



Dr.WEB

for macOS

User Manual



© **Doctor Web, 2018. All rights reserved**

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

Trademarks

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web for macOS
Version 11.1
User Manual
12/19/2018

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125040

Website: <https://www.drweb.com/>

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!



Table of Contents

| | |
|--|-----------|
| 1. Introduction | 6 |
| 1.1. Document Conventions | 6 |
| 1.2. About Dr.Web | 6 |
| 1.3. Main Components and Functions | 7 |
| 2. Installation and Removal | 8 |
| 2.1. System Requirements | 8 |
| 2.2. Installing and Removing Dr.Web | 8 |
| 3. Managing Licenses | 9 |
| 3.1. License Key File | 9 |
| 3.2. License Manager | 10 |
| 3.3. License Activation | 10 |
| 4. Basic Functions | 13 |
| 4.1. Starting and Quitting Dr.Web | 14 |
| 4.2. Updating Virus Databases | 15 |
| 4.3. Constant Anti-virus Protection | 15 |
| 4.4. Scanning System on Demand | 16 |
| 4.5. Neutralizing Threats | 18 |
| 4.6. HTTP Traffic Scan And Access Control to Web Resources | 20 |
| 4.7. Getting Help | 22 |
| 5. Advanced Use | 23 |
| 5.1. Quarantine | 23 |
| 5.2. Configuring Automatic Actions | 25 |
| 5.3. Excluding Objects from Scanning | 25 |
| 5.4. Scan Encrypted Traffic | 26 |
| 5.5. Notifications | 26 |
| 5.6. Administrator Privileges | 27 |
| 5.7. Optimizing Battery Use | 27 |
| 5.8. Dr.Web Cloud | 28 |
| 5.9. Operation Mode | 28 |
| 5.10. Restoring Default Settings | 30 |
| 6. Appendices | 31 |
| 6.1. Appendix A. Types of Computer Threats | 31 |
| 6.2. Appendix B. Fighting Computer Threats | 34 |



6.3. Appendix C. Central Anti-virus Protection

36

6.4. Appendix D. Hot Keys

38

6.5. Appendix E. Technical Support

39




1. Introduction

Thank you for purchasing Dr.Web for macOS (hereinafter referred to as Dr.Web). It offers reliable protection from various types of computer threats using the most advanced virus detection and neutralization technologies.

This manual is intended to help users of computers running macOS install and use Dr.Web.

1.1. Document Conventions

The following symbols and text conventions are used in this guide:

| Convention | Comment |
|---|---|
|  | Warning about possible errors or important notes to which you should pay special attention. |
| <i>Anti-virus network</i> | A new term or an accent on a term in descriptions. |
| <IP-address> | Placeholders. |
| Save | Names of buttons, windows, menu items and other program interface elements. |
| CTRL | Keyboard keys names. |
| /Volumes/Macintosh HD/ | Names of files and folders, code examples. |
| Appendix A | Cross-references on the document chapters or internal hyperlinks to web pages. |

1.2. About Dr.Web

Dr.Web is an anti-virus solution designed to help users of computers running macOS protect the machines from viruses and other types of threats.

The core components of the application (*anti-virus engine* and *virus databases*) are not only extremely effective and resource-sparing but also cross-platform, which allows specialists in Doctor Web to create secure anti-virus solutions for different operating systems. Components of Dr.Web are constantly updated and virus databases are supplemented with new signatures to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.



1.3. Main Components and Functions

Dr.Web consists of the following components each performing its own set of functions:

| Component | Description |
|-----------------|--|
| SpIDer Guard | This is a resident anti-virus component which scans all files (which are being used) in real time. |
| SpIDer Gate | This component scans the incoming HTTP traffic and blocks all malicious objects. It is also used to control access to web resources. |
| Scanner | This virus-detection component is used for: <ul style="list-style-type: none">• Express, full and custom system scan on user demand.• Neutralization of detected threats (Cure, Delete, Move to quarantine). The action is either selected by the user manually, or automatically according to the Dr.Web preferences for the corresponding type of threat. |
| Quarantine | This is a special folder which is used for isolation of infected files and other threats so that they cannot do harm to the system. |
| Updater | This is an automated updating utility that is used for updating virus databases and other application components. |
| License Manager | This component is used to simplify management of the licenses. It allows to view information about the current license, activate license or demo period or get a new license. |

Flexible settings of Dr.Web allow to configure sound and on-screen notifications for various events, automatic actions applied by the app to detected threats, updates periodicity, list of files and folders excluded from scanning, and so on.



2. Installation and Removal

Dr.Web is distributed as a single disk image file. The file can be found on the product CD/DVD or downloaded via the Internet from the official Doctor Web [website](#).



Dr.Web is not compatible with anti-virus software including its own earlier versions. Installing two anti-virus apps on one computer may lead to system crash and loss of important data. If you already have an anti-virus software installed, [uninstall](#) it before starting a new anti-virus installation.

2.1. System Requirements

Dr.Web can be installed on computers running macOS 10.7 or later. Other requirements are similar to those of the operating system.

2.2. Installing and Removing Dr.Web

Dr.Web software is distributed as a single disk image file.

To install Dr.Web

1. Download the installation file from <https://download.drweb.com/mac/>.
2. Run the installation file.
3. Double-click the Dr.Web for macOS icon or move it to the Applications folder.
4. Accept the License Agreement terms. The installation process starts.
5. Enter administrator password and click the Install Helper button.
6. Dr.Web for macOS will be copied into the Applications folder and start automatically.

To uninstall Dr.Web

To delete Dr.Web, you can simply move the app to Trash. If necessary, enter user name and password of the administrator account in the corresponding dialog.



3. Managing Licenses

To use Dr.Web, you need to activate a license. You can purchase a license with the product or on the official Doctor Web [website](#). A license allows to take advantage of all product features during the whole period. Parameters of the key file are set in accordance with the software license agreement. To activate a license, renew it after it is expired or purchase a new one, [License Manager](#) is used.



If Server.app is installed on your computer, the operating system is defined as macOS Server. In this case, to use Dr.Web, you need either to remove Server.app or purchase the Dr.Web for macOS Server license.

It is recommended that you activate the license after installation because it unlocks [updating](#), [constant protection](#) and [on-demand scanning](#) features.

If you want to evaluate the product before purchasing it, you can activate a demo period. It provides you with full functionality of the main components, but the period of validity is considerably restricted.



You can activate a demo period for the same computer no more than once a year.

Demo period is available for:

- 3 months. For that, register on the official Doctor Web [website](#) and receive a serial number.
- 1 month. For that purpose, no serial number is required and no registration data is requested.

3.1. License Key File

The license type is determined by a special file called the *license key file*. The license key file contains the following information:

- Duration of the application license
- List of components a user is allowed to use
- Other restrictions (for example, the number of users allowed to use the app)

A license for Dr.Web file satisfies the following criteria:

- License is not expired
- All application components required by the product are licensed
- Integrity of the license is not violated

If any of the conditions is violated, the license becomes *invalid* and Dr.Web stops detecting and neutralizing threats.



