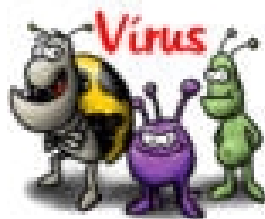


Índice

GENERALIDADES SOBRE ANTI-VÍRUS	2
Contaminação	3
Detecção de vírus	4
Algumas formas de evitar Vírus	4
Worms	5
Variantes	5
Trojan Horse (Cavalo de Tróia)	6
Spywares	7



GENERALIDADES SOBRE ANTI-VÍRUS

O primeiro passo para que você possa proteger o seu micro do ataque de vírus é compreender o que é um vírus, como ele atua, como pode ser "distribuído" e etc.

Os Vírus nada mais são do que programas de computador, contendo código malicioso, que possuem capacidade de se multiplicar mediante a infecção de outros programas maiores.

Dependendo da "capacidade" do "profissional" que gerou este programa, o efeito da execução do mesmo (infecção do seu micro pelo vírus) pode variar de alguns efeitos que desagradam ao usuário, porém não destroem as informações do micro como:

- ✓ O computador deixa de trabalhar corretamente, placas não são reconhecidas, apesar de estarem corretamente instaladas e etc;
- ✓ O surgimento de mensagens de erro constantes em determinados aplicativos, principalmente os relacionados aos trabalhos com a Internet (navegador, programa de e-mail e etc);
- ✓ Alguns aplicativos são finalizados automaticamente, sem que o usuário tenha solicitado esta operação;
- ✓ Seu sistema se torna extremamente lento, sem explicação aparente.

Os efeitos da contaminação podem gerar danos irreparáveis também, como por exemplo, perda total dos dados armazenados no disco do computador.

Contaminação



O vírus espalha-se pelo computador a partir do momento em que a máquina executa um programa contaminado. Isso pode ocorrer por meio de download's de programas, através de e-mails que tenham arquivos anexados, através de disquetes infectados, ou através de arquivos em uma rede (interligação entre computadores). Os vírus de computador podem ficar escondidos dentro da máquina por um determinado período, enquanto contaminam outros programas e até mesmo outras máquinas. O momento de início da transmissão do vírus varia bastante. Pode ser uma data comemorativa, um comando ou uma situação específica, como por exemplo, a centésima inicialização do computador. Existem várias formas de contágio e os efeitos da contaminação são diversos.



Apenas navegar pela Web pode parecer um gesto inocente, sem maiores problemas ou culpa, principalmente no que diz respeito a infecção do seu equipamento por vírus. Hoje um micro pode ser infectado (principalmente não possuindo um bom programa Anti-Vírus) através do simples processo de navegação. Conforme pesquisado no site da Symantec, foi descoberta tempos atrás uma classe de vírus chamada de "Vírus de Script". Como o próprio nome diz, estes vírus ficam armazenados em pequenos arquivos de Script que ficam armazenados em páginas da Internet e poderão infectar computadores que acessam os sites infectados. A principal forma de contágio deste tipo de vírus não se dá pela navegação em si, mas pelos problemas de segurança dos softwares de e-mail/navegação, ou seja, a partir do momento que um e-mail infectado é recebido (sem arquivos anexos) o script malicioso é executado no computador sem que o usuário perceba e a partir deste momento o micro já está infectado. Devido a este motivo é fundamental que você instale periodicamente os Services Packs (pacotes de atualização) do seu sistema de navegação/e-mail, bem como do sistema operacional de sua máquina.

Os vírus mais suaves se contentam em assustar o usuário, provocando alguns efeitos periódicos no equipamento, exibindo mensagens, produzindo sons etc., outros são bastante destrutivos, sendo o alvo dos vírus, em geral, o conteúdo dos discos rígidos.

Detecção de vírus

Infelizmente, não há solução genérica para se evitar o vírus. Por isso, não existe uma única forma de se descrever os passos necessários para se detectar uma possível contaminação de um sistema por vírus. Uma forma de se proteger dos vírus é a utilização de programas antivírus.

