USER'S GUIDE

Bitdefender® CONSUMER SOLUTIONS

Parental Control

Bitdefender Parental Control

User's Guide

Publication date 04/29/2024

Legal Notice

Bitdefender

Table of Contents

About This Guide 1
Purpose and Intended Audience 1
How to Use This Guide 1
Conventions used in This Guide 1
Typographical Conventions 1
Admonitions 2
Request for Comments 2
1. Getting Started 3
1.1. Setting up Parental Control 3
1.2. Installing Bitdefender Parental Control on your child's devices 4
1.2.1. On Windows devices: 4
1.2.2. On macOS devices: 4
1.2.3. On Android devices: 5
1.2.4. On iOS devices: 6
2. Features & Functionalities 8
2.1. Profiles 8
2.2. Statistics 9
2.3. Parental PIN Code 10
2.3.1. Forgot the PIN Code? 10
2.3.2. Changing your PIN Code 10
2.4. Content Filtering 11
2.4.1. Safe Search & YouTube Restrictions 11
2.4.2. Blocking & Allowing Website Categories 12
2.4.3. Exceptions 12
2.5. Daily Internet Time 13
2.5.1. Reward system 13
2.6. Turning off the Internet on your Child's device 14
2.7. Routines 15
2.7.1. Set up routines 15
2.8. Tracking your Child's Location 16
3. Uninstalling Parental Control 18
4. Getting Help 19
4.1. Asking for Help 19
4.2. Online Resources 19
4.2.1. Bitdefender Support Center 19
4.2.2. The Bitdefender Expert Community 20
4.2.3. Bitdefender Cyberpedia 20
4.3. Contact Information 20
4.3.1. Local distributors 21

Glossary **22**

ABOUT THIS GUIDE

Purpose and Intended Audience

This guide is intended to all Bitdefender users who have chosen Bitdefender Parental Control as their go-to solution for the safety, monitoring and continuous protection of their children's devices and online presence.

You will find out how to install, configure and make the best of Bitdefender Parental Control, for enhanced features and a better control over your child’s online activities.

We wish you a pleasant and useful lecture.

How to Use This Guide

This guide is organized around several major topics:

Getting Started

Get started with setting up your Bitdefender Parental Control.

Features & Functionalities (page 8)

Learn how to use Bitdefender Parental Control and all of its features.

Getting Help (page 19)

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

Conventions used in This Guide

Typographical Conventions

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

Appearance	Description
sample syntax	Syntax samples are printed with monospaced characters.
https://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
documentation@bitdefender.com	Email addresses are inserted in the text for contact information.
About this Guide (page 1)	This is an internal link, towards some location inside the document.
filename	File 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.

Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an email to documentation@bitdefender.com. Write all of your documentation-related emails in English so that we can process them efficiently.

1. GETTING STARTED

We will start off with an in-depth, step-by-step guide on how to set up Bitdefender Parental Control subscription on your Bitdefender central account. This is the first step in the straightforward process that is required in order to ensure you can manage and monitor the online activities of your children effectively.

1.1. Setting up Parental Control

Upon activating your subscription, in order to start setting up Bitdefender Parental Control on your account:

1. Go to your Bitdefender Central account and access the **Parental Control** tab on the left side of the screen.
2. Click on **Get started**.
3. Set an application PIN.

   > **Note**
   > This pin code will help prevent your children from disabling parental control features on their own by logging out from their child application.
   >
   > Make sure you remember this PIN.

4. Click **Next**.
5. Proceed by creating a child profile. Type in the child's name and select a profile picture. Then click **Next**.
6. Select the age that corresponds with that of your child. Once done, click **next**.
7. Indicate whether the Parental Control app is to be installed on the current device you are using or another device.

Note

If you select **Other devices** you'll be presented with three installation options. Select the preferred method:

- By scanning the QR code.
- By copying the provided link and opening it in the child's device browser.
- By sending the installation link via email.

8. Wait for the download to complete, and then run the installer on the device in question.

From here, the installation process will begin. The steps that need to be taken from here vary based on the type of device and operating system on which the installation is being conducted.

