GUIA DO UTILIZADOR

Bitdefender CONSUMER SOLUTIONS

# VPN

# Bitdefender VPN

**Manual do Utilizador**

Publication date 02/07/2024
Copyright © 2024 Bitdefender

## Aviso Legal

**Todos os direitos reservados.** Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por quaisquer meios, eletrónicos ou mecânicos, incluindo fotocópias, gravação, ou qualquer sistema de ficheiros de informação, sem a permissão por escrito de um representante autorizado de BitDefender. A inclusão de pequenas frases do texto em comparativas poderão ser feitas desde que seja feita a menção da fonte da frase em questão. O conteúdo não pode ser de forma alguma modificado.

**Aviso e isenção de responsabilidade.** Este produto e a sua documentação são protegidos por direitos de autor. As informações neste documento são fornecidas "no estado em que se encontram", sem garantia. Embora todas as precauções tenham sido tomadas no preparação deste documento, os autores não terão qualquer responsabilidade perante qualquer pessoa ou entidade com relação a qualquer perda ou dano causado ou supostamente causado direta ou indiretamente pelas informações contidas neste trabalho.

Este livro contém links para Websites de terceiras partes que não estão baixo controlo da BitDefender, e a BitDefender não é responsável pelo conteúdo de qualquer site acedido por link. Se aceder a um site de terceiras partes mencionado neste manual, faz isso à sua própria conta e risco. A BitDefender fornece esses links apenas para facilitar, e a inclusão do link não implica que a BitDefender endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiras partes.

**Marcas comerciais.** Poderão aparecer marcas registadas neste livro. Todas as marcas comerciais registadas e não registadas neste documento são da exclusiva propriedade dos seus respetivos proprietários e são devidamente reconhecidas.

Bitdefender

# Índice

# SOBRE ESTE GUIA

## Propósito e público-alvo

Este guia destina-se a todos os Bitdefender utilizadores que escolheram Bitdefender VPN como o seu serviço de referência que lhes concede anonimato online ao encriptar todo o tráfego de entrada e saída no seu PC, Mac ou dispositivos móveis .

Descobrirá como configurar e utilizar o Bitdefender VPN para manter a sua identidade e atividades online protegidas contra hackers, ISPs e bisbilhoteiros. Aprenderá como obter o melhor com o Bitdefender.

Desejamos-lhe uma agradável e útil leitura.

## Como utilizar este guia

Este manual está organizado em diversos tópicos importantes:

O que é Bitdefender VPN (página 4)

Comece a utilizar o Bitdefender VPN ao aprender o que é e como ele pode ajudá-lo a proteger-se ao garantir o verdadeiro anonimato online.

Utilizar o Bitdefender VPN (página 13)

Saiba mais como interagir com a Bitdefender VPN e a sua interface de utilizador.

Bitdefender VPN Definições e Características (página 17)

Saiba mais sobre as definições e funcionalidades da Bitdefender VPN.

Conseguindo ajuda (página 30)

Onde procurar e onde pedir ajuda se algo inesperado acontecer.

## Convenções utilizadas neste guia

### Convenções Tipográficas

São utilizados diversos estilos de texto neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela abaixo.

| Aparência | Descrição |
|---|---|
| sample syntax | As amostras de sintaxe são impressas com monospaced personagens. |
| https://www.bitdefender.com | A hiperligação URL aponta para uma localização externa em servidores http ou ftp. |
| documentation@bitdefender.com | Endereços de email são inseridos no texto para contactar a solicitar mais informação. |
| Sobre este Guia (página 1) | Esta é uma hiperligação interna que o leva para uma localização dentro do documento. |
| filename | Arquivos e diretórios são impressos usando monospaced Fonte. |
| **opção** | Todas as opções de produtos são impressas usando **audacioso** personagens. |
| **palavra-chave** | Palavras-chave ou frases importantes são destacadas usando **audacioso** personagens. |

## Avisos

Os avisos estão em notas internas do texto, com marcação gráfica, que chamam a sua atenção para informações adicionais relacionadas ao parágrafo atual.

### Observação

A nota é apenas uma observação curta. Apesar de a poder omitir, a nota providencia-lhe informação valiosa, tal como uma característica específica ou um link para um determinado tópico.

### Importante

Este ponto requer a sua atenção e não é recomendável ignorá-lo. Normalmente, providencia-lhe informação bastante importante.

### Aviso

Trata-se de informação critica que deve de tratar com cuidados redobrados. Nada de negativo acontecerá se você seguir as indicações. Deve de lê-lo e compreendê-lo, porque descreve algo extremamente arriscado.

# Pedido de Comentários

Convidamo-lo a ajudar-nos a melhorar este manual. Nós verificamos e testamos toda a informação com o máximo dos cuidados. Por favor escreva-nos acerca de quaisquer falhas que descubra neste manual ou a forma como acha que o mesmo poderia ser melhorado, de forma a ajudar-nos a dar-lhe a si a melhor documentação possível.

Informe-nos enviando um e-mail para documentation@bitdefender.com. Escreva todos os seus e-mails relacionados à documentação em inglês para que possamos processá-los com eficiência.

# 1. O QUE É BITDEFENDER VPN

A VPN serve como um túnel entre o seu dispositivo e a rede à qual você se conecta para proteger sua conexão, criptografando os dados usando criptografia de nível militar e ocultando seu endereço IP onde quer que você esteja. Seu tráfego é redirecionado através de um servidor separado; impossibilitando assim a identificação do seu dispositivo pelo seu ISP, através da infinidade de outros dispositivos que utilizam os nossos serviços. Além disso, enquanto estiver conectado à Internet através do Bitdefender VPN, você poderá acessar conteúdo que normalmente é restrito em áreas específicas.

**Observação**

Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banido por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a funcionalidade Bitdefender VPN pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

## 1.1. Protocolos de encriptação

O conjunto de encriptação predefinido ativado no cliente e servidor Hydra é fornecido abaixo. Todos os outros conjuntos de encriptação estão desativados.

Conjunto de encriptação de cliente Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

### Observação

A configuração da parte do servidor é muito mais restritiva e tanto o cliente como o servidor Hydra rejeitarão um modo diferente do GCM que utiliza AES. O servidor Hydra reforça a prioridade do lado do servidor de conjuntos de encriptação mais fortes e rejeitará o handshake TLS se um conjunto mais fraco for solicitado por parte de um cliente. Esta lista também é configurável no tempo de execução do servidor.

# 2. SUBSCRIÇÕES DE VPN

Com o Bitdefender VPN, pode escolher dois tipos de subscrições:

- A subscrição Básica
- A subscrição Premium

## 2.1. Subscrição Básica

O Bitdefender VPN oferece gratuitamente uma quota de 200 MB de tráfego diário por dispositivo para proteger a sua ligação sempre que precisar e permite-lhe estabelecer ligação com uma única localização, que não pode ser alterada.

A subscrição Básica está disponível para qualquer utilizador que transferir o Bitdefender VPN.

## 2.2. Subscrição Premium

Para obter acesso ilimitado a todas as funcionalidades incluídas no Bitdefender VPN, faça a atualização para a versão Premium. Os utilizadores com uma subscrição ativa da VPN Premium têm tráfego ilimitado protegido, podendo estabelecer ligação com qualquer um dos nossos servidores em todo o mundo.

Existem dois planos disponíveis para a subscrição Premium: o Plano Mensal e o Plano Anual.

- Plano Mensal: com este plano, os serviços VPN Premium ser-lhe-ão cobrados todos os meses. Pode cancelar este plano quando quiser.
- Plano Anual: requer um pagamento único, garantindo o acesso aos nossos serviços VPN Premium durante um ano inteiro.

