CYBER SECURITY PRO

for macOS

User Guide

(intended for product version 6.0 and higher)

Click here to download the most recent version of this document

Customer Care: www.eset.com/support

REV. 10. 1. 2017

Contents

1. ESET Cyber Security Pro

ESET Cyber Security Pro represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine, combined with Email client protection, Firewall and Parental control, utilizes speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert defending your computer against attacks and malicious software.

ESET Cyber Security Pro is a complete security solution produced from our long-term effort to combine maximum protection and a minimal system footprint. Based on artificial intelligence, the advanced technologies that comprise ESET Cyber Security Pro are capable of proactively eliminating infiltration by viruses, worms, trojan horses, spyware, adware, rootkits and other Internet-borne attacks without hindering system performance.

1.1 What's new in version 6

ESET Cyber Security Pro version 6 introduces the following updates and improvements:

- **Anti-Phishing** – prevents fake websites disguised as trustworthy ones from acquiring your personal information
- **System updates** – ESET Cyber Security Pro version 6 features various fixes and improvements including notifications for operating system updates. To learn more about this, see the System updates 15 section.
- **Protection statuses** – hides notifications from the Protection Status screen (E.g. *Email protection disabled* or *Computer restart required*)
- **Media to scan** – certain types of media can be excluded from the Real-time scanner (Local drives, Removable media, Network media)

1.2 System requirements

For optimal performance with ESET Cyber Security Pro, your system should meet or exceed the following hardware and software requirements:

	System requirements
Processor architecture	Intel 32-bit, 64-bit
Operating system	macOS 10.6 or later
Memory	300 MB
Free disk space	200 MB

2. Installation

Before you begin the installation process, please close all open programs on your computer. ESET Cyber Security Pro contains components that may conflict with other antivirus programs that may already be installed on your computer. ESET strongly recommends that you remove any other antivirus programs to prevent potential problems.

To launch the installation wizard, do one of the following:

- If you are installing from the installation CD/DVD, insert it into your computer, open it from your Desktop or **Finder** window and double-click the **Install** icon
- If you are installing from a file downloaded from the ESET website, open the file and double-click the **Install** icon

The installation wizard will guide you through basic setup. During the initial phase of installation, the installer will automatically check online for the latest product version. If a newer version is found, you will be given the option to download the latest version before continuing the installation process.

After agreeing to the End User License Agreement, you will be asked to select one of the following installation modes:

- Typical installation 4
- Custom installation 5

2.1 Typical installation

Typical installation mode includes configuration options that are appropriate for most users. These settings provide maximum security combined with excellent system performance. Typical installation is the default option and is recommended if you do not have particular requirements for specific settings.

ESET Live Grid
The Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed, processed and added to the virus signature database. **Enable ESET Live Grid (recommended)** is selected by default. Click **Setup...** to modify detailed settings for the submission of suspicious files. For more information see Live Grid 18.

Potentially Unwanted Applications
The last step of the installation process is to configure detection of **Potentially unwanted applications**. Such programs are not necessarily malicious, but can often negatively affect the behavior of your operating system. These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.

After installing ESET Cyber Security Pro, you should perform a computer scan for malicious code. From the main program

window click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see the section On-demand computer scan 8.

2.2 Custom installation

Custom installation mode is designed for experienced users who want to modify advanced settings during the installation process.

Proxy Server
If you are using a proxy server, you can define its parameters by selecting **I use a proxy server**. In the next window, enter the IP address or URL of your proxy server in the **Address** field. In the Port field, specify the port where the proxy server accepts connections (3128 by default). In the event that the proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. If you do not use a proxy server, select **I do not use a proxy server**. If you are not sure whether you use a proxy server or not, you can use your current system settings by selecting **Use system settings (recommended)**.

Privileges
In the next step you can define privileged users or groups who will be able to edit the program configuration. From the list of users on the left, select the users and **Add** them to the **Privileged Users** list. To display all system users, select **Show all users**. If you leave the Privileged Users list empty, all users are considered privileged.

ESET Live Grid
The Live Grid Early Warning System helps ensure that ESET is immediately and continuously informed of new infiltrations in order to quickly protect our customers. The system allows new threats to be submitted to the ESET Threat Lab, where they are analyzed, processed and added to the virus signature database. **Enable ESET Live Grid (recommended)** is selected by default. Click **Setup...** to modify detailed settings for the submission of suspicious files. For more information see Live Grid 18.

Potentially Unwanted Applications
The next step of the installation process is to configure detection of **Potentially unwanted applications**. Such programs are not necessarily malicious, but can often negatively affect the behavior of your operating system. These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.

Firewall
In the last step, you can select a Firewall filtering mode. For more information see Filtering modes 12.

After installing ESET Cyber Security Pro, you should perform a computer scan for malicious code. From the main program window click **Computer scan** and then click **Smart scan**. For more information about On-demand computer scans, see the section On-demand computer scan 8.

3. Product activation

After installation, the Product Activation window is displayed automatically. To access the product activation dialog at any time, click the ESET Cyber Security Pro icon located in the macOS Menu Bar (top of the screen) and then click **Product activation...**.

- **License Key** – a unique string in the format XXXX-XXXX-XXXX-XXXX-XXXX or XXXX-XXXXXXXX which is used for identification of the license owner and for activation of the license. If you purchased a retail boxed version of the product, activate your product using a License Key. It is usually located inside or on the back side of the product package.
- **Username and Password** – if you have a Username and Password and do not know how to activate ESET Cyber Security Pro, click **I have a Username and Password, what do I do?**. You will be redirected to my.eset.com where you can convert your credentials into a License Key.
- **Free BETA test** – select this option if you want to evaluate ESET Cyber Security Pro before making a purchase. Fill in your email address to activate ESET Cyber Security Pro for a limited time. Your test license will be emailed to you. Trial licenses can only be activated once per customer.
- **Purchase license** – if you do not have a license and would like to buy one, click Purchase license. This will redirect you to the website of your local ESET distributor.
- **Activate later** – click this option if you do not want to activate at this time.

4. Uninstallation

To uninstall ESET Cyber Security Pro, do one of the following:

- insert the ESET Cyber Security Pro installation CD/DVD into your computer, open it from your desktop or **Finder** window and double-click **Uninstall**
- open the ESET Cyber Security Pro installation file (*.dmg*) and double-click **Uninstall**
- launch **Finder**, open the **Applications** folder on your hard drive, CTRL+click the **ESET Cyber Security Pro** icon and select **Show Package Contents**. Open the **Contents** > **Helpers** folder and double-click the **Uninstaller** icon.

5. Basic overview

The main program window of ESET Cyber Security Pro is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.

The following sections are accessible from the main menu:

- **Home** – provides information about the protection status of your Computer, Firewall, Web and Mail protection and Parental control.
- **Computer scan** – this section allows you to configure and launch the On-demand computer scan 8.
- **Update** – displays information about updates of the virus signature database.
- **Setup** – select this section to adjust your computer's security level.

- **Tools** – provides access to Log files 16, Scheduler 16, Quarantine 17, Running processes 18 and other program features.
- **Help** – displays access to help files, Internet Knowledgebase, support request form and additional program information.

5.1 Keyboard shortcuts

Keyboard shortcuts that can be used when working with ESET Cyber Security Pro:

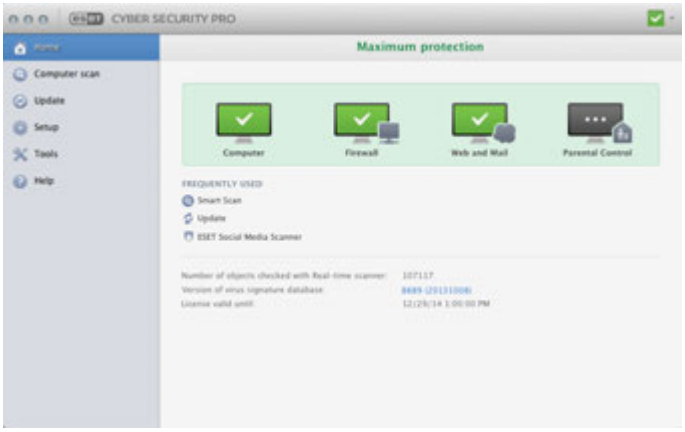
- *cmd+,* – displays ESET Cyber Security Pro preferences,
- *cmd+O* – resizes the ESET Cyber Security Pro main GUI window to the default size and moves it to the center of the screen,
- *cmd+Q* – hides the ESET Cyber Security Pro main GUI window. You can open it by clicking the ESET Cyber Security Pro icon in the macOS Menu Bar (top of the screen),
- *cmd+W* – closes the ESET Cyber Security Pro main GUI window.

