

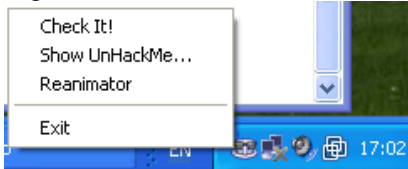
Rootkit Removal using UnHackMe - Master Class

Getting Started

First, open Start menu, choose "Programs", "UnHackMe", "UnHackMe" link.

You also can open UnHackMe using UnHackMe Monitor.

Right click on the "**UnHackMe Monitor**" icon near the clock and choose "Show UnHackMe" option.



After that click on the "**Check me now**" button.



Wait for a few seconds and UnHackMe will display results.

What is under the hood?

Why is the rootkit search so fast?

Other anti-rootkit programs take a lot of time to check the whole registry and all hard drives.

UnHackMe only checks for the hidden keys in the Services and in the Windows Run keys.

If a rootkit hides its registry auto start keys UnHackMe will reveal it.

Rootkit Revealer (by Mark Russinovich) uses the same method but it checks the whole registry.

You should know that UnHackMe was created before the Rootkit Revealer.

After that UnHackMe checks Windows services list and compares it with the registry keys list.

This allows to reveal hidden services.

In addition UnHackMe detects the hidden processes using UnHackMeDrv.sys.

It loads the kernel driver that scans the the kernel memory for hidden processes.

Note! *If you get BSOD during UnHackMe testing, you need to turn off "Detection of hidden processes" in the UnHackMe Options.*

But, that's not all!

UnHackMe checks for rootkits similar to Unreal. Those rootkits use the NTFS streams to hide their file bodies.

UnHackMe detects those rootkits using heuristics algorithm.

And in addition, **UnHackMe checks for rootkits using its signature database unhackmedb.unh.**

This quick check allows to detect a lot of hidden kernel rootkits.

UnHackMe combines heuristics algorithms and signature scanning!

Sometimes UnHackMe alerts are false positives.

Be careful!

But since the end of 2006 this check will not be able to detect deep hidden rootkits like a Rustock.

Also, this check is not able to remove some user mode rootkits/Trojans/Spyware/Adware components.

Therefore, choose the "**Test Windows boot process**" option to get full check.

Reboot is required!



UnHackMe will activate Partizan technology to trace events during Windows boot-up.

You will see these lines on a blue screen:

"Partizan - Rootkit Killer. Greatis Software (c) 2007"

"Partizan driver is active"

Partizan driver is started in the background at the low level stage on the Windows boot.

Partizan.exe (native Windows API application) starts later. It is used to check driver status, delete files and remove services registry keys.

After you log on to Windows, UnHackMe main application automatically starts.

It checks the information from the driver and detects the hidden drivers/services/registry keys.

Caution!

The UnHackMe alerts may be false positives.

Usually it happens if the driver/service starts and deletes its service registry key.

Use with care! How to get back.

Suggestion!

1. Always allow to use Windows System Restore.

UnHackMe automatically creates system restore points before applying changes.

2. Do not remove something if you are not sure.

Tip! Try to restart your computer immediately. If it is a false positive you will not see it again.

If you see repeatedly strange values but you are not familiar with viruses and rootkits - DO NOT CHANGE IT.

Ask Greatis Software Support center.

We remove rootkits everyday. It's our work. Please, let us do our work.

You only need to provide us with some information to test your computer.

Asking the support

What do you need to provide our support specialists with?

1. **Detailed System Report.**

It's a file with about 200K size.

Open Start menu, Programs, UnHackMe group, choose "Reanimator".

Choose "Ask Help from the Support team" tab.

Click on the "Send Detailed Report to Greatis Support Center".

You will receive "regrunlog.txt" on your desktop.

Attach it to your ticket at [Support Center](#)

or attach it to your e-mail message to support@greatissoftware.com

2. **UnHackMe history and error files.**

Open UnHackMe.

