What is UnHackMe?

UnHackMe allows you to detect and remove a new generation of Trojan programs - invisible Trojans. They are called "rootkits".

A rootkit is a collection of programs that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network. The intruder installs a rootkit on a computer using a user action, exploiting a known vulnerability or cracking a password. The rootkit installs a backdoor giving the hacker a full control of the computer. It hides their files, registry keys, and process names, and network connections from your eyes.

Your **antivirus can not detect** such programs because they use compression and encryption of its files. The sample software is Hacker Defender rootkit.

You need use UnHackMe to detect and remove Hacker Defender or its clones.

Good luck!

What's new?

Version 4.0

Added new Partizan rootkit detection/removal technology

Partizan allows you to detect hidden rootkits during Windows boot process.

Version 3.1

Added detection/removal of MRoot Rootkit.

Updated rookits database.

Fixed bugs and improved stability.

Version 3.0

Added detection/removal of HackTool Rootkit.

Added detection of Appros Adware Rootkit.

Fixed bugs and improved stability.

Version 2.5

Added detection of AFX Rootkit 2005, Elite Keylogger, hidden processes.

Added Exclusion list.

Version 2.0

Added detection of AFX Rootkit and Vanquish Rootkit,

Version 1.0

Public release.

Detected HackerDefender Rootkit and all its clones.

System Requirements

To use UnHackMe you need:

· A personal computer with Windows NT4/2000/XP/2003 or higher.

· You must use Administrator account privilege to use UnHackMe.

· The amount of disk space you need to install UnHackMe is approximately 3 MB.

· The memory requirements for UnHackMe are similar to those for your operating system (Windows NT4/2000/XP).

Getting Started

After the installation is completed, the program should be activated using the menu Start - Programs - UnHackMe - UnHackMe.

Removal Procedure

1. Click the **Check** button.
2. If a Trojan will be found you will see the **Results** page.
3. Click on the **Stop** button and restart your computer.
4. A rootkit will be completely deleted at the next reboot of your computer.

Copyright/License/Warranty Disclaimer

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

License Agreement

This is not free software. You are hereby licensed to: use the Shareware Version of the software for a 30-days evaluation period; make as many copies of the Shareware version of this software and documentation as you wish; give exact copies of the original Shareware version to anyone; and distribute the Shareware version of the software and documentation in its unmodified form via electronic means. There is no charge for any of the above.

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

Unregistered use of UnHackMe after the 30-days evaluation period is in violation of United States and International copyright laws. A single registered copy of UnHackMe can only be installed/executed on a single computer. For how to register and pay see Registration.

UnHackMe Single License

Recommended if you use the software on one computer.

All users of the computer can use the software.

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

UnHackMe Family License

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

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

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

UnHackMe Business License

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

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

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

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

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

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

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

Disclaimer of Warranty

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

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

How to register this software?

Why should you register?

·For many people, the most pressing reason to register is to get rid of the annoying nag box, which pops up at the most inconvenient times.

· But besides this, registration entitles you free technical support and minor upgrades to the software.

· Registration may also entitle you to discounts on new software releases from Greatis Software. We will also send you information bulletins by email to let you know about what's happening with Greatis Software' shareware products.

· Finally, by registering the software, you provide us with the resources and incentive to support the software with updates and to develop additional quality shareware products in the future.

Pricing and Ordering

You can try UnHackMe before you register. Download a 30-days evaluation version from website. After the evaluation period you have to register the software to continue using it.

If your company or institution is interested in licensing UnHackMe for several users, you can save a lot of money by purchasing a site license.

The registration fee for UnHackMe is $19.95 USD.

After registration an unlock code is e-mailed within one or two days, this enables the software to function beyond the 30 day evaluation period.

Payment can be done via the secure online registration services below; all major credit cards are accepted. We also support ordering by fax, phone, postal mail, wire transfer.