The following keyboard shortcuts work only if **Use standard menu** is enabled under **Setup** > **Enter application preferences ...** > **Interface**:

- *cmd+alt+L* – opens the **Log files** section,
- *cmd+alt+S* – opens the **Scheduler** section,
- *cmd+alt+Q* – opens the **Quarantine** section.

5.2 Checking protection status

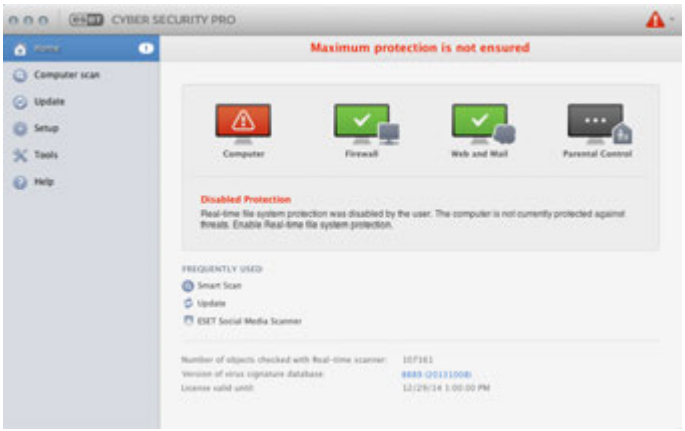
To view your protection status click **Home** from the main menu. A status summary about the operation of ESET Cyber Security Pro modules will be displayed in the primary window.



5.3 What to do if the program does not work properly

When a module is functioning properly, a green icon is displayed. When a module is not functioning properly, a red exclamation point or an orange notification icon is displayed. Additional information about the module and a suggested solution for fixing the issue is shown. To change the status of individual modules, click the blue link below each notification message.

If you are unable to solve a problem using the suggested solutions, you can search the ESET Knowledgebase for a solution or contact ESET Customer Care. Customer Care will respond quickly to your questions and help resolve any issues with ESET Cyber Security Pro.



6. Computer protection

Computer configuration can be found in **Setup** > **Computer**. It shows the status of **Real-time file system protection** and **Removable media blocking**. To turn off individual modules, switch the desired module's button to **DISABLED**. Note that this may decrease the level of protection of your computer. To access detailed settings for each module, click **Setup...**.

6.1 Antivirus and antispyware protection

Antivirus protection guards against malicious system attacks by modifying files that pose potential threats. If a threat with malicious code is detected, the Antivirus module can eliminate it by blocking it and then cleaning it, deleting it or moving it to quarantine.

6.1.1 General

In the **General** section (**Setup** > **Enter application preferences...** > **General**), you can enable detection of the following types of applications:

- **Potentially unwanted applications** – These applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the way it behaved before these applications were installed). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.
- **Potentially unsafe applications** – These applications are commercial, legitimate software that can be abused by attackers if installed without user consent. This classification includes programs such as remote access tools, for this reason this option is disabled by default.

- **Suspicious applications** – These applications include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection. Packer is a runtime self-extracting executable that rolls up several kinds of malware into a single package. The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

To set up File System or Web and Mail exclusions 7, click the **Setup...** button.

6.1.1.1 Exclusions

In the **Exclusions** section you can exclude certain files/folders, applications or IP/IPv6 addresses from scanning.

Files and folders listed in the **File System** tab will be excluded from all scanners: Startup, Real-time and On-Demand (Computer scan).

- **Path** – path to excluded files and folders
- **Threat** – if there is a name of a threat next to an excluded file, it means that the file is only excluded for that threat, but not completely. If that file becomes infected later with other malware, it will be detected by the antivirus module.
- + – creates a new exclusion. Enter the path to an object (you can also use the wild cards * and ?) or select the folder or file from the tree structure.
- − – removes selected entries
- **Default** – cancels all exclusions

In the **Web and Email** tab, you can exclude certain **Applications** or **IP/IPv6 addresses** from protocol scanning.

6.1.2 Startup protection

Startup file check automatically scans files at system startup. By default, this scan runs regularly as a scheduled task after a user logon or after a successful virus database update. To modify ThreatSense engine parameter settings applicable to the Startup scan, click the **Setup...** button. You can learn more about ThreatSense engine setup by reading this section 9.

6.1.3 Real-time file system protection

Real-time file system protection checks all types of media and triggers a scan based on various events. Using ThreatSense technology (described in ThreatSense engine parameter setup 9), Real-time file system protection may vary for newly created files and existing files. Newly created files can be more precisely controlled.

By default, all files are scanned upon **file opening**, **file creation** or **file execution**. We recommend that you keep these default settings, as they provide the maximum level of Real-time protection for your computer. Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (for example, if there is a conflict with another Real-time scanner), Real-time protection can be terminated by clicking the ESET Cyber Security Pro icon located in your Menu Bar (top of the screen) and selecting **Disable Real-time File System Protection**. Real-time file system protection can also be disabled from the main program window (click **Setup** > **Computer** and switch **Real-time file system protection** to **DISABLED**).

The following types of media can be excluded from the Real-time scanner:

- **Local drives** – system hard drives
- **Removable media** – CDs, DVDs, USB media, Bluetooth devices, etc.
- **Network media** – all mapped drives

We recommend that you use default settings and only modify scanning exclusions in specific cases, such as when scanning certain media significantly slows down data transfers.

To modify advanced settings for Real-time file system protection, go to **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Real-Time Protection** and click **Setup...** next to **Advanced Options** (described in Advanced scan options 7).

6.1.3.1 Advanced options

In this window you can define which object types are scanned by the ThreatSense engine. To learn more about **Self-extracting archives**, **Runtime packers** and **Advanced heuristics**, see ThreatSense engine parameters setup 9.

We do not recommend making changes in the **Default archives settings** section unless required to resolve a specific issue, as higher archive nesting values can impede system performance.

ThreatSense parameters for executed files – by default, **Advanced heuristics** is used when files are executed. We strongly recommend keeping Smart optimization and ESET Live Grid enabled to mitigate impact on system performance.

Increase network volumes compatibility – this option boosts performance when accessing files over the network. It should be enabled if you experience slowdowns while accessing network drives. This feature uses system file coordinator on macOS 10.10 and later. Be aware that not all applications support the file coordinator, for example Microsoft Word 2011 does not support it, Word 2016 does.

6.1.3.2 When to modify Real-time protection configuration

Real-time protection is the most essential component for maintaining a secure system with ESET Cyber Security Pro. Use caution when modifying the Real-time protection parameters. We recommend that you only modify these parameters in specific cases. For example, a situation in which there is a conflict with a certain application.

After installing ESET Cyber Security Pro, all settings are optimized to provide the maximum level of system security for users. To restore default settings, click **Default** at the bottom-left of the **Real-Time Protection** window (**Setup** > **Enter application preferences ...** > **Real-Time Protection**).

6.1.3.3 Checking Real-time protection

To verify that Real-time protection is working and detecting viruses, download the eicar.com test file and check to see that ESET Cyber Security Pro identifies it as a threat. This test file is a special, harmless file detectable by all antivirus programs. The file was created by the EICAR institute (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs.

6.1.3.4 What to do if Real-time protection does not work

In this chapter we describe problem situations that may arise when using Real-time protection, and how to troubleshoot them.

Real-time protection is disabled
If Real-time protection is inadvertently disabled by a user, it will need to be reactivated. To reactivate Real-time protection, from the main menu click **Setup** > **Computer** and switch **Real-time file system protection** to **ENABLED**. Alternatively, you can enable Real-time file system protection in the application preferences window under **Real-Time Protection** by selecting **Enable real-time file system protection**.

