Bitdefender

Bitdefender Endpoint Security Tools for Windows

USER'S GUIDE

Bitdefender Endpoint Security Tools for Windows User's Guide

Publication date 2019.01.29

Copyright© 2019 Bitdefender

Table of Contents

Using This Guide

1. Purpose and Intended Audience

This documentation is intended for the end users of **Bitdefender Endpoint Security Tools**, the Security for Endpoints client software installed on computers and servers to protect them against malware and other Internet threats and to enforce user control policies.

This guide is also intended for the end users of **Bitdefender Endpoint Security Tools for Windows Legacy**, which is designed for older Windows operating systems, such as XP and Vista families, with limited features and support.

The information presented herein should be easy to understand by anyone who is able to work under Windows. BEST for Windows Legacy is referred by specific notes throughout the guide, where it is the case.

2. How to Use This Guide

This guide is organized so as to make it easy to find the information you need.

Get familiar with the Bitdefender Endpoint Security Tools user interface.

Find out how to run scans for malware.

Find out about Bitdefender Endpoint Security Tools updates.

Check the activity of Bitdefender Endpoint Security Tools.

Where to look and where to ask for help if something unexpected appears.

3. Conventions Used in This Guide

Typographical Conventions

Several text styles are used in the guide for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
business-docs@bitdefender.com	E-mail addresses are inserted in the text for contact information.
"Using This Guide" (p. iv)	This is an internal link, towards some location inside the document.
`filename`	Files and directories are printed using `monospaced` font.
option	All the product options are printed using **bold** characters.
keyword	Important keywords or phrases are highlighted using **bold** characters.

Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note
The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

Important
This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

4. Request for Comments

Please write to tell us how you think this guide could be improved and help us provide you with the best documentation possible.

Let us know by sending an e-mail to business-docs@bitdefender.com.

1. GETTING STARTED

Bitdefender Endpoint Security Tools is a fully-automated computer security program, managed remotely by your network administrator. Once installed, it protects you against all kinds of malware (such as viruses, spyware and trojans), network attacks, phishing and data theft. It can also be used to enforce your organization's computer and Internet use policies. Bitdefender Endpoint Security Tools will make most security-related decisions for you and will rarely show pop-up alerts. Details of actions taken and information about program operation are available in the **Events** timeline.

1.1. The System Tray Icon

At installation time, Bitdefender Endpoint Security Tools places an icon **B** in the system tray. If you double-click this icon, the main window will open. If you right-click the icon, a contextual menu will provide you with some useful options.

- **Show** - opens the main window of Bitdefender Endpoint Security Tools.

- **About** - opens a window with information about Bitdefender Endpoint Security Tools and states where to look for help in case of unexpected issues. This window also includes a link to Bitdefender privacy policy.

System Tray Icon

- **Language** - allows you to change the user interface language.

- **Power User** - allows you to access and modify security settings, after providing the password in the login window. Control Center is being notified when an endpoint is in Power User mode and the Control Center administrator can always overwrite local security settings.
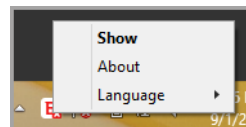
> ⚠️ **Important**
> This option is available only if granted by the network administrator through policy settins.
> This option is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

The Bitdefender Endpoint Security Tools icon in the system tray informs you when issues affect your computer by changing the way it looks:

B Critical issues affect the security of the system.

unfollow the traditional

Bₐ Some issues affect the security of the system.

> ⓘ **Note**
> The network administrator can choose to hide the system tray icon.

1.2. The Main Window

The main window of Bitdefender Endpoint Security Tools allows you to check the protection status and perform scan tasks. Everything is just a few clicks away. Protection configuration and management are performed remotely by your network administrator.

To access the main interface of Bitdefender Endpoint Security Tools, navigate from the Windows Start menu, following the path **Start → All Programs → Bitdefender Endpoint Security Tools → Open Security Console** or, quicker, double-click the Bitdefender Endpoint Security Tools **B** icon in the system tray.

Main Window

The window is organized into two main areas:

- Status area
- Events timeline

1.2.1. The Status Area

The **Status** area offers useful information regarding the security of the system.

Status Area

You can easily identify the current security status based on the status symbol displayed to the left of the status area:

- **Green check mark.** There are no issues to fix. Your computer and data are protected.
- **Yellow exclamation mark.** Non-critical issues are affecting the security of your system.
- **Red X mark.** Critical issues are affecting the security of your system.