## 2.3. Como atualizar para a VPN Premium

A forma mais fácil de atualizar para a versão Premium do Bitdefender VPN é clicar no botão **Atualizar** situado na parte inferior da interface principal. Selecione o modelo de subscrição desejado e, em seguida, siga as instruções no ecrã.

Se já tem um código de ativação, siga as instruções abaixo:

- **Para os utilizadores de Windows:**
  1. Clique no ícone A Minha Conta no lado esquerdo da interface da VPN.
  2. Clique em **Adicione-o aqui**.
  3. Introduza o código recebido por e-mail e, depois, clique no botão **Ativar código**.

- **Para utilizadores de macOS**
  1. Clique no símbolo da roda dentada no canto superior direito da interface da VPN e selecione **A Minha Conta**.
  2. Clique **Adicione aqui**.
  3. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

- **Para utilizadores de Android**
  1. Toque no símbolo da roda dentada no canto superior direito da interface da VPN e selecione **A Minha Conta**.
  2. Toque em **Adicionar código**.
  3. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

- **Para utilizadores de iOS**
  1. Toque na roda dentada no canto superior direito da interface VPN e selecione **Minha conta**.
  2. Tocar **Adicionar código**.
  3. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

# 3. INSTALAÇÃO

## 3.1. A preparar a instalação

Antes de instalar o Bitdefender VPN, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o dispositivo onde deseja instalar o Bitdefender tem os requisitos de sistema mínimos. Caso o dispositivo não cumpra os requisitos de sistema, o Bitdefender não será instalado ou caso seja instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade do sistema.
  Para a lista completa dos requisitos mínimos dos sistema, consulte o Requisitos do sistema (página 8)
- Ligue-se ao dispositivo utilizando uma conta de Administrador.
- Recomenda-se que o seu dispositivo esteja ligado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD. Se estiverem disponíveis versões mais recentes dos ficheiros da aplicação incluidos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

## 3.2. Requisitos do sistema

- **Para usuários do Windows**
  - **Sistema operativo:** Windows 7 com Service Pack 1, Windows 8, Windows 8.1 Windows 10 e Windows 11
  - **Memória (RAM):** 1 GB
  - **Espaço de disco rígido disponivel:** 500 MB de espaço livre
  - **Net Framework:** versão mín 4.5.2

    **Importante**
    O desempenho do sistema pode ser afetado em dispositivos com CPUs de geração antiga.

- **Para usuários macOS**
  - **Sistema operativo:** macOS Sierra (10.12) ou superior

- **Espaço de disco rígido disponivel:** 100 MB de espaço livre

- **Para usuários do Android**
  - **Sistema operativo:** Android 5.0 ou superior
  - **Armazenamento:** 100MB
  - Uma ligação à Internet ativa

- **Para usuários de iOS**
  - **Sistema operativo:** iOS 12 ou superior
  - **Armazenamento no Iphone:** 50MB
  - **Armazenamento no iPad:** 100MB
  - Uma conexão ativa com a Internet

## 3.3. A instalar o Bitdefender VPN

Para iniciar a instalação, siga as instruções correspondentes ao sistema operativo que utiliza:

- **Para usuários do Windows**

  1. Para iniciar a instalação do Bitdefender VPN no PC Windows, inicie simplesmente ao transferir o kit de instalação do https://www.bitdefender.com/solutions/vpn/download ou a partir do e-mail recebido após a compra.
  2. Faça duplo clique no instalador transferido para o executar.
  3. Escolha Sim caso seja apresentada uma caixa de diálogo do Controlo de Conta de Utilizador.
  4. Aguarde até que a transferência seja concluída.
  5. Selecione o idioma do produto utilizando o menu suspenso no instalador.
  6. Marque a caixa "Eu confirmo que li e concordo com o Acordo de Subscrição e a Política de Privacidade" e, em seguida, clique em **INICIAR INSTALAÇÃO**.
  7. Espere que a instalação termine.

8. **INICIE A SESSÃO** com a sua conta da Central Bitdefender. Se não tiver uma conta da Central, registe uma ao clicar no botão **CRIAR UMA CONTA**.
9. Selecione **Eu tenho um Código de Ativação** se comprou a subscrição do Premium VPN.
   Caso contrário, pode escolher **INICIAR VERSÃO DE TESTE** para experimentar o produto gratuitamente durante 7 dias antes de se comprometer a pagar por ele.
10. Introduza o código recebido por e-mail e, em seguida, clique no botão **ATIVAR PREMIUM**.
11. Após uma pequena espera, Bitdefender VPN é instalado e fica pronto para ser utilizado no computador.

❍ **Para usuários macOS**

1. Para iniciar a instalação do Bitdefender VPN no macOS, inicie simplesmente ao transferir o kit de instalação do https://www.bitdefender.com/solutions/vpn/download ou a partir do e-mail recebido após a compra.
2. O instalador será guardado no Mac. Na pasta Transferências, clique duas vezes no ficheiro do pacote .
3. Siga as instruções no ecrã. Selecione **Continuar**.
4. Será guiado através dos passos necessários para instalar Bitdefender VPN no seu Mac. Clique duas vezes no botão **Continuar**.
5. Clique em **Eu concordo**, depois de ler e concordar com os termos do acordo de licença do software.
6. Clique em **Instalar**.
7. Introduza um nome de utilizador e palavra-passe de administrador e, em seguida, clique em **Instalar software**.
8. Receberá a notificação de que uma extensão assinada pela Bitdefender foi bloqueada. Isto não é um erro, apenas uma verificação de segurança. Clique em **Abri Preferências de segurança**.
9. Clique no ícone de bloqueio para o desbloquear.

Introduza um nome e palavra-passe de administrador e, em seguida, prima **Desbloquear**.

10. Clique em **Permitir** para carregar a extensão do sistema BitdefenderBitdefender. Em seguida, feche a janela de Segurança e Privacidade e o instalador.

11. Aceda ao ícone do escudo na barra de menu e, em seguida, **Entre** na sua conta da Central Bitdefender. Se ainda não tiver uma conta da Central, crie uma.

12. Selecione Eu tenho um **Código de ativação** caso tenha adquirido a subscrição do VPN Premium.
    Caso contrário, você pode escolher **INICIAR TESTE** para testar o produto gratuitamente por 7 dias antes de se comprometer a pagar por ele.

13. Digite o código recebido por e-mail e clique no botão **Código de Ativação** botão.

14. Após uma pequena espera, Bitdefender VPN será instalado e ficará pronto a utilizar no seu Mac.

❍ **Para usuários do Android**

1. Para instalar o Bitdefender VPN no Android, abra primeiro a aplicação do **Google Play Store** no seu smartphone ou tablet.
2. Pesquise por Bitdefender VPN e selecione esta aplicação.
3. Clique no botão **Instalar** e aguarde que a transferência termine.
4. Toque em **Abrir** para executar a aplicação.
5. Marque a caixa "Eu concordo com o Acordo de Subscrição e a Política de Privacidade" e, em seguida, toque em **Continuar**.
6. **Inicie a Sessão** com a sua conta da Central Bitdefender. Se não tiver uma conta da Central, registe uma ao tocar em **Criar uma Conta**.
7. Selecione **Eu tenho um código de ativação** caso tenha comprado uma subscrição Premium VPN.
   Caso contrário, pode escolher Iniciar uma versão de teste de 7 dias para experimentar o produto gratuitamente durante 7 dias antes de se comprometer a pagar por ele.

