AnVir Task Manager

v5.2

User's Guide



Introduction \Rightarrow

AnVir Security Suite is utility software that gives users a comprehensive set of tools to put them in full control of their computer.

AnVir Security Suite gives full information about process, services, TCP/UPD connections, drivers, DLLs. It has descriptions for 70 000+ startup programs and services. It detects new and unknown Trojans using security analysis and alerts on new startups. It can speed up boot time (Delayed Startup), balance CPU usage, optimize memory. Tray icons shows status of disk, network, memory, CPU. Tray menu keeps last launched programs and folders. Also users can hide windows to system tray, set windows 'always on top', and change windows transparency.

AnVir Task Manager provides full set of Windows enhancements that help in every-day work

Security & Performance:

- Full information about <u>processes</u>, <u>services</u>, <u>Internet connections</u>, <u>drivers</u>, <u>DLLs</u> the best replacement for Windows Task Manager
- Descriptions for 70 000+ startup programs, Internet Explorer toolbars and services know what is running on your PC and remove what you don't need
- <u>Security analysis of programs behaviour detects Trojans and Spyware, alerts on new</u> <u>startups</u>
- keep your computer free from malicious programs
- <u>Speed up boot time (Delayed Startup)</u>, <u>balance CPU usage</u>, <u>optimize memory</u> *your computer can run faster*
- <u>Run programs as services on Windows startup, save process priority, monitor TCP/UPD</u> *best choice of IT Professionals*

Windows enhancements:

• Monitor <u>CPU</u>, <u>memory</u>, <u>HDD temperature and load</u>, <u>network</u>, <u>notebook battery</u> and show <u>icons in system tray</u>

how is utilized your hardware?

- <u>Click on title of any application to hide the window to tray, make it transparent, set it</u> <u>'always on top'</u>
- List of recently used folders in "Open"/"Save" dialogs
- Last launched programs and folders in tray menu

XP or Vista can be much more handy

Capabilities:

- Attractive user interface
- Can replace Windows Task Manager
- <u>Can run as portable application</u>
- Compatible with all popular antivirus
- Check files with 30+ antivirus engines
- Search on Google with one click

• Save HajackThis log

Requirements 🖶

Supported operation systems:

- Windows XP SP2
- Windows XP x64
- Windows 2003 SP2
- Windows Vista
- Windows Vista x64
- Windows 2008

Following features require admin rights:

- HDD temperature monitor
- Network traffic monitor

Software also works on following obsolete operation systems, but some features may be disabled:

- Windows 98
- Windows 2000
- Windows Me
- Windows XP

Editios

There are 4 editions of the product

- AnVir Task Manager Free freeware edition
- AnVir Task Manager basic features
- AnVir Task Manager Pro advanced features
- AnVir Security Suite all features

To compare editions have a look at this page.

Installation

Download the last version of setup file from <u>download page</u>.

Run the installer and follow instructions.

You can install simultaneously few editions of the product, but it's not recommended.

Uninstal 1 There are few ways to uninstall the product. Choose any of following ways.

- 1. Open Control Panel, switch to "Add/Remove Programs". Go to "AnVir Security Suite" and click Remove.
- 2. In the Start menu open AnVir Security Suite->Uninstall AnVir Security Suite.
- 3. In Explorer open folder where the product is installed and run "AnVir.exe Uninstall".

Settings of the program are not deleted during uninstall.

Note: if you disabled some startup items or moved them to delayed startup list, enable them before uninstall, if you want them to run on Windows startup.

Version Update

To get information about updates available, in the program main window go to Help->Check Version Update.

To update your installed version perform the same steps as for installation.

Download the last version of setup file from <u>download page</u>.

Run the installer and follow instructions.

You can install simultaneously few editions of the product, but it's not recommended.

Registration Key

To register the trial version of the program, go to Help->Enter Registration Key. Enter name and key into the registration dialog.

Portable Mode

You can run the program in portable mode.

Perform following steps to run AnVir Software program as portable application:

1. Install the software.

2. Copy AnVir.exe, AnvirHook.dll and VirusTotalUpload.exe (optional) to the destination folder.

3. Run AnVir.exe from the destination folder. Setup some program options that you need. Go to Tools->Options->Advanced->Where to store settings. Select anvir.ini. Press Apply. All settings will be stored in anvir.ini in the destination folder. If file anvir.ini is found in the folder of executable, all setting will be loaded and stored to this file (instead of registry).

4. Copy all files from "c:\Documents and Settings\{user name}\Local Settings\Application Data\AnVir" to the destination folder. If file startup.dat is found in the folder of executable, all extended setting will be stored to this folder instead of "Local Settings" folder.

5. If you run the program on USB device you will be asked for the registration data, when you run the program first time from the USB device (only 1 time for the device).

Title Menu

Title Menu - Notepad File Edit Format View H	On Ter (Always Visible) Create Icon in Tray And Hide Window	
File Edit Format View H Title menu (or syst Anvir Task Manager Menu commands: * On Top (Alwa) * Create Iconi * Always Place * Create Float * Transparent * Priority - Ch o Realtin = o High - o Above N o Normal o Below N o Low - F o Save Pr	Create Icon in Tray And Hide Window Always Place To Tray When Minimized Create Floating Icon Transparent Priority Resize Optio AnVir Security Suite Restore Move Size Minimize Maximize	when user right cli menu of window of 0% (Normal) front 10% m tray 20% nt dra 30% 40% dow 50% k othe 60% 70% 80% hile o 90% and au
o 320x240 × o 640x480 o 800x600 o 1024x768 o 1152x864 o 1280x800 o 1280x1024	Close Alt+F4	
		2 .::

Title menu (or system menu) is a menu that is shown when user right clicks on a title of any window. Other ways to open title menu: press Alt+Space, or left click on an icon in the left of a widow title.

AnVir Task Manager adds useful commands to the title menu of window of all applications.

<u>Menu commands:</u>

- On Top (Always Visible) The window always remains in the front
- Create Icon in Tray And Hide Window Place window to system tray
- Always Place To Tray When Minimized Window will be placed to tray instead of task bar when it is minimized
- **Create Floating Icon** Create small floating semi-transparent draggable icon that represent windows
- <u>**Transparent**</u> Make window semi-transparent
- **<u>Priority</u>** Change priority of the process that owns the window
 - Realtime Process can use all CPU resources and block other programs
 - High Process can use much CPU resources
 - Above Normal
 - Normal default priority
 - o Below Normal
 - Low Process can't use much CPU resources and wait while other programs do their jobs
 - Save Priority Save current priority of the process and automatically set this priority when the process starts
- <u>**Resize**</u> change size of the window to one of standard screen resolutions

- o 320x240
- o 640x480
- 800x600
- 1024x768
- 1152x864
- 1280x800
- o 1280x1024

Floating Icons

Create small floating semi-transparent draggable icon that represent windows



Hide windows to tray

Create an icon in system tray that represents a window. Minimize inactive windows to System Tray and save Taskbar space for minimized windows. Taskbar is located at the bottom of the screen. System Tray is located in the bottom right corner of the screen.



Open/Save Dialogs

Save	As				2103205910	125526		eneres e	? 🔀
	Save in:	🗀 project 1		~	G	1	ø	•	••
 C:\Documents and Settings\Administrator\My Documents\My Pictures C:\Documents and Settings\All Users\Documents C:\Program Files C:\ C:\Documents and Settings\Administrator\Desktop C:\Documents and Settings\Administrator\My Documents I. C:\Documents and Settings\Administrator\Desktop\project 1 2. C:\Documents and Settings\Administrator\Desktop\project 1									
Му	2. C:\Doc 3. C:\Doc 4. C:\Doc [Remove of Open AnV	uments and Settings uments and Settings current folder from F ir Security Suite	,Administrator(My Documen ,Administrator\My Documen ,Administrator\My Documen avorites]	ts\My Pi ts	ictures)	(Screi	ensh	ots	-
Му	My Computer								
		File name:	Title Menu				~		Save
M	y Network	Save as type:	Text Documents (*.txt)				*		Cancel
		Encoding:	ANSI				~]	.::

AnVir Task Manager allows you to access a list of recently used folder and favorites folders from the Save and Open dialogs.

AnVir Task Manager inserts an extra button in all Windows XP Open/Save dialogs and in all MS Office Open/Save dialogs. (On Vista this button appears in MS Office applicationsonly).

This button appear in the standard toolbar of Open/Save dialog.

When user clicks on this button, it shows a menu with list of recently used folders. Additionally, menu contains user's favorites folders. When user clicks on a menu item, Open/Save dialog navigates to the corresponding folder. This significantly saves time while opening and saving files.

Delayed Startup

😌 Delayed startup 🛛 🛛
Delayed startup items are started 1 minute after Windows is loaded (time interval can be customized) AnVir Security Suite must be included to the startup list. Move 'SynTPLpr' to Delayed Startup List?
You can set up delay time for the item. Delay time is time between Windows load and this startup item start.
O <u>C</u> ustom delay time 1
OK Cancel

Some programs are loaded by Windows after it starts. Such programs are listed in window Startup. When a user loads a computer he should wait while startup programs initialize.

You can speed up this process and not wait while all startup programs start.

Use Delayed Startup to speed up your computer's startup process. Delayed startup items will be started 1 minute (delay time can be customized) after Windows is loaded. So you can start using computer not waiting while Windows loads all startup programs.

To move a startup program to the delayed startup list select "Move to Delayed Startup List" in context menu on Startup page. In most cases you should use default delay time, but you can also setup custom delay time. Delay time is time between Windows loads and startup item is started.

When you place an application to delayed startup list, this application is removed from Windows startup list. This result in following rules:

- 1) AnVir Task Manager must run on Windows startup to launch delayed startup programs.
- 2) You should open settings of a program that was placed to delayed startup and set it not to run on Windows startup. This is because some programs will add itself to startup after they were removed from Windows startup list.
- 3) Only programs that are located in registry startup list can be placed to delayed startup. To move to delayed startup an application that stays in file system startup folders, run the program, switch to Process window, select the process and click Add to Startup. Item will be added to Windows startup. Then place the item to delayed startup.
- 4) Services and Internet Explorer extensions can not be placed to delayed startup.

To change custom delay time, right click on startup item, and select Edit Delayed Startup Item.

To remove the item from delayed startup list, right click on startup item, select **Edit Delayed Startup Item**, and click **Remove item from delayed startup list**.

The status of delayed startup items is shown on Startup window in column Delayed Startup.

User Interface

Program window contains:

- Main menu
- Toolbar
- Main Windows
- Detailed Information Windows
- Status bar

Command of main menu and toolbar depends on the active main window.

You can use menu View to hide and show Toolbar and Status bar.

You can use splitter between main windows and detailed information windows to change size of main windows.

You can dock detailed information windows to the left, top, or right border of the main window.

Main Windows

The program contains following main windows:

- Startup
- Applications
- Processes
- Services
- Log
- Antivirus

Window "Antivirus" is available in AnVir Security Suite.

Startup Window



Startup window contains following items:

- Programs that run on Windows startup, or on user login.
- Non Microsoft services that run on Windows startup.
- Internet Explorer extensions: browser helper objects, toolbars, menu items.

<u>Columns</u>

- Check mark If the item is disabled, check mark is cleared.
- Name Name of section in registry or name of file. If item is unchecked, it will not be

launched on startup.

- Value Command line: path to executable file and parameters
- Product Product description provided by file vendor
- Security Risk Overall security risk for this item. 'No risk' reliable program. 'Low'/'Medium' - pay attention, check on Virustotal. 'High' - remove this item. To change security risk on your opinion, in the context menu click 'Change Security Rating, Add Comment...' and add your comment to this item.
- Company Product vendor
- Startup location Where from item was loaded
- When Added to Startup When item was detected first time. Items detected in the last week are marked.
- State Is the corresponded process running
- Status Enabled items run on Windows startup. Disabled items does not run on Windows startup.
- Delayed Startup Use Delayed Startup to speed up your computer's startup process. Delayed startup items will be started 1 minute (delay time can be customized) after Windows is loaded. So you can start using computer not waiting while Windows loads all startup programs. To move a startup program to the delayed startup list select "Move to Delayed Startup List" in context menu on Startup page.

