Kaspersky Lab
TECHNICAL SUPPORT

Read the same in:

Home / Fighting malicious programs / Viruses and solutions

Search :

Search tips

Article ID # : search

Home products
1-10 computers

Business products
Workstations & Servers protection

Fighting malicious programs
How to disinfect...

- Common information
- Viruses and solutions
- Rogue security software
- Virus-fighting utilities
- Online Scanner
- Kaspersky Virus Removal Tool 2010

Training and Certification
Take an educational course and become a certified anti-virus security specialist

Self Service
More help online

Support Services and Contacts
Information about support services and rules

You are welcome to subscribe to "New articles in Knowledge base" mailing list.

View subscriptions

How to remove malware belonging to the family Rootkit.Win32.TDSS

In this section you will find recommendations how to fight malicious programs which cannot be disinfected by Kaspersky Lab's products. In order to disinfect/remove malicious programs you may have to modify the system registry or use an additional utility. If you failed to find the necessary information or you find these recommendations too complicated or inadequate, please send a request to the Technical Support service via the HelpDesk form.

How to remove malware belonging to the family Rootkit.Win32.TDSS

ID Article: **2663** | Other languages: | Will be translated: | 9 828 | 2010 Apr 03 22:42 | Printable version

A rootkit is a program or a suite of programs designed to obscure the fact that a system has been compromised.

For Windows operating systems, the term rootkit stands for a program that infiltrates the system and hooks system functions (Windows API). By hooking and modifying low-level API functions, such malware can effectively hide its presence in a system. Moreover, rootkits as a rule are able to conceal in the system any processes, folders and files on a disk as well as registry keys described in its configuration. Many rootkits install own drivers and services (hidden as well) into the system.

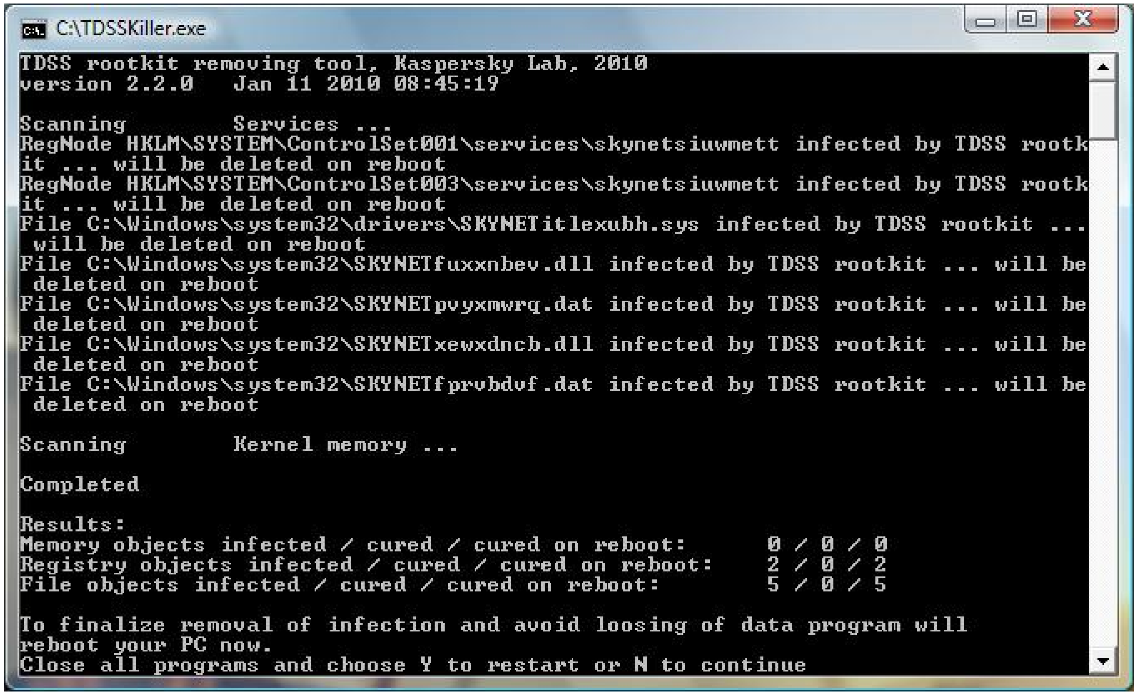
It is possible to disinfect a system infected with malware family ***Rootkit.Win32.TDSS*** using the utility ***TDSSKiller.exe***.