In addition to the status symbol, a detailed security status message is displayed to the right of the status area. You can see the detected security issues by clicking inside the status area. Existing issues will be fixed by your network administrator.

1.2.2. Events Timeline

Bitdefender Endpoint Security Tools keeps a detailed log of events concerning its activity on your computer, including activities monitored by Content Control.

Events Timeline

The **Events** timeline is an important tool in monitoring your Bitdefender protection. For instance, you can easily check if an update was successfully performed or if malware was found on your computer.

1.3. The Modules Window

The **Modules** window displays useful information about the status and activity of the installed protection modules. To open the **Modules** window, click the **Modules** button in the Bitdefender Endpoint Security Tools main window.

Modules Window

Antimalware

Antimalware protection is the foundation of your security. Bitdefender Endpoint Security Tools protects you in real time and on demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.

- **On-Access**. On-access scanning prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).
- **Advanced Threat Control**. It continuously monitors applications running on the endpoint for malware-like actions. Advanced Threat Control will automatically try to disinfect the detected file.
- **Quarantine** displays the list of quarantined files, their original path, quarantine action time and date and their security status. Use the buttons at the bottom to delete or restore the files you want. If you want to delete all files from the quarantine, click the **Empty** button.
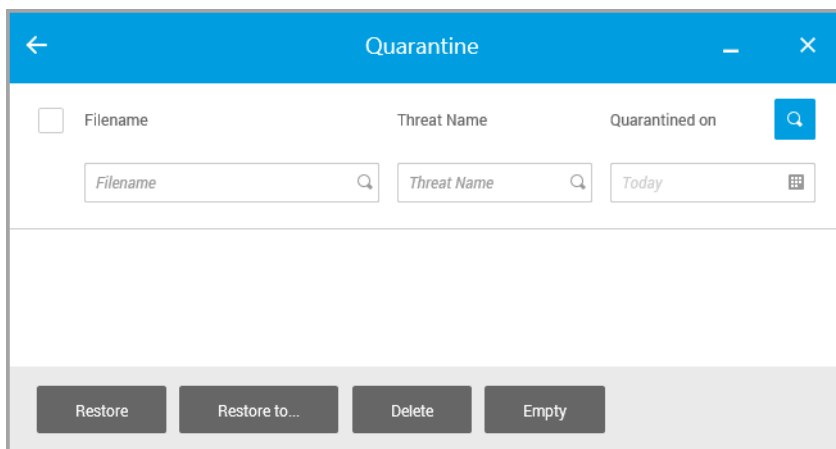
Quarantine

Content Control

The Content Control module protects you while on the Internet against phishing attacks, fraud attempts, private data leaks, and inappropriate web content. It also includes a comprehensive set of user controls that help the network administrator enforce computer and Internet use policies.

- **Traffic Scan.** This component prevents malware from being downloaded to the endpoint by scanning incoming emails and web traffic in real time. Outgoing emails are scanned to prevent malware from infecting other endpoints.
- **Application Blacklisting.** This component prevents access to unauthorized applications in your company. The administrator is responsible for creating rules for the allowed applications in the organization.
- **Web Access Control.** This component protects you from accessing dangerous websites based on administrator-defined rules.
- **Data Protection.** This component prevents unauthorized disclosure of sensitive data based on administrator-defined rules.
- **Antiphishing.** This component automatically blocks known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters.

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

Firewall

The firewall protects you while you are connected to networks and the Internet by filtering connection attempts and blocking suspicious or risky connections.

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

Device Control

It allows preventing sensitive data leakage and malware infections via external devices attached to endpoints, by applying blocking rules and exclusions via policy to a vast range of device types. The administrator is responsible for managing permissions for the following types of devices:
- Bluetooth Devices
- CDROM Devices
- Floppy Disk Drives
- IEEE 1284.4
- IEEE 1394
- Imaging devices
- Modems

- Tape Drives
- Windows Portable
- COM/LPT Ports
- SCSI Raid
- Printers
- Network Adapters
- Wireless Network Adapters
- Internal and External Storage

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

Application Control

The Application Control module blocks unauthorized applications and processes from running on the endpoint. Application Control decreases the frequency and impact of malware incidents, reducing the attack surface and vulnerabilities by controlling the number of unwanted applications in your network.

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

Sandbox Analyzer

The Sandbox Analyzer module provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not yet signed by Bitdefender antimalware engines. Sandbox Analyzer employs an extensive set of proprietary technologies to execute payloads in a contained virtual environment hosted by Bitdefender, analyze their behavior and report any subtle system changes that is indicative of malicious intent.