Read order.txt for more details.

http://www.greatis.com/security/unhackme

Registration

1. Open Start menu, Programs, UnHackMe.
2. Choose Register tab in UnHackMe.
3. Paste your registration code from registration message or click on the Browse button to locate for key file. You should save regkey.key file to your hard disk from registration message before this operation.
4. Click on the Register button.
5. Launch UnHackMe, Help, About dialog to check your license.

The legal users of the program receive the right to technical support via e-mail, free-of-charge program fixes and upgrades to the new versions of the program.

Technical support

If you discover an error in the program, visit our support center:

http://www.greatis.com/support

Or send an e-mail to support@greatis.com or ateam@greatis.com.

In the letter specify your name, second name, e-mail.

Try as far as possible to accurately describe all actions that you carried out leading up to the occurrence of the error.

After analysis of the report you will receive a reply with our recommendations for addressing the problem.

About Greatis Software

Greatis Software is a rapidly growing company based in Yaroslavl, Russia that specializes in system software development and programming components for developers.

You may contact us at:

support@greatis.com

Fax: 1-208-330-5710

Visit main site:

http://www.greatis.com

UnHackMe vs HackerDefender

How does it work?

As write an author of Hacker Defender:
*"**Hacker Defender (hxdef)** is a rootkit for Windows NT 4.0, Windows 2000 and Windows XP, it may also work on latest NT based systems.*
Program must be absolutely hidden for all others. Now the user is able to hide files, processes, system services, system drivers, registry keys and values, open ports, cheat with free disk space. Program also masks its changes in memory and hides handles of hidden processes. Program installs hidden backdoors, register as hidden system service and installs hidden system driver. The technology of backdoor allowed to do the implantation of redirector.
***Morphine** is very unique application for PE files encryption. Unlike other PE encryptors and compressors Morphine includes own PE loader which enables it to put whole source image to the text section of new PE file. This one is very powerful because you can compress source file with your favourite compressor like UPX and then encrypt its output with Morphine.*
Another powerful thing here is polymorphic engine which always creates absolutely different decryptor for the new PE file. This mean if your favourite trojan horse is detected by an antivirus you can encrypt it with Morphine. You will not get the virus alert again."
Antiviral software could not detect the HackerDefender encrypted by Morphine.
Please, take a look at McAffe description of HackerDefender.
We need the universal detector and removal too for HackerDefener.

UnHackMe can help you

UnHackMe allows you quickly and easily detect HackerDefener and its clones.
UnHackMe uses the fact that HackerDefender installs the service and driver.
HackerDefender hides these keys from enumeration by registry functions.
We can export the registry hive to a file. The export function writes all registry keys and values into binary file without filtering.
We can get the list of services from exported file and compare it with the current registry keys list. It's not easy because the format of Microsoft registry binary files is not documented. But we can do it!
After that the hidden keys will be easily found. **That's all!**

Removal Procedure

1. Click the **Check** button.
2. If a Trojan is found you will see the **Results** page.
3. Click on the **Stop** button and restart your computer.
4. HackerDefener Rootkit will be completely deleted at the next reboot of your computer.

UnHackMe vs AFX Rootkit

AFX Rootkit is created by Aphex in 2004. It works with WINDOWS NT/2000/XP/2003.
AFX Rootkit hides:

1. Processes
2. Handles
3. Modules
4. Files & Folders
5. Registry Values
6. Services
7. TCP/UDP Sockets
8. Systray Icons

How does it work?

AFX RootKit uses the driver "mc21.tmp" located in the Temp folder.
AFX RootKit installs the hidden service. The name of the service is chosen by the hacker. Usually a hacker installs AFX RootKit to the Windows subfolder. In this case the AFX Rootkit service name will be equal to the subfolder name.
AFX RootKit does not hide the registry keys of its service and driver. You can use regedit to stop the service manually.

UnHackMe can help you

UnHackMe detects the AFX Rootkit and kills it.
You should restart your computer to completely remove the AFX RootKit.
UnHackMe will delete the service and the Trojan's file at the next reboot.

