VÍRUS DE COMPUTADOR

O que é um vírus de computador _ Na realidade, o vírus de computador não é uma doença fisiológica que ataca disquetes e computadores, ele é um programa como outro qualquer. A maioria dos programas dos computadores visam o aumento da produtividade no ambiente de trabalho, no entanto, o objetivo dos vírus é justamente o contrário, visa a destruição de informações e a perda da produtividade. Ele guarda muitas semelhanças com o seu hormônio orgânico: ele necessita de um sistema ou programa hospedeiro; e capaz de programar-se de forma quase insuspeita; permanece por algum tempo latente; e sua ação pode variar desde ações brandas até a destruição de recursos de software/hardware do sistema onde se instala.
Apesar do grande potencial de destruição que tais programas possuem eles são responsáveis por uma porcentagem muito pequena do mau funcionamento dos computadores. Especialistas estimam que somente um em cada vinte casos de problemas atribuídos a vírus é realmente causado por um. Entretanto, o mistério que cerca este assunto leva profissionais a creditar que os vírus são capazes de realizar feitos sobrenaturais, como escrever sobre discos protegidos, ou que ele exista em discos virgens, tudo causado pela desinformação sobre este assunto.

Como funciona um vírus _ Um vírus é ativado quando executam um programa infectado, ou quando inicializamos um sistema utilizando um disquete contaminado, instalando-se na memória principal do equipamento. Quando estiver ativo, ele passa a executar duas rotinas distintas:

- Uma rotina de reprodução (ou duplicação), que procura programas e disquetes não contaminados e ao achar algum, copia nele seu código infectando-o.
- Uma rotina de atuação (ou ataque), que realiza uma função qualquer mas sempre prejudicial ao sistema. Esta função é ativada quando certa condição pré determinada for satisfeita.

Tipos de vírus mais comuns _ Muitos casos de vírus tem sido notificados ultimamente. Até o final de 1991 já haviam sido identificados mais de mil vírus em circulação, e esta número vem crescendo diariamente. Apesar de alguns dos vírus em circulação não passam de projetos de fins-de-semana de estudantes com alto conhecimento em informática e criatividade, hoje existe inúmeras variedades dos vírus mais conhecidos, que são justamente o resultado de “alterações” criadas por pessoas que se dedicaram a colecioná-los e estudá-los com a finalidade de criar um vírus realmente poderoso. Sua evolução é realmente espantosa, a inteligência e a criatividade dos programadores que os produzem só pode ser comparada com a sua irresponsabilidade. É impossível prever até onde a devastação causada por um vírus pode chegar. Mesmo os vírus lançados com fins didáticos, por autores conhecidos, são potencialmente perigosos, pois ensinam as técnicas básicas de concepção aos mal-intencionados. Infelizmente, os tipos mais comuns de vírus são os destrutivos. Com o surgimento de inúmeros utilitários para a detecção e eliminação dos primeiros casos de vírus e a sua respectiva fama adquirida, muitas pessoas de ambos os lados vieram juntar-se a esta guerra. atualmente existem tipos de vírus que afetam arquivos, o setor de **Boot** de disquetes, disco rígido e arquivos chaves do sistema operacional como, o **command.com** e a **tabela de alocação de arquivos** (**FAT**).

Alguns dos mais conhecidos são apresentados a seguir:

PAKISTANI BRAIN _ Detecção: Janeiro de 1986.

Características: Este tipo de vírus infecta o Setor de Boot de disquetes e discos rígidos, tornando-se resistente na memória do computador após a sua ativação. O Setor de Boot original do disco enfectado é salvo em setores que são marcados pelo vírus como **BAD** na **FAT** (Tabela de Alocação de Arquivos). A primeira versão deste vírus que entrou em circulação alterava o **LABEL** do disco para "(**C**) **BRAIN**", atualmente as novas versões que circulam não o fazem. Este tipo de vírus provoca o cruzamento de arquivos e por fim destrói a **FAT**. Algumas fontes afirmam tratar-se de um vírus criado como chantagem, para vender um antídoto por U$ 2.000 dólares, outras fontes afirmam que foi escrito como vingança por dois informatas pesquisadores que foram a falência por causa de cópias piratas feitas de seus programas.

CASCATA

Detecção : Outubro de 1987.

Características : infecta arquivos com as extensões .COM e .OVR. O tamanho (em bytes)dos arquivos infectados aumenta em 1.701 ou 1.704 bytes. Derruba as características alfanuméricos na última linha do monitor. Existem muitas variantes em circulação, uma delas chaga a reformatar o disco rígido. A variante -B do Cascata provoca o Boot do PC de forma aleatória, dando a impressão de um defeito de hardware.

PING-PONG

Detecção : Outubro de 1987.

Características Infecta o setor de Boot de disquetes e discos rígidos e fica residente em memória. Uma bolinha de ping-pong fica pulando na tela do monitor. A versão -B infecta também os discos rígidos conseguindo disseminar-se mundo a fora.

JERUSALÉM, ISRAELI, SEXTA-FEIRA 13

Detecção : Dezembro 1987.

Características : Infecta arquivos com as extensões .COM e .EXE aumentando seus tamanhos entre a faixa de 1.804 a 1.819 bytes. Por causa de uma "falha" de projeto, este vírus infecta os arquivos repetidamente, tornando-os tão grandes que não cabem mais na memória disponível. Trinta minutos após um programa ser infectado a velocidade do micro cai a 10% e uma janela preta aparece no quadrante inferior esquerdo da tela. Na sexta-feira 13 todos os programas que forem executados serão apagados.