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

Volume Encryption

The Volume Encryption module allows you to provide full disk encryption by managing BitLocker on Windows machines. You can encrypt and decrypt boot and non-boot volumes, with just one click, while GravityZone handles the entire

process, with minimal intervention from the users. Additionally, GravityZone stores the recovery keys needed to unlock volumes when the users forget their passwords.

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

EDR Sensor

The EDR (Endpoint Detection and Response) Sensor collects, handles and reports endpoint and application behavior data. Some of the information is processed locally, while a more complex set of data is reported to a backend component of GravityZone.

The module generates a small footprint when it comes to network bandwidth usage and hardware resource consumption.

> **Note**
> This module is not available for Bitdefender Endpoint Security Tools for Windows Legacy.

1.4. Actions Menu

To define or run a scan task, click the **Actions** button ◎ to open the **Actions** menu. This is where you can also check for updates.
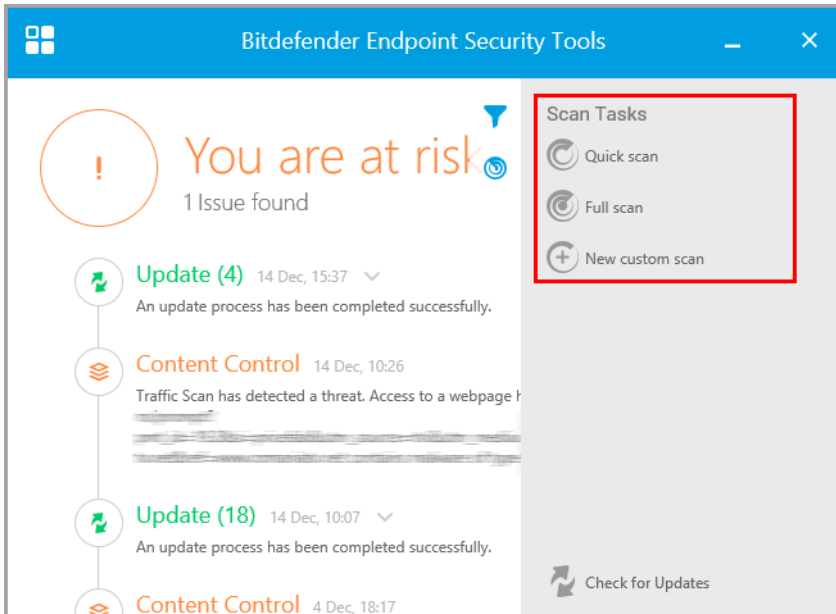
Actions Menu

Quick Scan
Uses in-the-cloud scanning to detect malware running in your system. Running a quick scan usually takes less than a minute and uses a fraction of the system resources of a regular virus scan.

Full Scan
Checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

Custom Scan
Allows you to choose the locations to scan and to configure scan options.

Check for updates

If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the update settings configured by you network administrator.

2. SCANNING FOR MALWARE

The main objective of Bitdefender Endpoint Security Tools is to keep your computer free of malware. It does that primarily by scanning in real time accessed files, e-mail messages and any new files downloaded or copied to your computer. Besides real-time protection, it also allows running scans to detect and remove malware from your computer.

You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). Scan tasks specify the scanning options and the objects to be scanned. If you want to scan specific locations on your computer or to configure the scan options, configure and run a custom scan.

At any point during the scan, you can see the progress in the **Events** timeline.

2.1. Scanning a File or Folder

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned and select **Scan with Bitdefender Endpoint Security Tools**. The scan will starts and you can monitor the progress on the **Events** timeline.

At the end of the scan, you will see the result. For detailed information, click **View Log**.

2.2. Running a Quick Scan

Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a quick scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

Quick Scan is preconfigured to allow scanning:

- Running processes, boot sectors and registry.
- Critical memory regions
- Only new and changed files
- For rootkits, adware, spyware and dialer applications in critical OS paths such as: `%windir%\\system32\\`, `%temp%`, `/etc`, `/lib`.
- For Potentially Unwanted Applications (PUA).

To run a quick scan, follow these steps:

1. Open the Bitdefender Endpoint Security Tools window.

2. Click the **Actions** button on the upper-right corner.

3. Click **Quick Scan**.

4. Wait for the scan to complete. You can see the progress of the scan in the timeline. Once complete, click **View Log** to see detailed results.