Disinfection of an infected system

- Download the file ***TDSSKiller.zip*** and extract it into a folder on the infected (or potentially infected) PC.
- Execute the file TDSSKiller.exe.
- Wait for the scan and disinfection process to be over. You do not have to reboot the PC after the disinfection is over.

When run without parameters, the utility will:

- The registry is scanned for hidden services. The utility will remove the services identified as belonging to TDSS.
  Otherwise, the user is prompted to eliminate the service.
  The services are eliminated upon a reboot.

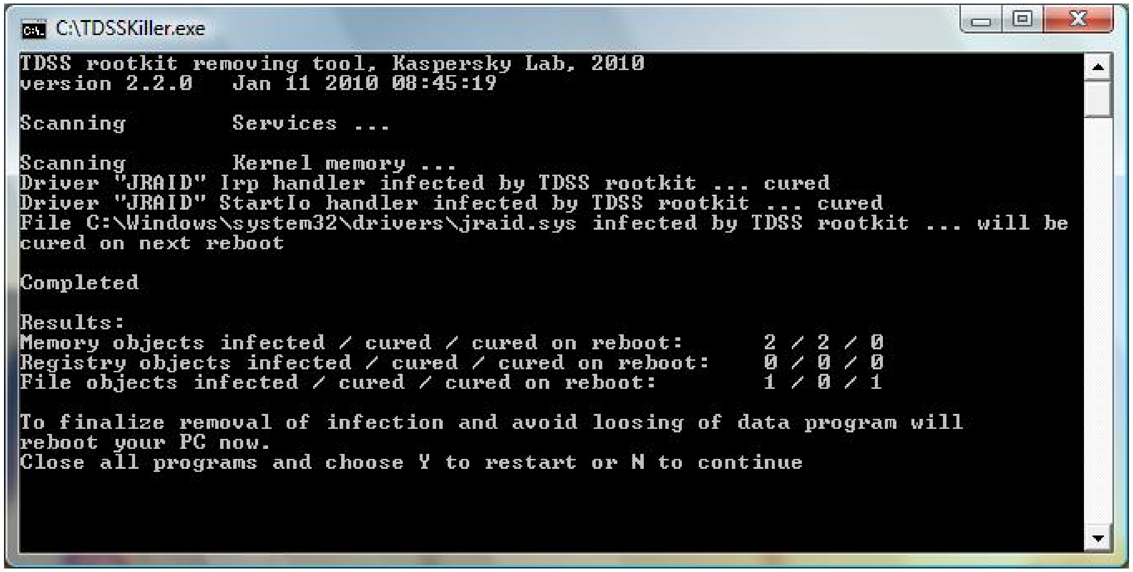


```
TDSS rootkit removing tool, Kaspersky Lab, 2010
version 2.2.0   Jan 11 2010 08:45:19

Scanning        Services ...
RegNode HKLM\SYSTEM\ControlSet001\services\skynetsiuwmett infected by TDSS rootk
it ... will be deleted on reboot
RegNode HKLM\SYSTEM\ControlSet003\services\skynetsiuwmett infected by TDSS rootk
it ... will be deleted on reboot
File C:\Windows\system32\drivers\SKYNETitlexubh.sys infected by TDSS rootkit ...
 will be deleted on reboot
File C:\Windows\system32\SKYNETfuxxnbev.dll infected by TDSS rootkit ... will be
 deleted on reboot
File C:\Windows\system32\SKYNETpvyxmwrq.dat infected by TDSS rootkit ... will be
 deleted on reboot
File C:\Windows\system32\SKYNETxewxdncb.dll infected by TDSS rootkit ... will be
 deleted on reboot
File C:\Windows\system32\SKYNETfprvbdvf.dat infected by TDSS rootkit ... will be
 deleted on reboot

Scanning        Kernel memory ...

Completed

Results:
Memory objects infected / cured / cured on reboot:      0 / 0 / 0
Registry objects infected / cured / cured on reboot:    2 / 0 / 2
File objects infected / cured / cured on reboot:        5 / 0 / 5

To finalize removal of infection and avoid loosing of data program will
reboot your PC now.
Close all programs and choose Y to restart or N to continue
```