<u>Menu commands</u>

File

Save HijackThisPro Log... – Save information about system to the file in HijackThis format

Save Startup Report as Html... - Save list of startup programs to html file

Export Startup to File... - Save list of startup programs to reg file

Import Registry File... – import data from reg file to system registry

Exit – exit program

<u>Startup</u>

Detailed Info Double Click – Show/hide detailed info window

Change Security Rating, Add Comment... – Change security rating of a file and add user comment to the file

File Properties Alt+Enter - Target File Properties

System Menu Shift+RClick – Show system context menu

Navigate

Show File In Explorer – Open Explorer and select file that run on startup

Switch To Process – Open Process window and select process of the startup program

Open Entry Location in Registry – Open Registry Editor and select startup program

Open Entry Location in Services Manager - Open Services Manager

Open Entry Location in Explorer - Open Explorer and select file that is located in startup location

Switch to Service - Open Services window and select the service of the startup program

Run Now – Run startup program

Stop Process – Stop process of the startup program

Edit Delayed Startup Program – Edit startup delay time or restore from Delayed Startup List

Move to Delayed Startup List - Move startup program to Delayed Startup List

Disable (Quarantine) – Disable startup program from running on Windows startup

Enable - Enable disabled startup program for running on Windows startup

<u>Edit</u>

Delete Entry Del – Delete record from Windows startup list

Edit Entry... – Change name, path or parameters

Add Entry... - Add new program to startup

Check with AntiViruses on VirusTotal - Check file with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about startup program in Google

Google News - Search information about startup program in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about startup program

Copy Path - Copy to clipboard path of startup program file

Find... Ctrl+F – Find text in the window

Find Next F3 – Find text in the window

Refresh F5 – refresh data in the window

View

Columns - select columns to show/hide in the window

Toolbar – show/hide toolbar

Grid - show/hide grids in all windows

Status Bar - show/hide status bar

Detailed Info - Show/hide detailed info window

Text Colors

Security Risk Rate [red/yellow/green] – Enable/disable colors of security analysis Hide Microsoft Programs [grey] – Show programs of Microsoft with grey text color Mark New Startup Entries [bold] – Mark new startup programs with bold font Mark Running Programs [blue] – Mark running startup programs with blue text color

<u>Programs that run on Windows startup, or on user login can be located in following locations:</u>

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKCU\Software\Microsoft\Windows\CurrentVersion\Run HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices

%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startup %SystemDrive%\Documents and Settings\<username>\Start Menu\Programs\Startup HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup

 $HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell\Folders,\ Common\AltStartup$

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common AltStartup

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, AltStartup HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, AltStartup

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows, load HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows, run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar HKLM\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars HKCU\Software\Microsoft\Internet Explorer\Extensions HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions HKCU\Software\Microsoft\Internet Explorer\Extensions HKCU\SOFTWARE\Microsoft\Internet Explorer\Extensions

Applications Window
Applications List

🕈 AnVir Task Manager Pro			
Eile Applications View Tools Help			
Save 🔻 🤁 🖳 🥅 🔯 🔇 🗱 🗃 🎘 🐟			
Startup 🦳 Applications 🥋 Proc	esses ở Services	Log	
Window 👻	Tray Icon Pr	rocess Process ID State	us 🔯
<i> б</i> . Аквариум - 06 - Без женщин - Winamp	Ø	Winamp Rus 2288 Runn	ning
🔮 AnVir Software, Security Suite, Task Manager Pro, Virus Destroyer: H	ome - Microsoft Int 👰 26.02.2008 01:46 🛛 🧕	Internet Explorer 1716 Runn	ning
🔮 AnVir Software, Security Suite, Task Manager Pro, Virus Destroyer: H	ome - Mozilla Firefox 🥮 26.02.2008 01:45 👹	Firefox 3728 Runr	ning
😁 An Vir Task Manager Pro		AnVir Task Manager Pro 3692 Runn	ning
🥦 my document.txt - Блокнот	<u> </u>	Блокно AnVir Software, Security Suite, Task Ma	anager Pro, 💡
WIR - Microsoft (instal Current Ch. WIP) (IP) bistom but 81	2011 - 10 - 10 - 10 - 10 - 10 - 10 - 10	Microso Virus Destroyer: Home - Microsoft Inter	net Explorer
Virtual I 🗹 Detailed Info Double Click		Virtual F Tray Icon: 26.02.2008 01:46	
🖉 besulv 💻 Create Icon in Tray And Hide Window	<u></u> 26.02.2008 01:46	Paint Process: Internet Explorer	ļ
	9 26.02.2008 01:46 9	Pant Process ib. 1710	μ
UI I POMKI U Bring To Front	26.02.2008 01:46	Тромка	d
Always Place To Tray When Minimized			
Manage Window	On Top (Always Visible)		
Suitch To Discose (3)	Close Window		
	Hide Window		
🗸 End Task Del 🔄			
Text Operations	Iransparent V% (Normal)		
	Minimize 10%		
	Maximize 20%		
X 🔰 General 📝 Product Information 🔊 DLL 🧔 Files	Connections Perform 30%	Windows 🛃 Threads 溸 Handles 🧿 Drivers	
Show connections for all processes Show I CP Show I CP			
Protocol Process Local Address Local F	ort Remote Address 50%	ate Network: Rec N	etwor 🔻 🛛 🔼
an TCP 😼 Firefox ilya.cpms.ru 3239	cp42.agava.net 80 (http)	🖉 Established (Established conne 🔸 5,91 KB 👔	1,57 KE
TOP Firefox ilva.cpms.ru 3242	(Wite) Switch To Dresses	CLUSE WAIT Connection has 453 6avr	<u>1,21 K5</u>
S TUP V Firefox ilya.cpms.ru 3240	CAR SWICE TO Process	ULUSE_WAIT (L'onnection has 🔸 537 δάνπ 🍸	1,15 Kb -
P VDP Piretox ilya.cpms.ru 3241	K Close TCP Connection	Established (Establishe TCP	
E UDP L Generic Host Pro * 2099	Kill Process	Process: Application Layer Gate	eway Service
TCD System Ilya.cpms.ru 3030		Established (Establishe Local Address: localhost	
Application Layer localnost 1027	Write Traffic of Process to File		
C TCD Strategy logalhest 2105	G File Properties	Established (Establishe Remote Port: 32998	
TCP Firefox localhost 2109		Established (Established State: Listen (Listening for inco	oming connection)
	Show File In Explorer	Time: 22.02.2008 04:25:10	, i
	System Menu	Module Name: alg.exe	2 - L
		Module Path: Ctl/386(System32	ziaig.exe

Window "Applications" contains list of running applications that have top level windows.

<u>Columns</u>

- Window- Window title of running application
- Tray Icon- Tray icon created by AnVir Security Suite and time when window was hidden to tray
- Process Process that owns the window
- Process ID Unique numerical identifier of process that owns the window
- Status Application status: "Running" or "Not Responding"

<u>Menu commands</u>

<u>File</u>

Save HijackThisPro Log ... - Save information about system to the file in HijackThis format

Save Applications Report as Html ... - Save list of running programs to html file

Exit – exit program

Applications

Detailed Info Double Click - Show/hide detailed info window

Create Icon in Tray And Hide Window – Place window to system tray

Restore From Tray And Remove Icon – Remove icon of a window from system tray and restore window

Create Floating Icon – Create small floating semi-transparent draggable icon that represent windows

Bring To Front – Bring application to front

Always Place To Tray When Minimized – Window will be placed to tray instead of task bar when it is minimized

Manage Window

On Top (Always Visible) - Place window on top of other windows

Close Window – Close window

Hide Window - Hide visible window

Unhide Window - Unhide hidden window

Transparent – Make window semi-transparent

Minimize - Minimize window

Maximize - Maximize window

Switch To Process - Open Process window and select process of the application

End Task Del – Terminate application

Text Operations

Copy to Clipboard - Copy to clipboard full information about application

Copy Title - Copy to clipboard title of application

Find... Ctrl+F – Find text in Applications window

Find Next F3 - Find text in Applications window

Refresh F5 – refresh data in Applications window

View

Columns - select columns to show/hide in the window

Toolbar – show/hide toolbar

Grid - show/hide grids in all windows

Status Bar - show/hide status bar

Detailed Info - Show/hide detailed info window

Processes Window
Processes List and Performance Graph

🕀 AnVir Task Ma	• AnVir Task Manager Pro										
<u>File Processes V</u>	jew <u>T</u> ools <u>H</u> elp										
Save 🔻 🤔 Viev	Save 🔹 🖓 View 🔹 🔍 📑 🝏 🐑 😞 🐟 🖓 🖄 🌲 🗱 🚺 🔿 🔍 📦 💭 🚳 💭										
Startup		Ę	<u>і</u>	rocesses	÷	Services		Log]		
Process	Product	Secu	rity	Startup		CPU %	Disk 💌	Net	Network:	Memory Usage	Window Title 🔼
💾 totalcmd.exe	💾 Total Commander 32 bi	🔰 Ne	o risk			5	460 Kb/s			14 580 K 불	Total Commander 7.02a - HE 3AP
崎 virtual pc.exe	🌖 Virtual PC 2007	🔰 No	o risk			3	138 Kb/s			20 668 K 🧕	Virtual PC Console
🟈 winamp.exe	🤣 Winamp Rus	🔰 No	o risk			3	13 Kb/s			AnVir Task Mar	nager Pro
🗂 svchost.exe	Generic Host Process f	🔰 No	o risk	🔗 Services: C/	тужба об	0	12 Kb/s	🦊 7	1 920 6	AnVir Task Manage	er Pro
🛨 anvir.exe	🛨 🗛 AnVir Task Manager Pro	🔰 Ne	o risk	👵 Registry: Us	er\Run\A	4	6 Kb/s		-	Process: anvir.exe	PID: 3692 (Joe) (In) (in Toeld Meneger Bre) (In) (in ea
alg.exe	Application Layer Gate	V No	o risk	🔗 Services: Cr	чужба шл	0	0			Command Line: "C	"Program Files)AnVir Task Manager
🖳 atiptaxx.exe	ATI Desktop Control P	🔰 No	o risk	😫 Registry: Ma	ichine\R	0	0			Company: AnVir So	ifware
🧧 calc.exe	🧕 Калькулятор для Win	V No	o risk			0	0			Process Start: 26.	02.2008 01:06 when Windows starts
📓 calc.exe	📓 Калькулятор для	🕖 N	o risk			61	0			Resources usage:	CPU-4%, Memory-10 Mb, Pagefile-1
🙋 calmain.exe	🚰 Canon Camera Access	V No	o risk	🧬 Services: Ca	anon Cam	0	0			User Name: ILYA\1	
🔇 cpgalert.exe	🔇 Insight Local Alert Serv	V No	o risk	🜮 Services: In:	sight Loc	0	0			Priority: High Decemt Decements 2	622
me cpqdmi.exe	Compaq DMI Service	V No	o risk	🜮 Services: cp	iqdmi	0	0			Parent Process: 2	032 - explorer.exe 12 2007 15:51:24 556
csrss.exe	Client Server Runtime	V No	o risk			0	0			Travicons Text: Cl	PIIIIsane: 17% a Diskl oad C:
Ctfmon.exe	Z CTF Loader	V No	o risk	🚡 Registry: Us	er\Run\c	0	0			U In: 3.40 KE/s	Out:0. байт/siCPU Usage: 17% а
dcsuserprot.exe	DiamondCS ProcessG	🔰 Ne	o risk	🔗 Services: Di	amondCS	0	0			2401	
g explorer.exe	🛃 Проводник	V No	o risk			6	0			18 008 K	Total Commander 7.02a - HE 3APE
😻 firefox.exe	🥘 Firefox	J No	o risk			2	0	🦊 7	1,29 КБ	94 984 K 🍓	Great software applications, every
G googletoolbarn	🧕 GoogleToolbarNotifier	V No	o risk	🔓 Registry: Us	er\Run (0	0			408 K	✓
<	ALIA										
본 🧊 General [者 Product Information 🛛 🛐 🛛	DLL 🚺	👂 Files	崎 Connection	ns 🔀 Per	formance	🦂 Statistics	🔲 Win	dows 🛃 Tł	nreads 🔚 📩 Handles	O Drivers
	100%		- CPI	min=2% may=96	12		A				
Air locesse			= Men			6		++++			
Period		S	 Disk 	min=0 Kb/s max	=12384 КЬ/	s i i i i					
Realtime	E CPU 8K/s		Dov =	inload Speed min	=0 Kb/s ma:	k=3 Kb/s					
O 2 hours	Memory			au sueeu min=u	NU/S IIIdx=L	INU/S		+			
O 1 dau	Disk Duž										وور بهدو وي بروي بووي
	Download	•						⊨⊨⇒			
C I week	Upload 🛛 🖌										
Chart Scale	4 K/s				tt het he		╢╢┼┼┼┼┼	+		╶╫┼┼╫┼	
CPU Memo	ru Disk Network	1			11 Î 6						
2 100% 1 Gb	4 Mb/s 8 K/s	40		++++++	IV [┼┼┟┼			
	. I . I . UKKe	11.5	Δ. Ι	Sala H	ti i i i	11	K HANN	ANIA		all tablik for the	
		╇ᢏᠵᢂ	CANN-	AND MANA AND AND AND AND AND AND AND AND AND	n m m	, san sa	᠋ᡁᢆᡣᢪᡆᠯᠵᠱᠵᡀ	A A TAU	ANN ANNA -	the destriction of the second s	
	Ч́с "Ц с ∣µкия			بدائر و و در د					كتويدوهم		
CPU Usage: 100%	CPU Usage: 100% cal: 61% system 8% ex; 50° Disk Load C: 87% 50°C D: 0% D: 1% totz 🖬 Memory Usage: 52% Total: 1023 Mb Used: 5 🛄 In: 4,37 KE/s Out: 0 Gayri/s Received: 1,76										