The license key file has the `.key` extension and it can be received during the [license activation](#) procedure at first launch of Dr.Web via the [License Manager](#).

The parameters of the license key file which specify the user's rights are set in accordance with the License agreement. The file also contains information on the user and seller of the app.

It is recommended that you keep the license key file until the license or demo period expires.



A license key file for a demo period activation can be used only on the computer where the activation procedure was run.

3.2. License Manager

To managing licenses, use the License Manager component.

To open License Manager, do one of the following:

- Click **License Manager** in the application menu (the menu bar is at the top of the main desktop)
- In the main application window, click the license information section.

The **Dr.Web License** window displays the information on your current license. The **Get New License** button allows you to activate your license for Dr.Web or renew an expired license.

3.3. License Activation

After installation, you need to activate Dr.Web to confirm legitimacy of using the app and unlock the [updating](#), [constant protection](#) and [on-demand scanning](#) features.

When you run Dr.Web for the first time, activation starts automatically. You can also launch activation from [License Manager](#) by clicking **Get New License**.

To activate a new license

1. If you have a serial number for activation of a license or a demo period for 3 months, on the first step of the activation procedure, click **Activate license**.
2. Enter the serial number and click **Next**. In case you are activating a demo period, go to the step 5.
3. If you have a previous license, provide its serial number. Select the corresponding option, then enter the serial number or drag the key file to the dotted area (alternatively, click the area to browse the key file).

If you have been a user of Dr.Web in the past and are activating a new license, you are eligible for extension of your new license for another 150 days. To get additional 150 days, you need to submit your previous license data: a serial number or a license key file.



If you have been a user of Dr.Web in the past and are activating a [renewal license](#), you need to submit serial number or a license key file of your previous license. In case neither a serial number nor a license key file is provided, the new license period will be reduced by 150 days.

Click **Next**.

4. Enter personal data (registration name, region, city, and so on). The **Registration name** field is obligatory and should be filled in. If you want to receive news about Doctor Web by email, select the corresponding check box. Click **Next**.
5. The license will be activated and installed on your Mac. Usually, this procedure does not require your active participation. If the activation procedure completed successfully, the corresponding message appears where the license validity period or demo period is specified.

Click **Done**. If the activation failed, an error message appears.

To get demo

If you installed Dr.Web with demonstration purposes, click **Get demo**. You can activate a demo period to evaluate Dr.Web:

- For 3 months. For that, register on the [website](#) and receive a serial number. Serial number is sent to the email address specified during the questionnaire. You can activate it by clicking **Activate license** in [License Manager](#).
- For 1 month. For that purpose, no serial number is required and no registration data is requested.

To purchase license

If you do not have a serial number, on the first step of the activation procedure, click **Purchase license** to purchase the license from Doctor Web online store.

It is recommended that you keep the [license key file](#) until it expires. If you re-install the product or install it on several computers, you will be able to use the previously activated license key file.

To install existing license key file

1. On the first step of the activation procedure, click **Other activation types**.
2. If you already have a license key file or a configuration file required for the connection to the [anti-virus network](#) and operation in the central protection mode, drag it to the dotted area or click to browse to select the file.
3. To activate you license, click **Next**.

Subsequent activation

You may need to reactivate a license or demo period if the license key file is lost.



When reactivating a license or a demo period you receive the same license key file as during the previous activation providing that the validity period is not expired.



A demo period can be reactivated only on the computer where the activation procedure was run.

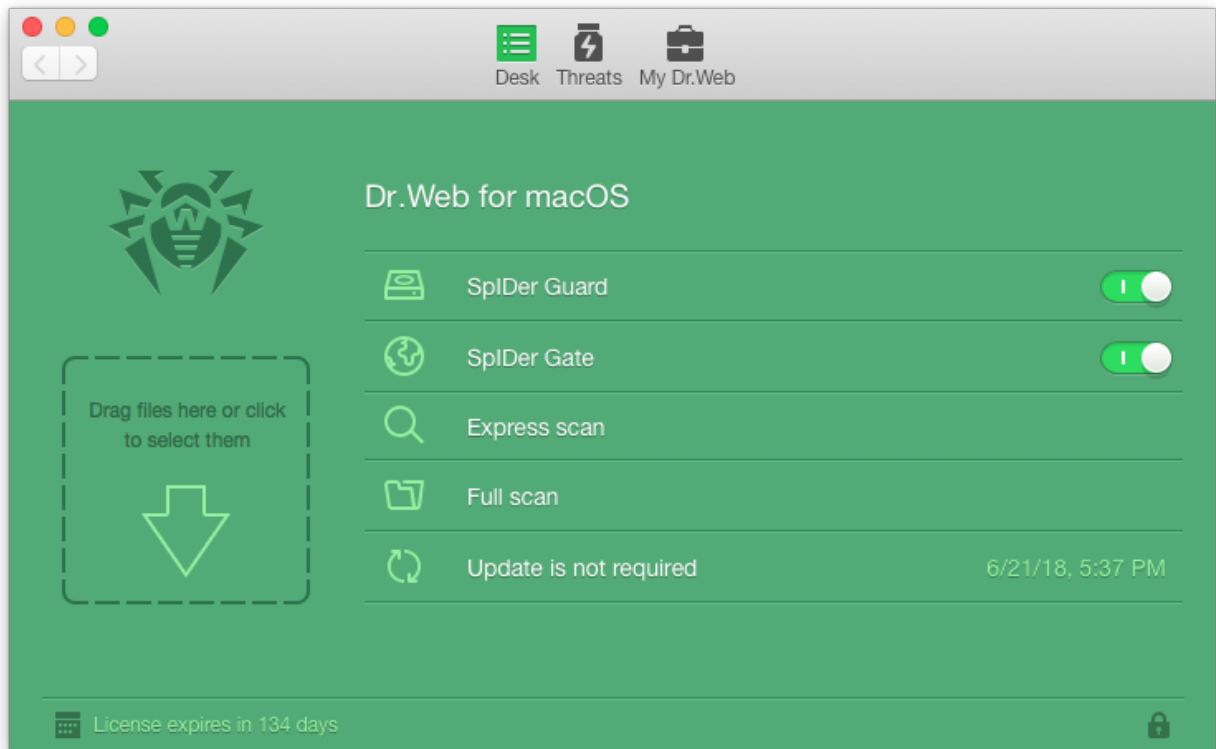
One serial number can be activated not more than 25 times. If more requests are sent, the license will not be activated. In this case, to receive a lost license key file, contact [technical support](#) describing your problem in detail, stating your personal data input during the license activation and the serial number.



4. Basic Functions

You can access all main functions from the Dr.Web window (see picture below). This window consists of sections that helps you control and access Dr.Web components:

| Section | Description |
|-----------|--|
| Desk | <p>In this section, you can:</p> <ul style="list-style-type: none">• Enable or disable constant anti-virus protection.• Enable or disable web traffic scan.• Review information about the last scan and start express or full system scan, as well as scan only critical files and folders.• Review information about the last virus databases update and start an update manually if necessary.• View information on the current license and run License Manager if necessary.• Open the Threats or My Dr.Web section. |
| Threats | <p>Lets you access the list of the detected threats, select actions to apply to them and to open the contents of quarantine.</p> |
| My Dr.Web | <p>Lets you review Doctor Web news, the latest special deals, the information on viruses and open your personal page on the official Doctor Web website, where you can review the information on your license, virus databases and last update, renew the license, contact technical support, and so on.</p> |



Picture 1. Main application window

4.1. Starting and Quitting Dr.Web

To start Dr.Web

Do one of the following:

- In the Finder, open the Applications folder and double-click **Dr.Web for macOS**;
- Start the Launchpad and then select to start **Dr.Web for macOS**.