1.2. Installing Bitdefender Parental Control on your child's devices

1.2.1. On Windows devices:

Once you run the newly downloaded installer:

1. Click **Yes** if a User account control dialogue prompts you to allow the installation file to make changes to the device.
2. Sign in with your Bitdefender Central account credentials if prompted.

1.2.2. On macOS devices:

Once the download of the installer is finished, double-click the Bitdefender file in order to start the installation process:

1. You will be guided through the steps necessary to install Bitdefender Parental Control for macOS. Click on **Allow** if prompted.
2. Click on the two consecutive **Continue** buttons.
3. To continue the installation, you will have to agree to the terms of the software subscription agreement.
4. Click on **Continue**. After that, click on **Install**.

5. When prompted, input an administrator name and password, then press the **Install Software** button.

Wait until you receive a pop-up notification that *a system extension has been blocked*. This is a natural occurrence during this procedure. To continue, you must allow the Parental Control system extension as per the instructions below:

1. Click on the **Open System Settings** button.

> **Note**
> On earlier macOS version, this button is referred to as **Open Security Preferences**.

2. Click the **Allow** button in the windows that appears on the screen, then input an administrator name and password to unlock the settings.

> **Note**
> On macOS 11 (Big Sur) and macOS 12 (Monterey), before you can click the **Allow** button you'll need to first click the padlock icon in the bottom left corner of the **Security & Privacy** window, then input an administrator name and password to make changes.

3. The **Filter Network Content** pop-up will appear. Click the **Allow** button within this window.
4. Next, click on the **Open System Settings** button.
5. Click the **Allow** button one more time.

1.2.3. On Android devices:

You will find Bitdefender's Google Play Store page for the Parental Control application:

1. Tap the **Install** button. The app will start downloading and installing.
2. Once the installation is complete, you will see an **Open** button. Tap on it to launch the Bitdefender Parental Control application.

After opening the application, follow the onscreen steps to set up Parental Control on your child's Android device:

1. Tap **Continue**.
2. Sing in to the app using your Bitdefender Central account credentials.

3. Select the child profile you want to assign to the Android device.
4. You will need to grant the necessary permissions for the app in order for it to function properly. To do that, Tap **Next**, then:
   a. Allow VPN access, then choose **Allow all the time** to filter online content on your child's device.
   b. To help locate your child's Android device, tap **Next**, then **Allow** and choose the **Allow all the time** option.
   c. Both VPN and Location permissions will display a green check mark. Tap **Finish setup** and then tap **Next**.
   d. At this point, there are 3 more permissions to block internet access and apps on the child's device. Tap **Set permission** on the **Device Administrator Rights** panel.
   e. Tap the **Finish** button once you're done setting up the Bitdefender Parental Control app.

1.2.4. On iOS devices:

You will find Bitdefender's App Store page for the Parental Control application:

1. Tap the cloud icon with an arrow pointing down. The application will start downloading and installing.
2. Once the installation is complete, you will see an **Open** button. Tap on it to launch the Bitdefender Parental Control app.
3. If any Mobile Device Management profiles are found on the child's iOS device, you will be asked to remove them. Tap **Next** and choose **Remove Profiles**.
4. In the iOS **Settings** app, go to **General**, then scroll down and tap on the **VPN & Device Management** section.
5. Tap on each entry in the **MOBILE DEVICE MANAGEMENT** section and choose **Remove Management** for each one.
   Repeat this process until there are no more MOBILE DEVICE MANAGEMENT entries left.

Reopen the app installed on the child's device and follow the onscreen steps to set up Bitdefender Parental Control:

1. Tap **Continue**.
2. Sign in to the app using your Bitdefender Central account credentials.
3. Select the child profile you want to assign to the iOS device.
4. You will then need to grant the necessary permissions for the application to function properly. Tap **Next**.
5. Allow VPN access in order to filter online content on your child's device. Tap **Allow** twice in a row in order to add the VPN configurations.
6. Tap **Next**, then choose **Allow** to help locate your child's iOS device.
7. Then go through the process of setting up Apple Family Control to block internet access and apps on the child's device.

> **Note**
> You can tap on **Learn how** for a step-by-step guide on how to do that.

8. After configuring Apple Family Control on your own device and on your child's device, select I **have configured Apple Family Control** in order to continue.
9. Then, allow Screen Time Access to filter online content on your child's iOS device.
10. Tap on **Finish setup**.