8. Introduza o código recebido por e-mail e, depois, clique em **Ativar código**.

❍ **Para usuários de iOS**

1. Para instalar o Bitdefender VPN no iOS, primeiro abra a **App Store** no seu iPhone ou iPad.
2. Procurar Bitdefender VPN e selecione este aplicativo.
3. Toque no ícone **Obter** e aguarde até que a transferência termine.
4. Tocar **Abrir** para executar o aplicativo.
5. Marque a caixa **Eu concordo com o Acordo de Subscrição e a Política de Privacidade** e, em seguida, toque em **Continuar**.
6. **Inicie a Sessão** com a sua conta da Central Bitdefender. Se não tiver uma conta, registe uma ao tocar em **Criar uma Conta**.
7. Toque em **Permitir** se desejar receber notificações do Bitdefender VPN.
8. Escolher **Eu tenho um código de ativação** se você comprou uma assinatura VPN Premium.
   Caso contrário, você pode escolher Iniciar 7 dias de teste para testar o produto gratuitamente por 7 dias antes de se comprometer a pagar por ele.
9. Digite o código recebido por e-mail e toque em **Código de Ativação**.

# 4. UTILIZAR O BITDEFENDER VPN

## 4.1. A abrir o Bitdefender VPN

- **Para Windows**
  Para aceder a **interface principal do Bitdefender VPN**, utilize um dos seguintes métodos:
  - **A partir da bandeja do sistema**
    Clique com o botão direito no ícone do escudo vermelho e depois selecione **Mostrar** no menu.
  - **Da interface doBitdefender**
    Se um produto de segurança da Bitdefender tal como o Bitdefender Total Security ou o Bitdefender Antivirus Plus etc. já estiver instalado no seu computador Windows, pode abrir o Bitdefender VPN a partir de lá:
    1. Clique em **Privacidade** na barra do lado esquerdo da interface do Bitdefender.
    2. Clique em **Abrir o VPN** no painel do VPN.
  - **A partir do seu ambiente de trabalho**
    Faça duplo-clique no atalho Bitdefender VPN no seu Ambiente de trabalho.
- **Para macOS**
  Pode abrir a aplicação do Bitdefender VPN ao clicar no ícone da barra de menu no lado superior direito do ecrã.
  Se o escudo do Bitdefender não puder ser encontrado na barra de menu, utilize o Launchpad ou o Finder do Mac para recuperá-lo:
  - **A partir do Launchpad**
    1. Prima **F4** no seu teclado para introduzir o Launchpad no seu Mac.
    2. Navegue pelas páginas das aplicações instaladas até localizar a aplicação do Bitdefender VPN. Como alternativa, pode introduzir **Bitdefender VPN** no Launchpad para começar a filtrar os seus resultados.

3. Assim que visualizar a aplicação Bitdefender VPN, clique no ícone para fixá-lo na barra de menu.

- **A partir do Finder**

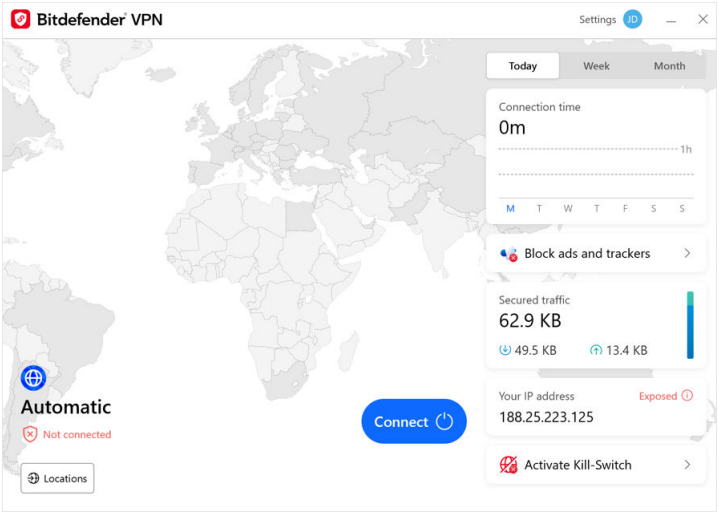
1. Clique no **Finder** na parte inferior esquerda do Dock (Finder é o ícone que se parece com um quadrado azul com um rosto sorridente).
2. Em seguida, clique em **Ir** no canto superior esquerdo do ecrã, na barra de menus.
3. Selecione **Aplicações** a partir do menu para entrar na pasta das Aplicações no seu Mac.
4. Na pasta de Aplicações, abra a pasta **Bitdefender** e clique duas vezes na aplicação **Bitdefender VPN**.

Observação

Para aceder ao Bitdefender VPN nos seus dispositivos móveis Android ou iOS, basta abrir a aplicação Bitdefender VPN depois de instalá-la.

## 4.2. Como ligar o Bitdefender VPN

A interface VPN exibe o estado da aplicação: ligar ou desligar. A localização do servidor para utilizadores com a versão gratuita é definida automaticamente pelo Bitdefender para o servidor mais apropriado, enquanto os utilizadores premium têm a possibilidade de alterar a localização do servidor que desejam ligar-se ao selecioná-lo na lista de localização virtual. Para ligar ou desligar, basta clicar no botão liga/desliga na interface VPN.




- **Para Windows:** o ícone da bandeja do sistema exibe uma marca de seleção verde quando a VPN está ligado e uma marca preta quando a VPN está desligada. Enquanto ligado a um local selecionado manualmente, o endereço IP é exibido na interface principal.
- **Para macOS:** o ícone da barra de menus fica preto quando a VPN está ligada e branco quando a VPN é desligada. Clique no botão circular no meio da interface e aguarde o estabelecimento da ligação.
- **Para Android e iOS:** Para se ligar ao Bitdefender VPN para Android, iOS e iPadOS:
  - **Na aplicação Bitdefender VPN:** Para ligar ou desligar, basta tocar no botão liga/desliga na interface VPN. O estado do Bitdefender VPN é exibido.
  - **Na aplicação Bitdefender Mobile Security:**
    1. Aceda o ícone VPN na barra de navegação inferior do Bitdefender Mobile Security.
    2. Toque em **LIGAR** sempre que desejar permanecer protegido enquanto estiver ligado a redes sem fio não seguras. Toque em **DESLIGAR** sempre que desejar desativar a ligação VPN.

## 4.3. Como se ligar a um servidor diferente

Com uma subscrição Premium, Bitdefender VPN permite-lhe ligar-se a qualquer um dos nossos servidores em todo o mundo, a qualquer momento. Para fazer isto, terá que:

1. Abrir a aplicação Bitdefender VPN.
2. Toque no botão **Localização virtual** na parte inferior da interface.
3. Selecione o país que desejar.
4. Clique no botão **Ligar a [país]** na parte inferior da interface.

- O ícone da bandeja do sistema exibe uma marca de seleção verde quando a VPN está conectada.
- O endereço IP do servidor virtual é mostrado na tela inicial enquanto estiver conectado ao Bitdefender VPN.
- Um resumo do seu tempo de conexão, a quantidade de tráfego seguro e os últimos 5 locais aos quais você se conectou também são mostrados no painel principal.

# 5. BITDEFENDER VPN DEFINIÇÕES E CARACTERÍSTICAS

## 5.1. A aceder às Definições

Para aceder às definições do Bitdefender VPN, deverá seguir os passos descritos abaixo:

- **No Windows:**
  1. Abra a aplicação do Bitdefender VPN no seu dispositivo clicando duas vezes no seu ícone no sistema ou clicando com o botão direito do rato nele e selecionando Mostrar.
  2. Clique no botão de **Definições** (representado por um símbolo de engrenagem) no lado esquerdo da interface.

- **No macOS:**
  1. Abra a aplicação do Bitdefender VPN no seu dispositivo macOS ao clicar no seu ícone na barra de menu.
  2. Clique no botão da engrenagem no canto superior direito da interface do Bitdefender VPN e selecione Definições.