Os antivírus devem ser atualizados ao menos semanalmente, buscando-se ter sempre o maior número de vírus que possam ser detectados. Mesmo assim, é importante lembrar que esta detecção não corresponde a 100%, pois todos os dias surgem novos vírus. Com o antivírus você reduzirá bastante a possibilidade de se infectar.

Algumas formas de evitar Vírus

- ✓ E-mails contaminados (principalmente com anexos executáveis). Suspeite de anexos de e-mail proveniente de origens desconhecidas. Abrir ou executar estes anexos é como "aceitar carona de estranhos". Os vírus mais recentes podem enviar mensagens de e-mail que parecem ter sido enviadas por pessoas que você conhece, mas na verdade não foram.
- ✓ Download de arquivos na Web ou rede local (principalmente em sites não confiáveis/desconhecidos). Sempre passar o antivírus em cada arquivo antes mesmo de descompactar.
- ✓ Através de disquetes que contenham arquivos contaminados. Não utilize disquetes sem antes passar o antivírus. Evite deixar um disco flexível no computador. Se você reiniciar um computador usando um disquete infectado, na reinicialização, o computador tentará ler a unidade de disquete e é neste momento que o vírus de setor de inicialização pode infectar o disco rígido. Sempre proteja seus disquetes contra gravação depois de terminar de gravar neles.
- ✓ Use o seu bom senso. Se um arquivo ou programa parecer muito bom para ser verdade, suspeite. Muitos dos vírus mais perigosos (incluindo o Melissa) foram originalmente obtidos por download de grupos de notícias, sites ou grupos de usuários pornográficos.
- ✓ Mantenha seu(s) programa(s) Antivírus sempre atualizados.

✓ Use permanentemente os módulos de escaneamento constante da memória (são chamadas de programas tipo vírus-shield), de tal sorte a ter uma segunda chance de pegar um vírus quando você esquecer de escanear um novo programa ou documento.

✓ Programas do tipo ICQ e MSN poderão contaminar o seu equipamento



com vírus. Observe por exemplo que o ICQ possui

um serviço de mensagens que possibilita a um determinado usuário enviar arquivos em anexo para outro usuário e, este arquivo poderá estar contaminado. Isso não significa que, o remetente tenha enviado o arquivo contaminado de forma proposital, pois na maioria dos casos, este usuário também desconhece que seu equipamento está contaminado.

Os códigos maliciosos não se resumem a vírus, que fazem parte de um grupo deste tipo de código. Ainda temos nesta mesma categoria dois outros grupos, conforme podemos observar na listagem abaixo:

- ✓ Worms;
- ✓ Variantes;
- ✓ Trojan Horse;
- ✓ Spywares.

Worms

Um programa que faz cópias de si mesmo, por exemplo: de uma unidade de disco para outra ou através de e-mail ou outro mecanismo de transporte. Ele pode danificar o computador e comprometer sua segurança, apresentando-se sob a forma de algum software.

Variantes

Novas linhagens de vírus que "tomam emprestado" o código de outros vírus conhecidos, em graus variados. As variantes em geral são identificadas por uma ou mais letras após o "sobrenome" do vírus, como: VBS.LoveLetter.B., VBS.LoveLetter.C etc.

Trojan Horse (Cavalo de Tróia)

Assim como na mitologia grega, a cidade de Tróia era extremamente fortificada, os militares gregos a consideravam inexpugnável. Para dominá-la os gregos construíram uma enorme estátua de madeira na forma de um cavalo e deram de presente para os troianos que a aceitaram de bom grado. O problema é que o cavalo foi recheado com centenas de soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos soldados gregos e a dominação de tróia. Daí surgiram os termos “presente de grego” e “Cavalo de Tróia”.