Choose "Help" in the menu, select "**Support**", "Display UnHackMe log file", "Display UnHackMe history file".

3. **Windows dump files.**

Those files are located in the hidden folder c:\Windows\Minidump.

Please check that you activated dump creation.

Open Control Panel, System, Additional, Settings.

Choose "Small memory dump 64K".

4. **Samples.**

We can test those files. Please rename file extension to "txt" to avoid e-mail virus checking.

What do you get back?

Support specialists analyze your files and they will send you a "**rnr**" file to automatically resolve the problem and instructions how to use it.

RNR file is a common text file with **Reanimator**'s commands.

You can discover the contents of RNR file using Windows notepad application.

Please! Do not hesitate to contact us.

Rootkit Removal in Depth

- If you have a problem with removing the rootkit *driver* you need to remember:

UnHackMe needs **2 reboots**.

If the driver is already in memory and the driver doesn't provide DriverUnload procedure, there is no way to remove the driver from memory.

We need to reboot.

At the first reboot UnHackMe tries to delete driver file and it's auto start entry in the registry.

But if it is a boot driver, Windows may already load the driver to memory, even after the first reboot.

This may happen because Windows loads the drivers fast, early and in the different threads.

Windows doesn't wait to finish loading the first driver and it tries to load a second one.

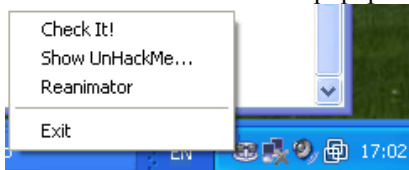
After the first reboot the rootkit driver will not start again but we need to get it out of the memory.

Let's go reboot again!

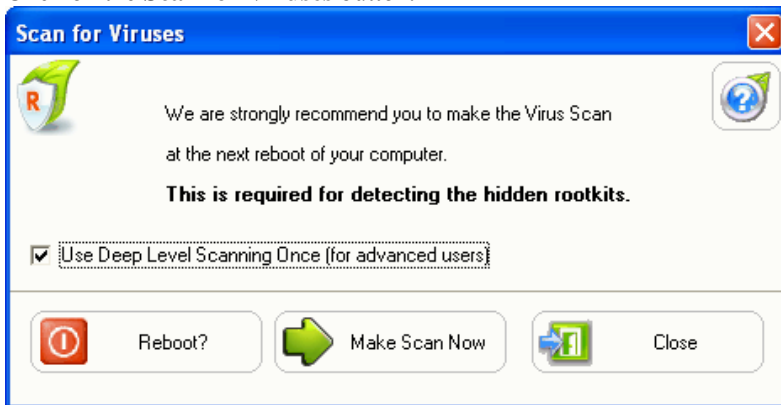
- I know that I am hacked but UnHackMe could not find a rootkit...

Right click on the UnHackMe Monitor icon.

Choose "Reanimator" in the popup menu.



Click on the **Scan for Viruses** button.



Set the box "Use **Deep Level Scanning Once** (for advanced users)"

After that click on the "**Reboot**" button.

What does that mean?

UnHackMe detects **several hundred files** during Windows startup process.

UnHackMe uses Application Database and its own internal database to detect if a file is good or not.

But on your computer there might be a lot of software unknown to UnHackMe.

UnHackMe tries to detect suspicious programs using rules based on the usual rootkit behavior.

These rules are protected by UnHackMe copyright.

But if a rootkit author is smarter than usual, he can mask the rookit file as a legitimate file.

Deep Level Scanning flag will turn off the auto detection rules.

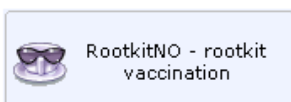
You will see all suspicious files and you will need to determin if a file is good or not.

You should be prepared to see some 10-50 suspicious files. That's OK.

Mark the files as good, if they are, and UnHackMe will never ask you again even during Deep Level Scanning.