On the application start the update settings are checked and the updates are downloaded if necessary.



On the first start of the Dr.Web virus databases are updated to the most recent version for the moment of application start. This may take some time.

To quit Dr.Web

Do one of the following:

- Click the **Quit Dr.Web for macOS** item in the application menu (the menu bar is at the top of the main desktop).
- Click and hold the application icon in Dock, then select **Quit** in the menu.



- Press COMMAND-Q on the keyboard when Dr.Web is active.



When you quit Dr.Web, SpIDer Guard remains active. It is a resident anti-virus monitor which scans all files in real time when they are used.

4.2. Updating Virus Databases

Anti-virus solutions of Doctor Web use Dr.Web virus databases to detect malicious software. These databases contain details and signatures for all virus threats known at the moment of the product release. However, modern virus threats are characterized by high-speed evolution and modification. Within several days and sometimes hours, new viruses and malicious programs emerge. To mitigate the risk of infection during the licensed period, Doctor Web provides you with regular updates to virus databases and product components, which are distributed via the Internet. With the updates, Dr.Web receives information required to detect new viruses, block their spreading and sometimes cure infected files which were incurable before. From time to time, the updates also include enhancements to anti-virus algorithms and issues fixed in software and documentation.

Updating the components and virus databases of Dr.Web ensures that your Mac's protection is always up-to-date and ready for any new threat types. Updating is performed by a special component called Updater.

On the first start of Dr.Web it is necessary to update the virus databases to the most recent for the moment of the application start. Further updates will be performed periodically, with interval specified in preferences of Dr.Web.

Configuring the update interval

1. In the application menu, open **Preferences** and select the **Update** tab.
2. Select an interval for updating.

4.3. Constant Anti-virus Protection

Constant anti-virus protection is carried out via a resident component called SpIDer Guard. The component performs real-time scan of all files accessed by the user or running programs and processes running on your Mac. By default, it is enabled as soon as you install and activate Dr.Web license. Whenever a threat is detected, SpIDer Guard displays a warning and applies actions according to the anti-virus [preferences](#).



macOS blocks kernel (system) extension loading. For SpIDer Guard to operate correctly, allow the loading of system software from Doctor Web Ltd. in the Security & Privacy System Preferences pane.

The issue is relevant for macOS High Sierra 10.13 and later.

To enable or disable SpIDer Guard

- On the **Desk** section of the Dr.Web main window (see [Picture 1](#)), enable/disable the **SpIDer Guard** option.
- Click the Dr.Web icon in the menu bar and select the corresponding item.



Only users with administrator privileges can disable SpIDer Guard.

Be extremely cautious when using this option. While SpIDer Guard functions are disabled, avoid connecting to the Internet and scan all removable media using Scanner before accessing.

4.4. Scanning System on Demand

Dr.Web scans objects in the file system on your demand and detects various threats that may be present in the system though inactive. To protect your computer, it is necessary to run a system scan with Dr.Web periodically.

To run a quick scan of the most vulnerable parts of the system, select **Express scan**. To perform a full scan of the entire file system, select **Full scan**. You can also specify files and folders for scanning.



Process load increases during scanning which may lead to rapid discharge of batteries. We recommend starting scans when portable computers are powered by mains electricity.

To start system scanning



1. In the main window of Dr.Web select the scan mode:
 - **Express scan**—run a quick scan of the most vulnerable parts of the system only.
 - **Full scan**—perform a full scan of the entire file system.

You can press the [hot keys combinations](#) CONTROL-COMMAND-E and CONTROL-COMMAND-F on the keyboard to start express or full scan.

2. To scan only certain files and folders, drag them to the main application window or click the dotted area in the left part of the window to select objects to scan.

In the list of objects, select files and folders to scan:



- To add an object to the list, click  under the list of objects or simply drag this object to the list.
- To delete an object from the list, select it and click  or drag it outside the application window.

Click **Start Scanning** to start scanning the selected objects.

To start a file or a folder scan from the shortcut menu

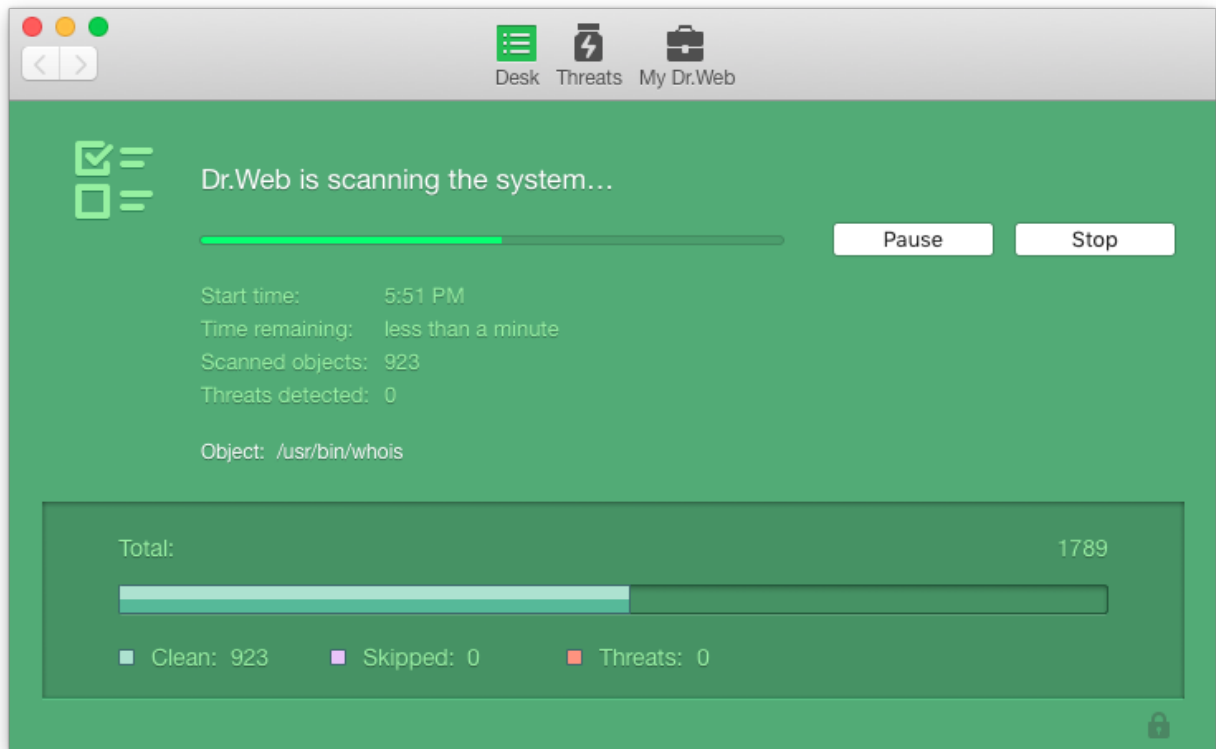
1. Select a file or folder icon on the Desktop or in the Finder.
2. Select **Scan with Dr.Web** in the shortcut menu.