2.3. Running a Full Scan

The **Full Scan** task scans the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

> **i Note**
> Because **Full Scan** performs a thorough scan of the entire system, the scan may take a while. Therefore, it is recommended to run this task when you are not using your computer.

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a custom scan. For more information, please refer to "Configuring and Running a Custom Scan" (p. 13).

Before running a full scan, make sure Bitdefender Endpoint Security Tools is up-to-date with its malware signatures. Scanning your computer using an outdated signature database may prevent Bitdefender Endpoint Security Tools from detecting new malware found since the last update. For more information, please refer to "Updates" (p. 21).

Full Scan is configured to allow scanning:

● Running processes, boot sectors and registry.

● Email archives and network files from all drives, including removable ones.

● For rootkits, adware, spyware, keylogger and dialer applications, on all drives, including removable ones.

● For Potentially Unwanted Applications (PUA)

● Browser cookies

To run a full scan, follow these steps:

1. Open the Bitdefender Endpoint Security Tools window.

2. Click the **Actions** button on the upper-right corner.

3. Click **Full Scan**.

4. Wait for the scan to complete. You can see the progress of the scan in the timeline. Click **View Details** to see the details of the scan in progress. You can also pause, postpone or stop the scan.

5. Bitdefender Endpoint Security Tools will automatically take the recommended actions on detected files. Once complete, click **View Log** to see detailed results.

2.4. Configuring and Running a Custom Scan

To configure a scan for malware in detail and then run it, follow these steps:

1. Open the Bitdefender Endpoint Security Tools main window.

2. Click the **Actions** button on the upper-right corner.

3. Click **New Custom Scan**. The **Custom Scan** window will open.

4. Configure the scanning options: **Aggressive**, **Normal**, **Permissive**, **Custom**. Use the description below the option to identify the scan level that better fits your needs.

5. Select the target of the scan on the left-side pane.

6. You can also configure the scan to run the task with low priority by selecting the corresponding check box. This decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.

   After configuring the custom scan, you can save it as a favourite. To do this, enter a name and click the **Favourite** button .

Advanced users might want to take advantage of the scan settings Bitdefender Endpoint Security Tools offers. To configure the scan options in detail, click **Custom** and then **Settings**.

Alternately, you can configure and run a custom scan by using the product command line utility. For details, refer to the "Using the Command Line Interface" (p. 24) chapter.

2.4.1. File Types

On the **File types** tab, specify which types of files you want to be scanned. You can set the security agent to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous.

Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan. Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt;
accdu; acl; acr; action; ade; adp; air; app; as; asd; asp;
awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl;
csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm;
dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv;
hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar;
js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr;
mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg;
msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg;
ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg;
pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox;
rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm;
snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe;
vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf;
xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx;
xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

Scan options for archives

Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

Scan email archives

Select this option if you want to enable scanning of email message files and email databases, including file formats such as `.eml`, `.msg`, `.pst`, `.dbx`, `.mbx`, `.tbb` and others.

2.4.2. What to Scan?

On the **Scan** tab, select the corresponding check boxes to enable the desired scan options.

Scan boot sectors

You can set Bitdefender Endpoint Security Tools to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

Scan for rootkits

Select this option to scan for rootkits and hidden objects using such software.

Scan memory

Select this option to scan programs running in your system's memory.

Scan registry

Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.

Scan for keyloggers

Select this option to scan for keylogger software.

Scan for Potentially Unwanted Applications (PUA)

A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

Scan only new and changed files

By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

Scan cookies

Select this option to scan the cookies stored by browsers on your computer.

2.4.3. What to Do?

On the **Actions** tab, set the action to be taken on the detected files, if any.

Infected files
> Files detected as infected match a malware signature in the Bitdefender Malware Signature Database.

Suspect files
> Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available.

Rootkits
> Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

Take Proper Actions

Depending on the type of detected files, one or several of the following options are available:

Delete
> Removes detected files from the disk.
> If infected files are stored in an archive together with clean files, Bitdefender Endpoint Security Tools will attempt to delete the infected files and reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid loosing clean files.

Ignore
> No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.

Move to quarantine
> Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

Disinfect
> Removes the malware code from the infected file and reconstruct the original file.

2.5. Checking Scan Logs

Each time you perform a scan, a scan log is created. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the main window, once the scan is completed, by clicking **View Log**.

