Vírus

O vírus de computador, assim denominado em função de uma analogia com o vírus biológico, são programas maliciosos desenvolvidos com o propósito de causar algum efeito danoso sobre o computador e/ou sobre as informações nele contidas e capazes de se reproduzir independente da vontade ou participação do usuário. O ato de se reproduzir, no caso destes vírus, é a capacidade do mesmo de se copiar de um computador a outro, utilizando-se de diversos meios.

Para os usuários em geral, qualquer tipo de código malicioso que apague os dados ou atrapalhe o funcionamento dos computadores é chamado de vírus. Atualmente, os chamados vírus de computador são classificados em vários tipos, cada um com suas particularidades de funcionamento, formas de contágio e disseminação. Existem programas que podem atuar de forma semelhante aos vírus, mas que apresentam características diferentes, como os worms e cavalos-de-tróia. Os principais tipos de vírus são os seguintes:

- **Vírus simples**: a RFC 2828 define um vírus de computador como sendo um software com capacidade de se duplicar, infectando outros programas, usualmente com alguma intenção maliciosa. Um vírus não pode executar-se sozinho, requer que o seu programa hospedeiro seja executado para ativar o vírus;

- **Cavalos de Tróia**: é definido pela RFC 2828 como sendo um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança. Não possui a capacidade de se auto-replicar. Como exemplo pode-se citar um jogo puxado pela Internet, que na verdade, ao ser executado, tira a atenção do usuário enquanto executa algum dano ao computador ou seus dados em segundo plano;

- **Worm** ou “verme”: definido pela RFC 2828 como sendo um programa de computador que pode se executar independentemente, propagar-se pelos computadores em uma rede sozinho, podendo consumir os recursos dos computadores destrutivamente;

- **Vírus polimorfo**: tipo de vírus que modifica a si mesmo a medida que se dissemina, dificultando a sua localização e eliminação;

- **Vírus de Macro**: utiliza-se da linguagem VBScript, podendo ser executado em qualquer computador que possua aplicativos baseados nessa linguagem (por exemplo, Word).

- **Vírus de disco**: infecta o setor de boot da máquina, responsável pela manutenção dos arquivos;

- **Vírus residente em memória**: O vírus permanece na memória após o uso do programa infectado;

- **Vírus residente em setor ou arquivos**: infectam arquivos executáveis ou de extensão .SYS, .OVL, .MNT;

- **Retrovírus**: são vírus que têm como alvo o programa antivírus;

- **Multi-partite**: infectam tanto o setor de boot quanto os arquivos executáveis e são extremamente sofisticados.

Outras Ameaças

Além dos programas maliciosos, uma rede de computadores pode ser ameaçada por outras fontes. Podemos destacar:

Código Móvel

Essa ameaça à segurança de redes é descrita como sendo aplicativos que usam tecnologias legítimas, como Java e Active X, com intenções de roubar informações, instalar backdoors nos computadores atingidos, entre outros. Essas tecnologias normalmente apresentam alguma vulnerabilidade, que poderá ser descoberta pelos crackers e utilizadas para alguma atividade maliciosa.

Os códigos podem ser disseminados como anexos de e-mail (comportam-se como vírus) ou simplesmente através da visita a páginas mal intencionadas (o código malicioso chega ao computador através da própria página Web).

As atividades em código móvel podem ser classificadas de acordo com os problemas que acarretam:

- Modificação do sistema: o código alterar o registro do sistema, alterar configurações de segurança do navegador de Internet, introduzir componentes Active X e Java adicionais para abrir portas de acesso, introduzir um vírus, alterar arquivos de dados e fazer com que um aplicativo se comporte de forma inesperada;

- Invasão de privacidade: o código móvel exporta do computador atingido informações do sistema para qualquer destino como envio de e-mail utilizando a conta do usuário, documentos, planilhas, senhas, etc;

- Recusa de serviço: o código tenta alocar toda a memória disponível ou criar várias de janelas na máquina para ocupá-la, evitando que outros programas funcionem adequadamente.

Hoax

Além do aparecimento de novas ameaças diariamente, os usuários de redes de computadores sofrem a ação do boato (hoax), que causa prejuízos semelhantes aos dos vírus. Um hoax é um alarme falso, um boato, enfim uma notícia sobre uma ameaça inexistente. Estas notícias são normalmente propagadas através de listas de e-mail, causando freqüentemente prejuízos devido a recomendações maliciosas e falsas para ajuste e atualização de programas e sistemas. Por exemplo, é comum um boato sugestionar que o usuário apague um arquivo manualmente.

