocks the deletion of registry items. However, you can suspend it from running. If you are not a computer specialist, then select the "Safe" option.

Check box "Active" and RegRun inserts the line with "regrun2d.exe" into your autoexec.bat file.

When the computer starts loading, you will see the Secure Start window.

Click message "Click here to select font for editor" to choose font for the editor. This font is used in edit autoexec.bat, config.sys, and winstart.bat.

Below you can see a radio button.

You can select the traffic-light idiom or the standard scheme for display in RegRun.

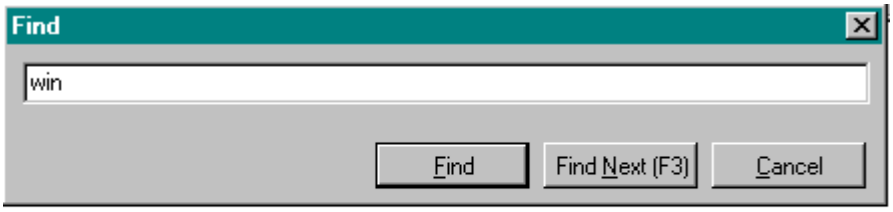
You need run RegRun again to see changes.

Check! Press F9 or click left mouse button on icon to search for changes.

To save changes: press F2 or click left mouse button on icon. Note: this function save the changes on all pages!

To find any program, press CTRL+F or click on the flash-lamp icon.
Enter any words to search on and then press Enter.

See example:

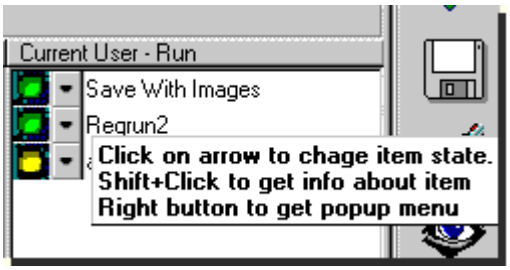



```
set winbootdrive=C:
%winbootdrive%
rem if not exist %winbootdir%\system\vmm32.o20 copy %wi:
rem cd %winbootdir%\system
```

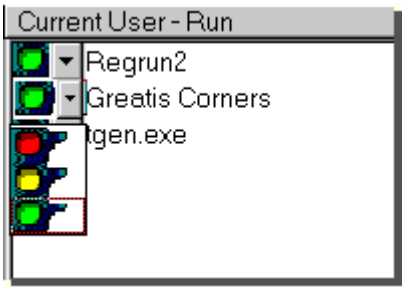
To refresh the content of all windows, press F5 or click on the icon. Use the refresh feature if you change content of some page with another program (not RegRun).

To close RegRun press ALT+F4 or click on the door icon.

Pause/resume items



You may suspend running of the program, however do not delete it. Select an item and click on its arrow to change the item's state. You will see a popup menu.



Select yellow light and click left mouse button (if you choose the red light, you will delete the item). After that, item light of changes to yellow and you will see item moved to the bottom of the list. RegRun shows green items before yellow items.

RegRun uses an algorithm compatible with Microsoft technology for suspending programs. If you have Microsoft Windows 98, you may run the System configuration utility and see that the item shows it has paused. However, RegRun works on Windows 95 and Windows NT 4.0. Those operating system's do not have a suspend feature.

You can easily pause or resume an item. If you use the keyboard, press CTRL+Enter and you will see a menu. Press Enter to change then item state.

You must restart computer to make changes.

When the computer starts loading, you will see the Secure Start window. Secure Start will await your commands for a specified delay time. Slide the "Delay time" for 3-4 marks. This is a 3-5 seconds. If you press the Spacebar within the delay time, Secure Start will check the RunOnce key and show the results. If you press any key (not Spacebar) within the delay time, Secure Start will activate and continue working. If you press the ESC key, the Secure Start closes.

If this box is checked, Secure Start will test the RegOnce keys. If these keys are not empty, you will see its contents.