Processes window contains list of running processes.

<u>Columns</u>

- Process Process name
- Product Product description provided by file vendor
- Security Risk Overall security risk for this item. 'No risk' reliable program. 'Low'/'Medium' - pay attention, check on Virustotal. 'High' - remove this item. To change security risk on your opinion, in the context menu click 'Change Security Rating, Add Comment...' and add your comment to this item.
- Startup Type of a process startup if it is run on Windows startup
- CPU % Processor usage
- Disk Load Summarized amount of data that process reads from disk and writes to disk per second
- Network: Received Amount of data downloaded by a process from Internet or network
- Network: Sent Amount of data uploaded by a process to Internet or network
- Download Speed Current download speed
- Upload Speed Current upload speed
- Memory Usage Set of memory pages visible to a process in physical RAM
- Pagefile Usage Amount of pagefile space that a process is using currently
- Work Time Time pasts since a process was created [days hours minutes] or [hh:mm:ss]
- Priority Scheduling priority of a process
- PID Numeric identifier used to distinguish one process from another. Process IDs are valid from process creation time to process termination.
- Parent Process Unique identifier, name and icon of process that created a process
- Window Title Title of a process window

- Tray Icons Text Text of tray icons and icon in system tray created by a process
- Company Product vendor
- Executable File Path to the process executable file
- CPU Time Processor time usage [hh:mm:ss]
- User Name Name of user started a process
- First Detected When process was detected first time. Items detected in the last week are marked.

<u>Menu commands</u>

<u>File</u>

Save HijackThisPro Log... - Save information about system to the file in HijackThis format

Save Processes Report as Html... - Save list of processes to html file

Exit – exit program

Processes

Detailed Info Double Click – Show/hide detailed info window

Change Security Rating, Add Comment... – Change security rating of a file and add user comment to the file

File Properties Alt+Enter – Properties of file of the process

System Menu Shift+RClick – Show system context menu of the file of the process

<u>Navigate</u>

Show File In Explorer – Open Explorer and select file of the process

Switch to Startup - Open Startup window and select the startup item of the process

Switch to Service - Open Services window and select the service of the process

Switch to Parent Alt+Up - Select parent process

Add to Startup – Add running process to Windows startup

Set Priority - Change priority of the process

Realtime - Process can use all CPU resources and block other programs

High – Process can use much CPU resources

Above Normal

Normal – default priority

Below Normal

Low - Process can't use much CPU resources and wait while other programs do their jobs

Auto Change Priority... – Open Processes Priority dialog, priority will be automatically changed when the process starts

Run As Service - Run application as service on Windows startup before user login

New Process... Ctrl+N - Run new process

Kill Process Del – Terminate process

Kill Process Tree Ctrl+Del - Terminate process with all process that it created

Block Process (Quarantine) – Open Blocked Processes dialog, automatically terminate process immediately after it starts

Restart – Terminate process and run it with the same parameters

Suspend Process - Suspend process, freeze all operations of the process

Resume Process - Resume suspended process

Free Memory – Swap all memory used by a process to the disk. When a process becomes foreground again and it needs its memory it reads memory from disk.

Check with AntiViruses on VirusTotal - Check file with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about process in Google

Google News - Search information about process in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about process

Copy Path - Copy to clipboard path of process file

Find... Ctrl+F – Find text in the Processes window

Find Next F3 – Find text in the Processes window

Refresh F5 - refresh data in the Processes window

View

Columns - select columns to show/hide in the window

Always On Top - Set application above all other applications

Toolbar – show/hide toolbar

Grid - show/hide grids in all windows

Status Bar - show/hide status bar

Detailed Info - Show/hide detailed info window

Text Colors

Security Risk Rate [red/yellow/green] – Enable/disable colors of security analysis

Hide Microsoft Processes [grey] - Show programs of Microsoft with grey text color

Mark New Processes [bold] - Mark new processes with bold font

Mark Processes that Consume Resources [blue+red] – Mark processes that consume resources with blue text color and consumed resources with red color

Services Window Services List

🗣 AnVir Task Manager Pro								
<u>Eile S</u> ervices <u>V</u> iew <u>T</u> ools <u>H</u> elp								
Save 🔹 🖓 View 🔹 🔍 🛐 💋 🛞 🕨 🔳 💥 🔀 🏵 🙎 🗊 🖾 🎘 🍪 🤹								
Startup 🦰 Applications 🥋	Processes Service	s 🛄 L	og					
Name Security Risk	Identifier Start Type	State	Description	Product				
TNetwork Provisioning Service 🔰 No risk	xmlprov 🖌 🖌 On demand		Manages XML configuration file	s on a domai 📰 Generic Host Process f				
Wireless Zero Configuration 🥑 No risk	WZCSVC 🥝 Auto on starl	up 🕨 Running	Provides automatic configuration	n for the 802 🧮 Generic Host Process f				
Security Center 📝 No risk	wscsvc 🤤 Disabled		Monitors system security setting	s and config 🛄 Generic Host Process f				
Automatic Indiates Deutsia Deutsia	wuauserv 🧭 Auto on starl	up 🕨 Running	Enables the download and insta	Ilation of Wi Generic Host Process f				
	WmiApSrv V On demand	N N	Provides performance library info	ormation fro 🔲 WMI Performance Ada				
Line Wind Change Security Rating, Add Comment	W321 me V321 me	up 📂 Hunning	Maintains date and time Wirel	ess Zero Configuration				
File Properties Alt+Enter	wmi Un demand	n 🕨 Duning	Provides systems manag	ity Risk: No risk				
Nicht Custon Manu Chifu DChilu	Winnight Auto on stat	up 📂 Hunning	Frovides a common intelidentif	ier: WZCSVC				
Portal	Charles The Tendence Coand	up 📂 Hunning	Betrieves the serial num State	ype: Auto on startup				
Navigate	Show File In Explorer hand		Manages and implemen PLOCE	ss ID: 824				
Vinua —	Switch To Process	un 🕨 Bunning	Provides support for shaDescri	iption: Provides automatic configuration fo				
Unive Stop		ap p roming	Provides support to hos	ct: Generic Host Process for Win32 Servic				
Unint Change Startup Type	Auto on startup and		Manages an uninterrupt	any: Microsoft Corporation				
Wind W Delate Del	and and		Enables Windows user	and Line: C:\VVINDOVVS\System32\svchos				
Telne			Enables a remote user t	TDI				
Check with AntiViruses on VirusTotal	Disabled (Quarantine)	un 🖿 Running	Maintaine linke hetweenFirst D	etected: 12/23/2007 20:30				
Search in Web			Type: :	shared process				
X V	Coogle	an 🥝 Chatlatian 🗖	🗌 Vičenlausi 📕 Theored 📑	Handles 🙆 Dúres				
Text Operations	Google News	ce 🥰 Statistics [windows 🛄 Threads 📊	Handles UTIVers				
Starup/Services Databaser 👔 Copy to Clipboard	Analysis		Process Properties					
Key: Automatic Updates/wu Velue: CVV/(NDQ)/(Sharata Copy Path	🔰 Runs on startup <servic< td=""><td>es></td><td>Generic Host Pro</td><td>cess for Win32 Services</td></servic<>	es>	Generic Host Pro	cess for Win32 Services				
Value. C. (WINDOWS (Syster) Copy I dui	Established Internet cor	nections: 3						
Generic Host Process for Wi 👷 Find Ctrl+I	F Startup database analys	is <regular entry=""></regular>	Process	Svchost.exe				
Enables the download and it 😪 Find Next E3	Product of Microsoft		Process ID Date	C(V) (ND OV (C) sustan 20) such set				
this service is disabled, this comparer minimized and the	Uverall security risk	: NO TISK	Fatri	C:\\u(NDO\u(S) Sustem22\suchast				
the Automatic Updates feature or the Windows Update Web			Process Start	2/10/2008 21:07				
site.			Startup	Services: Wireless Zero Configurati				
1 entry found in startup database:			Besources usage	CPU-0% Memory-20 Mb Pagefile-1				
Status: Part of Windows			User Name	NT AUTHORITY\SYSTEM				
otherwise updates available for download. Manual updates			Priority	8 - Normal				
via Windows Update Version 6 web site still requires	× <		> <					
🏼 CPU Usage: 12% anvir 7% explorer 3% 👘 📕 Disk Load	C: 5% explorer 3 Kb/s anvir 3 K 🧮	Memory Usage: 60%	Total: 255 Mb Used: 1 📕 In:	0 bytes/s Out: 0 bytes/s Received: 1.2				

Services window contains list of all system services.