- System drivers are scanned for infection. In case an infection has been detected, the utility will search for an available backup copy of an infected file.
  If an available backup copy of an infected file has been detected, the utility will restore the file from it. Otherwise, the utility will attempt to disinfect the file.

- By default, the utility outputs runtime log into the system disk root directory (the disk where the operating system is installed, *C:\* as a rule).
  The log is like *UtilityName.Version_Date_Time_log.txt*.
  for example, *C:\TDSSKiller.2.2.0_20.12.2009_15.31.43_log.txt*.

- When its work is over, the utility prompts for a reboot to complete the disinfection.
  The driver will execute all scheduled operations and kill itself upon the next system reboot.



```
TDSS rootkit removing tool, Kaspersky Lab, 2010
version 2.2.0   Jan 11 2010 08:45:19

Scanning        Services ...

Scanning        Kernel memory ...
Driver "JRAID" Irp handler infected by TDSS rootkit ... cured
Driver "JRAID" StartIo handler infected by TDSS rootkit ... cured
File C:\Windows\system32\drivers\jraid.sys infected by TDSS rootkit ... will be
cured on next reboot

Completed

Results:
Memory objects infected / cured / cured on reboot:      2 / 2 / 0
Registry objects infected / cured / cured on reboot:    0 / 0 / 0
File objects infected / cured / cured on reboot:        1 / 0 / 1

To finalize removal of infection and avoid loosing of data program will
reboot your PC now.
Close all programs and choose Y to restart or N to continue
```

Command line parameters to run the utility TDSSKiller.exe

-l <file_name> - write log to a file.
-v – write a detailed log (must be used together with the –l parameter).
-d <service_name> - search for a specific malicious service name.
-o <file_name> - save a dump into the specified file. This dump is needed for analysis in case of problems with detection.

For example, if you want to scan the PC with a detailed log saved into the file *report.txt* (it will be created in the folder with TDSSKiller.exe), use the following command:

```
TDSSKiller.exe -l report.txt
```