If this box checked, Secure Start will test the wininit.ini file. If this file is not empty, you will see its content.

If this box is checked, WatchDog will be active. You will see the RegRun icon in your system tray. Click with the right mouse button to access the popup menu.

If this box is checked, WatchDog will test your system when the Windows shuts down.

Enter a time interval in minutes when WatchDog will test your computer. Recommended value:10 minutes.

RegRun command line parameters

You can run RegRun using the menu item Start ->Run.

RegRun has the following parameters:

1) regrun2.exe file.rr2 - prompt to restore startup configuration profile.

2) regrun2.exe file.rbm - runs the Registry Bookmark and open bookmark file

3) regrun2.exe HKLM\Software\... - opens the specified registry key in Regedit.

4) regrun2.exe /c - checks and closes.

5) regrun2.exe 2 (or any number) - prevents from checking the NT Services for specified times.

6) regrun2.exe - opens Start Control.

7) regrun2d.exe file.rr2 - extracts information from a profile.

8) regrun2.exe /rbm - opens the Registry Bookmark.

9) regrun2.exe /proc - opens the Process List.

10) regrun2.exe /sysed - opens the System Files Editor.

11) regrun2.exe /repl - opens the Anti Replacement list.

12) regrun2.exe /nowatchdog - opens without WatchDog.

Change the level of the slider to set up optimal security level.

Check this box to prevent unauthorized access to the WatchDog icon and Secure Start screen.

Don't forget to set a password. To temporarily allow access without a password, uncheck it.

Setting the password for accessing the WatchDog icon and the Secure Start DOS screen.

If you don't set the Secure Start DOS password early, it will be set the same.

If you forget the password, please, contact greatissupport@gmail.com for help.

Clears current password.

Warning! Access is always allowed when you don't set the password.

Setting to the Safe mode blocks the deletion of registry items.

However, you can pause and turn on paused items.

Secure Start Windows allows you to fully manage startup before Windows loads.

It runs immediately after logging on to the computer.

However, programs in the Run Services list run before Secure Start (Win9X,WinMe).

Enabling File Protection allows you to track changes of files and easily restore them.

It's a fully customizable feature.

Click button to choose files to protect.

Prevents the confirmation questions in WatchDog when checked.

Enables the Anti Replacement feature. It tracks all attempts to replace system files.

Compatible with Windows NT/2000/XP/Vista. This is an equivalent of "Check wininit.ini" switch in Secure Start for Windows 9X/ME. But it will notify you when the computer shuts down.

You should enable the "Check on shutting computer" switch.

Checks for the dangerous applications loaded with startup using Application's database.

Tells WatchDog to not show its icon in the system tray.

Warning! To see the effect, you should restart WatchDog.

To unload hidden WatchDog, run it with parameter "/k".

watchdog /k.

Otherwise, close it using task manager or RegRun's process list..

Set up exclusions for Watch Dog. This is useful to prevent unwanted Watch Dog' warnings.

This table is used to manage RegRun's tabs.

Each tab may be hidden, read-only or not watched.

Sets the default RegRun's tab settings.

With Windows NT/2000 RegRun tries to determine user rights and automatically sets the tabs.

RegRun sets the trap for any virus infected exe files.

It runs "bait.exe" from autoexec.bat.

RegRun uses Secure Start to compare "bait.exe" with the original "bait.org" and warns you.

This method facilitates detecting unknown viruses.

RegRun sets the trap for any viruses infecting Windows exe files.

It runs "winbait.exe" from the registry.

RegRun uses Secure Start for Windows and Watch Dog to compare "winbait.exe" with the original "winbait.org" and warns you. This method allows you to detect unknown viruses.

List of installed antiviral programs on your computer.

RegRun can automatically detect a lot of known antivirual programs.

Adds new antiviral program to the list.

Disables showing of RegRun's splash screen.

Smart tips are very useful to display the values of the items in the lists.

Disable them only if you have troubles.