When you start scanning, the main window switches to the results section (see the illustration below). During scanning, this section displays the following information:

- scanning start time;
- number of scanned objects;
- time left to end scanning;
- number of the detected threats;
- name of the file that is currently being scanned.

Statistic summary of the current scanning session is displayed in the bottom part of the window.

You can pause or stop scanning use the **Pause** and **Stop** buttons.



Picture 2. Viewing the scanning results



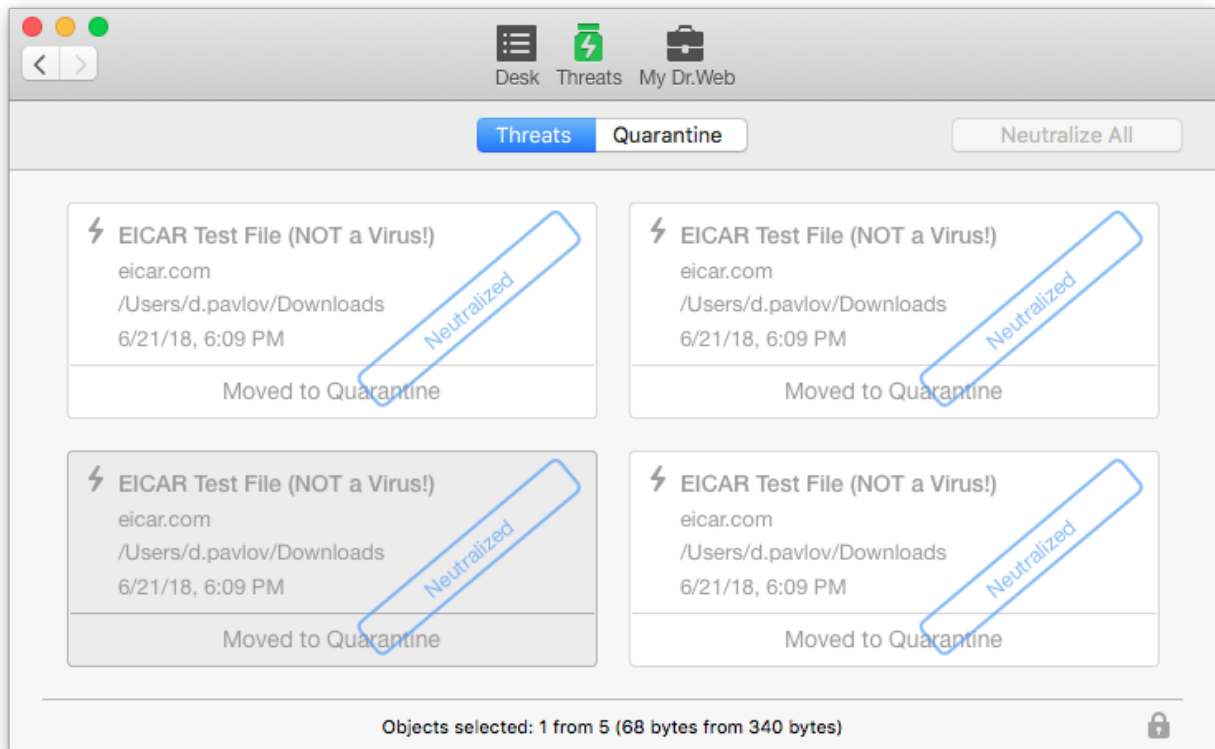
Some files may be omitted during scanning because they are corrupted or protected by password. If there are archives in the list of the skipped objects, try to extract them before scanning.

Dr.Web may require the [administrator privileges](#) to scan critical areas of the hard drive. To grant Dr.Web administrator privileges:

- Press the [combination](#) COMMAND-SHIFT-A on the keyboard, then enter the administrator password.
- Click the lock icon in the bottom of the window and then enter the administrator password.



4.5. Neutralizing Threats

To neutralize threats, you can specify the [automatic actions](#) or apply actions to the threats manually. To review the list of detected threats and apply actions to neutralize them, open the **Threats** tab on the main application window (see illustration below).



Picture 3. Threats tab

To view information on the threats

1. To view the list of the detected threats, open the **Threats** section. In the status bar in the bottom of the window, the total number and size of the detected threats and also the number and size of the selected threats are displayed.
2. To view the information in a threat, click the  button or double-click the threat.
3. To read about the type of the threat on Doctor Web website, click  button to the left of the threat name on the details window.

To neutralize detected threats

1. Open the **Threats** section.
2. To apply an action specified in the application [preferences](#) for the corresponding threat type, click the button with this action under the threat. To select an alternative action, click the arrow on the button with recommended action on the details window.
3. To neutralize several threats, select them holding the SHIFT key, then select the action to perform in the **Actions** section of the application menu or in the threat list shortcut menu.
4. To neutralize all threats, click **Neutralize All**. This will apply actions specified in the application [preferences](#) for the corresponding threat types.

You can also use the [hot keys combinations](#) on the keyboard to apply actions to the threats.



4.6. HTTP Traffic Scan And Access Control to Web Resources

Web traffic scan is carried out via a resident component called SpIDer Gate. It scans the incoming HTTP traffic and blocks all objects that contain security threats. HTTP is used by web browsers, download managers and other apps which exchange data with web servers, that is, which work with the Internet.

SpIDer Gate also allows you to control access to web resources and to prevent users from viewing undesirable websites (for example, pages on violence, gambling, adult content, and so on).

By default, SpIDer Gate is enabled automatically after you install and activate Dr.Web license.



Other apps for scanning web traffic and controlling access to web resources installed on your Mac may not work properly if SpIDer Gate is enabled.



macOS blocks kernel (system) extension loading. For SpIDer Gate to operate correctly, allow the loading of system software from Doctor Web Ltd. in the Security & Privacy System Preferences pane.

The issue is relevant for macOS High Sierra 10.13 and later.

To enable or disable SpIDer Gate

- On the **Desk** section of the main window (see [Picture 1](#)), enable/disable the **SpIDer Gate** option.
- Click the Dr.Web icon in the menu bar and select the corresponding item.



Only users with administrator privileges can disable SpIDer Gate.

Configuring HTTP traffic scan

By default, SpIDer Gate blocks all incoming malicious objects. You can select the types of malicious programs to block, configure actions for the not scanned objects and set up the maximum time for scanning one file by performing the following actions:

1. In the application menu, open **Preferences** and select the **SpIDer Gate** tab. Only users with administrator privileges can change SpIDer Gate settings. Click the icon of a lock at the bottom of the window and enter the administrator name and password, if necessary.
2. Click **Advanced**.
3. Select the malware types to block.