UnHackMe detects a rootkit but rootkit gets back even after 3 removal reboots. Nothing helps...

Try to use **RootkitNo** software.



Open UnHackMe, click on the "Check Me Now" button.

UnHackMe will not find anything and it will display the advanced menu.

Then choose "**RootkitNO**" in the menu.

You will see the RootkitNO main window.

Click on the "**Run**" button to proceed.

RootkitNO will ask you for reboot.

What does RootkitNO do?

Modern rootkits use a complex method to hide their service registry keys.

UnHackMe exports the tested registry keys to a binary file.

After that UnHackMe reads the registry keys and values from binary file and compares the binary file contents with the working registry contents.

The differences are the hidden registry keys/values.

But modern rootkits can patch the exported binary file to remove the hidden registry keys/values from the file.

As a result, UnHackMe doesn't see the rootkit.

RootkitNO trick is simple.

RootkitNO saves the "**services**" registry hive to a file. The rootkit cleans its hidden registry keys/values on the fly during normal registry file saving on the disk.

Now we have the "**services**" registry hive that is free of any rootkit!

RootkitNO executes a procedure to substitute the current Services hive with the recently made file.

This operation is executed during reboot.

And now we have a registry without rootkit!

We have used a working rootkit to remove itself.

It is absolutely safe to use RootkitNO.

If you are not infected you will get the same registry as you have before operation. No changes.

RootkitNO is a vaccine. You can use it from time to time.

RootkitNO requirements?

RootkitNO.exe must be stored on the same drive as your Windows folder. Otherwise RootkitNO will get an error and it will not work.

Anyway RootkitNO doesn't cause problems.

Solution: manually copy RootkitNO.exe to any folder on the same drive where Windows is stored. After that launch RootkitNO.

Inspecting hooked Native API functions

UnHackMe has additional features that allow you to see a list of the hooked Native API functions.

Open UnHackMe,

Go to the File menu, **Additional Information**.

You will see the list of the hooked function names with the full path to the related driver (if it is possible to determine the driver file).

Function	Driver
ZwConnectPort	\SystemRoot\System32\vsdatant.sys
ZwDeleteKey	\SystemRoot\System32\vsdatant.sys
ZwDeleteValueKey	\SystemRoot\System32\vsdatant.sys
ZwLoadKey	\SystemRoot\System32\vsdatant.sys
ZwOpenProcess	\SystemRoot\System32\vsdatant.sys
ZwReplaceKey	\SystemRoot\System32\vsdatant.sys
ZwRestoreKey	\SystemRoot\System32\vsdatant.sys
ZwSetValueKey	\SystemRoot\System32\vsdatant.sys

Note! UnHackMe doesn't use this information to detect rootkits using its usual check.

This information is only for power users who understand the hooks and how to use this info.

However it may be useful even if you have no rootkits on your computer to control the software that uses the kernel drivers.

Is it rootkit or not? False Positive?

Remember!

UnHackMe often alerts you about rootkit attacks after installing or removing software or after updating Windows.

Why?

Usually the important files or registry keys are created/deleted during Windows boot process after installing software or Windows updating.

That's normal!

UnHackMe informs you that you need to immediately reboot your computer to be sure that it's a false positive.

If the next reboot is successful - you may be sure that it is a false positive.

Soon you will get enough experience to detect the false positives at first glance.