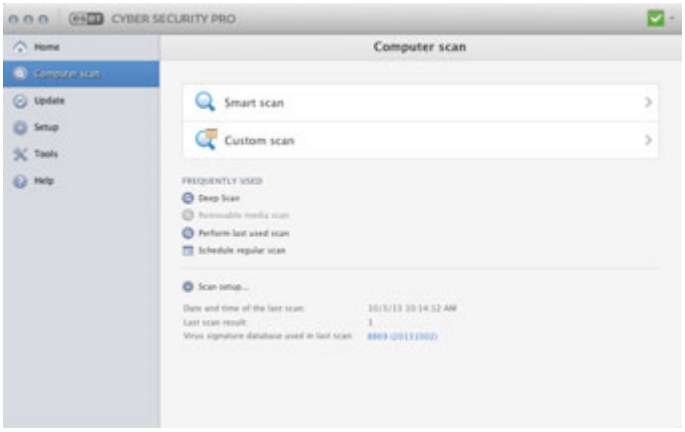
Real-time protection does not detect and clean infiltrations
Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs that may be on your system.

Real-time protection does not start
If Real-time protection is not initiated at system startup, it may be due to conflicts with other programs. If this is the case, please contact ESET Customer Care.

6.1.4 On-demand computer scan

If you suspect that your computer is infected (it behaves abnormally), run a **Smart scan** to examine your computer for infiltrations. For maximum protection, computer scans should be run regularly as part of routine security measures, not just when an infection is suspected. Regular scanning can detect infiltrations that were not detected by the Real-time scanner when they were saved to the disk. This can happen if the Real-time scanner was disabled at the time of infection, or if the virus signature database is not up-to-date.

We recommend that you run an On-demand computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**.



We recommend that you run an On-demand computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**.

You can also drag and drop selected files and folders from your Desktop or **Finder** window to the ESET Cyber Security Pro main screen, Dock icon, Menu Bar icon (top of the screen) or the application icon (located in the */Applications* folder).

6.1.4.1 Type of scan

Two types of On-demand computer scan are available. **Smart scan** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan** allows you to select any of the predefined scan profiles, as well as choose specific scan targets.

6.1.4.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantage is easy operation with no detailed scanning configuration. Smart scan checks all files in all folders and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see the section on Cleaning 10.

6.1.4.1.2 Custom scan

Custom scan is optimal if you would like to specify scanning parameters such as scan targets and scanning methods. The advantage of running a Custom scan is the ability to configure the parameters in detail. Different configurations can be saved as user-defined scan profiles, which can be useful if scanning is repeatedly performed using the same parameters.

To select scan targets, select **Computer scan** > **Custom scan** and then select specific **Scan Targets** from the tree structure. A scan target can also be more precisely specified by entering the path to the folder or file(s) you wish to include. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. Furthermore, you can choose from three cleaning levels by clicking **Setup...** > **Cleaning**.

NOTE: Performing computer scans with Custom scan is recommended for advanced users with previous experience using antivirus programs.

6.1.4.2 Scan targets

The Scan targets tree structure allows you to select files and folders to be scanned for viruses. Folders may also be selected according to a profile's settings.

A scan target can be more precisely defined by entering the path to the folder or file(s) you wish to include in scanning. Select targets from the tree structure that lists all available folders on the computer by selecting the check box that corresponds to a given file or folder.

6.1.4.3 Scan profiles

Your preferred scan settings can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, from the main menu click **Setup** > **Enter application preferences...** (or press *cmd+,*) > **Computer Scan** and click **Edit...** next to the list of current profiles.

To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup 9 section for a description of each parameter of the scan setup.

Example: Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you do not want to scan runtime packers or potentially unsafe applications and you also want to apply Strict cleaning. In the **On-demand Scanner Profiles List** window, type the profile name, click the **Add** button and confirm by clicking **OK**. Then adjust the parameters to meet your requirements by setting **ThreatSense Engine** and **Scan Targets**.

If you want to turn off the operating system and shut down the computer after the On-demand scan is finished, use the **Shutdown computer after scan** option.

6.1.5 ThreatSense engine parameters setup

ThreatSense is a proprietary ESET technology comprised of several complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, virus signatures) that work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully prevents rootkits.

The ThreatSense technology setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

To enter the setup window click **Setup > Enter application preferences ...** (or press *cmd+,*) and then click the ThreatSense Engine **Setup...** button located in the **Startup Protection**, **Real-Time Protection** and **Computer Scan** modules, which all use ThreatSense technology (see below). Different security scenarios may require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- **Startup Protection** - Automatic startup file check
- **Real-Time Protection** - Real-time file system protection
- **Computer Scan** - On-demand computer scan
- **Web Access Protection**
- **Email Protection**

The ThreatSense parameters are specifically optimized for each module, and their modification can significantly influence system operation. For example, changing settings to always scan runtime packers, or enabling advanced heuristics in the Real-time file system protection module could result in a slower system. Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

6.1.5.1 Objects

The **Objects** section allows you to define which files will be scanned for infiltrations.

- **Symbolic links** - (Computer scan only) scans files that contain a text string that is interpreted and followed by the operating system as a path to another file or directory.
- **Email files** - (not available in Real-time Protection) scans email files.
- **Mailboxes** - (not available in Real-time Protection) scans user mailboxes in the system. Incorrect use of this option may result in a conflict with your email client. To learn more about advantages and disadvantages of this option, read the following knowledgebase article.
- **Archives** - (not available in Real-time Protection) scans files compressed in archives (.rar, .zip, .arj, .tar, etc.).

- **Self-extracting archives** - (not available in Real-time Protection) scans files which are contained in self-extracting archive files.
- **Runtime packers** - unlike standard archive types, runtime packers decompress in memory. When this is selected, standard static packers (e.g. UPX, yoda, ASPack, FGS) are also scanned.

6.1.5.2 Options

In the **Options** section, you can select the methods used during a scan of the system. The following options are available:

- **Heuristics** – Heuristics use an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist, or was not included in the list of known viruses (virus signatures database).
- **Advanced heuristics** – Advanced heuristics is comprised of a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. The program's detection ability is significantly higher as a result of advanced heuristics.

6.1.5.3 Cleaning

Cleaning settings determine the manner in which the scanner cleans infected files. There are 3 levels of cleaning:

- **No cleaning** – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.
- **Standard cleaning** – The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow-up actions. The choice of follow-up actions will also be displayed if a predefined action could not be completed.
- **Strict cleaning** – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean a file, you will receive a notification and be asked to select the type of action to take.

Warning: In the Default Standard cleaning mode, entire archive files are deleted only if all files in the archive are infected. If an archive contains legitimate files as well as infected files, it will not be deleted. If an infected archive file is detected in Strict cleaning mode, the entire archive will be deleted even if clean files are present.

6.1.5.4 Exclusions

An extension is the part of a file name delimited by a period. The extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to be excluded from scanning.

By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. Using the + and − buttons, you can enable or prohibit the scanning of specific extensions.

Excluding files from scanning is sometimes necessary if scanning certain file types prevents the program from functioning properly. For example, it may be advisable to exclude *log*, *cfg* and *tmp* files. The correct format for entering file extensions is:
log
cfg
tmp

6.1.5.5 Limits

The **Limits** section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

- **Maximum Size:** Defines the maximum size of objects to be scanned. Once maximum size is defined, the antivirus module will scan only objects smaller than the size specified. This option should only be changed by advanced users who have specific reasons for excluding larger objects from scanning.
- **Maximum Scan Time:** Defines the maximum time allotted for scanning an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, whether or not the scan has finished.
- **Maximum Nesting Level:** Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.
- **Maximum File Size:** This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If scanning is prematurely terminated as a result of this limit, the archive will remain unchecked.

6.1.5.6 Others

Enable Smart optimization
With Smart Optimization enabled, settings are optimized to ensure the most efficient level of scanning without compromising scanning speed. The various protection modules scan intelligently, making use of different scanning methods. Smart Optimization is not rigidly defined within the product. The ESET Development Team is continuously implementing new changes which are then integrated into ESET Cyber Security Pro through regular updates. If Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular module are applied when performing a scan.

Scan alternative data stream (On-demand scanner only)
Alternate data streams (resource/data forks) used by the file system are file and folder associations which are invisible to ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.

6.1.6 An infiltration is detected

Infiltrations can reach the system from various entry points: webpages, shared folders, email or removable computer devices (USB, external disks, CDs, DVDs, etc.).