.

After finishing these steps on your child's device(s), the setup process is complete. As a parent, you can now monitor your child's online activities and view usage statistics in your Bitdefender Central account, within the Parental Control dashboard, which we will detail in the following chapters.

2. FEATURES & FUNCTIONALITIES

2.1. Profiles

A child profile is a customized set of rules that enable the Bitdefender Parental Control app to manage and monitor a child's online activities. It includes settings tailored to the child's age, such as content filters and time restrictions. Using the Bitdefender Central account parents can create, edit, and delete these profiles, as well as assign and remove devices to them, ensuring a safe and appropriate online experience for their children.

To create a Child Profile:

1. Go to Bitdefender Central and sign in to your account.
2. On the left-hand side menu, click on the **Parental Control** tab.
3. Click on **New profile** to create a new child profile.
4. Enter the child's details name, profile picture, and date of birth.

> **Note**
> Based on the child's age, Bitdefender automatically blocks certain categories such as chat, social networks, explicit content, and more. You can adjust blocked categories later.

5. Click the **Save** button.

The new profile is now created and will appear on the page.

To edit a Child Profile:

1. Click the **View details** button from the child's profile.
2. To modify your child's profile go to **Edit profile**.
3. Use the corresponding field to change the child's name, birthday and/or profile picture.
4. Click on **Save changes** after altering the necessary details.

To delete a Child Profile:

1. Click the **View details** button from the child's profile.
2. Go to **Edit profile**.

3. Click on the **Delete profile** button and confirm the deletion.

To assign devices to a Child Profile:

If your child has multiple devices (Windows, macOS, Android or iOS) you can assign them to the same child profile.

1. Click the **View details** button from the child's profile.
2. Click on the number of devices listed under their name.
3. Click on the **Assign devices** button.
4. Select the device name and then click the **Assign** button.

> **Note**
> If the device is not visible in the list, click on **Install a new device** then follow the on-screen instructions to install and set up Bitdefender Parental Control on the new device.

To remove devices from a Child Profile:

When you remove a device from a child's profile, it means that the device will no longer be under the management of Bitdefender Parental Control. The rules and settings specified in the child's profile will no longer apply to that device. Although the Parental Control app remains installed on the device, it ceases to function.

1. Click the **View details** button from the child's profile.
2. Click on the number of devices listed under their name.
3. Locate the child's device and click the **Unassign device** option.
4. Press the **Yes, unnassign device** button to confirm the action.

2.2. Statistics

Parental Control provides insights into how children utilize the internet and their devices. In this guide, we'll delve into the various statistics available to parents in Bitdefender Central, empowering them to make informed decisions and ensure a safe and balanced online experience for their children.

In order to view the statistics:

1. Go to Bitdefender Central and sign in to your account.

2. Once logged in, click on **Parental Control** tab on the left-hand side menu.
3. Click on the profile of the child who's statistics you wish to view.

Upon selecting your child's profile, you will be directed to a dashboard displaying various statistics panels. All refer to the other features described further down in this documentation.

2.3. Parental PIN Code

The Parental PIN Code is a security feature within the Bitdefender Central platform's Parental Control dashboard. It serves as a means for parents to maintain control over their child's access to the Bitdefender Parental Control app installed on their devices. Below is a detailed guide on how to set, find, and manage your Parental PIN.

The Parental PIN code prevents unauthorized logouts from the Bitdefender Parental Control app on your child's device. When your child attempts to log out, they will be prompted to enter this PIN Code. It ensures that only you, as the parent with access to the Bitdefender Central account, can control the app's settings.

> **Note**
> When setting up the Parental Control app for the first time, you'll be asked to establish a 4-8 digit long Parental PIN.

2.3.1. Forgot the PIN Code?

In case you forget your Parental PIN Code, you can easily retrieve it from your Bitdefender Central account:

1. Go to Bitdefender Central and sign in to your account.
2. Once logged in, click on the **Parental Control** tab on the left-hand side menu.
3. In the top right corner of the page, click on **Pin code**.
4. Click the eye-shaped icon to find your Parental PIN Code.