4. Specify the maximum time for scanning one file. Please note, that increasing the time for scanning a single file may slow down your Mac in some cases.
5. By default, the objects that cannot be scanned are blocked. To allow such objects, deselect the **Block not scanned content** check box.
6. Click **OK** to save changes.

Configuring access to websites

By default, in addition to HTTP traffic anti-virus scan, SpIDer Gate blocks URLs listed due to a notice from copyright owner and non-recommended sites. You can disable these functions on the **SpIDer Gate** tab of Dr.Web preferences. You can also select the website categories to block access to and create black and white lists of websites to automatically allow or block access to them regardless of other SpIDer Gate settings.




The default SpIDer Gate settings are optimal for most uses. Do not change them unnecessarily.

To select the categories of websites


1. In the application menu, open **Preferences** and select the **SpIDer Gate** tab. Only users with administrator privileges can change SpIDer Gate settings. Click the icon of a lock at the bottom of the window and enter the administrator name and password if necessary.
2. Select the categories of websites you want to block access to.

To create black and white lists of web addresses

1. In the application menu, open **Preferences** and select the **Exclusions** tab.
2. Click the **Websites** button. Only users with administrator privileges can change black and white lists. Click the icon of a lock at the bottom of the window and enter the administrator name and password, if necessary.
3. By default, both lists are empty. You can add addresses to the black and white lists. Click  under the corresponding list and enter a domain name or a part of a domain name for the website that you want block or allow access to:
 - To add a certain website, enter its name (for example, **www.example.com**). This allows access to all webpages located on this website.
 - To allow access to websites with similar names, enter the common part of their domain names. For example, if you enter **example**, then SpIDer Gate will allow access to the **example.com**, **example.test.com**, **test.com/example**, **test.example222.com** and other similar websites.
 - To allow access to websites within a particular domain, enter the domain name with a period ('.'). This allows access to all webpages located on this website. If the domain name includes a forward slash ('/'), the substring before the slash is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter **example.com/test**, SpIDer Gate will al-



low access to webpages such as **example.com/test11**, **template.example.com/test22**, and so on.

To delete websites from black or white list, select them in the corresponding list and click  or drag them outside the application window.

4. Click **OK** to save changes.

Safe search

To enable the safe search function in search engines automatically:

1. In the application menu, open **Preferences** and select the **SpIDer Gate** tab.
2. Select the corresponding check box in the **Safe search** section.

4.7. Getting Help

To get help about the app you can use **Dr.Web for macOS Help** which can be accessed via the Apple Help viewer.

To access **Dr.Web for macOS Help**, in the menu bar, click **Help** and select **Dr.Web for macOS Help**, or search for keywords using the text box.

If you cannot find a solution for your problem or necessary information about Dr.Web, you can request direct assistance from [technical support](#).



5. Advanced Use

This chapter contains information on performing more advanced tasks with Dr.Web and adjusting its settings.

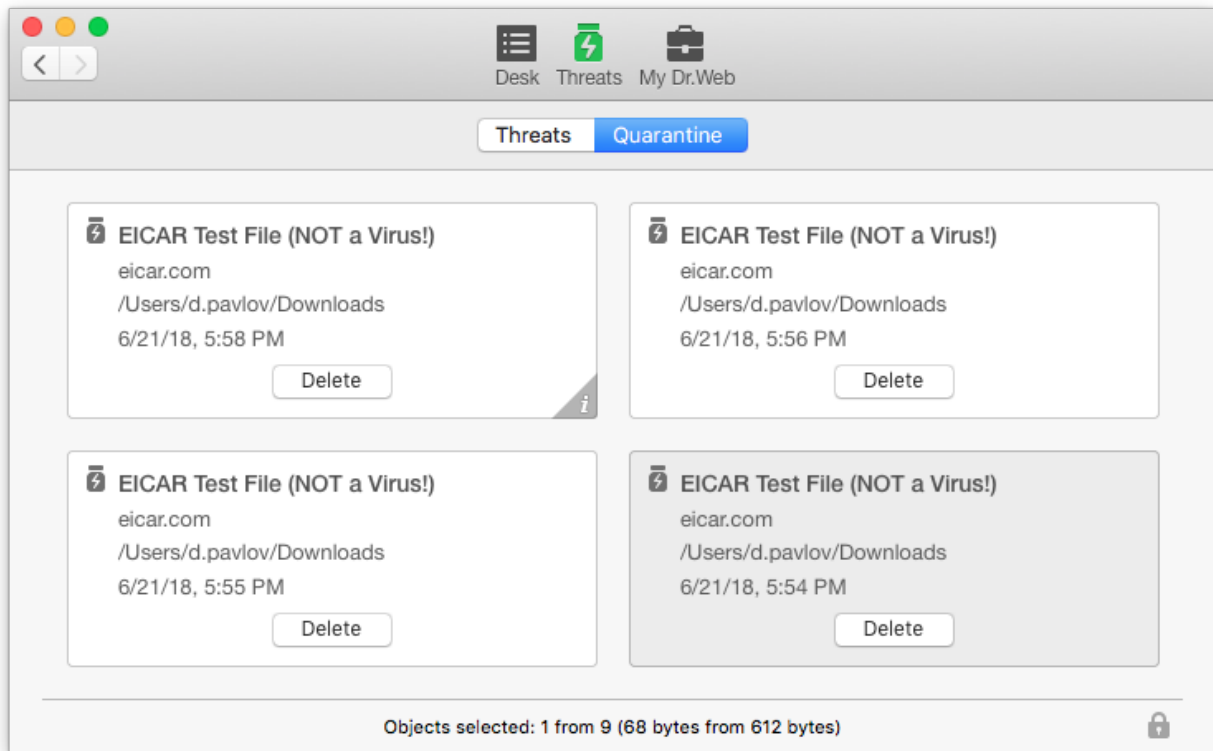
5.1. Quarantine

Quarantine allows you to isolate detected malicious or suspicious objects that cannot be cured from the rest of the system in case you need them. Curing algorithms are being constantly improved, therefore these objects may become curable after one of the updates.





Due to the privacy reasons, the quarantine folder is created for each user in the system. Therefore, if you switched to the administrator mode, the detected threats which are moved to the administrator quarantine and will not be available in the user quarantine folders.

You can view and manage the contents of quarantine using the **Quarantine** tab on the **Threats** section of the main window (see illustration below). In the status bar in the bottom of the window the total number and size of the threats and also the number and size of the selected threats are displayed.



Picture 4. Objects in quarantine

To view information on the objects in quarantine

1. Click  button or double-click the object.
2. To read about the type of the threat that the object is supposed to contain on Doctor Web website, click  button to the left of the threat name on the details window. This will open the page with information on this type of threats on Doctor Web website.

To process objects in quarantine

1. To apply a recommended action to an object in quarantine, click the button with this action under the object. To select an alternative action, click the arrow on the button with recommended action on the details window. You can select one of the following actions:
 - **Delete**—to completely remove the object from the file system.
 - **Restore**—to return the object from the quarantine to the initial folder it has been moved from.
 - **Restore To**—to select the folder to move the object from quarantine.
2. To process several objects, select them holding the SHIFT key, then select the action to perform in the **Actions** section of the application menu or in the object list shortcut menu.