Removal Procedure

1. Click the **Check** button.
2. If a Trojan is found you will see the **Results** page.
3. Click on the **Stop** button and restart your computer.
4. AFX Rootkit will be completely deleted at the next reboot of your computer.

UnHackMe vs Vanquish Rootkit

Vanquish is created by XShadow in 2003-2004.
It works with WINDOWS 2000/XP/2003.
Vanquish is a DLL-Injection based rootkit that hides files, folders, registry entries and logs passwords.

Vanquish Rootkit hides:

1. Processes
2. Handles
3. Modules
4. Files & Folders
5. Registry Values
6. Services

How does it work?

Vanquish RootKit hides all registry keys. If you open Registry Editor (regedit.exe) you will see no subkeys. Vanquish hides the registry subkeys and value names. It substitutes the subkey names with the empty strings.

Vanquish doesn't allow you to delete its service registry key even if you know the service name.

UnHackMe can help you

UnHackMe detects the Vanquish Rootkit and kills it.

You should restart your computer to completely remove the Vanquish RootKit.

UnHackMe will delete the service and the Trojan's file at the next reboot.

Removal Procedure

1. Click the **Check** button.
2. If a Trojan is found you will see the **Results** page.
3. Click on the **Stop** button and restart your computer.
4. Vanquish Rootkit will be completely deleted at the next reboot of your computer.

UnHackMe vs Elite Keylogger

Elite Keylogger is made by WideStep Security Software.
http://www.widestep.com/
The authors tell:
"The most powerful keylogger at the market! Experience unique functionality in WideStep's all-in-one Elite Keylogger stealth solution."

How does it work?

It hides the drivers: **usbkbd**.**sys** and **tdiip**.**sys** from driver list.
Also it hides and protects drivers' registry keys.

Hides related files: windump.exe, etc.

Elite Keylogger works similar to Hacker Defender and it is detected as "Hacker Defender" by UnHackMe 1.0-2.0.

Elite Keylogger prevents the removing it from your computer by protecting its files and registry keys.

UnHackMe can help you

UnHackMe detects the **Elite Keylogger** and kills it.

You should restart your computer to completely remove the **Elite Keylogger**.

UnHackMe will delete the service and the Trojan's file at the next reboot.

After restart you will get the Windows error (Blue Screen of Death).

It's normal, restart your computer again and it will work fine.

Removal Procedure

1. Click the **Check** button.
2. If a Trojan is found you will see the **Results** page.
3. Click on the **Stop** button and restart your computer.

Elite Keylogger will be completely deleted at the next reboot of your computer.

UnHackMe vs AFXRootKit 2005

AFX Rootkit 2005 is created by Aphex in 2005.
It works similar to AFX RootKit.
The main difference is that AFX2005 does not hide its service.
AFX2005 hides the process but the service is available and it can be detected using Service Manager or by RegRun.

How does it work?

AFX RootKit uses the driver "mc21.tmp" located in the Temp folder.
The name of the service is chosen by the hacker. Usually a hacker installs AFX RootKit 2005 to the Windows\System32. In this case the AFX Rootkit service name AFX RootKit 2005 does not hide the registry keys of its service and driver. You can use regedit to delete the service manually.

UnHackMe can help you

UnHackMe detects the AFX Rootkit 2005 and kills it.
UnHackMe searches for hidden process and related driver.
You should restart your computer to completely remove the AFX Rootkit 2005.
UnHackMe will delete the service and the Trojan's file at the next reboot.

Removal Procedure

1. Click the **Check** button.
2. If a Trojan is found you will see the **Results** page.
3. Click on the **Stop** button and restart your computer.
4. AFX Rootkit 2005 will be completely deleted at the next reboot of your computer.

UnHackMe vs Hidden Processes

UnHackMe detects the hidden processes.

Hidden process may be created by modifying Windows system process table. Windows Task Manager and other process managers (using PSAPI library) could not detect these processes.

How does it work?

UnHackMe uses own kernel-mode system driver (UnHackMedrv.sys) to check the Windows shadow process tables and to detect hidden process.

It's required to allow the installation of UnHackMedrv.sys to your computer.