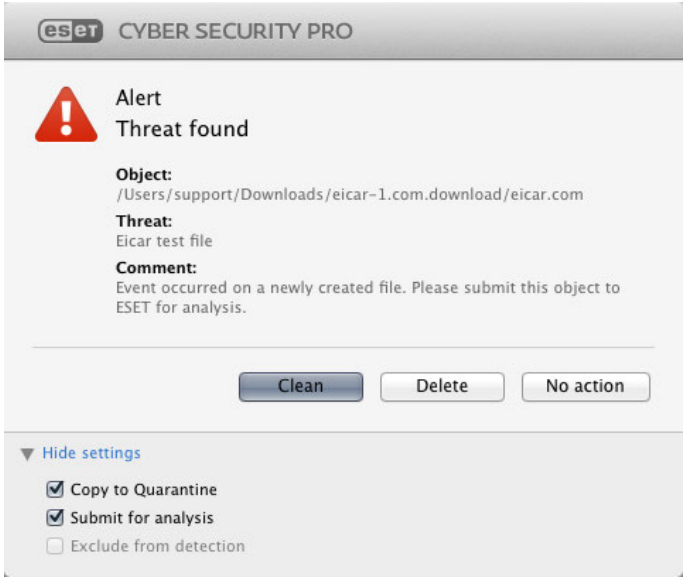
If your computer is showing signs of malware infection, for example it runs slower, often freezes, etc., we recommend that you take the following steps:

1. Click **Computer scan**.
2. Click **Smart scan** (for more information, see the Smart scan 8 section).
3. After the scan has finished, review the log for the number of scanned, infected and cleaned files.

If you only wish to scan a certain part of your disk click **Custom scan** and select targets to be scanned for viruses.

As a general example of how infiltrations are handled by ESET Cyber Security Pro, suppose that an infiltration is detected by the Real-time file system monitor using the default cleaning level. Real-time protection will attempt to clean or delete the file. If there is no predefined action available for the Real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, since the infected file(s) is left in its infected state. This option is intended for situations when you are sure that the file is harmless and has been detected by mistake.

Cleaning and deleting – Apply cleaning if a file has been attacked by a virus that has attached malicious code to it. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.



Deleting files in archives – In the default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. However, use caution when performing a **Strict cleaning** scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

6.2 Removable media scanning and blocking

ESET Cyber Security Pro can run an on-demand scan of inserted removable media devices (CD, DVD, USB, iOS device etc.).

Removable media may contain malicious code and put your computer at risk. To block removable media, click **Media blocking setup** (see the picture above) or from the main menu click **Setup** > **Enter application preferences ...** > **Media** from the main program window and select **Enable removable media blocking**. To allow access to certain types of media, deselect your desired media volumes.

NOTE: To allow access to external CD-ROM drive connected to your computer via USB cable, deselect the **CD-ROM** option.

7. Anti-Phishing

The term *phishing* defines a criminal activity that uses social engineering (the manipulation of users in order to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, credit card numbers, PIN numbers or usernames and passwords.

We recommend that you keep Anti-Phishing enabled (**Setup** > **Enter application preferences ...** > **Anti-Phishing Protection**). All potential phishing attacks coming from websites or domains listed in the ESET malware database will be blocked and a warning notification will be displayed informing you of the attack.

8. Firewall

The Personal firewall controls all network traffic to and from the system by allowing or denying individual network connections based on specified filtering rules. It provides protection against attacks from remote computers and enables blocking of some services. It also provides antivirus protection for HTTP, POP3 and IMAP protocols.

Personal firewall configuration can be found in **Setup** > **Firewall**. It allows you to adjust the filtering mode, rules and detailed settings. You can also access more detailed settings of the program from here.

If you switch **Block all network traffic: disconnect network** to **ENABLED**, all inbound and outbound communication will be blocked by the Personal firewall. Use this option only if you suspect critical security risks requiring the system to be disconnected from the network.

8.1 Filtering modes

Three filtering modes are available for the ESET Cyber Security Pro Personal firewall. Filtering mode settings can be found in ESET Cyber Security Pro preferences (press *cmd+,*) > **Firewall**. The behavior of the firewall changes based on the selected mode. Filtering modes also influence the level of user interaction required.

All traffic blocked - all inbound and outbound connections will be blocked.

Auto with exceptions - the default mode. This mode is suitable for users who prefer easy and convenient use of the firewall with no need to define rules. Automatic mode allows standard outbound traffic for the given system and blocks all non-initiated connections from the network side. You can also add custom, user-defined rules.

Interactive mode – allows you to build a custom configuration for your Personal firewall. When a communication is detected and no existing rules apply to that communication, a dialog window reporting an unknown connection will be displayed. The dialog window gives the option of allowing or denying the communication, and the decision to allow or deny can be remembered as a new rule for the Personal firewall. If you choose to create a new rule at this time, all future connections of this type will be allowed or blocked according to the rule.

To record detailed information about all blocked connections to a log file, select **Log all blocked connections**. To review the firewall log files, from the main menu click **Tools** > **Logs** and select **Firewall** from the **Log** drop-down menu.

8.2 Firewall rules

Rules represent a set of conditions used to test all network connections and determine the actions assigned to these conditions. Using the Personal firewall rules, you can define the type of action to take if a connection defined by a rule is established.

Incoming connections are initiated by a remote computer attempting to establish a connection with the local system. Outgoing connections work in the opposite way – the local system contacts a remote computer.

If a new unknown communication is detected, you must carefully consider whether to allow or deny it. Unsolicited, unsecured or unknown connections pose a security risk to the system. If such a connection is established, we recommend that you pay particular attention to the remote computer and the application attempting to connect to your computer. Many infiltrations try to obtain and send private data, or download other malicious applications to host workstations. The Personal firewall allows you to detect and terminate such connections.

By default, applications signed by Apple can automatically access the network. If you want to disable this, deselect **Allow software signed by Apple to access the network automatically**.

8.2.1 Creating new rules

The **Rules** tab contains a list of all rules applied to traffic generated by individual applications. Rules are added automatically according to user reactions to a new communication.

1. To create a new rule, click **Add...** , enter a name for the rule and drag-and-drop the application's icon into the blank field or click **Browse...** to look for the program in the */ Applications* folder. To apply the rule to all applications installed on your computer, select the **All applications** option.
2. In the next window, specify the **Action** (allow or deny the communication between selected application and network) and **Direction** of the communication (incoming, outgoing or both). You can record all communications related to this rule into a log file, to do so, select the **Log rule** option. To review the logs, click **Tools** > **Logs** from the ESET Cyber Security Pro main menu and select **Firewall** from the **Log** drop-down menu.
3. In the **Protocol/Ports** section, select a protocol through which the application communicates and port numbers (if TCP or UDP protocol is selected). The transport protocol layer provides secure and efficient data transfer.
4. Last, specify the **Destination** criteria (IP address, range, subnet, ethernet or Internet) for the rule.

8.3 Firewall zones

A zone represents a collection of network addresses which create one logical group. Each address in a given group is assigned similar rules defined centrally for the whole group.

These zones can be created by clicking **Add...**. Enter a **Name** and **Description** (optional) for the zone, select a profile this zone will belong to and add an IPv4/IPv6 address, address range, subnet, Wi-Fi network or an interface.

8.4 Firewall profiles

Profiles allow you to control the behavior of the ESET Cyber Security Pro Personal firewall. When creating or editing a Personal firewall rule, you can assign it to a specific profile. When you select a profile, only the global rules (with no profile specified) and the rules that have been assigned to that profile are applied. You can create multiple profiles with different rules assigned to easily alter Personal firewall behavior.

8.5 Firewall logs

The ESET Cyber Security Pro Personal firewall saves all important events in a log file. To access firewall logs from the main menu click **Tools** > **Logs** and then select **Firewall** from the **Log** drop-down menu.

Log files are a valuable tool for detecting errors and revealing intrusions into your system. ESET Personal firewall logs contain the following data:

- Date and time of event
- Name of event
- Source
- Target network address
- Network communication protocol
- Rule applied
- Application involved
- User

A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and can be defended against using Personal firewall such as: frequent connections from unknown locations, multiple attempts to establish connections, unknown applications communicating or unusual port numbers.

9. Web and Email protection

To access Web and Mail protection from the main menu, click **Setup** > **Web and Email**. From here you can also access detailed settings for each module by clicking **Setup...**.