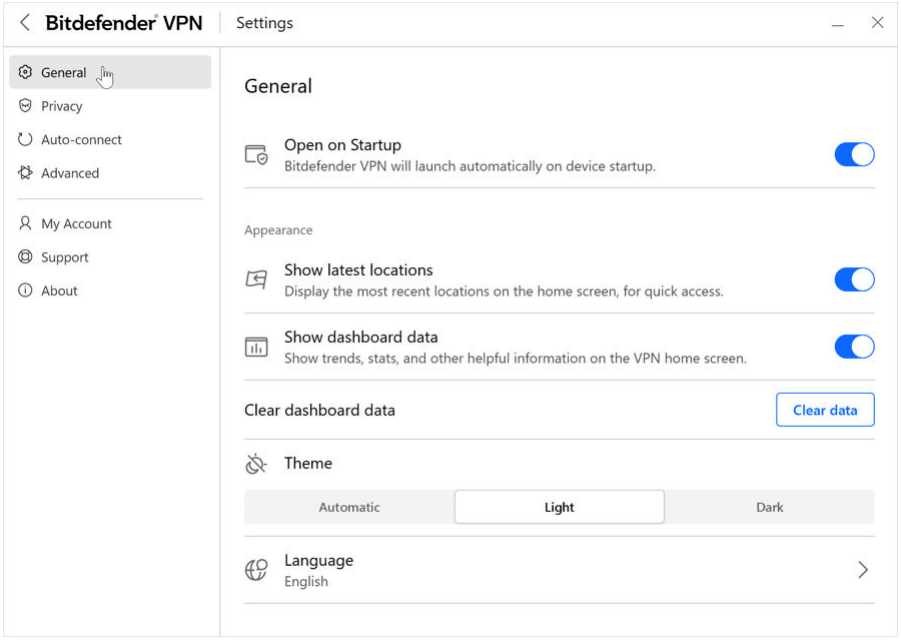
- **No Android:**
  1. Abra a aplicação Bitdefender VPN no seu dispositivo.
  2. Clique no botão de engrenagem no canto esquerdo superior da interface do Bitdefender VPN.

- **No iOS:**
  1. Abra o Bitdefender VPN aplicativo em seu dispositivo.
  2. Clique no botão roda dentada no canto superior direito do Bitdefender VPN interface.

## 5.2. Em geral

Aqui você pode modificar o seguinte:

- **Abrir na inicialização**– O Bitdefender VPN será iniciado automaticamente na inicialização do dispositivo.
- **Mostrar locais mais recentes**– Exiba os locais mais recentes na tela inicial, para acesso rápido.
- **Mostrar dados do painel** – Mostre tendências, estatísticas e outras informações úteis na tela inicial da VPN.
- **Limpar dados do painel**– Todos os dados do seu painel serão apagados e todos os contadores serão redefinidos.
- **Tema**– Tema claro/escuro
- **Linguagem**– Altere o idioma do Bitdefender VPN.
- **Notificações**– Gerencie suas preferências de notificações.
- **Ajude a melhorar a VPN Bitdefender**– Envie relatórios anônimos de produtos para nos ajudar a melhorar sua experiência.
- **Redefinir todas as configurações**– Redefina a VPN para suas configurações originais sem reinstalá-la.



# 5.3. Características

## 5.3.1. Privacidade

### Kill-Switch da Internet

O Kill-Switch é uma nova funcionalidade implementada no Bitdefender VPN. Quando, ativado, ele suspende temporariamente todo o tráfego da internet se a ligação VPN cair acidentalmente. Assim que estiver online novamente, a ligação VPN é restabelecida.

Para ativar o Kill-Switch, siga os passos abaixo:

- **No Windows**
  1. Abra a aplicação Bitdefender VPN no seu dispositivo ao clicar duas vezes no seu ícone na tentativa do sistema ou ao clicar com o botão direito nele e ao selecionar **Mostrar**.
  2. Clique no **Configurações** botão (representado por uma roda dentada) no lado esquerdo da interface.
  3. Selecione **Avançado**.
  4. Ative a opção **Kill-Switch da internet**.

- **No Android**
  1. Abra o Bitdefender VPN aplicativo em seu dispositivo.
  2. Clique no botão roda dentada no canto superior direito do Bitdefender VPN interface.
  3. Nas **Definições**, ative a opção **Kill-Switch**.

- **No iOS**
  1. Abra o Bitdefender VPN aplicativo em seu dispositivo.
  2. Clique no botão roda dentada no canto superior direito do Bitdefender VPN interface.
  3. Sob **Configurações**, habilite o **Botão de desligar** opção.

> **Observação**
> Este recurso também está disponível para dispositivos macOS com os sistemas operativos 10.15.4 ou versões posteriores.

## Bloqueador de anúncios e antitracker

Estas funcionalidades são projetados para ajudá-lo a manter a privacidade e aproveitar a web sem anúncios irritantes ou empresas a espiá-lo. Eles ajudam a bloquear anúncios e parar rastreá-lo online.

## Bloqueador de anúncios

O **Bloqueador de anúncios** é utiliza para bloquear anúncios, pop-ups, anúncios em vídeo altos ou abas de anúncios durante a navegação. Isto ajuda os sites a carregarem mais depressa e ficarem mais limpos, além de serem mais seguros para interagir.

Para ativar o Bloqueador de anúncios:

1. Localize a funcionalidade do **Bloqueador de anúncios e antirastreamento** na **Definições**.
2. Mude o interruptor para a posição **ON**.

## Antitracker

O **Anti-rastreador** é utilizado para bloquear rastreadores definidos por anunciantes para seguir e traçar o seu perfil online. Alguns sites podem apresentar mau funcionamento ao bloquear rastreadores, mas adicionar o URL à lista de permissões pode corrigir isso.

Para ativar o Anti-tracker:

1. Localize o **Bloqueador de anúncios e Antitracker** recurso em **Configurações**.
2. Mude o interruptor para o **SOBRE** posição.

## Lista de confiança

Alguns websites podem não carregar corretamente se bloquear o seu código localizador e de anúncios. Adicionar os URLs destes domínios específicos à lista de permissões pode resolver este problema, mas tenha em mente que, enquanto navega nestes websites, verá anúncios e o seu código localizador estará ativo.

Adicione os sites que deseja permitir a exibição de anúncios e o utilize os rastreadores:

1. Localize o **Bloqueador de anúncios e Antitracker** recurso em **Configurações**.
2. Clique na ligação **Gerir**. Em seguida, vá para a secção da Lista de permissões da janela e clique na ligação **Gerir** correspondente.
3. Clique em **Adicionar site** e insira o URL desejado.

## 5.3.2. Auto-conectar

Enquanto caminha, trabalha num café ou aguarda no aeroporto, ligar-se a uma rede pública sem fios para realizar pagamentos, verificar e-mails ou aceder às contas de redes sociais pode ser a solução mais rápida. Enquanto isso, pessoas curiosas tentam roubar os seus dados pessoais vendo como as informações fluem ao longo da rede.

Para o(a) proteger contra os perigos de hotspots públicos não seguros ou não encriptados, o Bitdefender VPN inclui uma funcionalidade de auto-conexão. Isto significa que o Bitdefender VPN pode ser ativado automaticamente em determinadas situações, dependendo das suas preferências e do sistema operativo que estiver a utilizar.

- No **Windows**, a funcionalidade de ligação automática pode ser ativado nas seguintes situações:
  - **Arranque:** Ligue-se ao VPN no arranque do Windows.
  - **Wi-Fi não seguro:** Utilize a VPN sempre que se ligar a redes Wi-Fi públicas ou não seguras.
  - **Aplicações ponto a ponto:** Ligue-se ao VPN ao iniciar uma aplicação de partilha de ficheiros ponto a ponto.
  - **Aplicações e domínios:** Utilize sempre o VPN para determinadas aplicações e sites.

    Observação

    1. Clique na ligação **Gerir**.
    2. Navegue até à localização da aplicação para o qual deseja utilizar o VPN, selecione o nome da aplicação e clique em **Adicionar**.

