Definindo softwares mal intencionados (malwares): Perguntas Mais Freqüentes

Por Robert Moir, MVP em segurança
Data de publicação: Outubro de 2003

Resumo

Este documento é uma compilação das Perguntas Freqüentes sobre "*malwares*", um termo geral usado para todos os formatos desse tipo de software.

Perguntas sobre softwares mal intencionados

P: O que são *malwares*, vírus, *spywares* e *cookies* e como diferenciá-los?

R: Vamos falar sobre o mais fácil primeiro. "Malware" é um termo geral normalmente usado para se referir a qualquer software desenvolvido para causar danos em computadores, servidores ou redes de computador, independentemente de ser vírus, *spyware*, etc.

P. O que exatamente é um vírus? Um "worm" também é um vírus?

Vírus são programas ou scripts de computador que tentam se espalhar de um arquivo para outro em um computador e/ou de um computador para outro usando vários métodos, sem o conhecimento e sem o consentimento do usuário desse computador. Um worm é um tipo específico de vírus que se propaga em vários computadores, normalmente criando cópias dele mesmo em cada memória do computador.

Muitos usuários definem vírus simplesmente como programas de truques desenvolvidos para excluir ou mover dados da unidade de disco rígido, o que, de certa forma, está correto. Do ponto de vista técnico, o que torna o vírus um vírus é a sua capacidade de espalhar-se. O dano que ele causa é freqüentemente incidental quando é feito um diagnóstico.

Obviamente, qualquer dano incidental é importante, mesmo quando os autores não pretendem criar problemas com seus vírus; eles ainda podem causar danos intencionalmente, pois o autor não antecipou o efeito total ou os efeitos colaterais não intencionais. O método mais comum usado para espalhar um vírus é por meio do anexo presente no e-mail. O envio de um vírus, mesmo que ele não seja prejudicial, pode causar danos imprevisíveis.

P. Como posso evitar que meu computador seja infectado por um vírus?

Um programa antivírus é a ferramenta mais comum para prevenção. Esse utilitário analisa um programa de computador antes de executá-lo e encerra-o se reconhecer a assinatura de um código mal-intencionado. Muitos antivírus também avaliam os programas para determinar se eles contêm quaisquer características relacionadas a vírus.

A melhor forma de evitar um vírus é usar o bom-senso. Se um programa de computador executável está anexado a um e-mail e você não confia na origem do e-mail, exclua-o imediatamente. Não baixe nenhum aplicativo ou arquivo executável de origem desconhecida e seja cuidadoso ao trocar arquivos com outros usuários.

P. O que é um "cavalo de Tróia"? Ele não é um vírus com um outro nome?

Já ouvi falar que o malware Cavalo de Tróia (*Trojan Horse*) é um subconjunto de vírus (e vice-versa), mas há diferenças que devem ser mencionadas.

Um Cavalo de Tróia enquadra-se na definição de vírus que a maioria das pessoas usa, no sentido de que ele tenta invadir um computador sem o conhecimento e sem o consentimento do usuário. Um Cavalo de Tróia, semelhante a sua contraparte mitológica grega, apresenta-se freqüentemente de uma forma quando, na verdade, ele tem outra. Um exemplo recente de software mal-intencionado agindo com um Cavalo de Tróia é a versão de e-mail do vírus "Swen" que, de modo falso, representa um aplicativo de atualização da Microsoft.

Os Cavalos de Tróia normalmente executam uma destas ações: eles destroem ou modificam dados, como apagar uma unidade de disco rígido, no momento em que são ativados ou tentam descobrir ou roubar senhas, números

de cartão de crédito e outras informações confidenciais.

Os Cavalos de Tróia podem representar um problema maior que outros tipos de vírus, pois são desenvolvidos para serem destrutivos, de modo oposto aos vírus e aos worms, em que o invasor pode não ter a intenção de causar nenhum dano. Essencialmente, essa diferença não é importante na prática. Você pode considerar vírus, Cavalos de Tróia e worms como "coisas que não quero no meu computador ou na minha rede".

P. Como posso evitar um ataque de Cavalo de Tróia?

Os métodos para lidar com Cavalos de Tróia são geralmente os mesmos usados para lidar com vírus. A maioria dos programas antivírus combate alguns dos Cavalos de Tróia comuns, com vários graus de sucesso. Há também programas "anti-cavalos de Tróia" específicos disponíveis, mas a sua melhor arma ainda é o bom-senso. Marque outro ponto para a computação segura!

P. O que são *cookies* e *spyware*? Qual a diferença entre eles?

Um *cookie* é apenas um bit de texto em um arquivo no computador, contendo uma pequena quantidade de informações que o identificam para um site específico e quaisquer outras informações que o site deseja manter sobre o usuário que o visita.