To check scan logs at a later time, follow these steps:

1. Open the Bitdefender Endpoint Security Tools main window.

2. Click the **Filter** button to open the **Filters** menu.

3. Click the **Antimalware** button. Here you can find all malware scan events, including threats detected by on-access scanning, recent scans, user-initiated scans and status changes for automatic scans.

4. Click an event to view details about it.

5. To open the scan log, click **View Log**. The scan log will be displayed.

3. USING VOLUME ENCRYPTION

The Volume Encryption module provides full disk encryption on your Windows system through policies applied by your security administrator.

3.1. Encrypting Your System

When an encryption policy is applied to your Windows system:

1. A configuration window prompts you to enter either:

    ●   A personal identification number (PIN) if the system has a Trusted Platform Module (TPM) chip (like newer laptops).

        > **i** **Note**
        > If your system has a functional TPM, your security administrator can configure such a policy that encrypts the volumes automatically, without requiring PIN.

    ●   A password if the system does not have a Trusted Platform Module (TPM) chip. The password is also required when the TPM is not functional or detected by Bitdefender Endpoint Security Tools.

Volume Encryption   _ ×
Set encryption password
Configure an EN-US password. You will need it to boot the operating system or to unlock the volume.
Encryption is a one time process and you can continue working as usual.
Enter your encryption password for volume C:. You will need this password to unlock your volume.
Choose password: [ ]
Retype password: [ ]
Password requirements:
● Have at least 8 characters
● Should contain upper and lower case
● Should contain a number
Dismiss   Save

2. Click the **Save** button. The encryption process starts immediately, first on the boot volume.

   You can postpone encryption by clicking **Dismiss**. However, the window will reappear after a while, prompting you to configure an encryption PIN or password.

You need a single PIN or password to encrypt all volumes, boot and non-boot, on fixed disks, on desktop systems and laptops. Removable disks are not encrypted. For details about configuring the encryption PIN or password, refer to this KB article.

After encryption, you may have to enter the PIN or the password each time Windows starts, in a pre-boot authentication screen, depending on the security policy applied to your system.

If you forget the encryption PIN or password, contact your security administrator.

3.2. Decrypting Your System

When a decryption policy is applied, the encrypted disks are automatically decrypted, without requiring any input from you. However, you cannot decrypt the system on your own, as long as an encryption policy is active.

3.3. Checking the Encryption Status

This is how you check the encryption status on your system:

1. In the system tray, double-click the ![B icon] icon to access the Bitdefender Endpoint Security Tools user interface.

2. In the upper-right corner, click the ![Modules button] button to open the **Modules** window.

3. Go to the **Volume Encryption** section, where you can view which volumes are encrypted and which are not.
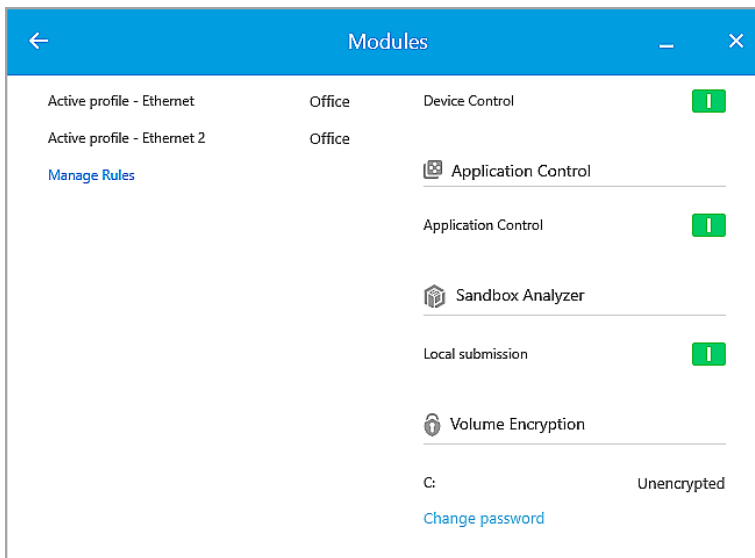
3.4. Changing the Encryption PIN or Password

This is how you change the encryption PIN or password:

1. Click the encrypted disk name in the main window of Bitdefender Endpoint Security Tools user interface.

2. Click the **Change password** option.

3. In the configuration window, enter the new PIN or password.

4. Click the **Save** button.

4. UPDATES

In a world where cyber criminals constantly try to come up with new ways to cause harm, having an up-to-date security program is essential if you are to stay one step ahead of them.

If you are connected to the Internet through broadband or DSL, Bitdefender Endpoint Security Tools takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that.

