



brasil

sites mundiais

produtos

compras symantec

serviço e suporte

security response

downloads

sobre a symantec

pesquisa

comentários

ameaças expandidas

As ameaças expandidas (ou expanded threats) existem paralelamente às definições mais comuns de vírus, worms e Cavalos de tróia, os quais podem fornecer acesso não-autorizado, ameaçar o sistema e a segurança dos dados e causar outros tipos de inconveniências. As ameaças expandidas podem ser descarregadas a partir de websites, mensagens de e-mail ou mensagens instantâneas sem o seu conhecimento. Elas também podem ser instaladas ao aceitar o Acordo de Licença do Usuário Final de outro software relacionado a ele ou conectado de alguma forma à ameaça expandida.

Procure por uma Ameaça Expandida (Site em inglês):

apagar

Refine a sua procura selecionando as opções abaixo

Vírus, Worms e Cavalos de tróia

Vulnerabilidades e Ameaças

Adware: Programas que secretamente obtêm informações pessoais do computador e as envia para outro computador através da Internet, geralmente para fins de propaganda. Muitas vezes isso é realizado através d coleta de dados referentes ao uso do navegador da Web ou hábitos de navegação.

Um Adware pode ser descarregado a partir de websites (tipicamente shareware ou freeware), mensagens de e-mail e mensagens instantâneas. Um usuário pode, inadvertidamente, ativar um adware ao aceitar o Acordo de Licença do Usuário Final de um programa ligado ao adware. [Mais informações](#) *(em inglês)*

Discadores: Programas que utilizam o sistema sem sua permissão ou conhecimento, para efetuar uma discagem através da Internet para um número 0900 ou um site FTP, tipicamente para acarretar cobranças. [Mais informações](#) *(em inglês)*

Ferramentas de Invasão: Ferramentas usadas por invadores (hackers) para obter acesso não-autorizado ao seu computador. Um exemplo de ferramenta de invasão é o registrador de toques no teclado -- um programa que detecta e registra os toques no teclado e pode enviar essas informações para o invasor. [Mais informações](#) *(em inglês)*

Programas Brincalhões: Programas que alteram ou interrompem o comportamento normal do computador, gerando distração ou inconveniências. [Mais informações](#) *(em inglês)*

Acesso Remoto: Programas que permitem que outro computador obtenha informações, ataque ou altere seu computador, geralmente através da Internet. Programas de acesso remoto detectados em verificações de vírus podem ser reconhecidos como softwares comerciais, os quais são apresentados ao usuário durante a verificação. [Mais informações](#) *(em inglês)*

Riscos à Segurança: Ameaças que não possuem características para serem definidas como vírus, Cavalos de tróia ou worms, mas que ameaçam seu computador e seus dados. [Mais informações](#) *(em inglês)*

Spyware: Programas independentes que podem monitorar as atividades do sistema de maneira secreta. Estes podem detectar senhas e outras informações confidenciais e enviá-las para outro computador.

Programas do tipo Spyware podem ser descarregados a partir de websites (tipicamente shareware ou freeware), mensagens de e-mail e mensagens instantâneas. O usuário pode ativar inadvertidamente o spyware ao aceitar o Acordo de Licença do Usuário Final de um software conectado ao spyware. [Mais informações](#) *(em inglês)*

Vírus, Worms e Cavalos de tróia: Um vírus é um programa ou código que se replica, ou seja, infecta outro programa, setor de boot, setor de partição ou documentos que suportam macros, inserindo-se naquele meio. Muitos vírus apenas replicam-se, embora também possam causar grandes danos.

Um worm é um programa que cria cópias de si mesmo - por exemplo, de uma unidade para a outra - ou copiando-se usando e-mail ou outro mecanismo de transporte. O worm pode comprometer a segurança do computador. Ele pode ser recebido na forma de um programa brincalhão ou software do tipo.

Um Cavalo de tróia é um programa que não se replica nem cria cópias de si mesmo, mas causa danos ou compromete a segurança do computador. Tipicamente uma pessoa envia, através de e-mail, o Cavalo de tróia para você - esse tipo de software não consegue propagar-se através de e-mail - e pode ser recebido na forma de um programa brincalhão ou software do tipo. [Mais informações](#) *(em inglês)*