<u>Columns</u>

- Name Display name of the service
- Security Risk Overall security risk for this item. 'No risk' reliable program. 'Low'/'Medium' - pay attention, check on Virustotal. 'High' - remove this item. To change security risk on your opinion, in the context menu click 'Change Security Rating, Add Comment...' and add your comment to this item.
- Identifier Identifier of the service
- Start Type When Windows starts the service. Auto start at boot time, Manual allows Windows to start a service when needed, Disabled stop a service from starting, even if needed.
- State Current state of the service
- Process ID Process identifier of the service
- Description Description of the service provided by vendor
- Product Description of the product provided by vendor
- Company Vendor of the service
- Command Line Full path to the service binary file with arguments
- Dependencies Names of services and drivers that must start before this service
- Group Load ordering group to which this service belongs
- First Detected When service was detected first time. Items detected in the last week are marked.
- Type Type of the service

<u>Menu commands</u>

File

Save HijackThisPro Log ... - Save information about system to the file in HijackThis format

Save Services Report as Html ...- Save list of services to html file

Exit - exit program

Services

Detailed Info Double Click - Show/hide detailed info window

Change Security Rating, Add Comment... – Change security rating of a file and add user comment to the file

File Properties Alt+Enter – Properties of file of the service

System Menu Shift+RClick - Show system context menu of the file of the service

Navigate

Show File In Explorer – Open Explorer and select file of the service

Switch To Process - Open Process window and select process of the service

Start - Start service

Stop – Stop service

Change Startup Type - Change startup type of the service

Auto on startup - Run on Windows startup

On demand – Run when other programs need this service

Disabled (Quarantine) – Block from running

Delete Del – Delete record of the service

Check with AntiViruses on VirusTotal - Check file with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about startup program in Google

Google News - Search information about startup program in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about service

Copy Path - Copy to clipboard path of service file

Find... Ctrl+F – Find text in Services window

Find Next F3 – Find text in Services window

Refresh F5 - refresh data in Services window

View

Columns - select columns to show/hide in Services window

Toolbar – show/hide toolbar

- Grid show/hide grids in all windows
- Status Bar show/hide status bar
- Detailed Info Show/hide detailed info window

Text Colors

Security Risk Rate [red/yellow/green] – Enable/disable colors of security analysis Hide Microsoft Services [grey] – Mark services of Microsoft with grey text color Mark Running Services [blue] - Mark running services with blue text color

Microsoft services - Show services of Microsoft in the window

Not Microsoft services - Show services of other companies in the window

Log Window

Log of Processes Activity Networks and the second second

Log window contains records of following system events:

- Processes created
- Processes terminated
- Windows created

<u>Columns</u>

- Time Date and Time of Event
- Event Process Name, Process ID, Parent Process Name, Process Working Time, etc.
- Data Command Line of Process, Window Title, or Description of Startup Item

<u>Menu commands</u>

<u>File</u>

Save HijackThisPro Log... - Save information about system to the file in HijackThis format

Save Log Report as Html... - Save log to html file

Exit – Exit program

Log

Text Operations

Copy to Clipboard - Copy to clipboard line from the log

Find... Ctrl+F – Find text in Log window

Find Next F3 – Find text in Log window

Clear All – Clear log

Switch To Process - Open Process window and select process that correspond to the log record

View

Columns – select columns to show/hide in Log window

Toolbar – show/hide toolbar

Grid – show/hide grids in all windows

Status Bar - show/hide status bar

Antivirus Window Antivirus scanner

🕈 AnVir Security Suite		
File Operations View Help		
Startup 📄 Applications 🥋 F	Processes I Log STOP Antivirus	
Folder Subfi	olders Checked files Infected files Status	Add Folder
C:\My Program Files\ Yes	88 72 Finished	
		Remove
		Bemove All
anvir securi	ty suite	
diffi securi	ry suite	
Check Pause See	Antivirus nage for more details	
Time 💌 Event	ОК	Clear
11/19 15:06:38 File contained virus Zhelati	Zhelatin_u	
11/19 15:06:38 File contained virus Zhelatin: uan uereteu	C. NMY Frogram Files Zineraum vam Zhelatin_dam	Save to File
11/19 15:06:38 File contained virus Warezov.pk. deleted	C:\My Program Files\Warezov\pk\Warezov_pk1	
11/19 15:06:39 File contained virus Warezov.pk deleted	C:\My Program Files\Warezov\pk\Warezov_pk2	
11/19 15:06:39 File contained virus Warezov.pk deleted	C:\My Program Files\Warezov\pk\Warezov_pk3	
11/19 15:06:39 File contained virus Warezov.pk deleted	C:\My Program Files\Warezov\pk\Warezov_pk4	
11/19 15:06:39 File contained virus Warezov.Is deleted	C:\My Program Files\Warezov\ls\Warezov_ls1	
11/19 15:06:40 File contained virus Warezov.ls deleted	C:\My Program Files\Warezov\Is\Warezov_Is2	
11/19 15:06:40 File contained virus Warezov.lc deleted	C:\My Program Files\Warezov\lc\Warezov_lc	
11/19 15:06:40 File contained virus Vidlo.Ae deleted	C:\My Program Files\Vidlo\ae\Video_Ae	
11/19 15:06:40 File contained virus tibs deleted	C:\My Program Files\tibs\tbs4	
11/19 15:06:40 File contained virus tibs deleted	C:\My Program Files\tibs\tibs	
11/19 15:06:41 File contained virus tibs deleted	C:\My Program Files\tibs\tibs2	
11/19 15:06:41 File contained virus tibs deleted	C:\Mv Program Files\tibs3	
• • • • • • • • • • • • • • • • • • •	>	
		-
III CPU Usage: 10%	Disk Usage: C:99% D:0% J:0% totalcmd 1135 Kb/s	explorer 4 Kb/s

Antivirus window allows to perform quick scan.

Virus database contains most propagated viruses only.

Menu Tools Menu commands

<u>Tools</u>

Options... – Settings dialog

Find DLL, File, Driver or Process

Find Loaded DLL – Find all processes that load a DLL

Find Locked File – Find all processes that use a file

Find Driver - Find driver with a specified name

Find Startup Program - Find a Startup Program with a specified name

Find Service - Find Service with a specified name

Find Process - Find Process with a specified name

Find Data in Log – Find text in the log

Check Any File with AntiViruses on VirusTotal - Check file with 30 AntiVirus engines on VirusTotal.com

System Information – Show detailed system information

Devices

Device Manager - Display and control the hardware attached to the computer

<u>Disk</u> – Some disk operation

Backup Files

Check Disk

Clean Disk

Disk Defragmenter

Set some Windows settings

<u>Display</u>

Keyboard

Mouse

Network Connections

Phone and Modem

Printers and Faxes

Sounds and Audio Devices

<u>Security Related</u> – Set some Windows settings

Security Center

Automatic Updates

Cookies

Internet Options

Shared Folders

Windows Firewall

Windows Settings

System Properties

Folders

Power Options

Regional and Language Options

Scheduled Tasks

User Accounts

Windows Task Manager

Edit Services

System Administrator Stuff

Computer Management

Disk Management

Event Viewer

Group Policy

Indexing Service

Msconfig

Performance Monitor

Registry Editor

Removable Storage

Removable Storage Operator Requests

Security Certificates

Security Policy

Users and Groups

Windows Management Instrumentation

Detailed Information Windows

Detailed information windows gives full information about startup items, running processes, services and drivers.

Full list of detailed information windows:

- General Window
- Product Information Window
- Dll List Window
- <u>Files List Window</u>
- <u>Connections List Window</u>
- Performance Window
- <u>Statistics Window</u>
- <u>Windows Tree Window</u>
- <u>Threads List Window</u>
- Handles List Window
- Drivers List Window

Detailed information windows available when one of following main windows is active:

- Startup
- Applications
- Processes
- Services

To get detailed information, open appropriate main window and select desired item in the main window. Detailed information about selected item will be shown in detailed information windows.

You can use splitter between main windows and detailed information windows to change size of main windows.

You can dock detailed information windows to the left, top, or right border of the main window.

General Window

General window contains following blocks:

- Startup/Services Database
- Security Risk Analysis
- Process Properties

Startup/Services Database

This block gives information about startup item or service. Colors:

- Green reliable item
- Red harmful item
- Yellow few variants found in the database

Security Risk Analysis

This block gives detailed security analysis of the item. Following possible results can be shown:

Harmful:

- Fake extension of this file disguises its real file type.
- Name of this file simulates valid Microsoft file.
- Your own comment for this program.
- Security status of the item that was found in startup database.
- Name of this file was found in database of Trojans file names.
- This file of the program has 'hidden' attribute.
- Not Microsoft file in Windows folder.
- File has no company name provided by vendor.
- File has no internal description provided by vendor.
- The program has no windows or system tray icons.
- Service has no description provided by vendor.
- Program was detected first time not long ago.
- Program runs on Windows startup.
- Program can connect to Internet or use phone.

Reliable:

- Your own comment for this program.
- File was signed by a registrar.
- Security status of the item that was found in startup database.
- Product of Microsoft.
- Program has visible elements of user interface: windows or icons in system tray.

Process Properties

- This block gives detailed information about running process:
- Process
- Process ID
- Path
- Command Line
- Process Start
- Startup

- Resources usage
- User Name
- Priority
- Parent Process
- Window Title
- Tray Icons Text
- Company

Product Information Window

Product Information window contains following blocks:

- Version
- Service Description
- Your Comment

Version

This block contains information about version and certificate of the file:

- File Version
- Description
- Copyright
- Comments
- Internal Name
- Legal Trademarks
- Original File name
- Product Name
- Product Version
- Private Build Description

Exact list of fields may be different for different files.

Service Description

This block contains description of the service provided by the vendor.

Your Comment

This block allows you to add some comments and set security risk rating for the file.

Dll List Window

Dll List	
Detailed Information	E
🥂 Performance 📔 🥞 Statistics 📔 🗔 Window	ws 🛃 Threads 🔚 🚼 Handles 🚺 🕥 Drivers
🦪 📝 General 🛛 📝 Product Information	💁 DLL 🛛 🧔 Files 🛛 🛸 Connections
Select All Processes Name Filter:	
Name Product First	t Detected 🔺 🛛 Full Path 🧧
Sprio.dll Prio Process Control 2 Image.exe Image.exe Application Layer Gatewa 07.12 Swshtcpip.dll Windows Sockets Helper 05.12 Image.exe Image.exe 05.12	21.02.2008 23:58 i:\Program Files\Prio\prio.dll 2.2007 15:03 C:\I386\System32\alg.exe 2.2007 15:37 C:\I386\System32\wshtcpip.dll
 Product: Application Layer Gateway Service Company: Microsoft Corporation Full Path: C:\l386\System32\alg.exe Version: 5.1.2600.2180 Date: 17.08.2004 15:04 Processes: Application Layer Gateway Service 	00 Image: Switch To Process Image: Switch To Process
S. Type: DLL S. Load Address: 0x01000000 Size: 53 248 Extension: exe First Detected: 07.12.2007 15:03	00 Save Report as Html .dll 00 Check with AntiViruses on VirusTotal .dll 01 Search in Web ≥

Dll list window shows list of dlls that are loaded by selected processes.

Columns

- Name Name of the module
- Product Description of the module
- Company Vendor of the module
- Full Path Full path of the module
- Version Version of the module
- Date Date and time when the module was created
- Processes In which processes of selected processes the module is loaded
- Type Type of the module (driver, font, library)
- Load Address Load address of the module
- Size Size of the module in bytes
- Extension Module extension
- First Detected When dll was detected first time. Items detected in the last week are marked.

Context Menu commands

Switch To Process - Open Process window and select process that use a DLL

File Properties - Open system dialog with properties of the DLL file

Show File In Explorer – Open Explorer and select file of the DLL

System Menu - Show system context menu of the file

Save Report as Html... - Save list of DLL to html file

Check with AntiViruses on VirusTotal - Check DLL with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about DLL in Google

Google News - Search information about DLL in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about DLL

Copy Path - Copy to clipboard path of DLL file

Files List Window

Files List						
Detailed Information			E			
Performance	Statistics	Vindows	🛃 Threads 📑 Handles 🕥 Drivers			
Select All Processes Name Filter:						
Name 🔻	Туре	Process	Path			
🔊 mshtml.tlb	Type Library	azureus	C:\1386\system32\mshtml.tlb			
🔊 msnetobj.dll	Компонент пр	ри 삼 azureus	C:\1386\system32\msnetobj.dll			
🚞 Му	Disk folder	🕣 👌 AnVir Task Ma	an 🛅 C:\Documents and Settings\1\Applicatio			
👩 Perflib_Perfdata_a	Файл "DAT"	🕑 🛛 AnVir Task Ma	an 👩 C:\Temp\Perflib_Perfdata_aac.dat			
📮 QTJava.zip	WinZip File	azureus	C:\Program Files\Java\ire1.6.0_02\lib\e>			
🔚 resources.jar	Архив WindA		Perflib_Perfdata_aac.dat \re_			
📜 rt.jar	Архив W 🧔	Switc <u>h</u> To Process	Туре: Файл "DAT"			
🔊 shdoovw.dll	Компоне		Process: AnVir Task Manager Pro			
🔊 stdole2.tlb	Type Libr 📉	File Properties	Path: C:\Temp\Perflib_Perfdata_aac.dat			
🗒 Sti_Trace.log	Текстові 🂋	Show File In <u>E</u> xplorer	Addrose: 95E02E00			
🔚 sunjce_provider.jar	Архив W 📻	Suctom Monu	pin nes waya gier.o.o_oz ma/8) _			
📜 sunmscapi, jar	Архив W 🛤	System Menu	am Files\Java\jre1.6.0_02\lib\e> 🎽			
<		Save <u>R</u> eport as Html				

Files list shows list of files that are opened by selected processes.