  - **Categorias de sites:** Ligue-se ao VPN ao visitar as categorias específicas dos sites. Bitdefender VPN pode-se ligar automaticamente para as seguintes categorias de sites:

- Finanças
- Pagamentos online
- Saúde
- Partilha de ficheiros
- Encontros Online
- Conteúdo para adultos

> **Observação**
> Para cada categoria, pode selecionar um servidor diferente para o VPN se ligar.

- No **macOS**, o recurso de ligação automática pode ser ativado nas seguintes situações:
  - **Arranque:** Ligue o VPN no arranque do macOS.
  - **Wi-Fi não seguro:** Use a VPN sempre que se conectar a redes Wi-Fi públicas ou não seguras.
  - **Aplicativos ponto a ponto:** Conecte-se à VPN ao iniciar um aplicativo de compartilhamento de arquivos ponto a ponto.
  - **Aplicações:** Ligue-se sempre ao VPN para determinadas aplicações.
- No **Android** e **iOS**, Bitdefender VPN pode ser definido para se ligar automaticamente apenas quando estiver num Wi-Fi não seguro ou público.

## 5.3.3. Avançado

### Túnel dividido

O túnel dividido da rede privada virtual (VPN) permite que direcione parte do tráfego da sua aplicação ou dispositivo por meio de um VPN encriptado, enquanto outras aplicações ou dispositivos têm acesso direto à Internet. Isto é particularmente útil se deseja beneficiar dos serviços que funcionam melhor quando a sua localização é conhecida, além de desfrutar de acesso seguro a comunicações e dados potencialmente confidenciais.

Ao ativar o recurso **Split tunneling**, as aplicações e os sites selecionados ignorarão a VPN e acederão a Internet diretamente.

Para gerir as aplicações e os sites que ignoram o VPN:

1. Clique no link **Gerir** assim que o recurso estiver ativado.
2. Clique no botão **Adicionar**.
3. Navegue até o local da aplicação em questão ou insira o URL do site desejado e clique em **Adicionar**.

> **Observação**
> Ao adicionar um site, todo o domínio, ao incluir todos os subdomínios, será ignorado.

> **Importante**
> Em dispositivos **macOS**, o recurso Split tunneling está disponível apenas para os sites.

## App Traffic Optimizer

O App Traffic Optimizer do Bitdefender VPN permite que priorize o tráfego para as aplicações mais importantes no seu dispositivo sem expor a sua ligação a riscos de privacidade. As VPNs redirecionam o tráfego da Internet através de um túnel seguro enquanto utilizam algoritmos de encriptação robustos para protegê-lo.

No entanto, esta combinação de técnicas pode ter algumas desvantagens, principalmente no que diz respeito à velocidade da ligação. Vários fatores podem desencadear lentidão na ligação, ao ser o mais comum a distância até o servidor ao qual está a ligar-se, congestionamento da rede e alta utilização de largura de banda. Se já sentiu que às vezes Bitdefender VPN coloca uma carga desnecessária na sua ligação e lentidão constantemente atrapalha, pode haver uma resposta melhor do que desligar.

**Como funciona o App Traffic Optimizer?**

Certas aplicações e serviços, como plataformas de streaming, clientes de torrent e jogos, exigem mais largura de banda. A utilização constante deles pode afetar a velocidade da sua ligação com a Internet. O encaminhamento do seu tráfego através de um túnel VPN já sujeita a sua ligação a uma lentidão relativa. Ao colocar tensão adicional na sua ligaão pode degradar seriamente a sua experiência online.

A funcionalidade App Traffic Optimizer do Bitdefender VPN pode ajudá-lo a lidar com a lentidão da ligação VPN, ao priorizá-lo para a aplicação da sua escolha. O recurso permite que decida quais as aplicações que devem receber a maior parte do seu tráfego e, em seguida, aloca o recursos de acordo. Por exemplo, se estiver numa reunião e perceber que a qualidade da sua chamada está abaixo da média, o App Traffic Optimizer permite que dê prioridade o tráfego para a aplicação de videoconferência para obter melhores resultados.

Normalmente, os utilizadores de VPN recorrem ao encerramento de todos os processos de interferência nos seus dispositivos ou até mesmo à desativação da sua ligação VPN para obter uma velocidade de Internet mais rápida. O App Traffic Optimizer permite que desfrute de proteção de privacidade ininterrupta sem comprometer a velocidade da sua ligação.

## Utilizar a Aplicação Traffic Optimizer

Atualmente, o recurso está disponível apenas em dispositivos Windows e permite priorizar o tráfego para até 3 aplicações.

Siga estas etapas para ativá-la e configurá-lo com o mínimo de esforço:

1. Inicie a aplicação Bitdefender VPN no seu computador Windows.
2. Clique no botão na barra lateral para aceder as definições da VPN.
3. Vá para à guia **Geral** e ative o recurso **App Traffic Optimizer**. A cor da chave mudará de cinza para azul.

Para gerir as aplicações priorizadas por este recurso:

1. Clique no**Gerenciar**link.
2. Navegue até ao local da aplicação para a qual deseja otimizar o tráfego, selecione o nome da aplicação e clique em **Adicionar**. A aplicação aparecerá na secção **Priorizado**.

> **Observação**
> Como alternativa, abriu-se recentemente a aplicação que deseja priorizar, ao pressionar o botão + na janela do App Traffic Optimizer.

3. Desligue e volte a ligar ao Bitdefender VPN após adicionar ou remover as aplicações da lista.

Para remover uma aplicação do App Traffic Optimizer, basta clicar no ícone ao lado do nome da aplicação.

Observação
O App Traffic Optimizer não está disponível no macOS.

## Protocolo

Aqui você pode escolher o tipo de protocolo que deseja usar para transferência de dados. As seguintes opções estão disponíveis:

- **Automático** - O Bitdefender VPN selecionará o protocolo ideal para seu dispositivo e rede específicos.
- **Catapulta Hidra** - Rápido e seguro, ideal para streaming e jogos.
- **OpenVPN UDP** - Otimizado para velocidades rápidas. No entanto, este protocolo não é tão confiável em termos de perda de dados como outros protocolos da lista.
- **OpenVPN TCP** - Projetado para confiabilidade. Garante que seus dados sejam entregues integralmente, mas não é tão rápido quanto o OpenVPN UDP.
- **Proteção de arame** - Protocolo mais recente, proporcionando forte segurança e alto nível de desempenho.

## Salto duplo

Com esse recurso você pode gerenciar os servidores através dos quais enviar e criptografar duas vezes o tráfego da Internet. Seus dados passarão por dois servidores VPN em vez de um, dificultando o rastreamento de sua atividade na Internet.

Observação
Você só pode adicionar um total de 5 locais de salto duplo. No entanto, você pode excluir os saltos duplos personalizados da sua lista e criar outros a qualquer momento.

Importante
Usar servidores localizados em continentes diferentes no mesmo salto duplo pode diminuir a velocidade da sua conexão.

# 6. DESINSTALAR BITDEFENDER VPN

O procedimento de remoção do Bitdefender VPN é similar ao que utiliza para remover outros programas do seu computador:

- **Ao desinstalado Bitdefender VPN de dispositivos Windows**
  - No **Windows 7**:
    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e dê um clique duplo em **Programas e Recursos**.
    2. Localize **Bitdefender VPN** e selecione **Desinstalar**.
       Aguarde até que o processo de desinstalação seja concluído.
  - No **Windows 8** e no **Windows 8.1**:
    1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
    2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
    3. Encontrar **Bitdefender VPN** e selecione **Desinstalar**.
       Aguarde a conclusão do processo de desinstalação.
  - No **Windows 10** e no **Windows 11**:
    1. Clique em **Iniciar**, depois clique em **Definições**.
    2. Clique no ícone **Sistema** na área de Definições e, em seguida, selecione **Aplicações instaladas**.
    3. Encontrar **Bitdefender VPN** e selecione **Desinstalar**.
    4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
       Aguarde a conclusão do processo de desinstalação.
- **Desinstalação dos dispositivos macOS**
  1. Clique no **Ir** na barra de menu e selecione **Aplicações**.
  2. Clique duas vezes na pasta **Bitdefender**.

