



Vulnerabilidades de Computador

Everson Santos Araujo

everson@por.com.br

Definição

- Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.
- Vulnerabilidades podem existir e serem conhecidas sem que sejam largamente exploradas.



BUG

- E o erro no funcionamento comum de um software, tecnicamente conhecido como falha na lógica programacional.
- O termo *bug* como defeito inexplicável é parte do jargão de engenharia a várias décadas.

Primeiro Bug de Computador

- 1945: Um inseto fica preso na relê do Mark II na Universidade de Harvard.
- A documentação se encontra hoje no Museu Nacional de História Americana do Instituto Smithsonian.



Bugs Históricos

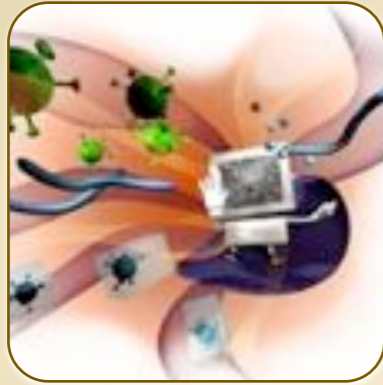
- Bug do milênio: As necessidades de economia de recursos computacionais fizeram com que muitos programas fossem escritos utilizando apenas 2 dígitos para informar o ano.
- Bug do ano 2038: Programas que utilizam a representação de tempo POSIX com sistemas de 32 bits.

Binary : 01111111 11111111 11111111 11110000

Decimal : 2147483632

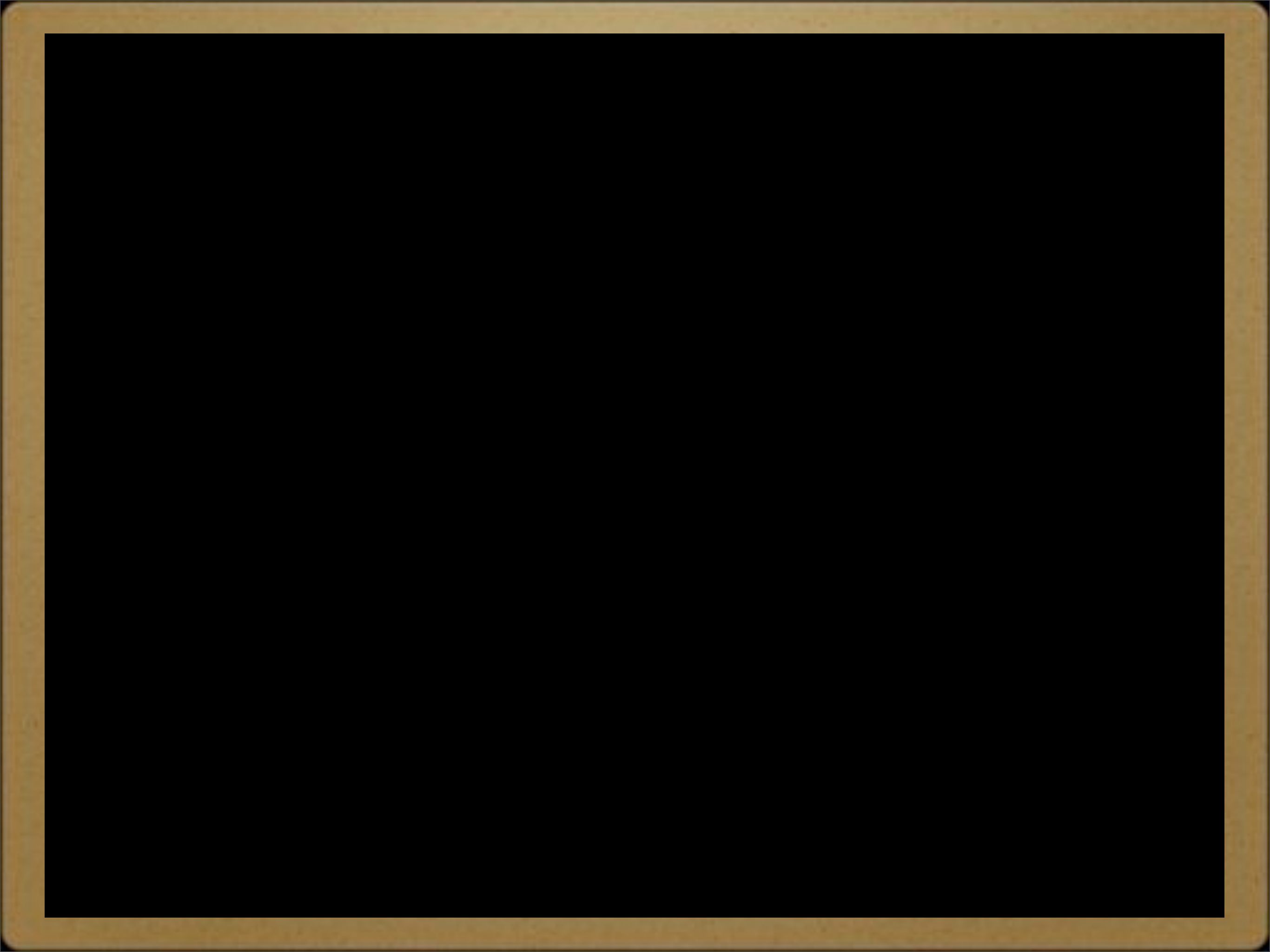
Date : 2038-01-19 03:13:52 (UTC)

Date : 2038-01-19 03:13:52 (UTC)



Códigos maliciosos

- São softwares criados para infiltrar ou danificar um sistema de computador sem consentimento de seu usuário.
- Alguns tipos de códigos maliciosos: Vírus, Worms, Trojans, Spyware, Adware desonesto.