<u>Columns</u>

- Name File Name
- Type File Type
- Process Process that opened the file
- Path File full path
- Handle Handle number

• Address - Kernel address

Context Menu commands

Switch To Process - Open Process window and select process that use a file or folder

File Properties – Open system dialog with properties of the file or folder

Show File In Explorer – Open Explorer and select file or folder

System Menu - Show system context menu of the file or folder

Save Report as Html ... - Save list of files and folders to html file

Check with AntiViruses on VirusTotal - Check file with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about file in Google

Google News - Search information about file in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about file

Copy Path - Copy to clipboard path of file

Connections List Window Connections List

Deta	Detailed Information								
	Performance Image: Statistics Image: Windows Image: Threads Image: Statistics Image: Statistics								
✓	Show connecti	ons for all process	es 🛛 🗹 Show TC	P 🗹 Show UDP					
Pr	ocess	Network: R	Network: Sent	 Remote Address 	Remot	State 🔥			
4	azureus	🦊 88,9 КБ	👚 1,90 МБ	ppp91-77-247	43737	📀 Established (Esta			
4	azureus	🦊 103 КБ	🚹 93,3 КБ	-	-	-			
4	azureus	🤳 971 байт	🚹 9,98 КБ 👝	82 200 172 17	46793	📀 Established (Esta			
4	azureus		1 5,49 KB TC	P					
	Generic Ho	🦊 9,17 КБ 👘	1 3,98 K5 Pro	cess: azureus					
	Generic Ho	🦊 10,5 КБ	1 2,89 K5 LOC	al Address: ilya.cpms -l Rest: 2557	s.ru				
	Generic Ho	1/0KE	2,67 K6 Dom	al Ροπ: 3557 Note Addresse: 02.200	064.60				
0	Switc <u>h</u> To Proc	ess	920 бай Ren	note Port: 54228	1.204.02				
37	Close TCP Con	pection	686 бай Stat	e: Established (Estat	olished cor	nnection between a loca			
~	Ciose rer con	inection	468 байл <mark>Net</mark>	work: Received: 5,69	КБ				
23	Kill Process		196 байл <mark>Net</mark> s	work: Sent: 98,0 KB					
4	Write Traffic o	f Process to File	, 196 байл Dow	196 байл Download Speed: 359 байт/s					
			156 Kain Uplo	ad Speed: 4,76 KE/s					
9	File Properties		Mod	lule Name: Azureus.e	Xe Eiloc\Azur				

Connections list shows network connections that are opened by selected processes.

<u>Columns</u>

- Protocol Connection protocol: TCP or UDP
- Process The name of the process that issued a context bind for this link
- Local Address The IPv4 address and name of the local endpoint in the link
- Local Port The number and name of the port used by the local endpoint
- Remote Address The IPv4 address and name of the remote endpoint in the TCP link
- Remote Port The number and name of the port used by the remote endpoint
- State State of the local TCP link
- Network: Received Amount of data downloaded by a process from Internet or network
- Network: Sent Amount of data uploaded by a process to Internet or network
- Download Speed Current download speed
- Upload Speed Current upload speed
- Time System time value which indicates when the context bind operation that created this link occurred
- Module Name Module name
- Module Path Module full path

Context Menu commands

Switch To Process - Open Process window and select process that opened the connection

Close TCP Connection – Close connection (only for TCP connections that have remote IP address)

Kill Process – Kill process that use this connection

Write Traffic of Process to File... – Show file section dialog, start sniffing traffic of the connection (socket) and writing traffic to the file in binary format.

Stop Writing Traffic of Process – Stop writing traffic of the socket to the file in binary format.

File Properties – Open system dialog with properties of the process file or dll that uses the connection

Show File In Explorer – Open Explorer and select process file or dll that uses the connection

System Menu - Show system context menu of the process file or dll that uses the connection

Save Report as Html... - Save list of connections to html file

Check with AntiViruses on VirusTotal - Check file with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about process in Google

Google News - Search information about process in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about connection

Copy Path - Copy to clipboard path of the process file or dll that use the connection



Performance Window

Performance Window shows performance graphs for the selected process. You can set check box

"All Processes" to see total graph for all processes. Following graphs are available:

- CPU Processor usage
- Memory Memory usage
- Disk Amount of data that process reads and writes to disk per second
- Download Amount of data downloaded by a process from Internet or network per second
- Upload Amount of data uploaded by a process to Internet or network per second

You can select one of available periods for visualization:

- Realtime (approx 10 minutes)
- 2 hours
- 1 day
- 1 week

You can use scale sliders to set up charts scale.

Statistics Window

Detailed Information								
🔰 General	📝 Product I	nformation 🔰 🔊 DL	.L 🛛 🧔 Fi	iles 🛛 🦄 Connectio	ons			
Performance	i Statistics	🔲 Windows 📔	🚦 Threads 📗	📩 Handles 📔 🧔 Dr	ivers			
Select All Processes Selected 46: System Idle Process, alg, anvir, atiptaxx, azureus, calmain, cpqalert, cpqdmi, science csrss, ctfmon, dcsuserprot, divxsm, explorer, googletoolbarnotifier, hibserv, i_view32,								
Performance		Memory		-Input/Output Operation	ns			
Work Time	3697:23:11	Memory Size	91 400 K	Read Operations	20			
CPU Usage	86%	Pagefile Usage	412 084 K	Write Operations	2			
Kernel Time	350:21.387	Virtual Size	2 694 700 K	Other IO Operation	367			
User Mode Time	115:32.298							
CPU Total Time	465:53.685	Peak Memory Size	559 576 K	Read Bytes	11			
		Peak Pagefile Usage	532 604 K	Write Bytes	E			
Threads	566	Peak Virtual Size	3 128 192 K	Other IO Bytes	121			
Handles	13 360			IO Activity				
GDI objects	6 426							
USER objects	3 1 9 0							
Page Faults	9 798 932							
<				<	>			

Statistics shows performance counters of selected processes. This window contains following blocks:

- Performance
- Memory
- Input/Output Operations

Performance

This block shows following counters:

- Work Time Time pasts since a process was created [days hours minutes] or [hh:mm:ss]
- CPU Usage Processor usage by a process
- Kernel Time Kernel mode processor usage mm:ss.ms
- User Mode Time User mode processor usage mm:ss.ms
- CPU Total Time Processor time usage. Sum of Kernel mode usage and User mode usage.
- Threads Number of active threads associated with a process. A thread is the object that executes an instruction. Each running process has at least one thread.
- Handles Total number of open handles owned by the process. Handles count is the sum of the handles currently open by each thread in this process. A handle is used to examine or modify the system resources. Each handle has an entry in a table that is maintained internally. Entries contain the addresses of the resources and data to identify the resource type.
- GDI objects The count of GDI objects in use by the process
- USER objects The count of USER objects in use by the process
- Page Faults Number of page faults generated by the process

Memory

This block shows following counters:

- Memory Size Set of memory pages visible to the process in physical RAM. These pages are resident, and available for an application to use without triggering a page fault. If adequate memory is not available, "disk thrashing" occurs. (Disk thrashing refers to those times when the operating system must repeatedly access the hard disk.)
- Pagefile Usage Amount of pagefile space currently used by the process
- Virtual Size Current size of the virtual address space that a process is using, not the physical or virtual memory actually used by the process. Using virtual address space does not necessarily imply corresponding use of either disk or main memory pages. Virtual space is finite, and by using too much, the process might not be able to load libraries.
- Peak Memory Size Maximum size of the working set used by the process since it was created
- Peak Pagefile Usage Maximum amount of page file space used during the life of a process
- Peak Virtual Size Maximum virtual address space a process uses at any one time

Input/Output Operations

This block shows following counters:

- Read Operations Number of read operations performed
- Write Operations Number of write operations performed
- Other IO Operation Number of I/O operations performed, other than read and write operations

- Read Bytes Amount of data read
- Write Bytes Amount of data written
- Other IO Bytes Amount of data transferred during operations that are not read or write operations
- IO Activity IO speed, summarized amount of data read, write and transferred per second

Windows tree									
Detailed Information	Detailed Information								
🧊 📝 General 🛛 📝 Produ	et Information	DLL	🧔 Files		Connections				
🛛 🕅 Performance 🛛 🦂 Statisti	cs 🔲 🛄 Windows	🚽 Threa	ids 🛛 📩	Handles	O Drivers				
List Invisible Windows									
Window Title Process	; Visible	State	Size	Position	Class				
🖃 🕒 Detailed Informar 🔁 AnVir	Security S 🗖 Visible 🛛	🗸 Enabled	584x358	221,805-80	WTL_Floati 🔼				
📄 🗖 Detailed Info	Security S 🗖 Visible	✔ Enabled	576x332	225,801-80	#32770				
🖨 🗖 AnVirPagI 🔂 AnVir	Security S 🗖 Visible	💎 Enabled	576x289	225,801-80	#32770				
<u> </u>	jecurity S 🗖 Visible	🛛 🎸 Enabled	576x260	225,801-80	SysTreeVie				
	Security S 🗖 Visible	✔ Enabled	572x20	227,799-79	ATL:SysHe				
Enabled	Security S 🗖 Visible	✔ Enabled	572x219	227,799-79	ATL:SysTre				
	000.040	🗸 Enabled	128×16	230,358-35	Button				
	<u>3</u> 20x240	Cisabled 🤤	125×16	372,497-49	Button				
🗄 🗖 A 👩 Close	<u>6</u> 40×480	🔹 🗹 Enabled	576x289	225,801-80	#32770				
	000.000	🖌 🗹 Enabled	576x331	225,801-80	SysTabCon				
🖻 🥅 AnVirPagI 🔂 AnVir	800x600	🔹 🗹 Enabled	576x289	225,801-80	#32770				
🗄 🧮 AnVirPagI 🔂 AnVir	10 <u>2</u> 4x768	🔹 🗹 Enabled	576x289	225,801-80	#32770				
🗎 🛅 AnVirPagI 🄁 rAnVir	1150-064	🔹 🗹 Enabled	576x289	225,801-80	#32770				
🚊 🗇 🗖 AnVirPag I 🖶 AnVir	11 <u>5</u> 2X864	🖌 🖌 Enabled	576x289	225.801-80	#32770				
<	1280×800			annan is j	>				

Windows Tree Window

Windows tree shows windows of selected processes. Windows are shown as parent/child tree.

<u>Columns</u>

- Windows Title Text shown in the title of a window
- Process Process created the window
- Visible Is window visible or hidden
- State Is window enabled or disabled
- Size Size of window
- Position Position of a window
- Class Name of window class
- Handle Handle of a window

Context Menu commands

Visible – Hide visible window / unhide invisible window

Enabled – Enable disabled window / disable enabled window

Resize - change size of the window to one of standard screen resolutions

320x240
640x480
800x600
1024x768
1152x864
1280x800
1280x1024

Close - close window

Threads List Window

Detailed Infor	mation					×
🔰 Gener	al 🛛 📝 P	roduct Information	n 🚺 💽 DLL		Files	Sonnections
🛛 🛛 Performa	ance 🛛 🦂 Si	tatistics 📃 🔲	Windows 🛛 🗳	Threads	📩 Handle	es 🛛 🔘 Drivers
Kernel Time	User Time	CPU % 🔻	Window Title		Cre	ation Time
08:21.411	09:51.430	13.0%			26.0	02.2008 13:45:58.246
00:14.901	05:39.448	3.5%			26.0	02.2008 13:45:58.246
00:40.448	01:11.873	1.5%	mv-1. avi - Media Pla	iyer Classic	26.0	02.2008 13:44:49.908
00:14.100	00:09.133	1.0%		070 (04)	201	
00:00.130	00:00.060	0.0%	ffdshowaudio_tray_	52 07 U (210	50)	
00:00.010	00:00.020	0.0%		Kernel Til	me: 00:41.3	380
00:01.602	00:01.462	0.0%		User Tim	e: 01:14.04	6
00:00.010	00:00.000	0.0%	ActiveMovie Windo	w CPU %: 3.	5%	
00:00.050	00:00.000	0.0%		Creation	Time: 26.02	2.2008 13:44:49.908
00:00.000	00:00.000	0.0%		Priority: 1	0	
00:00.000	00:00.000	0.0%		Base Pric	ority: 10	
00.00.000	noo	0.0%		Context S	witches: 6	06621
0 🚮 Suspen	id '71	0.0%		State: \Ala	ait	
				Mait Roa	eon•lleor¤	toquoet
Resume	e			Mindow 1	SULL OSELA	equest vi Modio Diovor Clo
💓 Termina	ate			Vyinuow	fille. IIIV-1.c	
				Hanules (JI WINGOWS	S 9046A AFUSEC 6D
				7405EA 6	18062C 6EU	JOAZ 520544 55052E
<				Process:	mplayerc	
				Address:	7C810665	

Threads window shows all threads of selected processes.

