Protect your PC from stealth malware with Anti-Rootkit technology

Fighting malicious software is a non-stop "arms race". In response to the emergence of the new types of threats, antivirus vendors release new security technologies to combat them. Cybercriminals respond by trying to find ways to bypass that protection. The security of users depends on which side can make its mechanisms more sophisticated.

One highly sophisticated and dangerous type of malware is the rootkit. TDSS, PMax, Zbot are just a few of the dangerous malicious programs that use rootkit technologies. With different methods of masking their presence in the system, these malicious programs often penetrate into computers even when they are protected by anti-virus solutions.

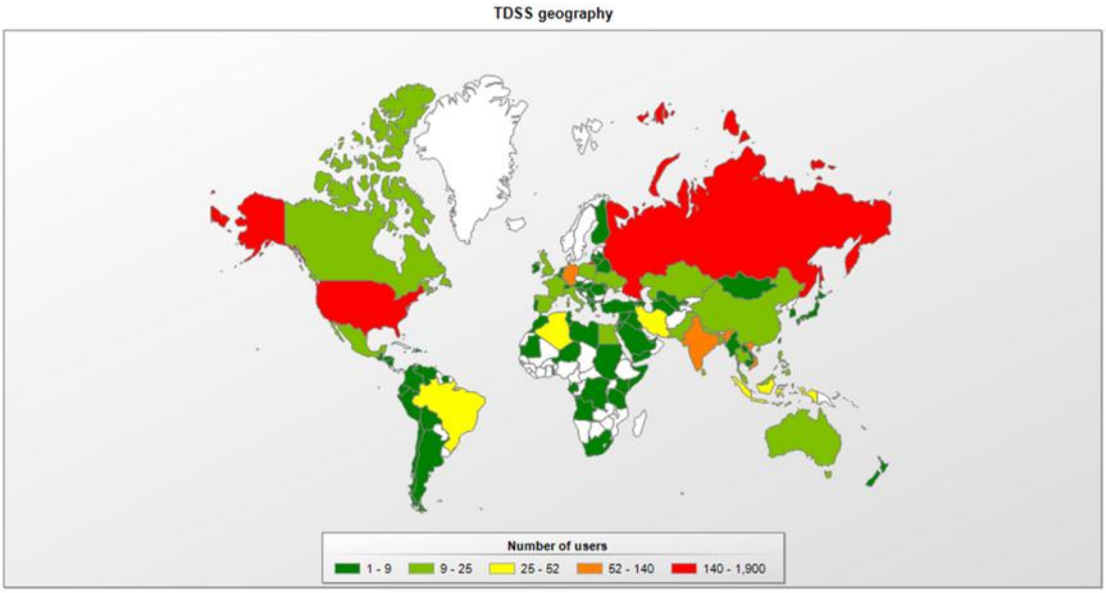


Figure 1. The geographical distribution of TDSS over the period of one month (April 2013) according to Kaspersky Security Network.

Rootkit in details

The use of rootkit technology on an infected PC allows cybercriminals to perform all sorts of illegal operations without the user's knowledge: to steal payment information or personal data, to interfere with software processes, to thwart the work of the security solution, to distort or completely delete user files. In other words, rootkits offer full control over all processes in the operating system.

To mask their presence in the system, rootkits utilize a variety of tools: intercepting system services, file blocking, modifying access rights to information resources, injecting code into trusted system processes, etc. Some examples of this type of malicious software (the so called bootkits) modify the master boot record on the hard disk in order to gain control over the user's operating system before it is even loaded, and therefore before the launch of any protection software.

When the above techniques are used to conceal the presence of malware in the OS, it makes serious demands of any anti-virus protection on the computer:

- The anti-virus solution should be able to detect the presence of rootkit components and prevent their malicious operations in the OS
- On detecting a rootkit, the anti-virus solution should be able to completely remove all its components from the system and to restore any functions which may have impaired
- Anti-virus software should include reliable self-protection tools to combat rootkit components, because many malicious programs possess functionality that allows them to disable protective solutions

Kaspersky Lab’s approaches to fight rootkits

Rootkits utilize many techniques to stay invisible to protection tools. Rootkits often inject into the earlier stages of loading the operating system, working before any security solution can run. To fight these so-called bootkits, Kaspersky Lab’s integrated technology controls every call addressed to the boot partition of the hard drive and detects malware. The technology uses heuristic algorithms to identify even unknown bootkit types based on their behavior in the system, and can effectively roll back any changes made by the malicious program.