2.3.2. Changing your PIN Code

If you suspect that your PIN code has been compromised or simply want to update it for security reasons:

1. Within the Parental Control section of your Bitdefender Central account, click on the **Pin code** option.
2. Choose the option **Change PIN** and follow the prompts on your screen to set a new PIN code.

2.4. Content Filtering

Content Filtering enables parents to restrict their child's access to online content, such that they can block entire categories of websites or make exceptions based on specific URLs or topics.

> **Note**
> Bitdefender Parental Control's Content Filtering feature does not stop your child from using applications of websites offline, as it only manages the online internet traffic of the devices they use.

To access Content Filtering:

1. Sign in to your Bitdefender Central account.
2. On the left-hand side menu, click on the **Parental Control** tab.
3. Go to your child's profile and click the **More** menu in the top right. Then, select **Content Filtering**.

2.4.1. Safe Search & YouTube Restrictions

In the **Privacy and Safety** section on the right side of the screen, you can enable the Safe Search and YouTube Restricted switches.

- **Safe Search:** When using search engines, Safe Search prevents the display of content deemed unsafe by Google in search results.
- **YouTube restricted:** Provides the child with age-appropriate videos on YouTube.

> **Note**
> **Safe Search** and **YouTube restricted** redirect all DNS requests from **google.com** to **safe.google.com**. The actual content filtering is done by Google. Bitdefender Parental Control does not filter content within Safe Search or Google. Similarly, YouTube may not effectively control tags on videos, potentially exposing children to inappropriate content.

2.4.2. Blocking & Allowing Website Categories

> **Note**
> In the **Categories** section, the types of websites your child can see online are allowed or blocked by default, depending on the age set when the child's profile was created.

You can block or allow various types of websites at any time:

1. Select a category.
2. To block access to this category, choose **Blocked** from the drop-down menu. To allow access, choose **Allowed**.

> **Important**
> If you block the **File Sharing** category for your child's profile, the macOS update won't work. We recommend temporarily allowing File Sharing when updating macOS.

2.4.3. Exceptions

In the **Exceptions** tab, website and application exclusions can be set:

- **Website exceptions:**
  1. Click on the **Add exception** button.
  2. Select **Website only** then click on the **Next** button.
  3. Type in the website address and select whether to allow or block it from the drop-down menu.
  4. Then click on the **Add** button.
- **App and web platform exceptions:**
  1. Click the **Add exception** button.
  2. Select **App and web platform** then click on the **Next** button.
  3. Choose the platform you wish to make an exception for from the provided list. Alternatively, use the search bar to find what you are looking for.
  4. Then click on the **Add** button.
- **Removing exceptions:**
  All exceptions that you set up will appear in Content Filtering within their designated list at the bottom.

To delete an exception, simply click on the trash icon located to the right of the entry.

2.5. Daily Internet Time

In your Bitdefender Central account under the Parental Control section, for each child profile created, there is a Daily Internet Time card displayed. This card shows the total time the child has spent online across all assigned devices. To limit a child's online time:

1. Go to the child profile and click the **Set time limit** button within the **Daily Internet Time** panel. Alternatively, you can click the **More** menu in the top right corner and select **Daily Internet Time**.
2. Click the **Enable time limit** button to activate this feature.

> **Note**
> By default, the child is given 1 hour and 30 minutes of internet access per day. If the parent doesn't extend this time limit, the child's internet access is stopped after reaching the 1 hour and 30-minute mark.

Removing Daily Time Limit:

- To turn off the Daily Internet time feature, go to your child's profile dashboard, click the **Edit time** button within the **Daily internet time** panel, then hit the **Pause** button in the **Time limit** panel.
- To remove the time limit for a particular day, click the ⊗ button corresponding to that day of the week in the **Schedule** panel.

Changing Time limit:

- To set a different time limit for a specific day of the week, click on the day's name in the **Schedule** panel, select the desired limit from the drop-down menu, and then click the **Save changes** button. You can select more than one day at a time.

2.5.1. Reward system

The **Reward** feature allows you to reward or extend screen time for your child, promoting healthy online habits. You can use the reward system in two different ways:

- **Manual reward:**

1. Navigate the the Parental Control section within your Bitdefender Central account.
2. Go to the child profile and click the **Reward** button within the **Daily Internet time** panel.
3. Select the amount of extra time you want to add and confirm by clicking **Reward**.

