VÍRUS DE COMPUTADOR

O que é?

Vírus de computador são softwares maliciosos que se replicam e se disseminam, prejudicando sistemas e dispositivos. A transmissão ocorre principalmente por ações dos usuários, como download de arquivos contaminados e uso de dispositivos de armazenamento externos infectados. Sistemas operacionais desatualizados são vulneráveis a esses softwares. Existem várias categorias de vírus, cada uma com suas peculiaridades. A diversidade e complexidade dos vírus destacam a importância de práticas de segurança digital robustas, como a instalação de antivírus atualizados, realização de backups frequentes e educação dos usuários sobre riscos e medidas preventivas. A conscientização e comportamentos seguros na internet são fundamentais para minimizar os riscos de infecção e garantir a integridade dos sistemas e a privacidade dos dados.

Linha do tempo

A história dos vírus de computador começou em 1983 com Fred Cohen, que cunhou o termo "Vírus de Computador", e Len Eidelmen, que demonstrou um programa autoreplicante. Em 1984, o conceito foi formalizado na 7ª Conferência Anual de Segurança da Informação. O primeiro vírus específico para PCs, chamado Brain, surgiu em 1986 e danificava o setor de inicialização do disco rígido. No entanto, o Elk Cloner, criado por Rich Skrenta para o Apple II, foi o primeiro código malicioso documentado. A história dos vírus de computador evidencia a evolução da compreensão e resposta à ameaça desses códigos maliciosos, representando um desafio contínuo para a segurança digital.

Detecção

Atualizações Periódicas;
Ferramentas de Segurança;
Backup Regular;
Software Antivírus;
Evitar Softwares Piratas;
Cuidado com Dispositivos Removíveis;
Discernimento ao Executar Programas;

Hackers e Crackers:

Nos anos 90, jovens entusiastas da informática criavam vírus para testar os limites de propagação desses softwares. Com o tempo, o perfil desses indivíduos mudou, e os ataques cibernéticos passaram a ser realizados por pessoas com intenções criminosas, visando obter dados sensíveis para exploração ilegal ou ganho financeiro. Surgiu uma distinção entre "hackers", que exploram e identificam vulnerabilidades em sistemas por prazer intelectual, e "crackers", que usam seus conhecimentos técnicos para cometer crimes digitais. Essa distinção reflete a evolução do cenário de segurança cibernética, onde hackers contribuem para a melhoria da segurança digital, enquanto crackers representam uma ameaça à integridade dos sistemas e à privacidade dos usuários.