Virus

Elk Cloner: The program with a personality

It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

It will stick to you like glue
It will modify RAM too
Send in the Cloner!

- 1982: Elk Cloner, Richard Skrenta
- 1986: Brain.A, Bassid e Amjad Farooq Alvi

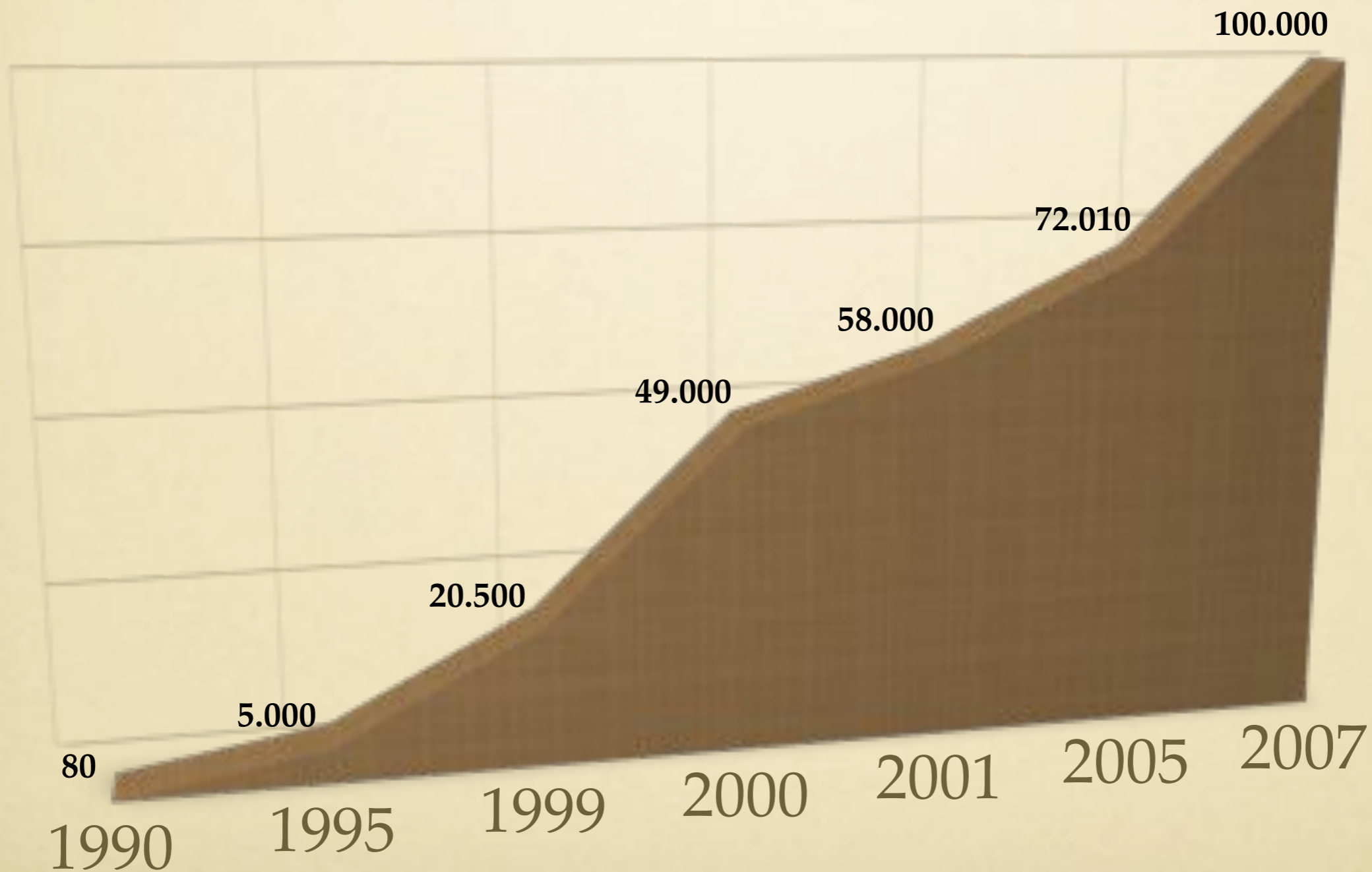
Tipos de vírus

- Vírus de Boot: Infectam a área de informações de inicialização do computador.
- Vírus de arquivos: Infectam arquivos executáveis comuns (.exe, .com) ou arquivos que executam ações em programas (macros, scripts).

Características de Vírus

- Polimorfismo: O vírus altera seu código a cada vez que é replicado para outro arquivo.
- Invisibilidade: O vírus utiliza técnicas de remoção de seu código da memória para que não possa ser identificado.
- Encriptação: Dificulta a utilização de vacinas, seu código fica mais difícil de ser identificado por completo em meio ao arquivo infectado.

Número de Vírus





Worm

- Programa autónomo que se auto-replica através da utilização de falhas de sistemas.
- Não dependem de um programa hospedeiro.
- 1988: Morris Worm, Robert T. Morris Jr
- 1999: Melissa, Word e Outlook. ExploreZip, Office.
- 2000: VBS / Loveletter, US\$ 10.000.000,00



Trojan

- Funciona como a lenda do Cavalo de Tróia, disfarçado de um programa normal esconde um programa malicioso que é executado sem o consentimento do usuário.
- Suas utilizações mais comuns são a abertura de portas para controle remoto e a captura de informações.
- Netbus, Back Orifice, Sub-7



Engenharia Social

- Práticas utilizadas para obter acesso a sistemas computacionais por meio da enganação ou exploração da confiança das pessoas.
- Exploração de falhas de segurança nas pessoas que não são treinadas contra esse tipo de ataque.
- Kevin Mitnick