You can also use the [hot keys combinations](#) on the keyboard to apply actions to the objects in quarantine.



5.2. Configuring Automatic Actions

You can specify actions that will be applied automatically by Dr.Web to various types of computer threats unless it is required to choose an action manually. You can set different automatic reaction for Scanner and SpIDer Guard.

To configure automatic actions

1. To open the automatic actions settings for Dr.Web components, do one of the following:
 - To configure automatic actions for Scanner, in the application menu, open **Preferences** and select the **Scanner** tab.
 - To configure automatic actions for SpIDer Guard, in the application menu, open **Preferences** and select the **SpIDer Guard** tab.
2. Select necessary action for infected and suspicious objects.
3. Click **Other** to select actions for malware (adware, dialers, jokes, riskware and hacktools).
4. The actions specified in the SpIDer Guard settings will be applied automatically every time a threat is detected by this components. To apply action automatically to the threats detected during the system scan performed by Scanner, select the **Apply actions automatically** check box in the Scanner settings section.
5. Click **Advanced** to set up the scan of the complex objects (archives and email files) and specify the maximum time for scanning a single file. Please note that scanning the contents of archives and email files, as well as increasing the time for scanning a single file leads to increasing of the overall scanning time and may slow down your Mac in some cases.



The default automatic actions are optimal for most uses. Do not change them unnecessarily.

By default, all SpIDer Guard settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, select the **SpIDer Guard** section of the application preferences, click the icon of a lock at the bottom of the window and enter the administrator name and password.

5.3. Excluding Objects from Scanning




If necessary, you can exclude from scanning the following objects:

- files and folders;
- websites;
- applications.

To configure exclusions

1. In the application menu, open **Preferences** and select the **Exclusions** tab.



2. To configure the exclusions of files and folders, websites or apps, click the corresponding button. By default, the exclusion settings are locked. To unlock these settings, click the icon of a lock at the bottom of the preferences window and enter the administrator name and password.
3. If necessary, modify the list of exclusions:
 - To add a file, folder or application to the list, click the  button and select the object.
 - To add a website to the list, click the  button under the white list and enter a domain name or a part of a domain name for the website.
 - To delete an object from the exclusions list, select it and click  or drag it outside the application window.



The default exclusions settings are optimal for most uses. Do not change them unnecessarily.

By default, all quarantine folders are excluded from scans, because they are used to isolate detected threats and, as access to them is blocked, there is no use scanning these folders.

5.4. Scan Encrypted Traffic

By default, Dr.Web does not scan the data transmitted in accordance with SSL protocol.

To scan the encrypted traffic

1. In the application menu, open **Preferences** and select the **Network** tab.
2. If the settings are locked, click the icon of a lock at the bottom of the window and enter the administrator name and password.
3. Select the **Scan encrypted traffic** check box.

To obtain Doctor Web Certificate

If the encrypted traffic scan is enabled, some browsers and mail clients which send and receive this traffic and do not refer to the system certificate storage, may need Doctor Web certificate to operate.

1. In the application menu, open **Preferences** and select the **Network** tab.
2. Press the **Export** button and save the certificate to a convenient folder.

5.5. Notifications

The notifications about various events that may occur during operation of the app are configured on the **Main** tab of Dr.Web preferences.



Types of notifications

- On-screen messages
- Sound alerts

To configure sound notifications

Sound alerts are enabled by default. To disable or enable sound alerts, deselect or select the **Use sound alerts** check box on the **Main** tab of the application preferences.

To configure on-screen notifications

1. On-screen notifications are enabled by default. To disable or re-enable on-screen notifications, deselect or select the **Enable notifications** check box on the **Main** tab of the application preferences.
2. Select the notification system:
 - **Dr.Web** (selected by default);
 - **System** (macOS standard notifications);
 - **Growl**.
3. For Dr.Web notifications, you can configure additional parameters by clicking **Configure** to the right of the selected notification system:
 - Specify the notifications appearing time
 - Select the area on the screen to show notifications

Click **OK** to apply settings.

5.6. Administrator Privileges

Dr.Web may require administrator privileges to access and scan critical areas of the hard drive. To start scanning with administrator privileges:

1. In the application menu, open **Preferences** and select the **Main** tab.
2. Select the **Start scanning with administrative privileges** check box. You will need to enter the administrator password before scanning (express, full or custom) starts.

5.7. Optimizing Battery Use

By default, when your Mac is operating under battery power, the scanning is paused to prevent the battery from quick draining. Dr.Web displays a corresponding message where you can confirm pausing or continue scanning. To disable scanning pausing:

1. In the application menu, open **Preferences** and select the **Main** tab.
2. If you do not want to pause scanning when you Mac is on battery power, deselect the **Pause scanning while on battery power** check box.



5.8. Dr.Web Cloud

Dr.Web Cloud services provide most recent information on threats which is updated on Doctor Web servers in real-time mode and used for anti-virus protection. Depending on [update settings](#), information on threats used by anti-virus components may become out of date. Cloud services can reliably prevent users from viewing unwanted websites.

To connect to the services

1. In the application menu, open **Preferences** and select the **Dr.Web Cloud** tab.
2. To connect to cloud services, select **I want to connect to services (recommended)**.

5.9. Operation Mode

If necessary, you can use Dr.Web installed on your Mac to connect to corporate anti-virus networks or to access Dr.Web AV-Desk anti-virus service of your IT provider. To operate in such central protection mode, you do not need to install additional software or uninstall Dr.Web.

In the central protection mode, virus databases updates are downloaded automatically from the central protection server. If on the central protection server mobile mode is enabled, the updates will be downloaded via the Internet from Dr.Web update servers in case the connection to the server is lost and virus databases are out-of-date. When the connection is restored, Dr.Web automatically starts downloading the updates from the central protection server.

Some features and settings of Dr.Web, particularly concerning the constant protection and on-demand scanning, may be modified and blocked for compliance with the company security policy or according to the list of purchased services. A [license key file](#) for operation in this mode is received from central protection server. Your personal license is not used.



By default, Dr.Web mode settings are locked in order to prevent anyone without administrative privileges from changing these settings. To unlock them, click the icon of a lock at the bottom of the mode preferences window and enter the administrator name and password.

To use central protection mode

1. Contact an anti-virus network administrator of your company or IT provider for a license and parameters of connection to the central protection server.
2. In the application menu, open **Preferences** and select the **Mode** tab.
3. To connect to the central protection server of your company or IT provider, select the **Enable central protection mode** check box.



In the central protection mode the scanning of your computer can be launched manually or according to schedule directly from the server.

4. On switching to the central protection mode Dr.Web restores parameters of the previous connection. If you are connecting to the server for the first time or connection parameters have been changed, do the following:



The `install.cfg` file provided by administrator of anti-virus network contains settings to connect to the central protection server. To use this file:

1. Click **Other activation types** in the [License Manager](#).
2. Drag the configuration file to the opened window or click the dotted area to select the file.

If the file is mounted, fields for entering the connection settings will be specified automatically.

