Kaspersky
Internet Security

Ameaças e Exclusões

Configurações	Descrição
Tipos de objetos detectados	O Kaspersky Internet Security detecta vários tipos de objetos, como vírus, worms, cavalos de Troia e adware. Para obter detalhes, consulte a Enciclopédia Kaspersky. É possível desativar a detecção dos seguintes tipos de objetos: • Outros softwares que podem ser usados por criminosos para danificar o seu computador ou os dados pessoais. O software inclui aplicativos de administração remota que os administradores de sistema podem usar para acessar a interface de um computador remoto para fins de monitoramento ou gerenciamento. • Arquivos com várias compactações. Arquivos que são compactados várias vezes, inclusive por vários empacotadores. A embalagem múltipla torna mais difícil a verificação de objetos.
Gerenciar exclusões	Ao clicar nesse link, a janela **Exclusões** é aberta com a lista de exclusões de verificação. Uma *Exclusão de verificação* é um conjunto de condições que, se atendidas, faz com que o Kaspersky Internet Security não verifique um determinado objeto em busca de vírus e outras ameaças. É possível adicionar, editar ou remover exclusões da lista. Na janela para adicionar ou editar uma exclusão, é possível definir condições específicas que, se atendidas, impedirão que os objetos sejam verificados (o Kaspersky Internet Security não os verificará): • Arquivo ou pasta que devem ser excluídos das verificações (também é possível excluir arquivos executáveis de aplicativos e processos). É possível usar máscaras de acordo com as seguintes regras: • O caractere `*` (asterisco) substitui qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos a arquivos com a extensão TXT localizados em pastas na unidade C:, mas não em subpastas. • Dois caracteres `*` consecutivos substituem qualquer conjunto de caracteres (incluindo um conjunto vazio) no nome do arquivo ou da pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes

de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos de arquivos com a extensão TXT localizados na pastas nomeadas `Pasta` e suas subpastas. A máscara deve incluir pelo menos um nível de aninhamento. A mascára `C:\**\*.txt` não é uma máscara válida.

- O caractere `?` (ponto de interrogação) substitui qualquer caractere único, exceto os caracteres `\` e `/` (delimitadores dos nomes de arquivos e pastas em caminhos para arquivos e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos localizados na pasta denominada `Pasta` que tenham a extensão TXT e um nome composto por três caracteres.

- Tipos de objetos que devem ser excluídos das varreduras. Digite o nome do objeto de acordo com a classificação da Enciclopédia da Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). Você pode usar máscaras com o caractere `?` (substitui qualquer caractere único) e o caractere `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Cliente*` for especificada, o Kaspersky Internet Security exclui os objetos `Cliente-IRC`, `Cliente-P2P` e `Cliente-SMTP` das verificações.

- Soma de verificação do objeto. Comparar a soma de verificação de um objeto com a soma de verificação indicada nesta configuração permite que a verificação exclua um objeto que não foi modificado desde a última verificação.

- Componentes de proteção para os quais a exclusão é aplicada.

Em vez de remover uma exclusão da lista, é possível alterar o status de uma exclusão para **Inativo** (na janela para adição ou edição de uma exclusão). Quando inativo, a exclusão não será aplicada.

Especificar os aplicativos confiáveis	Ao clicar neste link, é aberta uma janela com a lista dos aplicativos confiáveis. O Kaspersky Internet Security não monitora as atividades do arquivo e da rede de aplicativos confiáveis (incluindo os maliciosos) e não monitora as consultas desses aplicativos no registro do sistema. É possível adicionar, editar ou excluir aplicativos confiáveis da lista.

Mesmo se um aplicativo estiver na lista de confiáveis, o Kaspersky Internet Security continua a verificar o arquivo executável e o processo desse aplicativo em busca de vírus e outras ameaças. Caso não queira verificar o arquivo executável e o processo de um aplicativo confiável, adicione o aplicativo à lista de exclusões.

Ao adicionar ou editar um aplicativo confiável, na janela **Exclusões do aplicativo**, é possível especificar as regras que serão usadas pelo Kaspersky Internet Security para monitorar a atividade do aplicativo confiável.

Na janela **Exclusões do aplicativo**, as seguintes regras estão disponíveis:

- Não verificar arquivos abertos.
- Não monitorar a atividade de aplicativos. O Controle de Aplicativos não monitora nenhuma atividade de aplicativos.
- Não herdar restrições do processo principal (do aplicativo), se as restrições de um processo ou aplicativo principal não forem herdadas, a atividade de aplicativos será monitorada de acordo com as suas regras definidas ou de acordo com as regras do grupo de confiança ao qual o aplicativo pertence.
- Não monitorar a atividade de aplicativos secundários.
- Não bloquear a interação com a interface do Kaspersky Internet Security. O aplicativo tem permissão para gerenciar o Kaspersky Internet Security usando a interface gráfica do Kaspersky Internet Security. Poderá ser necessário permitir que o aplicativo gerencie a interface do Kaspersky Internet Security ao usar um aplicativo de conexão remota à área de trabalho ou um aplicativo que suporte a operação de um dispositivo de inserção de dados. Exemplos desses dispositivos incluem painéis táteis e tablets gráficos.
- Não verificar todo o tráfego (ou tráfego criptografado). Dependendo da opção selecionada (**Não verificar todo o tráfego** ou **Não verificar o tráfego criptografado**), o Kaspersky Internet Security exclui da verificação todo o tráfego de rede do aplicativo ou o tráfego transmitido por SSL. O valor dessa configuração não afeta a operação do Firewall: O Firewall verifica o tráfego de aplicativos de acordo com as configurações do Firewall. As exclusões afetam o Antivírus de email, o Antivírus da Web e o Antispam. É possível especificar os endereços IP ou as portas de rede aos quais a restrição de controle de tráfego deve ser aplicada.

	Se o status de um aplicativo for alterado para **Inativo**, na janela **Exclusões do aplicativo**, o Kaspersky Internet Security não tratará o aplicativo como um aplicativo confiável. Dessa forma, é possível excluir temporariamente um aplicativo da lista de confiáveis sem realmente excluí-lo da lista.
Usar armazenamento de certificado do sistema confiável	Se um dos armazenamentos/repositórios de certificados de sistema confiáveis for selecionado, o Kaspersky Internet Security exclui os aplicativos assinados com uma assinatura digital confiável das verificações. O Kaspersky Internet Security atribui automaticamente esses aplicativos ao grupo *Confiável*. Se **Não usar** for selecionado, o Kaspersky Internet Security verifica os aplicativos independentemente de eles terem ou não uma assinatura digital. O Kaspersky Internet Security coloca um aplicativo em um grupo de confiança, dependendo do nível de perigo que esse aplicativo pode representar para o computador.

ID do artigo 201385, Última revisão: 1 de abr. de 2021