Allows to setup the run order of the programs in the Registry tab.

Select list and click Sort Order button on the toolbar or use the popup menu.

Set the order by clicking on the arrow buttons or using the keyboard's CTRL+PgUp and CTRL+PgDn keys.

Attention! You cannot set the order of programs in Startup and Common Startup folders. These load in alphabetic order. You should rename files if you need to control their execution order.

If this box is checked you will never be asked to launch Start Control when clicking on the WatchDog icon.

This is the main registry tracer switch. If this box is unchecked file extension tracing, active setup key tracing and custom registry tracing are disabled.

This is the list for file extensions that RegRun traces. If any changes found the user will be notified. The user has possibility to decline changes. The user can add own file extension to the trace list. Right click on the list to get popup menu.

This switch controls the tracing of the Active Setup registry key.

Click on this button to set up your registry keys for tracing.

Click on this button to set up Antivirus Coordinator.

Click on this button to associate RegRun with "rbm" and "rr2" extension if you don't do it yet.

Removes antiviral program from the list.

RegRun Rescue offers two backup schemes. Both schemes suppose to backup one time per day.

Smart Backup Scheme provides **maximum** number of useful backups with the **minimum of the used disk space**.

This scheme includes:

- Last six days backups.
- Three last weeks backups;
- Two last months backups;
- Three last quarters backups;
- One last year backup.

It includes about 15 backups. Old backups are automatically erased.

Every day "Save One Copy" scheme uses only one backup per day.

"***START CONTROL***" - Provides an unusually friendly interface to users, who can easily and quickly provide detailed information about, suspend, resume, alter, or delete any of the programs within the Windows startup.

"***STARTUP OPTIMIZER***" - Allows to remove useless and dangerous applications from Windows startup **by one click**.

"***SECURE START***" -Analyzes the Windows registry, initialization files and warns the user if any changes have occurred. Secure Start is activated BEFORE Windows startup - in both W9x and W2K/WXP.

"***WATCH DOG***" - Provides silent monitoring of the startup programs during your Windows working session.

"STARTUP PROFILER" - Creates a specially designed file, called startup profile, that contains all of the startup information. Users may create their own profiles and restore them in WINDOWS and DOS. "STARTUP PROFILER" has a unique feature for startup troubleshooting - "Clean Boot". Using the "Clean Boot," the user will boot in really clean Windows.

"BOOTLOG ANALYSER" - Allows you to troubleshoot Windows startup and shutdown with Windows 95/98/Me/NT4/2000/XP/Vista.

"STARTUP ANALYSER" - Allows to unhide Windows startup processes by tracing file operations during bootup.

"***APPLICATION DATABASE***" - Includes descriptions of often-used programs as well as malware. WatchDog automatically checks this database and looks for dangerous programs. Users may query Greatis Software for all unknown programs; Users can add programs.

"***ANTI SPYWARE*** " - Allows users to quickly detect and remove any Spyware, Adware, Trojan or virus.

"***TROJAN ANALYSER"*** - Allows users to determine if a suspicious file is **useful or harmful**. It traces all files that the application tried to open or write, and all registry operations.

"***REGISTRY TRACER***" - Traces changes in the selected registry keys.

"***INFECTION DETECTOR***"- This is not signature scanning, but rather "infection scanning". During the session, RegRun opens and monitors a number of "bait" program and macro files, which are vulnerable to infection by any active virus. If any of these files

change, RegRun will advise you, and facilitate your communication with your antivirus supplier by providing you with before and after samples.

"***ANTIVIRUS COORDINATOR***" - Coordinator detects the well-known antivirus programs (it can be customized to incorporate lesser-known AV programs), and uses this information to quickly check startup files and folders, if necessary.

"***FILE PROTECTION***" - is one of the most useful functions serving to protect your computer from viruses, Trojans and malfunctioning programs.

"RUNGUARD" is a tool allows you to automatically check a file before its execution. If the file will be suspicious, RunGuard will warn a user to proceed execution or decline it.