- **Web access protection** - monitors HTTP communication between web browsers and remote servers.
- **Email client protection** - provides control of email communication received through POP3 and IMAP protocols.
- **Anti-Phishing protection** - blocks potential phishing attacks coming from websites or domains listed in the ESET malware database.

9.1 Web protection

Web access protection monitors communication between web browsers and remote servers for compliance with HTTP (Hypertext Transfer Protocol) rules.

Web filtering can be achieved by defining the port numbers for HTTP communication 13 and/or URL addresses 13.

9.1.1 Ports

In the **Ports** tab you can define the port numbers used for HTTP communication. By default the port numbers 80, 8080 and 3128 are predefined.

9.1.2 URL lists

The **URL Lists** section enables you to specify HTTP addresses to block, allow or exclude from checking. Websites in the list of blocked addresses will not be accessible. Websites in the list of excluded addresses are accessed without being scanned for malicious code.

To allow access only to the URL addresses listed in the **Allowed URL** list, select the **Restrict URL addresses** option.

To activate a list, select **Enabled** next to the list name. If you want to be notified when entering an address from the current list, select **Notified**.

In any list, the special symbols *(asterisk) and ?(question mark) can be used. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list.

9.2 Email protection

Email protection provides control of email communication received through the POP3 and IMAP protocols. When examining incoming messages, the program uses all the advanced scanning methods included in the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of the POP3 and IMAP protocol communications is independent of the email client used.

ThreatSense Engine: Setup – advanced virus scanner setup enables you to configure scan targets, detection methods, etc. Click **Setup** to display the detailed scanner setup window.

Append tag message to email footnote – after an email has been scanned, a notification containing scan results can be appended to the message. Tag messages cannot be relied on without question, since they may be omitted in problematic HTML messages and can be forged by some viruses. The following options are available:

- **Never** – no tag messages will be added at all
- **To infected email only** – only messages containing malicious software will be marked as checked
- **To all scanned email** – the program will append messages to all scanned email

Append note to the subject of received and read infected email – select this check box if you want email protection to include a virus warning in the infected email. This feature allows for simple filtering of infected emails. It also increases the level of credibility for the recipient and, if an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

Template added to the subject of infected email – edit this template to modify the subject prefix format of an infected email.

In the bottom part of this window, you can also enable/ disable checking of email communication received through the POP3 and IMAP protocols. To learn more about this, see the following topics:

- POP3 protocol checking 14
- IMAP protocol checking 14

9.2.1 POP3 protocol checking

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET Cyber Security Pro provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. Make sure the module is enabled for protocol filtering to work correctly, POP3 protocol checking is performed automatically with no need to reconfigure your email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

If **Enable POP3 protocol checking** option is selected, all POP3 traffic is monitored for malicious software.

9.2.2 IMAP protocol checking

The Internet Message Access Protocol (IMAP) is another Internet protocol for e-mail retrieval. IMAP has some advantages over POP3, for example multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. ESET Cyber Security Pro provides protection for this protocol, regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. Make sure that IMAP protocol checking is enabled for the module to work correctly; IMAP protocol control is performed automatically with no need to reconfigure your email client. By default, all communication on port 143 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

If **Enable IMAP protocol checking** is selected, all traffic through IMAP is monitored for malicious software.

10. Parental control

The **Parental control** section allows you to configure Parental control settings, which provide parents with automated tools to help protect their children. The goal is to prevent children and young adults from accessing pages containing inappropriate or harmful content. Parental control lets you block webpages that may contain potentially offensive material. Additionally, parents can prohibit access to up to 27 pre-defined website categories.

Your user accounts are listed in the **Parental Control** window (**Setup** > **Enter application preferences ...** > **Parental Control**). Select the one you want to use for parental control. To specify a level of protection for the selected account, click **Setup...** . To create a new account click **Add...** . This will redirect you to the macOS system accounts window.

In the **Parental control setup** window, select one of the predefined profiles from the **Setup profile** drop-down menu or copy parental setup from another user account. Each profile contains a modified list of allowed categories. If a category is checked, it is allowed. Moving the mouse over a category will show you a list of web pages that fall into that category.

To modify the list of **Allowed and Blocked Web Pages**, click **Setup...** at the bottom of a window and add a domain name into the desired list. Do not type *http://* . Using wildcards (*) is not necessary. If you type just a domain name, all subdomains will be included. For example, if you add *google.com* into the **List of Allowed Web Pages**, all subdomains (*mail.google.com*, *news.google.com*, *maps.google.com* etc.) will be allowed.

NOTE: Blocking or allowing a specific web page can be more accurate than blocking or allowing a whole category of web pages.

11. Update

Regularly updating ESET Cyber Security Pro is necessary to maintain the maximum level of security. The Update module ensures that the program is always up to date by downloading the most recent virus signature database.

Click **Update** from the main menu to view the current update status of ESET Cyber Security Pro, including the date and time of the last successful update and if an update is needed. To begin the update process manually, click **Update virus signature database**.

Under normal circumstances, when updates are downloaded properly, the message **Update is not necessary - the installed virus signature database is current** will appear in the Update window. If the virus signature database cannot be updated, we recommend that you check the update settings 14 - the most common reason for this error is incorrectly entered authentication data (Username and Password) or incorrectly configured connection settings 20.

The Update window also contains information about the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added during the given update.

11.1 Update setup

To delete all temporarily stored update data, click **Clear** next to **Clear Update Cache**. Use this option if you are experiencing difficulty while updating.

11.1.1 Advanced options

To disable notifications displayed after each successful update, select **Do not display notification about successful updates**.

Enable **Pre-release update** to download development modules that are completing final testing. Pre-release updates often contain fixes for product issues. **Delayed update** downloads updates a few hours after they are released, to ensure that clients will not receive updates until they are confirmed to be free of any issues in the wild.

ESET Cyber Security Pro records snapshots of virus signature database and program modules for use with the **Update Rollback** feature. Leave **Create snapshots of update files**

enabled to have ESET Cyber Security Pro record these snapshots automatically. If you suspect that a new update of the virus database and/or program modules may be unstable or corrupt, you can roll back to the previous version and disable updates for a set period of time. Alternatively, you can enable previously disabled updates if you had postponed them indefinitely. When rolling back to a previous update, use the **Set suspend period to** drop-down menu to specify the time period for which you want to suspend updates. If you select **until revoked**, normal updates will not resume until you restore them manually. Use caution when selecting this setting.

Set maximum database age automatically – Allows you to set the maximum time (in days) after which the virus signature database will be reported as out of date. The default value is 7 days.

11.2 How to create update tasks

Updates can be triggered manually by clicking **Update** from the main menu and then clicking **Update virus signature database**.

Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET Cyber Security Pro:

- **Regular automatic update**
- **Automatic update after user logon**

Each of the update tasks can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see the Scheduler 16 section.

11.3 Upgrading ESET Cyber Security Pro to a new version

For maximum protection, it is important to use the latest build of ESET Cyber Security Pro. To check for a new version, click **Home** from the main menu. If a new build is available, a message will be displayed. Click **Learn more...** to display a new window containing the version number of the new build and the changelog.

Click **Yes** to download the latest build or click **Not now** to close the window and download the upgrade later.

If you click **Yes**, the file will be downloaded to your downloads folder (or the default folder set by your browser). When the file has finished downloading, launch the file and follow the installation directions. Your Username and Password will be automatically transferred to the new installation. We recommend that you check for upgrades regularly, especially when installing ESET Cyber Security Pro from a CD or DVD.

11.4 System updates

The macOS system updates feature is an important component designed to protect users from malicious software. For maximum security, we recommend that you install these updates as soon as they become available. ESET Cyber Security Pro will notify you about missing updates according to the level you specify. You can adjust the availability of update notifications in **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Alerts and notifications > Setup...** by changing the **Display Conditions** options next to the **Operating system updates**.

- **Show all updates** - a notification will be displayed any time that a system update is missing
- **Show only recommended** - you will be notified about recommended updates only

If you do not want to be notified about missing updates, deselect the check box next to **Operating system updates**.

The notification window provides an overview of the updates available for the macOS operating system and the applications updated through the macOS native tool - Software updates. You can run the update directly from the notification window or from the **Home** section of ESET Cyber Security Pro by clicking **Install the missing update**.