<u>Columns</u>

- ID Thread ID: hex (and dec)
- Kernel Time Amount of time that the thread has executed in kernel mode
- User Time Amount of time that the thread has executed in user mode
- CPU % Processor usage
- Creation Time Creation time of the thread
- Priority Thread priority

- Base Priority Thread base priority
- Context Switches Context switches
- State Thread state
- Wait Reason Thread wait reason: "Executive", "FreePage", "PageIn", "PoolAllocation", "DelayExecution", "Suspended", "UserRequest", "EventPair", "Queue", "LpcReceive", "LpcReply", "VirtualMemory", "PageOut", "Rendezvous", "Kernel"
- Window Title Title of a window associated with a thread
- Handles of Windows Handles of windows associated with a thread
- Process Process owner of the thread
- Address Start address of the thread

Context Menu commands

Suspend – Suspend thread execution

Resume – Resume thread execution

Terminate – Kill thread

Copy - Copy to clipboard full information about selected threads

Save Report as Html... - Save list of threads to html file

Handles List Window

Handles List

lianuics	LISU									
Detailed I	nformation									×
General	Product Informati	ion	Statistics	DLL	Connections	Windows	Files	Threads	Handles	Drivers
H 🔻	Туре		Name				Pr	ocess	Address	-
4	Process		PID 4,				sy:	stem	82BCA8	30 💻
4	KeyedEvent		\KernelC)bjects\C	ritSecOutOfMe	moryEvent	sm	SS	E10096E	0
4	KeyedEvent		\KernelC)bjects\C	ritSecOutOfMe	moryEvent	CS	ISS	E10096E	0
4	KeyedEvent		\KernelC)bjects\C	ritSecOutOfMe	moryEvent	wir	nlogon	E10096E	EO 0.
4	KeyedEivent		\KernelC)bjects\C	ritSecOutOfMe	moryEvent	se	rvices	E10096E	EO 0.
4	KeyedEivent		\KernelC)bjects\C	ritSecOutOfMe	moryEvent	lsa	SS	E10096E	EO 0.
4	KeyedEivent	Λ						levxx	E10096E	20
4	KeyedEivent	-		-				:host[1036]	E10096E	20
4	KeyedEivent	тур	ie: Keyeai	Event				chost[1152]	E10096E	50
4	KeyedEivent	Nar	ne: Ikern	elObjec	tsiCritSecOut	Otmemory	Event	chost[1248]	E10096E	0
4	KeyedEivent	Pro	cess: se	rvices				chost[1344]	E10096E	0
4	KeyedEivent	Add	iress: E1	0096E0)			chost[1540]	E10096E	20
4	KeyedEivent		KernelC)bjects\C	ritSecOutOfMe	moryEvent	ati	2evxx	E10096E	0
4	KeyedEivent		\KernelC)bjects\C)ritSecOutOfMe	moryEvent	ex	plorer	E10096E	0
4	KeyedEivent		\KernelC)bjects\C)ritSecOutOfMe	moryEvent	av	gamsvr	E10096E	0
4	KeyedEvent		\KernelC)bjects\C	critSecOutOfMe	moryEvent	av	gupsvo	E10096E	0
4	KeyedEivent		\KernelC)bjects\C	critSecOutOfMe	moryEvent	ср	qalert	E10096E	20
4	KeyedEvent		\KernelC)bjects\C	critSecOutOfMe	moryEvent	syr	ntplpr	E10096E	0 🗸
<					1111					>

Handles window shows all handles of selected processes. Columns:

- Handle Handle number
- Type Handle type: Port, Directory, Event, KeyedEvent, WindowStation, Desktop, Mutant, Semaphore, Key, Thread, Section, IoCompletion, etc.
- Name Object name or description

- Process Owner of the handle
- Address Kernel address

Drivers List									
Detailed Informati	on								×
🔰 General	Pro	duct Information	🕥 D	LL		<i>(</i>	Files	- 	Connections
🛛 🕅 Performance	🛛 🤐 Sta	itistics 📄 🗔 V	Vindows	4	Threa	ds	🔥 📩 Hand	lles	🔘 Drivers
Name Filter: s									
Name	Product		State	S	tart Ty	pe	Туре		First Detecte
📿 fasg	Free Anti-F	Rootkit Tool	🕨 Runni	V	In ke	rnel		(26.02.20(
🔘 spmx	<file misse<="" td=""><td>:d></td><td>▶ Runni</td><td>V</td><td colspan="2">🗹 In kernel</td><td></td><td>1</td><td>22.02.20</td></file>	:d>	▶ Runni	V	🗹 In kernel			1	22.02.20
🔿 procguard	<file misse<="" td=""><td>:d></td><td colspan="2">🕩 Runni 🤤 Disabl</td><td colspan="2">led Kernel driver</td><td>river 🧯</td><td colspan="2">0 22.02.20</td></file>	:d>	🕩 Runni 🤤 Disabl		led Kernel driver		river 🧯	0 22.02.20	
📿 Prio	Prio Netwo	ork Activity Driver	▶ Runni	\checkmark	🖉 System		Kernel dr	river	18.02.2008 1
🔘 Partizan	<file td="" 🔍<=""><td>File Properties</td><td></td><td colspan="2">þ</td><td>led</td><td>Kernel dr</td><td>river</td><td>17.02.2008 1</td></file>	File Properties		þ		led	Kernel dr	river	17.02.2008 1
SMCLIB						man	d Kernel dr	river	11.02.2008 1
Product: Smard Ca	rd Drive 🎾	Show File In <u>E</u> xplorer							21.01.2008 0
Company: Microsof	t Corpoi 🛐	System <u>M</u> enu					<u>n v n</u> u		~~~ 1008.0
State: Running							ROOC		008.0
Start Type: In kernel Full Path: C:\\386\system32 Version: 5.1.2600.0 Date: 20.10.2001.15:00		Stop				 Image: A set of the set of the	<u>S</u> ystem		008.0
		Change Startup Type					Auto on sta	artun	008 1
								rcap	008.0
Size: 14592		Save <u>R</u> eport as	Html				<u>O</u> n demand		008 0 ⊻
First Detected: 21.0	01.2008 🧊	Check with Antiv	/iruses on Virus	Tota	1		Disable (Qu	arantin	.e)

Drivers List Window

Drivers window shows all drivers installed in system.

<u>Columns</u>

- Name Display name of the driver
- Description Description of the driver provided by vendor
- Product Description of the file provided by vendor
- Company Vendor of the driver
- State Current state of the driver
- Start Type When Windows starts the driver: Disabled, On demand, Auto on startup, System, Boot, In kernel
- Type Type of the driver: Kernel driver, File system driver
- Full Path Full path to the driver binary file
- Version Version of the driver
- Date Date and time when the file was created
- Size Size of the module in bytes
- Dependencies Names of drivers that must start before this driver
- Group Load ordering group to which this driver belongs
- First Detected When driver was detected first time. Items detected in the last week are marked.

Context Menu commands

File Properties - Open system dialog with properties of the file of the driver

Show File In Explorer – Open Explorer and select file of the driver

System Menu - Show system context menu of the file of the driver

Stop – stop running driver

Start – start driver

<u>Change Startup Type</u> – change start type of the driver

Boot - Start device driver by the system loader at Window load

System - Start device driver by the IoInitSystem function at Window load

Auto on startup - Start driver automatically by the service control manager during system startup

On demand - Start driver by the service control manager when a process needs this driver and calls the StartService function

Disable (Quarantine) - A driver cannot be started. Attempts to start the driver result in the error

Save Report as Html... - Save list of drivers to html file

Check with AntiViruses on VirusTotal - Check file of the driver with 30 AntiVirus engines on site VirusTotal.com

Search in Web

Google - Search information about file of the driver in Google

Google News - Search information about file of the driver in Google News

Text Operations

Copy to Clipboard - Copy to clipboard full information about driver

Copy Path - Copy to clipboard path of the file of the driver

System Tray Icons and Menu

System tray is an area in the right bottom corner of a screen near of clock.

The program creates following dynamic icons in system tray:

- <u>CPU Icon</u>
- Disk Icon
- <u>Memory Icon</u>
- <u>Network Icon</u>
- <u>Battery Icon</u>
- <u>Combined Icon</u>
- <u>Icons of windows minimized to system tray</u>

You can place a mouse pointer on an icon to see icon tooltip. If you left click on an icon, tooltip will stay on the screen and not disappear. To hide tooltip, click on the tooltip once more.

If you right click on an icon, tray menu appears.

When you minimize windows to tray, the program creates tray icon for each minimized window.

Dynamic tray icons and icons of minimized windows

a Ph		
12	Outlook Express Placed to tray: 8/3/2008 12:54	
EN	🗑 🗿 % 🍋 🍻 🖉 🖸 🖉 🚺 🗭 📰 🚺 📰 12:55.PM	

Dynamic tray icons, tooltips, tray menu

testionel 1.445,027 2.15 1.52 1.	-	paglation (second	New Joint Control of C	information of the second seco
Conceptor (Conceptor (Concep	ö	province takes Designation per method to index the set		Statut (%)
Marine Marine	1	Carrier Tax Reager Fr.		M

System Tray Menu

y menu				
Most Recently (Opened Folders		Most Recently Launched Programs	
C:\Documents a	and Settings\Administrator	۲	Internet Explorer	
C:\Documents a	and Settings\All Users\Favorites		Media Center	
C:\Program File	s\AnVir Task Manager Pro		Notepad	
C:\		Θ	Windows Media Player	
C:\Reports		3	Windows Messenger	
C:\Reports\200	8		Add File To This List	
Add Folder To T	his List	6	C:\Reports\2008\Sales report.txt	
2008	Open		C:\Documents and Settings\Sample Pictures\Fish.jpg	
Desktop DVD Drive (D	Explore Search		Hide Window To System Tray	•
My Document My reports	Open Folder Remove Shortcut from This List Properties of the Folder	•	Open AnVir Task Manager Pro Tray Icons	,
	Most Recently (C:\Documents a C:\Documents a C:\Program File C:\ C:\Reports C:\Reports\200 Add Folder To T 2008 Desktop DVD Drive (D My Document My reports	Most Recently Opened Folders C:\Documents and Settings\Administrator C:\Documents and Settings\All Users\Favorites C:\Program Files\AnVir Task Manager Pro C:\ C:\Reports C:\Reports C:\Reports\2008 Add Folder To This List 2008 Desktop Desktop DVD Drive (D My Document My reports Properties of the Folder	Most Recently Opened Folders Image: Section of Sectio	Y menu Most Recently Opened Folders Most Recently Launched Programs C:\Documents and Settings\Administrator Internet Explorer C:\Documents and Settings\All Users\Favorites Image: Properties Anvir Task Manager Properties Modia Center C:\Program Files\Anvir Task Manager Pro Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Modia Center C:\Program Files\Anvir Task Manager Pro Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Modia Player C:\Reports Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Modia Player C:\Reports Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Modia Player C:\Reports\2008 Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Modia Player 2008 Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Properties Anvir Task Manager Properties DvD Drive (D Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties Image: Properties Anvir Task Manager Properties My reports Properties of the Ender Image: Properties Anvir T

When you right click on any of dynamic icons in system tray, tray menu appears.