> **Note**
> The default automatic update frequency may be changed by your network administrator.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update Bitdefender by user request. For more information, please refer to "Performing an Update" (p. 22).

4.1. Types of Updates

Updates come in the following forms:

● **Updates for the malware signatures** - as new threats appear, the files containing malware signatures must be updated to ensure permanent up-to-date protection against them.

● **Product updates** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance.

   A product upgrade is a major version release.

4.2. Checking If Your Protection Is Up-to-Date

To check if your protection is up-to-date, follow these steps:

1. Right-click the Bitdefender Endpoint Security Tools icon in the system tray and choose **About**.

2. You can see the update status and the time of the most recent update check and update installation.

For detailed information about the latest updates, check the update events:

1. In the main window, click the **Filter** button to open the **Filters** menu.

2. Click the **Update** button. The latest updates will be displayed in the **Events** timeline.

   You can see when updates were initiated and information about them - whether they were successful or not, if they require a restart to complete the installation. If required, restart the system at your earliest convenience.

4.3. Performing an Update

In order to perform updates, an Internet connection is required.

To start an update:

● Double-click the Bitdefender Endpoint Security Tools icon in the system tray.

● Click the **Actions** button to open the **Actions** menu.

● Click **Check for updates**. The Update module will connect to the Bitdefender update server and it will check for updates.

● If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the update settings configured by you network administrator.

> **Important**
> If required, restart the system at your earliest convenience. We recommend doing it as soon as possible.

5. EVENTS

Bitdefender Endpoint Security Tools displays a detailed log of events concerning its activity on your computer, including computer activities monitored by Content Control and applications blocked by Application Control. The **Events** timeline in an important tool in monitoring your Bitdefender protection. For instance, you can easily check if an update was successfully performed, if malware was found on your computer etc. To check the events log, follow these steps:

1. Open the Bitdefender Endpoint Security Tools main window.

2. All events are displayed in the **Events** timeline.

3. Click the **Filter** button to open the **Filters** menu.

4. Select the event category from the menu. Events are grouped into the following categories:
   ● **General Settings**
   ● **Antimalware**
   ● **Firewall**
   ● **Update**
   ● **Content Control**
   ● **Device Control**
   ● **Application Control**
   ● **Sandbox Analyzer**
   ● **Volume Encryption**

Each event relates with the following information: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred. To see detailed information about a particular event in the list, click **View Log**.

You can also filter events by their importance to the protection level. There are three types of events:

indicates successful operations.

indicates non-critical issues.

indicates critical issues.

Some of the critical and non-critical issues displayed in the **Events** timeline are associated with the recommended actions in order to fix them.

6. USING THE COMMAND LINE INTERFACE

Bitdefender Endpoint Security Tools allows you to automatically run local on-demand scanning tasks and updates by using the Product Console, a command line interface found in the product installation folder on your Windows machines.

The BEST command line interface has two working modes:

- **Multiple commands at once**. This mode uses own command line interface and allows you to enter commands and receive results until you exit.

  To access this mode:
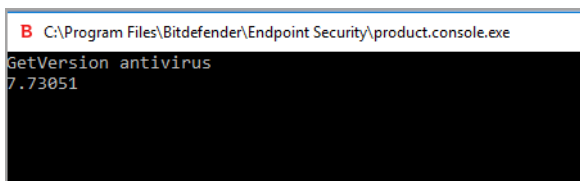
  1. Go to `c:\Program Files\Bitdefender\Endpoint Security` or to the folder where BEST was installed.

  2. Find and double-click the **product.console** executable. The command line interface opens up.

  3. Execute the desired command.

     Example:

     ```
     GetVersion antivirus
     ```

     The returned result represents the version number of the antimalware signatures.

  4. Execute `exit` to close the command line interface.

- **One command at a time**. This mode uses the Command Prompt and returns to the system prompt after the command is executed.

  To access this mode:
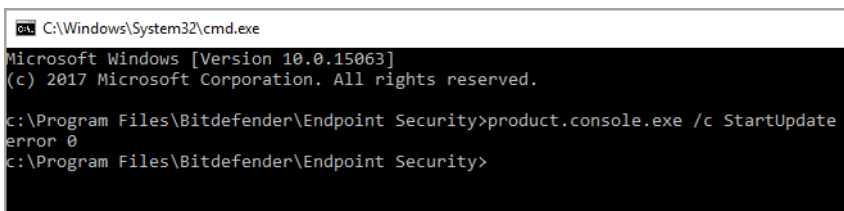
  1. Open Command Prompt (`cmd.exe`).