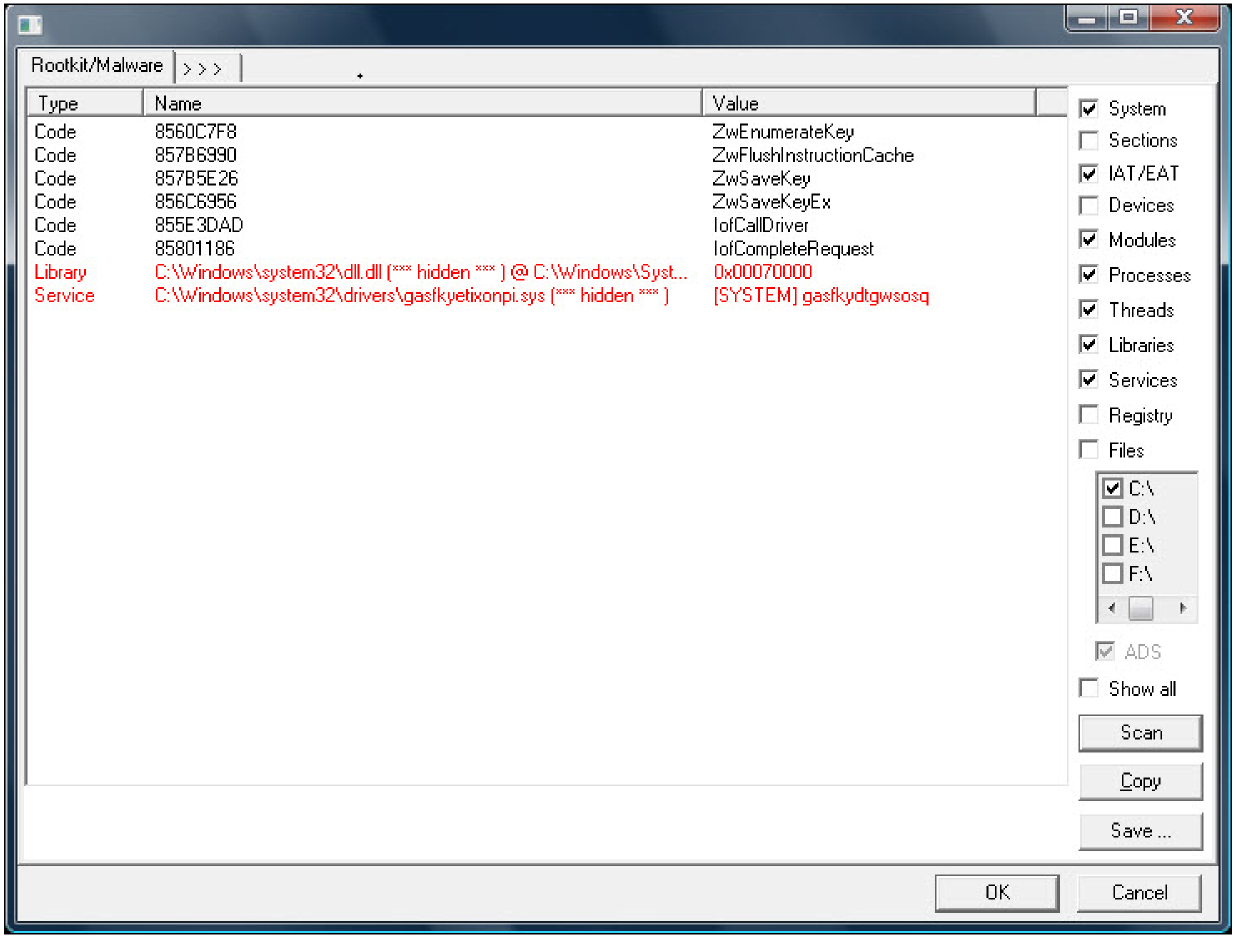
Symptoms of an infection

- Symptoms of infection with Rootkit.Win32.TDSS first and second generation (TDL1, TDL2)

  Experienced users may try to monitor the following kernel function hooks:

  - IofCallDriver;
  - IofCompleteRequest;
  - NtFlushInstructionCache;
  - NtEnumerateKey;
  - NtSaveKey;
  - NtSaveKeyEx.

  Using the utility ***Gmer***.

