Vírus de Computador

O que é ?

Um vírus de computador é um programa malicioso projetado para se replicar e se espalhar de um computador para outro, causando danos ao sistema ou roubando informações. Ao contrário de programas normais, os vírus se propagam adicionando cópias de si mesmos ao código existente de outros programas ou documentos.

Finalidades

Os vírus de computador podem ter várias finalidades, incluindo a destruição de dados, interrupção de operações normais do computador, roubo de informações pessoais, espionagem ou mesmo transformar o computador em parte de uma rede de computadores controlada remotamente por hackers.

Proteção

Para proteger contra vírus, é fundamental utilizar software antivírus atualizado, manter o sistema operacional e outros programas sempre atualizados e ter cuidado ao abrir anexos de e-mails ou baixar arquivos da internet.

Hackers: Hackers são indivíduos especializados em explorar e manipular sistemas de computadores, redes e software.

Crackers: Crackers são indivíduos especializados em quebrar ou contornar medidas de segurança de software, sistemas ou redes. Ao contrário dos hackers, que podem ter motivações diversas, os crackers geralmente estão associados a atividades maliciosas, como a quebra de proteções contra cópias de software ou a violação de sistemas para roubo de informações.

Os tipos mais comuns e suas funções principais:

1. **Vírus de Boot:**
   - Atacam o setor de boot do disco rígido, sendo ativados durante a inicialização do computador. Buscam infectar o sistema operacional antes de sua carga completa, dificultando detecção e remoção.
2. **Vírus de Macro:**
   - Escritos em linguagem de macro, comumente afetam softwares como Microsoft Word ou Excel. Propagam-se ao infectar documentos e são ativados ao abrir o arquivo, podendo se replicar e contaminar outros documentos.
3. **Vírus de Arquivo ou Programa:**
   - Infectam arquivos executáveis ou programas. Ao ser executado, o programa infectado ativa o vírus, que pode se replicar e infectar outros programas. Podem causar alterações, corrupção de dados ou até exclusão de arquivos.

4. **Cavalos de Troia (Trojans):**
   - Não se replicam como vírus, mas se disfarçam de software legítimo.
   - Após instalação, executam ações maliciosas, como roubo de dados ou permitindo controle remoto do computador infectado.
5. **Worms:**
   - Auto-replicáveis, propagam-se através de redes, enviando cópias para outros sistemas.
   - Não necessitam se anexar a programas ou arquivos, podendo causar danos, consumir largura de banda e se espalhar rapidamente.
6. **Rootkits:**
   Projetados para ocultar processos ou programas, evitando detecção convencional.
   Permitem que vírus ou software malicioso permaneça indetectado, alterando o funcionamento do sistema e concedendo acesso administrativo ao atacante.
7. Ransomware:
   - Bloqueia ou restringe o acesso ao sistema, exigindo resgate para liberação.
   - Alguns tipos também criptografam arquivos, tornando-os inacessíveis até o pagamento.
8. Adware e Spyware:
   - Não são estritamente vírus, mas são softwares indesejados.
   - Adware exibe anúncios sem consentimento, enquanto o Spyware monitora atividades e coleta informações sem permissão.
9. Backdoors:
   - Criam uma "porta dos fundos" no sistema, permitindo acesso não autorizado.
   - Usadas para roubo de informações, instalação de malwares adicionais ou criação de redes de computadores infectados (botnets).

Linha do Tempo

- **1983**: O termo "Vírus de Computador" foi cunhado por Fred Cohen, doutorando em Engenharia Elétrica na Universidade do Sul da Califórnia. Len Eidelmen demonstrou um programa autoreplicante em um sistema VAX11/750, marcando um dos primeiros registros de comportamento viral em software.
- **1984**: Durante a 7ª Conferência Anual de Segurança da Informação, a definição formal de vírus de computador foi estabelecida como um programa que "infecta" outros, modificando-os para permitir a instalação de cópias de si mesmo.
- **1986:** O primeiro vírus específico para PCs, chamado Brain, foi descoberto. Pertencente à classe dos Vírus de Boot, danificava o setor de inicialização do disco rígido e se espalhava por meio de disquetes infectados. O Elk Cloner, destinado ao Apple II e criado por Rich Skrenta, foi o primeiro código malicioso documentado, estabelecendo um precedente para futuros vírus.