- **Child request:**
  When your child reaches the daily limit, they can request additional time through the Parental Control app installed on their mobile device. As a parent, you'll receive a notification in your Bitdefender Central account.

  1. When logged in to your Bitdefender Central account, look for a red dot on the notifications bell in the top right corner of the screen, indicating a pending request from your child.
  2. Review the request and decide how much extra time to grant.

  > **Note**
  > Children habe the option to request extentions to their daily internet time only on Android and iOS devices.

2.6. Turning off the Internet on your Child's device

As a parent, managing your child's internet usage can be important for their well-being and productivity. To temporarily disable internet access on your child's device using Bitdefender Parental Control:

1. Go to Bitdefender Central and sign in to your account.
2. Once logged in, click on the **Parental Control** tab on the left-hand side menu.
3. Select **View details** from the child's profile whose internet you wish to disable.
4. Click the **Stop internet** button in the upper right-hand corner of the child's dashboard

> **Note**
> Internet will be cut off on all your child's devices. This action overrides any existing Parental Control settings, such as routines, daily time limit or allowed categories.

5. While access to the internet is cut off, the **Stop internet** button is changed to **Resume internet**. To restore the internet access, simply click the **Resume internet** button.

2.7. Routines

Within Bitdefender Parental Control you can set up to 3 distinct routines to schedule when your child's internet access is turned off. They provide a structured approach to managing a child's online activities, promoting healthy habits and family engagement while ensuring their safety. These routines are independent of each other, meaning you can choose to activate just one, two, or all three of them according to your preferences:

- **Focus time**
  Create a schedule that includes time for homework, study, and other activities.
- **Bedtime**
  Use the Bedtime routine to lock out a resting period for your child.
- **Family time**
  Use the Family time routine to block out time for your child to be present during family meals for example.

> **Note**
> **Routines vs Daily Internet time:**
>
> During routines, the time spent online doesn't count toward the Daily Internet time limit. Once the routine ends, the Daily Internet Time function resumes counting the child's internet usage.
>
> To prevent confusion for parents, while a routine is in progress, the Daily Internet Time card won't be visible on the child's profile dashboard until the routine concludes. Instead, the name of the active routine will be displayed during this time.

2.7.1. Set up routines

To set up any of the parental control routines:

1. Go to Bitdefender Central and sign in to your account.
2. On the left-hand side menu, click on the **Parental Control** tab.
3. Go to the child profile and select a desired routine from the **More** menu.
4. Click the **Enable** button to activate the selected routine.
5. This will prompt the **Schedule** and **Internet access** panels to appear.
   - **Schedule:**
     To set a routine for one or multiple days of the week:
     a. Select the desired days.
     b. Select the start and end times for the routine from the drop-down menu provided.
     c. Finally, click the **Save changes** button to confirm your selections.

     To remove the routine for a particular day, click the ⊗ button corresponding to that day of the week.
   - **Internet access:**
     The Internet access panel within a routine offers two main functions to control a child's online activities during specific time frames:
     - **Complete Internet cutoff:** Parents have the option to completely disable internet access for their child during the scheduled routine time. By toggling off the **Internet access** switch, the child's devices will be unable to access the internet within the designated time frame.
     - **Selective Category or Website:** Alternatively, parents can choose to allow internet access during routine hours but restrict certain websites or categories of content. When you toggle on the **Internet access** switch, two additional tabs, namely the **Categories** and the **Exceptions** tabs, become visible, giving you access to further Content Filtering (page 11) settings.

2.8. Tracking your Child's Location

With the prevalence of smartphones and other mobile devices, tracking your child's location has become an essential tool for many families.

Whether it’s knowing their whereabouts after school or during outings with friends, having the ability to monitor their location provides peace of mind for parents. Here’s a step-by-step guide on how to track your child’s location using Bitdefender Parental Control’s Location feature.

1. Go to Bitdefender Central and sign in to your account.
2. Once logged in, click on **Parental Control** on the left-hand side menu.
3. If you have multiple children, select **View details** from the child's profile whose location you wish to track.
4. Within the Location panel, select the Android or iOS device you want to track, then click on the **Locate** button.