2. Use the `cd` command to navigate to the Bitdefender Endpoint Security Tools installation folder.

3. Execute the desired command.

   Example:

   ```
   C:\Program Files\Bitdefender\Endpoint Security>
            product.console.exe /c StartUpdate
   ```

4. If the command is succesfully executed the returned result is `error  0`.

6.1. Supported Commands

The command line interface supports several commands, some of them requiring parameters to return valid results.

All examples in this section are given using the Product Console from the BEST installation folder.

GetUpdateStatus `product|antivirus`

Retrieve information about the last update(s).

This command requires one of the these parameters:
- `product` – refers to the BEST version.
- `antivirus` – refers to the version of the antimalware signatures.

Example:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetUpdateStatus product
lastSucceededTime: 1504513705
lastAttemptedTime: 1504513705
lastError: 0
GetUpdateStatus antivirus
lastSucceededTime: 1505739144
lastAttemptedTime: 1505739144
lastError: 0
```

GetVersion `product|antivirus`

Retrieve information about the product's current version.

This command requires one of these parameters:
- `product` – refers to the BEST version.
- `antivirus` – refers to the version of the antimalware signatures.

Example:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion product
6.2.24.938
GetVersion antivirus
7.73205
```

IsUpdateInProgress

Verify if a product update is in progress.

Output values:
- `true` - a product update is in progress.
- `false` - no product update is in progress.

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateInProgress
false
```

IsUpdateRestartNeeded

Verify if a machine requires a system restart after the update.

Output values:
- `true` - the machine requires a system restart after the update.
- `false` - the machines does not require a system restart after the update.

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateRestartNeeded
false
```

StartUpdate

Start an update and retrieve the result without waiting for the task to finish.

Example:

```
StartUpdate
```

Output format: `error  0` (the command has been executed successfully)

`FileScan.OnDemand.RunScanTask` custom [option]

Starts an on-demand scan and displays the path to the scan log and the summary of the scan.

This command requires the parameter `custom`, followed, if needed, by one or more options. For example:

With options, you can customize a scanning task. These options are not mandatory.

Each option has two or more available values, but you can use only one value.

When the `FileScan.OnDemand.RunScanTask` command does not specify any option, the custom scan takes into account the default value of that option. For example, if you run this command without mentioning the `scanKeyloggers` option, that means Bitdefender Endpoint Security Tools will still scan for keyloggers, according to the `scanKeyloggers` default value (`true`).

> **ⓘ Note**
>
> There are not specific commands for **Quick scan** or **Full scan**. However, you can configure `FileScan.OnDemand.RunScanTask` to scan either only the OS location or the entire system, with all options enabled, as needed.

Options

```
path="<path>"
```
Enter the path of the scan target location. For multiple paths use: `path="<path1>" path="<path2>"`.

Example:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program
         Files"
```

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505746495_1_01.xml
Scanned items: 74074
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

```
infectedAction1=ignore|disinfect|disinfectOnly|delete|quarantine
```
Select the first action taken when an infected file is detected: ignore, disinfect, delete or move it to quarantine. You can use this action together with `infectedAction2`.

Default value: `disinfect`

Example:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" infectedAction1=ignore
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505813252_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

```
infectedAction2=ignore|disinfect|disinfectOnly|delete|quarantine
```
Select the second action taken when an infected file is detected, if the first action fails.

Default value: `quarantine`

Example:

```
FileScan.OnDemand.RunScanTask custom infectedAction1=disinfect infectedAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505824102_1_01.xml
Scanned items: 500139
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`suspiciousAction1=ignore|delete|quarantine`

Select the first action to take when a suspicious file is detected. You can use this action together with `suspiciousAction2`.

Default value: `ignore`

Example:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" suspiciousAction1=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505824920_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`suspiciousAction2=ignore|delete|quarantine`

Select the second action taken when a suspicious file is detected, if the first action fails.

Default value: `ignore`

Example:

```
FileScan.OnDemand.RunScanTask custom path="C:\Users" suspiciousAction1=delete suspiciousAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505825170_1_01.xml
Scanned items: 54455
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanBootSectors=true|false`

Scan the boot sectors of your hard disk.

Default value: `false`

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanBootSectors=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073447_1_01.xml
Scanned items: 416206
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRegistry=true|false

Scan the registry keys on your machine.

Default value: `false`

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRegistry=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073099_1_01.xml
Scanned items: 419060
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanMemory=true|false

Scan the programs running in your system's memory.

Default value: `false`

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanMemory=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506072517_1_01.xml
Scanned items: 427016
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom scanMemory=true
```

smartScan=true|false

Scan only new and changed files.