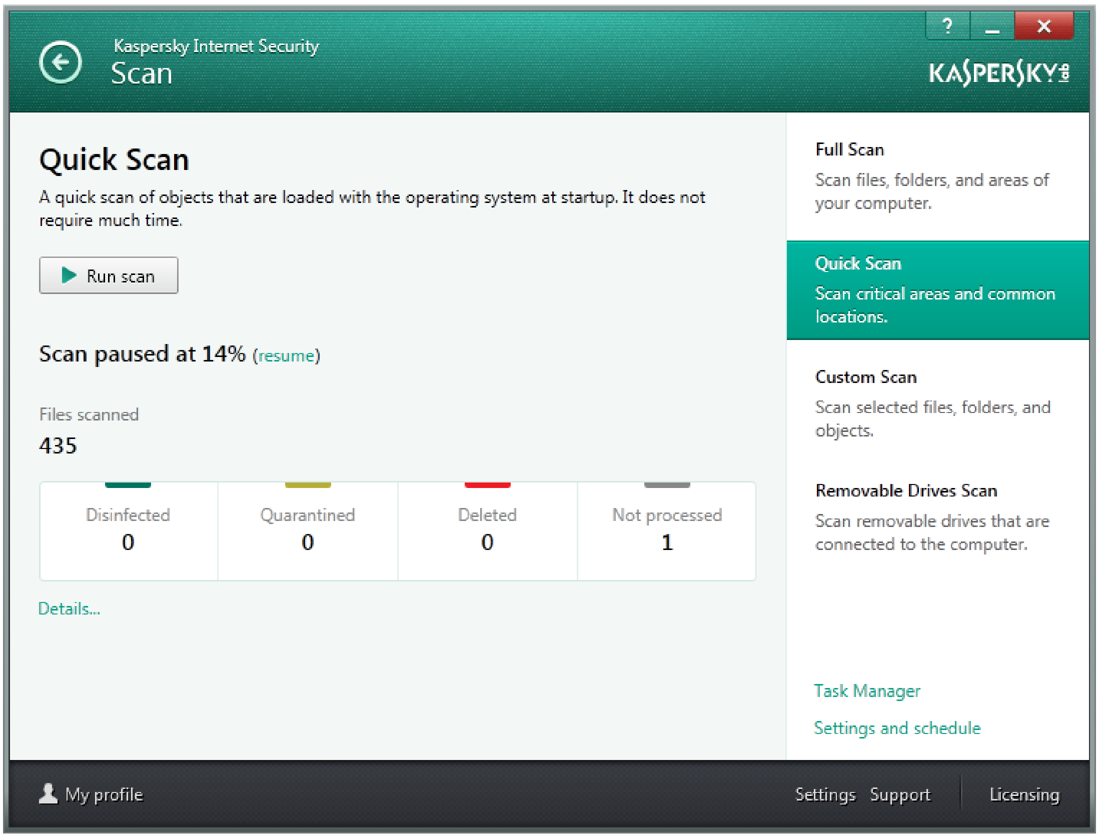
Proprietary low-level file system analyzers also perform a scan of hard disk volumes. In combination with low-level disk access this can use signature-based detection to determine all currently known rootkits that may be hiding their presence in the file system.

Treating a system which has been attacked by a rootkit is another serious challenge requiring special tools. Many of these programs use a host of means of self-defense. For example, they may change standard OS mechanisms to make it as difficult as possible to detect and remove their components.

Kaspersky Lab’s Anti-Rootkit technology contains an original mechanism to bypass these malicious modifications in the operating system, as well as technology which offers multi-level control over the treatment process. In combination, they can effectively detect and remove rootkit components. In other words, even if the rootkits are able to modify the OS code in their favor, the Anti-Rootkit from Kaspersky Lab "knows" how to bypass the restrictions resulting from such modifications and remove the malware.

In this case, Kaspersky Lab’s treatment is able to deal with any possible negative consequences of the rootkit infection. For example, if an object cannot be disinfected, the antivirus is able to remove it. However, the removal of certain objects (for example, file system drivers) may cause system failure. That is why Kaspersky Lab’s security solutions do not remove all infected objects but maintain a list of critical system objects and checks before removing them.

In addition, rootkits use a wide variety of techniques to deactivate antivirus products by compromising or deleting their key components. Kaspersky Lab’s products provide mechanisms to monitor the performance of its components and neutralize any malicious attempts to block the performance of the anti-virus solution.



Kaspersky Internet Security
Scan

Quick Scan

A quick scan of objects that are loaded with the operating system at startup. It does not require much time.

Scan paused at 14% (resume)

Files scanned
435

Disinfected	Quarantined	Deleted	Not processed
0	0	0	1

Full Scan
Scan files, folders, and areas of your computer.

Quick Scan
Scan critical areas and common locations.

Custom Scan
Scan selected files, folders, and objects.

Removable Drives Scan
Scan removable drives that are connected to the computer.

Availability

Anti-Rootkit technology is integrated into the following products for home users and business:

For home users

- Kaspersky Internet Security
- Kaspersky Internet Security – Multi-Device
- Kaspersky Total Security – Multi-Device
- Kaspersky Anti-Virus

For business

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security

Benefits of Anti-Rootkit technology

Cybercriminals will always try to develop malware which passes unnoticed through antivirus solutions. So when choosing a protection product for your home computer, pay special attention to the product's ability to cope with sophisticated types of malware – rootkits and other similar programs. Kaspersky Lab's solutions contain all the technologies necessary:

- An advanced algorythm of low-level access to data can detect threats which modify hard disk structures
- An advanced mechanism for bypassing malicious modifications in the operating system
- Control over critical system files
- Multi-level control over the treatment process
- Control over the performance of the anti-virus solution

The use of Kaspersky Lab’s protection solutions with integrated Anti-Rootkit technology ensures the safety of the user’s important information, e-payments and other valuable online information.