Noções de Vírus, Worms

Noções De Vírus Worms e Pragas Virtuais

Hoje em dia é comum utilizarmos o computador para realizar diversas atividades no dia a dia. Para auxiliar nestas tarefas utilizamos programas que são criados com o objetivo de facilitar o uso do computador. Mas existem também programas que são utilizados para prejudicar quem usa o computador, esses são os vírus. Existem diferentes tipos de vírus para computador veja a seguir como identificar cada um deles.

Segundo o site da Microsoft, os vírus de computador são pequenos programas desenvolvidos para se espalhar de um computador a outro e interferir no funcionamento do computador. Um vírus pode corromper ou excluir dados de seu computador, usar seu programa de e-mail para se espalhar para outros computadores ou até mesmo apagar todos os dados de seu disco rígido. Os vírus de computador são frequentemente espalhados por meio de anexos em mensagens de e-mail ou mensagens instantâneas. Por isso, é essencial nunca abrir anexos de e-mail, a menos que sua origem seja conhecida e você esteja esperando pelo arquivo.

Os vírus podem ser disfarçados na forma de anexos com imagens divertidas, cartões ou arquivos de áudio e vídeo.

Os vírus de computador também se espalham por meio de downloads na internet. Eles podem estar escondidos em software ilícito ou em outros arquivos ou programas que você baixe.

Para ajudar a evitar vírus de computador, é essencial manter seu computador em dia com as atualizações mais recentes e ferramentas antivírus, mantenha-se informado sobre ameaças recentes, execute seu computador como usuário padrão (não como administrador), e siga algumas regras básicas ao navegar na Internet, baixar arquivos e abrir anexos.

Depois que um vírus se instalou em seu computador, saber seu tipo ou o método utilizado para se instalar não é tão importante quanto removê-lo e evitar novas infecções.

Tipos

Cavalo-De-Tróia

A denominação “Cavalo de Tróia” (Trojan Horse) foi atribuída aos programas que permitem a invasão de um computador alheio com espantosa facilidade. Nesse caso, o termo é análogo ao famoso artefato militar fabricado pelos gregos espartanos. Um “amigo” virtual presenteia o outro com um “presente de grego”, que seria um aplicativo qualquer. Quando o leigo o executa, o programa atua de forma diferente do que era esperado.

Ao contrário do que é erroneamente informado na mídia, que classifica o Cavalo de Tróia como um vírus, ele não se reproduz e não tem nenhuma comparação com vírus de computador, sendo que seu objetivo é totalmente diverso. Deve-se levar em consideração, também, que a maioria dos antivírus faz a sua detecção e os classificam como tal. A expressão “Trojan” deve ser usada, exclusivamente, como definição para programas que capturam dados sem o conhecimento do usuário.

O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conectar-se à Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente. Só quem já esteve dentro de um computador alheio sabe as possibilidades oferecidas.

Worm

Os worms (vermes) podem ser interpretados como um tipo de vírus mais inteligente que os demais. A principal diferença entre eles está na forma de propagação: os worms podem se propagar rapidamente para outros computadores, seja pela Internet, seja por meio de uma rede local.

Geralmente, a contaminação ocorre de maneira discreta e o usuário só nota o problema quando o computador apresenta alguma anormalidade. O que faz destes vírus inteligentes é a gama de possibilidades de propagação. O worm pode capturar endereços de e-mail em arquivos do usuário, usar serviços de SMTP (sistema de envio de e-mails) próprios ou qualquer outro meio que permita a contaminação de computadores (normalmente milhares) em pouco tempo.

Spywares, Keyloggers E Hijackers

Apesar de não serem necessariamente vírus, estes três nomes também representam perigo. Spywares são programas que ficam “espionando” as atividades dos internautas ou capturam informações sobre eles. Para contaminar um computador, os spywares podem vir embutidos em softwares desconhecidos ou serem baixados automaticamente quando o internauta visita sites de conteúdo duvidoso.

Os keyloggers são pequenos aplicativos que podem vir embutidos em vírus, spywares ou softwares suspeitos, destinados a capturar tudo o que é digitado no teclado. O objetivo principal, nestes casos, é capturar senhas.