3. Execute **BitdefenderUninstaller**.
4. Na nova janela, marque a caixa ao lado de **Bitdefender VPN** e, em seguida, clique em **Desinstalar**.
5. Introduza um nome de conta de administrador válido e uma palavra-passe e, em seguida, clique em **OK**.
6. Finalmente, receberá uma notificação de que o Bitdefender VPN foi desinstalado com sucesso. Clique em **Fechar**.

- **Desinstalação dos dispositivos Android**
  1. Abra a aplicação **Play Store**.
  2. Procurar por **Bitdefender VPN**.
  3. Na Bitdefender VPN página da loja de aplicações, selecione **Desinstalar**.
  4. Confirme ao tocar em **OK**.

- **Desinstalação de dispositivos iOS**
  1. Mantenha o dedo na aplicação Bitdefender VPN.
  2. Selecione **Apagar a Aplicação**.
  3. Toque em **Excluir**.

# 7. PERGUNTAS FREQUENTES

**Quando devo utilizar o Bitdefender VPN?**

Deve ter cuidado ao aceder, transferir ou carregar conteúdo na Internet. Para garantir a sua segurança ao navegar na Web, recomendamos que utilize a VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, endereços de email, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

**Posso escolher uma cidade com o Bitdefender VPN?**

Sim. Atualmente, a Bitdefender VPN para Windows, macOS, Android e iOS podem ser utilizados para selecionar uma cidade específica. Aqui está a lista de cidades atualmente disponíveis:

- **EUA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, Nova York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **RU:** Londres, Manchester

**O Bitdefender VPN pode ser instalado como uma aplicação independente?**

A aplicação VPN é instalada automaticamente em conjunto com a sua solução de segurança Bitdefender. Também pode ser instalado como uma aplicação independente na página do produto, da Google Play Store e App Store.

**O Bitdefender partilhará o meu endereço IP e dados pessoais com terceiros?**

Não, com o Bitdefender VPN a sua privacidade é 100% segura. Ninguém (agências de publicidade, ISPs, seguradoras, etc.) terá acesso aos seus registos online.

**Qual algoritmo de encriptação ele utilizar?**

Bitdefender VPN utiliza o protocolo Hydra em todas as plataformas, encriptação AES de 256 bits ou a cifra mais alta disponível suportada por cliente e servidor, com Perfect Forward Secrecy. Isto significa que as chaves de encriptação são geradas para cada nova sessão VPN e apagadas da memória quando a sessão terminar.

**Posso ter acesso ao conteúdo restrito GEO-IP?**

Com o VPN Premium, tem acesso a uma extensa rede de localizações virtuais em todo o mundo.

**Isto terá um impacto negativo na duração da bateria do meu dispositivo?**

Bitdefender VPN é projetado para proteger os seus dados pessoais, ocultar o seu endereço IP enquanto estiver ligado a redes sem fio não seguras e aceder a conteúdos restritos em determinados países. Para evitar o consumo desnecessário de bateria do seu dispositivo, recomendamos que utilize apenas a VPN quando precisar e desligar quando estiver offline.

**Porque é que a VPN torna a minha ligação com a Internet mais lenta?**

O Bitdefender VPN foi projetado para oferecer uma experiência leve ao navegar na web. Dependendo da distância entre a sua localização atual e a localização que selecionou do servidor para se ligar, alguma penalidade na velocidade é esperada, no entanto é por norma suficientemente pequena para não ser sentida durante a atividade online normal. Além disso, contamos com uma das infraestruturas de VPN mais rápidas do mundo. Se não for obrigatório ligar-se da sua localização a um servidor hospedado distante (por exemplo, do EUA para a França), recomendamos que permita que a VPN o ligue automaticamente ao servidor mais próximo ou encontre um servidor mais próximo da sua localização atual.

# 8. CONSEGUINDO AJUDA

## 8.1. Pedir Ajuda

O Bitdefender se empenha em oferecer aos seus clientes um nível incomparável de apoio preciso e rápido. Se tiver qualquer problema ou pergunta sobre o seu produto Bitdefender, pode utilizar vários recursos online para encontrar uma solução ou uma resposta. Ao mesmo tempo, pode entrar em contacto com a equipe de Atendimento ao Cliente da Bitdefender. Os nossos representantes de apoio responderão às suas perguntas em tempo hábil e oferecerão a assistência de que precisa.

## 8.2. Recursos Em Linha

Estão disponíveis vários recursos online para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte da Bitdefender:
  https://www.bitdefender.pt/consumer/support/
- A Comunidade de Especialistas da Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

### 8.2.1. Centro de Suporte da Bitdefender

A Bitdefender Support Center é um repositório de informação online acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das atividades de reparação de erros por parte da equipa técnica do suporte BitDefender e da equipa de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de ameaças, a administração de soluções BitDefender e explicações pormenorizadas e muitos outros artigos.

A Bitdefender Support Center encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma

outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na Bitdefender Support Center, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

O Centro de Suporte Bitdefender está disponível a qualquer momento no seguinte endereço: https://www.bitdefender.pt/consumer/support/.

### 8.2.2. A Comunidade de Especialistas da Bitdefender

A Comunidade de Especialistas da Bitdefender é um ambiente onde os utilizadores, entusiastas e fãs da Bitdefender podem interagir, trocar ideias, apoiar-se mutuamente e partilhar os seus conhecimentos e soluções. É também um lugar de criação de ideias que fornece um feedback valioso para as nossas equipas de desenvolvimento. Os membros da comunidade são utilizadores experientes da Bitdefender que têm todo o prazer em ajudar outros colegas no seu tempo livre. Com a sua imensa contribuição e os seus esforços genuínos e voluntários, criámos uma base de conhecimento onde os utilizadores podem encontrar respostas e orientação, mas com um toque humano.

Aqui encontrará conversas significativas com pessoas que utilizam a Bitdefender nos seus dispositivos. A comunidade oferece uma verdadeira ligação com os nossos membros e faz com que sua voz seja ouvida. É um lugar onde é encorajado a participar sabendo que sua opinião e sua contribuição são respeitadas e bem recebidas. Ao ser um fornecedor valioso, esforçamo-nos para oferecer um nível inigualável de apoio rápido e preciso e desejamos aproximar os nossos utilizadores de nós. Projetamos a nossa comunidade com este propósito em mente.

Pode encontrar a nossa página da Comunidade de Especialistas aqui:

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

### 8.2.3. Bitdefender Cyberpedia

A Bitdefender Cyberpedia tem toda a informação de que precisa sobre as últimas ameaças cibernéticas. Este é o lugar onde os especialistas da Bitdefender partilham dicas e truques sobre como se protegerem contra hackers, violações de dados, roubo de identidade e tentativas de personificação social.

A página da Bitdefender Cyberpedia pode ser encontrada aqui:

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

## 8.3. Informações de Contato

Uma comunicação eficiente é a chave para um negócio de sucesso. Desde 2001 a BITDEFENDER estabeleceu uma reputação inquestionável por buscar constantemente uma melhor comunicação para superar as expectativas de nossos clientes e parceiros. Se você tiver alguma dúvida, não hesite em nos contatar diretamente através do nosso Centro de Suporte da Bitdefender (página 30).