- Enter the IP address of the central protection server provided by administrator of anti-virus network.
- Enter the port number that is used to connect to the server.
- Drag the license key file received from the central protection server to the settings window or double-click the license key area and browse the file.
- As an option, enter the authentication parameters: station ID which is assigned to your computer for registration at the server and password. The entered values are saved with Key-chain system. Therefore, you need not enter them again when reconnecting to the server.
- Click **Connect** to access central protection server with specified parameters.



Depending on the authorization settings of the central protection server, the station can be connected to the server in one of the following modes:

- As a newbie. In this case it may require to be approved on the server (ID and password will be assigned automatically) or it may be authorized automatically if the corresponding authorization mode is specified on the server.
- If the station has already been created on the server and it has an ID and password, it will be authorized automatically when connecting to the server regardless of its settings.

For detailed information on connecting a station to the server refer to Dr.Web Control Center and Dr.Web AV-Desk Administrator manuals.

To use standalone mode

1. In the application menu, open **Preferences** and select the **Mode** tab.
2. To switch to the standalone mode, deselect the **Enable central protection mode** check box.

On switching to this mode, all settings of the app are unlocked and restored to their previous or default values. You can once again access all features of the app.



3. For correct operation in standalone mode, Dr.Web requires a valid personal [license key file](#). The license received from the central protection server cannot be used in this mode. If necessary, you can receive or update a personal license with [License Manager](#).

5.10. Restoring Default Settings

If you experience any difficulties with configuring Dr.Web, you can restore the default application settings.



By default, the restoring defaults option is locked in order to prevent anyone without administrator privileges from changing it. To unlock it, click the icon of a lock at the bottom of the window and enter the administrator password.

1. In the application menu, open **Preferences** and select the **Main** tab.
2. Click **Restore Defaults**. Confirm restoring the default application configuration by clicking **Restore** in the corresponding dialog.



6. Appendices

6.1. Appendix A. Types of Computer Threats

Herein, the term “threat” defines any kind of software that can potentially or directly inflict damage on a computer or network or compromise the user's information or rights (in other words, malicious and other unwanted programs). However, generally speaking, the term “threat” may be used to indicate any potential danger to computer or network security (that is, vulnerabilities that can be exploited to launch attacks).

All program types described below have the ability to endanger the user's data or confidentiality. Programs that do not hide their presence from the user (for example, spam-sending software or traffic analyzers) usually are not considered to be computer threats, although they can become threats under certain circumstances.

In the documentation and products by Doctor Web, threats are divided into two categories in accordance with the severity of danger they pose:

- **Major threats** are classic computer threats that can perform destructive or illegal actions in the system on their own (erase or steal important data, crash networks, and so on). To this type of computer threats belong programs that are traditionally referred to as “malicious” (viruses, worms, and Trojans).
- **Minor threats** are less dangerous than major threats, but may be used by a third party to carry out malicious activities. Moreover, mere presence of minor threats in the system indicates its low protection level. Information security specialists sometimes refer to this type of threats as “grayware” or potentially unwanted programs. This category consists of adware, dialers, jokes, riskware, and hacktools.

Major threats

Computer viruses

This type of computer threats is characterized by their ability to inject malicious code into running processes of other programs. This action is called *infection*. In most cases, the infected file becomes a virus carrier itself, and the injected code does not necessarily match the original one. The majority of viruses are created with a purpose to damage or destroy data in the system.

Doctor Web divides viruses by the type of objects they infect into the following categories:

- **File viruses** infect operating system files (usually, executable files and dynamic-link libraries) and are activated when an infected file is run.
- **Micro viruses** infect documents used by Microsoft® Office or other programs supporting macro commands (usually, written in Visual Basic). Macro commands are a type of built-in programs (macros) that are written in a fully functional programming language and can be



launched under specific circumstances (for example, in Microsoft® Word, macros can be activated upon opening, closing, or saving a document).

- **Script viruses** are created using script languages, and, mostly, they infect other scripts (such as OS service files). By exploiting vulnerable scripts in web applications, they can also infect other file types that support script execution.
- **Boot viruses** infect boot sectors of disks and partitions or master boot records of hard disks. They require little memory and can perform their tasks until the operating system is rolled out, restarted, or shut down.

Most viruses have special mechanisms that protect them against detection. These mechanisms are constantly improved, and ways to overcome them are constantly developed. According to the type of protection they use, all viruses can be divided into two following groups:

- **Encrypted viruses** self-encrypt their malicious code upon every infection to make its detection in a file, boot sector, or memory more difficult. Each sample of such viruses contains only a short common code fragment (decryption procedure) that can be used as a virus signature.
- **Polymorphic viruses** use a special decryption procedure in addition to code encryption. This procedure is different in every new virus copy. This means that such viruses do not have byte signatures.

Viruses can also be classified according to the language they are written in (most viruses are written in Assembly, high-level programming languages, script languages, and so on) and operating systems that can be infected by these viruses.

Computer worms

Recently, worms have become much more widespread than viruses and other malicious programs. Like viruses, these malicious programs can replicate themselves. A worm infiltrates a computer from a network (usually, as an email attachment) and spreads its functional copies among other computers. Distribution can be triggered by some user action or automatically.

Worms do not necessarily consist of only one file (the worm's body). Many of them have a so-called infectious part (shellcode) that is loaded into the main memory. After that, it downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be easily removed by restarting the system (at that, RAM is reset). However, if the worm's body infiltrates the computer, only an anti-virus program can fight it.

Even if worms do not bear any payload (do not cause direct damage to a system), they can still cripple entire networks because of how intensely they spread.

Doctor Web classifies worms in accordance with their distribution methods as follows:

- **Network worms** spread via various network and file-sharing protocols.
- **Mail worms** spread via mail protocols (POP3, SMTP, and others).



Trojan programs (Trojans)

These programs cannot replicate themselves. However, they can perform malicious actions on their own (damage or delete data, forward confidential information, and others) or provide cybercriminals with authorized access to a computer to harm a third party.

Like viruses, these programs can perform various malicious activities, hide their presence from the user, and even be a virus component. However, usually, Trojans are distributed as separate executable files (through file-exchange servers, data carriers, or email attachments) that are run by users themselves or by some specific system process.

Here are some Trojan types divided by Doctor Web into separate categories as follows:

- **Backdoors** are Trojans that allow an intruder to get privileged access to the system bypassing any existing protection mechanisms. Backdoors do not infect files—they register themselves in the registry modifying registry keys.
- **Droppers** are file carriers that contain malicious programs in their bodies. Once launched, a dropper copies malicious files to a hard disk without user consent and runs them.
- **Keyloggers** can log data that users enter by means of a keyboard. These malicious programs can steal various confidential information (including network passwords, logins, bank card data, and so on).
- **Clickers** redirect users to specified Internet resources (may be malicious) in order to increase traffic to those websites or to perform DDoS attacks.
- **Proxy Trojans** provide cybercriminals with anonymous Internet access via the victim's computer.
- **Rootkits** are used to intercept operating system functions in order to hide their presence. Moreover, a rootkit can conceal processes of other programs, registry keys, folders, and files. It can be distributed either as an independent program or as a component of another malicious application. Based on the operation mode, rootkits can be divided into two following categories: User Mode Rootkits (UMR) that operate in user mode (intercept functions of user-mode libraries) and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions at the system kernel level, which makes these malicious programs hard to detect).