The notification window contains the application name, version, size, properties (flags) and additional information about available updates. The **Flags** column contains the following information:

- **[recommended]** - the operating system manufacturer recommends that you install this update to increase the security and stability of the system
- **[restart]** - a computer restart is required on following installation
- **[shutdown]** - the computer must be shut down and then powered back on following installation

The notification window shows the updates retrieved by the command line tool called 'softwareupdate'. Updates retrieved by this tool can vary from the updates displayed by the 'Software updates' application. If you want to install all available updates displayed in the 'Missing system updates' window and also those not displayed by the 'Software updates' application, you have to use the 'softwareupdate' command line tool. To learn more about this tool, read the 'softwareupdate' manual by typing `man softwareupdate` into a **Terminal** window. This is recommended for advanced users only.

12. Tools

The **Tools** menu includes modules that help simplify program administration and offer additional options for advanced users.

12.1 Log files

The Log files contain information about important program events that have occurred and provides an overview of detected threats. Logging acts as an essential tool in system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on current log verbosity settings. It is possible to view text messages and logs directly from the ESET Cyber Security Pro environment, as well as to archive logs.

Log files are accessible from the ESET Cyber Security Pro main menu by clicking **Tools** > **Logs**. Select the desired log type using the **Log** drop-down menu at the top of the window. The following logs are available:

1. **Detected threats** – use this option to view all information about events related to the detection of infiltrations.
2. **Events** – this option is designed to help system administrators and users solve problems. All important actions performed by ESET Cyber Security Pro are recorded in the Event logs.
3. **Computer scan** – results of all completed scans are displayed in this log. Double-click any entry to view details for the respective On-demand computer scan.
4. **Parental** – list of all web pages blocked by Parental control.
5. **Firewall** – this log contains the results of all network-related events.
6. **Filtered websites** – this list is useful if you want to view a list of websites that were blocked by Web access protection. In these logs you can see the time, URL, status, IP address, user and application that opened a connection to the particular website.

In each section, the displayed information can be directly copied to the clipboard by selecting the entry and clicking on the **Copy** button.

12.1.1 Log maintenance

The logging configuration for ESET Cyber Security Pro is accessible from the main program window. Click **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Log Files**. You can specify the following options for log files:

- **Delete old log records automatically** - log entries older than the specified number of days are automatically deleted (90 days by default)
- **Optimize log files automatically** - enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded (25% by default)

All the relevant information displayed in the graphic user interface, threat and event messages can be stored in human readable text formats such as plain text or CSV (Comma-separated values). If you want to make these files available for processing using third-party tools, select the check box next to **Enable logging to text files**.

To define the target folder to which the log files will be saved, click **Setup** next to **Advanced Options**.

Based on the options selected under **Text Log Files: Edit**, you can save logs with the following information written:

- Events such as *Invalid username and password*, *Virus signature database can not be updated* etc. are written to the eventslog.txt file
- Threats detected by the Startup scanner, Real-Time Protection or Computer Scan are stored in the file named threatslog.txt
- The results of all completed scans are saved in the format scanlog.NUMBER.txt
- All events related to communication through the Firewall are written to firewalllog.txt

To configure the filters for **Default Computer Scan Log Records** , click **Edit** and select/deselect log types as required. Further explanation to these log types can be found in Log Filtering 16.

12.1.2 Log filtering

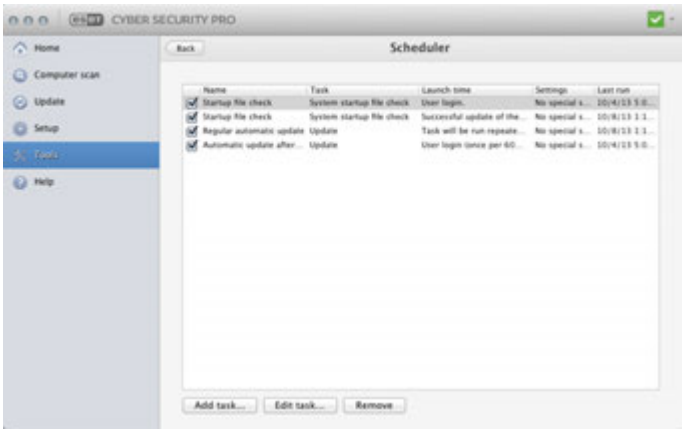
Logs store information about important system events. The log filtering feature allows you to display records about a specific type of event.

The most frequently used log types are listed below:

- **Critical warnings** – critical system errors (e.g., Antivirus protection failed to start)
- **Errors** - error messages such as "*Error downloading file*" and critical errors
- **Warnings** – warning messages
- **Informative records** - informative messages including successful updates, alerts, etc.
- **Diagnostic records** - information needed for fine-tuning the program as well as all records described above.

12.2 Scheduler

The **Scheduler** can be found in the ESET Cyber Security Pro main menu under **Tools**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used.



The Scheduler manages and launches scheduled tasks with predefined configurations and properties. The configuration and properties contain information such as the date and time as well as specified profiles to be used during execution of the task.

By default, the following scheduled tasks are displayed in the Scheduler:

- Log maintenance (after enabling the **Show system tasks** option in the scheduler setup)

- Startup file check after user logon
- Startup file check after successful update of the virus signature database
- Regular automatic update
- Automatic update after user logon

To edit the configuration of an existing scheduled task (both default and user-defined), CTRL+click the task you want to modify and select **Edit...** or select the task and click **Edit task...** .

12.2.1 Creating new tasks

To create a new task in Scheduler, click **Add task...** or CTRL+click in the blank field and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run application**
- **Update**
- **Log maintenance**
- **On-demand computer scan**
- **System startup file check**

NOTE: By choosing **Run application**, you can run programs as a system user called "nobody". Permissions for running applications through the Scheduler are defined by macOS.

In the example below, we will use the Scheduler to add a new update task, since update is one of the most frequently used scheduled tasks:

1. From the **Scheduled task** drop-down menu select **Update**.
2. Enter the name of the task into the **Task name** field.
3. Select the frequency of the task from the **Run task** drop-down menu. Based on the frequency selected, you will be prompted to specify different update parameters. If you select **User-defined**, you will be prompted to specify date/time in cron format (see the Creating user-defined task 17 section for more details).
4. In the next step, define what action to take if the task cannot be performed or completed at the scheduled time.
5. In the last step, a summary window with information about the current scheduled task is displayed. Click **Finish**. The new scheduled task will be added to the list of currently scheduled tasks.

By default ESET Cyber Security Pro contains pre-defined scheduled tasks to ensure correct product functionality. These should not be altered, and are hidden by default. To make these tasks visible, from the main menu click **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Scheduler** and select **Show system tasks**.

12.2.2 Creating user-defined tasks

Date and time of the **User-defined** task has to be entered in year-extended cron format (a string containing 6 fields each separated by a space):

```
minute(0-59) hour(0-23) day of month(1-31) month (1-12) year(1970-2099) day of week(0-7)(Sunday = 0 or 7)
```

Example:

```
30 6 22 3 2012 4
```

Special characters supported in cron expressions:

- asterisk (`*`) - expression will match for all values of the field; e.g. asterisk in the 3rd field (day of month) means every day
- hyphen (`-`) - defines ranges; e.g. `3-9`
- comma (`,`) - separates items of a list; e.g. `1,3,7,8`
- slash (`/`) - defines increments of ranges; e.g. `3-28/5` in the 3rd field (day of month) means 3rd day of the month and then every 5 days.

Day names (Monday-Sunday) and month names (January-December) are not supported.

NOTE: If you define both day of month and day of week, command will be executed only when both fields match.

12.3 Quarantine

The main purpose of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by ESET Cyber Security Pro.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to the ESET Threat Lab.

Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (e.g., added by user...) and number of threats (e.g., if it is an archive containing multiple infiltrations). The quarantine folder with quarantined files (*/Library/Application Support/Eset/esets/cache/quarantine*) remains in the system even after uninstalling ESET Cyber Security Pro. Quarantined files are stored in a safe encrypted form and can be restored again after installing ESET Cyber Security Pro.

12.3.1 Quarantining files

ESET Cyber Security Pro automatically quarantines deleted files (if you have not deselected this option in the alert window). You can quarantine any suspicious file manually by clicking **Quarantine...** . The context menu can also be used for this purpose, CTRL+click the blank field, select **Quarantine**, select a file you want to quarantine and click **Open**.