"***SUBSTITUTION DETECTOR*** " - This is a very effective tool detecting "masked" Trojans. These Trojans use the same names as the legitimate programs, but are located in different folders. As a result a user does not suspect deception.

"***REGISTRY ASSISTANT***" - Includes registry search and replace, tips and tricks collection, registry shortcuts, useful links and utilities.

"***REGISTRY TRACER***" - Traces changes in the selected registry keys.

"RESCUE" - Allows to **easily** create/restore the backup copies of your registry or system files on the hard drive, network or floppy disks.

"***REGISTRY COMPRESSOR*** " - Can decrease the size of your registry and the memory it uses by removing deleted records from registry files.

"***RECOVERING WINSOCK2*** " - Resolving Internet connection problems when the Winsock2 registry key is damaged or infected by a virus.

"***PROCESS MANAGER***" - Allows you to analyze and control all of the processes and modules that are running on your computer.

"SYSTEM FILES EDITOR" - Looks like a Microsoft's SysEdit but it is more handier and allows you to automatically open your files subset.

"***RUN JOB***" - Advanced batch manager. Allows you to launch several programs simultaneously, delayed, or by "chain" - a series of jobs; each waiting for completion of a previous program.

"LAUNCH SOON" - Provides an easy way to launch applications with delay, recurrent or one time for day.

"FILE EXTENSION MANAGER" - helps to manage file extensions.

Choosing Security Level

You may set up Security Level via RegRun Control Center utility.

Click on the Options button.

What does mean each level for you?

Ultra High Level

Recommended for experienced users

1. WatchDog is ON.
2. Secure Start is Active (if you do have Windows 9X it is active in Windows mode too.)
3. File Protection is ON.
4. Anti Replacement is ON.
5. Check system on Shutdown is ON.
6. Infection Detector is ON.
7. Registry Tracer is ON.
8. Check Active Setup items is ON.

9. Suggested file extensions are MONITORED.
10. VxD and Drivers list is MONITORED.
11. Checking interval is set to 3 minutes.

High Level

Recommended for power users.

1. Watch Dog is ON.
2. Secure Start is Active (if you do have Windows 9X it is active in Windows mode too.)
3. File Protection is ON.
4. Anti Replacement is ON.
5. Check system on Shutdown is ON.
6. Infection Detector is ON.
7. Registry Tracer is ON.
8. Check Active Setup items is ON.
9. Suggested file extensions are MONITORED.
10. VxD and Drivers list is NOT MONITORED.
11. Checking interval is set to 10 minutes.

Medium Level

Recommended for most of users.

1. WatchDog is ON.
2. Secure Start Windows is Active.
3. File Protection is ON.
4. Anti Replacement is OFF.
5. Check system on Shutdown is OFF.
6. Infection Detector is ON.
7. Registry Tracer is OFF.
8. Check Active Setup items is OFF.
9. Suggested file extensions are NOT MONITORED.
10. VxD and Drivers list is NOT MONITORED.
11. Checking interval is set to 10 minutes.

Fast Launching

Recommended for using with notebooks or for computer rarely Internet used.

1. WatchDog is ON.
2. Secure Start Windows is NOT Active.
3. File Protection is OFF.
4. Anti Replacement is OFF.
5. Check system on Shutdown is OFF.
6. Infection Detector is ON.
7. Registry Tracer is OFF.
8. Check Active Setup items is OFF.
9. Suggested file extensions are NOT MONITORED.
10. VxD and Drivers list is NOT MONITORED.

11. Checking interval is set to 15 minutes.

Low Level

Only for manual manage startup, all protection features are deactivated.

1. WatchDog is OFF.
2. Secure Start Windows is NOT Active.
3. File Protection is OFF.
4. Anti Replacement is OFF.
5. Check system on Shutdown is OFF.
6. Infection Detector is OFF.
7. Registry Tracer is OFF.
8. Check Active Setup items is OFF.
9. Suggested file extensions are NOT MONITORED.
10. VxD and Drivers list is NOT MONITORED.