   Note
   The Location feature in Bitdefender Parental Control is unavailable for Windows and macOS devices.

5. After a short wait, a red pin will indicate your child's current location on the map.

   Note
   Location updates occur every 20 minutes. If you attempt to track your child’s location in less than 20 minutes since the previous locate, the location displayed may not reflect their whereabouts in real-time.

3. UNINSTALLING PARENTAL CONTROL

Uninstalling Bitdefender Parental Control on Windows devices:

1. Remove the device from your child's profile within Bitdefender Central.
2. Open the Control Panel on the device in question and locate Bitdefender Parental Control in the **Programs and Features** list.
3. Uninstall Bitdefender Parental Control.

Uninstalling Bitdefender Parental Control on macOS devices:

1. Remove the device from your child's profile within Bitdefender Central.
2. Open **Finder** on the macOS device.
3. Access your Applications and locate the Bitdefender folder.
4. Open it and run **Bitdefender Uninstaller**.
5. Choose Bitdefender Parental Control from the list of products to uninstall.
6. Provide Administrator credentials and wait for the uninstallation to finish.

Uninstalling Bitdefender Parental Control on Android and iOS devices:

1. Remove the device from your child's profile within Bitdefender Central.
2. Uninstall Parental Control from the mobile device like any other application or through Google Play Store or Appstore respectively.

4. GETTING HELP

4.1. Asking for Help

Bitdefender provides its customers with an unparalleled level of fast and accurate support. If you experience any issue or if you have any question about your Bitdefender product, you can use several online resources to find a solution or an answer.

4.2. Online Resources

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center:
  https://www.bitdefender.com/consumer/support/
- The Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

4.2.1. Bitdefender Support Center

The Bitdefender Support Center is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about threat prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Support Center is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Support Center, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Support Center is available any time at at the following address: https://www.bitdefender.com/consumer/support/.

4.2.2. The Bitdefender Expert Community

The Expert Community is an environment where Bitdefender users, enthusiasts and fans can engage, exchange ideas, support each other and share their knowledge and solutions. It is also a place of ideation and provides valuable feedback to our development teams. The community members are experienced Bitdefender users happy to help other peers on their own time.

Here you will find meaningful conversations with people that use Bitdefender on their devices. The community offers a true connection with our members and makes your voice heard. It is a place where you are encouraged to participate knowing that your opinion and input are respected and cherished. As a valued provider, we strive to offer an unparalleled level of fast, accurate support and we wish to bring our users closer to us. We have designed our community with this purpose in mind.

You can find our Expert Community webpage here:

https://community.bitdefender.com/en/

4.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia has all the info you need about the latest cyber-threats. This is the place where Bitdefender experts share tips & tricks about how to stay protected from hackers, data breaches, identity theft and social impersonation attempts.

The Bitdefender Cyberpedia webpage can be found here:

https://www.bitdefender.com/cyberpedia/.

4.3. Contact Information

Efficient communication is the key to a successful business. Since 2001 BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us directly through our **Bitdefender Support Center:**

https://www.bitdefender.com/consumer/support/

4.3.1. Local distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to https://www.bitdefender.com/partners/partner-locator.html.
2. Choose your country and city using the corresponding options.

GLOSSARY

Activation code

Is a unique key that can be bought from retail and used to activate a specific product or service. An activation code enables the activation of a valid subscription for a certain period of time and number devices and can also be used to extend a subscription with the condition to be generated for the same product or service.

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive webpages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the webpage. ActiveX controls are often written using Visual Basic. Active X is notable for a complete lack of security controls; computer security experts discourage its use over the internet.

Advanced persistent threat

Advanced persistent threat (APT) exploits vulnerabilities of systems to steal important information to deliver it to the source. Big groups such as organizations, companies, or governments, are targeted by this threat. The objective of an advanced persistent threat is to remain undetected for a long time being able to monitor and gather important information without damaging the targeted machines. The method used to inject the threat into the network is through a PDF file or an Office document that look harmless so that every user can run the files.