Os cavalos de tróia ou trojan horses estes programas são construídos de tal maneira que, uma vez instalados nos computadores, abrem portas em seus micros, tornando possível o roubo de informações (arquivos, senhas, etc.).

Normalmente você receberá o cavalo de tróia como “presente”. Ele pode ser dado a você de várias maneiras, mas na maioria das vezes ele vem anexado a algum e-mail. Estes e-mails vêm acompanhados de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. A melhor política é nunca abrir um arquivo anexado, principalmente se o remetente for desconhecido.

Programas piratas, adquiridos pela rede, poderão conter cavalos de tróia, assim, evite a instalação de programas de procedência desconhecida ou duvidosa.

Estes programas de invasão, na maioria das vezes, vai possibilitar aos hacker's o controle de sua máquina. Ele poderá ver e copiar todos os seus arquivos, descobrir todas as senhas que você digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado. A idéia deste tipo de vírus é entrar em silêncio para que você não perceba e quando você descobrir ser tarde demais.

Os programas anti-vírus normalmente detectam os programas cavalos de tróia e tratam de eliminá-los; suas atualizações possibilitam a detecção dos cavalos de tróia mais recentes.

Exemplo de detecção de vírus pelo AVG



Spywares

São programas instalados no computador, sem a autorização e o conhecimento do usuário. A forma de contaminação é semelhante à do vírus, e pode acontecer quando se instala algum software ou até mesmo quando se visita algum site na internet.

Talvez a melhor descrição para spyware (espião) software de dupla personalidade. Ele reside no disco rígido de seu computador e normalmente tem um conjunto prático e atrativo de funções primárias. Essa funcionalidade principal não tem nada a ver com espionagem. Ela pode ser um utilitário, um tocador de MP3 ou algum tipo de jogo e normalmente é oferecida gratuitamente, um freeware. O problema é que, além de suas funções primárias, o spyware também tem um segundo componente menos evidente. Esse segundo componente recolhe informações sobre os seus hábitos computacionais e envia essa informação para o editor do software pela Internet. Como essa ação secundária geralmente ocorre sem o seu conhecimento, um software com esse tipo de funcionalidade dual passa a ser chamado de spyware.

Os principais sintomas destes espiões são:

- ✓ Múltiplas janelas pop-up;
- ✓ Sua caixa postal fica lotada com spams (propaganda);
- ✓ Travamentos, falhas do tipo "Operação Ilegal", etc onde a única solução é reiniciar o sistema;
- ✓ Pede acesso à Internet mesmo que você não esteja rodando nada que precise de conexão;
- ✓ Apresente sintomas como lentidão;
- ✓ Falta de memória para executar aplicativos;
- ✓ Muita atividade em disco (a luz vermelha do disco rígido, na frente do gabinete, fica muito tempo acesa);
- ✓ Acesso constante à Internet sem ter solicitado;
- ✓ "Piscadas" na tela, (alguns spywares "fotografam" o seu monitor).

Eles rodam sem nenhuma intervenção, capturando e estudando as suas URL's (endereços que você visita na internet) e após abrindo pop-ups baseadas nessas URL's específicas. Também alteram várias funções do seu browser (principalmente as configurações de segurança), mudam a página inicial, adicionam novas barras de ferramentas, etc...

Às vezes você visita um site na internet e vários pop-ups com propaganda se abrem. Então você fica irritado, pensando que esses pop-ups são do site. Podem ser, porém, o mais provável, é que os mesmos estejam sendo gerados pelos próprios Spywares instalados em sua máquina.

São também responsáveis pela facilitação de captura de endereços de e-mail, para o envio de algum tipo de spam aos usuários.

Também capturam senhas e tudo mais o que é digitado, e pode inclusive, bloquear permanentemente a sua conexão com a internet.

Embora caracterizados como Spywares, estas verdadeiras pragas digitais, também são consideradas como vírus. Entretanto, são detectados por softwares antivírus convencionais.