What is a virus?

A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:

- It must execute itself. It will often place its own code in the path of execution of another program.
- It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

What is a Trojan horse?

Trojan Horses are impostors--files that claim to be something desirable but, in fact, are malicious. A very important distinction between Trojan horse programs and true viruses is that they do not replicate themselves. Trojans contain malicious code that when triggered cause loss, or even theft, of data. For a Trojan horse to spread, you must, invite these programs onto your computers--for example, by opening an email attachment or downloading and running a file from the Internet.

What is a worm?

Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host

file. Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm.

What is Adware?

It is software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own. Usually they change the IE homepage and search engine.

What is Spyware?

Any product that employs a user's Internet connection in the background without their knowledge, and gathers/transmits info on the user or their behavior. Many spyware products will collect referrer info (information from your web browser which reveals what URL you linked from), your IP address (a number that is used by computers on the network to identify your computer), system information (such as time of visit, type of browser used, the operating system and platform, and CPU speed.) Spyware products sometimes are wrapped in other commercial products, and are introduced to machines when those commercial products are installed. See also Adware.

Secure Start can remove Trojans/usermode rootkits/spyware/adware using **RegRun Reanimator** with Application Database.

In addition…

1. **WMI tracing** opening file images during Windows boot. WMI logging is the great feature added to all versions since Windows XP. It allows to start Windows in the logged mode. We can detect all files used during Windows boot by analyzing the log. Feature is available in the **Bootlog XP** included to the Platinum.
2. **Registry boot logger**. RegRunRM boot driver collects full information about registry keys used during Windows boot.

Does Partizan is a panacea?

Hackers use a lot of rootkit modification combining with spyware components.

RegRun Platinum guarantees that you can clean your computer from a deep hidden rootkits and from common spyware.

Does it clean rootkits in the auto mode?

No. It uses Greatis Application Database for detecting known rootkits/viruses/spyware. We suggest you to update the database.

But some of the software will be detected as unknown – suspicious.

What you need to do in this case?

If you have enough computer skill to use professional tools included to the RegRun Platinum – OK, you can do it.

If not, you can send detailed system report to the Greatis Support center: http://greatis.com/support and we will send the special file for auto cleaning your computer. The service is free for RegRun's users.

What's about self-protection?

1. You can specify the own file name for Partizan executable.
2. RegRun generates the random name for executable in the Windows mode. In addition, it will crypt the executable for preventing detection using MD5 signature and strings.

How to start rootkit detection using Partizan?

Open RegRun Control Center.

Choose the "Partizan" tab and set up the Partizan checkbox.

Does Partizan work with Platinum Edition only?

The rootkit auto detection is allowed for RegRun Platinum users only. Other users can use it for deleting virus files.

Partizan is included to the free Reanimator software too.

How to uninstall Partizan?

Open RegRun Start Control.

Go to the Features menu.

Choose "Partizan" item.

Click on the "Remove" button.

Enable/disable RegRun Registry Guard.

RegGuard is used for protecting startup registry keys from modification. WatchDog icon is in red if the Registry Guard is active.

Enable/disable RegRun RunGuard.

RunGuard is used for controlling executed applications, pif, bat, scr files.

Enable/Disable using RegGuard before Virus Scan feature.

Suggest to disable if you have problems with using RegGuard.

RegGuard is activated before Virus Scan on default because it allows to the viruses from modification startup registry keys.

Scanning for Viruses at each Windows start is very useful for your safety.

Disable it only if you are sure.

Enable this option only if you are sure.

Scan for Viruses will not stop the Windows boot process even if it found something dangerous. You will see WatchDog notifying message and you will need to check your computer again.

Set up **Secure Scan for Viruses** only once for day.

Of course, if the first scan found problems and you will reboot, scanning will be active. The next scan will be skipped only after successful check.

Enable/Disable RegRun anti-rootkit technology.

Read more …