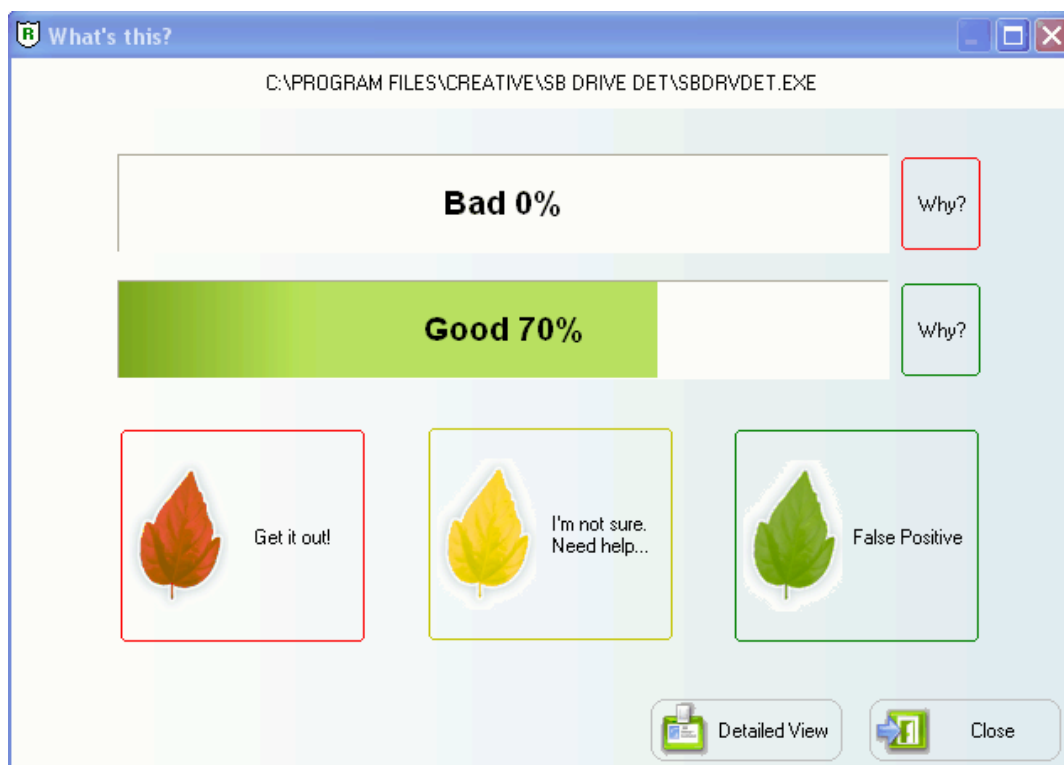
The second false positive issue is the anti-rootkits/antiviral software.

Remember!

Usually this software uses a similar strategy as the rootkits and UnHackMe detects their presence as well.

Take a look at the manufacturer of the software. Contact Gratis Software support and we will help you to make the right decision.

UnHackMe displays the file risk percentage. How to interpret it?



UnHackMe takes a first look at the file and displays the risk percentage using its own evaluative technology.

That helps very well for a quick detection.

You can click on the "Why" buttons to get more information about risks.

But if you have questions, click on the "**I'm not sure**" button.

You will see the additional discovery options:

1) **Search the registry.**

UnHackMe will search the registry for a file name.

Please, be patient. The searching make take a 2-5 minutes.

2) **Get strings.**

UnHackMe will retrieve all text strings (or similar to the human string).

Usually "normal" programs have a lot of readable strings and you can make a decision about if it's good software.

Rootkits are always encrypted and you can see only a minimum number of the strings.

Note! Useful for professionals!

3) **On-line check by several antiviral software.**

Useful for common users.

It allows you to upload a suspicious file to the **www.virustotal.com** site.

The uploaded file will be checked by several (10-20) antiviral engines and you will see the on-line report after 1-15 minutes.

4) **Internet Search.**

UnHackMe will search for the file name using **Gratis File Search**.

Gratis File Search uses the Google search but it gets more information than standard Google searching.

Gratis File Search downloads the linked files, uses Google Search results and searches the text for a file name.

This allows us to get more text information about the file name than any usual Google Search.

You can make a decision using provided information or get advanced discovery.

5) **Send request to the Gratis Software.**

Gratis Software support team will start discovery process after receiving your e-mail.

Gratis Software support team uses the latest information from different sources.

Please, provide a valid e-mail address and check your spam filter to be sure that you can get replies from

"gratissoftware.com", "gratis.com", "gmail.com".