12.3.2 Restoring from Quarantine

Quarantined files can also be restored to their original location, to do so, select a quarantined file and click **Restore**. Restore is also available from the context menu, CTRL+click a given file in the Quarantine window and then click **Restore**. The context menu also offers the option **Restore to...**, which allows you to restore a file to a location other than the one from which it was deleted.

12.3.3 Submitting file from Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (e.g., by heuristic analysis of the code) and subsequently quarantined, please send the file to the ESET Threat Lab. To submit a file from quarantine, CTRL+click the file and select **Submit file for analysis** from the context menu.

12.4 Running processes

The list of **Running processes** displays the processes running on your computer. ESET Cyber Security Pro provides detailed information on running processes to protect users using ESET Live Grid technology.

- **Process** – name of the process that is currently running on your computer. To see all running processes you can also use Activity Monitor (found in */Applications/Utilities*).
- **Risk level** – in most cases, ESET Cyber Security Pro and ESET Live Grid technology assign risk levels to objects (files, processes, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level. Known applications marked green are definitely clean (whitelisted) and will be excluded from scanning. This improves the speed of both the On-demand and Real-time scans. When an application is marked as unknown (yellow), it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about a file, you can submit it to the ESET Threat Lab for analysis. If the file turns out to be a malicious application, its signature will be added to one of the upcoming updates.
- **Number of Users** – the number of users that use a given application. This information is gathered by ESET Live Grid technology.
- **Time of discovery** – period of time since the application was discovered by ESET Live Grid technology.
- **Application Bundle ID** – name of the vendor or application process.

By clicking a given process, the following information will appear at the bottom of the window:

- **File** – location of an application on your computer
- **File Size** – physical size of the file on the disk
- **File Description** – file characteristics based on the description from the operating system
- **Application Bundle ID** – name of the vendor or application process
- **File Version** – information from the application publisher
- **Product name** – application name and/or business name

12.5 Live Grid

The Live Grid Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional Live Grid Early Warning System has a single purpose – to improve the protection that we can offer you. The best way to ensure that we see new threats as soon as they appear is to "link" to as many of our customers as possible and use them as our threat scouts. There are two options:

1. You can choose not to enable the Live Grid Early Warning System. You will not lose any functionality from your software, and you will still receive the best protection that we offer.
2. You can configure the Live Grid Early Warning System to submit anonymous information about new threats and where new threatening code is contained. This information can be sent to ESET for detailed analysis. Studying these threats will help ESET update its database of threats and improve the program's threat detection ability.

The Live Grid Early Warning System will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer's operating system.

While there is a chance this may occasionally disclose some information about you or your computer (usernames in a directory path, etc.) to the ESET Threat Lab, this information will not be used for ANY purpose other than to help us respond immediately to new threats.

To access Live Grid setup from the main menu, click **Setup** > **Enter application preferences …** (or press *cmd+,*) > **Live Grid**. Select **Enable Live Grid Early Warning System** to activate Live Grid and then click **Setup…** located next to **Advanced Options**.

12.5.1 Live Grid setup

By default, ESET Cyber Security Pro is configured to submit suspicious files to the ESET Threat Lab for detailed analysis. If you do not wish to submit these files automatically, deselect **Submit files**.

If you find a suspicious file, you can submit it to our Threat Lab for analysis. To do so, click **Tools** > **Submit sample for analysis** from the main program window. If it is a malicious application, its signature will be added to the next virus signature database update.

Submit anonymous statistics – The ESET Live Grid Early Warning System collects anonymous information about your computer related to newly detected threats. This information includes the name of the infiltration, the date and time it was detected, the ESET security product version, your operating system version and the location setting. These statistics are typically delivered to ESET servers once or twice daily.

Below is an example of a statistical package submitted:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

Exclusion Filter – This option allows you to exclude certain file types from submission. For example, it may be useful to exclude files which may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, .rtf etc.). You can add file types to the list of excluded files.
Contact Email (optional) – Your email address will be used if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

13. User interface

The user interface configuration options allow you to adjust the working environment to fit your needs. These options are accessible from the main menu by clicking **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Interface**.

- To display the ESET Cyber Security Pro splash screen at system startup, select **Show splash-screen at startup**.
- **Present application in Dock** allows you to display the ESET Cyber Security Pro icon in the macOS Dock and switch between ESET Cyber Security Pro and other running applications by pressing *cmd+tab*. Changes take effect after you restart ESET Cyber Security Pro (usually triggered by computer restart).
- The **Use standard menu** option allows you to use certain keyboard shortcuts (see Keyboard shortcuts 6) and see standard menu items (User interface, Setup and Tools) on the macOS Menu Bar (top of the screen).
- To enable tooltips for certain options of ESET Cyber Security Pro, select **Show tooltips**.
- **Show hidden files** allows you to see and select hidden files in the **Scan Targets** setup of a **Computer scan**.
- By default, ESET Cyber Security Pro icon is displayed in the Menu Bar Extras that appear at the right of the macOS Menu Bar (top of the screen). To disable this, deselect **Show icon in menu bar extras**. This change takes effect after you restart ESET Cyber Security Pro (usually triggered by computer restart).

13.1 Alerts and notifications

The **Alerts and notifications** section allows you to configure how threat alerts and system notifications are handled by ESET Cyber Security Pro.

Disabling **Display alerts** will disable all alert windows and is only recommended in specific situations. For most users, we recommend that this option be left on its default setting (enabled). Advanced options are described in this chapter 19.

Selecting **Display notifications on desktop** will cause alert windows that do not require user interaction to display on the desktop (in the upper-right corner of your screen by default). You can define the period for which a notification will be displayed by adjusting the **Close notifications automatically after** X **seconds** value (5 seconds by default).

Since ESET Cyber Security Pro version 6.2, you can also prevent certain **Protection statuses** from displaying in the program's main screen (**Protection status** window). To learn more about this, see the Protection statuses 19.

13.1.1 Display alerts

ESET Cyber Security Pro displays alert dialog windows informing you of new program versions, operating system updates, the disabling of certain program components, the deletion of logs etc. You can suppress each notification individually by selecting **Do not show this dialog again**.

List of Dialogs (**Setup** > **Enter application preferences ...** > **Alerts and notifications** > **Setup...**) shows the list of all alert dialogs triggered by ESET Cyber Security Pro. To enable or suppress each notification, select the check box left of the **Dialog Name**. Additionally, you can define **Display Conditions** under which notifications about new program versions and operating system updates will be displayed.

13.1.2 Protection statuses

The current protection status of ESET Cyber Security Pro can be altered by activating or deactivating statuses in **Setup** > **Enter application preferences...** > **Alerts and Notifications** > **Display in Protection status screen: Setup**. The status of various program features will be displayed or hidden from the ESET Cyber Security Pro main screen (**Protection status** window).

You can hide protection status of the following program features:

- Firewall
- Anti-Phishing
- Web access protection
- Email client protection
- Operating system update
- License expiration
- Computer restart required

13.2 Privileges

ESET Cyber Security Pro settings can be very important to your organization's security policy. Unauthorized modifications may endanger the stability and protection of your system. For this reason, you can define which users have permission to edit the program configuration.

To specify privileged users, click **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Privileges**. Select the users or groups from the list on the left and click **Add**. To display all system users/groups, select **Show all users/groups**. To remove a user, select a name from the **Selected Users** list on the right and click **Remove**.

NOTE: If you leave the Selected Users list empty, all users are considered privileged.

13.3 Context menu

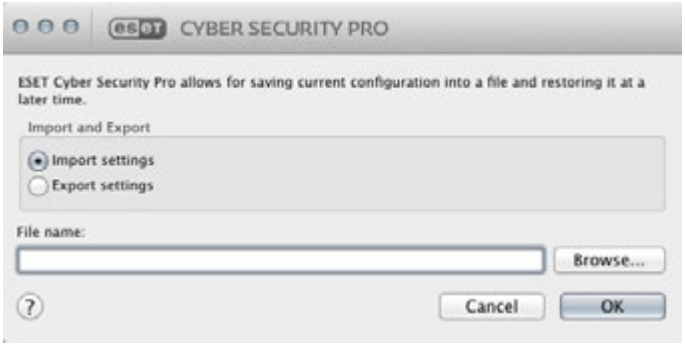
Context menu integration can be enabled by clicking **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Context Menu** section by selecting the **Integrate into the context menu** option. Logging out or restarting the computer is required for changes to take effect. Context menu options will be available in the **Finder** window when you CTRL+click on any file.