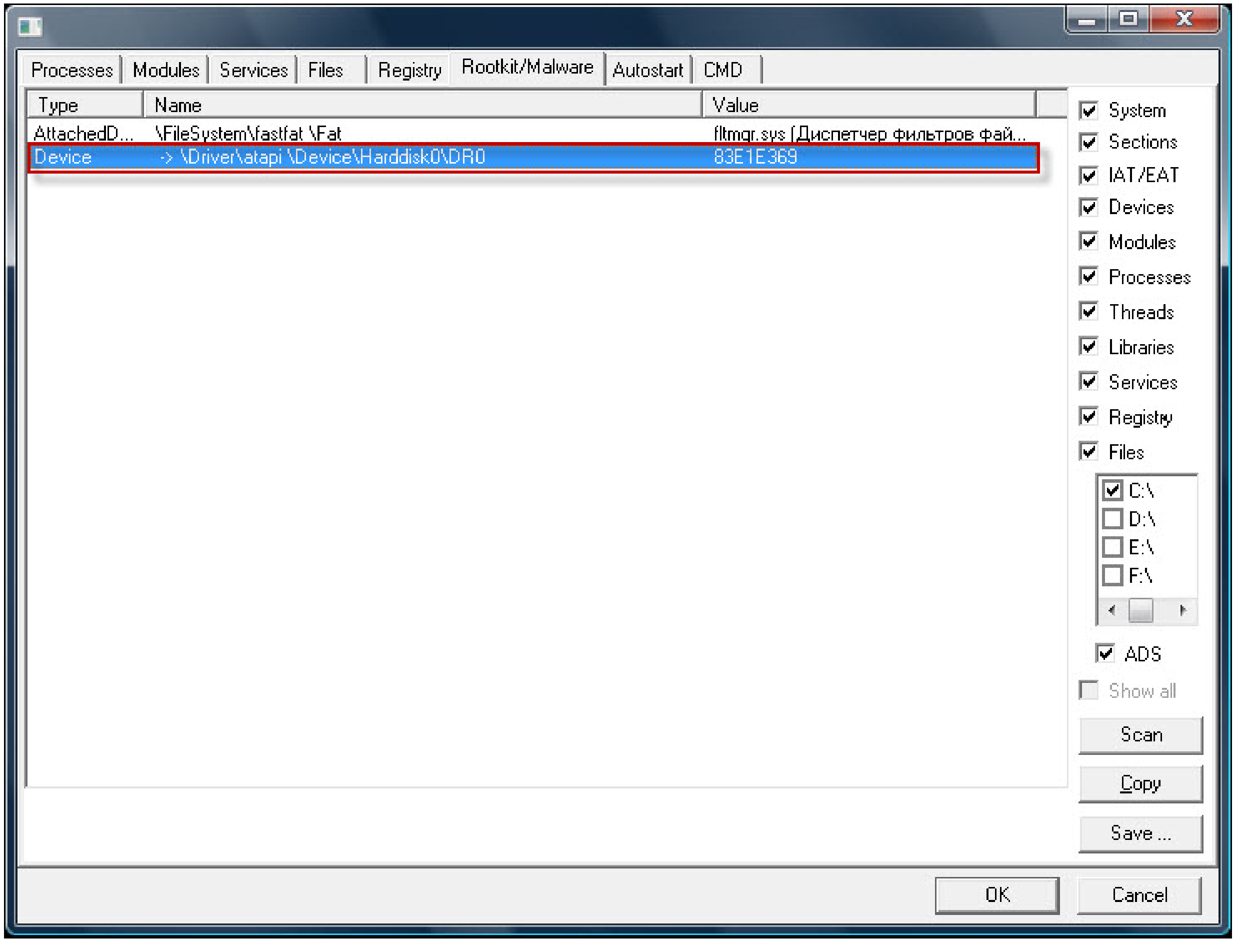


Type	Name	Value
Code	8560C7F8	ZwEnumerateKey
Code	857B6990	ZwFlushInstructionCache
Code	857B5E26	ZwSaveKey
Code	856C6956	ZwSaveKeyEx
Code	855E3DAD	IofCallDriver
Code	85801186	IofCompleteRequest
Library	C:\Windows\system32\dll.dll (*** hidden ***) @ C:\Windows\Syst...	0x00070000
Service	C:\Windows\system32\drivers\gasfkyetixonpi.sys (*** hidden ***)	[SYSTEM] gasfkydtgwsosq

☑ System
□ Sections
☑ IAT/EAT
□ Devices
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
□ Registry
□ Files
☑ C:\
□ D:\
□ E:\
□ F:\
☑ ADS
□ Show all

- Symptoms of infection Rootkit.Win32.TDSS third generation (TDL3)

  An infection can be detected with utility ***Gmer***. It detects replacement of a “device” object of the system driver ***atapi.sys***.



Type	Name	Value
AttachedD...	\FileSystem\fastfat \Fat	fltmgr.sys (Диспетчер фильтров фай...
Device	-> \Driver\atapi \Device\Harddisk0\DR0	83E1E369

Did the provided info help you?

Yes No

Give your detailed feedback.