Hijackers são programas ou scripts que “sequestram” navegadores de Internet, principalmente o Internet Explorer. Quando isso ocorre, o hijacker altera a página inicial do browser e impede o usuário de mudá-la, exibe propagandas em pop-ups ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de software antivírus, por exemplo).

Os spywares e os keyloggers podem ser identificados por programas anti-spywares. Porém, algumas destas pragas são tão perigosas que alguns antivírus podem ser preparados para identificá-las, como se fossem vírus. No caso de hijackers, muitas vezes é necessário usar uma ferramenta desenvolvida especialmente para combater aquela praga. Isso porque os hijackers podem se infiltrar no sistema operacional de uma forma que nem antivírus nem anti-spywares conseguem “pegar”.

Hoaxes, O Que São?

São boatos espalhados por mensagens de correio eletrônico, que servem para assustar o usuário de computador. Uma mensagem no e-mail alerta para um novo vírus totalmente destrutivo que está circulando na rede e que infectará o micro do destinatário enquanto a mensagem estiver sendo lida ou quando o usuário clicar em determinada tecla ou link. Quem cria a mensagem hoax normalmente costuma dizer que a informação partiu de uma empresa confiável, como IBM e Microsoft, e que tal vírus poderá danificar a máquina do usuário. Desconsidere a mensagem.

Antivírus Podem Ser Pagos Ou Gratuitos

Os **antivírus** são programas de computador concebidos para prevenir, detectar e eliminar vírus de computador.

Existe uma grande variedade de produtos com esse intuito no mercado, e a diferença entre eles está nos métodos de detecção, no preço e nas funcionalidades.

Para o usuário doméstico, existe a opção de utilizar um antivírus gratuito ou um pago. A diferença está nas camadas a mais de proteção que a versão paga oferece, além do suporte técnico realizado por equipe especializada.

Antispywares Eliminam Adwares Também

Um antispyware é um software de segurança que tem o objetivo de detectar e remover adwares e spywares.

A principal diferença de um anti-spyware de um antivírus é a classe de programas que eles removem. Adwares e spywares são consideradas áreas “cinza”, pois nem sempre é fácil determinar o que é um adware e um spyware.

Muitos antivírus já incorporam detecção de spyware e adware, mas um antispyware específico ainda faz parte da programação de segurança da maioria dos usuários.

Firewall Controla Tráfego Da Rede

Firewall em português é o mesmo que parede corta-fogo, um tipo de parede, utilizada principalmente em prédios, e que contém o fogo em casos de incêndio. O firewall da informática faz jus ao nome, funcionando de maneira análoga ao mecanismo de contenção de fogo. Ao invés de barrar o avanço deste, age interceptando e impedindo a difusão de conexões não autorizadas e/ou nocivas em uma rede.

Um firewall trabalha controlando o tráfego em uma rede, usando para isso um conjunto de regras. Ele determina qual o conteúdo poderá trafegar pela rede, bem como as conexões que serão aceitas ou negadas. Se, por exemplo, um hacker tentar acessar a rede, ou até mesmo um único computador ligado à internet, e há um firewall configurado adequadamente, o acesso dele será interceptado e bloqueado. O mesmo vale para os worms, pragas que utilizam a rede para se disseminarem.

Os firewalls podem se apresentar sob duas formas: software e hardware. A primeira, mais comum, são programas que o usuário instala na máquina para realizar o controle das conexões, tanto as que entram, como as que saem.

Já sob a forma de hardware, temos equipamentos específicos que reforçam a segurança de uma rede. Esses geralmente são empregados em redes de grande porte, principalmente em empresas que necessitam de mais segurança a suas máquinas, uma vez que são equipamentos nem um pouco baratos.

Embora utilizar os dois tipos seja o ideal para reforçar a segurança de uma rede, dispor de um bom software e navegar com cautela pela Iinternet são medidas triviais que ajudarão, e muito, a impedir que o computador — ou rede — seja invadido por um hacker.