STONED, MARIJUANA

Detecção : Fevereiro de 1988.

Características : Sua versão original infectava somente o Setor de Boot. As versões mais recentes infectam a Tabela de Partição de discos Rígidos tornando-os muito comuns. Aleatoriamente a mensagem "YOU PC IS NOW STONED" da Boot.

DARK AVENGER

Detecção: Setembro de 1989.

Características: Este tipo de vírus infecta arquivos com as extensões **COM** e **EXE** e **OVERLAYS.** O tamanho original do arquivo é acrescido em 1.800 BYTES. A partir do momento em que o vírus se instala na memória principal do computador, qualquer arquivo que for aberto, por qualquer motivo, é imediatamente infectado. Isto significa que um programa anti-vírus que reastreie todos os arquivos de um disco, fará com que todos estes arquivos fiquem infectados. Este é um tipo de vírus de computador muito perigoso porque após 16 arquivos infectados, ele sobregrava, aleatoriamente, setores do disco rígido, resultando em estragos nos arquivos executáveis e de dados.

JOSHI

Detecção: Janeiro de 1990.

Características: Infecta o Setor de Boot de disquetes e a Tabela de Partição dos discos rígidos, tornando-se resistente em memória quando o micro da Boot. No dia 5 de janeiro de qualquer ano o vírus provoca a exibição da mensagem "TYPE HAPPY BIRTHDAY JOSHI" travando o micro até que o usuário digite "HAPPY BIRTHDAY JOSHI". Por causa de seu projeto, os discos com formatação não padrão e disquetes de 1.2 MB podem ser destruídos.

AZUSA

Detecção: Fevereiro de 1991.

Características: Infecta o setor de Boot de disquetes e a Tabela de Partição dos Discos rígidos> Este vírus sobrecarregava a Tabela de Partição e não salva uma cópia. torna-se resistente em memória e a partir daí infecta os disquetes que são acessados para gravar um arquivo ou quando do Boot do micro. O setor de Boot original é copiado para o setor 8 da trilha 40, e se este setor estiver em uso, será sobrecarregado.

Como posso me prevenir?

Periodicamente revistas e jornais especializados publicam receitas de como evitar a contaminação por vírus de computador. hoje a maioria das empresas já sofreu algum ataque de vírus e muitas outras tem normas publicadas para regulamentar a utilização de software na empresa. Algumas delas ameaçam até com demissão qualquer funcionário que for flagrado utilizando disquetes de dados ou programas que não pertencem ao próprio estabelecimento. entretanto, muitos executivos utilizam micros em casa para atender as tarefas não completadas em horário comercial. A fiscalização sobre cópias piratas de jogos e aplicativos dificilmente se estenderá as residências dessas pessoas. Os disquetes de dados podem então fazer uma ponte entre um micro caseiro contaminado e micros da empresa> Mesmo no ambiente de trabalho, sempre aparece algum vendedor ou consultor com programas ou disquetes de dados. ele pode, sem querer, deixar com você algum vírus recolhido em outro cliente anteriormente. Porém, existem no mercado alguns bons utilitários disponíveis para o usuário leigo, que tem demonstrado eficácia na detecção, prevenção e eliminação de muitos tipos de vírus. Além destes utilitários, existem algumas medidas elementares que, se tomadas, podem minimizar a atuação destes vírus de computador. São elas:

* Manter os disquetes protegidos contra a gravação, sempre que possível.
* Realizar cópias de segurança periodicamente, a fim de retornar a um ambiente estéril caso um vírus tenha sido detectado.
* Tomar cuidado com programas novos, especialmente os e origem duvidosa, de domínio público e os obtidos através de rede.
* Colocar estes programas de quarentena até comprovar efetivamente que eles não contem vírus.
* Rodar programas novos em um ambiente restrito, verificar qualquer comportamento anormal, como o aumento de tamanho dos programas executáveis. Se possível adiantar o relógio do sistema e repetir os testes. Manter os programas novos em disquetes até ser comprovada a ausência de vírus; **NUNCA** instalar um programa novo diretamente em disco rígido. depois de rodar programas novos, desligar completamente o computador antes de executar qualquer outro programa, a fim de eliminar eventuais vírus de memória.
* Nunca utilizar a opção "**WARM START**" através de chaves de "**RESET**". É preferível desligar completamente o computador e realizar um "**COLD START**"(ligar novamente a máquina na fonte).

* Nunca trabalhar com os disquetes originais; fazer cópias de proteção contra a escrita.

* Nunca usar temporariamente disquetes emprestados ou emprestar disquetes. Caso seja necessário, **FORMATAR** os disquetes após sua devolução.

* Em sistemas de disco rígido, carregar o sistema sempre a partir deste disco. **NUNCA** realizar a carga a partir de disquetes, **PRINCIPALMENTE DISQUETES DE TERCEIROS.**

* Realizar verificações periódicas no diretório, examinando a data de criação e tamanho de arquivos. setores de **Bootstrap** podem ser verificados com editores de disco como o **Pctools** e **Norton Utilities.** Alterações nos programas em disco podem ser detectados através do controle de seus checsums, o que ser realizado **CHKDSK** do **MS-DOS.**

* Ficar atento para um comportamento anormal do sistema, como demora para carga de programas, excessiva atividade de acesso a discos, acesso inesperado a disco, mensagens de erro anormais e quedas freqüentes de sistema.

* restringir o uso do equipamento a pessoas autorizadas e tentar evitar o uso do equipamento, tais como jogos no período de almoço ou outras atividades fora do habito normal.