Trojans can also perform other malicious actions besides those listed above. For example, they can change the browser home page or delete certain files. However, such actions can also be performed by threats of other types (viruses or worms).

Minor threats

Hacktools

Hacktools are designed to assist intruders with hacking. The most common among these programs are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Such tools can be used not only by hackers but also by administrators



to check security of their networks. Sometimes various programs that use social engineering techniques are designated as hacktools too.

Adware

Usually, this term refers to a program code incorporated into freeware programs that forcefully display advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements, for example, in web browsers. Many adware programs operate based on data collected by spyware.

Jokes

Like adware, this type of minor threats cannot be used to inflict any direct damage on the system. Joke programs usually just generate messages about allegedly detected errors and threaten to perform actions that may lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that, after asking for user's permission, employ Internet connection to access specific websites. Usually, these programs have a signed certificate and inform the user about all their actions.

Riskware

These programs are not intended to be computer threats. However, they can still cripple system security due to certain features and, therefore, are classified as minor threats. This type of threats includes not only programs that can accidentally damage or delete data but also programs that can be used by hackers or some malicious applications to harm the system. Among such programs are various remote chat and administrative tools, FTP-servers, and so on.

Suspicious objects

These are potential computer threats detected by the heuristic analyzer. Such objects can be any type of threat (even unknown to information security specialists) or turn out safe in case of a false detection. It is strongly recommended to move files containing suspicious objects to quarantine and send them for analysis to Doctor Web anti-virus laboratory.

6.2. Appendix B. Fighting Computer Threats

Doctor Web anti-virus solutions use several malicious software detection methods simultaneously, which allows them to perform thorough checks on suspicious files and control software behavior.



Detection Methods

Signature analysis

The scans begin with signature analysis that is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing™

On completion of signature analysis, Dr.Web anti-virus solutions use the unique Origins Tracing method to detect new and modified viruses that use the known infection mechanisms. Thus, Dr.Web users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the Origins Tracing mechanism allows to considerably reduce the number of false triggering of the heuristic analyzer. Objects detected using the Origins Tracing algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator*—a programming model of the processor and runtime environment. The emulator operates with protected memory area (*emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristic analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) that might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristic analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristic analyzer also uses the FLY-CODE™ technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of mali-



cious objects in files compressed not only by packagers Dr.Web is aware of, but also by new, previously unexplored programs. While checking packed objects, Dr.Web anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristic analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristic analyzer are treated as "suspicious".

While performing any of the above mentioned checks, Dr.Web anti-virus solutions use the most recent information about known malicious software. As soon as experts of Doctor Web virus laboratory discover new threats, the update for virus signatures, behavior characteristics, and attributes is issued. In some cases, updates can be issued several times per hour. Therefore, even if a brand new virus passes through Dr.Web resident guards and penetrates the system, after an update it is detected on the list of processes and neutralized.

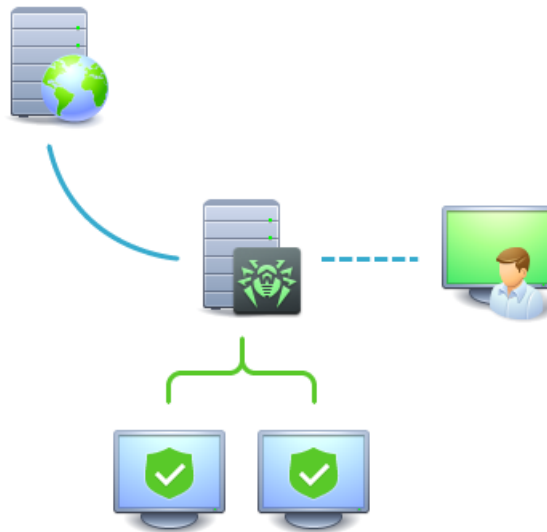
6.3. Appendix C. Central Anti-virus Protection








Solutions for central protection from Doctor Web help automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one anti-virus network which security is monitored and managed from central server by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

Solutions for central protection from Doctor Web use client-server model (see picture below).

Workstations and servers are protected by *local anti-virus components* (agents, or clients; herein, Dr.Web) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.



| | | | |
|---|----------------------------------|---|-------------------------------|
|  | Central protection server |  | Network based on TCP, NetBIOS |
|  | Anti-virus network administrator |  | Management via HTTP/HTTPS |
|  | Protected local computer |  | Transmitting updates via HTTP |
|  | Doctor Web update server | | |

Picture 5. Logical structure of anti-virus networks

Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from Dr.Web update servers.

Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.



Local anti-virus components are not compatible with other anti-virus software including versions of Dr.Web anti-virus solutions that do not support operation in central protection mode (i.e. Dr.Web version 5.0). Installing two anti-virus apps on one computer may lead to system crash and loss of important data.

Central Protection Solutions

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite is a complex solution for corporate networks of any size that provides reliable protection of workstations, mail and file servers from all types of modern computer threats. This solution also provides diverse tools for anti-virus network administrators that allow them to keep track and manage operation of local anti-virus components including components deployment and update, network status monitoring, statistics gathering, and notification on virus events.

Dr.Web AV-Desk Internet Service

Dr.Web AV-Desk is an innovative Internet service created by Doctor Web for providers of various types of Internet services. With this solution, providers can deliver information security services to home customers and companies providing them with a selected package of services for protection from viruses, spam and other types of computer threats for as long as is necessary. Services are provided online.

For more information on Dr.Web AV-Desk Internet service, visit the official Doctor Web website at <https://www.av-desk.com/>.

6.4. Appendix D. Hot Keys

You can use the special hot keys combinations to start a system scan, to apply action to the detected threats or to set up Dr.Web.

| Combination | | Description |
|--------------|-------------------|------------------------|
| Scan menu | CONTROL-COMMAND-E | Express scan |
| | CONTROL-COMMAND-F | Full scan |
| | CONTROL-COMMAND-C | Select objects to scan |
| Actions menu | COMMAND-SHIFT-C | Cure |
| | COMMAND-SHIFT-M | Move to quarantine |



| Combination | | Description |
|----------------|-----------------|------------------------------------|
| | COMMAND-SHIFT-I | Ignore |
| | COMMAND-SHIFT-D | Delete |
| | COMMAND-SHIFT-R | Restore |
| | COMMAND-SHIFT-P | Restore to |
| | COMMAND-SHIFT-A | Work with administrator privileges |
| General | COMMAND-, | Preferences |
| | COMMAND-A | Select all |
| | COMMAND-W | Close |

6.5. Appendix E. Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Download and review the latest manuals and guides at <https://download.drweb.com/doc/>.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at <https://forum.drweb.com/>.

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

- Fill in the web form in the corresponding section at <https://support.drweb.com/>.
- Call by phone in Moscow: +7 (495) 789-45-86.

Refer to the official website at <https://company.drweb.com/contacts/offices/> for regional and international office information of Doctor Web company.