Tray menu contains following blocks of commands:

- Most recently opened folders
- Custom favorite folders
- Most recently launched programs
- Custom favorite programs and files

CPU Icon



CPU icon stays in system tray and represents how much of CPU (processor) resources are currently in use.

Tooltip shows following information:

- Total usage of CPU
- List of processes that use CPU (processor) most of all
 - Name of the processes
 - Processes usage of CPU

To activate tray-monitoring left-click on the CPU icon.

Disk Icon



Disk icon stays in system tray and represents

- Current load of logical disks
- Current temperature of physical disks (HDD)

Tray icon gets temperature via S.M.A.R.T. Some external disks don't support SMART so temperature of such HDD is not shown. If there are few hard disk drives, tray icon shows current temperature of the most hot physical disk.

If there are few logical disks, tray icon shows disk load of the most loaded logical disk. High load of a disk means that programs currently read and write a lot of data to the disk.

Tray icon tooltip shows following data:

- Disk load of each logical disk
- Temperature of each physical disk (admin rights required, disks must support S.M.A.R.T.)
- Processes that use disks most of all
- Free space on each logical disk

To activate tray-monitoring left-click on the Disk icon.

Memory Icon



Memory icon stays in system tray and represents usage of physical memory

Tray icon tooltip shows following data:

- Percent of total memory usage
- Total amount of physical memory on PC
- Amount of physical memory in use
- List of processes that use memory most of all
 - Name of the process
 - Amount of physical memory that the process uses

To activate tray-monitoring left-click on the Memory icon.

Network Icon



Network icon stays in system tray and represents current usage of network adapter(s).

Tooltip shows following information:

- Inbound speed
- Outbound speed
- Amount of received data
- Amount of sent data
- Name of connection
- Status of connection: Disabled, Unreachable, Disconnected, Connecting, Connected
- Network connection speed

To activate tray-monitoring left-click on the Network icon.

Combined Icon



You can use combined icon to save system tray space. Combined icon can show few of following dynamic indicators:

- CPU usage
- Disk load
- Disk temperature
- Memory usage
- Network load
- Battery state

Icons of Minimized Windows

	Outlook Express Placed to tray: 8/3/2008 12:54	Alar-disardering
EN) 🔊 🌉 🚺 🚺 12:55 PM

When you minimize window to system tray, AnVir Security Suite creates an icon for that window in system tray. You can click on the icon to restore window. You can right click on the icon to open tray menu. Tray menu for minimized windows allows to restore window, hide window, make window always on top, or hide other windows to system tray.

Battery Icon



Battery icon stays in system tray and represents current state of notebook battery.

Tooltip shows following information:

- Remaining time and percent
- Battery status: High, Low, Critical, Charging, No system battery (not notebook)
- AC power: Online, Offline

To activate tray-monitoring left-click on the Battery icon.

Notifications

AnVir Security Suite monitors system settings and shows following notifications when some programs tries to change system settings:

- <u>New Startup Item</u>
- Internet Explorer Homepage Changed

New Startup Item



When any program tries to add new startup item, AnVir Security Suite shows notification. Following startup items are monitored:

- Programs that run on Windows startup, or on user login.
- Non Microsoft services that run on Windows startup.
- Internet Explorer extensions: browser helper objects, toolbars, menu items.

Notification dialog shows following information:

Name and value of new startup item

Company name and product description

Startup database analysis

When new startup item found, you can choose one of following actions:

Allow – No action will be performed. Select this action if you need this item.

Quarantine – Startup item will be disabled. Select this action if you don't need this startup item, but you may need this in future.

Delete - Startup item will be deleted. Select this action if you definitely don't need this startup item.

For some annoying startup items you can set check box "Don't ask any more about this startup item." In this case selected action will be performed always when this startup item detected.

Internet Explorer Homepage Changed



When any program tries to change Internet Explorer home page, AnVir Security Suite shows notification.

When Internet Explorer home page changed, you can choose one of following actions:

- Allow new home page
- Restore old home page

Settings To open settings dialog, go to Tools-Options.

General Settings dialog



Load program on startup - start the program every time when Windows starts

Hotkey to bring program to the foreground – press combination of key that brings program to the foreground. Default: Ctrl-Shift-F1

Enable Startup Monitor - Show alert when any new program is added to startup

Enable Home Page Guard - Show alert when Internet Explorer home page is changed

Tray

📀 Options - AnVir Security	Suite	
 Program Settings General Tray Icons and Menue Vindows Usability Windows Usability Windows Enhancem Minimize To Tray Security Startup Guard Blocked Processes Performance Performance Processes Priority Run As Service 	Program Appearance	
K	<u>B</u> estore default Apply Cancel	

Program Appearance

Close to tray - When you press X button in the right-upper corner, the program will not shut down.

Minimize to tray - When you minimize the program, it removes its window from system taskbar.

Hidden mode - When you press X button in the right-upper corner, program hides its window. To bring the program out of this mode, click the program link in start menu or use hotkey.

Tray Icons

Set up which icons are shown in system tray.

CPU - Amount of CPU resources that are currently in use. Tooltip shows most active processes that use CPU.

Disk - Current load and temperature of HDD. Tooltip shows most active processes that use HDD. This icon is fully yellow when programs actively read or write to disk.

Disk temperature: °C or °F

Memory - Current usage of physical memory.

Network - State, current speed and amount of data transferred.

Battery - Current state of notebook battery.

Combined Icon - Save space in system tray and place all or some indicators on one tray icon.

Tray Menu

Number of programs and folders in tray menu - Tray menu keeps the list of recently launched programs, and folders recently opened in Explorer.

Tray menu columns - Appearance of tray menu with list of programs and folders.

Advanced

 Program Settings General Tray Icons and Menu Advanced Windows Usability Windows Usability Minimize To Tray Security Startup Guard Blocked Processes Performance Performance Performance Performance Run As Service 	□ Beplace Windows Task Manager. Start when Ctrl-Shift-Esc pressed. □ Delayed Startup Use Delayed Startup to speed up your computer's startup process. Delayed startup items are started 1 minute (time can be customized) after Windows is loaded. You can start using computer not waiting while Windows loads all startup programs. To move a startup program to the delayed startup list select "Move to Delayed Startup List" in context menu on Startup page. Delay after Windows has started, to begin loading applications from delay startup list. ●0 🛫 sec. Igterval between loading of applications from delay startup list. ●0 🛫 sec. Igterval between loading of applications from delay startup list. ●0 🛫 sec. Program interface (restart required): ● Skin ○ Windows settings Icons of main windows (restart required): ● Big icons ● Small icons □ Processes created ♥ Processes terminated Windows created □ Processes treating: ● Registry ● Anvir.mi □ Enable Internet traffic monitoring. (May cause incompatibility errors with some 3rd party network drivers). ● Ask gonfirmation on killing and running processes and threads Where to store settings: ● Registry ● Anvir.mi

Replace Windows Task Manager - Start program when Ctrl-Shift-Esc pressed.

Delayed Startup

Use Delayed Startup to speed up your computer's startup process. Delayed startup items are started 1 minute (time can be customized) after Windows is loaded. You can start using computer not waiting while Windows loads all startup programs. To move a startup program to the delayed startup list select "Move to Delayed Startup List" in context menu on Startup page.

Settings:

- Delay after Windows has started, to begin loading applications from delay startup list.
- Interval between loading of applications from delay startup list.

Appearance

Program interface (restart required): skin or Windows system settings

Icons of main windows (restart required): big 32px icons or small 16px icons

Show color tooltips only when Ctrl pressed

Log

Events that are placed to the log:

- Processes created
- Processes terminated
- Windows created

Save log to file – path to the log file

Enable Internet traffic monitoring. May cause incompatibility errors with some 3rd party network drivers. Requires admin rights.

Ask confirmation on killing and running processes and threads

Where to store settings: registry or anvir.ini (portable)

Windows Enhancement

😌 Options - AnVir Security	Suite	
 Program Settings General Tray Icons and Menu Advanced Windows Usability Windows Enhancement Minimize To Tray Security Startup Guard Blocked Processes Performance Performance Processes Priority Run As Service 	Minimize Windows To Tray Settings Minimize inactive windows to System Tray and save Taskbar space for minimized windows. Applications page or menu in the tray to hide a window. (Taskbar is located at the bottom of the screen. System Tray is located in the bottom right of Click on a tray icon to bring hidden window to front, or hide window back to the tray. Use: Image: Hide tray icon when hidden window is activated to front Image: Disable Windows auto-hide feature for tray icons of inactive minimized applications Floating Icons Switch windows to floating icons and save Taskbar and System Tray space. Floating icons rectangles (icon and title) that represent minimized windows. Floating icon size: Small Show title of window as text Igon Transparent 50% Add useful commands to system menu of all windows (Transparent, Priority, On Top, Hide Add list of recent folders to "Save As" and "Open" dialogs of all programs Folders in menu of dialogs: 7	Use context menu on comer of the screen.) <u>S</u>ingle Click <u>D</u>ouble Click are small transparent draggable to Tray)
<	<u>B</u> estore default	Apply Cancel

Minimize Windows To Tray

Minimize inactive windows to System Tray and save Taskbar space for minimized windows. Use context menu on Applications page or menu in the tray to hide a window. Taskbar is located at the bottom of the screen. System Tray is located in the bottom right corner of the screen.

Click on a tray icon to bring hidden window to front, or hide window back to the tray. Use single click or double click

Hide tray icon when hidden window is activated to front – hide tray icon, or keep it always in tray

Disable Windows auto-hide feature for tray icons of inactive minimized applications – don't let Windows to hide inactive icons

Floating Icons

Switch windows to floating icons and save Taskbar and System Tray space. Floating icons are small transparent draggable rectangles (icon and title) that represent minimized windows.

Floating icon size - Size of the icon on a floating window

Show title of window as text - Show text or just icon

Icon Transparency - Initial transparency level of a floating icon

Windows Enhancements

Add useful commands to system menu of all windows (Transparent, Priority, On Top, Hide to Tray) - Adds useful commands to the title menu of window of all applications

Add list of recent folders to "Save As" and "Open" dialogs of all programs - access a list of recently used folder and favorites folders from the Save and Open dialogs

Folders in menu of dialogs - Number of folders in menu of "Save" and "Open" dialogs

Minimize to Tray

Options - Anvir Task /	Manager Pro			
General Tray Advanced Startup Guard Blocked Processes Processes Priority	Manager Pro List of windows that v On the Applications p hidden when you min Process @ dexplore.exe @ dexplore.exe @ firefox.exe [1] finifox.exe [2] fiblibrary.exe [3] firefox.exe [4] finifox.exe [5] firefox.exe [6] notepad.exe [6] orbosoft.exe [6] sndvol32.exe [6] taskmgr.exe [6] winamp.exe	vill be hidden to tray when minim age set the checkbox 'Always F imize that window. Product Microsoft Document Expl Проводник FB2Librarian Firefox Lingvo Microsoft (R) Developer Блокнот Quiet Internet Pager Advanced Software Sub Громкость Диспетчер задач Wind Winamp Rus	ized. You can minimize windows to tray and save taskba Place To Tray When Minimized' for a window that you wo Window Title HDITEM Structure - MSDN Library - Visual Studio 200 Свойства: WebKeySoft Process Manager 2 Lite FB2 Librarian Anvir Task Manager • Ответить - Mozilla Firefox Lingvo 5.0 VIR - Microsoft Visual C++ - [Output] Безымянный - Блокнот [qip] - 63700418 RoboSoft Громкость Диспетчер задач Windows 35. 2607 - 2607 - Winamp [naysa]	r space. uld like to be <u>R</u> emove
	<			

Minimize to Tray settings dialog shows list of windows that will be hidden to tray when minimized. You can minimize windows to tray and save taskbar space.