14. Miscellaneous

14.1 Import and export settings

To import an existing configuration or export your ESET Cyber Security Pro configuration, click **Setup** > **Import or export settings**.

Import and export are useful if you need to backup your current configuration of ESET Cyber Security Pro for use at a later date. Export settings is also convenient for users who want to use their preferred configuration of ESET Cyber Security Pro on multiple systems. You can easily import a configuration file to transfer your desired settings.



To import a configuration, select **Import settings** and click **Browse** to navigate to the configuration file you want to import. To export, select **Export settings** and use the browser to select a location on your computer to save the configuration file.

14.2 Proxy server setup

Proxy server settings can be configured in **Setup** > **Enter application preferences ...** (or press *cmd+,*) > **Proxy Server**. Specifying the proxy server at this level defines global proxy server settings for all ESET Cyber Security Pro functions. Parameters defined here will be used by all modules that require a connection to the Internet. ESET Cyber Security Pro supports the Basic Access and NTLM (NT LAN Manager) types of authentication.

To specify proxy server settings for this level select **Use proxy server** and enter the IP address or URL of your proxy server in the **Proxy Server** field. In the Port field, specify the port where the proxy server accepts connections (3128 by default). You can also click **Detect** to let the program fill out the both fields.

If communication with the proxy server requires authentication, enter a valid **Username** and **Password** into the respective fields.

15. Glossary

15.1 Types of infiltration

An Infiltration is a piece of malicious software that attempts to enter and/or damage a user's computer.

15.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses typically attack executable files, scripts and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. Conversely, some viruses do not cause any damage, they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term "virus" is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term "malware" (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state, usually by cleaning them using an antivirus program.

15.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves; they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours of their release, in some cases, even in minutes. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend that you delete the infected files because they likely contain malicious code.

15.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations that attempt to present themselves as useful programs, tricking users into letting them run. Today, there is no longer a need for trojan horses to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

- Downloader – A malicious program with the ability to download other infiltrations from the Internet
- Dropper – A type of trojan horse designed to drop other types of malware onto compromised computers
- Backdoor – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it
- Keylogger – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers

- Dialer – Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection has been created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

Trojan horses usually take the form of executable files. If a file on your computer is detected as a trojan horse, we recommend deleting it, since it most likely contains malicious code.

15.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system while concealing their presence. After accessing a system (usually exploiting a system vulnerability), rootkits use functions built into the operating system to avoid detection by antivirus software: they conceal processes and files. For this reason it is almost impossible to detect them using ordinary testing techniques.

15.1.5 Adware

Adware is a shortened term for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing creators of freeware programs to cover development costs of their (usually useful) applications.

Adware itself is not dangerous, users may only be bothered by the advertisements. The danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This often means that adware may access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry. If there is a file detected as adware on your computer, it is advisable that you delete it, since there is a high probability that it contains malicious code.

15.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory, they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, we recommend deleting it, since there is a high probability that it contains malicious code.

15.1.7 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands they may be misused for malicious purposes. ESET Cyber Security Pro provides the option to detect such threats.

Potentially unsafe applications are typically commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

15.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the way it behaved before their installation). The most significant changes are:

- new windows you haven't seen previously are opened
- activation and running of hidden processes
- increased usage of system resources
- changes in search results
- applications communicate with remote servers

15.2 Types of remote attacks

There are many special techniques that allow attackers to compromise remote systems. These are divided into several categories.

15.2.1 DoS attacks

DoS, or Denial of Service, is an attempt to make a computer or network unavailable for its intended users. The communication between afflicted users is obstructed and can no longer continue in a functional way. Computers exposed to DoS attacks usually need to be restarted in order to work properly.

In most cases, the targets are web servers and the aim is to make them unavailable to users for a certain period of time.

15.2.2 DNS Poisoning

Using DNS (Domain Name Server) poisoning, hackers can trick the DNS server of any computer into believing that the fake data they supplied is legitimate and authentic. The fake information is cached for a certain period of time, allowing attackers to rewrite DNS replies of IP addresses. As a result, users trying to access Internet websites will download computer viruses or worms instead of their original content.

15.2.3 Port scanning

Port scanning is used to determine which computer ports are open on a network host. A port scanner is software designed to find such ports.

A computer port is a virtual point that handles incoming and outgoing data; this is crucial from a security point of view. In a large network, the information gathered by port scanners may help to identify potential vulnerabilities. Such use is legitimate.

Still, port scanning is often used by hackers attempting to compromise security. Their first step is to send packets to each port. Depending on the response type, it is possible to determine which ports are in use. The scanning itself causes no damage, but be aware that this activity can reveal potential vulnerabilities and allow attackers to take control of remote computers.

Network administrators are advised to block all unused ports and protect those that are in use from unauthorized access.

15.2.4 TCP desynchronization

TCP desynchronization is a technique used in TCP Hijacking attacks. It is triggered by a process in which the sequential number in incoming packets differs from the expected sequential number. Packets with an unexpected sequential number are dismissed (or saved in the buffer storage, if they are present in the current communication window).

In desynchronization, both communication endpoints dismiss received packets, at which point remote attackers are able to infiltrate and supply packets with a correct sequential number. The attackers can even manipulate or modify communication.

TCP Hijacking attacks aim to interrupt server-client, or peer-to-peer communications. Many attacks can be avoided by using authentication for each TCP segment. It is also advised that you use the recommended configuration for your network devices.

15.2.5 SMB Relay

SMBRelay and SMBRelay2 are special programs that are capable of carrying out attacks against remote computers. These programs take advantage of the Server Message Block file sharing protocol, which is layered onto NetBIOS. A user sharing any folder or directory within a LAN most likely uses this file sharing protocol.

Within local network communication, password hashes are exchanged.

SMBRelay receives a connection on UDP port 139 and 445, relays the packets exchanged by the client and server, and modifies them. After connecting and authenticating, the client is disconnected. SMBRelay creates a new virtual IP address. SMBRelay relays SMB protocol communications except for negotiation and authentication. Remote attackers can use the IP address, as long as the client computer is connected.

SMBRelay2 works on the same principle as SMBRelay, except it uses NetBIOS names rather than IP addresses. Both can carry out “man-in-the-middle” attacks. These attacks allow remote attackers to read, insert and modify messages exchanged between two communication endpoints without being noticed. Computers exposed to such attacks often stop responding or unexpectedly restart.

To avoid attacks, we recommend that you use authentication passwords or keys.

15.2.6 ICMP attacks

The ICMP (Internet Control Message Protocol) is a popular and widely-used Internet protocol. It is used primarily by networked computers to send various error messages.

Remote attackers attempt to exploit the weaknesses of the ICMP protocol. The ICMP protocol is designed for one-way communication requiring no authentication. This enables remote attackers to trigger DoS (Denial of Service) attacks, or attacks which give unauthorized individuals access to incoming and outgoing packets.

Typical examples of an ICMP attack are ping floods, ICMP_ECHO floods and smurf attacks. Computers exposed to an ICMP attack are significantly slower (this applies to all applications that use the Internet) and have problems connecting to the Internet.

15.3 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, do not publish your email address on the Internet
- only give your email address to trusted individuals
- if possible, do not use common aliases. With more complicated aliases, the probability of tracking is lower
- do not reply to spam that has already arrived in your inbox
- be careful when filling out Internet forms, be especially cautious of options such as *Yes, I want to receive information*
- use "specialized" email addresses, for example one for business, one for communication with your friends, etc.
- from time to time, change your email address
- use an Antispam solution

15.3.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what is more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with their current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

15.3.2 Hoaxes

A hoax is misinformation that is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

15.3.3 Phishing

The term phishing defines a criminal activity that uses social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email that impersonates a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

15.3.4 Recognizing spam scams

Generally, there are a few indicators that can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message.

- Sender address does not belong to someone on your contact list
- you are offered a large sum of money, but you have to provide a small sum first
- you are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- it is written in a foreign language
- you are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer)
- some of the words are misspelled in an attempt to trick your spam filter. For example *vaigra* instead of *viagra*, etc.