Default value: `true`

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom smartScan=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506070911_1_01.xml
Scanned items: 1614889
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRootKits=true|false

Scan for rootkits and hidden objects using such software.

Default value: `false`

Example:


```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRootKits=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506070601_1_01.xml
Scanned items: 416548
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanKeyloggers=true|false

Scan for keylogger software.

Default value: `true`

Example:


```
FileScan.OnDemand.RunScanTask custom scanKeyloggers=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanPUA=true|false

Scan Potentially Unwanted Applications (PUA).

Default value: `false`

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe

FileScan.OnDemand.RunScanTask custom scanPUA=true
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanArchives=true|false`

Scan for infected files inside archives.

Default value: `true`
Example:

```
FileScan.OnDemand.RunScanTask custom scanArchives=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`extensionType=all|application|custom|none`

Scan files depending on their extension: all files, only executable files, only files with the extensions you want or do not scan any file.

Default value: `all`

Example:

```
B  C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom extensionType=application
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`customExt="<string>"`

This option helps you scan only the files with the extensions you want. It requires a string with each extension between vertical bars (such as

"|exe|ini|txt|"). This option is valid only together with the option `extensionType=custom`.

Example:

`lowPriority=true|false`
Run the task with low priority.

Default value: `false`

Example:

These options are an alternative to the options available in BEST console. For more information refer to "Configuring and Running a Custom Scan" (p. 13).

6.2. Command Line Error Codes

The command line utility may return the following error codes:

Error code	Description
0	Command executed successfully.
87	Invalid Parameter.

Error code	Description
160	Bad Arguments.
1627	Function Failed – an error occurred while executing the command.

7. GETTING HELP

For any problems or questions concerning Bitdefender Endpoint Security Tools, please contact your network administrator.

To find product and contact information, right-click the Bitdefender Endpoint Security Tools icon in the system tray and select **About** to open the **About** window.

Glossary

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Antivirus storm

An intensive use of system resources that occurs when antivirus software simultaneously scans multiple virtual machines on a single physical host.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Bootkit

A bootkit is a malicious program having the ability of infecting the master boot record (MBR), volume boot record (VBR) or boot sector. The bootkit remains active even after a system reboot.

Browser

Short for Web browser, a software application used to locate and display Web pages.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Downloader

It is a generic name for a program having a primary functionality of downloading content for unwanted or malicious purposes.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

Exploit
> An exploit generally refers to any method used to gain unauthorized access to computers or a vulnerability in a system's security that opens a system to an attack.

False positive
> Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension
> The portion of a filename, following the final point, which indicates the kind of data stored in the file.
>
> Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Grayware
> A class of software applications between legitimate software and malware. Though they are not as harmful as malware which affects the system's integrity, their behavior is still disturbing, driving to unwanted situations such as data theft and unauthorized usage, unwanted advertising. Most common grayware applications are spyware and adware.

Heuristic
> A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP
> Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Keylogger
> A keylogger is an application that logs anything you type.
>
> Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they

are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Malware signature

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware. Signatures are also used to remove the malware code from infected files.

The Bitdefender Malware Signature Database is a collection of malware signatures updated hourly by the Bitdefender malware researchers.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Password stealer

A password stealer collects pieces of data that can be account names and associated passwords. These stolen credentials are then used for malicious purposes, like account takeovers.

Phishing

The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to

visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Ransomware

A malware that locks you out of your computer or blocks access to your files and applications. Ransomware will demand that you pay a certain fee (ransom payment) in return for a decryption key that allows you to regain access to your computer or files.

Report file

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Suspicious files and network traffic

Suspicious files are those with a doubtful reputation. This ranking is given by many factors, among which to name: existence of the digital signature, number of occurrences in computer networks, packer used, etc. Network traffic is considered suspicious when it deviates from the pattern. For example, unreliable source, connection requests to unusual ports, increased bandwidth usage, random connection times, etc.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

Targeted attacks

Cyber-attacks that mainly aim financial advantages or denigration of reputation. The target can be an individual, a company, a software or a system, well studied before the attack takes place. These attacks are rolled out over a long period of time and in stages, using one or more infiltration points. They are hardly noticed, most times when the damage has already been done.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.