On the Applications page set the checkbox 'Always Place To Tray When Minimized' for a window that you would like to be hidden when you minimize that window.

To remove an item from the list, select an item and click Remove.

Startup Guard **Startup Guard**

📀 Options - AnVir Security	Suite		
Program Settings General Tray Icons and Menu	ist of programs that are automatically del fo add items to this list remove an existen 'New startup program found'' alert.	eted from the startup list when these programs try to be added to th it startup program from the startup list on Startup page, or remove s	ne startup. startup program on
 Advanced Windows Usability Windows Enhancem Minimize To Tray Security Startup Guard Blocked Processes Blocked Processes Performance Performance Perocesses Priority Run As Service 	Name Value 1111 22222 CoreIDRAW Grap J:\Program File Folder Cache i:\PROGRA~1 Tet-a-Tet c:\Temp\Tet+ Uconomix SnapLo 'J:\Program File VCWATCHER50SE C:\PR0JECTS VCWATCHER50SE J:\Program File VCWATCHER50SE J:\Program File VCWATCHER50SE J:\Program File VCWATCHER50SE J:\Program File	es\Corel\Corel Graphics 12\Languages\EN\Programs\Registr I\FOLDER~1\FOLDER~1.EXE A-Tet.exe -m iles\Uconomix\Uconomix SnapLogger 1.1\SnapLogger.exe'' S\VCWatcher\src\Client\Release\client.exe es\VCWatcher\client.exe	<u>R</u> emove
<		Apply	Cancel

Startup Guard settings dialog shows list of programs that are automatically deleted from the startup list when these programs try to be added to the startup.

To add items to this list remove an existent startup program from the startup list on Startup page, or remove startup program on "New startup program found" alert.

To remove an item from the list, select an item and click Remove.

Blocked Processes
Blocked processes

Program Settings	'Black list' of processes that are automatically terminated immediately after these processes start.	
Windows Usability Security Startup Guard	C:\program files\canon\cal\calmain.exe	Add
Blocked Processes	C. Sprogram mes wholes: exe [1] (C. Suris Vingvo32: exe [2] (C. Suris Vingvo32: e	<u>E</u> dit
		<u>R</u> emove
	New blocked process	
	Enter full path to executable file of the process, or enter any part of the path (e.g. file name or folder name). Examples: "msmsgs.exe", "c:\program files\mon", "c:\WINNT\system32\notepad.exe"	
	OK Cancel	

Blocked Processes settings dialog shows 'black list' of processes that are automatically terminated immediately after these processes start. Add to this list annoying and undesired processes that are started automatically without your will.

To remove an item from the list, select an item and click Remove.

Performance

📀 Options - AnVir Security	/ Suite		
 Program Settings General Tray Icons and Menu Advanced Windows Usability Windows Enhancem Minimize To Tray Security Startup Guard Blocked Processes Performance 	Balance CPU Utilization Reduce the priority (limit the CPU usage) of background processes that eat a lot of CPU, temporary, until CPU usage returns to a reasonable level Iotal system wide CPU usage when start to limit CPU usage of processes Maximum allowed CPU usage per a process before reduce its priority CPU usage of a process before increase its priority back Show notification in system tray when priority changed:		
 Processes Priority Run As Service 	Optimize memory	50 🌍 MB of memory.	
< >	<u>B</u> estore defaul	t Apply Cancel	

Balance CPU Utilization

Reduce the priority (limit the CPU usage) of background processes that eat a lot of CPU, temporary, until CPU usage returns to a reasonable level -Turn this feature On or Off

Total system wide CPU usage when start to limit CPU usage of processes - When CPU usage becomes greater than specified value, AnVir Task Manager reduces the priority of all processes that run in foreground and use a lot of CPU.

Maximum allowed CPU usage per a process before reduce its priority - If a process uses less CPU than specified value, its priority will not be reduced.

CPU usage of a process before increase its priority back - When process with reduced priority finished its activity and it uses less CPU than specified value, its priority will be increased back.

Show notification in system tray when priority changed: never, first time only, or each time - When show notification about changing of processes priorit.

Optimize memory

Free memory of processes that use more than ___ **MB of memory** - AnVir Task Manager once in 15 minutes swaps half of all memory of processes that use more than 50Mb to disk. It may useful for example when you use Firefox.

 Program Settings General Tray Icons and Menu Advanced Windows Usability Windows Enhancem 	Save Changed Processes Priority List of the processes which priority is automatically changed. Set the priority of applications that must not freeze to 'High', and the priority of bar to 'Low'. For example, set the priority of movie player to 'High'. Set the priority of backgrour operation to 'Low'. You can use context menu on Processes page to add proces	ckground services that nd antivirus check, vide ses to this list.	consume resources eo converter, backup
📕 Minimize To Tray	Path 🐨	Priority	Add
Security	anvir.exe C:\i386\system32\dfrgfat.exe	Above Normal Low	Edit
Blocked Processes	sc.\i386\system32\notepad.exe T c:\i386\system32\searchindexer.exe	Below Normal Below Normal	Remove
Performance	C:\i386\system32\wuauclt.exe	Low	
Processes Priority	c:\program files\anvir security suite\anvir.exe	Below Normal	
gr Hun As Service	🔽 🌆 c:\program files\astonsoft\deepburner\deepburner.exe	High	
	C:\program files\foldersize\foldersizesvc.exe	Low	
	5 million of the codec nack/media player classic/mplayerc exe	High	
📀 Edit proc	ess priority entry	Low	
and the second se		Low	
Enter full path	to executable file of the process, or enter any part of the path (e.g. file name or	_ow	
folder name).		Low	
Examples: m	smsgs.exe , c. sprogram niessmon , c. switsis i ssystemaz snotepad.exe	High	
c:\i386\syste	m32\notepad.exe	High	
Priority Belo	w Normal		
Rea High Abo Norr Beid	Itime ve Normal mal W Normal		

Save Changed Processes Priority

List of the processes which priority is automatically changed. Set the priority of applications that must not freeze to 'High', and the priority of background services that consume resources to 'Low'. For example, set the priority of movie player to 'High'. Set the priority of background antivirus check, video converter, backup operation to 'Low'. You can use context menu on Processes page to add processes to this list.

To remove an item from the list, select an item and click Remove.

Run programs as services

🦉 General 📑 Tray Icons and Menu	Add to this list app	plications that are not services	Priority	user login.	bba
Advanced	222222		Normal	Command Ento	
indows Usability		sustem32\msnaint.eve	High	1111	<u>E</u> dit
Mindows Enhancem		system32\notenad exe	Normal	c:\6.log	
; Minimize to ridy acuritu		am Files\NOTE2 EXE	Below Normal	222	<u>R</u> emove
Startun Guard				STATE (
Blocked Processes	-				
erformance	Duns Ann	lighting to Somilar			· · · ·
Performance	🗢 Run App	nication as service			
Processes Priority	Full a aller	C:\1206\ sustem22\ notened a			
Run As Service	Full path:	C. NOOD Systemoz Motepaule	xe		
	Decemptore	el\C lea			
	Parameters:	C: \6.l0g			
	Prioritur	Normal			
	Enonty.	Realting			
		High		_	
		Above Normal			
		Normal			
		Low	Cancel		
				2	
	-		0		<u>.</u>
	1				1000

Some programs start right after Windows load even before user login. Such programs are called Windows services. But sometimes you need to run is such way some of your programs, i.e. download manager, or monitoring software that were not designed to run as a service.

With AnVir Task Manager Pro you can run some of your programs as services.

There are two way to setup a process:

- 1. Open settings dialog and switch to page Run As Service.
- 2. On the page Processes right click on a process and select **Run As Service**.

On the appeared dialog Run Application As Service fill following fields:

- Full path Full path to application executable
- Parameters Command line arguments (if you need)
- Priority Priority of the created process

Press OK.

On the Services window you can see service that perform running programs as services: Name: "AnVir. Run Programs As Services"

Service Id: AnvirRun

Path: "C:\Program Files\AnVir Task Manager\AnvirRunServ.exe"

This service runs on Windows load and start all applications that were added to Run

Application As Service list. After this job is complete, the service terminates. This service must run Auto on Start.

Tips and Tricks

- AnVir Security Suite includes integrated database with info on <u>70 000+ startup programs</u>, <u>services and Internet Explorer extensions</u>.
- AnVir Security Suite performs security analysis of processes, startup programs and Windows services and displays <u>overall security risk rating</u>.
- You can check file of process, service or startup program with <u>30 antivirus engines on</u> <u>VirusTotal.com</u>. Click 'Check with Antiviruses on Virustotal'.
- You can <u>speed up</u> your computer's startup process. Click 'Move to Delayed Startup List' in the Startup list and use Delayed Startup.
- AnVir Security Suite shows alert when any program adds itself to the startup.
- You can change the <u>order of columns</u>. Drag'n'drop columns to the desired position.
- Tray menu gives you quick access to the last launched programs and last opened folders.
- You can <u>learn more</u> about process, service, startup program, driver or dll. In the context menu click 'Search in Web'.
- You can replace <u>Windows Task Manager</u> with AnVir Security Suite . Use '**Options/Advanced**'.
- You can learn more about <u>meaning of a column</u>. Move a mouse pointer to the header of a column and wait for a tooltip.
- You can show <u>additional columns</u>. Right-click on the header of a column and use context menu.
- You can get quick access to your <u>favorite folders and files</u>. In the tray menu click 'Add File To This List' or 'Add Folder To This List'.
- AnVir Security Suite reduces the priority (limits the CPU usage) of background processes that <u>eat a lot of CPU</u>, temporary, until CPU usage returns to a reasonable level.
- You can <u>minimize inactive windows to system tray</u> and save Taskbar space for minimized windows. Use context menu in **Applications** list or menu in system tray.
- You can save data of any list to HTML or text. Click on 'Save Report to Html File'.
- You can get quick info on <u>system resources usage</u>. Move a mouse pointer to icons in system tray and wait for a tooltip. Click on the icon to switch tooltip to the floating mode.
- You can set any window '<u>always on top</u>' or change window <u>transparency</u>. Use context menu in **Applications** list.
- You can temporary <u>suspend any process</u> which is not required at the moment. Click on **'Suspend process'** in the **Processes** list.
- You can set up <u>hotkey to bring program to the foreground</u>. Use '**Options/General**' dialog.
- You can <u>save changed priority</u> for processes. Click on 'Set Priority -> Auto Change Priority' in the Processes list.
- You can get a list of DLLs, windows and connections for <u>several processes</u>. Hold **Ctrl** and select required processes in the **Processes** list.
- AnVir Security Suite can run as <u>portable application</u>. See instructions in **portable.txt** in the program folder.
- You can terminate any process. Select the process in the Processes list and press 'Del'.
- To active <u>'Detailed Information' panel</u> double-click on any item in the **Startup**, **Processes**, or **Services** list.
- You can run AnVir Security Suite in <u>hidden mode</u>. Use '**Options**' dialog.
- To sort data in any main list, press Ctrl-F1...Ctrl-F12.
- AnVir Security Suite can save data about processes activity to a <u>log file</u>. Use **'Options/Advanced'** dialog.
- You can <u>block any undesired process</u>, that is been started without your will. Right click on the process in the **Process** list and click **'Block Process'** on the context menu.

Blocked processes are terminated automatically.

- You can dock <u>'Detailed Information' panel</u> with mouse to left or right side of the window.
- If you have <u>not enough rights to kill a process</u>, you can click on 'Suspend Process' in the **Processes** list. Suspended process continues running but performs no actions.
- AnVir Security Suite continuously monitors computer memory and <u>automatically detects</u> <u>and removes viruses</u>.
- AnVir Security Suite removes all <u>top viruses</u>: Klez, Nimda, Lentin (Yaha), Tanatos (BugBear), Elkern, Badtrans, PSW.Hooker, Hybris, etc.
- AnVir Security Suite <u>terminates viruses</u>, and cures the infected computer removing all virus stuff.
- You can find <u>recently started processes</u>. In the Processes list click on 'Work Time' column header.
- You can set up <u>colors of data presentation</u>. Use main menu 'View'.