O hoax é escrito de forma a parecer um alerta autêntico, geralmente fazendo referências a fontes conhecidas e respeitadas. Não é raro que o alerta instrua os usuários a passarem a mensagem para outros usuários, criando uma corrente que espalha o boato com grande velocidade.

As mensagens de boatos geralmente utilizam uma linguagem técnica de difícil compreensão. Um hoax típico alerta para vírus não monitorados pelos programas de antivírus, havendo casos em que o alerta avisa que o vírus é capaz de destruir até mesmo o hardware. Na verdade, elas visam causar pânico, coletar dados de usuários ou mesmo aumentar o tráfego nas linhas de comunicação ou sites famosos, congestionando-os.

Cookies

Cookies são blocos de texto recebidos pelo usuário ao acessar um site. O cookie pode ficar armazenado em um computador e ser ativado a cada novo acesso. O principal propósito do cookie é identificar o usuário e personalizar a navegação. Por esse motivo, são considerados coletores de informações pessoais.

Os cookies podem ser usados pelos sites para rastrear a identificação on-line do usuário, o número de visitas que fez e para guardar a sua identificação e senha quando se pula de uma página para outra, e de forma que o internauta não precise reescrevê-la quando retornar ao site, entre outras aplicações.

Embora os cookies sejam geralmente utilizados para agilizar a resposta do site, o usuário nem sempre sabe, no instante em que recebe o cookie, qual a sua finalidade. O grande problema é que os cookies são utilizados por empresas que vasculham as preferências pessoais do usuário e espalham estas informações para outros sites de comércio eletrônico. Assim o usuário de internet sempre terá páginas de promoções ou publicidade, nos sites de comércio eletrônico, dos produtos de seu interesse. Na verdade, não se trata de um problema de segurança, mas alguns usuários podem considerar este tipo de atitude uma invasão de privacidade.

Spam

Spams são as famosas mensagens eletrônicas não solicitadas. A palavra spam é uma alusão ao barulho que os vikings faziam ao bater na mesa das

tabernas para aborrecer o cliente. O spam não é oficialmente proibido, mas considera-se, na Internet, uma falta de ética.

Deve-se ter cuidado ao remeter dados pessoais (nome, e-mail, endereço, números de documentos e, principalmente, número de cartão de crédito) para qualquer site visitado. Deve-se ter sempre em mente que estas informações são guardadas em algum banco de dados do site e podem ser vendidas para outras empresas.

Programas de Troca Instantânea de Mensagens

São programas que possibilitam a troca de mensagens e endereços de sites da Internet. O programa utiliza a Internet para se conectar a um servidor específico. Vírus e worms também podem ser enviados em mensagens instantâneas, sem estarem sujeitos à análise dos antivírus, filtragem de conteúdo e outras medidas geralmente usadas na segurança de programas corporativos de correio eletrônico.

Normalmente, a troca de mensagens não passa pelo servidor. Toda vez que a conexão é feita, o servidor passa a conhecer o endereço na Internet (endereço IP) do computador. Os programas que utilizam a Internet para prestar algum serviço (neste caso troca de mensagens) ficam conectados permanentemente a um servidor e, como normalmente esses programas possuem backdoors, ficam sujeitos a ataques externos.

Programas de Distribuição de Arquivos

Arquivos podem ser enviados (upload) ou recebidos (download) por um computador por vários meios diferentes. Os meios mais comuns são através do e-mail, programas de mensagem instantânea e através dos browsers.

Quando um programa de distribuição de arquivos se conecta ao servidor, envia uma lista dos arquivos que estão em uma pasta específica (já pré-configurada na instalação do programa) e esta lista fica disponível para os demais usuários do programa no mundo todo. Quando se busca por um tipo de arquivo específico (música, por exemplo), o programa pergunta ao servidor quais computadores possuem aquele arquivo. Quando se escolhe um dos arquivos, o programa que está rodando na máquina se conectará ao programa da outra máquina e baixará o arquivo escolhido para alguma pasta do computador (já pré-configurada e, normalmente, diferente da pasta anterior). Assim, o único trabalho do servidor é manter uma lista de quais computadores estão no ar (conectados à internet e rodando o programa de distribuição de arquivos) e a lista dos arquivos disponíveis. O trabalho de baixar os arquivos e enviar os arquivos é do computador.

Dificilmente arquivos de música, foto ou vídeo apresentarão problemas, a dificuldade maior será com os arquivos de programas que poderão conter vírus ou Cavalo de Tróia embutidos. Assim, quanto à segurança, vale a mesma regra dos casos anteriores, evite baixar da rede programas ou arquivos de desconhecidos, pois eles podem conter vírus ou cavalos-de-tróia.