The driver doesn't start automatically and it doesn't change stability or security of your computer.

UnHackMe starts the drivers and uses its results to detect the hidden processes.

Removal Procedure

1. Click the **Check** button.
2. If a Trojan is found you will see the **Results** page.
   You will see the list of hidden processes.
   If you want to kill a hidden process, right click on the process and choose "Kill" in the popup menu.
   UnHackMe detects if a service is used to start the process (example AFX 2005).
   In this case you can kill the service too.

3. Click on the **Stop** button and restart your computer.
4. Rootkit will be completely deleted at the next reboot of your computer.

Exclusion List

Use Exclusion list to avoid annoying false positive alarms.
When you receive an alarm, click on the "**False Positive**" button.
You will be prompted to accept list of allowed items.
UnHackMe supports both types of scanned items:

1) Drivers/Services names;
2) Process names.

Confirm your action and you will never be asked again.

Tip!

You can get Exclusion List form using "Options" dialog.
Click on the "Open Exclusion List" button.

Additional Information

"Additional Information" dialog displays the list of the hooked API functions.
You will get the driver names of the hooked functions only if it is possible.

Detecting hidden rootkits using Partizan

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

The simple way to do it is using Windows PE boot CD for checking a computer.

But how often you will do it?

Sometimes… May be one time per week, may be not. It's not enough!

The rootkit can start his work today or tomorrow.

This why you need a way to quickly check a computer for rootkits without luck.

We can offer you to check your computer every Windows boot-up!

How does the Partizan work?

Partizan starts using the **BootExecute** registry key on the early stage of the Windows boot process.

It can get the access to any file or registry keys.

Using another words, Partizan is a king on your computer at the moment.

Partizan executes 2 main tasks:

1) Getting file/registry information.
2) Delete Files/Registry Keys.

The kernel rootkits can cause the trouble with detecting hidden registry keys/files etc. But rootkits are not invulnerable!

The simple way to kill a rootkit is to shutdown your computer.

A rootkit can revive after reboot using:

1) Rootkit service/driver with auto start setting (to be more hidden for user mode checkers).
2) Injection to the executable file or to the process memory. The body may be hidden in the mother file.
3) Using registry startup keys.
4) Infection from network.

The last chance is very dangerous but it can be resolved by simple cut off the network cable.

The second chance is not the simple because the user can control the file integrity using Microsoft or another software.

Third chance is more often used. But rootkit detectors easily detect it.

The fake Winlogon DLLs are not the surprise for us very long ago:-)

The hidden kernel driver is the top of the hacker skills.

This is one reason why the Partizan was created.

Unfortunately Microsoft prevents Partizan for interacting with user using keyboard and it is a

real problem for creating the shell like "cmd". Why they don't?

I think you need ask Microsoft.

Anyway it's not a technical problem. It's the Microsoft decision.

We need to get a workaround.

We use the command file. Partizan opens the command file and executes the tasks listed in it.

After that the Windows boot will continue and UnHackMe will compare Partizan information with current visible.

It will be notify you if it found something suspicious.

To be sure that it's not false positive alert you will be prompted to reboot again. It's required because the some services drivers may be deleted at startup and this will cause the alarm.

Does Partizan is a panacea?

Hackers use a lot of rootkit modification combining with spyware components.

UnHackMe guarantees that you can clean your computer from a deep hidden rootkits.

Does it clean rootkits in the auto mode?

No. You need to make remedy.

If you have enough computer skill to use professional tools – OK, you can do it.

If not, you can send UnHackMe report to the Greatis Support center: http://greatis.com/support and we will send the special file for auto cleaning your computer. The service is for free.

What's about self-protection?

1. You can specify the own file name for Partizan executable.
2. You can change the "Partyizan.exe" name to your desired name.

How to start rootkit detection using Partizan?

Open UnHackMe, choose Options.

Check the "Partizan" box.

How to uninstall Partizan?

Open UnHackMe, choose Options.

Uncheck the "Partizan" box.