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

### 8.3.1. Distribuidores locais

Os distribuidores locais BitDefender estão preparados para responder a quaiquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor da Bitdefender no seu país:

1. Vá para https://www.bitdefender.com/partners/partner-locator.html.
2. Escolha o seu país e cidade utilizando as opções correspondentes.

# GLOSSÁRIO

**Código de ativação**

É um código exclusivo que pode ser comprado no varejo e usado para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma assinatura válida por um determinado período de tempo e determinados dispositivos e também pode ser usado para estender uma assinatura com a condição de ser gerada para o mesmo produto ou serviço.

**ActiveX**

ActiveX é um modelo para escrever programas para que outros programas e o sistema operacional possam chamá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interativas que se parecem e se comportam como programas de computador, em vez de páginas estáticas. Com o ActiveX, os usuários podem fazer ou responder perguntas, usar botões de pressão e interagir de outras maneiras com a página da web. Os controles ActiveX geralmente são escritos usando o Visual Basic. Active X é notável por uma completa falta de controles de segurança; especialistas em segurança de computadores desencorajam seu uso pela internet.

**Ameaça persistente avançada**

Ameaça persistente avançada (APT) explora vulnerabilidades de sistemas para roubar informações importantes para entregá-las à fonte. Grandes grupos, como organizações, empresas ou governos, são alvo dessa ameaça. O objetivo de uma ameaça persistente avançada é permanecer indetectável por muito tempo, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas visadas. O método usado para injetar a ameaça na rede é por meio de um arquivo PDF ou documento do Office que pareça inofensivo para que todos os usuários possam executar os arquivos.

**Adware**

O adware geralmente é combinado com um aplicativo host fornecido gratuitamente, desde que o usuário concorde em aceitar o adware. Como os aplicativos de adware geralmente são instalados depois que o usuário concorda com um contrato de licenciamento que declara a finalidade do aplicativo, nenhuma ofensa é cometida. No entanto, anúncios pop-

up podem se tornar um aborrecimento e, em alguns casos, degradar o desempenho do sistema. Além disso, as informações que alguns desses aplicativos coletam podem causar problemas de privacidade para usuários que não estavam totalmente cientes dos termos do contrato de licença.

**Arquivo**

Um disco, cassete, ou diretório que contém ficheiros que foram armazenados.

Um arquivo que contém um ou mais arquivos em um formato compactado.

**Porta dos fundos**

Uma brecha na segurança de um sistema deliberadamente deixada por designers ou mantenedores. A motivação para tais buracos nem sempre é sinistra; alguns sistemas operacionais, por exemplo, vêm com contas privilegiadas destinadas ao uso por técnicos de serviço de campo ou programadores de manutenção do fornecedor.

**Setor de inicialização**

Um setor no início de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster e assim por diante). Para discos de inicialização, o setor de inicialização também contém um programa que carrega o sistema operacional.

**Vírus de inicialização**

Uma ameaça que infecta o setor de inicialização de um disco fixo ou disquete. Uma tentativa de inicializar a partir de um disquete infectado com um vírus do setor de inicialização fará com que a ameaça se torne ativa na memória. Toda vez que você inicializar seu sistema a partir desse ponto, você terá a ameaça ativa na memória.

**botnet**

O termo “botnet” é composto pelas palavras “robô” e “rede”. Botnets são dispositivos conectados à Internet infectados com ameaças e podem ser usados para enviar e-mails de spam, roubar dados, controlar remotamente dispositivos vulneráveis ou espalhar spyware, ransomware e outros tipos de ameaças. Seu objetivo é infectar o maior número possível de dispositivos conectados, como PCs, servidores, dispositivos móveis ou IoT pertencentes a grandes empresas ou indústrias.

**Navegador**

Abreviação de navegador da web, um aplicativo de software usado para localizar e exibir páginas da web. Os navegadores populares incluem Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são navegadores gráficos, o que significa que eles podem exibir gráficos, bem como texto. Além disso, a maioria dos navegadores modernos pode apresentar informações multimídia, incluindo som e vídeo, embora exijam plug-ins para alguns formatos.

**Ataque de força bruta**

Ataque de adivinhação de senha usado para invadir um sistema de computador inserindo possíveis combinações de senha, geralmente começando com a senha mais fácil de adivinhar.

**Linha de comando**

Em uma interface de linha de comando, o usuário digita comandos no espaço fornecido diretamente na tela usando a linguagem de comando.

**Biscoitos**

Na indústria da Internet, os cookies são descritos como pequenos arquivos contendo informações sobre computadores individuais que podem ser analisados e usados por anunciantes para rastrear seus interesses e gostos online. Neste domínio, a tecnologia de cookies ainda está sendo desenvolvida e a intenção é direcionar os anúncios diretamente para o que você disse que são seus interesses. É uma faca de dois gumes para muitas pessoas porque, por um lado, é eficiente e pertinente, pois você só vê anúncios sobre o que está interessado. Por outro lado, envolve realmente "rastrear" e "seguir" onde você vai e o que você clicar. Compreensivelmente, há um debate sobre privacidade e muitas pessoas se sentem ofendidas com a noção de que são vistas como um "número SKU" (você sabe, o código de barras no verso dos pacotes que é escaneado na fila do caixa do supermercado) . Embora esse ponto de vista possa ser extremo, em alguns casos é preciso.

**Cyberbullying**

Quando colegas ou estranhos estão cometendo atos abusivos contra crianças com o propósito de machucá-las fisicamente. Para prejudicar emocionalmente, os agressores estão enviando mensagens maldosas ou fotos pouco lisonjeiras, fazendo com que suas vítimas se isolem dos outros ou se sintam frustradas.

**Ataque de dicionário**

Ataques de adivinhação de senha usados para invadir um sistema de computador inserindo uma combinação de palavras comuns para gerar senhas em potencial. O mesmo método é usado para adivinhar as chaves de descriptografia de mensagens ou documentos criptografados. Os ataques de dicionário são bem-sucedidos porque muitas pessoas tendem a escolher senhas curtas e simples que são fáceis de adivinhar.

**Unidade de disco**

É uma máquina que lê e grava dados em um disco. Uma unidade de disco rígido lê e grava discos rígidos. Uma unidade de disquete acessa disquetes. As unidades de disco podem ser internas (alojadas em um computador) ou externas (alojadas em uma caixa separada que se conecta ao computador).

**Download**

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um dispositivo periférico. O termo é frequentemente usado para descrever o processo de copiar um arquivo de um serviço online para o próprio computador. O download também pode se referir à cópia de um arquivo de um servidor de arquivos de rede para um computador na rede.

**E-mail**

Correio eletrônico. Um serviço que envia mensagens em computadores através de redes locais ou globais.

**Eventos**

Uma ação ou ocorrência detectada por um programa. Os eventos podem ser ações do usuário, como clicar em um botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

**Exploits**

Uma forma de aproveitar diferentes bugs ou vulnerabilidades que estão presentes em um computador (software ou hardware). Assim, os hackers podem obter o controle de computadores ou redes.

**Falso positivo**

Ocorre quando um mecanismo de varredura identifica um arquivo como infectado quando, na verdade, não está.

**Extensão de nome de arquivo**

A parte de um nome de arquivo, após o ponto final, que indica o tipo de dados armazenados no arquivo. Muitos sistemas operacionais usam extensões de nome de arquivo, por exemplo, Unix, VMS e MS-DOS. Eles geralmente têm de uma a três letras (alguns sistemas operacionais antigos e tristes não suportam mais do que três). Os exemplos incluem "c" para código-fonte C, "ps" para PostScript, "txt" para texto arbitrário.

**Heurística**

Um método baseado em regras para identificar novas ameaças. Este método de verificação não depende de um banco de dados de informações de ameaças específico. A vantagem da verificação heurística é que ela não é enganada por uma nova variante de uma ameaça existente. No entanto, ocasionalmente pode relatar códigos suspeitos em programas normais, gerando o chamado "falso positivo".