Os *cookies* são ferramentas legítimas usadas por muitos sites para rastrear as informações do visitante. Como exemplo, posso acessar uma loja online de um computador e colocar um item na cesta, mas decidir não comprá-lo imediatamente porque desejo comprar preços. A loja pode optar por gravar as informações sobre os produtos colocados na minha cesta em um *cookie* armazenado no meu computador. Esse é um exemplo de um bom uso de *cookies* para aprimorar a experiência do usuário.

Os únicos sites que devem recuperar as informações armazenadas em um *cookie* são aqueles que gravaram as informações nesse *cookie* específico. Isso deve assegurar sua privacidade impedindo que qualquer outro site que esteja visitando possa ler os *cookies* criados por aquele site.

P. Alguns sites usam *cookies* para explorar as informações do usuário?

R. Infelizmente sim. Alguns podem enganar os usuários ou omitir suas diretivas. Por exemplo, eles podem rastrear seus hábitos de navegação na Web em site diferentes, sem que você saiba, e usar esses dados para personalizar os anúncios que você vê nos sites, etc, o que é normalmente considerado invasão de privacidade.

É difícil identificar essa e outras formas de "mau uso de *cookies*", o que dificulta decidir se, quando e como bloqueá-los no sistema. Além disso, o nível aceitável de informações compartilhadas varia entre os usuários, tornando difícil criar um programa "anticookie" para atender às necessidades de cada um.

P. Como o *spyware* explora as informações do usuário?

O problema de *spyware* é semelhante ao problema dos *cookies* pelo fato de ambos serem considerados uma invasão de privacidade, embora o *spyware* seja diferente dos *cookies*, tecnicamente falando. O *spyware* é um programa executado no computador, que rastreia seus hábitos e personaliza esses padrões para anúncios, etc. Como ele é um programa de computador e não apenas um bit de texto em um cookie, o *spyware* também pode realizar ações irritantes para garantir seu funcionamento e influenciar o que você vê.

P. Como sei se o *spyware* está em execução no meu computador?

É possível usar programas de detecção como o AdWare e outros. Semelhante ao software antivírus, esses programas comparam uma lista de *spyware* conhecidos aos arquivos no computador e remove o que for detectado. Mas o que alguns consideram inaceitável é perfeitamente aceitável para outros.

P. Como o *spyware* é instalado nos computadores?

Táticas comuns para instalações ilegais incluem execução de programas de anúncios em downloads de programas de shareware "gratuitos", e, quando instalado, o *spyware* pode baixar anúncios 24 horas por dia e sobrepô-los em sites e programas em uso. Os programas anti-*spyware* podem impedir que o *spyware* seja instalado, mas a melhor estratégia é saber o que irá baixar e instalar.

P. O *spyware* pode enviar informações rastreadas a outras pessoas?

Algumas formas de *spyware* monitoram o uso da Web de destino ou, até mesmo, o uso geral do computador e

enviam essas informações de volta para o autor do programa *spyware* para serem usadas. Para enfrentar esse tipo de problema, uma ferramenta de remoção de *spyware* é certamente útil, caso seja um firewall que monitore as conexões de saída do computador. Outras formas de o *spyware* assumir partes da sua interface de navegação da Web são forçá-lo a utilizar os mecanismos de pesquisa impostos por ele, onde é possível rastrear seus hábitos de navegação e enviar anúncios pop-up a você sempre que quiserem.

A maior preocupação em relação ao *spyware* está no fato de a maioria deles ser mal-escrita ou mal-projetada. Muitas pessoas percebem que um *spyware* está em execução no computador somente quando este se torna lento ou pára de responder, especialmente ao realizar determinadas tarefas como procurar sites ou recuperar e-mails. Além disso, o *spyware* mal-escrito pode freqüentemente fazer com que o computador funcione de forma incorreta mesmo *depois* de ser removido.

P. Você possui um resumo rápido sobre como evitar problemas de software mal-intencionado?

R: Sim - veja abaixo.

Duas das maiores preocupações dos usuários de computador hoje são vírus e *spyware*. Nos dois casos, vimos que, embora eles sejam um problema, você pode defender-se deles muito bem com apenas um pouco de planejamento:

- Mantenha seu software de computador corrigido e atualizado. O sistema operacional e o aplicativo antivírus devem ser atualizados regularmente.
- Baixe as atualizações somente de fontes confiáveis. Para sistemas operacionais Windows, sempre visite http://windowsupdate.microsoft.com, e para outros softwares acesse os sites legítimos das empresas ou das pessoas que os produziram.
- Pense sempre antes de instalar algo, compare os riscos e os benefícios e esteja ciente das particularidades. O enorme contrato de licença que não deseja ler esconde um aviso informando que você está prestes a instalar um *spyware*?
- Instalar e usar um firewall. Se você estiver executando o Windows XP, será possível usar o firewall de software interno no Painel de Controle; além disso, há versões gratuitas de firewalls que funcionam em todas as versões do Windows.
- Prevenir e sempre melhor que remediar.