Adware

Adware is often combined with a host app that is provided at no charge as long as the user agrees to accept the adware. Because adware apps are usually installed after the user has agreed to a licensing agreement that states the purpose of the app, 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 apps collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

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 threat 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 threat to become active in memory. Every time you boot your system from that point on, you will have the threat active in memory.

Botnet

The term “botnet” is composed of the words “robot” and “network”. Botnets are internet-connected devices infected with threats and can be used to send spam emails, steal data, remotely control vulnerable devices, or spread spyware, ransomware, and other kinds of threats. Their objective is to infect as many connected devices as possible, such as PCs, servers, mobile or IoT devices belonging to big companies or industries.

Browser

Short for web browser, a software app used to locate and display webpages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. These are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Brute Force Attack

Password guessing attack used to break into a computer system by entering possible password combinations, mostly starting with the easiest-to-guess password.

Command line

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

Cookies

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.

Cyberbullying

When peers or strangers are committing abusive acts against children on purpose to physically hurt them. To damage emotionally, the assaulters are sending mean messages or unflattering photos, thus making their victims isolate from others or feel frustrated.

Dictionary Attack

Password guessing attacks used to break into a computer system by entering a combination of common words to generate potential passwords. The same method is used to guess decryption keys of encrypted messages or documents. Dictionary attacks succeed because many people incline to choose short and single words passwords that are easy to be guessed.

Disk drive

It's a machine that reads data from and writes data onto a disk. A hard disk drive reads and writes hard disks. A floppy drive accesses floppy

disks. Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

Email

Electronic mail. A service that sends messages on computers via local or global networks.

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.

Exploits

A way to take advantage of different bugs or vulnerabilities that are present in a computer (software or hardware). Thus, hackers may gain the control of computers or networks.

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.

Heuristic

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

Honeypot

A decoy computer system set to attract hackers to study the way they act and identify the heretical methods they use to collect system information. Companies and corporations are more interested in implementing and using honeypots to improve their overall state of security.

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.

Java applet

A Java program which is designed to run only on a webpage. To use an applet on a webpage, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the webpage is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from apps in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Keylogger

A keylogger is an app 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 threat that is encoded as a macro embedded in a document. Many apps, such as Microsoft Word and Excel, support powerful macro languages. These apps allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An email client is an app that enables you to send and receive email.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

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

Online predators

Individuals who seek to attract minors or adolescents into conversations on purpose to involve them into illegal sexual activities. Social networks are the ideal place where vulnerable children can easily be hunted and seduced into committing sexual activities, online or face-to-face.

Packed programs

A file in a compression format. Many operating systems and apps contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

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 website 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 website, however, is bogus and set up only to steal the user's information.

Photon

Photon is an innovative non-intrusive Bitdefender technology, designed to minimize the performance impact of your security solution. By monitoring your PC's activity in the background, it creates usage patterns that help optimize booting and scanning processes.

Polymorphic virus

A threat that changes its form with each file it infects. Since they have no consistent binary pattern, such threats 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

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. CryptoLocker, CryptoWall, and TeslaWall, are only some variants that hunt personal systems of users.

The infection can be spread by accessing spam emails, downloading email attachments, or installing apps, without letting the user know about what is happening on his system. Daily users and companies are targeted by ransomware hackers.

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 apps hide critical files using rootkits. However, they are mostly used to hide threats or to conceal the presence of an intruder into the system. When combined with threats, 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 apps 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 apps 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 threat 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 apps running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or apps can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

Subscription

Purchase agreement that gives the user the right to use a particular product or service on a specific number of devices and for a certain period of time. An expired subscription can be automatically renewed using the information provided by the user at the first purchase.

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.

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.

Threat

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

Threat Information Update

The binary pattern of a threat, used by the security solution to detect and eliminate the threat.

Trojan

A destructive program that masquerades as a benign app. Unlike malicious software programs and worms, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse threats is a program that claims to rid your computer of threats but instead introduces threats 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 feature that allows you to manually check for updates, or let it automatically update the product.

Virtual Private Network (VPN)

Is a technology that enables a temporary and encrypted direct connection to a certain network over a less secure network. This way, sending and receiving data is secure and encrypted, difficult to be caught by snoopers. A proof of security is the authentication, which can be done only using a username and password.

Worm

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