**Pote de mel**

Um sistema de computador isca criado para atrair hackers para estudar a maneira como eles agem e identificar os métodos heréticos que usam para coletar informações do sistema. Empresas e corporações estão mais interessadas em implementar e usar honeypots para melhorar seu estado geral de segurança.

**IP**

Protocolo de Internet - Um protocolo roteável no conjunto de protocolos TCP/IP que é responsável pelo endereçamento IP, roteamento e fragmentação e remontagem de pacotes IP.

**miniaplicativo Java**

Um programa Java projetado para ser executado apenas em uma página da Web. Para usar um applet em uma página da web, você deve especificar o nome do applet e o tamanho (comprimento e largura, em pixels) que o applet pode utilizar. Quando a página é acessada, o navegador baixa o applet de um servidor e o executa na máquina do usuário (o cliente). Os applets diferem dos aplicativos porque são regidos por um protocolo de segurança estrito.

Por exemplo, embora os applets sejam executados no cliente, eles não podem ler ou gravar dados na máquina do cliente. Além disso, os applets são ainda mais restritos para que possam apenas ler e gravar dados do mesmo domínio do qual são servidos.

**Keylogger**

Um keylogger é um aplicativo que registra tudo o que você digita. Keyloggers não são maliciosos por natureza. Eles podem ser usados para fins legítimos, como monitorar atividades de funcionários ou crianças. No entanto, eles estão sendo cada vez mais usados por cibercriminosos para fins maliciosos (por exemplo, para coletar dados privados, como credenciais de login e números de CPF).

**Vírus de macro**

Um tipo de ameaça de computador codificada como uma macro incorporada a um documento. Muitos aplicativos, como Microsoft Word e Excel, oferecem suporte a poderosas linguagens de macro. Esses aplicativos permitem que você incorpore uma macro em um documento e execute a macro sempre que o documento for aberto.

**cliente de e-mail**

Um cliente de e-mail é um aplicativo que permite enviar e receber e-mails.

**Memória**

Áreas de armazenamento interno no computador. O termo memória identifica o armazenamento de dados que vem na forma de chips, e a palavra armazenamento é usada para memória que existe em fitas ou discos. Todo computador vem com uma certa quantidade de memória física, geralmente chamada de memória principal ou RAM.

**Não heurístico**

Este método de verificação depende de um banco de dados de informações de ameaças específico. A vantagem da verificação não heurística é que ela não é enganada pelo que pode parecer uma ameaça e não gera alarmes falsos.

**predadores online**

Indivíduos que procuram atrair menores ou adolescentes para conversas com o propósito de envolvê-los em atividades sexuais ilegais. As redes sociais são o local ideal onde crianças vulneráveis podem ser facilmente caçadas e induzidas a praticar atividades sexuais, online ou face a face.

**Programas compactados**

Um arquivo em um formato de compactação. Muitos sistemas operacionais e aplicativos contêm comandos que permitem compactar um arquivo para que ele ocupe menos memória. Por exemplo, suponha

que você tenha um arquivo de texto contendo dez caracteres de espaço consecutivos. Normalmente, isso exigiria dez bytes de armazenamento.

No entanto, um programa que compacta arquivos substituiria os caracteres de espaço por um caractere de série de espaço especial seguido pelo número de espaços sendo substituídos. Nesse caso, os dez espaços exigiriam apenas dois bytes. Esta é apenas uma técnica de empacotamento - existem muitas outras.

**Caminho**

As direções exatas para um arquivo em um computador. Essas direções geralmente são descritas por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre quaisquer dois pontos, como o canal de comunicação entre dois computadores.

**Phishing**

O ato de enviar um e-mail a um usuário que afirma falsamente ser uma empresa legítima estabelecida na tentativa de enganar o usuário para que entregue informações privadas que serão usadas para roubo de identidade. O e-mail direciona o usuário a visitar um site onde é solicitado que ele atualize as informações pessoais, como senhas e números de cartão de crédito, previdência social e contas bancárias, que a organização legítima já possui. O site, no entanto, é falso e criado apenas para roubar as informações do usuário.

**Fóton**

Photon é uma tecnologia inovadora não intrusiva da Bitdefender, concebida para minimizar o impacto da solução de segurança. Ao monitorizar a atividade do seu PC em segundo plano, ele cria padrões de utilização que ajudam a otimizar os processos de arranque e de análise.

**Vírus polimórfico**

Uma ameaça que muda a sua forma com cada ficheiro que infeta. Como não têm um padrão binário consistente, essas ameaças são difíceis de identificar.

**Porta**

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais tendo vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs e teclados.

Externamente, os computadores pessoais portas para ligar modems, impressoras, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

**Ransomware**

Ransomware é um programa malicioso que tenta lucrar com os utilizadores através do bloqueio dos seus sistemas vulneráveis. CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem os sistemas pessoais dos utilizadores.

A infeção pode ser espalhada através do acesso a um e-mail de spam, transferência de anexos de e-mail ou da instalação de aplicações, sem que o utilizador saiba o que está a acontecer no seu sistema. Os utilizadores diários e as empresas são os alvos dos hackers ransomware.

**Arquivo de relatório**

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

**Rootkit**

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, são principalmente utilizados para ocultar ameaças ou esconder a presença de um intruso no sistema. Quando combinados com ameaças, os rootkits são uma grande ameaça à integridade e à segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

**Script**

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interação do utilizador.

**Spam**

Lixo de correio electrónico ou lixo de avisos de newsgroups. Geralmente atribuído a qualquer e-mail não solicitado.

**Spyware**

Qualquer software que encobertamente reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também ser capaz de obter endereços de e-mail e até mesmo palavras-passe e números de cartão de crédito.

O spyware é similar a uma ameaça Cavalo de Troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

**Itens de inicialização**

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã de arranque, um ficheiro de som a ser reproduzido quando o computador arranca, um calendário de lembretes ou aplicações podem ser itens de arranque. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

**Inscrição**

Acordo de compra que dá ao utilizador o direito de utilizar um produto ou serviço específico num número específico de dispositivos e durante um período de tempo determinado. Uma subscrição expirada pode ser automaticamente renovada utilizando as informações fornecidas pelo utilizador na primeira compra.

**Bandeja do sistema**

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

**TCP/IP**

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

**Ameaça**

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria das ameaças também se pode replicar. Todas as ameaças de computador são criadas pelo homem. Uma simples ameaça pode copiar-se várias vezes e é relativamente fácil de produzir. Mesmo uma simples ameaça é perigosa porque pode rapidamente utilizar toda memória disponível e fazer o sistema parar. O tipo de ameaça mais perigoso é aquele que é capaz de se transmitir através de uma rede ou contornando sistemas de segurança.

**Atualização de informações sobre ameaças**

O padrão binário de uma ameaça é utilizado pela solução de segurança para detetá-la e eliminá-la.

**Troiano**

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário de programas de software maliciosos e worms, os Trojans não se replicam, mas podem ser igualmente destrutivos. Um dos tipos mais

insidiosos de ameaças de cavalo de Troia é um programa que afirma remover as ameaças do seu computador, mas, em vez disso, introduz ameaças no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

**Atualizar**

Uma nova versão de um produto de software ou hardware concebida para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da atualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a atualização.

O Bitdefender tem a sua própria funcionalidade de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

**Rede Privada Virtual (VPN)**

É uma tecnologia que ativa uma conexão direta temporária e criptografada para uma certa rede sobre uma rede menos segura. Dessa forma, enviar e receber dados é seguro e criptografado, difícil de virar alvo de espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com o uso de um nome de usuário e senha.

**Worm**

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.